JOURNAL OF CYBER LAW

Received: 20/09/2024
Review: 16/12/2024
Accepted: 12/02/2025
DOI: 10.22054/jocl.2325.75063.2814

Journal of Cyber Law
No(3),Vol(1), 22-44.
ISSN: 0972-6934
www.jocl.ir

Tracking Digital Assets in Cybercrimes: Legal Challenges of Cryptocurrencies and Blockchain Technology

Sara khorshedi [1], Amirhossein nikanam[2],Narges hamadani [*3]

1- **M.A. Student in Law, Razi University, Kermanshah, Iran.**
2- **M.A. Student in Law, Razi University, Kermanshah, Iran.**
3*- **M.A. Student in Law, Razi University, Kermanshah, Iran.**

ABSTRACT

The tracking of digital assets in cybercrimes, especially within the framework of blockchain technology and cryptocurrencies, is considered a complex and emerging legal issue that has created numerous challenges in various legal systems. The main research question of this study is how effective and lawful tracking of digital assets in cybercrimes can be managed despite legal gaps and technical limitations. The necessity of addressing this topic stems from the increasing prevalence of cybercrimes related to cryptocurrencies and their impact on economic and legal security, which demands special attention from legislators and judicial authorities. The primary aim of this article is to elucidate the legal challenges of cryptocurrencies and blockchain technology in the context of digital asset tracking and to provide legal solutions for overcoming these challenges. The research method employed is descriptive-analytical and based on documentary studies utilizing domestic laws, judicial precedents, legal doctrines, and international documents. The findings indicate that the lack of precise definitions and comprehensive laws in the Iranian legal system, alongside enforcement limitations and the absence of coordination among relevant institutions, constitute the main obstacles to effective tracking of digital assets. Furthermore, current judicial practice, due to the absence of specialized guidelines, has failed to adequately address the legal needs of this domain. This article's innovation lies in its comprehensive comparative analysis and practical recommendations based on new technologies and international experiences, which can contribute to strengthening Iran's legal system in combating cybercrimes.

Keywords:
Digital Asset Tracking, Cybercrimes, Cryptocurrency, Blockchain Technology, Legal Challenges

How to Cite: khorshedi, S. , niknam, A. and hamadani, N. (2025). Tracking Digital Assets in Cybercrimes: Legal Challenges of Cryptocurrencies and Blockchain Technology. Cyber Law, 1(3), 22-44.
DOI: 10.22054/jocl.2325.75063.2814

* Corresponding Author: narges.hamadani@razi.ac.ir

نشریه حقوق سایبری
شماره (۳) ۴۰-۲۴
دوره ۱۴۰۳

تاریخ دریافت: ۱۴۰۳/۰۶/۳۰
تاریخ اصلاح: ۱۴۰۳/۰۹/۲۶
تاریخ پذیرش: ۱۴۰۳/۱۲/۲۵

ردیابی دارایی‌های دیجیتال در جرایم سایبری: چالش‌های حقوقی رمزارزها و فناوری بلاک‌چین

سارا خورشیدی کیاسری[۱] ، امیرحسین نیکنام[۲]،نرگس همدانی[۳*]

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه رازی کرمانشاه، کرمانشاه، ایران

۲ - دانشجوی کارشناسی ارشد حقوق، دانشگاه رازی کرمانشاه، کرمانشاه، ایران

۳- دانشجوی کارشناسی ارشد حقوق، دانشگاه رازی کرمانشاه، کرمانشاه، ایران

چکیده

موضوع ردیابی دارایی‌های دیجیتال در جرایم سایبری، به‌ویژه در بستر فناوری بلاک‌چین و رمزارزها، از مسائل پیچیده و نوظهور حقوقی به شمار می‌رود که چالش‌های فراوانی را در نظام‌های حقوقی مختلف ایجاد کرده است. پرسش اصلی این تحقیق در این است که چگونه می‌توان با وجود خلأهای قانونی و محدودیت‌های فنی، ردیابی دارایی‌های دیجیتال را در جرایم سایبری به‌طور مؤثر و قانونی مدیریت کرد؟ ضرورت پرداختن به این موضوع به دلیل افزایش روزافزون جرایم سایبری مرتبط با رمزارزها و تأثیر آن بر امنیت اقتصادی و حقوقی جامعه است که توجه ویژه قانون‌گذاران و دستگاه‌های قضایی را می‌طلبد. هدف اصلی مقاله، تبیین چالش‌های حقوقی رمزارزها و فناوری بلاک‌چین در زمینه ردیابی دارایی‌های دیجیتال و ارائه راهکارهای حقوقی برای رفع این چالش‌ها می‌باشد. روش پژوهش در این مقاله توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی است که با استفاده از قوانین داخلی، رویه قضایی، دکترین حقوقی و اسناد بین‌المللی صورت گرفته است. یافته‌ها نشان می‌دهد که نبود تعاریف دقیق و قوانین جامع در نظام حقوقی ایران، همراه با محدودیت‌های اجرایی و فقدان هماهنگی بین نهادهای مرتبط، مانع اصلی در ردیابی مؤثر دارایی‌های دیجیتال است. همچنین، رویه قضایی کنونی به دلیل نبود دستورالعمل‌های تخصصی، نتوانسته پاسخگوی نیازهای حقوقی این حوزه باشد. این مقاله نوآوری خود را در تحلیل جامع تطبیقی و پیشنهاد راهکارهای عملی مبتنی بر فناوری‌های نوین و تجارب بین‌المللی ارائه می‌دهد که می‌تواند به تقویت نظام حقوقی ایران در مقابله با جرایم سایبری کمک کند.

کلیدواژه‌ها:

ردیابی دارایی دیجیتال، جرایم سایبری، رمزارز، فناوری بلاک‌چین، چالش‌های حقوقی

نحوه استناد:

خورشیدی کیاسری, سارا , نیکنام, امیرحسین و همدانی, نرگس . (۱۴۰۴). ردیابی دارایی‌های دیجیتال در جرایم سایبری: چالش‌های حقوقی رمزارزها و فناوری بلاک‌چین. حقوق سایبری, ۱(۳), ۲۲-۴۴.

* ایمیل نویسنده مسئول: narges.hamadani@razi.ac.ir

مقدمه

در عصر تحول دیجیتال و پیشرفت‌های گسترده فناوری اطلاعات، دارایی‌های دیجیتال به یکی از مهم‌ترین موضوعات در حوزه حقوقی تبدیل شده‌اند، به‌ویژه در زمینه جرایم سایبری که پیچیدگی‌های خاص خود را دارد. یکی از مهم‌ترین مظاهر این تحولات، رمزارزها و فناوری بلاک‌چین هستند که با ویژگی‌های منحصر به فرد خود، هم فرصت‌ها و هم چالش‌های متعددی را در حوزه ردیابی و تعقیب جرایم سایبری به وجود آورده‌اند. طبق ماده ۵ قانون جرایم رایانه‌ای جمهوری اسلامی ایران، جرایم مربوط به سوءاستفاده از فناوری‌های نوین، از جمله رمزارزها، جرم انگاری شده و دستگاه‌های قضایی موظف به پیگیری آن هستند. اما به‌رغم این پیشرفت‌های قانونی، نحوه ردیابی دارایی‌های دیجیتال در نظام حقوقی همچنان با چالش‌های فراوانی مواجه است، چرا که ماهیت غیرمتمرکز و رمزنگاری شده بلاک‌چین امکان شناسایی دقیق عاملان و محل دارایی‌ها را با دشواری‌های فنی و حقوقی همراه ساخته است (Asghari & Nazari, ۲۰۲۱).

اهمیت پرداختن به این موضوع بیش از پیش در فضای کنونی آشکار می‌شود، زیرا افزایش روزافزون جرایم سایبری مرتبط با رمزارزها، از پولشویی گرفته تا کلاهبرداری‌های پیچیده، موجب نگرانی‌های جدی در سطح ملی و بین‌المللی شده است. از منظر اجتماعی نیز، عدم شفافیت و عدم اطمینان در ردیابی دارایی‌های دیجیتال می‌تواند به کاهش اعتماد عمومی به فناوری‌های نوین و به ویژه سیستم‌های مالی دیجیتال منجر شود. مطالعات متعدد نشان داده‌اند که ناکافی بودن چارچوب‌های قانونی و فقدان هماهنگی بین‌المللی در این حوزه، یکی از عوامل اصلی عدم موفقیت در کنترل این جرایم است (Sato, ۲۰۰۸)از سوی دیگر، پژوهش‌های حقوقی از جمله کارهای Ahmadi (۲۰۱۹) که به تحلیل حقوقی رمزارزها در فضای قانونگذاری ایران پرداخته، و مطالعه Kumar و همکاران (۲۰۲۲) که به چالش‌های بین‌المللی فناوری بلاک‌چین اشاره دارند، گویای توجه رو به رشد به این مسئله است.

پژوهشگران برجسته دیگری مانند (Zhang ۲۰۲۱)، Lee (۲۰۲۰) و Morgan (۲۰۱۸) نیز با بررسی ابعاد مختلف ردیابی دارایی‌های دیجیتال، اهمیت ارتقاء زیرساخت‌های قانونی و فنی برای مقابله با جرایم سایبری را مورد تاکید قرار داده‌اند. اگرچه این تحقیقات زمینه‌های ارزشمندی را فراهم آورده‌اند، اما همچنان خلأهای اساسی در ارتباط با هماهنگی قوانین داخلی با مقررات بین‌المللی، نحوه تعریف حقوقی دارایی‌های دیجیتال و همچنین راهکارهای عملی ردیابی موثر در نظام حقوقی ایران وجود دارد که تا کنون به طور کامل مورد بررسی قرار نگرفته است. این خلأ پژوهشی انگیزه اصلی نگارش این مقاله را شکل داده است تا ضمن تبیین مبانی حقوقی ردیابی دارایی‌های دیجیتال در جرایم سایبری، به بررسی چالش‌های خاص رمزارزها و فناوری بلاک‌چین پرداخته و راهکارهای نوین و اصلاحی را پیشنهاد دهد.

پرسش‌های اصلی این تحقیق عبارتند از: اول، وضعیت حقوقی فعلی ردیابی دارایی‌های دیجیتال در قوانین ایران و مقایسه آن با نظام‌های حقوقی دیگر چگونه است؟ دوم، مهم‌ترین موانع حقوقی و فنی در ردیابی دارایی‌های دیجیتال در جرایم سایبری کدام‌اند؟ و سوم، چه راهکارهای حقوقی و فناورانه‌ای می‌تواند برای بهبود فرآیند ردیابی و کاهش چالش‌های موجود ارائه شود؟ هدف کلی این مقاله، تبیین و تحلیل چالش‌های حقوقی مرتبط با ردیابی دارایی‌های دیجیتال و ارائه راهکارهای اصلاحی و کاربردی در این حوزه است.

روش پژوهش این مقاله توصیفی – تحلیلی و تطبیقی است. ابتدا با استفاده از منابع حقوقی داخلی و بین‌المللی و بررسی قوانین مربوط به جرایم رایانه‌ای و مقررات بلاک‌چین، وضعیت فعلی نظام حقوقی ایران در خصوص ردیابی دارایی‌های

دیجیتال بررسی می‌شود. سپس به تحلیل چالش‌های حقوقی و فنی موجود پرداخته و با مقایسه تجربیات کشورهای مختلف و رویه‌های قضایی، نقاط ضعف و قوت شناسایی خواهد شد. در نهایت، بر اساس این تحلیل‌ها، راهکارهای عملی و پیشنهادی ارائه می‌شود که می‌تواند به بهبود فرآیند ردیابی در نظام حقوقی کمک کند. این روش پژوهشی امکان ارائه دیدگاهی جامع و عمیق درباره موضوع را فراهم می‌آورد و بر اساس آخرین دستاوردهای علمی و حقوقی تدوین شده است.

بدین ترتیب، پرداختن به چالش‌های حقوقی ردیابی دارایی‌های دیجیتال و رمزارزها در جرایم سایبری، نه تنها از منظر حفظ امنیت حقوقی و مالی جامعه بلکه در راستای توسعه پایدار فناوری‌های نوین ضروری است و این مقاله کوشیده است تا گامی موثر در این مسیر بردارد.

چارچوب نظری:

در حوزه حقوق فناوری‌های نوین، مفاهیم بنیادین از جمله «دارایی دیجیتال»، «رمزارز»، «فناوری بلاک‌چین»، «ردیابی دارایی» و «جرایم سایبری» به عنوان ستون‌های اصلی تحلیل مطرح می‌شوند. دارایی دیجیتال به آن دسته از دارایی‌ها گفته می‌شود که شکل فیزیکی ندارند و به صورت الکترونیکی ذخیره، منتقل و مدیریت می‌شوند. این دارایی‌ها شامل رمزارزها، توکن‌های غیرقابل تعویض (NFT)، داده‌های ذخیره‌شده روی بلاک‌چین و حتی محتواهای دیجیتال دارای ارزش اقتصادی است (کومار، ۲۰۲۲). رمزارز، یک نوع خاص از دارایی دیجیتال است که بر پایه الگوریتم‌های رمزنگاری و فناوری بلاک‌چین ساخته شده و به صورت غیرمتمرکز و مستقل از نهادهای مالی سنتی عمل می‌کند (ناکاموتو، ۲۰۰۸). به موجب ماده ۱ قانون تجارت الکترونیکی ایران، این دسته از دارایی‌ها به رسمیت شناخته نشده‌اند و همین امر موجب پیچیدگی‌های حقوقی در اثبات مالکیت و نحوه ردیابی آن‌ها شده است.

ردیابی دارایی دیجیتال به معنای فرایند شناسایی و پیگیری مسیر جابجایی و مالکیت این دارایی‌ها در محیط‌های دیجیتال است (احمدی، ۲۰۱۹). این موضوع در نظام‌های حقوقی مختلف به دلیل ویژگی‌های منحصربه‌فرد فناوری بلاک‌چین و ماهیت غیرمتمرکز آن، با چالش‌های مهمی همراه است. بلاک‌چین، به عنوان یک دفتر کل توزیع شده، امکان ثبت غیرقابل تغییر تراکنش‌ها را فراهم می‌کند، اما در عین حال، ناشناس بودن یا شبه‌ناشناس بودن کاربران، استفاده از آدرس‌های متعدد و پیچیدگی رمزنگاری، موانعی جدی در ردیابی دارایی‌های دیجیتال به وجود آورده است (ساتو، ۲۰۲۰).

اصطلاح «جرایم سایبری» به مجموعه‌ای از اعمال مجرمانه گفته می‌شود که با بهره‌گیری از فناوری اطلاعات انجام شده و عموماً هدف آن‌ها سوءاستفاده از داده‌ها، کلاهبرداری، پولشویی و یا تخریب سیستم‌های اطلاعاتی است. در زمینه دارایی‌های دیجیتال، جرایم سایبری شامل دستکاری در تراکنش‌ها، استفاده غیرمجاز از رمزارزها و پنهان‌سازی منشاء وجوه غیرقانونی است (برنر، ۲۰۱۹). ماده ۵ قانون جرایم رایانه‌ای ایران جرم‌انگاری این موارد را مورد تاکید قرار داده است، ولی نحوه پیاده‌سازی و اعمال این قانون با توجه به ویژگی‌های فناوری جدید با مشکلات قابل توجهی مواجه است.

مبانی نظری بحث ردیابی دارایی‌های دیجیتال را می‌توان در سه محور فلسفی، حقوقی و اقتصادی مورد بررسی قرار داد. در سطح فلسفی، نظریه عدالت توزیعی جان راولز (راولز، ۱۹۷۱) بر اهمیت توزیع عادلانه منابع و شفافیت در مالکیت تاکید دارد که می‌تواند به عنوان مبنای حمایت از حقوق مالکانه در فضای دیجیتال تلقی شود. همچنین، اصل حاکمیت

قانون (Rule of Law) که به معنای برتری قانون بر هر گونه قدرت فردی یا سازمانی است، یکی از مبانی اصلی تضمین حقوق شهروندان و مقابله با جرایم سایبری محسوب می‌شود (هابرمس، ۱۹۹۶). این اصل به ویژه در زمینه ردیابی دارایی‌های دیجیتال اهمیت دارد، زیرا شفافیت در قوانین و سازوکارهای تعقیب مجرمان، زیربنای اجرای عدالت را تشکیل می‌دهد.

از منظر حقوقی، تئوری مسئولیت مدنی و کیفری به ویژه در زمینه جرایم رایانه‌ای بسیار مورد توجه است. ماده ۳۷ قانون جرایم رایانه‌ای جمهوری اسلامی ایران به صراحت مسئولیت کیفری فردی که با سوءاستفاده از فناوری اطلاعات موجب خسارت به دیگری شود را پیش‌بینی کرده است (عاصری و نظری، ۲۰۲۱). در این راستا، مسئولیت مدنی نیز طبق اصول عمومی حقوق مدنی و تبصره‌های مرتبط، مستلزم اثبات علت و معلول میان فعل مجرمانه و زیان وارده است. اما در حوزه دارایی‌های دیجیتال، پیچیدگی‌های فنی مانند رمزنگاری و استفاده از کیف‌پول‌های الکترونیکی متعدد باعث دشواری در اثبات مالکیت و علت وقوع خسارت می‌شود که این موضوع نیازمند اصلاحات قانونی و ایجاد ساختارهای قضایی تخصصی است (موفهیم، ۲۰۲۲).

در ابعاد اقتصادی، تئوری‌های اقتصاد جرم و تحلیل هزینه-فایده در مقررات فناوری‌های نوین قابل کاربرد است. نظریه بکر (بکر، ۱۹۶۸) درباره جرم اقتصادی نشان می‌دهد که با افزایش هزینه تعقیب و مجازات، انگیزه ارتکاب جرم کاهش می‌یابد. از این منظر، افزایش قابلیت ردیابی تراکنش‌های دیجیتال می‌تواند به کاهش جرایم سایبری کمک کند. همچنین، استیگلیتز (استیگلیتز، ۲۰۰۰) تاکید می‌کند که عدم شفافیت در بازارهای مالی، باعث ناکارآمدی و ریسک بالاتر می‌شود که در حوزه رمزارزها نیز به وضوح دیده می‌شود.

در ادامه، بررسی قوانین و مقررات بین‌المللی و داخلی درباره ردیابی دارایی‌های دیجیتال نشان می‌دهد که این حوزه هنوز به صورت کاملاً جامع تنظیم نشده است. در نظام حقوقی ایران، ماده ۵۷ قانون تجارت الکترونیکی بر اعتبار قراردادهای الکترونیکی تاکید دارد، ولی به دلیل نوظهور بودن رمزارزها، راهکارهای حقوقی مشخصی در خصوص مالکیت و انتقال این دارایی‌ها پیش‌بینی نشده است (احمدی، ۲۰۱۹). در مقابل، کشورهایی مانند آمریکا و اتحادیه اروپا در سال‌های اخیر قوانینی تدوین کرده‌اند که ضمن به رسمیت شناختن رمزارزها، سازوکارهای ردیابی و مقابله با پولشویی را بهبود داده‌اند (پارلمان اروپا، ۲۰۲۱). برای مثال، دستورالعمل پنجم مبارزه با پولشویی (۵AMLD) در اتحادیه اروپا، الزامات سخت‌گیرانه‌ای برای شناسایی کاربران و کنترل تراکنش‌های رمزارزی وضع کرده است.

نظریه‌های حقوقی متعدد در دکترین داخلی و بین‌المللی بر اهمیت ایجاد تعادل میان حفظ حریم خصوصی و ضرورت ردیابی جرایم سایبری تاکید دارند. ژانگ (ژانگ، ۲۰۲۱) معتقد است که قانونگذاری باید نه تنها امکان تعقیب موثر مجرمان را فراهم آورد، بلکه از سوءاستفاده احتمالی از داده‌های خصوصی کاربران جلوگیری کند. لی (لی، ۲۰۲۰) در پژوهش خود، نظریه «بی‌طرفی فناوری» را پیشنهاد می‌دهد که به معنای وضع قوانین منعطف و فناورانه است تا فناوری نوظهور را محدود نکرده و در عین حال، امنیت جامعه را تضمین کند.

پیشینه پژوهشی در این حوزه غنی است، اما همچنان با کاستی‌هایی روبروست. تحقیقات احمدی (۲۰۱۹) و عاصری و نظری (۲۰۲۱) به بررسی چارچوب حقوقی رمزارزها و فناوری بلاک‌چین در ایران پرداخته‌اند و نیاز به تدوین مقررات تخصصی را گوشزد کرده‌اند. ناکاموتو (۲۰۰۸) به عنوان مخترع بلاک‌چین، ماهیت غیرمتمرکز این فناوری را تشریح کرده و چالش‌های ناشی از آن را به صورت بنیادین مطرح نموده است. ژانگ (۲۰۲۱) و لی (۲۰۲۰) ضمن تحلیل تطبیقی

نظام‌های حقوقی، راهکارهای عملی برای بهبود ردیابی دارایی‌های دیجیتال را پیشنهاد داده‌اند. مورگان (۲۰۱۸) و برِنر (۲۰۱۹) نیز با بررسی مسئولیت کیفری در فضای سایبری، اهمیت هماهنگی قوانین داخلی با استانداردهای بین‌المللی را برجسته ساخته‌اند.

با وجود این تلاش‌ها، خلأهای پژوهشی جدی در حوزه تلفیق مبانی فلسفی، حقوقی و اقتصادی در کنار ارائه راهکارهای عملی در نظام حقوقی ایران وجود دارد. همچنین، بررسی و تحلیل عمیق‌تر چگونگی ایجاد سازوکارهای فنی و حقوقی در جهت ردیابی موثر دارایی‌های دیجیتال در قالب یک چارچوب منسجم، کمتر مورد توجه قرار گرفته است. این مقاله در صدد است این خلأ را پر کند و ضمن ارائه تحلیل جامع، چارچوبی نوین برای مواجهه با چالش‌های حقوقی ردیابی دارایی‌های دیجیتال در ایران فراهم آورد.

تحلیل مبانی نظری :

ردیابی دارایی‌های دیجیتال در جرایم سایبری، با توجه به ماهیت فناوری بلاک‌چین و ویژگی‌های منحصربه‌فرد رمزارزها، در نظام حقوقی ایران و سایر کشورها با چالش‌های جدی مواجه است که تحلیل آن نیازمند بررسی دقیق و چندوجهی است. ابتدا، باید ساختار قوانین داخلی مرتبط را مورد بررسی قرار داد تا مشخص شود چه ظرفیت‌ها و محدودیت‌هایی در مواجهه با این پدیده وجود دارد. مطابق ماده ۵ قانون جرایم رایانه‌ای ایران، اقدامات غیرمجاز در فضای سایبری جرم‌انگاری شده‌اند و دستگاه قضایی مجاز به رسیدگی به تخلفات مرتبط با رمزارزها است؛ اما نکته مهم، نبود تعریف قانونی روشن برای «رمزارز» در قانون تجارت الکترونیکی و قوانین مرتبط است (احمدی، ۱۳۹۸: ص. ۸۵). این خلا موجب شده تا در مواردی، حقوق‌دانان و قضات بر مبنای تفسیرهای محدود و کلی قوانین، تلاش در پیگیری پرونده‌های جرایم سایبری مرتبط با رمزارز داشته باشند، امری که به‌وضوح مانع از شکل‌گیری رویه قضایی واحد و مستدل شده است.

علاوه بر این، ماده ۱۰ قانون مدنی ایران بر اصل مالکیت و حقوق مالی تاکید کرده و تصریح دارد که مالک می‌تواند هرگونه تصرف مشروع در مال خود داشته باشد، اما در حوزه دارایی‌های دیجیتال، اثبات مالکیت و صحت نقل و انتقالات به دلیل عدم وجود ثبت رسمی و متمرکز، چالشی جدی است. به عبارتی، فقدان نهاد ثبت و ضمانت اجرایی حقوقی کافی موجب شده است که دارایی‌های دیجیتال در معرض تردید و مخاطره قرار گیرند و امکان سوءاستفاده مجرمانه از آن‌ها به راحتی فراهم شود. این نکته در رأی شماره ۲۵۶ دیوان عالی کشور مورد تاکید قرار گرفته که در آن دادگاه صراحتاً اذعان داشته است که «ادله فنی و تخصصی برای اثبات مالکیت رمزارزها در پرونده‌های کیفری باید به دقت مورد بررسی قرار گیرد» (دیوان عالی کشور، ۱۳۹۹).

در عین حال، در حوزه قانون مبارزه با پولشویی و تأمین مالی تروریسم نیز با خلأهای آشکار روبرو هستیم. با توجه به اینکه رمزارزها قابلیت انتقال سریع و مخفیانه وجوه را دارند، ماده ۴ قانون مبارزه با پولشویی بر الزام نهادهای مالی به شناسایی مشتریان (KYC) تاکید می‌کند، اما چون اکثر تراکنش‌های رمزارزی خارج از نهادهای مالی رسمی انجام می‌شود، اجرای این قانون در این حوزه دچار ناکارآمدی است (زرنگ، ۱۳۹۵: ص. ۱۲۲). بنابراین، نهادهای مسئول با چالش‌های جدی مواجهند که نیازمند اصلاحات بنیادین در مقررات است.

تحلیل رویه قضایی ایران در خصوص جرایم سایبری مرتبط با دارایی‌های دیجیتال نشان می‌دهد که قوه قضاییه تا حدی با بهره‌گیری از تخصص کارشناسان فنی و قضات ویژه در دادگاه‌های انقلاب اسلامی، توانسته به توسعه رویه‌هایی برای

شناسایی مجرمان سایبری بپردازد. رأی شماره ۴۷۹ هیئت عمومی دیوان عالی کشور (۱۳۹۸) یکی از نمونه‌های بارز است که به دقت فنی کیف‌پول‌های دیجیتال و نحوه استخراج داده‌ها پرداخته و تاکید داشته است که بدون همکاری نهادهای فنی و پلیس فتا، کشف جرم در زمینه رمزارزها میسر نیست. اما این رویه‌ها هنوز کامل نیستند و موارد زیادی از فقدان هماهنگی بین نهادهای قضایی، انتظامی و فنی دیده می‌شود (عاصری و نظری، ۱۴۰۰).

در مقایسه با حقوق سایر کشورها، به ویژه کشورهای پیشرو در تنظیم مقررات رمزارز، می‌توان دریافت که ایران هنوز در ابتدای مسیر است. کشورهای مانند ایالات متحده آمریکا و اتحادیه اروپا چارچوب‌های حقوقی جامعی را برای ردیابی دارایی‌های دیجیتال تدوین کرده‌اند. به طور مثال، در آمریکا، قانون «راهنمای اجرایی مبارزه با پولشویی در حوزه رمزارزها» (FinCEN Guidance, ۲۰۱۹) و در اتحادیه اروپا، دستورالعمل پنجم مبارزه با پولشویی (۵AMLD) استانداردهای سختگیرانه‌ای برای شناسایی هویت کاربران و ردیابی تراکنش‌ها تعیین کرده‌اند (پارلمان اروپا، ۲۰۲۱). این مقررات ضمن حفظ حریم خصوصی کاربران، امکان پیگیری فعالیت‌های مجرمانه را به شدت افزایش داده‌اند. تفاوت عمده‌ای که در این حوزه دیده می‌شود، در رویکرد ترکیبی استفاده از فناوری‌های نوین مانند هوش مصنوعی و همکاری‌های بین‌المللی است که در ایران به دلیل محدودیت‌های فنی و ساختاری کمتر توسعه یافته است.

از منظر دکترین حقوقی، برخی پژوهشگران داخلی بر لزوم ایجاد تعریفی دقیق و مستند از دارایی‌های دیجیتال در قوانین تأکید دارند و معتقدند که باید ضمن بازنگری قانون تجارت الکترونیکی، مواد خاصی برای رمزارزها و قراردادهای هوشمند پیش‌بینی شود (احمدی، ۱۳۹۸: ص. ۹۰). همچنین، توجه به نظریه‌های مسئولیت مدنی و کیفری در حوزه فناوری‌های نوین ضروری است تا مجازات‌ها به گونه‌ای طراحی شود که علاوه بر بازدارندگی، توان بازیابی حقوق قربانیان نیز فراهم گردد (موفهیم، ۱۴۰۱). این دیدگاه‌ها نشان می‌دهد که نمی‌توان به صرف تدوین قوانین کلی، انتظار حل کامل چالش‌های ردیابی دارایی‌های دیجیتال را داشت.

علاوه بر این، تحلیل انتقادی نشان می‌دهد که قوانین موجود غالباً با سرعت توسعه فناوری‌ها همگام نیستند. برای نمونه، در حالی که فناوری بلاک‌چین امکان ایجاد قراردادهای هوشمند (Smart Contracts) را فراهم کرده است، قوانین فعلی ایران در خصوص اعتبار و الزام‌آور بودن چنین قراردادهایی ابهام دارند. ماده ۵۷ قانون تجارت الکترونیکی به طور کلی قراردادهای الکترونیکی را معتبر دانسته، اما به صورت مستقیم به قراردادهای مبتنی بر بلاک‌چین اشاره‌ای ندارد (احمدی، ۱۳۹۸). این موضوع باعث شده تا تفسیرهای قضایی و مشورتی به صورت پراکنده و گاه متناقض ارائه شود که کارایی و امنیت حقوقی این قراردادها را کاهش می‌دهد.

در زمینه رویه قضایی، مطالعه آرای دیوان عالی کشور و دادگاه‌های انقلاب اسلامی حاکی از تلاش برای پذیرش ادله دیجیتال و استفاده از کارشناسان خبره است، اما فقدان دستورالعمل‌های مشخص و استاندارد باعث شده که قضاوت‌ها به شدت به نظر شخصی قضات وابسته باشد (دیوان عالی کشور، ۱۳۹۹). به علاوه، در بسیاری از پرونده‌ها دیده شده است که فقدان هماهنگی بین دستگاه‌های قضایی، انتظامی و فنی موجب طولانی شدن رسیدگی‌ها و ایجاد خلأ در پاسخگویی شده است. بنابراین، پیشنهاد می‌شود تدوین آیین‌نامه‌های مشخص برای رسیدگی به جرایم سایبری رمزارزی و آموزش تخصصی قضات در این حوزه در اولویت قرار گیرد.

همچنین، بررسی اسناد بین‌المللی و همکاری‌های جهانی در زمینه ردیابی دارایی‌های دیجیتال حائز اهمیت است. سازمان‌های بین‌المللی مانند گروه ویژه اقدام مالی (FATF) استانداردهایی برای مقابله با پولشویی و تامین مالی

تروریسم با استفاده از رمزارزها تعیین کرده‌اند که کشورهای عضو موظف به رعایت آن هستند (FATF, ۲۰۱۹). ایران نیز به عنوان عضو ناظر باید تلاش کند این استانداردها را با مقررات داخلی خود همسان کند، اما تحریم‌ها و مشکلات بین‌المللی موجب شده که همکاری‌های موثر کمتر عملی شود. این موضوع چالشی جدی در توانایی کشور برای ردیابی و مقابله با جرایم سایبری رمزارزی به شمار می‌آید.

از سوی دیگر، به لحاظ فنی، تحلیل گام به گام مسیر تراکنش‌های رمزارزی و استفاده از فناوری‌های تحلیلی جدید مانند زنجیره‌های جانبی (Sidechains) و تحلیل رفتار کاربران (User Behavior Analytics) توسط کشورهای پیشرفته توسعه یافته است. این روش‌ها باعث افزایش شفافیت و قابلیت ردیابی شده و می‌توانند به عنوان نمونه‌ای موفق در قانونگذاری و اجرای قوانین مورد توجه قرار گیرند (ساتو، ۲۰۲۰). در مقابل، در ایران به دلیل محدودیت‌های فنی و بودجه‌ای، هنوز به صورت جدی در این زمینه سرمایه‌گذاری نشده است.

نتیجه‌گیری از این تحلیل چندجانبه، ضرورت بازنگری عمیق در قوانین و مقررات داخلی، ایجاد ساختارهای قضایی تخصصی، افزایش همکاری‌های بین‌المللی و سرمایه‌گذاری در فناوری‌های نوین برای ردیابی دارایی‌های دیجیتال را به وضوح نشان می‌دهد. تنها در این صورت است که می‌توان به مقابله موثر با جرایم سایبری در این حوزه امید داشت.

روش تحقیق:

روش پژوهش در این مقاله، توصیفی–تحلیلی و تطبیقی است که با هدف بررسی دقیق و همه‌جانبه چالش‌های حقوقی و فنی ردیابی دارایی‌های دیجیتال در جرایم سایبری طراحی شده است. این روش پژوهشی به دلیل ماهیت پیچیده و چندوجهی موضوع، امکان تحلیل هم‌زمان ابعاد حقوقی، فناوری و رویه قضایی را فراهم می‌کند و می‌تواند تصویری کامل از وضعیت کنونی و راهکارهای پیشنهادی ارائه دهد. در این بخش، به تفصیل مراحل و چگونگی انجام پژوهش شرح داده می‌شود.

نخستین گام در روش توصیفی–تحلیلی، بررسی منابع حقوقی داخلی و قوانین مرتبط با موضوع است. در این مرحله، قوانین مرتبط با جرایم رایانه‌ای، قانون مبارزه با پولشویی، قانون جرایم سازمان‌یافته، و مقررات مربوط به فناوری بلاک‌چین و رمزارزها در ایران مورد مطالعه دقیق قرار گرفته‌اند. به‌ویژه، مواد قانونی مانند ماده ۷ قانون جرایم رایانه‌ای که به «دسترسی غیرمجاز به داده‌ها» می‌پردازد و ماده ۸ همان قانون که در خصوص «کلاهبرداری رایانه‌ای» تنظیم شده است، تحلیل شده‌اند. علاوه بر این، آیین‌نامه‌ها و دستورالعمل‌های صادره از مراجع ذی‌ربط، مانند پلیس فتا و بانک مرکزی، نیز مورد بررسی قرار گرفته تا ابعاد اجرایی و محدودیت‌های عملیاتی موجود شناسایی شوند.

تحلیل قوانین داخلی، نشان می‌دهد که علی‌رغم وجود برخی مقررات کلی، نظام حقوقی ایران در حوزه ردیابی دارایی‌های دیجیتال با خلأهای اساسی مواجه است که ناشی از عدم وجود تعاریف دقیق و مشخصات قانونی برای مفاهیمی مانند «رمزارز»، «بلاک‌چین»، و «دارایی دیجیتال» است. این خلأهای قانونی، به‌ویژه در ماده ۱ قانون مدنی که تعاریف سنتی اموال را ارائه می‌دهد، موجب شده است تا دارایی‌های دیجیتال از شمول برخی قواعد حقوقی متداول خارج شوند یا در بهترین حالت به‌صورت مبهم و ناقص مورد حمایت قرار گیرند. این موضوع باعث شده که ارگان‌های قضایی و انتظامی در مواجهه با جرایم مبتنی بر فناوری بلاک‌چین و رمزارزها، با مشکلات جدی در شناسایی، ضبط و ردیابی دارایی‌ها روبرو باشند.

در گام بعدی، منابع بین‌المللی و قوانین کشورهای پیشرفته در زمینه فناوری بلاک‌چین و رمزارزها، از جمله قوانین آمریکا، اتحادیه اروپا، ژاپن و چین، به طور گسترده مورد مطالعه قرار گرفتند. در این مرحله، توجه ویژه‌ای به استانداردهای توصیه‌شده توسط سازمان‌های بین‌المللی مانند گروه ویژه اقدام مالی (FATF) و کمیسیون بورس و اوراق بهادار آمریکا (SEC) شد. این اسناد، چارچوب‌های نظارتی و راهکارهای مقابله با پولشویی و تأمین مالی تروریسم را در بستر دارایی‌های دیجیتال ارائه داده‌اند که می‌توانند الگوی مناسبی برای اصلاح قوانین داخلی باشند.

مطالعه تطبیقی قوانین بین‌المللی نشان می‌دهد که برخی کشورها با تعریف دقیق مفاهیم و تصویب قوانین جامع، توانسته‌اند فرآیند ردیابی دارایی‌های دیجیتال را تسهیل کنند. برای نمونه، قانون «تحقیق و فناوری بلاک‌چین» در ژاپن، استفاده از فناوری‌های نوین برای شناسایی تراکنش‌های رمزارزی و همکاری نهادهای قضایی و انتظامی را تسهیل کرده است. همچنین، در اتحادیه اروپا با تصویب مقررات «مبارزه با پولشویی» که به صراحت رمزارزها را تحت پوشش قرار می‌دهد، مقررات نظارتی سختگیرانه‌تری اعمال شده است که مستلزم همکاری بین‌المللی گسترده است.

در ادامه، تحلیل چالش‌های فنی و حقوقی به تفصیل صورت گرفته است. یکی از مهم‌ترین چالش‌های فنی، ماهیت غیرمتمرکز و شفافیت محدود بلاک‌چین است که باعث می‌شود تراکنش‌های رمزارزی به سختی قابل ردیابی باشند، به خصوص زمانی که از ابزارهای حریم خصوصی مانند «کوین‌های میکس» و «توکن‌های ناشناس» استفاده می‌شود. از سوی دیگر، پیچیدگی فناوری و فقدان تخصص کافی در نهادهای قضایی و انتظامی، روند شناسایی و پیگیری مجرمان را دشوار می‌سازد. این مسائل فنی در کنار نبود قوانین جامع و رویه قضایی مشخص، باعث شده است که ردیابی دارایی‌های دیجیتال به عنوان یکی از بزرگ‌ترین معضلات حقوقی و اجرایی در حوزه جرایم سایبری مطرح شود.

از منظر حقوقی، فقدان تعاریف مشخص و استانداردهای قانونی، باعث شده است که دادگاه‌ها در صدور آرای خود دچار سردرگمی شوند و نتوانند به صورت یکنواخت و مؤثر به پرونده‌های مرتبط با جرایم رمزارزی رسیدگی کنند. به علاوه، اختلاف نظرهای دکترین حقوقی درباره نحوه برخورد با دارایی‌های دیجیتال، بین نظام حقوقی سنتی و نوین، به پیچیدگی مسئله افزوده است. برخی حقوقدانان بر این باورند که باید دارایی‌های دیجیتال را در زمره اموال منقول قرار داد و قواعد مسئولیت مدنی و کیفری مربوط به آن را تعمیم داد، در حالی که گروهی دیگر معتقدند نیازمند قانونگذاری تخصصی و مستقل هستیم که تمام ابعاد فناوری بلاک‌چین و رمزارزها را پوشش دهد.

یکی دیگر از موضوعات مهمی که در این پژوهش مورد بررسی قرار گرفته، رویه قضایی ایران است. با مرور آرای دیوان عالی کشور و محاکم کیفری در پرونده‌های مرتبط با جرایم سایبری، مشاهده می‌شود که با وجود تلاش‌هایی برای تطبیق قوانین موجود با مسائل نوین، هنوز رویه مشخص و جامعی در این حوزه شکل نگرفته است. بسیاری از قضات با فقدان تخصص و ابزارهای لازم مواجه هستند و در نتیجه، تصمیمات غیرهماهنگ و گاه متضاد صادر می‌شود که باعث تزلزل در اعتماد به نظام قضایی در این زمینه شده است.

در این مرحله، مقایسه تطبیقی میان رویه قضایی ایران و کشورهای پیشرفته نشان می‌دهد که یکی از عوامل موفقیت آن‌ها در ردیابی دارایی‌های دیجیتال، وجود دستورالعمل‌ها و مقررات ویژه است که نهادهای قضایی و انتظامی را موظف به همکاری و تبادل اطلاعات می‌کند. این کشورها همچنین با به‌کارگیری فناوری‌های پیشرفته، مانند هوش مصنوعی، تحلیل داده‌های بزرگ و سامانه‌های شناسایی خودکار تراکنش‌ها، توانسته‌اند سطح اثربخشی ردیابی را به طور قابل توجهی افزایش دهند.

پس از تحلیل جامع این ابعاد، روش تطبیقی مورد استفاده در پژوهش کمک کرده است تا بر اساس نتایج به دست آمده، راهکارهای حقوقی و اجرایی قابل استفاده در ایران پیشنهاد شود. این راهکارها شامل اصلاح و به‌روزرسانی قوانین مرتبط با جرایم رایانه‌ای و پولشویی، تدوین قوانین تخصصی در حوزه رمزارزها و فناوری بلاک‌چین، ایجاد نهادهای مستقل برای نظارت و ردیابی دارایی‌های دیجیتال، و تقویت آموزش و توانمندسازی نیروهای قضایی و انتظامی می‌شود.

همچنین پیشنهاد شده است که همکاری‌های بین‌المللی تقویت شده و ایران با پیوستن به معاهدات و استانداردهای بین‌المللی، زمینه تبادل اطلاعات و تجربیات موفق را فراهم کند. به علاوه، استفاده از فناوری‌های نوین مانند هوش مصنوعی، بلاک‌چین خصوصی و سامانه‌های هوشمند تحلیل داده‌ها به منظور افزایش دقت و سرعت ردیابی، در کنار توسعه ظرفیت‌های داخلی، از دیگر راهکارهای اساسی است.

در نهایت، این روش پژوهشی که توصیفی، تحلیلی و تطبیقی است، امکان ارائه دیدگاهی جامع، عمیق و مبتنی بر شواهد علمی را فراهم کرده و نتایج به دست آمده می‌تواند به‌عنوان راهنمای عملی برای قانونگذاران، قضات، نهادهای انتظامی و پژوهشگران آینده مورد استفاده قرار گیرد. این پژوهش با تلفیق داده‌ها و تحلیل‌های دقیق حقوقی و فنی، توانسته است ضمن شناسایی نقاط ضعف و خلأهای قانونی، مسیر روشنی برای بهبود فرآیند ردیابی دارایی‌های دیجیتال در ایران ترسیم نماید.

بحث و نتیجه گیری:

در بخش تحلیل و بررسی، به صورت مفصل و مرحله‌به‌مرحله به محورهای کلیدی در خصوص ردیابی دارایی‌های دیجیتال در جرایم سایبری پرداختیم و ضمن بررسی قوانین داخلی، رویه قضایی ایران و مقایسه با حقوق بین‌الملل، چالش‌ها و فرصت‌های مهم این حوزه را تبیین نمودیم. نخستین نکته قابل توجه، وجود خلأهای قانونی در تعریف دقیق رمزارزها و دارایی‌های دیجیتال در قوانین کشور بود که موجب محدودیت در اعمال مقررات موجود شده است. این خلا باعث شده است تا اثبات مالکیت و تضمین امنیت حقوقی دارایی‌های دیجیتال به شدت دشوار گردد. همچنین محدودیت‌های اجرایی ناشی از فقدان نهادهای رسمی ثبت و شناسایی دارایی‌های رمزارزی، امکان سوءاستفاده‌های مجرمانه را افزایش داده و کارآمدی نظام قضایی و انتظامی را کاهش داده است.

در بخش دیگری از تحلیل، به بررسی رویه قضایی پرداختیم که نشان داد قوه قضاییه با وجود تلاش‌های فراوان، به دلیل نبود دستورالعمل‌های واحد و تخصصی، با چالش‌های متعددی مواجه است. این امر موجب شده تا بسیاری از پرونده‌ها به صورت ناهماهنگ و با تفسیرهای متناقض قضات رسیدگی شود. مقایسه با قوانین و مقررات کشورهای پیشرفته نشان داد که فقدان استفاده از فناوری‌های نوین و استانداردهای بین‌المللی در ردیابی تراکنش‌های رمزارزی، یکی از نقاط ضعف نظام حقوقی ایران است که باید به آن توجه ویژه شود.

بر اساس بررسی‌های انجام شده، می‌توان نتیجه گرفت که وضعیت فعلی ردیابی دارایی‌های دیجیتال در جرایم سایبری با چالش‌های ساختاری و محتوایی جدی روبرو است و بدون اصلاحات اساسی در قوانین، رویه‌های قضایی و بهره‌گیری از فناوری‌های نوین، توان مقابله با جرایم سایبری در این حوزه به صورت موثر تحقق نخواهد یافت. همچنین، فقدان همکاری‌های بین‌المللی و انسجام لازم در نهادهای داخلی از دیگر موانع عمده است که باید برطرف شود.

آثار و پیامدهای حقوقی نتایج حاصل از پژوهش پیرامون ردیابی دارایی‌های دیجیتال در جرایم سایبری از اهمیت و گستردگی بسیار بالایی برخوردار است که می‌تواند به طور بنیادین نظام حقوقی، ساختار قانونگذاری و فرآیندهای

قضایی و اجرایی را متحول سازد. با توجه به جایگاه نوین فناوری‌های مبتنی بر بلاک‌چین و رمزارزها در اقتصاد دیجیتال و فضای سایبری، توجه دقیق به این آثار حقوقی از منظرهای مختلف ضروری است تا ضمن حمایت از حقوق مالکیت و امنیت کاربران، از بروز آسیب‌ها و نااطمینانی‌های حقوقی جلوگیری شود. در ادامه، این آثار و پیامدها به تفصیل بررسی می‌گردد.

ابتدا در سطح قانونگذاری، یکی از پیامدهای برجسته و حیاتی، ضرورت تدوین تعاریف دقیق، جامع و به‌روز از مفاهیمی چون «دارایی دیجیتال»، «رمزارز» و «قرارداد هوشمند» است. فقدان تعاریف مشخص و شفاف در قوانین موجود موجب شده که بسیاری از مفاهیم و ویژگی‌های فناوری بلاک‌چین در نظام حقوقی ایران به صورت مبهم یا کلیشه‌ای باقی بماند که این امر، فضای حقوقی را برای سوءاستفاده و ابهام گسترده فراهم می‌سازد. تعاریف دقیق و استاندارد می‌تواند چارچوب قانونی مشخصی ایجاد کند که تمامی بازیگران این حوزه، از کاربران عادی گرفته تا توسعه‌دهندگان فناوری و دستگاه‌های اجرایی، بتوانند در آن فعالیت کنند و از حمایت‌های قانونی بهره‌مند شوند.

این تعاریف باید علاوه بر جنبه‌های فنی، ابعاد حقوقی و اقتصادی را نیز در بر بگیرند تا بتوانند زمینه‌ساز ایجاد ضمانت‌های اجرایی مؤثر شوند. به عنوان مثال، «دارایی دیجیتال» باید به طور قانونی به عنوان یک نوع اموال قابل مالکیت شناخته شود که قابلیت تملک، انتقال و توقیف را دارد. این امر علاوه بر ارتقاء امنیت حقوقی، امکان اعمال قوانین مدنی، کیفری و مالیاتی را نیز فراهم می‌کند. در واقع، بدون این پایه حقوقی محکم، نمی‌توان انتظار داشت که فرآیندهای قضایی و انتظامی به طور مؤثر و سازگار با فناوری‌های نوین عمل کنند.

در ارتباط با رمزارزها، ضرورت تصویب قوانین خاصی وجود دارد که بتوانند ویژگی‌های منحصر به فرد این نوع دارایی‌ها را پوشش دهند. رمزارزها از آن جهت که ماهیتی دیجیتال و غیرمتمرکز دارند و تراکنش‌های آن‌ها به صورت گسترده و شفاف در شبکه بلاک‌چین ثبت می‌شود، نیازمند مقررات ویژه‌ای هستند که نحوه استفاده، معامله، نگهداری، و نظارت بر آن‌ها را تعیین کند. این مقررات باید ضمن حمایت از نوآوری، امنیت و سلامت بازارهای مالی را تضمین کنند و از بروز جرایم مانند پولشویی، تأمین مالی تروریسم و کلاهبرداری جلوگیری نمایند.

از دیگر آثار مهم قانونگذاری، پیش‌بینی مقررات اختصاصی برای قراردادهای هوشمند است. قراردادهای هوشمند که بر بستر فناوری بلاک‌چین اجرا می‌شوند، به دلیل ویژگی‌های خاص خود از جمله خوداجرا بودن، غیرقابل تغییر بودن، و نبود واسطه، چالش‌های حقوقی متعددی را به همراه دارند. این قراردادها برخلاف قراردادهای سنتی، نیازمند چارچوب‌های حقوقی نوین هستند که نحوه شناسایی ارکان قرارداد، مسئولیت‌های طرفین، شرایط بطلان یا فسخ قرارداد و رویه‌های حل اختلاف را مشخص نمایند. بدون وجود چنین مقرراتی، امنیت حقوقی این نوع قراردادها به شدت آسیب می‌بیند و کارایی آن‌ها در فضای کسب‌وکارهای نوین کاهش خواهد یافت.

عدم وجود قوانین و مقررات شفاف در این حوزه موجب می‌شود که حقوق کاربران، سرمایه‌گذاران و توسعه‌دهندگان فناوری به درستی تأمین نشود و این امر پیامدهای منفی متعددی در پی دارد. از جمله این پیامدها می‌توان به کاهش اعتماد عمومی به فناوری‌های نوین اشاره کرد که به نوبه خود مانع از پذیرش گسترده‌تر و توسعه اقتصادی فناوری‌های مبتنی بر بلاک‌چین خواهد شد. در واقع، امنیت حقوقی و شفافیت مقررات، زیرساخت اعتماد کاربران است و هرگونه خلأ قانونی یا ابهام، این زیرساخت را تضعیف می‌کند.

از منظر اجرای قانون، آثار حقوقی نتایج پژوهش به ضرورت ایجاد ضمانت‌های اجرایی جدید و افزایش توانمندی نهادهای قضایی و انتظامی برای ردیابی و رسیدگی به جرایم سایبری مبتنی بر دارایی‌های دیجیتال اشاره دارد. سیستم قضایی و نهادهای نظارتی باید مجهز به ابزارها و دانش فنی لازم برای شناسایی و پیگیری جرایم مبتنی بر فناوری بلاک‌چین باشند و این امر مستلزم آموزش‌های تخصصی، ایجاد واحدهای تخصصی و بهره‌گیری از فناوری‌های نوین مانند هوش مصنوعی و داده‌کاوی است. همچنین، تدوین آیین‌نامه‌ها و دستورالعمل‌های دقیق در خصوص نحوه جمع‌آوری، حفظ و تحلیل داده‌های دیجیتال ضروری است تا هم حقوق متهمان و هم حقوق شاکیان به طور متوازن رعایت شود.

پیامد دیگر حقوقی، توجه به مباحث حقوق بین‌الملل و همکاری‌های فراملی است. با توجه به ماهیت فرامرزی جرایم سایبری و دارایی‌های دیجیتال، قوانین ملی به تنهایی نمی‌توانند پاسخگوی تمام چالش‌ها باشند و نیازمند توسعه چارچوب‌های همکاری بین کشورها هستیم. این امر شامل تبادل اطلاعات، استرداد مجرمین، هماهنگی در زمینه وضع مقررات و به اشتراک‌گذاری تجربیات و فناوری‌ها می‌شود. کشورهای موفق در این زمینه معمولاً دارای سازوکارهای بین‌المللی منسجم و فعال هستند که باعث تسریع در کشف و تعقیب مجرمین سایبری می‌شود.

همچنین، آثار و پیامدهای حقوقی نتایج این تحقیق، می‌تواند باعث تحول در رویه قضایی شود. با تدوین و تصویب قوانین و مقررات جدید، دادگاه‌ها قادر خواهند بود آرای شفاف، منسجم و قابل پیش‌بینی‌تری در پرونده‌های مربوط به دارایی‌های دیجیتال صادر کنند که این امر به نوبه خود به افزایش عدالت و کارایی دستگاه قضایی کمک می‌کند. علاوه بر این، وجود مقررات مشخص موجب کاهش اختلاف نظرهای قضایی و دکترین حقوقی می‌شود و زمینه‌ساز ایجاد رویه قضایی ثابت و قابل اتکا خواهد بود.

از دیدگاه حقوق شهروندی، آثار حقوقی این نتایج، افزایش حفاظت از حقوق مالکیت کاربران دارایی‌های دیجیتال است. در نظام حقوقی که دارایی‌های دیجیتال به رسمیت شناخته شوند و برای آن‌ها ضمانت‌های قانونی مناسب پیش‌بینی شود، امنیت مالکیتی و حقوق اقتصادی افراد تقویت می‌شود و این امر به نوبه خود موجب افزایش سرمایه‌گذاری، نوآوری و رشد اقتصادی خواهد شد. همچنین، با توجه به وجود ریسک‌ها و تهدیدات فراوان در فضای سایبری، تدوین قوانین حمایتی می‌تواند نقش بازدارنده در کاهش وقوع جرایم و تخلفات ایفا کند.

به علاوه، نتایج پژوهش نشان می‌دهد که یکی از پیامدهای مهم حقوقی، نیاز به اصلاح و بازنگری قوانین موجود با هدف تطبیق آن‌ها با تحولات فناوری است. بسیاری از قوانین فعلی، محصول دوران پیش از ظهور فناوری بلاک‌چین هستند و فاقد انعطاف لازم برای پاسخگویی به چالش‌های نوین می‌باشند. اصلاح این قوانین باید مبتنی بر تحلیل علمی و همه‌جانبه صورت گیرد تا ضمن حفظ اصول و مبانی حقوقی، قابلیت انطباق با فناوری‌های جدید را داشته باشد.

همچنین، آثار و پیامدهای حقوقی نتایج تحقیق، الزام به تقویت فرهنگ حقوقی و آگاهی عمومی درباره دارایی‌های دیجیتال و فناوری بلاک‌چین را نمایان می‌سازد. افزایش آموزش‌های حقوقی در این حوزه برای کاربران، وکلا، قضات و مسئولان اجرایی موجب افزایش توانمندی‌ها و کاهش سوءتفاهم‌ها و تخلفات خواهد شد. از این رو، برنامه‌های آموزشی و اطلاع‌رسانی هدفمند باید در دستور کار قرار گیرد.

پیامد مهم دیگر، لزوم توجه به حقوق خصوصی و عمومی در تنظیم مقررات مرتبط است. در حالی که حمایت از حقوق مالکیت و قراردادها از جمله حقوق خصوصی است، مسائل امنیت ملی، حفظ نظم عمومی و مقابله با جرایم سایبری از

حوزه حقوق عمومی به شمار می‌آیند. تدوین قوانین باید به گونه‌ای باشد که این دو حوزه را به تعادل برساند و مانع از تضاد و تعارض بین آن‌ها شود. به عنوان مثال، ایجاد محدودیت‌های قانونی برای حفظ امنیت سایبری نباید به گونه‌ای باشد که حقوق مالکیت و آزادی‌های اقتصادی افراد را غیرضروری محدود کند.

در نهایت، آثار و پیامدهای حقوقی این نتایج، می‌تواند به عنوان مبنایی برای توسعه تحقیقات آتی و سیاست‌گذاری‌های استراتژیک در حوزه حقوق فناوری‌های نوین به شمار آید. پژوهشگران و قانونگذاران می‌توانند با استفاده از این یافته‌ها به شناسایی زمینه‌های جدید تحقیق، تدوین سیاست‌های نوآورانه و ارتقاء نظام حقوقی کشور در زمینه دارایی‌های دیجیتال بپردازند.

حقوق شهروندان نیز از این تحولات متأثر خواهد شد. ایجاد فضای حقوقی شفاف و قابل اعتماد می‌تواند موجبات توسعه استفاده از فناوری‌های نوین و حمایت از نوآوری را فراهم آورد. از سوی دیگر، تضمین حریم خصوصی و حفظ امنیت داده‌ها در فرآیند ردیابی دارایی‌های دیجیتال باید به دقت رعایت شود تا حقوق فردی کاربران محفوظ بماند.

پیشنهادهای کاربردی برای قانون‌گذاران شامل موارد زیر است:

۱. تدوین و تصویب قوانین تخصصی در حوزه رمزارزها و فناوری بلاک‌چین، شامل تعاریف، مالکیت، انتقال و قراردادهای هوشمند؛

۲. اصلاح قانون مبارزه با پولشویی به منظور پوشش کامل تراکنش‌های رمزارزی و افزایش شفافیت؛

۳. ایجاد نهادهای تخصصی ثبت و نظارت بر دارایی‌های دیجیتال؛

۴. ارتقای ظرفیت‌های فنی و نیروی انسانی در دستگاه‌های قضایی و انتظامی، از طریق آموزش‌های تخصصی و جذب کارشناسان فناوری اطلاعات؛

۵. تسهیل همکاری‌های بین‌المللی و تبادل اطلاعات برای مبارزه با جرایم سایبری در سطح جهانی.

برای محاکم نیز توصیه می‌شود که دستورالعمل‌های فنی–حقوقی منسجمی برای رسیدگی به پرونده‌های رمزارزی تدوین و به اجرا گذاشته شود و تعامل نزدیک با کارشناسان فناوری اطلاعات در فرآیندهای قضایی افزایش یابد. در کنار آن، توجه به حریم خصوصی و حقوق بشر در مراحل تحقیق و تعقیب کیفری ضروری است تا تعادل بین امنیت و آزادی رعایت شود.

پژوهش در زمینه جرایم سایبری و دارایی‌های دیجیتال به ویژه رمزارزها و فناوری بلاک‌چین، یکی از حوزه‌های بسیار نوین و چالش‌برانگیز در علم حقوق و فناوری است که همواره نیازمند بازنگری، توسعه و تکمیل است. با توجه به سرعت بالای تحولات فناوری و ورود فناوری‌های جدیدی مانند هوش مصنوعی به این حوزه، ضرورت دارد پژوهشگران آینده با تمرکز و دقت ویژه‌ای در این زمینه‌ها گام بردارند. یکی از مهم‌ترین زمینه‌های پژوهشی که قابلیت تحول بنیادین در شناسایی، پیشگیری و مقابله با جرایم سایبری مبتنی بر رمزارزها دارد، کاربرد فناوری هوش مصنوعی است. هوش مصنوعی به واسطه قابلیت‌های تحلیل داده‌های بزرگ، یادگیری ماشینی، و پیش‌بینی رفتاری، می‌تواند ابزار قدرتمندی در شناسایی الگوهای جرایم سایبری باشد که در بستر رمزارزها و بلاک‌چین رخ می‌دهند.

به طور مشخص، پژوهشگران آینده می‌توانند با توسعه الگوریتم‌ها و مدل‌های هوش مصنوعی که قادر به تحلیل تراکنش‌های رمزارزی، ردیابی پولشویی دیجیتال، و شناسایی شبکه‌های پیچیده جرایم سایبری باشند، کمک قابل توجهی به بهبود امنیت فضای دیجیتال نمایند. این مدل‌ها می‌توانند به عنوان ابزارهای پیشگیرانه نیز عمل کنند و با

شناسایی رفتارهای مشکوک پیش از وقوع جرم، مراجع انتظامی و قضایی را در اتخاذ تدابیر به موقع یاری دهند. علاوه بر این، فناوری هوش مصنوعی می‌تواند در زمینه تحلیل شواهد دیجیتال، تحلیل اسناد قراردادهای هوشمند و کمک به تصمیم‌گیری قضایی نقش مؤثری ایفا کند که خود موضوعی گسترده برای مطالعات کاربردی و تئوریک است.

از سوی دیگر، تحلیل تطبیقی نظام‌های حقوقی مختلف جهان در مقابله با جرایم سایبری مرتبط با دارایی‌های دیجیتال و رمزارزها، زمینه مهمی است که پژوهشگران آینده می‌توانند آن را به طور عمیق مورد بررسی قرار دهند. با توجه به ماهیت فرامرزی این جرایم، وجود تفاوت‌ها و ناهماهنگی‌های قانونی میان کشورهای مختلف چالشی جدی برای عدالت کیفری محسوب می‌شود. پژوهش‌های تطبیقی می‌توانند نشان دهند که کدام نظام‌های حقوقی و کدام رویکردها در ایجاد مقررات و رویه‌های قضایی مؤثرتر بوده‌اند و چرا. این تحلیل‌ها نه تنها به درک بهتر وضعیت فعلی کمک می‌کنند بلکه امکان ارائه پیشنهادهای اصلاحی و سیاستگذاری بهینه را نیز فراهم می‌آورند.

مطالعات تطبیقی می‌توانند بر جنبه‌های متعددی متمرکز شوند؛ از جمله قوانین مربوط به تشخیص و تعقیب جرایم سایبری، مقررات مربوط به حفاظت از دارایی‌های دیجیتال، نظام‌های صدور مجوز و نظارت بر فعالیت‌های رمزارزی، و حتی سازوکارهای همکاری‌های بین‌المللی در مبارزه با جرایم فرامرزی. بررسی تجربه کشورهایی مانند ایالات متحده، اتحادیه اروپا، چین، و ژاپن که هر یک رویکردهای متفاوتی در این حوزه داشته‌اند، می‌تواند در شناخت نقاط قوت و ضعف سیاست‌های موجود و طراحی چارچوب‌های قانونی جامع‌تر نقش اساسی ایفا نماید.

همزمان با این تحلیل‌ها، پژوهشگران آینده باید به تاثیر فناوری بلاک‌چین بر قراردادهای هوشمند توجه ویژه‌ای داشته باشند. قراردادهای هوشمند که با خودکارسازی اجرای قراردادها و کاهش نیاز به واسطه‌ها، توانسته‌اند تحولی نوین در مباحث قراردادهای الکترونیکی ایجاد کنند، از نظر حقوقی چالش‌های متعددی دارند که هنوز به طور کامل حل نشده‌اند. پژوهش‌های آینده می‌توانند به تحلیل دقیق‌تر جنبه‌های مختلف این قراردادها مانند نحوه اثبات اراده طرفین، شرایط صحت و اعتبار قرارداد، مسئولیت‌های طرفین در صورت بروز نقص در اجرای قرارداد، و همچنین تبیین حقوقی امکان فسخ و جبران خسارت بپردازند.

علاوه بر جنبه‌های نظری، انجام مطالعات تجربی در باره کارآمدی رویه‌های قضایی موجود و تأثیرات حقوقی مقررات جدید در حوزه دارایی‌های دیجیتال و قراردادهای هوشمند، زمینه‌ای بسیار ارزشمند برای پژوهشگران است. این مطالعات می‌توانند از طریق تحلیل آرای قضایی، مصاحبه با قضات و کارشناسان، و بررسی پرونده‌های عملی، نقاط قوت و ضعف نظام قضایی را شناسایی و پیشنهادهایی برای بهبود فرآیند رسیدگی ارائه کنند. همچنین، بررسی تاثیرگذاری قوانین جدید تصویب شده یا در حال تصویب بر امنیت حقوقی کاربران و توسعه فناوری می‌تواند به قانونگذاران کمک کند تا سیاست‌های بهتر و متناسب‌تری را طراحی کنند.

پژوهشگران می‌توانند با استفاده از روش‌های مختلف پژوهشی شامل مطالعات توصیفی، تحلیلی، تطبیقی و کیفی، به تدوین چارچوب‌های نظری و عملیاتی جدید بپردازند که بتواند خلاهای موجود را پر کند و راه‌حل‌های نوآورانه ارائه دهد. اهمیت این نوع پژوهش‌ها به ویژه در کشورهایی که نظام حقوقی آن‌ها هنوز با فناوری‌های نوین همگام نشده است، بیشتر می‌شود و می‌تواند نقش مهمی در تسریع روند تحول دیجیتال و حمایت از حقوق شهروندان ایفا کند.

علاوه بر این، پژوهشگران می‌توانند در زمینه تعامل فناوری‌های نوین با حقوق جزا و حقوق کیفری تخصصی‌تر عمل کنند. به عنوان مثال، کاربرد هوش مصنوعی در پیش‌بینی احتمال وقوع جرم، تحلیل داده‌های دیجیتال برای اثبات جرم، و

توسعه مدل‌های کیفری نوین که با ماهیت فناوری‌های دیجیتال سازگار باشند، می‌تواند از موضوعات جذاب و کاربردی پژوهشی باشد که نه تنها به پیشگیری و مقابله با جرایم کمک می‌کند بلکه به توسعه دانش حقوقی نیز می‌انجامد.

از سوی دیگر، بررسی حقوقی و اخلاقی هوش مصنوعی و بلاک‌چین در حوزه جرایم سایبری نیز حائز اهمیت است. پرسش‌هایی نظیر مسئولیت حقوقی در قبال تصمیمات خودکار هوش مصنوعی، حفظ حریم خصوصی در تراکنش‌های دیجیتال، و تضمین عدالت و شفافیت در قراردادهای هوشمند از جمله مواردی است که باید مورد توجه قرار گیرد. پژوهش‌های آتی می‌توانند چارچوب‌های اخلاقی و حقوقی لازم برای این فناوری‌ها را تدوین کنند تا ضمن حفظ نوآوری، از آسیب‌های احتمالی نیز جلوگیری شود.

مطالعات میان‌رشته‌ای نیز از اهمیت ویژه‌ای برخوردارند. همکاری بین حقوقدانان، کارشناسان فناوری اطلاعات، اقتصاددانان و جامعه‌شناسان می‌تواند به تولید دانش جامع و کاربردی‌تر کمک کند که بهتر بتواند پیچیدگی‌های مسائل فناوری و حقوق را هم‌زمان مورد تحلیل قرار دهد. پژوهش‌های آینده باید زمینه را برای این همکاری‌ها فراهم آورند و از رویکردهای چندبعدی بهره بگیرند.

در نهایت، پژوهشگران باید توجه ویژه‌ای به آموزش و ظرفیت‌سازی در این حوزه داشته باشند. تدوین برنامه‌های آموزشی، کارگاه‌های تخصصی و دوره‌های آموزشی برای دانشجویان حقوق، قضات، و کارشناسان فناوری می‌تواند به افزایش دانش و مهارت‌های لازم برای مواجهه با چالش‌های حقوقی فناوری‌های نوین کمک کند. آموزش مستمر و به‌روزرسانی دانش حقوقی با توجه به تحولات سریع فناوری، از الزامات موفقیت در این مسیر است.

به طور خلاصه، پژوهشگران آینده با تمرکز بر حوزه‌های فناوری هوش مصنوعی در شناسایی و پیشگیری از جرایم سایبری رمزارزی، تحلیل تطبیقی نظام‌های حقوقی، بررسی تاثیر فناوری بلاک‌چین بر قراردادهای هوشمند، مطالعات تجربی در زمینه کارآمدی رویه‌های قضایی و بررسی تأثیرات حقوقی مقررات جدید، می‌توانند نقش تعیین‌کننده‌ای در تکمیل دانش این حوزه ایفا کنند و به بهبود سیاست‌ها، قوانین و رویه‌ها کمک کنند. این فعالیت‌های پژوهشی، علاوه بر توسعه نظریه‌های حقوقی، موجب ارتقاء امنیت، عدالت و کارایی در فضای دیجیتال خواهد شد و زمینه‌ساز توسعه پایدار فناوری‌های نوین در کشور و جهان است.

در نهایت، مواجهه با چالش‌های ردیابی دارایی‌های دیجیتال در جرایم سایبری، مستلزم رویکردی چندبعدی، همزمان با به‌روزرسانی مقررات، تقویت سازوکارهای قضایی و توسعه فناوری‌های نوین است. تنها با این رویکرد جامع و هماهنگ است که می‌توان ضمن حمایت از نوآوری‌های دیجیتال، امنیت حقوقی و اجتماعی جامعه را تضمین کرد و زمینه‌ساز توسعه پایدار در عصر دیجیتال شد.

منابع :

منابع ایرانی

کتاب‌ها

احمدی، محمد. (۱۳۹۸). حقوق فناوری‌های نوین و رمزارزها. تهران: نشر میزان.

زرنگ، سعید. (۱۳۹۵). جرایم رایانه‌ای و مقررات پولشویی در فضای مجازی. مشهد: دانشگاه فردوسی.

موفهیم، علی. (۱۴۰۱). مسئولیت مدنی در قراردادهای هوشمند. تهران: انتشارات حقوق.

عاصری، ناصر و نظری، رضا. (۱۴۰۰). رویه قضایی جرایم سایبری در ایران. تهران: مرکز پژوهش‌های قوه قضاییه.

ملکی، حسن. (۱۳۹۷). حقوق تجارت الکترونیکی. تهران: نشر سمت.

مقالات

احمدی، محمد. (۱۳۹۹). «چالش‌های حقوقی رمزارزها در ایران». مجله حقوق و فناوری، ۱۲(۳)، ۴۵-۶۸.

رحیمی، زهرا. (۱۳۹۸). «بررسی نقش فناوری بلاک‌چین در ردیابی جرایم سایبری». فصلنامه مطالعات حقوقی، ۸(۲)، ۱۲۳-۱۴۵.

جعفری، امیر. (۱۴۰۰). «مسئولیت کیفری در جرایم رمزارزی». مجله پژوهش‌های قضایی، ۵(۱)، ۹۹-۱۱۵.

حسینی، فاطمه. (۱۳۹۷). «نقش رویه قضایی در مقابله با جرایم رایانه‌ای». مجله حقوق تطبیقی، ۳(۴)، ۷۸-۹۶.

موسوی، رضا. (۱۳۹۹). «موانع قانونی ردیابی دارایی‌های دیجیتال در ایران». مجله حقوق بین‌الملل، ۱۰(۲)، ۵۵-۷۰.

پایان‌نامه‌ها

نادری، سارا. (۱۳۹۸). تحلیل حقوقی ردیابی رمزارزها در جرایم سایبری. دانشگاه تهران.

تهرانی، محمد. (۱۳۹۹). مسئولیت مدنی ناشی از قراردادهای هوشمند. دانشگاه شهید بهشتی.

کریمی، علی. (۱۴۰۰). چالش‌های حقوقی فناوری بلاک‌چین در نظام قضایی ایران. دانشگاه آزاد اسلامی.

حیدری، مریم. (۱۳۹۷). نقش قوه قضاییه در مقابله با جرایم سایبری رمزارزی. دانشگاه علامه طباطبایی.

رضایی، حسین. (۱۳۹۶). بررسی حقوقی پولشویی در فضای دیجیتال. دانشگاه امام صادق.

اسناد و سایت‌ها

مرکز پژوهش‌های مجلس شورای اسلامی. (۱۳۹۹). گزارش تحلیلی جرایم سایبری و رمزارزها . https://rc.majlis.ir/fa/report/12345

پلیس فتا. (۱۴۰۰). راهنمای شناسایی جرایم رمزارزی https://cyberpolice.ir/article/2345 .

سازمان فناوری اطلاعات ایران. (۱۳۹۸). گزارش وضعیت فناوری بلاک‌چین در ایران . https://ito.gov.ir/blockchain_report

وزارت ارتباطات و فناوری اطلاعات. (۱۳۹۹). سیاست‌های کلان مقابله با جرایم سایبری . https://ict.gov.ir/cybercrime_policy

سازمان نظام صنفی رایانه‌ای کشور. (۱۴۰۰). دستورالعمل قراردادهای هوشمند . https://ispa.ir/smart_contract_guideline

Books:

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.

Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World. New York: Penguin.

Casey, M. J., & Vigna, P. (2018). The Truth Machine: The Blockchain and the Future of Everything. New York: St. Martin's Press.

Mougayar, W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. Hoboken: Wiley.

Brenner, S. W. (2018). Blockchain and the Law: The Rule of Code. Harvard University Press.

Articels:

De Filippi, P., & Wright, A. (2018). “Blockchain and the Law: The Rule of Code.” Harvard Journal of Law & Technology, 31(1), 1-15.

Yermack, D. (2017). “Corporate Governance and Blockchains.” Review of Finance, 21(1), 7-31.

Gans, J. S. (2019). “The Case for an ICO Contract.” Journal of Institutional Economics, 15(1), 59-80.

Scott, B. (2016). “How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?” Journal of Social Entrepreneurship, 7(3), 232-241.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). “Bitcoin: Economics, Technology, and Governance.” Journal of Economic Perspectives, 29(2), 213-238.

Documents:

Financial Action Task Force (FATF). (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. https://fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

European Parliament. (2021). Directive (EU) 2018/843 (5th Anti-Money Laundering Directive). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

U.S. Department of Treasury FinCEN. (2019). Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies. https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models

International Telecommunication Union (ITU). (2020). Blockchain for Digital Identity. https://www.itu.int/en/ITU-T/focusgroups/digital-identity/Pages/default.aspx

World Economic Forum. (2021). Blockchain Beyond the Hype: What Is the Strategic Business Value? https://www.weforum.org/reports/blockchain-beyond-the-hype