Research Journal on Business Law and Investment
پژوهشنامه حقوق کسب و کار و سرمایه گذاری

# Iran's Criminal Policy toward Cryptocurrencies with an Emphasis on the Prevention of Money Laundering in Digital Business Environments

**Mojtaba Ghoodarzi [1], Mahdi Khaghani Isfahani [2]✉ Mohammad Ali Kanaani[3]**

1. Ph.D. Student in Criminal Law and Criminology, Department of Law, International Kish Branch, Islamic Azad University, Kish Island, Iran.Email: m.goodarzi184@iau.ir

2. Assistant Professor of Criminal Law and Criminology, Department of Law, Research Institute for Humanities and Cultural Studies (SAMT), Tehran, Iran. (Corresponding Author). Email: khaghani@samt.ac.ir

3. Assistant Professor of Criminal Law and Criminology, Department of Law, Roudehen Branch, Islamic Azad University, Tehran, Iran. Email: m.kanani@riau.ac.ir

| | |
|---|---|
| **Received:** 2025-11-22 | **How to cite this article:** Ghoodarzi, M., Khaghani Isfahani, M., & Kanaani, M. A. (2026). Iran's Criminal Policy toward Cryptocurrencies with an Emphasis on the Prevention of Money Laundering in Digital Business Environments. Research Journal on Business Law and Investment, 1(2) (2): 95-115. |
| **Revised:** 2026-02-09 | |
| **Accepted:** 2026-02-12 | |
| **Available Online:** 2026-03-06 | |

## Introduction

The rapid evolution of financial technologies and the expansion of a novel phenomenon known as cryptocurrencies have posed fundamental challenges to the traditional structures of economic systems and criminal justice. Cryptocurrencies, owing to distinctive features such as decentralization, the relative anonymity of users, and the capacity for fast and cross-border transfers, while creating unprecedented economic opportunities, have also provided an attractive and complex platform for the commission of financial crimes—particularly money laundering. In this context, criminal policy—as a coordinated system of societal responses to criminality—plays a pivotal role in striking a balance between harnessing the economic benefits of this technology and controlling its criminal risks. Iran, in parallel with the expansion of cryptocurrency-related activities in areas such as electronic commerce and digital investment, is likewise in need of a reassessment of its criminal policy. Focusing on this issue, the present study examines Iran's approach in this field. The primary objective of the research is to comprehensively examine and analyze Iran's criminal policy toward cryptocurrencies and to assess its effectiveness in preventing money laundering within digital business environments. To this end, the study pursues several specific goals: analyzing the legislative, judicial, and executive dimensions of the country's criminal policy in the field of cryptocurrencies; identifying existing challenges, gaps, and deficiencies within this policy; conducting a comparative study of successful models and experiences of leading legal systems in regulating cryptocurrencies and combating digital money laundering; and ultimately proposing a conceptual framework and practical strategies to enhance Iran's criminal policy toward a preventive, intelligent, and technology-driven model.

## Method

This research adopts a descriptive–analytical and comparative approach. Data were collected through library-based and documentary methods, encompassing domestic laws and regulations (such as the Anti-Money Laundering Law and Central Bank directives), policy documents issued by relevant institutions, judicial decisions and practices, as well as official reports of supervisory authorities. In addition, reputable domestic and international academic sources in the fields of criminal law, financial criminology, and blockchain technology were utilized. In the comparative section of the study, the legal systems of the European Union, the United States of America, and Singapore were selected and analyzed as leading examples that possess explicit legal frameworks, effective enforcement experience, and significant influence on international standards. Data analysis was conducted using a legal-institutional analysis method, with a focus on the principles of criminal policy, the constituent elements of the crime of money laundering, and mechanisms of criminal and non-criminal prevention.

## Findings

The findings indicate that Iran's criminal policy toward cryptocurrencies lacks the necessary coherence, comprehensiveness, and effectiveness, and is largely reactive, fragmented, and temporary in nature. In the legislative dimension, the most significant challenge is the absence of a specific and comprehensive legal framework for defining, classifying, and regulating cryptocurrency-related activities. Existing laws, such as the Anti-Money Laundering Law, although extending their scope to "new financial instruments," do not explicitly encompass cryptocurrencies. This legislative ambiguity has resulted in the emergence of a legal "grey zone" that both increases opportunities for criminal abuse and undermines the legal certainty of legitimate actors. Moreover, policy fluctuations between prohibition and conditional acceptance (such as banning banking transactions while permitting mining activities) reflect the lack of a coherent strategy and a systematic risk-assessment approach. In the judicial dimension, the lack of specialization and uniformity of judicial practice constitutes a major challenge. The absence of specialized courts for cryptocurrency-related crimes, the unfamiliarity of many judges and experts with complex technical concepts such as blockchain, digital wallets, and on-chain transactions, and consequently divergent interpretations of the legal nature of cryptocurrencies (as property, instruments of crime, etc.) have led to prolonged proceedings, reduced accuracy of judgments, and inconsistent case law. Related cases are often adjudicated under general and traditional legal provisions that are ill-suited to the complexities of such crimes. In the executive and supervisory dimension, weak inter-institutional coordination and the lack of technological infrastructure are evident. Multiple bodies—including the Central Bank, the Cyber Police (FATA), the Anti-Money Laundering Headquarters, and the Financial Intelligence Unit—operate without effective cooperation or system-based information sharing and lack a shared strategic vision. Oversight of domestic cryptocurrency exchanges is weak, there is no clear licensing regime, and know-your-customer (KYC) requirements and suspicious transaction reporting (STR) obligations are not applied uniformly or mandatorily. Most importantly, supervisory authorities lack advanced tools for blockchain analytics and intelligent transaction tracing. By contrast, the comparative study demonstrates that leading countries have been more successful by adopting smart and preventive regulatory approaches rather than relying solely on criminalization. Examples such as the Markets in Crypto-Assets Regulation (MiCA) in the European Union, the stringent requirements of the Financial Crimes Enforcement Network (FinCEN) in the United States, and Singapore's Payment Services Act all emphasize transparency, registration and reporting obligations, mandatory digital identification for virtual asset service providers (VASPs), and the use of data analytics and artificial intelligence technologies for supervision and tracing. These approaches have significantly reduced money-laundering risks while providing a secure environment for legitimate activity and innovation.

## Conclusion

In conclusion, it can be stated that Iran's current criminal policy in the field of cryptocurrencies, due to structural weaknesses in the legislative, judicial, and executive dimensions, lacks the necessary capacity for the effective prevention of digital money laundering and remains largely reactive and ad hoc. Transitioning toward an effective, preventive, and technology-oriented criminal policy requires a fundamental transformation. This transformation necessitates the enactment of a comprehensive digital assets law that clearly defines the legal status of cryptocurrencies, supervisory requirements, AML/CFT standards, and the responsibilities of relevant institutions. Concurrently, the establishment of specialized judicial branches accompanied by extensive training for judges and law-enforcement officers, as well as the strengthening of inter-institutional coordination and equipping supervisory bodies with national smart-monitoring systems and blockchain analytics tools, are essential. Drawing on successful international experiences while taking into account domestic specificities can help Iran both to benefit from the economic opportunities of cryptocurrencies and to prevent their transformation into platforms for organized financial crime. Achieving this balance would foster sustainable alignment between the development of the digital economy and the protection of financial transparency and security in the country.

**English Keywords:** Cryptocurrency, Criminal Policy, Money Laundering Prevention, Digital Economy, Blockchain.

پژوهشنامه حقوق کسب و کار و سرمایه گذاری
Research Journal on Business Law and Investment

# سیاست جنایی ایران در قبال رمزارزها با تأکید بر پیشگیری از پولشویی در بستر کسب‌وکارهای دیجیتال

**مجتبی گودرزی [۱]، مهدی خاقانی اصفهانی [۲]✉ محمدعلی کنعانی [۳]**

۱. دانشجوی دکتری حقوق جزا و جرم‌شناسی، گروه حقوق، واحد بین‌المللی کیش، دانشگاه آزاد اسلامی، جزیره کیش، ایران. رایانامه: m.goodarzi184@iau.ir

۲. استادیار حقوق جزا و جرم‌شناسی، گروه حقوق، پژوهشکده تحقیق و توسعه علوم انسانی (سمت)، تهران، ایران. (نویسنده مسئول). رایانامه: khaghani@samt.ac.ir

۳. استادیار حقوق جزا و جرم‌شناسی، گروه حقوق، واحد رود هن، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: m.kanani@riau.ac.ir

## اطلاعات مقاله

**نوع مقاله:**
مقاله پژوهشی

**تاریخ دریافت:** ۱۴۰۴/۰۹/۰۱

**تاریخ بازنگری:** ۱۴۰۴/۱۱/۲۳

**تاریخ پذیرش:** ۱۴۰۴/۱۱/۲۳

**تاریخ انتشار:** ۱۴۰۴/۱۱/۲۳

## چکیده

تحول شتابان فناوری‌های مالی و گسترش رمزارزها، ساختار سنتی نظام‌های اقتصادی و عدالت کیفری را با چالش‌های نوینی مواجه ساخته است. رمزارزها با ویژگی‌هایی چون غیرمتمرکز بودن، ناشناسی کاربران و قابلیت انتقال فرامرزی، علاوه بر فرصت‌های اقتصادی، بستر مناسبی برای ارتکاب جرائم مالی به‌ویژه پولشویی فراهم کرده‌اند. در ایران، گسترش فعالیت‌های رمزارزی در شرایطی صورت گرفته که سیاست جنایی کشور هنوز فاقد چارچوبی جامع، هماهنگ و فناورانه برای تنظیم‌گری و پیشگیری از سوءاستفاده از این ابزارهاست. پژوهش حاضر با رویکردی توصیفی – تحلیلی و تطبیقی، به بررسی ابعاد تقنینی، قضایی و اجرایی سیاست جنایی ایران در قبال رمزارزها پرداخته و کارآمدی آن را در پیشگیری از پولشویی در بستر کسب‌وکارهای دیجیتال ارزیابی می‌کند. یافته‌ها نشان می‌دهد که خلأ قانون خاص رمزارزها، ناهماهنگی نهادی میان مراجع نظارتی و قضایی و فقدان سازوکارهای نظارت فناورانه، مانع از تحقق سیاست جنایی مؤثر شده است. در مقابل، مطالعه تطبیقی نظام‌های پیشرو مانند اتحادیه اروپا، ایالات‌متحده و سنگاپور نشان می‌دهد که بهره‌گیری از فناوری‌هایی نظیر تحلیل زنجیره بلاک‌چین، احراز هویت دیجیتال و گزارش‌دهی هوشمند تراکنش‌های مشکوک می‌تواند به طور چشمگیری احتمال بروز پولشویی رمزارزی را کاهش دهد. بر این اساس، مقاله حاضر با تأکید بر ضرورت تدوین قانون جامع دارایی‌های دیجیتال، توسعه نظارت هوشمند و هم‌افزایی نهادی، چارچوبی برای سیاست جنایی پیشگیرانه و فناورانه در ایران پیشنهاد می‌کند.

**کلیدواژه‌ها:** رمزارز، سیاست جنایی، پیشگیری از پولشویی، اقتصاد دیجیتال، بلاک‌چین.

**استناد:** گودرزی، مجتبی؛ خاقانی اصفهانی، مهدی و کنعانی، محمدعلی (۱۴۰۴). سیاست جنایی ایران در قبال رمزارزها با تأکید بر پیشگیری از پولشویی در بستر کسب‌وکارهای دیجیتال. *حقوق کسب و کار و سرمایه‌گذاری*، ۱(۲) (پیاپی ۲)، ۱۱۵-۹۵.

ناشر: دانشگاه آزاد اسلامی.

http//doi.org/10.82466/jbli.2026.1225482

## مقدمه

تحولات شتابان پدیده‌های حوزه دیجیتال در دهه‌های اخیر، چهره نظام‌های اقتصادی، حقوقی و مالی جهان را به‌گونه‌ای بنیادین دگرگون ساخته است. ظهور فناوری‌های مالی غیرمتمرکز و به‌ویژه رمزارزها، مفهوم سنتی پول، حاکمیت پولی و حتی صلاحیت قضایی را با چالش‌های نوپدیدی مواجه کرده است. رمزارزها نه صرفاً ابزار مبادله یا سرمایه‌گذاری، بلکه جلوه‌ای از «اقتصاد بدون مرز» به شمار می‌آیند که در آن قدرت کنترل دولت‌ها بر جریان مالی، به‌واسطه ناشناسی کاربران و ساختار زنجیره بلوکی، محدود می‌شود. در چنین شرایطی، سیاست جنایی – به‌عنوان نظام هماهنگ واکنش جامعه در برابر بزهکاری – ناگزیر از بازاندیشی مفهومی و نهادی است تا بتواند میان آزادی‌های اقتصادی و الزامات امنیت مالی تعادل برقرار کند.

در بستر این تحولات، رمزارزها با فراهم کردن امکان انتقال سریع، ارزان و ناشناس سرمایه، زمینه شکل‌گیری گونه‌ای جدید از جرائم مالی را مهیا ساخته‌اند که مهم‌ترین آن‌ها پدیده پولشویی رمزارزی است (رحمانی و باباجانی محمدی، ۱۴۰۰: ۳۶). این پدیده به دلیل ماهیت غیرمتمرکز و جهانی رمزارزها، موجب فروپاشی مرزهای سنتی صلاحیت کیفری و تضعیف ابزارهای نظارتی کلاسیک شده است. گزارش‌های بین‌المللی از جمله گروه ویژه اقدام مالی[1] (FATF) و صندوق بین‌المللی پول[2] (IMF) نشان می‌دهد که بخش قابل‌توجهی از تراکنش‌های رمزارزی جهان در معرض استفاده مجرمانه برای تطهیر دارایی‌ها و تأمین مالی فعالیت‌های غیرقانونی قرار دارد. در نتیجه، کشورها در سطح جهانی به سمت بازتعریف راهبردهای پیشگیرانه و فناورانه در سیاست جنایی حرکت کرده‌اند تا از تبدیل‌شدن رمزارزها به «پناهگاه امن جرم مالی» جلوگیری کنند (ادواردز[3]، ۲۰۱۹: ۶).

در ایران، هم‌زمان با گسترش استفاده از رمزارزها در حوزه تجارت الکترونیک، سرمایه‌گذاری دیجیتال و پرداخت‌های برون‌مرزی، نظام حقوقی و جنایی کشور با چالشی مضاعف روبه‌رو شده است. از یک‌سو، فرصت‌های ناشی از فناوری بلاک‌چین می‌تواند به شفافیت و توسعه اقتصاد دیجیتال یاری رساند؛ و از سوی دیگر، فقدان چارچوب قانونی شفاف و ضعف هماهنگی نهادی میان بانک مرکزی، قوه قضاییه، پلیس فتا و شورای عالی مبارزه با پولشویی، موجب شده است تا سیاست جنایی ایران در قبال رمزارزها بیشتر جنبه واکنشی و مقطعی داشته باشد تا نظام‌مند و پیشگیرانه (بهره‌مند و عامری ثانی، ۱۳۹۸: ۸۷). قانون مبارزه با پولشویی مصوب ۱۳۸۶ و اصلاحات بعدی آن هرچند دربرگیرنده مفاهیم کلی مبارزه با تطهیر دارایی‌هاست، اما به‌صراحت رمزارزها و دارایی‌های مجازی را در شمول خود نمی‌داند و همین خلأ سبب شده بسیاری از مصادیق نوین پولشویی، خارج از قلمرو نظارت مؤثر باقی بمانند (شاملو و خلیلی پاجی، ۱۳۹۹: ۱۱۲).

پژوهش حاضر با هدف بررسی کارآمدی سیاست جنایی ایران در قبال رمزارزها و نقش آن در پیشگیری از پولشویی در بستر کسب‌وکارهای دیجیتال انجام شده است. این مطالعه از حیث ماهیت، توصیفی–تحلیلی و از نظر رویکرد، تطبیقی است. داده‌ها به روش کتابخانه‌ای و از طریق مطالعه قوانین و مقررات داخلی، اسناد سیاست‌گذاری، آراء و گزارش‌های رسمی نهادهای نظارتی و منابع علمی معتبر داخلی و خارجی گردآوری شده است. در بخش تطبیقی، نظام‌های حقوقی اتحادیه اروپا، ایالات‌متحده آمریکا و سنگاپور به‌عنوان نمونه‌های پیشرو در تنظیم‌گری رمزارزها و مقابله با پولشویی دیجیتال انتخاب شده‌اند که معیار انتخاب آن‌ها، برخورداری از چارچوب قانونی صریح، تجربه اجرایی مؤثر و تأثیرگذاری در استانداردهای بین‌المللی مبارزه با پولشویی بوده است. تحلیل داده‌ها با بهره‌گیری از روش تحلیل حقوقی–نهادی و با تمرکز بر اصول سیاست جنایی، ارکان جرم پولشویی و سازوکارهای پیشگیری کیفری و غیر کیفری انجام شده و در نهایت، بر اساس یافته‌ها، چارچوبی پیشنهادی برای ارتقای سیاست جنایی ایران ارائه شده است. ایران به‌عنوان کشوری در حال گذار به اقتصاد دیجیتال، هنوز فاقد چارچوب قانونی جامع برای تنظیم‌گری رمزارزهاست. تصمیمات پراکنده بانک مرکزی، مصوبات هیئت دولت و ابلاغیه‌های شورای عالی فضای مجازی هرچند نشانه‌هایی

[1] Financial Action Task Force
[2] International Monetary Fund
[3] Edwards

از سیاست‌گذاری اولیه‌اند، اما رویکردی منسجم و هماهنگ در سطح تقنینی، قضایی و اجرایی شکل نگرفته است (خداوردی آرش، رضوی و منتظر، ۱۴۰۲: ۱۳۶). این خلأ سبب شده تا صرافی‌های رمزارزی داخلی بدون نظارت مؤثر فعالیت کرده و امکان سوءاستفاده مجرمان از این بستر افزایش یابد. به‌علاوه، شرایط خاص ایران از حیث تحریم‌های بین‌المللی و محدودیت دسترسی به‌نظام بانکی جهانی، سبب شده است تا بخشی از مبادلات مالی به‌صورت رمزارزی انجام شود. این وضعیت اگرچه می‌تواند فرصتی برای دور زدن تحریم‌ها تلقی شود، اما در صورت فقدان نظارت و شفافیت، به بستری برای گسترش جرائم مالی بدل خواهد شد ؛ لذا طراحی سیاست جنایی هوشمند که میان بهره‌برداری اقتصادی از رمزارزها و کنترل مخاطرات کیفری آن تعادل برقرار کند، ضرورتی استراتژیک است.

در ادبیات پژوهش، مطالعات متعددی به بررسی ابعاد اقتصادی، فناورانه و حقوقی رمزارزها پرداخته‌اند. در سطح داخلی، پژوهش‌هایی چون رحمانی و باباجانی محمدی، بهره‌مند و عامری ثانی و مددی و قماشی عمدتاً بر پیامدهای اقتصادی رمزارزها یا چالش‌های فنی پولشویی دیجیتال تمرکز داشته و کمتر به تحلیل منسجم سیاست جنایی در این حوزه پرداخته‌اند. برخی مطالعات نیز با رویکرد حقوق کیفری، به مسئله جرم‌انگاری یا خلأهای تقنینی رمزارزها اشاره کرده‌اند، اما اغلب فاقد تحلیل نهادی و پیشگیرانه بوده و سیاست جنایی را صرفاً به جرم‌انگاری تقلیل داده‌اند.

در ادبیات خارجی، پژوهش‌هایی مانند پژوهش ادواردز و لوی[1] و گزارش‌های FATF بیشتر بر چارچوب‌های تنظیم‌گری، نقش ارائه‌دهندگان خدمات دارایی مجازی[2] (VASPs) و سازوکارهای فناورانه مقابله با پولشویی متمرکز بوده‌اند. با این حال، این مطالعات عمدتاً ناظر به نظام‌های حقوقی توسعه‌یافته بوده و به اقتضائات خاص کشورهایی مانند ایران ـ از جمله شرایط تحریمی، ساختار نهادی متفاوت و اقتصاد نیمه‌رسمی ـ توجه نداشته‌اند.

ازاین‌رو، خلأ پژوهشی موجود ناظر بر فقدان تحلیلی است که با تلفیق سیاست جنایی، پیشگیری فناورانه و مطالعه تطبیقی، به ارزیابی منسجم سیاست جنایی ایران در قبال رمزارزها بپردازد. نوآوری پژوهش حاضر در پر کردن این خلأ و ارائه چارچوبی تحلیلی برای گذار از سیاست جنایی واکنشی به سیاست جنایی پیشگیرانه و هوشمند در بستر کسب‌وکارهای دیجیتال است.

اهمیت این تحقیق از دو جنبه نظری و عملی قابل‌توجه است. از حیث نظری، بررسی پیوند میان رمزارزها و سیاست جنایی، گامی در جهت گسترش دانش بومی در حوزه جرم‌شناسی مالی دیجیتال است؛ و از حیث عملی، یافته‌های آن می‌تواند مبنایی برای طراحی قانون جامع دارایی‌های دیجیتال و اصلاح نظام نظارتی کشور فراهم آورد. ایران به دلیل شرایط خاص تحریم‌های مالی و وابستگی نسبی به مبادلات غیررسمی، بیش از سایر کشورها نیازمند سیاست جنایی شفاف، فناورانه و پیشگیرانه در قبال رمزارزهاست. از منظر حقوقی نیز، نبود جرم‌انگاری دقیق و عدم تعیین صلاحیت قضایی روشن در پرونده‌های مرتبط با رمزارزها، اجرای عدالت کیفری را دشوار می‌سازد (مددی و قماشی، ۱۴۰۰: ۷۵).

بررسی تطبیقی تجربه نظام‌های حقوقی پیشرو مانند اتحادیه اروپا، ایالات‌متحده، ژاپن و سنگاپور نیز نشان می‌دهد که موفقیت در مهار پولشویی رمزارزی مستلزم هم‌افزایی میان فناوری، قانون و نهادهای نظارتی است.

بر این اساس، پژوهش حاضر می‌کوشد با تحلیل انتقادی سیاست جنایی ایران و تطبیق آن با الگوهای بین‌المللی، ضمن شناسایی نارسایی‌های تقنینی و نهادی، چارچوبی برای گذار از سیاست جنایی واکنشی به سیاست جنایی پیشگیرانه و هوشمند ارائه کند. این مطالعه می‌تواند به‌مثابه نقشه راهی برای قانون‌گذاران، سیاست‌گذاران اقتصادی و نهادهای نظارتی در جهت ایجاد تعادل میان توسعه اقتصاد دیجیتال و صیانت از شفافیت مالی در ایران عمل کند.

[1] Levi
[2] Virtual Asset Service Providers

## ۲. مبانی نظری و چارچوب مفهومی سیاست جنایی در حوزه رمزارزها

### ۲-۱. مفهوم و ماهیت رمزارز

مبانی نظری این پژوهش بر تلفیقی از نظریه‌های سیاست جنایی پیشگیرانه، جرم‌شناسی اقتصادی و تنظیم‌گری ریسک‌محور استوار است. بر اساس این رویکرد، پدیده‌هایی مانند رمزارزها صرفاً موضوع مداخله کیفری پسینی نیستند، بلکه نیازمند سیاست‌گذاری پیشینی، تنظیم‌گری نهادی و مدیریت ریسک‌اند. در این چارچوب، کارآمدی سیاست جنایی نه با شدت مجازات، بلکه با میزان پیشگیری، شفافیت نهادی و کاهش فرصت‌های ارتکاب جرم سنجیده می‌شود. رمزارز[1] مفهومی چندوجهی است که در مرز میان دانش فناوری اطلاعات، اقتصاد پولی و حقوق مالی شکل‌گرفته است. رمزارز در سطح فنی، رمزارز نوعی دارایی دیجیتال مبتنی بر رمزنگاری نامتقارن است که تراکنش‌های آن در بستر زنجیره بلوکی[2] و بدون نیاز به نهاد واسطه مانند بانک یا مؤسسه مالی انجام می‌شود. از دیدگاه نظریه‌های پول، رمزارزها را می‌توان نقطه عطفی در تحول مفهوم پول دانست؛ زیرا برای نخستین بار امکان انتقال ارزش را بدون دخالت قدرت حاکمیتی فراهم کرده‌اند.

در تعریف دقیق‌تر، رمزارز را می‌توان چنین توصیف کرد: «رمزارز، داده‌ای رمزنگاری شده است که با اتکا بر الگوریتم‌های اجماع و ساختار توزیع‌شده دفتر کل، ارزش اقتصادی مشخصی یافته و قابلیت مبادله در محیط‌های مجازی را داراست.» (ناکاموتو[3]، ۲۰۰۸: ۳). این ویژگی‌ها سبب شده رمزارزها به پدیده‌ای فرا سرزمینی، غیرمتمرکز و مقاوم در برابر مداخله دولت‌ها تبدیل شوند.

بنابراین، باید گفت رمزارزها نوعی دارایی دیجیتال است که بر پایه فناوری زنجیره بلوکی و نظام رمزنگاری پیشرفته شکل‌گرفته و بدون نیاز به واسطه‌های مالی رسمی، امکان انجام تراکنش‌های مالی را در بستر اینترنت فراهم می‌سازد. برخلاف پول‌های فیات که توسط بانک‌های مرکزی منتشر می‌شوند، رمزارزها ماهیتی غیرمتمرکز داشته و در قالب شبکه‌ای از نودهای (گره‌های) هم‌عرض فعالیت می‌کنند (ناکاموتو ۲۰۰۸: ۳). این ساختار، ضمن افزایش امنیت تبادل، ناشناسی کاربران را نیز تضمین می‌کند و از همین رو، قابلیت سوءاستفاده در فعالیت‌های غیرقانونی را داراست (FATF، ۲۰۱۹: ۱۲).

در نظام مالی سنتی، تراکنش‌ها به‌وسیله مؤسسات مالی و بانک‌ها انجام می‌شود که ملزم به رعایت قواعد مبارزه با پولشویی و شناسایی مشتری هستند؛ اما در فضای رمزارزها، هیچ نهاد متمرکزی برای تأیید هویت طرفین وجود ندارد. به همین دلیل، شناسایی منشأ تراکنش‌ها و کنترل جریان سرمایه دشوارتر است (عبدالهی قهفرخی و همکاران، ۱۴۰۰: ۳۹۳). افزون بر این، امکان تبدیل رمزارزها به سایر دارایی‌های دیجیتال یا ارزهای فیات از طریق صرافی‌های غیرمجاز، فرآیند ردیابی را پیچیده‌تر کرده است.

در ایران نیز رمزارزها از منظر حقوقی هنوز جایگاه مشخصی ندارند. بانک مرکزی در سال ۱۳۹۷ با صدور بخشنامه‌ای، استفاده از رمزارزها را در مبادلات بانکی ممنوع اعلام کرد، اما از سال ۱۳۹۹ به استخراج قانونی رمزارز با مجوز وزارت صمت اجازه داد. این سیاست دوگانه، خود نشانه‌ای از سردرگمی سیاست جنایی تقنینی در مواجهه با این پدیده است (خلیلی پاجی و شاملو، ۱۴۰۰: ۵۴).

در نظام پولی سنتی، انتشار و گردش پول تابع سیاست‌های پولی بانک‌های مرکزی است. در مقابل، رمزارزها فاقد پشتوانه حاکمیتی بوده و از طریق فرآیند ماینینگ (استخراج) یا صدور اولیه توسط توسعه‌دهندگان ایجاد می‌شوند. به همین سبب، از دیدگاه حقوق عمومی، رمزارزها مصداق «پول قانونی[4]» نیستند؛ اما از منظر اقتصادی، واجد کارکردهایی مشابه پول یعنی ذخیره ارزش، واحد سنجش و وسیله مبادله هستند.

---
[1] Cryptocurrency
[2] Blockchain
[3] Nakamoto
[4] Legal Tender

ساختار هم‌عرض شبکه‌های رمزارزی که در آن هزاران «نود» یا گره با یکدیگر تعامل دارند، ضامن امنیت تراکنش‌هاست. هر تراکنش، پس از تأیید در شبکه، در بلوکی ثبت می‌شود که به بلوک قبلی پیوند می‌خورد و تغییر آن بدون اجماع کل شبکه تقریباً ناممکن است. این خاصیت «تغییرناپذیری[1]» سبب اعتماد کاربران به صحت تراکنش‌ها می‌شود؛ اما از سوی دیگر، همین غیرمتمرکز بودن، به معنای فقدان نظارت نهاد حاکمیتی بر منشأ یا مقصد وجوه است؛ بنابراین، رمزارزها درعین‌حال که امنیت فنی بالایی دارند، امنیت حقوقی و مالی محدودی ایجاد می‌کنند (FATF، ۲۰۱۹: ۱۲).

## ۲-۲. رمزارز و چالش شفافیت مالی

در نظام مالی کلاسیک، تراکنش‌های پولی از مجرای بانک‌ها یا مؤسسات مالی انجام می‌شود که موظف به اجرای مقررات مبارزه با پولشویی و شناسایی هویت مشتری هستند. این نظام «مبتنی بر اعتماد نهادی» است؛ اما در فضای رمزارزها، اعتماد از نهاد به الگوریتم منتقل شده و هیچ مقام مرکزی برای احراز هویت یا نظارت وجود ندارد. به همین دلیل، شناسایی منشأ وجوه، کنترل جریان سرمایه و اعمال الزامات ضد پولشویی دشوار می‌شود (عبدالهی قهفرخی و همکاران، ۱۴۰۰: ۳۹۳)

ویژگی «شبه ناشناس بودن»[2] رمزارزها به این معنا که هویت واقعی کاربر پشت نشانی کیف پول دیجیتال پنهان است امکان رهگیری اشخاص را تقریباً از میان برده است. هرچند تمامی تراکنش‌ها در دفتر کل عمومی قابل مشاهده‌اند، اما پیوند میان نشانی و شخص حقیقی یا حقوقی تنها از طریق تحلیل پیچیده داده‌های زنجیره‌ای ممکن است. در نتیجه، رمزارزها در صورت سوءاستفاده می‌توانند ابزار مؤثری برای تطهیر دارایی‌های غیرقانونی، فرار مالیاتی و حتی تأمین مالی گروه‌های مجرمانه باشند.

افزون بر این، قابلیت تبدیل رمزارزها به سایر دارایی‌های مجازی (مانند NFTها یا توکن‌های پایدار) و نیز تبدیل سریع به ارزهای فیات از طریق صرافی‌های غیرمجاز، مسیر ردیابی تراکنش‌ها را به‌شدت پیچیده کرده است. به همین دلیل، سازمان‌های بین‌المللی چون FATF در توصیه‌های سال ۲۰۲۱ خود، ارائه‌دهندگان خدمات دارایی مجازی (VASP) را مکلف کرده‌اند فرآیندهای «احراز هویت دیجیتال» و «گزارش معاملات مشکوک» را در حوزه رمزارزها نیز اجرا کنند (FATF، ۲۰۱۹: ۸). از منظر سیاست جنایی، اهمیت ویژگی شبه ناشناس بودن رمزارزها نه در توصیف فنی آن، بلکه در تأثیر مستقیم آن بر تضعیف سازوکارهای پیشگیری پیشینی و دشوارسازی کشف جرم نهفته است. در نتیجه، هرگونه مواجهه حقوقی با پولشویی رمزارزی ناگزیر باید از سطح توصیف فناوری عبور کرده و به طراحی ابزارهای نهادی و فناورانه برای جبران این خلأ نظارتی معطوف شود.

## ۲-۳. دیدگاه حقوقی در ایران

در ایران، رمزارزها هنوز جایگاه حقوقی روشنی نیافته‌اند و قانون‌گذار در مرحله «سیاست‌گذاری موقتی و متناقض» قرار دارد. بانک مرکزی جمهوری اسلامی ایران در بخش‌نامه سال ۱۳۹۷، استفاده از رمزارزها در پرداخت‌های بانکی را ممنوع اعلام کرد، با این استدلال که ماهیت این ابزارها ناشناخته و ریسک مالی بالایی دارند؛ اما در سال ۱۳۹۹، دولت طی مصوبه‌ای استخراج رمزارز را با مجوز وزارت صنعت، معدن و تجارت قانونی کرد و حتی استفاده از رمزارز استخراج‌شده را برای واردات مجاز دانست.

این دوگانگی نشان می‌دهد که سیاست جنایی تقنینی کشور هنوز میان «ممنوعیت مطلق» و «پذیرش مشروط» در نوسان است (خلیلی پاجی و شاملو، ۱۴۰۰: ۵۴). از منظر حقوق جزا، چنین ناپایداری قانونی می‌تواند زمینه‌ساز ابهام در تعیین عنصر قانونی جرم، مسئولیت کیفری فعالان حوزه رمزارز و حتی صلاحیت مراجع قضایی شود. در غیاب تعریف قانونی از رمزارز، نمی‌توان به طور دقیق رفتارهای مجرمانه مرتبط با آن (مانند کلاهبرداری رمزارزی، پولشویی دیجیتال یا سوءاستفاده از کیف پول‌های غیرمجاز) را شناسایی و تعقیب کرد.

[1] Immutability
[2] Pseudo-Anonymity

افزون بر آن، در سیاست جنایی تقنینی ایران، ارتباط مؤثر میان نهادهای تخصصی وجود ندارد. شورای عالی فضای مجازی، بانک مرکزی، وزارت صمت و پلیس فتا هرکدام در حوزه خود مقرراتی صادر کرده‌اند، بی‌آنکه نظام واحد و جامعی برای تنظیم رفتارهای رمزارزی ایجاد شود. این پراکندگی، نه‌تنها اجرای مؤثر سیاست‌های پیشگیرانه را دشوار می‌کند، بلکه انگیزه مجرمان برای بهره‌برداری از خلأهای قانونی را نیز افزایش می‌دهد.

### ۲-۴. ماهیت دوگانه رمزارز: فرصت و تهدید

رمزارزها را نمی‌توان صرفاً به‌عنوان یک تهدید مالی و جرم‌زا تلقی کرد؛ بلکه این فناوری، در صورت تنظیم صحیح، ظرفیت بالایی برای رشد اقتصادی، جذب سرمایه و توسعه کسب‌وکارهای دیجیتال دارد. بسیاری از کشورها با بهره‌گیری از «سیاست جنایی هوشمند» توانسته‌اند میان آزادی نوآوری و کنترل مخاطرات توازن برقرار کنند.

به‌عنوان نمونه، اتحادیه اروپا با تصویب مقررات بازار دارایی‌های رمزنگاری شده (مقررات MiCA[1]، ۲۰۲۳)، چارچوبی جامع برای شناسایی، نظارت و گزارش‌دهی دارایی‌های دیجیتال ایجاد کرده است. در این نظام، هر پلتفرم رمزارزی موظف به ثبت هویت کاربران، نگهداری سوابق تراکنش و گزارش‌دهی فوری موارد مشکوک است. نتیجه این سیاست، افزایش شفافیت مالی و کاهش قابل‌توجه جرائم رمزارزی بوده است.

در مقابل، رویکرد احتیاطی ایران که مبتنی بر ممنوعیت و محدودسازی است، موجب انتقال بخش بزرگی از فعالیت‌های رمزارزی به فضای غیررسمی و خارج از نظارت شده است. ازاین‌رو، عدم تنظیم‌گری هوشمند، خود نوعی بی‌سیاستی جنایی محسوب می‌شود؛ زیرا فرصت جرم را از طریق گسترش بازار سیاه افزایش می‌دهد.

به همین خاطر رمزارزها محصول پیوند دانش رمزنگاری با نظام پولی هستند و در نتیجه، سیاست جنایی در قبال آن‌ها نمی‌تواند صرفاً مبتنی بر قواعد سنتی جرم‌انگاری باشد. ویژگی‌های خاص این پدیده از جمله غیرمتمرکز بودن، ناشناس بودن کاربران و قابلیت تراکنش‌های فرامرزی سبب می‌شود که سیاست جنایی کلاسیک کارایی خود را از دست بدهد.

در ایران، نبود تعریف قانونی و ناهماهنگی نهادی موجب شده که سیاست جنایی در مرحله «تعارف نظری» باقی بماند. تا زمانی که چارچوبی واحد برای شناسایی رمزارز به‌عنوان دارایی مشروع یا ابزار مالی طراحی نشود، مقابله با جرائم مرتبط با آن کارآمد نخواهد بود. راه‌حل، طراحی یک سیاست جنایی چندلایه است که هم جنبه‌های فناورانه (نظارت هوشمند و تحلیل داده) و هم جنبه‌های تقنینی و آموزشی را در برگیرد.

### ۲-۵. پولشویی در بستر رمزارزها

پولشویی، به‌عنوان یکی از پیچیده‌ترین جرائم مالی معاصر، فرآیندی است که طی آن درآمدهای ناشی از فعالیت‌های غیرقانونی باهدف مشروعیت‌بخشی و ادغام در اقتصاد رسمی، از مسیرهایی پیچیده عبور داده می‌شوند. در حوزه رمزارزها، این فرآیند به‌واسطه‌ی ماهیت فناورانه و ساختار غیرمتمرکز این دارایی‌ها، از سویی سهولت و سرعت بیشتری پیدا کرده و از سوی دیگر، شناسایی و ردیابی آن با چالش‌های جدی مواجه شده است (لوی، ۲۰۲۰: ۶۷). ظهور رمزارزها و دارایی‌های مجازی، چرخه سنتی پولشویی را وارد مرحله‌ای تازه کرده و آن را از شکل کلاسیک به شکل «پولشویی دیجیتال» سوق داده است؛ شکلی که در آن، جرم نه در فضای فیزیکی بلکه در بستر شبکه‌های جهانی و کیف پول‌های رمزگذاری شده انجام می‌گیرد.

رمزارزها دست‌کم سه ویژگی کلیدی دارند که آن‌ها را به ابزاری جذاب برای مجرمان مالی تبدیل می‌کند. نخست، ناشناس بودن نسبی تراکنش‌ها است. گرچه همه تراکنش‌ها در بلاک‌چین ثبت می‌شوند، اما اطلاعات هویتی اشخاص در قالب آدرس‌های رمزنگاری شده پنهان است و این امر، امکان ردیابی اشخاص حقیقی پشت تراکنش‌ها را دشوار می‌سازد. دوم، قابلیت انتقال فرامرزی

[1] Markets in Crypto-Assets Regulation

بدون نیاز به واسطه‌های بانکی است؛ انتقالی که در عرض چند دقیقه و بدون محدودیت‌های مالی بین‌المللی انجام می‌شود و عملاً از کنترل نظام‌های نظارتی ملی خارج است. سوم، امکان اختفای منشأ دارایی‌ها از طریق ابزارهایی مانند «کوین میکسرها»، «تورنادو کش‌ها» یا صرافی‌های همتا به همتا (P2P) است؛ ابزارهایی که با ترکیب یا شکستن تراکنش‌ها، منشأ واقعی وجوه را از میان می‌برند (گزارش شرکت سایفرتریس[1]، ۲۰۲۰: ۲۲)

در چرخه کلاسیک پولشویی، مرحله «جایگذاری»، «لایه‌گذاری» و «ادغام» سه رکن اصلی هستند؛ اما در فضای رمزارزها، بیشترین سوءاستفاده در مرحله لایه‌گذاری و ادغام رخ می‌دهد. در مرحله لایه‌گذاری، مجرمان با انتقال پشت سرهم رمزارز میان کیف پول‌های متعددی که غالباً روی شبکه‌های مختلف ایجاد شده‌اند، منشأ دارایی را پنهان می‌کنند. سپس در مرحله ادغام، این دارایی‌ها به‌تدریج در صرافی‌های خارجی، پلتفرم‌های فاقد نظارت یا حتی پروژه‌های مالی غیرمتمرکز (DeFi) وارد شده و به ارزهای فیات یا دارایی‌های قانونی تبدیل می‌گردند. فناوری بلاک‌چین اگرچه شفافیت تراکنش‌ها را تضمین می‌کند، اما شفافیت در سطح داده الزاماً به معنای شفافیت در سطح «هویت» نیست؛ زیرا آدرس‌ها قابل‌رؤیت‌اند، اما اشخاص پشت آدرس‌ها غالباً قابل‌تشخیص نیستند (هان، کیم و پارک[2]، ۲۰۲۰: ۵۱).

بر اساس گزارش صندوق بین‌المللی پول (IMF، ۲۰۱۹)، رمزارزها درصورتی‌که در چارچوب نظام مالی شفاف و تنظیم‌گری شده قرار گیرند، می‌توانند ابزار مؤثری برای تجارت بین‌المللی، کاهش هزینه‌های انتقال پول و تسهیل نوآوری باشند؛ اما در غیاب نظام نظارت کارآمد، همین مزایا می‌توانند به نقطه‌ضعف تبدیل شده و بستر مساعدی برای جرم سازمان‌یافته مالی، فرار مالیاتی، پولشویی و انتقال وجوه غیرقانونی فراهم کنند. این هشدار را FATF نیز بارها تکرار کرده و دولت‌ها را ملزم ساخته تا دارایی‌های مجازی را در چارچوب مقررات مبارزه با پولشویی وارد کنند.

در نتیجه، مبارزه با پولشویی در بستر رمزارزها نیازمند رویکردی چندوجهی است که ابعاد حقوقی، کیفری، اقتصادی و فناورانه را توأمان در برگیرد. از یک‌سو، باید قوانین مشخص و صریحی برای شناسایی، ثبت، نظارت و پیگیری تراکنش‌های رمزارزی تدوین شود؛ و از سوی دیگر، لازم است نهادهای نظارتی به ابزارهای تحلیل داده، ردیابی زنجیره بلوک، هوش مصنوعی و همکاری‌های بین‌المللی مجهز شوند. تحقق توازن میان «آزادی اقتصادی» که لازمه شکوفایی فناوری مالی است و «امنیت مالی»، تنها با تلفیق تنظیم‌گری هوشمند، تقویت زیرساخت‌های فنی و همکاری مستمر میان مراجع قضایی، امنیتی و مالی امکان‌پذیر خواهد بود.

## ۲-۶. مفهوم سیاست جنایی و ابعاد آن در اقتصاد دیجیتال

سیاست جنایی[3] به‌عنوان یکی از بنیادی‌ترین مفاهیم در نظام عدالت کیفری، چارچوبی علمی و راهبردی برای واکنش جامعه، قانون‌گذار و حاکمیت نسبت به پدیده جرم فراهم می‌آورد. این مفهوم «مجموعه‌ای از تدابیر تقنینی، قضایی، اجرایی و اجتماعی برای پیشگیری از جرم و اصلاح بزهکاران» است (نجفی ابرندآبادی، ۱۳۸۲: ۱۱). مارک آنسل نیز سیاست جنایی را «هنر تنظیم واکنش جامعه در برابر جرم» می‌خواند؛ هنری که باید میان حفظ آزادی‌های فردی و تأمین نظم عمومی تعادل ایجاد کند .این دو تعریف نشان می‌دهد که سیاست جنایی صرفاً مجموعه‌ای از قواعد کیفری نیست، بلکه ساختاری چندلایه است که از فلسفه حقوق کیفری، دانش جرم‌شناسی، تدابیر پلیسی، سیاست‌گذاری عمومی و الزامات اجتماعی تأثیر می‌پذیرد.

اما ورود جهان به عصر اقتصاد دیجیتال، سیاست جنایی را با چالش‌هایی بنیادین مواجه کرده است. فناوری‌های نوین – از جمله رمزارزها، بلاک‌چین، سیستم‌های مالی غیرمتمرکز (DeFi)، قراردادهای هوشمند و صرافی‌های همتا به همتا – نه‌تنها ابزارهای سنتی ارتکاب جرم را متحول کرده‌اند، بلکه شکل، ماهیت، سرعت و گستره جرائم مالی را نیز دگرگون ساخته‌اند. به همین دلیل، سیاست جنایی در این عرصه باید واجد نگاه آینده محور، فهم فناورانه، قدرت تطبیق سریع و ظرفیت تنظیم‌گری هوشمند باشد. در

[1] CipherTrace Report
[2] Han, Kim & Park
[3] Criminal Policy

حوزه رمزارزها، سیاست جنایی به معنای تنظیم مجموعه‌ای از راهبردهاست که از یک‌سو از نوآوری و رشد اقتصاد دیجیتال حمایت کند و از سوی دیگر، راه‌های سوءاستفاده مجرمان را سد نماید.

در این چارچوب، سیاست جنایی در حوزه رمزارزها سه بعد کلیدی دارد:

### الف) سیاست جنایی تقنینی: تنظیم‌گری هوشمند در فضای دارایی‌های مجازی

سیاست جنایی تقنینی، نخستین سنگ بنای حکمرانی کیفری در فضای دیجیتال است. وظیفه قانون‌گذار آن است که با تعریف دقیق مفاهیم، تعیین حدود مسئولیت‌ها و پیش‌بینی ضمانت اجراهای روشن، محیط حقوقی قابل پیش‌بینی برای فعالان اکوسیستم رمزارزها ایجاد کند. در بسیاری از نظام‌های حقوقی، قانون‌گذاران از نخستین سال‌های ظهور بیت کوین به‌ضرورت تنظیم‌گری این فضا پی برده و به‌تدریج قوانین جامعی را برای شناسایی دارایی‌های رمزارزی، ثبت فعالیت صرافی‌ها و نظارت بر تراکنش‌های مشکوک تدوین کرده‌اند (شیروی، ۱۳۹۵: ۲۹۵). در ایران، قانون مبارزه با پولشویی (۱۳۸۶ و اصلاحیه ۱۳۹۷) دامنه شمول خود را به «ابزارهای مالی نوین» گسترش داده، اما عدم اشاره صریح به رمزارزها موجب شده است تفسیر دامنه مشمول قانون، محل اختلاف محاکم و مراجع اجرایی گردد. این خلأ، عملاً سبب شده برخی رفتارهای مجرمانه در حوزه رمزارزها در قلمرو «منطقه خاکستری» قرار گیرد؛ یعنی رفتارهایی که ماهیت مجرمانه دارند؛ اما به دلیل ابهام قانونی، هم امکان پیگیری دشوار است و هم فعالان اقتصادی به طور کامل از حدود قانونی مطلع نیستند؛ بنابراین، تدوین قانون جامع دارایی‌های مجازی که بتواند وضعیت رمزارزها، صرافی‌های رمزارزی، استانداردهای احراز هویت، الزامات AML/CFT، نحوه گزارش‌دهی تراکنش‌های مشکوک و حدود دخالت نهادهای نظارتی را تعیین کند، بایسته اساسی سیاست جنایی تقنینی در ایران است. بدون چنین قانون مشخصی، فضای رمزارزها در معرض دو خطر قرار می‌گیرد:

۱. جرم‌خیزی بالا به‌واسطه نبود چهارچوب شفاف؛

۲. بی‌ثباتی حقوقی که مانع جذب سرمایه‌گذاری مشروع در اقتصاد دیجیتال می‌شود.

### ب) سیاست جنایی قضایی: تخصص‌گرایی در تفسیر و اعمال قانون

سیاست جنایی قضایی، ستون دوم واکنش اجتماعی به جرائم رمزارزی است. در مواجهه با پدیده‌ای پیچیده؛ مانند رمزارز، کارآمدی دستگاه قضایی نه‌تنها مستلزم شناخت قواعد حقوقی، بلکه نیازمند درک دقیق سازوکارهای فناورانه است. قاضی، کارشناس رسمی و ضابط قضایی باید قادر باشند کیف پول‌ها، تراکنش‌های زنجیره بلوکی، هویت‌پوشانی، میکسرها، زنجیره‌های موازی و صرافی‌های غیرمتمرکز را تحلیل کنند.

در حال حاضر، یکی از چالش‌های جدی اجرای عدالت در ایران، نبود «شعب تخصصی رمزارز» در دستگاه قضایی است. بسیاری از پرونده‌ها با مشکلاتی چون تعیین صلاحیت، نحوه احراز هویت کیف پول‌ها، تشخیص منشأ دارایی، تعیین مجرمانه بودن رفتار و تحلیل دیجیتال تراکنش‌ها مواجه می‌شوند. اختلاف‌نظر میان قضات در تفسیر رمزارز به‌عنوان «مال»، «ابزار»، «وسیله ارتکاب جرم» یا «موضوع جرم» نیز نمونه‌ای از همین چالش‌هاست (میر مجیدی، ۱۴۰۳: ۱۶۲). در کشورهای پیشرو، دادگاه‌های تخصصی جرائم سایبری یا واحدهای ویژه تحلیل بلاک‌چین در کنار دادگاه فعالیت می‌کنند. ایجاد چنین بسترهایی سبب می‌شود عدالت کیفری، سریع‌تر، دقیق‌تر و متناسب با واقعیت‌های فنی دنیای رمزارزها اعمال شود. برای ایران نیز، ایجاد شعب تخصصی قضایی، تدوین دستورالعمل‌های رسیدگی به جرائم رمزارزی و آموزش قضات، ضرورتی فوری در تحقق سیاست جنایی قضایی کارآمد است.

### پ) سیاست جنایی اجرایی: تنظیم‌گری عملیاتی و نظارت هوشمند

بعد اجرایی سیاست جنایی، نقطه‌ای است که سیاست‌ها از سطح قانون و تفسیر به مرحله عمل عینی و نظارت عملیاتی می‌رسند. نهادهایی مانند بانک مرکزی، مرکز اطلاعات مالی، پلیس فتا، وزارت اقتصاد و ستاد مبارزه با پولشویی، بازیگران اصلی این عرصه‌اند.

وظیفه آنان این است که از طریق نظارت، پایش، تحلیل داده و همکاری با صرافی‌های رمزارزی، چرخه پولشویی دیجیتال را مختل کنند (خداوردی آرش و همکاران، ۱۴۰۲: ۱۴۴).

در بسیاری از کشورها، صرافی‌ها موظف‌اند:

- اطلاعات هویتی کاربران را ثبت کنند،
- تراکنش‌های مشکوک را گزارش دهند،
- با نهادهای مالی همکاری کنند،
- از ورود آدرس‌های مرتبط با جرائم سازمان‌یافته جلوگیری کنند.

اما در ایران، سیاست جنایی اجرایی به دلیل نبود اصول مشترک نظارتی، هماهنگی نهادی و زیرساخت‌های یکپارچه با کارآمدی محدود روبه‌روست. صرافی‌های داخلی بخشی از مقررات KYC را اجرا می‌کنند، اما نه الزام قانونی فراگیر وجود دارد و نه اتصال گسترده میان آن‌ها و مرکز اطلاعات مالی برقرار است. ضعف نظارت الکترونیک و نبود بانک داده ملیِ تراکنش‌های رمزارزی، موجب شده است بسیاری از عملیات پولشویی، یا شناسایی نشوند یا دیر شناسایی شوند.

در نتیجه، سیاست جنایی اجرایی در ایران نیازمند:

- ایجاد سامانه جامع نظارت بر دارایی‌های مجازی،
- اتصال صرافی‌ها به مرکز اطلاعات مالی،
- استانداردسازی KYC وAML ،
- و استفاده از ابزارهای تحلیل بلاک‌چین است.

### ت) پیشگیری از پولشویی در بستر رمزارزها: رویکرد فناورانه سیاست جنایی نوین

سیاست جنایی نوین دیگر به واکنش کیفری پس از وقوع جرم بسنده نمی‌کند؛ بلکه بر پیشگیری پیشینی، هوشمند و فناورانه تکیه دارد (گارلند[1]، ۲۰۰۱: ۸۹). در زمینه رمزارزها، پیچیدگی فنی و سرعت گردش سرمایه موجب شده است روش‌های سنتی نظارت و مقابله با جرم کارآمد نباشند. پیشگیری مؤثر تنها زمانی محقق می‌شود که حقوق، فناوری و آموزش در کنار یکدیگر قرار گیرند.

برخی عناصر کلیدی این رویکرد عبارت‌اند از:

– **احراز هویت دیجیتال[2]:** بدون شناسایی کاربر، شناسایی منشأ دارایی ممکن نیست. تجربه جهانی نشان می‌دهد الزام صرافی‌ها به اجرای e-KYC مهم‌ترین سد پیشگیرانه در برابر سوءاستفاده مجرمان است.

[1] Garland
[2] e-KYC- Digital KYC

– **تحلیل زنجیره تراکنش‌ها**[۱]**:** شرکت‌های تخصصی تحلیل داده (مانند Chainalysis و Elliptic) با الگوریتم‌های بلاک‌چین، آدرس‌های آلوده، جریان‌های مرتبط با باج‌افزار، قمار غیرقانونی و پولشویی را شناسایی می‌کنند. استفاده از چنین ابزارهایی برای ایران ضروری است.

– **نظارت هوشمند بر ارائه‌دهندگان خدمات دارایی مجازی**[۲]**:** اجرای استانداردهای (AML/CFT)[۳] باید برای همه صرافی‌ها و پلتفرم‌های رمزارزی الزامی شود، نه اختیاری.

– **آموزش قضات و ضابطان:** درک پرونده‌های رمزارزی بدون مهارت تحلیلی ممکن نیست. کشورهای موفق، دوره‌های آموزشی گسترده برای قضات و متخصصان نظارتی برگزار کرده‌اند.

کشورهایی مانند سنگاپور و ژاپن توانسته‌اند با به‌کارگیری این تدابیر، نه‌تنها از گسترش پولشویی جلوگیری کنند بلکه بستر امنی برای فعالیت کسب‌وکارهای رمزارزی مشروع فراهم آورند (لی و کیان[۴]، ۲۰۱۶: ۴۸). این تجربه‌ها نشان می‌دهد که هم‌افزایی فناوری و حقوق، عنصر اصلی سیاست جنایی موفق در اقتصاد دیجیتال است. تجربه کشورهایی چون سنگاپور و ژاپن نشان می‌دهد که ترکیب توانمندی فناوری و چارچوب حقوقی دقیق، نه‌تنها موجب کنترل پولشویی شده، بلکه زمینه رشد سالم و شفاف کسب‌وکارهای نوآورانه را نیز فراهم کرده است.

## ۳. تحلیل انتقادی سیاست جنایی ایران در قبال رمزارزها و مقایسه با الگوهای بین‌المللی

بررسی سیاست جنایی ایران در قبال رمزارزها مستلزم توجه هم‌زمان به ابعاد تقنینی، قضایی و اجرایی است؛ چراکه ناکارآمدی در هر یک از این سطوح می‌تواند کل نظام مقابله با پولشویی دیجیتال را تضعیف کند. ازاین‌رو، در این بخش تلاش می‌شود با رویکردی تحلیلی، وضعیت موجود سیاست جنایی ایران در مواجهه با رمزارزها ارزیابی و چالش‌های اصلی آن شناسایی شود.

### ۳–۱. وضعیت سیاست جنایی تقنینی ایران در حوزه رمزارزها

وضعیت سیاست جنایی تقنینی ایران در حوزه رمزارزها بیانگر مرحله گذار، غیر منسجم و فاقد انسجام راهبردی است. در حال حاضر، هیچ قانون جامع و مستقلی که به طور مستقیم به «تعریف، طبقه‌بندی، نظارت و تنظیم فعالیت‌های رمزارزی» بپردازد، در نظام حقوقی ایران وجود ندارد. این در حالی است که از سال ۲۰۱۷ به بعد، بسیاری از کشورها قوانین مستقل برای دارایی‌های مجازی تصویب کرده‌اند و حتی FATF نیز دولت‌ها را ملزم به تعریف شفاف «Virtual Assets» و «VASPs»[۵] کرده است.

از منظر اصول بنیادین حقوق کیفری، وضعیت نامتعین رمزارزها در نظام حقوقی ایران، چالشی جدی برای اصل قانونی بودن جرم و مجازات ایجاد می‌کند. در شرایطی که ماهیت حقوقی رمزارزها، حدود فعالیت مجاز و ممنوع و مسئولیت کیفری بازیگران این حوزه به‌صورت شفاف در قانون تعریف نشده است، امکان انتساب رفتار مجرمانه با تردید مواجه می‌شود. این ابهام، نه‌تنها امنیت

---

۱ Blockchain Analytics

۲ VASPs: Virtual Asset Service Providers

۳ AML/CFT مخفف دو عبارت است:

Anti-Money Laundering:AML (مبارزه با پولشویی)

Counter-Financing of Terrorism: CFT (مبارزه با تأمین مالی تروریسم)

این اصطلاح به مجموعه قوانین، مقررات و رویه‌هایی اشاره دارد که برای کشف و جلوگیری از استفاده از سیستم مالی برای پولشویی یا تأمین مالی فعالیت‌های تروریستی طراحی شده‌اند. اقدامات KYC بخشی اساسی از یک چارچوب جامع AML/CFT محسوب می‌شود.

۴ Lee & Qian

۵ VASPs مخفف Virtual Asset Service Providersاست. این اصطلاح به شرکت‌هایی مانند صرافی‌های ارز دیجیتال و ارائه‌دهندگان کیف پول اشاره دارد که تحت مقررات AML/KYC فعالیت می‌کنند.

حقوقی فعالان اقتصادی را مخدوش می‌سازد، بلکه کارایی سیاست جنایی را نیز کاهش می‌دهد؛ زیرا سیاست کیفری مؤثر مستلزم پیش‌بینی‌پذیری و شفافیت هنجارهای الزام‌آور است.

در ایران، اگرچه قانون مبارزه با پولشویی مصوب ۱۳۸۶ و اصلاحیه ۱۳۹۷، دامنه شمول خود را به «ابزارهای مالی نوین» گسترش داده است، اما در هیچ یک از این اسناد، واژه‌های رمزارز، دارایی دیجیتال، دارایی مجازی یا ارز رمز پایه به‌صراحت ذکر نشده‌اند. همین خلأ موجب شده است که نهادهای نظارتی و قضایی در تعیین مصادیق رفتارهای مشمول قانون، با ابهام و گاه برداشت‌های متفاوت روبه‌رو شوند (شاملو و خلیلی پاجی، ۱۳۹۹: ۱۰۴). برای نمونه، برخی صرافی‌های رمزارزی مدعی‌اند که چون «رمزارز» در قانون تعریف نشده، مشمول مقررات رسمی مبارزه با پولشویی نمی‌شوند؛ حال‌آنکه نهادهای نظارتی، این دارایی‌ها را ذیل عنوان «ابزار مالی جدید» قرار می‌دهند.

بانک مرکزی در سال ۱۳۹۷ با صدور بخشنامه‌ای، استفاده از رمزارزها در تبادلات مالی رسمی کشور را ممنوع اعلام کرد، اما تنها دو سال بعد، یعنی در ۱۳۹۹، هیئت‌وزیران استفاده از رمزارزهای استخراج‌شده داخلی برای واردات کالا را مجاز دانست. این چرخش سیاستی، نشانه‌ای از عدم وجود استراتژی تقنینی منسجم، فقدان نظام ارزیابی ریسک و ناهماهنگی نهادی میان تنظیم‌کنندگان مختلف است (خلیلی پاجی و شاملو، ۱۴۰۰: ۴۲). چنین نوساناتی سبب شده فعالان اقتصادی، سرمایه‌گذاران و حتی دستگاه قضایی نتوانند تصویری روشن از حدود و ثغور فعالیت‌های مجاز و غیرمجاز در این حوزه داشته باشند.

از منظر جرم‌انگاری نیز وضعیت مشابهی دیده می‌شود. در حال حاضر، قانون‌گذار ایرانی رفتارهایی چون پنهان‌سازی منشأ دارایی‌ها از طریق رمزارز، ایجاد صرافی یا پلتفرم رمزارزی بدون مجوز، اجرای خدمات رمزارزی بدون احراز هویت مشتری، یا استفاده از ابزارهای اختفای تراکنش مانند میکسرها را به‌صورت مستقل جرم‌انگاری نکرده است. این در حالی است که در حقوق تطبیقی، چنین رفتارهایی در زمره جرائم «تسهیل پولشویی»، «اقدام علیه نظام مالی»، یا «عدم رعایت الزامات KYC/AML توسط VASPs» قرار می‌گیرند و دارای ضمانت اجراهای کیفری مشخص‌اند (تِش[1]، ۲۰۲۱: ۵۱).

فقدان قانون جامع رمزارزها در ایران صرفاً یک خلأ تقنینی ساده نیست، بلکه از منظر سیاست جنایی، به معنای تضعیف اصل پیش‌بینی‌پذیری رفتار مجرمانه و اخلال در کارکرد بازدارندگی قانون کیفری است. در چنین وضعیتی، نه فعالان اقتصادی از حدود رفتار مجاز آگاه‌اند و نه نهادهای نظارتی ابزار حقوقی لازم برای مداخله به‌موقع در چرخه پولشویی دیجیتال را در اختیار دارند. نتیجه این وضعیت، انتقال بخش قابل‌توجهی از فعالیت‌های رمزارزی به حوزه غیررسمی و افزایش جذابیت این فضا برای بزهکاران مالی است؛ امری که خود، ناکارآمدی سیاست جنایی واکنشی را آشکار می‌سازد.

### ۳-۲. چالش‌های سیاست جنایی قضایی و رویه‌های قضات

سیاست جنایی قضایی زمانی کارآمد و منسجم خواهد بود که قانون‌گذار بسترِ روشن و قابل‌اتکایی برای اعمال عدالت کیفری فراهم کرده باشد؛ اما در ایران، به دلیل فقدان قانون مستقل و شفاف در حوزه رمزارزها، دستگاه قضایی با چالش‌های جدی در تفسیر، تحلیل و رسیدگی به پرونده‌های مرتبط مواجه است. در پرونده‌های مطروحه در سال‌های اخیر، رویه‌های مختلف و گاه متعارضی شکل‌گرفته که نشان‌دهنده نبود یک الگوی ثابت برای مواجهه با رمزارزها در نظام قضایی کشور است.

در عمل، برخی مصادیق پولشویی رمزارزی در ایران شامل تبدیل عواید حاصل از جرائم اقتصادی به رمزارز از طریق صرافی‌های غیرمجاز، انتقال دارایی‌ها میان کیف پول‌های متعدد به‌منظور اختفای منشأ، استفاده از پلتفرم‌های خارجی فاقد الزاماتKYC و در نهایت تبدیل مجدد رمزارزها به پول رایج یا دارایی‌های دیجیتال دیگر است. بررسی پرونده‌های قضایی منتشرشده و گزارش‌های رسمی نهادهای نظارتی نشان می‌دهد که فقدان نظارت مؤثر بر درگاه‌های تبدیل و ضعف همکاری نهادی، نقش مهمی در تسهیل این فرآیندها داشته است. در برخی پرونده‌ها، دادگاه‌ها رمزارز را «مال» دانسته و بر این اساس، سرقت، کلاهبرداری، خیانت‌درامانت

[1] Tesch

یا تصرف غیرقانونی در رمزارزها را مشمول عناوین کیفری موجود تلقی کرده‌اند. چنین رویکردی عمدتاً بر پایه اصول کلی حقوقی و با استناد به قابلیت مبادله‌پذیری و ارزش اقتصادی رمزارزها شکل‌گرفته است؛ اما در مقابل، برخی قضات با این استدلال که رمزارز جایگاه حقوقی مشخصی در قوانین ندارد، از شمول عناوین کیفری بر رفتارهای مرتبط با رمزارز خودداری کرده‌اند و حتی برخی جرائم مالی را فاقد وصف جزایی دانسته‌اند (میر مجیدی، ۱۴۰۳: ۱۶۵). این اختلاف رویه، نتیجه مستقیم نبود تعریف قانونی از مفاهیمی چون «دارایی مجازی»، «موضوع مال»، «حق مالی» یا «ابزار الکترونیکی» در زمینه رمزارزهاست.

علاوه بر این، نبود شعب تخصصی رمزارزها در دستگاه قضایی یکی از جدی‌ترین خلأهای سیاست جنایی قضایی ایران است. جرائم رمزارزی نه‌تنها از لحاظ حقوقی پیچیده‌اند، بلکه مستلزم آشنایی عمیق با مفاهیم فنی همچون تراکنش‌های بلاک‌چینی، کیف پول‌های دیجیتال، میکسرها، قراردادهای هوشمند و تحلیل مسیر تراکنش‌هاست. بسیاری از قضات، کارشناسان رسمی و ضابطان قضایی به دلیل فقدان آموزش تخصصی در این زمینه، قادر به تحلیل دقیق عناصر مادی و معنوی این جرائم نیستند (خداوردی آرش و همکاران، ۱۴۰۲: ۱۴۶). همین موضوع موجب شده فرآیند رسیدگی طولانی‌تر شود، برخی پرونده‌ها به کارشناسی‌های متعدد ارجاع گردد و نهایتاً، دقت و قطعیت احکام کاهش یابد.

تحقق عنصر مادی پولشویی در بستر رمزارزها، برخلاف اشکال سنتی، غالباً از طریق زنجیره‌ای از رفتارهای فنی و حقوقی مانند تبدیل دارایی‌های نامشروع به رمزارز، انتقال میان کیف پول‌های متعدد، استفاده از خدمات میکسینگ و در نهایت تبدیل مجدد به پول رایج یا دارایی‌های دیجیتال دیگر صورت می‌گیرد. این فرآیند، به دلیل ماهیت فرامرزی و سرعت بالای تراکنش‌ها، امکان مداخله به‌موقع نهادهای تعقیب را محدود می‌سازد و نشان می‌دهد که اتکای صرف به سازوکارهای سنتی کشف جرم، پاسخگوی واقعیت‌های پولشویی دیجیتال نیست.

در سطح کلان سیاست‌گذاری قضایی، تاکنون دستورالعمل جامع و رسمی از سوی قوه قضاییه درباره نحوه مواجهه با پرونده‌های رمزارزی صادر نشده است. نتیجه آنکه دادسراها، دادگاه‌های کیفری و حتی مراجع تجدیدنظر، در مواجهه با پرونده‌های مشابه، رویکردهای متفاوتی اتخاذ می‌کنند. این امر نه‌تنها موجب تشتت رویه، بلکه باعث افزایش ناپایداری قضایی و کاهش پیش‌بینی‌پذیری برای فعالان اقتصادی می‌شود؛ چراکه نمی‌دانند یک رفتار معین در حوزه رمزارز در کدام وضعیت قانونی قرار دارد و چه پیامد کیفری یا مدنی به همراه خواهد داشت.

علاوه بر آن، بخش قابل‌توجهی از پرونده‌های بزرگ رمزارزی – مانند کلاهبرداری‌های گسترده، طرح‌های پانزی دیجیتال یا پولشویی در صرافی‌های غیرمجاز – به دلیل فقدان تخصص و نبود دستورالعمل‌های فنی، یا در مرحله تعقیب با بن‌بست مواجه می‌شوند یا بر اساس قوانین عمومی و سنتی مورد بررسی قرار می‌گیرند. چنین قوانینی، هرچند دارای ظرفیت کلی برای حمایت کیفری‌اند، اما پاسخگوی پیچیدگی‌های ماهوی و فنی تراکنش‌های رمزارزی نیستند.

این وضعیت، نشان می‌دهد که سیاست جنایی قضایی ایران برای مواجهه مؤثر با جرائم رمزارزی نیازمند اصلاحات ساختاری و تخصص‌گرایی نظام‌مند است. ایجاد شعب ویژه جرائم رمزارزی، تربیت کارشناسان رسمی متخصص در تحلیل بلاک‌چین، تدوین دستورالعمل‌های قضایی و آموزش گسترده برای قضات و ضابطان، پیش‌شرط‌هایی هستند که بدون تحقق آن‌ها، امکان اعمال سیاست جنایی قضایی منسجم در فضای اقتصاد دیجیتال فراهم نخواهد شد.

### ۳–۳. سیاست جنایی اجرایی و ضعف ساختاری نهادهای نظارتی

سیاست جنایی اجرایی، ستون عملیاتی سیاست جنایی است؛ جایی که قوانین و مقررات به رفتار واقعی نهادهای نظارتی، انتظامی و مالی تبدیل می‌شوند. کارآمدی این بعد، بیش از هر چیز به هماهنگی نهادی، وجود زیرساخت‌های فناورانه، استانداردهای مشترک

و انسجام عملیاتی بستگی دارد. بااین‌حال، در ایران، سیاست جنایی اجرایی در حوزه رمزارزها با مجموعه‌ای از ضعف‌های ساختاری و نهادی روبه‌روست که مانع تحقق یک نظام نظارت مؤثر بر دارایی‌های مجازی شده است.

در سطح کلان، چند نهاد مهم همچون بانک مرکزی، وزارت امور اقتصادی و دارایی، پلیس فتا، ستاد مبارزه با پولشویی و مرکز اطلاعات مالی[1] (FIU) به‌صورت پراکنده در حوزه رمزارزها فعالیت دارند؛ اما این فعالیت‌ها عمدتاً جزیره‌ای، فاقد ارتباط سامانه‌ای و بدون چشم‌انداز مشترک انجام می‌شود. بانک مرکزی، مطابق وظایف ذاتی خود، مسئول سیاست‌گذاری پولی و ارزی است، اما هنوز سامانه جامع نظارت هوشمند بر تراکنش‌های رمزارزی ایجاد نکرده و فاقد سازوکار تحلیل زنجیره بلاک‌چین است. این در حالی است که بانک‌های مرکزی کشورهای پیشرو، واحدهای ویژه «Crypto Surveillance» با ابزارهای تحلیل زنجیره‌ای پیشرفته مانند Chainalysis ایجاد کرده‌اند.

پلیس فتا نیز به‌عنوان ضابط قضایی، گرچه در سال‌های اخیر به‌صورت موردی به پرونده‌های مرتبط با کلاهبرداری‌های رمزارزی ورود کرده، اما از منظر فنی هنوز دسترسی کامل به ابزارهای ردیابی کیف پول‌ها، تحلیل تراکنش‌های بین زنجیره‌ای (Cross-chain) و شناسایی آدرس‌های آلوده را ندارد. نبود همکاری سازمان‌یافته میان پلیس فتا و بانک مرکزی یا مرکز اطلاعات مالی، موجب می‌شود شناسایی مسیرهای پول‌شویی رمزارزی با تأخیر یا با اتکا به اطلاعات ناقص انجام گیرد.

شورای عالی مبارزه با پولشویی نیز باوجود جایگاه قانونی، تاکنون استانداردهای اختصاصی برای حوزه رمزارزها تدوین نکرده است و حتی تعریفی یکپارچه از «ارائه‌دهنده خدمات دارایی مجازی» (VASP) در سطح مقررات ملی ارائه نشده است. نتیجه این خلأ، نبود چارچوب الزام‌آور برای نظارت بر صرافی‌ها، سامانه‌های رمزارزی، پلتفرم‌های همتا به همتا و کیف پول‌های تحت مدیریت شرکت‌های داخلی است (مددی و قماشی، ۱۴۰۰: ۷۳).

در این میان، بخش خصوصی رمزارزی نیز در غیاب سازوکار مجوز دهی مشخص، بدون نظارت مؤثر فعالیت می‌کند. صرافی‌های داخلی غالباً بدون اخذ مجوز از بانک مرکزی یا وزارت اقتصاد فعالیت دارند و حتی در مواردی که فرآیند احراز هویت (KYC) انجام می‌شود، استاندارد آن یکدست، دقیق و قابل نظارت نیست. برخی صرافی‌ها صرفاً اطلاعات اولیه کاربران را ثبت کرده و از هرگونه پایش الگوی تراکنش‌ها یا گزارش تراکنش‌های مشکوک (STR) خودداری می‌کنند. این وضعیت، هم احتمال وقوع پولشویی سازمان‌یافته را افزایش می‌دهد و هم اعتماد عمومی نسبت به بازار رمزارز را تضعیف می‌کند؛ چراکه کاربران در مواجهه با کلاهبرداری یا سرقت‌های رمزارزی، عملاً مرجع نظارتی مشخصی برای پیگیری ندارند.

به‌طورکلی، سیاست جنایی اجرایی ایران در حوزه رمزارزها با چهار ضعف بنیادین مواجه است:

۱. فقدان هماهنگی نهادی و نبود سامانه مشترک میان بانک مرکزی، پلیس فتا و FIU؛

۲. نبود زیرساخت‌های تحلیل بلاک‌چین و نظارت هوشمند؛

۳. عدم وجود نظام مجوز دهی و استانداردهای نظارتی برای صرافی‌های رمزارزی؛

۴. فاصله قابل‌توجه میان توان فنی نهادهای نظارتی ایران و ابزارهای پیچیده مورداستفاده مجرمان در فضای رمزارزی.

از منظر سیاست جنایی، رمزارزها نه صرفاً یک ابزار مالی نوین، بلکه یک پدیده جرم‌زا با ظرفیت‌های دوگانه هستند که می‌توانند هم در خدمت نوآوری اقتصادی و هم در خدمت جرائم مالی سازمان‌یافته قرار گیرند. ازاین‌رو، مواجهه کیفری با رمزارزها نمی‌تواند صرفاً واکنشی و پسینی باشد، بلکه مستلزم طراحی سیاست جنایی پیشگیرانه، چندلایه و متناسب با ریسک است؛ سیاستی که در آن، تنظیم‌گری هوشمند و نظارت فناورانه جایگزین مداخلات کیفری گسترده و غیر هدفمند شود.

[1] Financial Intelligence Unit

## ۴. مقایسه تطبیقی: الگوهای بین‌المللی در سیاست جنایی رمزارزها

سیاست جنایی در حوزه رمزارزها در سطح جهانی، طی دهه اخیر دچار تحولاتی بنیادین شده است. بسیاری از کشورها، با درک ماهیت فراملی، فناورانه و پیچیده این دارایی‌ها، تلاش کرده‌اند از طریق تنظیم‌گری هوشمند، هم زمینه‌های سوءاستفاده مجرمانه را کاهش دهند و هم بستر رشد نوآوری‌های مالی را فراهم سازند. بررسی تطبیقی سیاست‌های کشورهای پیشرو، معیارهایی روشن برای ارزیابی وضعیت ایران ارائه می‌دهد و می‌تواند الگوی مناسبی برای اصلاح سیاست جنایی ملی باشد. در ادامه، سه رویکرد برجسته در اتحادیه اروپا، ایالات‌متحده و چند کشور آسیایی، مورد تحلیل تطبیقی قرار می‌گیرد.

### ۴–۱. اتحادیه اروپا

در اتحادیه اروپا، تنظیم‌گری رمزارزها با تصویب «مقرره بازار دارایی‌های رمزینه» (MiCA) وارد مرحله‌ای ساختارمند شده است. این مقرره، ضمن تعریف انواع دارایی‌های رمزینه و شناسایی ارائه‌دهندگان خدمات دارایی رمزینه (CASPs)، الزامات شفافیت، ثبت، گزارش‌دهی و کنترل ریسک را بر این نهادها تحمیل کرده است. از منظر مبارزه با پولشویی، پیوند MiCA با مقررات AML اتحادیه اروپا نشان‌دهنده رویکردی پیشگیرانه و مبتنی بر تنظیم‌گری هوشمند است که به‌جای جرم‌انگاری گسترده، بر کنترل نهادی و نظارت فناورانه تمرکز دارد (کمیسیون اروپا[1]، ۲۰۲۳). در این نظام، هر صرافی رمزارزی موظف است به‌عنوان «نهاد گزارش‌دهنده» عمل کند و اطلاعات تراکنش‌ها را در پایگاه داده مشترک اتحادیه ثبت نماید. این سازوکار نه‌تنها موجب افزایش شفافیت مالی شده، بلکه امکان همکاری مؤثر میان کشورهای عضو در ردیابی جرائم مالی را فراهم آورده است.

### ۴–۲. آمریکا

در ایالات‌متحده، رویکرد مقابله با پولشویی رمزارزی عمدتاً از طریق مقررات نهادهایی چون شبکه مقابله با جرائم مالی[2] (FinCEN) و اعمال «قانون رازداری بانکی (BSA)[3]» بر ارائه‌دهندگان خدمات دارایی مجازی دنبال می‌شود. بر اساس این چارچوب، صرافی‌ها و واسطه‌های رمزارزی به‌عنوان «کسب‌وکار خدمات پولی» شناسایی شده و مکلف به اجرای الزامات شناخت مشتری (KYC) و گزارش تراکنش‌های مشکوک هستند. این رویکرد نشان‌دهنده اولویت سیاست جنایی پیشگیرانه و نظارتی بر مداخله کیفری مستقیم است (ادواردز، ۲۰۱۹: ۹۴). علاوه بر آن، همکاری میان وزارت دادگستری (DOJ) و پلیس فدرال (FBI) منجر به تشکیل «واحد مبارزه با جرائم رمزارزی» شده است که مأموریت اصلی آن ردیابی دارایی‌های دیجیتال مجرمانه است. این مدل، نمونه‌ای از هم‌افزایی نهادی در سیاست جنایی اجرایی محسوب می‌شود.

### ۴–۳. سنگاپور و ژاپن

در آسیا، کشورهای سنگاپور و ژاپن با درک اهمیت رمزارزها در اقتصاد دیجیتال، چارچوب‌های نظارتی پیشرفته‌ای تدوین کرده‌اند. سنگاپور با تصویب «قانون خدمات پرداخت[4]» در سال ۲۰۱۹ چارچوبی شفاف برای فعالیت‌های رمزارزی ایجاد کرده است. این قانون، ارائه‌دهندگان خدمات دارایی دیجیتال را تحت نظارت مستقیم نهاد پولی سنگاپور (MAS) قرار داده و الزامات سخت‌گیرانه‌ای در حوزه مبارزه با پولشویی و تأمین مالی تروریسم مقرر کرده است. تجربه سنگاپور نشان می‌دهد که تنظیم‌گری مبتنی بر مجوز دهی و نظارت مستمر می‌تواند بدون تضعیف نوآوری، ریسک‌های پولشویی رمزارزی را به‌طور مؤثری کاهش دهد. در ژاپن نیز، آژانس خدمات مالی[5] (FSA) با ایجاد سامانه نظارت بر صرافی‌ها و اجرای بازرسی‌های دوره‌ای، موفق شده است سطح جرائم رمزارزی را به میزان چشمگیری کاهش دهد (لی و کیان، ۲۰۱۶: ۴۹). مقایسه نظام‌های حقوقی یادشده نشان می‌دهد که

[1] European Commission
[2] Financial Crimes Enforcement Network
[3] Bank Secrecy Act
[4] https://www.mas.gov.sg/regulation/acts/payment-services-act
[5] Financial Services Authority

سیاست‌های موفق مقابله با پولشویی رمزارزی، بیش از آنکه متکی بر گسترش جرم‌انگاری باشند، بر تنظیم‌گری پیشگیرانه، شناسایی بازیگران کلیدی بازار و بهره‌گیری از ابزارهای فناورانه نظارت استوارند. این الگو می‌تواند مبنای بازاندیشی در سیاست جنایی ایران و گذار از رویکرد واکنشی به رویکرد پیشگیرانه و ریسک‌محور قرار گیرد.

### ۴-۴. جمع‌بندی تطبیقی

۱. به‌کارگیری فناوری‌های تحلیل داده و هوش مصنوعی در ردیابی تراکنش‌های مشکوک.

۲. هم‌افزایی نهادی میان بانک مرکزی، نهادهای مالی، پلیس و دستگاه قضایی؛

۳. الزام گزارش‌دهی تراکنش‌های مشکوک؛

۴. توازن میان حمایت از نوآوری و مقابله با جرم.

در مقایسه با این استانداردها، سیاست جنایی ایران همچنان در مرحله مقدماتی این فرآیند و واکنش‌های موردی و فاقد انسجام میان نهادهای ذی‌ربط است که نتیجه آن، افزایش مخاطرات پولشویی و کاهش اعتماد عمومی به‌نظام نظارتی است.

## ۵. نتایج و پیشنهادات

### ۵-۱. بحث و جمع‌بندی یافته‌ها

تنظیم‌گری کیفری رمزارزها در ایران باید بر اصول بنیادین حقوق کیفری از جمله اصل شفافیت، تناسب، ضرورت مداخله کیفری و تفسیر مضیق قوانین کیفری استوار باشد. مداخلات کیفری گسترده و فاقد چارچوب شفاف، نه‌تنها به کاهش پولشویی منجر نمی‌شود، بلکه می‌تواند موجب گسترش فعالیت‌های غیررسمی و کاهش همکاری فعالان مشروع بازار شود. تحلیل انجام‌شده در بخش‌های پیشین نشان داد که رمزارزها، اگرچه فرصت‌هایی بی‌بدیل برای توسعه اقتصاد دیجیتال و تسهیل مبادلات مالی فراهم می‌کنند، اما در صورت فقدان چارچوب نظارتی مناسب، می‌توانند به بستری برای ارتکاب جرائم مالی به‌ویژه پولشویی تبدیل شوند. ویژگی‌هایی همچون ناشناس بودن تراکنش‌ها، فقدان نهاد ناظر مرکزی، قابلیت انتقال فرامرزی و ابزارهای اختفای منشأ دارایی‌ها سبب شده است که رمزارزها در مرحله لایه‌گذاری و ادغام پول‌های مجرمانه نقش کلیدی ایفا کنند (تِش، ۲۰۲۱: ۴۴). در ایران، سیاست جنایی در قبال رمزارزها را می‌توان «پراکنده، موقتی و غیر منسجم» توصیف کرد. قانون‌گذار هنوز تعریف روشنی از رمزارز و جایگاه آن در نظام پولی ارائه نکرده است. در نتیجه، ابهام تقنینی باعث شده است که نهادهای اجرایی (نظیر بانک مرکزی، پلیس فتا و شورای عالی فضای مجازی) بدون هماهنگی عمل کنند.

از سوی دیگر، سیاست جنایی قضایی کشور نیز به دلیل نبود شعب تخصصی و دستورالعمل‌های جامع برای رسیدگی به جرائم رمزارزی، با چالش‌های فراوانی روبه‌رو است (خداوردی آرش و همکاران، ۱۴۰۲: ۱۳۶).

در مقابل، نظام‌های حقوقی پیشرو همچون اتحادیه اروپا، آمریکا و سنگاپور توانسته‌اند با تصویب قوانین خاص (MiCA، BSA و PSA) و الزام صرافی‌ها به احراز هویت دیجیتال (KYC) و گزارش‌دهی تراکنش‌های مشکوک، سیاست جنایی کارآمدی را در پیش بگیرند. این کشورها با بهره‌گیری از فناوری‌های نوین نظارتی، از جمله تحلیل زنجیره بلاک‌چین و الگوریتم‌های یادگیری ماشین برای شناسایی رفتارهای غیرعادی کاربران، توانسته‌اند نرخ بروز پولشویی رمزارزی را به میزان قابل‌توجهی کاهش دهند (ادواردز، ۲۰۱۹: ۸۹).

در مقایسه، یافته‌های این مقاله تأیید می‌کند که سیاست جنایی ایران در وضعیت فعلی بیشتر ماهیتی واکنشی دارد تا پیشگیرانه؛ یعنی نظام حقوقی پس از وقوع جرم وارد عمل می‌شود و فاقد سازوکارهای شناسایی و ممانعت از بروز جرم در مرحله نخست است. این امر مغایر با اصول سیاست جنایی مدرن است که بر «پیشگیری هوشمند و فناورانه» تأکید دارد (گارلند، ۲۰۰۱: ۹۲)؛ بنابراین،

برای دستیابی به سیاست جنایی کارآمد در قبال رمزارزها، ضروری است که نظام حقوقی ایران به سمت یک مدل سه سطحی از پیشگیری تقنینی، اجرایی و فناورانه حرکت کند. چنین مدلی، ضمن حفظ منافع اقتصادی رمزارزها، از تبدیل‌شدن آن‌ها به ابزار جرم اقتصادی جلوگیری خواهد کرد. لذا به‌طورکلی باید گفت که بر اساس یافته‌های پژوهش، سیاست جنایی مطلوب ایران در قبال رمزارزها می‌تواند در سه سطح طراحی شود:

نخست، سطح پیشگیرانه شامل شناسایی و نظارت بر ارائه‌دهندگان خدمات دارایی مجازی و تقویت سازوکارهای شفافیت مالی؛ دوم، سطح تنظیم‌گری نهادی با تأکید بر هماهنگی نهادهای نظارتی و بهره‌گیری از ابزارهای فناورانه؛ سوم، سطح کیفری هدفمند که مداخله کیفری را به موارد پر ریسک و سازمان‌یافته محدود می‌کند.

### ۵-۲. پیشنهادات

### الف) پیشنهادهای تقنینی

### ۱. تدوین قانون جامع دارایی‌های دیجیتال

مجلس شورای اسلامی باید قانونی مستقل تحت عنوان «قانون دارایی‌های مجازی و رمزارزها» تصویب کند که در آن مفاهیمی نظیر «رمزارز»، «صرافی دیجیتال»، «دارایی مجازی» و «خدمات رمزارزی» به‌صورت دقیق تعریف شده و جایگاه نظارتی هر نهاد مشخص شود.

### ۲. جرم‌انگاری رفتارهای خاص مرتبط با پولشویی رمزارزی

رفتارهایی چون «ایجاد یا اداره صرافی رمزارزی بدون مجوز»، «پنهان‌سازی منشأ دارایی دیجیتال»، «استفاده از کوین‌میکسرها» و «ارائه خدمات ناشناس انتقال دارایی» باید صریحاً جرم‌انگاری شوند تا از خلأ تفسیر جلوگیری گردد.

### ۳. الحاق رمزارزها به فهرست مصادیق اموال مشمول ضبط و مصادره

اصلاح ماده ۵ قانون مبارزه با پولشویی و تصریح در شمول رمزارزها در فرآیند توقیف و مصادره اموال ناشی از جرم.

### ب) پیشنهادهای قضایی



### ۱. ایجاد شعب تخصصی رمزارز در قوه قضاییه

برای رسیدگی تخصصی به جرائم مالی و رمزارزی، لازم است در هر استان یک شعبه ویژه با کارشناسان فنی بلاک‌چین تشکیل شود.

### ۲. آموزش تخصصی قضات و ضابطان قضایی

قوه قضاییه باید دوره‌های آموزش رمزارز، ردیابی دیجیتال و تحلیل بلاک‌چین را برای قضات و کارشناسان برگزار کند تا درک فنی از ادله دیجیتال ارتقا یابد.

### ۳. تدوین دستورالعمل رسیدگی به پرونده‌های رمزارزی

صدور بخش‌نامه جامع از سوی رئیس قوه قضاییه مبنی بر نحوه استعلام، توقیف و اجرای احکام مربوط به دارایی‌های رمزارزی، برای وحدت رویه ضروری است.

### ج) پیشنهادهای اجرایی و فناورانه

### ۱. ایجاد سامانه ملی نظارت بر تراکنش‌های رمزارزی

این سامانه باید تحت مدیریت بانک مرکزی و با همکاری مرکز اطلاعات مالی ایجاد شود تا امکان ردیابی تراکنش‌ها، شناسایی آدرس‌های مشکوک و تطبیق اطلاعات کاربران را فراهم کند.

### ۲. الزام صرافی‌های داخلی به رعایت استانداردهای FATF

صرافی‌های رمزارزی باید موظف شوند فرآیند احراز هویت دیجیتال (e-KYC) و گزارش تراکنش‌های مشکوک (STR) را انجام دهند.

### ۳. توسعه همکاری‌های بین‌المللی

پیوستن ایران به شبکه همکاری‌های نظارتی رمزارزی و تبادل داده با نهادهای مالی جهانی می‌تواند موجب افزایش شفافیت شود.

### ۴. توانمندسازی نهادهای نظارتی با فناوری تحلیل زنجیره‌ای

استفاده از ابزارهای هوش مصنوعی و یادگیری ماشین برای تحلیل رفتار تراکنش‌ها و شناسایی الگوهای پولشویی.

### ۵. تدوین آیین‌نامه حمایت از کسب‌وکارهای رمزارزی مشروع

برای تفکیک فعالیت‌های مجاز از غیرمجاز، باید نظام مجوز دهی شفاف برای کسب‌وکارهای رمزارزی قانونی تدوین گردد تا ضمن حمایت از نوآوری، زمینه سوءاستفاده کاهش یابد.

در خاتمه باید گفت که تحول دیجیتال، مرزهای سنتی نظام عدالت کیفری را درنوردیده و سیاست جنایی کلاسیک را با چالش‌های نوینی روبه‌رو کرده است. در چنین شرایطی، سیاست جنایی ایران ناگزیر از گذار به الگوی «هوشمند، فناورانه و پیشگیرانه» است؛ الگویی که به‌جای اتکای صرف بر جرم‌انگاری و مجازات، از ابزارهای تحلیل داده، هوش مصنوعی و همکاری نهادی برای پیشگیری از وقوع جرم بهره گیرد.

بدون قانون جامع، نظارت هوشمند و همکاری بین‌المللی، هرگونه تلاش جزئی برای مقابله با پولشویی رمزارزی ناکام خواهد ماند؛ بنابراین، پیشنهاد می‌شود سیاست‌گذاران کشور با استفاده از تجارب بین‌المللی، چارچوبی ملی برای تنظیم‌گری رمزارزها و پیشگیری از پولشویی در بستر اقتصاد دیجیتال تدوین نمایند.

به‌طورکلی می‌توان گفت که پیشنهادهای پژوهش حاضر را می‌توان به سه بازه زمانی تقسیم کرد:

**کوتاه‌مدت:** تدوین دستورالعمل‌های نظارتی برای صرافی‌های رمزارزی و تقویت الزامات گزارش‌دهی؛

**میان‌مدت:** تصویب قانون جامع رمزارزها با رویکرد تنظیم‌گری ریسک‌محور؛

**بلندمدت:** توسعه زیرساخت‌های فناورانه نظارت و ارتقای همکاری‌های بین‌المللی در حوزه مبارزه با پولشویی دیجیتال.

چنین چارچوبی می‌تواند ضمن تضمین شفافیت مالی، بستر مناسبی برای رشد سالم و قانونی بازار رمزارزها در ایران فراهم آورد و از تبدیل آن به تهدیدی برای نظام اقتصادی و عدالت کیفری جلوگیری کند.

### ملاحظات اخلاقی

نویسندگان اصول اخلاقی را در انجام و انتشار این پژوهش علمی رعایت نموده‌اند و این موضوع مورد تأیید همه آنهاست.

**تعارض منافع**

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

**حامی مالی**

این مقاله حامی مالی ندارد.

**سپاسگزاری**

از اساتید گران‌قدر دانشگاه آزاد اسلامی واحد خمینی‌شهر؛ دکتر عبداللهی، دکتر شیروی، دکتر محمودیان اصفهانی و خانم دکتر ملکی به خاطر حمایت معنوی در اجرا و انتشار پژوهش حاضر سپاسگزاری می‌شود.

از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.

## منابع

بهره‌مند، حمید و عامری ثانی، امیر کیا (۱۳۹۸). چالش‌ها و راهکارهای جرم‌یابی پولشویی از طریق ارزهای رمزنگاری شده. *مجله کارآگاه*، ۴۸(۴)، ۵۵-۷۳.

خداوردی آرش، حسین؛ رضوی، محمد و منتظر، مهدی (۱۴۰۲). آسیب‌شناسی حقوقی تنظیم‌گری دولت در حوزه رمز ارزها. *فصلنامه علمی پژوهش‌های نوین حقوق اداری*، ۵(۱۴)، ۶۷-۸۸. https://doi.org/10.22034/mral.2022.554417.1318

خلیلی پاجی، عارف و شاملو، باقر (۱۴۰۰). جرم انگاری در حوزه رمزارزها. *آموزه‌های حقوق کیفری*، ۱۸(۲۱)، ۲۹-۶۸. https://doi.org/10.30513/cld.2021.1420.1230

رحمانی، امیر و باباجانی محمدی، سعیده (۱۴۰۰). تأثیر ارزهای دیجیتال بر اقتصاد ایران، فرصت‌ها و چالش‌ها. *اکتشاف و پردازش هوشمند دانش*، ۱(۱): ۲۰-۳۳. https://doi.org/10.30508/kdip.2021.138776

شاملو، باقر و خلیلی پاجی، عارف (۱۳۹۹). چالش‌های حقوقی- اقتصادی ارزهای مجازی برای نظام‌های سیاسی در پرتو نظریه جایگزینی. *رهیافت‌های سیاسی و بین‌المللی*، ۱۲(۱)، ۱۲۵-۱۵۲.https://doi.org/10.29252/piaj.2020.100631

شیروی، عبدالحسین (۱۳۹۵). *حقوق تجارت بین‌الملل*. تهران: انتشارات سمت.

عبدالهی قهفرخی، شهیار؛ پاکزاد، بتول؛ عالی پور، حسن و الهی منش، محمدرضا (۱۴۰۰). پیشگیری از پولشویی الکترونیکی: رویکرد دفاعی و رویکرد هجومی. *پژوهش‌های حقوق جزا و جرم‌شناسی*، ۹(۱۸)، ۳۸۵-۴۰۶. https://doi.org/10.22034/jclc.2021.290298.1510

مددی، مهدی و قماشی، سعید (۱۴۰۰). جستاری در پول‌شویی از طریق ارزهای رمزنگاری شده. *مطالعات حقوق کیفری و جرم‌شناسی*، ۵۱(۲)، ۵۰۳-۵۲۱. https://doi.org/10.22059/jqclcs.2022.292559.1499

میر مجیدی، سپیده (۱۴۰۳). بررسی سیاست جنایی تقنینی و قضایی ایران در حوزه رمزارزها؛ با تأکید بر جرم اخلال در نظام اقتصادی کشور. *پژوهشنامه حقوق کیفری*، ۱۵(۲)، ۱۵۹-۱۷۲. https://doi.org/10.22124/jol.2024.27220.2465

نجفی ابرندآبادی، علی حسین (۱۳۸۲). *درآمدی بر سیاست جنایی*. تهران: انتشارات میزان.

## References

Abdollahi Ghahfarrokhi, Sh., Pakzad, B., Alipour, H., & Elahimanesh, M. R. (2021). Prevention of electronic money laundering: defensive approach and offensive approach. *Criminal Law and Criminology Research*, 9(18): 385-406. https://doi.org/10.22034/jclc.2021.290298.1510 (In Persian)

Bahremand, H., & Ameri Sani, A. K. (2019). Challenges and solutions for criminal investigation of money laundering through cryptocurrencies. *Detective Journal*, 48(4): 55-73. (In Persian)

CipherTrace. (2020). *Cryptocurrency Anti-Money Laundering Report Q2 2020*. California: CipherTrace.

Edwards, M. (2019). *Regulating Virtual Currencies and Anti-Money Laundering*. Oxford University Press.

European Commission. (2023). *Markets in Crypto-Assets Regulation (MiCA)*. Brussels.

FATF. (2019). *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Paris: FATF Secretariat.

Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford University Press.

Han, J., Kim, D., & Park, J. (2020). Blockchain Analytics for AML: Detecting Illicit Transactions. *Journal of Financial Crime*, 27(2), 49–58.

Khalili Paji, A., & Shamlou, B. (2021). Criminalization in the field of cryptocurrencies. *Criminal Law Teachings*, 18(21): 29-68. https://doi.org/10.30513/cld.2021.1420.1230 (In Persian)

Khodaverdi Arash, H., Razavi, M., & Montazer, M. (2023). Legal pathology of government regulation in the field of cryptocurrencies. *Scientific Journal of Modern Administrative Law Research*, 5(14): 67-88. https://doi.org/10.22034/mral.2022.554417.1318 (In Persian)

Lee, S., & Qian, L. (2016). Regulatory Responses to Cryptocurrency in Asia. *Singapore Journal of Legal Studies*, 44(3), 45–59.

Levi, M. (2020). Money Laundering and Digital Currencies: Challenges for the Future. *Crime, Law and Social Change*, 73(4), 65–79.

Madadi, M., & Ghamashi, S. (2021). An inquiry into money laundering through cryptocurrencies. *Criminal Law and Criminology Studies*, 51(2): 503-521. https://doi.org/10.22059/jqclcs.2022.292559.1499 (In Persian)

Mirmajidi, S. (2024). Examining Iran's legislative and judicial criminal policy in the field of cryptocurrencies; with emphasis on the crime of disrupting the country's economic system. *Criminal Law Research Journal*, 15(2): 159-172. https://doi.org/10.22124/jol.2024.27220.2465 (In Persian)

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Modern Economy*, 6(7).

Rahmani, A., & Babajani Mohammadi, S. (2021). The impact of digital currencies on Iran's economy: opportunities and challenges. *Knowledge Discovery and Intelligent Processing*, 1(1): 20-33. https://doi.org/10.30508/kdip.2021.138776 (In Persian)

Shamlou, B., & Khalili Paji, A. (2020). Legal-economic challenges of virtual currencies for political systems in light of substitution theory. *Political and International Approaches*, 12(1): 125-152. https://doi.org/10.29252/piaj.2020.100631 (In Persian)

Shiravi, A. (2016). *International Trade Law*. Tehran: Samt Publications. (In Persian)

Tesch, P. (2021). *Digital Currencies and Global Anti-Money Laundering Frameworks*. Cambridge University Press.