Studies of Islamic Jurisprudence and the Basis of Law
Online ISSN: 2783-0837 Print ISSN : 2783-2368
Homepage: fvh.journals.miu.ac.ir

Cryptocurrency Crimes and Iran's Criminal Policy: The Necessity of Transition to a Risk-Based Approach Based on "FATF Recommendations"

Seyyed Mohammad Tousi [1], Abbas Sheikholeslami [2]✉, majid shayganfard [3]

1.Ph.D Student, Department of Criminal Law and Criminology, Ma.C., Islamic Azad University, Mashhad, Iran. Email: 0944882536@iau.ac.ir
2.Associate Professor, Department of Criminal Law and Criminology, Ma.C., Islamic Azad University, Mashhad, Iran. (Corresponding author) Email: sheikholeslami@ iau.ac.ir
3.Associate Professor, Department of Criminal Law and Criminology, Ma.C., Islamic Azad University, Mashhad, Iran. Email: drshayganfard@iau.ac.ir

ضرورت گذار به رویکرد سیاست جنایی خطرمدار در جرایم رمزارزها مبتنی بر توصیه های "گروه اقدام مالی"

سید محمد طوسی[۱]، عباس شیخ الاسلامی[۲]✉، مجید شایگان فرد[۳]

۱. دانشجوی دکتری گروه حقوق جزا و جرمشناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران. رایانامه: 0944882536@iau.ac.ir

۲. دانشیار گروه حقوق جزا و جرمشناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران. (نویسنده مسئول). رایانامه: sheikholeslami@iau.ac.ir

۳. استادیار گروه حقوق جزا و جرمشناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران. رایانامه: drshayganfard@iau.ac.ir

Article Info

Article type:
Research Article

Article history:
Received

Received in revised form

Accepted

Available online

Keywords:
Risk-based criminal policy,
cryptocurrency crimes,
risk management,
FATF
Recommendation 15,
proactive supervision

Criminal Policy , Risk-Based Approach , Cryptocurrency Crimes , FATF

ABSTRACT

The rapid expansion of cryptocurrencies and blockchain technology, alongside economic opportunities and financial innovations, has created new grounds for organized financial crimes. Features such as cross-border nature, relative user anonymity, high transaction speed, and weaknesses in traditional oversight systems have made cryptocurrencies an attractive platform for money laundering, terrorist financing, cyber fraud, and related offences. In response, the Financial Action Task Force (FATF) has adopted a risk-based approach, revising its recommendations to provide a flexible, risk-assessment-driven framework for addressing virtual asset risks, most notably through Recommendation 15. This recommendation mandates virtual asset service providers to implement customer identification, report suspicious transactions, and comply with information transfer requirements, promoting proactive risk management for emerging technologies. In Iran, criminal policy regarding cryptocurrencies has shifted from complete prohibition to a risk-based approach. However, this transition encounters obstacles, including unclear laws defining cryptocurrency-related crimes, inadequate regulatory enforcement, a shortage of judicial understanding of blockchain analysis, tension between Islamic law's acceptance and legal requirements, and constrained international collaboration due to sanctions. This descriptive-analytical study, drawing on international documents and domestic sources, examines the dimensions of risk-based criminal policy in confronting cryptocurrency-related crimes. Iran's legal framework is analyzed, shortcomings and challenges are elucidated, and selected international experiences in regulation and criminal response are assessed. Findings indicate that the absence of a coherent risk-assessment framework in Iran's criminal law, combined with institutional and legislative opacity in the cryptocurrency domain, has diminished the effectiveness of criminal policy in preventing and combating related offences. The study concludes by stressing the need to shift from reactive, traditional approaches to a risk-based criminal policy. It proposes solutions for designing a localized model aligned with international standards.

Cite this article: Last Name, Initial. , Last Name, Initial. , & Last Name, Initial. (2025). Title of the paper: All words in the title should be in lowercase (except for the first letter of the title and any nouns, initial letter of first word, initial of first word after a colon, and proper nouns). *Studies of Islamic Jurisprudence and Basis of Law, 19*(X). http//doi. org/000000000000000000

DOI: http//doi. org/000000000000000000

مطالعات فقه اسلامی و مبانی حقوق
شاپا برخط: ۰۸۳۷-۲۷۸۳ شاپا چاپی: ۲۳۶۸-۲۷۸۳
Homepage: fvh.journals.miu.ac.ir

ضرورت گذار به رویکرد سیاست جنایی خطرمدار در جرایم رمزارزها مبتنی بر توصیه‌های «گروه ویژه اقدام مالی»

Cryptocurrency Crimes and Iran's Criminal Policy: The Necessity of Transition to a Risk-Based Approach Based on "FATF Recommendations"

Seyyed Mohammad Tousi [1], Abbas Sheikholeslami [2]✉, majid shayganfard [3]

1.Ph.D Student, Department of Criminal Law and Criminology, Ma.C., Islamic Azad University, Mashhad, Iran. Email: 0944882536@iau.ac.ir
2.Associate Professor, Department of Criminal Law and Criminology, Ma.C., Islamic Azad University, Mashhad, Iran. (Corresponding author) Email: sheikholeslami@ iau.ac.ir
3.Associate Professor, Department of Criminal Law and Criminology, Ma.C., Islamic Azad University, Mashhad, Iran. Email: drshayganfard@iau.ac.ir

ضرورت گذار به رویکرد سیاست جنایی خطرمدار در جرایم رمزارزها مبتنی بر توصیه های "گروه اقدام مالی"

سید محمد طوسی[۱]، عباس شیخ الاسلامی[۲]✉، مجید شایگان فرد[۳]

۱. دانشجوی دکتری گروه حقوق جزا و جرمشناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران. رایانامه: 0944882536@iau.ac.ir

۲. دانشیار گروه حقوق جزا و جرمشناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران. (نویسنده مسئول). رایانامه: sheikholeslami@iau.ac.ir

۳. استادیار گروه حقوق جزا و جرمشناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران. رایانامه: drshayganfard@iau.ac.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخچه مقاله:
تاریخ دریافت:
تاریخ بازنگری:
تاریخ پذیرش:
تاریخ انتشار:

کلیدواژه‌ها:
سیاست جنایی خطرمدار، جرایم رمزارزی، مدیریت ریسک، توصیه ۱۵ گروه ویژه اقدام مالی (FATF)، نظارت پیش‌دستانه.

سیاست جنایی، رویکرد خطرمدار، جرایم رمزارز، FATF

چکیده

گسترش رمزارزها و بلاک‌چین، علاوه بر فرصت‌های اقتصادی، زمینه‌های جدیدی برای جرایم مالی سازمان‌یافته فراهم کرده است. ویژگی‌های فرامرزی، ناشناسی نسبی، سرعت بالا و ضعف نظارت سنتی، رمزارزها را به بستری جذاب برای پولشویی، تأمین مالی تروریسم، کلاهبرداری سایبری و جرایم مرتبط تبدیل کرده است. گروه ویژه اقدام مالی (FATF) با رویکرد خطرمدار، چارچوب انعطاف‌پذیری مبتنی بر ارزیابی ریسک ارائه داده که در توصیه ۱۵ نمود بارز دارد. این توصیه، ارائه‌دهندگان خدمات دارایی مجازی را ملزم به شناخت مشتری، گزارش تراکنش‌های مشکوک و رعایت قاعده انتقال اطلاعات می‌کند و پیشگیری پیش‌دستانه را پیشنهاد می‌دهد. در ایران، سیاست جنایی از ممنوعیت مطلق به رویکرد نیمه‌خطرمدار گذار کرده، اما با چالش‌های جدی مواجه است: خلأهای تقنینی، ضعف نظارت اجرایی، عدم تخصص قضایی در قضایی در ردیابی بلاک‌چین، تعارض اباحه‌گری فقهی و محدودیت همکاری فراملی ناشی از تحریم‌ها. این پژوهش پژوهش حاضر، با بهره‌گیری از اسناد بین‌المللی و منابع داخلی، ابعاد سیاست جنایی خطرمدار در برابر جرایم رمزارزی را بررسی می‌کند. وضعیت ایران تحلیل شده، کاستی‌ها تبیین گردیده است. سؤال اصلی پژوهش این است: سیاست جنایی ایران تا چه حد با الزامات رویکرد خطرمدار همخوانی دارد و چه اصلاحاتی برای گذار کامل به این رویکرد لازم است؟

یافته‌ها نشان می‌دهد فقدان چارچوب منسجم مبتنی بر ارزیابی ریسک در حقوق کیفری ایران، همراه با عدم شفافیت نهادی و تقنینی، کارایی سیاست جنایی را کاهش داده است.

استناد: نام خانوادگی، نام؛ نام خانوادگی، نام؛ و نام خانوادگی، نام (۱۴۰۴). عنوان مقاله.. *مطالعات فقه اسلامی و مبانی حقوق*، ۱۹ (X).
http//doi. org/000000000000000000

مقدمه

در دهه‌های اخیر، گسترش فناوری‌های دیجیتال تحولات عمیقی در ساختارهای اقتصادی، اجتماعی و حقوقی جوامع ایجاد کرده است. ظهور پدیده‌هایی نظیر تجارت الکترونیک، بانکداری دیجیتال، سکوهای برخط سکوهای برخط خدمات مالی و هوش مصنوعی، نه‌تنها شیوه‌های سنتی تعامل و مبادله را دگرگون ساخته، بلکه نظام‌های حقوقی و سیاست‌گذاری کیفری را نیز با چالش‌های نوینی مواجه کرده است. در این میان، رمزارزها به‌عنوان یکی از شاخص‌ترین دستاوردهای فناوری‌های نوظهور، توجه گسترده قانون‌گذاران، نهادهای نظارتی و پژوهشگران حقوقی را به خود جلب کرده‌اند.

رمزارزها نخستین‌بار با معرفی بیت‌کوین در سال ۲۰۰۸ و بر پایه فناوری بلاک‌چین مطرح شدند. این فناوری با ایجاد یک دفتر کل توزیع‌شده و غیرمتمرکز، امکان ثبت و تأیید تراکنش‌ها را بدون نیاز به نهادهای واسط فراهم می‌کند. استفاده از الگوریتم‌های اجماع، رمزنگاری پیشرفته و ساختار غیرقابل‌تغییر داده‌ها، سبب شده است که این نظام مالی نوین از بسیاری جهات با نظام‌های پولی و بانکی سنتی متفاوت باشد. ویژگی‌هایی همچون غیرمتمرکز بودن، ناشناسی نسبی کاربران، ماهیت فرامرزی تراکنش‌ها، سرعت بالا و هزینه پایین انتقال ارزش، رمزارزها را به ابزاری جذاب برای مبادلات مالی در سطح جهانی تبدیل کرده است (خضری نیا، ۱۴۰۳، صص. ۲۷-۳۲).

این ویژگی‌ها، از یک سو، ظرفیت‌های قابل توجهی برای نوآوری اقتصادی و توسعه بازارهای مالی ایجاد کرده‌اند. امکان انجام مبادلات مستقیم، کاهش وابستگی به نظام‌های بانکی بین‌المللی و تسهیل دسترسی به بازارهای جهانی، به‌ویژه برای کشورهایی که با محدودیت‌های اقتصادی یا تحریم‌های مالی مواجه‌اند، از جمله مزایای مهم رمزارزها به شمار می‌رود.

در مقابل، همین ویژگی‌ها بستر مناسبی برای بروز و گسترش انواع جدیدی از بزهکاری نیز فراهم کرده‌اند. ناشناسی نسبی، فرامرزی بودن و دشواری نظارت بر تراکنش‌ها، رمزارزها را به ابزاری جذاب برای ارتکاب جرایمی نظیر پولشویی، کلاهبرداری‌های سایبری، فرار مالیاتی و تأمین مالی فعالیت‌های مجرمانه سازمان‌یافته و غیره، تبدیل کرده است. به این ترتیب، جرایم مرتبط با رمزارزها اغلب ماهیتی پیچیده، شبکه‌ای و فراملی یافته‌اند (احمدپور و علوی رضوی، ۱۴۰۲، صص. ۵۷۰-۵۶۹).

در ایران، مواجهه با رمزارزها در بستر شرایط خاص اقتصادی، سیاسی و حقوقی کشور، ابعاد پیچیده‌تری یافته است. از یک سو، محدودیت‌های ناشی از تحریم‌های بین‌المللی و مشکلات ساختاری نظام بانکی، توجه به ظرفیت‌های رمزارزها را به‌عنوان ابزاری برای تسهیل مبادلات مالی افزایش داده است. از سوی دیگر، فقدان چارچوب قانونی جامع و منسجم، زمینه بروز مخاطرات جدی در حوزه جرایم اقتصادی مرتبط با رمزارزها را فراهم کرده و مقابله با این پدیده را فراتر از چارچوب‌های سنتی سیاست جنایی کرده است (Faghih, Barzegarzadeh & Safaei, 2025, pp. 1–10). به گونه‌ای که افزایش

کلاهبرداری‌های مبتنی بر پلتفرم‌های سکوهای برخط جعلی، سوءاستفاده از استخراج غیرمجاز و دشواری ردیابی جریان‌های مالی مشکوک، از جمله چالش‌هایی است که ضرورت بازاندیشی در سیاست جنایی این حوزه را برجسته می‌سازد.

بررسی پیشینه پژوهشی سیاست جنایی رمزارزها نشان می‌دهد که رویکرد غالب در سطح جهانی، از سیاست‌های مبتنی بر ممنوعیت مطلق به سمت الگوهای واقع‌گرایانه و خطرمدار حرکت کرده است. مطالعات اولیه عمدتاً بر چالش‌های فنی و ابهامات حقوقی رمزارزها تمرکز داشتند، اما با گسترش استفاده از این ابزارها و افزایش مخاطرات کیفری، توجه پژوهش‌ها به مدیریت ریسک و پیشگیری پیش‌دستانه معطوف شده است. در ایران نیز با وجود رشد سریع بازار رمزارزها، همچنان خلأ تقنینی محسوسی مشاهده می‌شود و بخش قابل توجهی از پژوهش‌ها ماهیتی توصیفی دارند و کمتر به ارائه مدل‌های بومی و اجرایی پرداخته‌اند. این خلأ پژوهشی، ضرورت بررسی عمیق‌تر و ارائه راهکارهای عملی برای گذار به رویکرد خطرمدار را در سیاست جنایی ایران بیش از پیش آشکار می‌سازد.

سیاست جنایی ایران در قبال رمزارزها تاکنون مسیری تدریجی و بعضاً متناقض را طی کرده است. در مراحل ابتدایی، رویکردی مبتنی بر احتیاط و ممنوعیت اتخاذ شد که بیشتر بر نگرانی‌های پولی، ارزی و امنیتی استوار بود. با این حال، به‌تدریج و همزمان با درک برخی ظرفیت‌های اقتصادی رمزارزها، به‌ویژه در حوزه استخراج، سیاست‌گذاری‌ها به سمت پذیرش محدود و تنظیم‌گری حداقلی حرکت کرده‌اند. این تحول اگرچه نشان‌دهنده نوعی واقع‌گرایی در مواجهه با فناوری‌های نوین است، اما همچنان از منظر مدیریت ریسک‌های جرم‌زا، با کاستی‌های جدی مواجه است (میرمجیدی، ۱۴۰۳، صص. ۱۶۰–۱۶۳).

یکی از مهم‌ترین نقدها به سیاست جنایی موجود در ایران آن است که این سیاست، علی‌رغم پذیرش برخی ظرفیت‌های اقتصادی رمزارزها، همچنان ماهیتی واکنشی دارد و فاقد مکانیزم‌های پیشگیرانه و مدیریت ریسک نظام‌مند است. به‌گونه‌ای که تأکید اصلی در سیاست‌گذاری‌ها بر جنبه‌های اقتصادی مانند صدور مجوز استخراج بوده و سازوکارهای مؤثر برای شناسایی و ارزیابی ریسک، نظارت پیش‌دستانه بر تراکنش‌ها، الزام به شفافیت مالی و همکاری نهادی در مقابله با جرایم رمزارزی، کمتر مورد توجه قرار گرفته‌اند، حال آن‌که فقدان این ابزارها موجب ضعف کارآمدی سیاست جنایی در مواجهه با تهدیدات مربوط به رمزارزها شده است (Ghaemi Asl, Abolhasani & Farhoud, 2025, pp. 1–11).

در ادبیات سیاست جنایی معاصر، رویکرد خطرمدار به‌عنوان یکی از کارآمدترین الگوها برای مواجهه با جرایم نوظهور مطرح شده است. این رویکرد به‌جای تمرکز صرف بر مجازات پس از وقوع جرم، بر شناسایی، ارزیابی و مدیریت ریسک‌های جرم‌زا در مراحل پیشینی تأکید دارد. در حوزه فناوری‌های مالی و رمزارزها، چنین رویکردی می‌تواند با ترکیب ابزارهای حقوقی، نظارتی و فناورانه، تعادلی میان حمایت از نوآوری و کنترل مخاطرات کیفری، ایجاد کند.

با این حال، پرسش اساسی آن است که سیاست جنایی ایران تا چه اندازه با الزامات رویکرد خطرمدار همخوانی دارد و چه خلأهایی مانع از تحقق کامل آن شده است. بررسی میزان انطباق سیاست‌های داخلی با استانداردهای بین‌المللی، از جمله توصیه‌های نهادهایی نظیر گروه ویژه اقدام مالی (FATF) و ارزیابی

ظرفیت‌های حقوقی و نهادی موجود، می‌تواند تصویری روشن‌تر از وضعیت فعلی ارائه دهد. در همین راستا، شناسایی نقاط ضعف و قوت سیاست جنایی ایران، پیش‌شرط ارائه راهکارهای اصلاحی و عملی به شمار می‌رود.

پژوهش حاضر با هدف تحلیل انتقادی سیاست جنایی ایران در مواجهه با جرایم مرتبط با رمزارزها و ارائه الگویی مبتنی بر رویکرد خطرمدار، انجام شده است. این پژوهش می‌کوشد نشان دهد که سیاست جنایی موجود، علی‌رغم برخی گام‌های مثبت، همچنان ماهیتی نیمه‌خطرمدار دارد و برای ارتقای کارآمدی، نیازمند بازنگری در ابعاد تقنینی، قضایی و اجرایی است. بر این اساس، تلاش می‌شود با بهره‌گیری از تجارب بین‌المللی و در نظر گرفتن شرایط بومی ایران، چارچوبی پیشنهادی برای مدیریت ریسک‌های جرم‌زا در حوزه رمزارزها ارائه شود.

در نهایت، اهمیت این پژوهش در آن است که می‌کوشد میان دو ضرورت ظاهراً متعارض – یعنی بهره‌برداری از ظرفیت‌های اقتصادی و فناورانه رمزارزها و مقابله مؤثر با مخاطرات کیفری آن‌ها – نوعی تعادل عقلانی برقرار کند. دستیابی به چنین تعادلی، می‌تواند زمینه‌ساز توسعه‌ای امن، پایدار و قانون‌مند در حوزه اقتصاد دیجیتال ایران باشد و از تحمیل هزینه‌های بلندمدت ناشی از بزهکاری سازمان‌یافته و سایبری جلوگیری کند.

پیشینه

مطالعات داخلی مرتبط با رمزارزها عمدتاً از دهه ۱۳۹۰ و هم‌زمان با گسترش بازار کریپتو (Crypto – رمزنگاری) شکل گرفته‌اند. در این پژوهش‌ها، رمزارزها غالباً به‌عنوان تهدیدی برای نظام پولی و مالی کشور تلقی شده و تمرکز اصلی بر پیشگیری وضعی از جرایم اقتصادی قرار داشته است. ایزدی و ارزانیان (۱۳۹۸) در مقاله‌ای با عنوان «پیشگیری از جرایم پولشویی و کلاهبرداری در بستر استفاده از رمزارزهای جهانی»، به پیشگیری وضعی و اجتماعی اشاره کرده و بر لزوم کنترل ناشناسی تراکنش‌ها و آگاه‌سازی کاربران تأکید دارند. هرچند پیشنهادهای آنان، به دلیل فقدان پشتوانه تقنینی منسجم، از کارآمدی محدودی، برخوردار است.

در گام بعدی، شاملو و خلیلی پاجی (۱۳۹۹) در مقاله «سیاست‌گذاری جنایی ریسک‌مدار در برابر فناوری ارزهای مجازی»، با تبیین نظریه مدیریت ریسک جرم، زمینه نظری رویکرد خطرمدار در حوزه جرایم رمزارزی را فراهم کرده‌اند. این پژوهش بر اهمیت تحلیل ریسک‌های فناورانه تأکید دارد. همچنین خلیلی پاجی (۱۴۰۰) در رساله دکتری خود با موضوع «تأثیر ارزهای مجازی بر جهانی شدن بزهکاری»، با تمرکز بر فراملی شدن بزهکاری در بستر ارزهای مجازی، سیاست جنایی خطرمدار با رویکرد فراملی را پیشنهاد می‌کند. با این حال، چالش‌های داخلی نظیر موانع اجرایی در نظام حقوقی ایران و محدودیت‌های ساختاری ناشی از تحریم‌های مالی، در این اثر کمتر مورد توجه قرار گرفته است.

از منظر جرم‌شناختی، صفاری و همکاران (۱۳۹۹) در مقاله «کارکردهای مجرمانه ارزهای مجازی»، به بررسی کارکردهای مجرمانه رمزارزها، به‌ویژه پولشویی و کلاهبرداری، پرداخته و ترکیبی از پیشگیری

وضعی و اجتماعی را پیشنهاد می‌دهند. همچنین حسانی و همکاران (۱۴۰۰) در مقاله «رهیافت مدیریت ریسک جرم و جلوه‌های آن در نظام عدالت کیفری ایران»، جلوه‌های مدیریت ریسک جرم را در نظام عدالت کیفری ایران تحلیل کرده و درجه‌بندی مجازات‌ها و قرارهای تأمین را نمونه‌های خطرمدار می‌دانند. با این حال، تحلیل‌ها عمدتاً ناظر بر جرایم سنتی است و به دلیل ماهیت فراملی ریسک در جرایم رمزارزی، کفایت لازم را ندارد.

در حوزه مبانی تقنینی، محمدی (۱۴۰۳) در رساله «اباحه‌گری در حوزه رمزارزهای دیجیتال و تعارض با سیاست جنایی تقنینی»، به تعارض میان اباحه‌گری فقهی و سیاست جنایی پرداخته و جرم‌انگاری پیش‌دستانه را مطرح می‌کند. هرچند این رساله تعارض فقهی را به خوبی تبیین کرده است، اما کمتر به ابعاد اجرایی توجه دارد. گودرزی (۱۴۰۳) نیز در رساله «سیاست جنایی ایران در قبال رمزارزها؛ با تأکید بر پیشگیری از پولشویی»، سیاست جنایی در پیشگیری از پولشویی رمزارز را ارزیابی کرده و نظارت فناوری‌محور را پیشنهاد می‌دهد. با این حال، تمرکز اصلی این پژوهش بر پولشویی است و سایر جرایم رمزارزی کمتر مورد توجه قرار گرفته‌اند. در نهایت، الگوی پیشگیری چهارگانه ارائه‌شده توسط قائمی اصل (۱۴۰۴) در رساله «پیشگیری از فعالیت مجرمانه مرتبط با ارزهای مجازی در سیاست جنایی ایران»، با تأکید بر هماهنگی ابعاد تقنینی، قضایی، اجرایی و مشارکتی، از جمله منابع داخلی است که ظرفیت مناسبی برای بومی‌سازی رویکرد خطرمدار در ایران دارد..

در سطح بین‌المللی، سیاست‌گذاری و پژوهش در حوزه رمزارزها از انسجام و عمق بیشتری برخوردار است. نهادهای بین‌المللی، به ویژه گروه اقدام مالی (FATF)، نقش محوری در تدوین استانداردهای جهانی ایفا کرده‌اند. توصیه ۱۵ FATF، ارائه‌دهندگان خدمات دارایی مجازی (VASPs) را ملزم به اجرای الزامات شناخت مشتری (KYC)، گزارش‌دهی تراکنش‌های مشکوک (STR) و قاعده انتقال اطلاعات (Travel Rule) می‌کند. این توصیه نمونه‌ای روشن از رویکرد خطرمدار پیش‌دستانه است که ریسک پولشویی و تأمین مالی تروریسم را مدیریت می‌نماید شود (FATF, 2019، Recommendation 15 ؛ به‌روزرسانی ۲۰۲۵).

گزارش‌های تخصصی مانند Chainalysis 2024 Crypto Crime Report نیز با تمرکز بر ردیابی تراکنش‌ها، بازیابی دارایی‌های مجرمانه و استفاده از ابزارهای فناورانه مانند تحلیل زنجیره بلاکچین، مدل‌های پیشرفته‌ای برای مقابله با جرایم رمزارزی ارائه می‌دهند (Chainalysis 2024). همچنین، گزارشElliptic (۲۰۲۱) نشان می‌دهد که کشورهای تحت تحریم مانند ایران از استخراج رمزارز برای دور زدن محدودیت‌های بانکی استفاده می‌کنند، اما این فرصت بدون نظارت کافی، ریسک جرایم را افزایش می‌دهد (Elliptic 2021). با این حال، فرض ضمنی این الگوها، وجود همکاری بین‌المللی و دسترسی آزاد به زیرساخت‌های مالی جهانی است.

مبانی نظری و مفهومی پژوهش

مفهوم رمزارزها و تمایز ساختاری آن با نظام های مالی سنتی

رمزارزها به‌عنوان یکی از مهم‌ترین جلوه‌های نوآوری مالی در قرن بیست‌ویکم، نقشی تعیین‌کننده در بازتعریف مناسبات پولی و مالی ایفا کرده‌اند و از همین رو، تبیین دقیق مفهوم و ویژگی‌های آن‌ها برای تحلیل سیاست جنایی در این حوزه، ضرورتی اجتناب‌ناپذیر است. رمزارز (Cryptocurrency) به دارایی دیجیتال رمزنگاری‌شده‌ای اطلاق می‌شود که مبتنی بر فناوری بلاکچین بوده و امکان انجام مبادلات مالی را به‌صورت مستقیم و بدون نیاز به واسطه‌های سنتی فراهم می‌سازد.

بلاکچین، به‌عنوان یک دفتر کل توزیع‌شده، تراکنش‌ها را در قالب بلوک‌های به‌هم‌پیوسته ثبت می‌کند و از طریق الگوریتم‌های اجماع، اعتبار آن‌ها را بدون اتکا به نهاد مرکزی تضمین می‌نماید (خضری‌نیا، ۱۴۰۳، صص. ۲۸–۳۲). این فناوری نخستین بار با معرفی بیت‌کوین در سال ۲۰۰۸ مطرح شد و هدف اصلی آن، کاهش وابستگی به نظام مالی متمرکز و حذف واسطه‌های سنتی در مبادلات پولی بود (شاملو و خلیلی پاجی، ۱۳۹۹، صفحه ۲۴۸).

رمزارزها به واسطه مجموعه‌ای از ویژگی‌های خاص، تمایزی بنیادین با پول‌های رایج دولتی (پول‌های فیات) دارند. غیرمتمرکز بودن – به این معنا که کنترل و نظارت آن‌ها در اختیار یک مرجع واحد مانند بانک مرکزی قرار ندارد و اعتبارسنجی تراکنش‌ها توسط شبکه انجام می‌شود – بهره‌گیری از رمزنگاری پیشرفته مبتنی بر کلیدهای عمومی و خصوصی، ناشناسی نسبی کاربران علی‌رغم ثبت عمومی تراکنش‌ها، ماهیت فرامرزی و بی‌توجهی به محدودیت‌های جغرافیایی، سرعت بالا و هزینه نسبتاً پایین انتقال ارزش، از جمله مهم‌ترین این ویژگی‌ها به شمار می‌روند (خضری‌نیا، ۱۴۰۳، صص. ۲۸–۳۲).

ترکیب این ویژگی‌ها نوعی پارادوکس ساختاری ایجاد می‌کند: از یک سو، بلاکچین سطح بالایی از شفافیت را فراهم می‌آورد و از سوی دیگر، ناشناسی نسبی کاربران سبب می‌شود که شناسایی هویت واقعی اشخاص و ردیابی مسئولیت کیفری با دشواری مواجه گردد. این پارادوکس، یکی از چالش‌های اصلی سیاست جنایی در مواجهه با رمزارزها را شکل می‌دهد.

در ایران، اهمیت این ویژگی‌ها دوچندان است. محدودیت‌های ناشی از تحریم‌های بین‌المللی، دسترسی به نظام بانکی جهانی را با موانع جدی مواجه ساخته و در نتیجه، رمزارزها به‌عنوان ابزاری جایگزین برای مبادلات ارزی و انتقال ارزش مطرح شده و مورد توجه قرار گرفته‌اند. از سوی دیگر، استخراج رمزارز با اتکا به منابع انرژی داخلی، فرصت‌هایی اقتصادی ایجاد کرده است. با این حال، فقدان نظارت مؤثر و چارچوب‌های حقوقی شفاف، زمینه افزایش ریسک‌های جرم‌زا را نیز فراهم آورده است (گودرزی، ۱۴۰۳، ضرورت تحقیق).

تمایز میان رمزارزها و ارز دیجیتال بانک مرکزی (Central Bank Digital Currency - CBDC) در این میان اهمیتی اساسی دارد. ارزهای دیجیتال دولتی، برخلاف رمزارزها، ماهیتی متمرکز دارند و صدور، نظارت و کنترل آن‌ها در اختیار بانک مرکزی است. تجربه‌هایی مانند یوآن دیجیتال چین نشان

می‌دهد که ارز دیجیتال بانک مرکزی می‌توانند به ابزاری برای اعمال سیاست‌های پولی و نظارت بر جریان سرمایه تبدیل شوند (خضری‌نیا، ۱۴۰۳، صص. ۴۸-۴۶). در مقابل، رمزارزها بر الگوریتم‌های اجماع غیرمتمرکز متکی‌اند و هیچ نهاد مرکزی از جمله بانک‌های مرکزی کشورها، کنترل کامل آن‌ها را در اختیار ندارد (شاملو و خلیلی پاجی، ۱۳۹۹، صفحه ۲۵۱). همین تفاوت بنیادین، کارآمدی شیوه‌های سنتی نظارت را کاهش داده و ضرورت اتخاذ رویکردهای نوین و خطرمدار را برجسته می‌سازد.

در این رویکرد، تمرکز اصلی بر شناسایی گروه‌های خطردار، دسته‌بندی انواع خطر، شناسایی وضعیت‌ها و محیط‌های خطرزا و در نهایت کاهش فراوانی خطر ارتکاب جرم و تکرار آن است، به‌گونه‌ای که با افزایش خطر شناسایی، خنثی‌سازی و دور کردن مجرمان بالقوه و بالفعل از چرخه بزهکاری، امنیت اجتماعی تقویت شود (نجفی ابرندآبادی، ۱۳۸۸، صص. ۶-۱۸).

جرایم مرتبط با رمزارزها و تحول الگوهای بزهکاری

جرایم مرتبط با رمزارزها از مهم‌ترین چالش‌های سیاست جنایی معاصر به شمار می‌روند. این دسته از جرایم که عمدتاً ماهیتی اقتصادی دارند، به واسطه ویژگی‌های ذاتی رمزارزها نظیر ناشناسی نسبی، فرامرزی بودن، سرعت بالا و غیرمتمرکز بودن، تسهیل می‌شوند. در نتیجه، بزهکاری از الگوهای محلی و سنتی فاصله گرفته و به شکلی سازمان‌یافته، سایبری و جهانی تحول یافته است؛ تحولی که ابزارها و سازوکارهای سنتی مقابله با جرم را با محدودیت‌های جدی مواجه کرده است.

پولشویی، شایع‌ترین و در عین حال پیچیده‌ترین جرم مرتبط با رمزارزها محسوب می‌شود. فرآیند پولشویی، شامل مراحل جایگذاری، لایه‌بندی و یکپارچه‌سازی، در بستر رمزارزها با سهولت بیشتری انجام می‌گیرد. برای درک بهتر، یک مثال عملی بیان می‌شود. فرض کنید مجرمی وجوه حاصل از فساد مالی را به بیت‌کوین تبدیل می‌کند (جایگذاری)، سپس این بیت‌کوین را به چندین والت (کیف پول) تقسیم می‌کند، از صرافی‌های ناشناس برای مخلوط کردن با تراکنش‌های قانونی استفاده می‌کند (لایه‌بندی) و در نهایت به ریال یا دارایی دیگر تبدیل می‌کند (یکپارچه‌سازی). بر این اساس، امکان جابه‌جایی سریع وجوه، استفاده از چندین کیف پول و بهره‌گیری از ابزارهای اختفای تراکنش، موجب می‌شود که منشأ وجوه نامشروع به‌سادگی، پنهان گردد. به عبارت دیگر، در حالت معمول و در امور بانکی، گزارش واریز نقدی وجوه بیش از سقف مقرر، تکلیف قانونی است، بدین گونه که در فرم اطلاعاتی، مواردی همچون علت پرداخت وجوه، منشأ پول واریزکننده و صاحب حساب دریافت شود و بانک موظف است، اطلاعات این فرم را با مدارک مراجعه‌کننده تطبیق داده و سپس اقدام به واریز یا انتقال وجوه کند. این در حالی است که چنین اقدامی نسبت به مبادلات رمزارزها محال بوده، زیرا چنین سیستمی در استفاده از رمزارزها به علت نبود بانک‌ها و سیستم نظارتی، وجود ندارد (ایزدی و ارزانیان، ۱۳۹۸، صفحه ۳۷). گزارش‌های نهادهایی مانند FATF نیز حاکی از آن است که بخش قابل توجهی از تراکنش‌های رمزارزی در معرض ریسک پولشویی و تأمین مالی فعالیت‌های غیرقانونی قرار دارد (FATF, 2019، Recommendation 15).

به نظر نگارنده، در ایران، این ریسک با تحریم‌های بین‌المللی تشدید شده است، چون رمزارزها به جایگزینی برای کانال‌های بانکی سنتی تبدیل شده‌اند و مجرمان از این خلأ برای لایه‌بندی وجوه غیرقانونی، استفاده می‌کنند.

قاچاق غیرقانونی مواد مخدر و روان‌گردان نیز از عمده‌ترین فعالیت‌های مجرمانه با استفاده از رمزارزها است. در حقیقت، امروزه در کنار روش‌های سنتی فروش مواد مخدر، روش‌های جنایی جدید برای فروش این مواد، یعنی فروش از راه دور و با استفاده از ارزهای مجازی، روزبه‌روز در حال افزایش است (صفاری و همکاران، ۱۳۹۹، صفحه ۲۶).

تأمین مالی تروریسم با استفاده از رمزارزها یکی دیگر از جرایم مرتبط با رمزارزها محسوب می‌شود. در این فرآیند، گروه‌های تروریستی معمولاً از پلتفرم‌های رسانه‌های اجتماعی و وب‌سایت‌های خاص برای تبلیغ فعالیت‌های خود و جذب کمک‌های مالی استفاده می‌کنند. این گروه‌ها معمولاً از رمزارز به عنوان روش پرداخت استفاده می‌کنند. این انتخاب به دلیل ویژگی‌های خاص ارزهای دیجیتال، از جمله ناشناسی بودن و عدم نیاز به احراز هویت، بسیار جذاب بوده و حامیان می‌توانند به راحتی وجوه خود را به آدرس‌های رمزارزی مشخص‌شده توسط گروه‌های تروریستی منتقل کنند، بدون اینکه هویت واقعی آنها شناسایی شود (قائمی اصل، ۱۴۰۴، چکیده).

به نظر نگارنده، تحول بزهکاری در این حوزه، صرفاً به تنوع جرایم محدود نمی‌شود، بلکه شامل تغییر در مقیاس، ساختار و شیوه ارتکاب جرم نیز هست. به عبارت دیگر، تحول بزهکاری با رمزارزها عمیق و چندبعدی شده است، از جرایم فردی به سازمان‌یافته (شبکه‌های بین‌المللی پولشویی)، از محلی به فراملی (تراکنش‌های جهانی بدون مرز) و از سنتی به سایبری (استفاده از ابزارهای دیجیتال پیشرفته)، دگرگون شده است. این تغییر و تحولات، سیاست جنایی را ناگزیر به عبور از رویکردهای صرفاً واکنشی و حرکت به سمت مدیریت خطرمدار، سوق می‌دهد.

سیاست جنایی در پرتو رویکرد خطرمدار

سیاست جنایی به‌عنوان چارچوب کلی مواجهه نظام حقوقی با پدیده جرم، مجموعه‌ای از تدابیر تقنینی، قضایی، اجرایی و مشارکتی را در بر می‌گیرد که هدف آن پیشگیری از جرم، واکنش متناسب به بزهکاری و حفظ نظم اجتماعی است. همان‌گونه که گفته شد، در مواجهه با پدیده‌های نوظهوری همچون رمزارزها، الگوهای سنتی سیاست جنایی که عمدتاً بر سرکوب و مجازات پس از وقوع جرم تمرکز دارند، با کاستی‌های جدی روبه‌رو شده‌اند.

رویکرد خطرمدار به عنوان پارادایم مدرن سیاست جنایی، جایگزینی کارآمد برای مدل سنتی ارائه می‌دهد. این رویکرد ریشه در نظریه «جامعه ریسک» اولریش بک (Ulrich Beck) دارد که جامعه معاصر را پر از ریسک‌های ساختگی (ناشی از پیشرفت‌های فناوری و جهانی‌شدن)، توصیف می‌کند و نیاز به مدیریت پیشگیرانه این ریسک‌ها را تأکید می‌نماید (نجفی ابرندآبادی، ۱۳۸۸، صص. ۷۳۲-۷۳۱).

رویکرد مدیریت خطرمدار، به‌ویژه با گسترش جهانی‌شدن جرایم و رشد سریع بزهکاری سازمان‌یافته در سراسر جهان، به عنوان یک نگرش نوین شکل گرفته و دامنه و روش‌های ساختاری آن روزبه‌روز گسترده‌تر شده است. به حدی که امروزه در حوزه سیاست جنایی، چه در سطح ملی و چه فراملی، می‌توان به وضوح از یک روش مستقل و متمایز به نام مدیریت خطرمدار، سخن به میان آورد (پاکنهاد، ۱۳۸۸، صص. ۳۱-۳۵).

به نظر نگارنده، در این رویکرد، تمرکز اصلی بر شناسایی، ارزیابی و کاهش ریسک‌ها پیش از تبدیل شدن به جرم واقعی است. به عبارت دیگر، با بهینه مصرف نمودن منابع محدود جامعه، ریسک‌ها پیش‌بینی شده و از وقوع جرایم پیشگیری می‌کند، نه اینکه فقط به مجازات بپردازد.

در ایران، جلوه‌های رویکرد خطرمدار در نظام عدالت کیفری وجود دارد، اما محدود و بیشتر در جرایم سنتی اعمال می‌شود. برای مثال، درجه‌بندی مجازات‌های تعزیری در قانون مجازات اسلامی (از درجه ۱ تا ۸) بر اساس شدت ریسک و خطر جرم تعیین می‌شود که نمونه‌ای از مدیریت خطر است. همچنین، قرارهای تأمین مانند کفالت، وثیقه یا نظارت الکترونیکی (در جرایم خاص) امکان کنترل خطر پیش از صدور حکم قطعی را فراهم می‌کند و به کاهش جمعیت کیفری کمک کرده است. این ابزارها در جرایم مانند سرقت، قتل یا اختلاس مفید بوده‌اند و نشان‌دهنده حرکت به سمت خطرمدار هستند. با این حال، در حوزه رمزارزها که جرایم آن فراملی، سایبری و پیچیده هستند، این جلوه‌ها ناکافی به نظر می‌رسند. دلیل اصلی، عدم اجرای کامل پیشگیری چهارگانه است: تقنینی (قوانین ناقص برای جرم‌انگاری فعالیت‌های پرریسک رمزارز)، قضایی (عدم تخصص قضات در تحلیل بلاکچین)، اجرایی (نظارت محدود پلیس فتا و بانک مرکزی بر تراکنش‌ها) و مشارکتی (کمبود همکاری بخش خصوصی مانند صرافی‌های رمزارز با نهادهای دولتی). علاوه بر این، ریسک‌های فراملی مانند پولشویی بین‌المللی که از طریق رمزارزها انجام می‌شود، بدون ابزارهای پیشرفته مانند سامانه‌های رصد بلاکچین مدیریت نمی‌شود و سیاست را واکنشی نگه می‌دارد (قائمی اصل، ۱۴۰۴، چکیده صفحه ۶).

در سطح بین‌المللی، رویکرد خطرمدار با استانداردهای گروه ویژه اقدام مالی، به‌ویژه توصیه ۱۵، همخوانی کامل دارد. این توصیه که در سال ۲۰۱۹ معرفی و در به‌روزرسانی‌های بعدی تا ۲۰۲۵ تکمیل شده، بر شناسایی و مدیریت ریسک‌های ناشی از فناوری‌های نوین تمرکز دارد. منظور از فناوری‌های نوین، توسعه ابزارها، فرایندها یا پلتفرم‌های جدیدی است که می‌توانند فرصت‌ها یا ریسک‌های تازه‌ای برای پولشویی و تأمین مالی تروریسم و غیره ایجاد کنند. بر اساس این توصیه، کشورها و نهادهای مالی موظف‌اند این ریسک‌ها را پیش از معرفی محصول یا فناوری جدید شناسایی و مدیریت کنند تا از سوءاستفاده‌های احتمالی جلوگیری شود (Recommendation 15،FATF, 2019 ؛ به‌روزرسانی ۲۰۲۵).

توصیه ۱۵ مورد اشاره، دامنه گسترده‌ای دارد و بدون محدود شدن به بیت‌کوین یا رمزارزهای خاص، شامل هر نوع نمایندگی دیجیتال ارزش می‌شود که قابلیت معامله، انتقال یا استفاده برای پرداخت و سرمایه‌گذاری را داشته باشد. در مرکز این توصیه، ارائه‌دهندگان خدمات دارایی مجازی (VASPs) قرار دارند؛ یعنی اشخاص حقیقی یا حقوقی که به صورت حرفه‌ای حداقل یکی از خدمات از قبیل مبادله بین

دارایی‌های مجازی و پول‌های رایج، مبادله بین انواع دارایی‌های مجازی، انتقال دارایی مجازی از یک آدرس به آدرس دیگر برای دیگران، نگهداری یا مدیریت دارایی‌های مجازی، و ارائه خدمات مالی مرتبط با عرضه یا فروش این دارایی‌ها را انجام می‌دهند. این الزامات، ارائه‌دهندگان خدمات دارایی مجازی را ملزم به اجرای شناسایی مشتریان، گزارش‌دهی تراکنش‌های مشکوک و رعایت استانداردهای پیشگیرانه می‌کند تا ریسک‌های مجرمانه کاهش یابد.

یکی دیگر از مهم‌ترین مؤلفه‌های عملی توصیه ۱۵، قانون سفر (Travel Rule) است. این قانون، ارائه‌دهندگان خدمات دارایی مجازی را موظف می‌کند در تراکنش‌های واجد شرایط، اطلاعات اصلی فرستنده (originator) و گیرنده (beneficiary) را جمع‌آوری، نگهداری و منتقل کنند تا ردیابی کامل تراکنش‌ها، ممکن شود. این اطلاعات معمولاً شامل نام، آدرس، شناسه ملی یا معادل آن و شناسه کیف پول یا حساب است. این قانون که ابتدا برای انتقال‌های بانکی بین‌المللی طراحی شده بود، توسط گروه ویژه اقدام مالی، به حوزه دارایی‌های مجازی گسترش یافت تا خلأهای نظارتی پر شود و زنجیره انتقال وجوه، قابل پیگیری باقی بماند. این و سازوکار، رویکرد خطرمدار را عملیاتی می‌کند و به عنوان مثال، از لایه‌بندی پولشویی جلوگیری می‌نماید شود (Recommendation 15،FATF, 2019 ؛ به‌روزرسانی ۲۰۲۵).

در ایران، فاصله با این استانداردها مشهود است. تحریم‌های بین‌المللی همکاری فراملی را سخت کرده و اجرای کامل توصیه‌ها را دشوار می‌نماید، اما این به معنای نادیده گرفتن اصول خطرمدار نیست. نگارنده معتقد است، ایران می‌تواند از روش مبتنی بر ریسک گروه ویژه اقدام مالی برای اولویت‌بندی ریسک‌های داخلی استفاده کند؛ به عنوان مثال، بدون نیاز به عضویت، تمرکز روی تراکنش‌های ناشناس با حجم بالا یا مرتبط با کیف پول های پرریسک خارجی را اعمال نماید.

تحلیل سیاست جنایی ایران در مواجهه با جرایم رمزارزی

سیاست جنایی ایران در مواجهه با رمزارزها، مسیری تدریجی؛ اما ناتمام را طی کرده است. این سیاست از ممنوعیت مطلق اولیه به سمت پذیرش واقعیت‌های اقتصادی و فناورانه حرکت کرده، اما همچنان ماهیتی واکنشی دارد و فاقد پیشگیری پیش‌دستانه منسجم است. فشار تحریم‌های بین‌المللی موجب شده اولویت‌های اقتصادی، به‌ویژه بهره‌برداری از استخراج رمزارز برای تأمین ارز، بر ملاحظات امنیتی و کنترلی، غلبه یابد. نتیجه این وضعیت، شکل‌گیری سیاستی نیمه‌خطرمدار است که برخی جلوه‌های مدیریت ریسک را پذیرفته، اما فاقد انسجام نهادی و تقنینی لازم برای کنترل بزهکاری رمزارزی است.

سیاست جنایی تقنینی

سیاست تقنینی ایران در مواجهه با رمزارزها، از یک ممنوعیت سخت‌گیرانه و مبتنی بر نگرانی‌های پولی و امنیتی، به سمت رویکردی تدریجی و تنظیم‌گرایانه حرکت کرده است. با این حال، این گذار بیش از آنکه بر منطق پیشگیری خطرمدار، استوار باشد، تحت تأثیر ضرورت‌های اقتصادی و فشارهای ناشی از تحریم‌های بین‌المللی شکل گرفته است. در نتیجه، چارچوب تقنینی موجود را می‌توان نوعی تنظیم‌گری

واکنشی، دانست که به‌صورت مقطعی به برخی ریسک‌ها پاسخ داده، اما فاقد انسجام نظام‌مند در مدیریت بزهکاری رمزارزی است.

در مرحله نخست، مصوبه هیئت وزیران در سال ۱۳۹۶، استفاده از رمزارزها به‌عنوان ابزار پرداخت رسمی را ممنوع اعلام کرد و آن‌ها را تهدیدی برای حاکمیت پولی و نظام مالی کشور دانست. این رویکرد مبتنی بر منطق کنترل حداکثری بود و رمزارزها را پدیده‌ای خارج از قلمرو مشروع اقتصادی تلقی می‌کرد. در ادامه، بانک مرکزی با صدور سند «الزامات و ضوابط حوزه رمزارزها» در سال ۱۳۹۷، از ممنوعیت مطلق فاصله گرفت و سیاست «منتظر بمان و ببین» را اتخاذ کرد؛ به‌گونه‌ای که ضمن عدم تضمین اصالت رمزارزها، مسئولیت ریسک سرمایه‌گذاری را بر عهده اشخاص گذاشت. هرچند این سند گامی به‌سوی واقع‌گرایی تقنینی بود، اما همچنان فاقد سازوکارهای نظارتی و پیشگیرانه مؤثر، به‌ویژه در حوزه شفافیت تراکنش‌ها و شناسایی کاربران، باقی ماند.

نقطه عطف بعدی، تصویب آیین‌نامه اجرایی استخراج رمزدارایی‌ها در سال ۱۴۰۱ بود. این آیین‌نامه با به‌رسمیت شناختن استخراج رمزارز و اعطای مجوز فعالیت تحت شرایط خاص، تلاش کرد از ظرفیت اقتصادی این پدیده در شرایط تحریم بهره‌برداری کند. تمرکز اصلی این مقررات بر مدیریت مصرف انرژی و بازگشت ارز حاصل از استخراج به چرخه اقتصادی کشور بود. با وجود این، ابعاد پیشگیرانه سیاست جنایی، از جمله نظارت بر گردش داخلی رمزارزها، کنترل صرافی‌ها و الزامات شناسایی مشتریان، در حاشیه قرار گرفت و سیاست تقنینی همچنان اولویت را به ملاحظات اقتصادی داد (گودرزی، ۱۴۰۳، چکیده صفحه ۲۵).

در سال ۱۴۰۳ «نظام‌نامه رمز ارز ملی و ساماندهی رمز ارزهای جهانی» مصوب کمیسیون عالی تنظیم مقررات فضای مجازی کشور، گام مهمی در جهت سامان‌دهی نهادی این حوزه برداشت. این نظام‌نامه، برای نخستین‌بار تلاش کرد با تفکیک میان رمز ارز ملی و رمز ارزهای جهانی، چارچوبی کلان برای تنظیم‌گری فعالیت‌های مرتبط با رمزارزها ارائه دهد. با این حال، رویکرد حاکم بر این سند نیز بیش از آنکه مبتنی بر ارزیابی نظام‌مند ریسک‌های کیفری باشد، معطوف به حکمرانی فضای مجازی و کنترل کارکردهای اقتصادی و فناورانه رمزارزها است و پیوند مستقیمی با سیاست جنایی خطرمدار، برقرار نمی‌کند.

این روند در سال ۱۴۰۴ با تصویب «دستورالعمل تأسیس، فعالیت، انحلال و نظارت بر کارگزاران رمزپول» تکمیل شد. دستورالعمل مزبور، با تمرکز بر تنظیم فعالیت کارگزاران و صرافی‌های رمزارزی، نشانه‌ای از چرخش تدریجی به سمت نظارت ساختاریافته و پذیرش واقعیت بازار رمزارزهاست. پیش‌بینی الزامات حداقلی نظارتی، بیانگر گذار از رویکرد انفعالی به تنظیم‌گری فعال است؛ با این وجود، همچنان خلأهای جدی در زمینه شناسایی مشتریان، پایش تراکنش‌های مشکوک و اتصال نظام نظارتی به سازوکارهای مبارزه با پولشویی، مشاهده می‌شود.

این گذار از رویکرد انفعالی به تنظیم‌گری فعال، یکی از نقاط قوت قابل توجه سیاست تقنینی ایران به شمار می‌رود، زیرا برای نخستین بار چارچوبی رسمی برای فعالیت کارگزاران داخلی ایجاد کرده و زمینه‌ای برای کنترل محدود تراکنش‌ها فراهم آورده است.

در مجموع، همانگونه که گفته شد، سیاست تقنینی ایران در حوزه رمزارزها را می‌توان نیمه‌خطرمدار، توصیف کرد؛ به این معنا که برخی عناصر مدیریت ریسک را پذیرفته، اما فاقد انسجام تقنینی و پیوند روشن با قوانین مبارزه با پولشویی و تأمین مالی جرایم سازمان‌یافته است. به عنوان مثال، عدم شمول صریح رمزارزها در قوانین مبارزه با پولشویی و قاچاق ارز، به‌ویژه در مرحله لایه‌بندی پولشویی، امکان سوءاستفاده از ناشناسی تراکنش‌ها را افزایش داده است. افزون بر این، تعارض میان اصل اباحه‌گری فقهی و الزامات سیاست جنایی، موجب شده رمزارزها بدون تعریف حقوقی دقیق و چارچوب کنترلی شفاف، رها شوند؛ وضعیتی که با منطق رویکرد خطرمدار، ناسازگار است (محمدی، ۱۴۰۳؛ صص ۱۴۰–۱۴۴)

با این حال، نقاط ضعف جدی همچنان باقی است. خلأهای اصلی در زمینه شناسایی مشتریان (KYC)، پایش تراکنش‌های مشکوک و اتصال نظام نظارتی به سازوکارهای مبارزه با پولشویی مشاهده می‌شود. در مجموع، سیاست تقنینی ایران در حوزه رمزارزها را می‌توان «نیمه‌خطرمدار» توصیف کرد؛ به این معنا که برخی عناصر مدیریت ریسک (مانند مجوزدهی مشروط و الزامات حداقلی) را پذیرفته، اما فاقد انسجام تقنینی و پیوند روشن با قوانین مبارزه با پولشویی و تأمین مالی جرایم سازمان‌یافته است. به عنوان مثال، عدم شمول صریح رمزارزها در قوانین مبارزه با پولشویی و قاچاق ارز، به‌ویژه در مرحله لایه‌بندی پولشویی، امکان سوءاستفاده از ناشناسی تراکنش‌ها را افزایش داده است. افزون بر این، تعارض میان اصل اباحه‌گری فقهی و الزامات سیاست جنایی، موجب شده رمزارزها بدون تعریف حقوقی دقیق و چارچوب کنترلی شفاف رها شوند؛ وضعیتی که با منطق رویکرد خطرمدار ناسازگار است و ضعف کارآمدی سیاست تقنینی را در پیشگیری پیش‌دستانه از جرایم رمزارزی نشان می‌دهد (محمدی، ۱۴۰۳، صص. ۱۴۰–۱۴۴).

سیاست جنایی قضایی و اجرایی

در سطح قضایی، رسیدگی به جرایم مرتبط با رمزارزها با چالش‌های ساختاری و کارکردی متعددی مواجه است که کارآمدی سیاست جنایی را به‌طور جدی تحت‌تأثیر قرار می‌دهد. ماهیت فناورانه و فرامرزی رمزارزها، ردیابی جریان وجوه، شناسایی مرتکبان و اثبات عناصر ذهنی جرم را با دشواری‌های مضاعف، همراه ساخته است. ناشناسی نسبی تراکنش‌ها در بستر بلاک‌چین و استفاده از ابزارهای اختفای

هویت، سبب شده است که ادله سنتی اثبات جرم در بسیاری از پرونده‌های کلاهبرداری، پولشویی و جرایم مالی مرتبط با رمزارزها، کارایی لازم را نداشته باشد (نبوی و صابر، ۱۳۹۹؛ صص ۱۹۶-۱۹۷).

به نظر نگارنده، این چالش‌ها در پرونده‌های واقعی برخی طرح‌های کلاهبرداری رمزارزی (مانند موارد تبلیغ‌شده در شبکه‌های اجتماعی با وعده سودهای غیرواقعی) مشهود است، جایی که اثبات قصد مجرمانه و ردیابی کیف‌های پول ارز دیجیتال، ماه‌ها طول می‌کشد و در برخی از موارد، به نتیجه قطعی نیز نمی‌رسد.

به عنوان نمونه در پرونده «کینگ مانی»، یکی از بزرگ‌ترین موارد کلاهبرداری شبکه‌ای رمزارزی در ایران است که با فریب سرمایه‌گذاران از طریق وعده سودهای بالا (تا ۵۰ درصد ماهانه) و تبلیغ رمزارز جعلی «کینگ مانی» انجام شد. متهمان با ایجاد یک طرح هرمی، هزاران نفر را به خرید این رمزارز تشویق کردند و وجوه جمع‌آوری‌شده را به حساب‌های شخصی منتقل کردند. این پرونده با حدود ۵۰۰۰ شاکی، از سال ۱۴۰۰ آغاز شد و متهمان اصلی به اتهام کلاهبرداری شبکه‌ای و اخلال در نظام اقتصادی محاکمه شدند. مرجع قضایی، احکام سنگینی از جمله حبس طولانی و رد مال، صادر کرد، اما فرآیند طولانی دادرسی و دشواری ردیابی تراکنش‌های رمزارزی، روند رسیدگی را سخت کرد (خبرگزاری میزان، آبان ۱۴۰۳؛ ایرنا، آبان ۱۴۰۴).

این پرونده نمونه بارزی از چالش‌های قضایی در جرایم رمزارزی است، زیرا با وجود وعده‌های تبلیغاتی در شبکه‌های اجتماعی، پراکندگی شاکیان در سراسر کشور، ناتوانی در ردیابی کامل جریان وجوه به دلیل لایه‌بندی تراکنش‌ها، علی‌رغم صدور احکام، بسیاری از شاکیان هنوز اموال‌شان را کامل دریافت نکرده‌اند، که نشان‌دهنده ضعف ابزارهای پیش‌دستانه و نیاز به نظارت تخصصی در این حوزه است.

افزون بر این، فقدان شعب تخصصی رسیدگی به جرایم رمزارزی و کمبود آموزش‌های هدفمند برای قضات و ضابطان قضایی، به ناهمگونی رویه‌ها و تفسیرهای متعارض دامن زده است. در چنین شرایطی، فرآیند دادرسی بیش از آنکه مبتنی بر تحلیل ریسک و شناخت الگوهای بزهکاری نوظهور باشد، به واکنش موردی و پسینی محدود می‌شود.

در بعد اجرایی نیز، نهادهای متولی مانند پلیس فتا و بانک مرکزی با محدودیت‌های جدی مواجه‌اند. نبود سامانه‌های پیشرفته رصد بلاکچین، ضعف هماهنگی نهادی و موانع ناشی از تحریم‌های بین‌المللی، امکان نظارت مؤثر و همکاری فرامرزی را به‌شدت کاهش داده است.

به نظر نگارنده و از منظر سیاست جنایی خطرمدار، خلأ اصلی در حوزه قضایی و اجرایی، فقدان نگاه پیش‌دستانه و داده‌محور است. مادامی که شناسایی الگوهای پرخطر، تحلیل تراکنش‌های مشکوک و اولویت‌بندی ریسک‌ها در دستور کار نهادهای اجرایی و قضایی قرار نگیرد، واکنش کیفری صرف نمی‌تواند مانع گسترش بزهکاری رمزارزی شود. این امر نشان می‌دهد که سیاست فعلی بیش از آنکه مبتنی بر مدیریت ریسک باشد، همچنان در چارچوب‌های سنتی دادرسی و کنترل کیفری، باقی مانده است.

ارزیابی میزان انطباق سیاست جنایی ایران با رویکرد خطرمدار

ارزیابی مجموع سیاست‌های تقنینی، قضایی و اجرایی ایران حاکی از آن است که نظام موجود واجد برخی عناصر پراکنده سیاست جنایی خطرمدار است، اما این عناصر فاقد انسجام نظری و نهادی‌اند. اقداماتی نظیر مجوزدهی به استخراج رمزارزها، اعمال محدود برخی الزامات شناسایی مشتریان و پذیرش ضمنی مدیریت ریسک اقتصادی، نشان‌دهنده فاصله گرفتن از رویکرد انکاری و حرکت به سوی پذیرش واقعیت‌های فناورانه است. با این حال، این اقدامات بیشتر ناظر به مدیریت پیامدها هستند تا پیشگیری ساختاری از بزهکاری.

نیمه‌خطرمدار بودن سیاست فعلی، به‌ویژه در شرایطی که ایران سهم متوسطی در استخراج جهانی رمزارزها دارد، ریسک جهانی‌شدن بزهکاری را تشدید می‌کند. فقدان چارچوب جامع مبارزه با پولشویی در حوزه رمزارزها، نبود سامانه ملی رصد تراکنش‌ها و تعارض میان منطق اباحه اقتصادی و الزامات کنترل کیفری، موجب شده است که سیاست جنایی نتواند به‌طور مؤثر خطرات ناشی از این فناوری را مهار کند. در نتیجه، فضای رمزارزی به بستری مستعد برای جرایم مالی پیچیده و فرامرزی بدل شده است.

جدول۱- جدول ۱- مقایسه سیاست جنایی ایران با رویکرد خطرمدار

بعد	وضعیت فعلی ایران	الزامات رویکرد خطرمدار FATF Recommendation) (15	خلأ اصلی
تقنینی	تنظیم‌گری اقتصادی‌محور، خلأ تعریف حقوقی	تعریف دارایی مجازی، KYC/STR اجباری	عدم انسجام و تمرکز روی ریسک کیفری
قضایی	رسیدگی موردی، عدم تخصص بلاکچین	دادگاه تخصصی، تحلیل ریسک پیش از حکم	واکنشی بودن، ناهمگونی رویه
اجرائی	نظارت محدود، تمرکز روی استخراج	سامانه رصد، گزارش مشکوک، Travel Rule	ضعف فناورانه و همکاری نهادی

(منبع: یافته‌های پژوهش)

پیشنهادها

برای گذار کامل به رویکرد خطرمدار در مدیریت رمزارزها، پیشنهادها در چهار حوزه تقنینی، قضایی، اجرایی و مشارکتی ارائه می‌شود. این پیشنهادها با توجه به خلأهای فعلی سیاست جنایی ایران، محدودیت‌های ناشی از تحریم‌های بین‌المللی، تعارض اباحه‌گری فقهی و نیاز به تعادل میان نوآوری اقتصادی و امنیت جامعه، طراحی شده‌اند. تحلیل سیاست موجود، نشان می‌دهد که رویکرد فعلی نیمه‌خطرمدار، فاقد انسجام ساختاری و پیشگیری پیش‌دستانه مؤثر است و به‌طور مستقیم در افزایش ریسک جرایم اقتصادی مانند پولشویی، کلاهبرداری و سوءاستفاده از تراکنش‌های ناشناس و غیره، نقش دارد.

مدل پیشنهادی این پژوهش بر پایه تلفیق پیشگیری چهارگانه، جرم‌انگاری محدود، مدیریت ریسک قضایی و نظارت داخلی طراحی شده است. این مدل، علاوه بر حفظ نوآوری و بهره‌برداری اقتصادی از رمزارزها، قابلیت کاهش ریسک‌های مجرمانه را دارد و همزمان با شرایط خاص ایران، از جمله تحریم‌های بین‌المللی، سازگار است.

پیشنهادهای تقنینی

تحلیل سیاست تقنینی ایران نشان می‌دهد که فقدان قانون جامع و اختصاصی برای رمزارزها موجب شده است که ماهیت حقوقی این دارایی‌ها، شامل مالکیت، انتقال و مسئولیت، به‌طور شفاف مشخص نشود. همچنین، شمول قوانین موجود مانند قانون مبارزه با پولشویی و قانون قاچاق کالا و ارز، بدون تعریف صریح رمزارزها، از تفسیرهای متغیر متأثر است و این خلأ، مرحله لایه‌بندی پولشویی را تسهیل می‌کند.

به نظر نگارنده، جرم‌انگاری پیش‌دستانه و محدود، مانند گزارش تراکنش‌های مشکوک با مجازات متناسب، نه تنها اصل تناسب را رعایت می‌کند، بلکه تعارض اباحه‌گری فقهی را نیز کاهش می‌دهد. در این چارچوب، رمزارزها همچنان جوازدار شمرده می‌شوند، اما با شرط‌های نظارت پیشگیرانه از سوءاستفاده جلوگیری می‌شود (محمدی، ۱۴۰۳؛ ص ۱۴۴).

همچنین قانون پیشنهادی باید با الهام از توصیه های گروه ویژه اقدام مالی، شامل KYC، STR و Travel Rule باشد، همچنین قانون پیشنهادی باید با الهام از توصیه‌های گروه ویژه اقدام مالی، شامل الزام شناخت مشتری (KYC)، گزارش‌دهی تراکنش‌های مشکوک (STR) و رعایت قاعده انتقال اطلاعات (Travel Rule) باشد، اما با توجه به تحریم‌ها، تمرکز روی نظارت داخلی و اولویت‌بندی تراکنش‌های پرریسک کافی است تا ریسک پولشویی کاهش یابد. به‌عنوان مثال، الزام ارائه‌دهندگان خدمات دارایی مجازی داخلی به ثبت در بانک مرکزی، گزارش تراکنش‌های پرریسک و شناسایی مشتریان بدون وابستگی به سیستم‌های خارجی، می‌تواند ضمن حفظ نوآوری، امکان پیشگیری مؤثر را فراهم کند. بر این اساس، با توجه به توصیه مورد اشاره، سیاست تقنینی خطرمدار در حوزه رمزارزها می‌تواند شامل موارد زیر باشد:

۱. تحلیل ریسک پولشویی و تأمین مالی تروریسم پیش از ارائه خدمات رمزارز و شناسایی تراکنش‌های پرریسک.
۲. ثبت رسمی ارائه‌دهندگان خدمات دارایی مجازی و الزام رعایت مقررات ضدپولشویی.
۳. جمع‌آوری و انتقال اطلاعات هویتی فرستنده و گیرنده تراکنش‌های مشمول.
٤. پایش تراکنش‌ها و گزارش تراکنش‌های مشکوک به نهادهای نظارتی.
٥. آموزش کارکنان و مقامات نظارتی برای مدیریت ریسک‌های دارایی مجازی و استفاده از ابزارهای تحلیل بلاکچین.
٦. اطلاع‌رسانی عمومی و مشارکت صرافی‌ها و کاربران در پیشگیری.
۷. درجه‌بندی اقدامات و مجازات‌ها متناسب با شدت تراکنش و تمرکز بر پیشگیری پیش‌دستانه پیش از وقوع جرم.

ادغام این موارد در سیاست تقنینی، امکان تطبیق مدل خطرمدار ایران با استانداردهای بین‌المللی و کاهش ریسک سوءاستفاده از رمزارزها را فراهم می‌آورد.

پیشنهادهای قضایی

حوزه قضایی در سیاست رمزارزها با چالش‌های ساختاری و عملی مواجه است. تحلیل نشان می‌دهد که ناشناسی تراکنش‌ها، فرامرزی بودن آن‌ها و ضعف تخصص قضات و ضابطان، موجب شده است اثبات جرم و پیگرد قانونی کلاهبرداری‌های رمزارزی دشوار باشد. این وضعیت زمینه افزایش بزهکاری یقه‌سفیدی و کاهش اثر بازدارندگی مجازات‌ها را فراهم کرده است (خلیلی پاجی، ۱۴۰۰، صص ۸۵-۸۹).

به نظر نگارنده، راهکار پیشنهادی بر اساس تحلیل خطرمدار؛ شامل ایجاد دادگاه‌های تخصصی جرایم رمزارز، آموزش تخصصی قضات و ضابطان برای ردیابی بلاکچین و درجه‌بندی مجازات‌ها بر اساس ریسک است. بدین معنا که جرایم کم‌ریسک مانند معاملات شخصی با مجازات نرم و جرایم پرریسک مانند پولشویی سازمان‌یافته با مجازات سنگین مواجه شوند. همچنین، استفاده از قرارهای تأمین خطرمدار، مانند نظارت الکترونیکی بر کیف پول‌ها، امکان پیشگیری از تکرار جرم پیش از صدور حکم نهایی را فراهم می‌کند.

بر این اساس، آموزش قضات با استفاده از ابزارهای تحلیلی داخلی، امکان اثبات قصد مجرمانه در کلاهبرداری‌های سایبری را افزایش می‌دهد و خلأهای اثباتی را کاهش می‌دهد. درجه‌بندی مجازات‌ها، ضمن رعایت اصل تناسب، از مجازات‌های حداکثری برای جرایم کم‌ریسک جلوگیری کرده و امکان کاهش پرونده‌های معلق را فراهم می‌آورد. تجربه سنگاپور در ایجاد دادگاه‌های تخصصی در دعاوی پیچیده بلاکچین و رمزارزها، نمونه‌ای موفق از این رویکرد است که می‌تواند به بومی‌سازی سیاست قضایی در ایران کمک کند (Pereire & Lin, 2025).

پیشنهادهای اجرایی و مشارکتی

سیاست اجرایی فعلی عمدتاً واکنشی است و فاقد سامانه‌های پیشگیرانه مؤثر برای تحلیل و شناسایی تراکنش‌های پرریسک است. تحلیل نشان می‌دهد که ایجاد سامانه ملی رصد تراکنش‌های بلاکچین، با استفاده از هوش مصنوعی و الگوریتم‌های داخلی، امکان شناسایی الگوهای پرریسک و پیشگیری پیش‌دستانه را فراهم می‌آورد (صفاری و همکاران، ۱۳۹۹، صص ۲۴۵-۲۴۶).

در این راستا و همانگونه که قبلا گفته شد ایران می‌تواند از روش مبتنی بر ریسک‌گروه ویژه اقدام مالی، برای اولویت‌بندی ریسک‌های داخلی استفاده کند. به عبارت دیگر، به جای اینکه قوانین ضدپولشویی یا نظارت را به طور یکسان و سختگیرانه روی همه اعمال کند (مثل چک کردن همه تراکنش‌های کوچک)، اول ریسک‌ها را ارزیابی کرده و منابع (زمان، پول، نیروی انسانی) را بر روی موارد پرریسک تمرکز می‌نماید. این روش حتی با وضعیت ترحیمی تحریمی ایران، دارای تأثیرات مفیدی است. به عنوان مثال، بانک مرکزی یا پلیس فتا ریسک‌های رمزارز داخل کشور (مثل تراکنش‌های پرحجم در صرافی‌های ایرانی) را اولویت‌بندی کرده و بدون نیاز به سیستم‌های خارجی، نظارتی هوشمندانه داشته باشد.

مدل پیشنهادی خطرمدار برای ایران

تحلیل ترکیبی نشان می‌دهد که یک مدل جامع خطرمدار برای ایران، باید شامل چهار مؤلفه اصلی باشد:

۱. پیشگیری چهارگانه: تقنینی، قضایی، اجرایی و مشارکتی
۲. جرم‌انگاری محدود و متناسب با ریسک
۳. نظارت داخلی خطرمحور و فرامرزی محدود
٤. مدیریت ریسک قضایی یا درجه بندی مجازات‌ها و ابزارهای پیش دستانه

این مدل، امکان گذار تدریجی اما پایدار به سیاست جنایی خطرمدار را فراهم می‌آورد. تلفیق این مؤلفه ها، ظرفیت پیشگیری پیش‌دستانه، بازدارندگی و بهره‌برداری اقتصادی از رمزارزها را به‌طور همزمان فعال می‌کند و سیاست را هم از نظر اقتصادی و هم از منظر امنیتی، تقویت می‌نماید.

به نظر نگارنده، پیشگیری چهارگانه به عنوان هسته مدل، هماهنگی نهادها را تضمین می‌کند، به گونه‌ای که تقنینی با قانون جامع و تعریف حقوقی رمزارز، قضایی با دادگاه تخصصی و آموزش بلاکچین، اجرایی با سامانه رصد داخلی و گزارش مشکوک و مشارکتی با آگاه‌سازی عمومی و همکاری صرافی‌ها. همچنین در جرم‌انگاری محدود، با تمرکز بر فعالیت‌های پرریسک، مانند عدم گزارش تراکنش‌های مشکوک، اصل تناسب را رعایت می‌کند. در بخش نظارت داخلی خطرمحور، با اولویت‌بندی تراکنش‌های پرحجم بدون وابستگی به سیستم‌های خارجی، در شرایط تحریم، عملی است. در نهایت در مدیریت ریسک قضایی نیز با درجه‌بندی مجازات‌ها و قرارهای تأمین، پیشگیری را پیش از حکم، تقویت می‌کند.

نتیجه‌گیری

این پژوهش با هدف ارزیابی سیاست جنایی ایران در مدیریت رمزارزها انجام شد و نشان داد که این سیاست، از ممنوعیت مطلق اولیه به سمت رویکرد نیمه‌خطرمدار گذار کرده، اما این گذار ناقص، واکنشی و بدون انسجام ساختاری باقی مانده است. تحلیل نشان می‌دهد که خلأهای قانونی، ضعف پیشگیری اجرایی، محدودیت‌های ناشی از تحریم‌ها، کارآمدی سیاست جنایی را محدود کرده‌اند و ریسک جرایم مانند پولشویی، کلاهبرداری و سوءاستفاده از تراکنش‌های ناشناس و غیره را افزایش داده‌اند.

تجربه بین‌المللی، به‌ویژه در اسناد گروه ویژه اقدام مالی، نشان می‌دهد که مدیریت ریسک رمزارزها بیش از آنکه مبتنی بر ممنوعیت یا کنترل مطلق باشد، نیازمند تنظیم‌گری خطرمحور، جرم‌انگاری محدود و نظارت پیش‌دستانه است. توصیه ۱۵ و گزارش‌های اجرای آن، الگوی حداقلی اما عملی برای ایجاد تعادل میان نوآوری اقتصادی و امنیت کیفری ارائه می‌دهند؛ الگویی که قابلیت بومی‌سازی در نظام حقوقی ایران را نیز دارد.

رویکرد فعلی، به‌ویژه در زمینه توصیه‌های مورد اشاره، همخوانی کامل ندارد و تمرکز اصلی بر بهره‌برداری اقتصادی (مانند مجوز استخراج) است، در حالی که پیشگیری پیش‌دستانه و مدیریت ریسک ساختاری در سطح ملی و فرامرزی محدود است. در شرایط تحریم‌های بین‌المللی، رمزارزها فرصت دور زدن محدودیت‌ها و تأمین ارز فراهم می‌کنند، اما بدون نظارت مؤثر، این فرصت به تهدید تبدیل شده و امکان سوءاستفاده مجرمانه افزایش می‌یابد.

به نظر نگارنده، رویکرد خطرمدار، با تمرکز بر مدیریت ریسک پیش از وقوع جرم، پیشگیری چهارگانه، جرم‌انگاری محدود و نظارت پیش‌دستانه، تعادل میان امنیت و نوآوری اقتصادی را برقرار می‌سازد، به گونه‌ای که مدلی عملی برای ایران ارائه می‌دهد و به ویژه چالش تحریم‌ها را حل می‌کند.

اجرای پیشنهادهایی مانند قانون جامع رمزارز، سامانه رصد داخلی، آموزش قضات و ضابطان و پیشگیری مشارکتی، نه تنها ریسک‌های مجرمانه را کاهش می‌دهد، بلکه امکان بهره‌برداری پایدار از مزایای اقتصادی رمزارزها، از جمله تقویت اقتصاد دیجیتال، جذب سرمایه‌گذاری و دور زدن تحریم‌ها را فراهم می‌سازد. این مدل، به‌واسطه تطبیق با شرایط خاص ایران و بهره‌گیری از تجربیات جهانی، نوآوری پژوهشی است و امنیت جامعه و اقتصاد دیجیتال را همزمان تقویت می‌کند.

منابع

احمدپور، محسن، و علوی رضوی، سید یحیی (۱۴۰۲). واکاوی تهدیدات و فرصت‌های رمزارزها بر امنیت اقتصادی به عنوان مولفه امنیت ملی. *نشریه پژوهش‌های پولی – بانکی*، (۵۸)، ۵۵۱–۵۷۷.

ایزدی، زهرا، و ارزانیان، نسترن (۱۳۹۸). پیشگیری از جرایم پولشویی و کلاهبرداری در بستر استفاده از رمزارزهای جهانی. *فصلنامه رهیافت پیشگیری از جرم*، (۱)، ۱–۵۰.

پاک‌نهاد، امیر (۱۳۸۸). *سیاست جنایی ریسک‌مدار* (چاپ اول). تهران: انتشارات بنیاد حقوقی میزان.

حسانی، جلال الدین، و دیگران (۱۴۰۰). رهیافت مدیریت ریسک جرم و جلوه‌های آن در نظام عدالت کیفری ایران. *فصلنامه حقوق کیفری و علوم جنایی*، (ویژه‌نامه)، ۶–۲۰.

خبرگزاری میزان (۱۴۰۳). *بررسی پرونده کلاهبرداری شبکه‌ای رمزارز جعلی کینگ‌مانی و صدور احکام سنگین قضایی*. خبرگزاری میزان. بازیابی شده از https://www.mizanonline.ir/fa/news/4800771/

خضری نیا، صادق (۱۴۰۳). *مبانی نظری و الزامات جرم‌انگاری و تعیین مجازات در قلمرو ارزهای دیجیتال* [رساله دکتری، دانشگاه آزاد اسلامی واحد چالوس].

خلیلی پاجی، عارف (۱۴۰۰). *تأثیر ارزهای مجازی بر جهانی شدن بزهکاری* [رساله دکتری، دانشگاه شهید بهشتی].

شاملو، باقر، و خلیلی پاجی، عارف (۱۳۹۹). سیاست‌گذاری جنایی ریسک‌مدار در برابر فناوری ارزهای مجازی. *فصلنامه مجلس و راهبرد*، (۱۰۳)، ۲۴۷–۲۷۸.

صفاری، علی، و دیگران (۱۳۹۹). کارکردهای مجرمانه ارزهای مجازی. *مجله اقتصاد و حقوق*، ۳–۲۸.

قائمی اصل، محمد (۱۴۰۴). *پیشگیری از فعالیت مجرمانه مرتبط با ارزهای مجازی در سیاست جنایی ایران* [رساله دکتری، دانشگاه آزاد اسلامی واحد اهواز].

گودرزی، مجتبی (۱۴۰۳). *سیاست جنایی ایران در قبال رمزارزها؛ با تأکید بر پیشگیری از پولشویی* [رساله دکتری، دانشگاه آزاد اسلامی واحد بین‌الملل کیش].

محمدی، امیرحسین (۱۴۰۳). *اباحه‌گری در حوزه رمزارزهای دیجیتال و تعارض با سیاست جنایی تقنینی* [رساله دکتری، دانشگاه آزاد اسلامی واحد سمنان].

میرمجیدی، 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.

نبوی، سید مهدی، و صابر، محمود (۱۳۹۹). مطالعه تطبیقی چالش‌های نظام عدالت کیفری ایران در دادرسی جرایم مرتبط با ارزهای مجازی. *فصلنامه تحقیقات حقوق تطبیقی*، ۵–۲۵.

نجفی ابرندآبادی، علی‌حسین (۱۳۸۸). کیفرشناسی نو ـ جرم‌شناسی نو؛ درآمدی بر سیاست جنایی مدیریتی خطرمدار. در علی‌حسین نجفی ابرندآبادی (به کوشش)، *تازه‌های علوم جنایی (مجموعه مقالات)*. تهران: انتشارات میزان.

احمدپور، محسن، و علوی رضوی، سید یحیی (۱۴۰۲). واکاوی تهدیدات و فرصت‌های رمزارزها بر امنیت اقتصادی به عنوان مولفه امنیت ملی. نشریه پژوهش‌های پولی – بانکی، (۵۸)، ۵۵۱–۵۷۷.

ایزدی، زهرا، و ارزانیان، نسترن (۱۳۹۸). پیشگیری از جرایم پولشویی و کلاهبرداری در بستر استفاده از رمزارزهای جهانی. فصلنامه رهیافت پیشگیری از جرم، (۱)، ۱–۵۰.

پاک‌نهاد، امیر (۱۳۸۸). سیاست جنایی ریسک‌مدار (چاپ اول). تهران: انتشارات بنیاد حقوقی میزان.

حسانی، جلال الدین، و دیگران (۱۴۰۰). رهیافت مدیریت ریسک جرم و جلوه‌های آن در نظام عدالت کیفری ایران. فصلنامه حقوق کیفری و علوم جنایی، (ویژه‌نامه)، ۶–۲۰.

خضری نیا، صادق (۱۴۰۳). مبانی نظری و الزامات جرم‌انگاری و تعیین مجازات در قلمرو ارزهای دیجیتال [رساله دکتری، دانشگاه آزاد اسلامی واحد چالوس].

خلیلی پاجی، عارف (۱۴۰۰). تأثیر ارزهای مجازی بر جهانی شدن بزهکاری [رساله دکتری، دانشگاه شهید بهشتی].

شاملو، باقر، و خلیلی پاجی، عارف (۱۳۹۹). سیاست‌گذاری جنایی ریسک‌مدار در برابر فناوری ارزهای مجازی. فصلنامه مجلس و راهبرد، (۱۰۳)، ۲۴۹–۲۵۱.

صفاری، علی، و دیگران (۱۳۹۹). کارکردهای مجرمانه ارزهای مجازی. مجله اقتصاد و حقوق، ۳–۲۸.

قائمی اصل، محمد (۱۴۰۴). پیشگیری از فعالیت مجرمانه مرتبط با ارزهای مجازی در سیاست جنایی ایران [رساله دکتری، دانشگاه آزاد اسلامی واحد اهواز].

گودرزی، مجتبی (۱۴۰۳). سیاست جنایی ایران در قبال رمزارزها؛ با تأکید بر پیشگیری از پولشویی [رساله دکتری، دانشگاه آزاد اسلامی واحد بین‌الملل کیش].

محمدی، امیرحسین (۱۴۰۳). اباحه‌گری در حوزه رمزارزهای دیجیتال و تعارض با سیاست جنایی تقنینی [رساله دکتری، دانشگاه آزاد اسلامی واحد سمنان].

میرمجیدی، 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.

نبوی، سید مهدی، و صابر، محمود (۱۳۹۹). مطالعه تطبیقی چالش‌های نظام عدالت کیفری ایران در دادرسی جرایم مرتبط با ارزهای مجازی. فصلنامه تحقیقات حقوق تطبیقی، ۵–۲۵.

نجفی ابرندآبادی، علی‌حسین (۱۳۸۸). کیفرشناسی نو ـ جرم‌شناسی نو؛ درآمدی بر سیاست جنایی مدیریتی خطرمدار. در علی‌حسین نجفی ابرندآبادی (به کوشش)، تازه‌های علوم جنایی (مجموعه مقالات). تهران: انتشارات میزان.

خبرگزاری میزان (۱۴۰۳). بررسی پرونده کلاهبرداری شبکه‌ای رمزارز جعلی کینگ‌مانی و صدور احکام سنگین قضایی. خبرگزاری میزان. بازیابی شده از https://www.mizanonline.ir/fa/news/480077/

Chainalysis. (2024). *2024 crypto crime report*. Chainalysis Inc. Retrieved from https://www.chainalysis.com/blog/2024-crypto-crime-report-introduction

Elliptic. (2021). *How Iran uses Bitcoin mining to evade sanctions*. Elliptic. Retrieved from https://www.elliptic.co/blog/analysis/how-iran-uses-bitcoin-mining-to-evade-sanctions

Faghih, A., Barzegarzadeh, A., & Safaei, M. (2025). A comparative analysis of legislative criminal policies in Iran and the United Kingdom in addressing cryptocurrency-related financial crimes. *Legal Studies in Digital Age, 4*(1). https://doi.org/10.61838/kman.lsda.157

Financial Action Task Force (FATF). (2019). *Recommendation 15: New technologies (2019 and targeted update 2025)*. Retrieved from https://www.fatf-gafi.org/en/topics/virtual-assets.html

Ghaemi Asl, M., Abolhasani, S., & Farhoud, N. (2025). Identifying and analyzing preventive components in Iran's criminal policy toward crimes related to virtual currencies to provide efficient solutions for improved effectiveness. *Legal Studies in Digital Age*. https://doi.org/10.61838/kman.lsda.231

Pereire, K., & Lin, Y. (2025). Blockchain & cryptocurrency laws and regulations 2026 – Singapore. In Global Legal Insights (Ed.), *Blockchain & cryptocurrency laws 2026*. Global Legal Group. Retrieved from https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/singapore/