

<http://doi.org/10.22133/mtlj.2024.429710.1276>

The Approach of the Criminal Justice System to the Criminal Risk of Virtual Assets

Aref Khalili Paji^{1*}, Somaye Parhizkary²

¹ Ph.D. in criminal law and criminology, Faculty of Law Shahid Beheshti University, Tehran, Iran.

² Ph.D. Student in criminal law and criminology, Faculty of Law Shahid Beheshti University, Tehran, Iran.

Article Info	Abstract
Original Article	As a technological tool with criminal capabilities, virtual assets have also attracted the attention of criminals. The unique features of this technology have become the beginning of conceptual changes and examples of some crimes. Hence, curbing the criminal risks of this technology and taking preventive and confrontational measures against it seems inevitable. In the meantime, the risks of money laundering of virtual assets have made it the focus of criminal policy measures. Features such as speed, anonymity, not being tracked have caused criminals to use these assets widely. Therefore, within the framework of their criminal justice system, countries are trying to control the criminal risks of money laundering of virtual assets in two preventive and confrontational dimensions. Based on this, in order to adopt optimal strategies at the level of the criminal justice system, first of all, it is very important to know what virtual assets are from a technical and legal point of view, and then to examine its criminal capacities. Because the prerequisite for adopting any action or reaction strategy is to know the exact phenomenon of the subject of these actions. This will provide the necessary background for presenting the ideal model of criminal policy at two both preventive and penal levels. Therefore, in the present study, the approach of the criminal justice system to the criminal risk of virtual assets will be investigated with a descriptive-analytical approach and by examining library sources such as transnational documents, domestic laws, and regulations. In this framework, by examining the existing situation in Iran's legal-criminal system, the needs of the criminal policy in this field will be outlined.
Received: 09-12-2023	
Accepted: 14-02-2024	
Keywords: Criminal Justice System Delinquency Virtual Assets Risk	
*Corresponding author e-mail: Arefkhalilipaji@gmail.com	
How to Cite: Khalili Paji, A., & Parhizkary, S. (2025). The Approach of the Criminal Justice System to the Criminal Risk of Virtual assets. <i>Modern Technologies Law</i> , 6(11), 75-95.	
Published by University of Science and Culture https://www.usc.ac.ir Online ISSN: 2783-3836	

1. Introduction

The process of transition to a global society is rapidly evolving with the development of international trade exchanges, international economic cooperation, and extensive communication at the world level; which ultimate example has crystallized in the global economy. Breaking social boundaries and becoming a single global society and introducing technological tools made economic exchanges easier. These technological tools with the function of money or as a new method of payment are known as virtual assets and quickly spread in different countries. This new technology, although provided a platform for ease of exchanges; But at the same time, due to its special features, such as the anonymity of individuals, the impossibility of tracking the chain of transactions, and sometimes the lack of governmental support, attracted the attention of criminals.

Wide networks of communication and information technology have created many fields for abuse by international criminals in the form of crimes such as money laundering, which are less materially controllable. Money laundering aims to clear illegal money by hiding the source of income. Perpetrators of money laundering consider the use of virtual assets as a safe platform to hide the traces of criminal proceeds and the anonymity of the chain of people involved in transactions, and pursue their criminal goals from this path. Virtual assets can be accessed through the Internet and with tools, including mobile phones, even in cross-border payments. Additionally, these technologies typically rely on complex infrastructures, involving multiple entities in different countries, used to transfer funds or perform payment operations. This way of providing services and involving several countries, as different jurisdictions, will create problems in determining the responsible for combating money laundering and terrorist financing, the supervisor and the enforcer of these regulations.

In this regard, the Financial Action Task Force (FATF), which aims to prevent and combat money laundering and terrorist financing, as a transnational organization, provided recommendations to countries to prevent and combat these crimes. This group, in reviewing its recent recommendations, has paid particular attention to virtual assets and by following a risk-based approach to identifying this category and including anti-money laundering requirements, has focused on virtual asset service providers.

Thus, considering the formation of national and transnational approaches regarding the criminal risk of virtual assets, how the criminal justice system intervenes in this field and how it faces the criminal risks of virtual assets is of great importance. In this regard, by looking at the existing and relevant regulations and approvals in Iran's legal system, in the first part of this research, virtual assets are examined in terms of their technical and legal nature and then their criminal capacities are introduced. It is through this that in the second part, the necessity of including the requirements of the anti-money laundering system on virtual assets will be discussed with a view to transnational approaches and finally, the needs of the criminal policy in this field, which includes two preventive and punitive strategies, will be examined.

2. Methodology

this study is applied in terms of purpose and descriptive-analytic in terms of methodology and nature. the necessary data and statistics were collected by library method

3. Results and Discussion

The nature of some virtual assets is such that it enables person-to-person transactions without the need for an intermediary. This feature has attracted the attention of countries that have always been economically unstable and the risk of bankruptcy of institutions and financial institutions in them is considered high. This has increased people's desire to use virtual assets, especially cryptocurrencies. In fact, for people who do not consider such institutions to be reliable enough, virtual assets are considered a suitable alternative.

It is necessary to comprehensively examine the dimensions and types of virtual assets as a new and expanding phenomenon. Among the various dimensions, identifying the legal nature of virtual assets is a fundamental element

in the formulation and regulation of appropriate laws and regulations. In fact, although the function of virtual assets can be considered similar to money in terms of legal and economic foundations, they can be accepted in exchanges; But this issue requires the recognition and acknowledgment of governments.

Based on this, the invention and development of virtual assets appeared as a new manifestation of the globalization of the economy. In addition to all its advantages, it has provided the uncontrollable access of humans to geographical areas, financial resources and information, which itself has become a platform for illegal activities.

In the meantime, the combination of virtual assets with some other technologies in the context of cyber space has led to the development of criminal capacities, the most obvious result of which is flexibility in identity. This means that there is no specific information about the users of this technology (sender, receiver and extractor) or this information does not necessarily match their real identity information. In fact, they can not only use fake identities, but they can also change their identities frequently.

In fact, due to the lack of a supervisory body, it is difficult to trace the origin of the income. The absence of a central controlling body as well as the lack of identification of users is significant from another point of view. This dimension is the possibility of transnational alliances to commit crimes. Investigations show that the defendants of some cases related to virtual assets resided in different countries such as the United States and Thailand and participated remotely in criminal activities using virtual currencies. The presence of these features has attracted the attention of money launderers in order to clean up the criminal proceeds. In fact, the perpetrators of money laundering consider the use of virtual assets as a safe platform to achieve their goals, that is, to hide the origin of the proceeds and the anonymity of the transaction chain. Therefore, the need to provide a safe solution to prevent and deal with this phenomenon is inevitable.

4. Conclusions and Future Research

Virtual assets can be examined from several aspects in the criminal justice system. This issue will have a considerable scope when it is to be examined in the framework of the concept of criminal policy. In this regard, it should be seen what combination of criminal policy should be taken into account in the two areas of preventive and reactive measures with regard to the criminal capacities of virtual assets. A prerequisite is the accurate identification of the criminal profile and criminal capacities of this technology so in the light of that set of effective criminal policy interventions from the passage of a combination of interventions; Criminal, non-criminal and preventive measures, be considered. First; In the field of reactive measures, first, by drawing the criminal profile and determining the criminal capacities of virtual assets, it is necessary to check on what basis the measures in this area should be based. Does this area require criminal interventions, or is it sufficient for legal regulation and non-criminal responses? Or should a combination of criminal and non-criminal measures be considered?

Undoubtedly, in terms of criminal, this space includes possible and real capacities in creating quantitative and qualitative changes, and the examples and concepts of crimes. Therefore, answers to important questions such as what changes virtual assets make in the quantity and quality of crimes? How much crime will increase with the use of this technology? What new types of crime will be created, which are essentially different from the current crimes related to the Internet, artificial intelligence, etc.? Are the crimes that can be committed in the real world also punishable by using virtual assets, or does criminal intervention in this space require the criminalization of new types of behaviors specific to this space? It is an important part of justifying criminal intervention in this field and its types. Also, criminal response in this area and identification of the guarantee of criminal executions are also important. Questions such as the effectiveness of existing punishments or the need to adopt new approaches to criminal response based on the fundamental components of virtual assets are among the most important questions that are used in the application of criminal policy packages based on a combination of measures. However, the need for criminal intervention does not negate the need to adopt non-criminal responses within the framework of the regulatory system of this technology. A significant part of regulating relations regarding this

technology can be based on union, administrative and civil actions. This is confirmed by the principle of minimum criminal law.

Second; In the field of preventive measures, the criminal capacities of virtual assets and their criminal functions can be effective. In this framework, a combination of criminal policy measures can be planned. On the one hand, preventive measures based on criminological teachings of prevention at the level of situational and social prevention can be effective in curbing possible crimes with this technology, and on the other hand, the legal and criminal measures that prevent the passage of criminalizations in accordance with criminal justice can be prevented by the realization of deterrence through the development of criminalization of crimes and the guarantee of legal-criminal enforcement for preventive measures to curb important crimes in this area. Thus, if the approach of criminal policy against the risks of money laundering of virtual assets takes into account the mentioned cases, we can be optimistic about the beneficial results of its implementation.





<http://doi.org/10.22133/mtlj.2024.429710.1276>

رویکرد نظام عدالت کیفری به ریسک مجرمانه‌داری‌های مجازی

عارف خلیلی پاجی^{۱*}، سمیه پرهیزکاری^۲

^۱ دکتری حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.

^۲ دانشجوی دکتری حقوق کیفری و جرم‌شناسی، دانشکده حقوق، دانشگاه شهید بهشتی، تهران، ایران.

چکیده

اطلاعات مقاله

مقاله پژوهشی

تاریخ دریافت:

۱۴۰۲/۰۹/۱۸

تاریخ پذیرش:

۱۴۰۲/۱۱/۲۵

واژگان کلیدی:

نظام عدالت کیفری

بزهکاری

داری‌های مجازی

ریسک

داری‌های مجازی به‌عنوان ابزاری فناورانه با برخورداری از ظرفیت‌های جنایی، نظر بزهکاران را نیز به خود جلب کرده است. ویژگی‌های منحصر به فرد این فناوری، سرآغاز تحولات مفهومی و مصداقی برخی جرایم شده است؛ ازاین‌رو مهار مخاطرات جنایی این فناوری و اتخاذ تدابیر و اقدامات کنشی و واکنشی در برابر آن، اجتناب‌ناپذیر به نظر می‌رسد. در این میان، مخاطرات پول‌شویی داری‌های مجازی آن را محور تدابیر سیاست جنایی قرار داده است. ویژگی‌هایی مانند سرعت و گم‌نامی و ردیابی‌نشدن سبب شده بزهکاران از این داری‌ها به‌طور گسترده‌ای استفاده کنند؛ ازاین‌رو کشورها در چهارچوب نظام عدالت کیفری خود در تلاش‌اند نسبت به مهار مخاطرات جنایی پول‌شویی داری‌های مجازی در دو بُعد پیشگیرانه و واکنشی اقدام کنند. براین اساس، برای اتخاذ راهبردهای مطلوب در سطح نظام عدالت کیفری، در وهله نخست شناخت چیستی داری‌های مجازی از حیث فنی و حقوقی و سپس بررسی ظرفیت‌های جنایی آن از اهمیت بسیار زیادی برخوردار است؛ چراکه پیش‌شرط اتخاذ هر راهبرد کنشی یا واکنشی شناخت دقیق پدیده موضوع این اقدامات خواهد بود. امری که زمینه لازم را برای ارائه الگوی مطلوب سیاست جنایی در دو سطح پیشگیرانه و کیفری فراهم خواهد ساخت؛ ازاین‌رو در پژوهش حاضر، با رویکردی توصیفی-تحلیلی و با بررسی منابع کتابخانه‌ای ازجمله اسناد فراملی، قوانین و مقررات داخلی، رویکرد نظام عدالت کیفری به ریسک مجرمانه‌داری‌های مجازی بررسی خواهد شد. در این چهارچوب، با بررسی وضعیت موجود در نظم حقوقی-کیفری ایران، بایسته‌های سیاست جنایی در این زمینه ترسیم خواهد شد.

*نویسنده مسئول

رایانامه: Arefkhalilipaji@gmail.com

نحوه استناددهی:

خلیلی پاجی، عارف، و پرهیزکاری، سمیه (۱۴۰۴). رویکرد نظام عدالت کیفری به ریسک مجرمانه‌داری‌های مجازی. حقوق فناوری‌های نوین، ۶(۱۱)، ۷۵-۹۵.

ناشر: دانشگاه علم و فرهنگ <https://www.usc.ac.ir>

شاپای الکترونیکی: ۳۸۳۶-۲۷۸۳

فرایند گذار به جامعه‌ای جهانی با توسعه مبادلات تجاری بین‌المللی، همکاری‌های اقتصادی بین‌المللی و ارتباطات گسترده در سطح جهان به سرعت در حال تکامل است که نمونه اجلی آن در اقتصاد جهانی تبلور یافته است. گسستن قیود و مرزبندی‌های اجتماعی و تبدیل شدن به یک جامعه جهانی واحد و معرفی ابزارهای فناوریانه سبب شد مبادلات اقتصادی تسهیل شود. این ابزارهای فناوریانه با کارکرد پول یا به عنوان روش جدیدی از پرداخت با نام دارایی‌های مجازی^۱ شناخته شده و به سرعت در کشورهای مختلف رواج یافتند. این فناوری جدید بستری را برای سهولت در تبادلات فراهم کرد؛ اما در عین حال به سبب ویژگی‌های خاص خود، نظیر گمنامی هویت افراد، نبود امکان رهگیری زنجیره معاملات و بعضاً برخوردار نبودن از پشتوانه حاکمیتی، توجه بزهکاران را به خود جلب کرد.

ماهیت برخی از دارایی‌های مجازی به گونه‌ای است که بدون نیاز به واسطه، امکان معاملات شخص به شخص را فراهم کرده است. این ویژگی نظر کشورهایی را که همواره از نظر اقتصادی بی‌ثبات بوده‌اند و ریسک ورشکستگی نهادها و مؤسسات مالی در آن‌ها بالا ارزیابی شده به خود جلب کرده است، امری که سبب افزایش تمایل مردم به استفاده از دارایی‌های مجازی، به ویژه رمزارزها، شده است. در واقع، برای اشخاصی که چنین نهادهایی را به اندازه کافی مطمئن نمی‌دانند، دارایی‌های مجازی جایگزینی مناسب تلقی می‌شوند^۲ (Bershidsky, 2017).

براین اساس، ابداع و توسعه دارایی‌های مجازی توانسته به منزله جلوه نوینی از جهانی شدن اقتصاد رخ‌نمایی کند. این امر در کنار همه مزیت‌هایی که دارد، دستیابی کنترل‌ناپذیر انسان‌ها به مناطق جغرافیایی و منابع مالی و اطلاعاتی را فراهم آورده که خود بستر ساز فعالیت‌های غیرقانونی شده است (Ritzer, 2007, p. 30)؛ زیرا جرایم تابعی از فرصت‌ها هستند و جهانی شدن، که به واسطه توسعه فناوری شتاب بیشتری به خود گرفته، فرصت‌های فراوانی را برای انواع فعالیت‌های مجرمانه به وجود آورده است (Simpson and Weisburd, 2009, p. 201). شبکه‌های گسترده فناوری ارتباطات و اطلاعات زمینه‌های فراوانی برای سوءاستفاده بزهکاران بین‌المللی در قالب جرایمی همچون پول‌شویی به وجود آورده است که قابلیت کنترل مادی کمتری دارند (Viano, 2008, p. 88).

پول‌شویی از رهگذر پنهان کردن منشأ عواید، در پی پاک‌نمایی پول‌های نامشروع است. مرتکبان پول‌شویی استفاده از دارایی‌هایی مجازی را بستری امن برای مخفی کردن رد عواید مجرمانه و ناشناس ماندن زنجیره افراد درگیر در معاملات تلقی کرده، اهداف مجرمانه‌ی خود را از این مسیر پیگیری می‌کنند. دارایی‌های مجازی می‌تواند از طریق اینترنت و با ابزارهایی از جمله تلفن همراه، حتی در پرداخت‌های برون‌مرزی در دسترس باشد. افزون‌براین، این فناوری معمولاً به زیرساخت‌های پیچیده‌ای متکی هستند که شامل چندین نهاد در کشورهای مختلف می‌شوند و برای انتقال وجوه یا عملیات پرداخت استفاده می‌شوند. این گونه از ارائه خدمات و درگیر بودن چندین کشور، به منزله حوزه‌های قضایی مختلف، مشکلاتی را در تعیین مسئول مبارزه با پول‌شویی و تأمین مالی تروریسم، ناظر و مجری این مقررات ایجاد خواهد کرد (Khalili Paji, 2019, 113-134).

درواقع ویژگی‌های چشمگیر دارایی‌های مجازی موجب بروز دل‌نگرانی‌هایی در سطح جهانی شده و کشورها را وادار به چاره‌اندیشی برای حل چالش‌های پیش‌رو کرده است.

1. virtual assets

۲. «از دیگر ویژگی‌های مهم دارایی‌های مجازی، استقلال آنها از ارزش‌های ملی رایج و به ویژه دلار است که این امر منجر به کسب محبوبیت بیشتر آن، به خصوص برای کشورهای تحت تحریم شده است. همچنین از آنجا که بسیاری از شهروندان کشورهای ضعیف اقتصادی در برقراری ارتباطات بانکی جهانی با مشکلات زیادی مواجه هستند، رمزارزهایی چون بیت‌کوین به عنوان یکی از مصادیق دارایی‌های مجازی می‌تواند منجر به مشارکت آن‌ها با استفاده از اینترنت در اقتصاد جهانی شود» (خلیلی پاجی، ۱۴۰۰، ص ۷۲-۷۴)

در این راستا، گروه ویژه اقدام مالی (FATF) که اهداف خود را به پیشگیری و مقابله با پول شویی و تأمین مالی تروریسم معطوف ساخته است، به منزله سازمانی فراملی، توصیه هایی را به منظور پیشگیری و مقابله با این جرایم به کشورها ارائه کرد. رویکرد اتخاذی توصیه ها مبتنی بر شفافیت در حوزه های مالی و همچنین به کارگیری رویکرد ریسک محور است.

گروه مذکور در بازبینی توصیه های اخیر خود^۱، به طور خاص به دارایی های مجازی نیز توجه نشان داده است. دارایی های مجازی ابزاری فناوریانه با ریسک بالا هستند که در جهت خدمت به پول شویان استفاده می شوند؛ از این رو گروه ویژه اقدام مالی، با پیروی از رویکرد ریسک محور به شناسایی این دسته و شمول الزامات مبارزه با پول شویی بر ارائه دهندگان خدمات دارایی های مجازی تمرکز کرده است. هدف از این امر، از یک سو پیشگیری از جرایم مذکور و از سوی دیگر، در صورت ارتکاب جرم، کشف سریع جرم و مداخله کیفری پیرامون آن است.

با توجه به شکل گیری رویکردهای ملی و فراملی در خصوص ریسک مجرمانه دارایی های مجازی، چگونگی مداخله نظام عدالت کیفری در این زمینه و نحوه مواجهه آن با ریسک های جنایی دارایی های مجازی از اهمیت زیادی برخوردار است. این امر در وهله اول مستلزم شناخت ماهیت فنی و حقوقی این دارایی هاست تا زمینه لازم برای شناسایی ظرفیت های مجرمانه این فناوری به منظور ارائه بایسته های کنشی و واکنشی در برابر آن فراهم شود. در این راستا، با نگاهی به مقررات و مصوبات موجود و مرتبط در نظام حقوقی ایران، در قسمت اول پژوهش حاضر، دارایی های مجازی از حیث ماهیت فنی و حقوقی بررسی می شوند و سپس ظرفیت های مجرمانه آن ها معرفی می شود. از این رهگذر است که در قسمت دوم به ضرورت شمول الزامات نظام مبارزه با پول شویی بر دارایی های مجازی با نگاهی به رویکردهای فراملی پرداخته خواهد شد و در نهایت بایسته های سیاست جنایی در این زمینه که در بردارنده دو راهبرد پیشگیرانه و کیفرمدارانه است، بررسی خواهد شد.

۱. دارایی های مجازی؛ از چیستی تا ظرفیت های مجرمانه

ارز مجازی نشانه رقومی از ارزشی است که قابلیت معامله را به صورت الکترونیکی دارد و عملکردی مانند یک ابزار مبادله یا یک واحد حساب یا یک مجموعه ارزش دارد، اما وضعیت قانونی پول رایج را در هیچ کشوری ندارد و عملیات فوق تنها با توافق در جامعه کاربران پول مجازی انجام می گیرد (FATF, 2015, p. 26). برای درک بهتر مفهوم دارایی های مجازی، ناگزیر به بررسی ماهیت فنی و حقوقی آن ها هستیم تا علاوه بر شناخت ظرفیت جنایی آن ها، رویکرد مناسبی در برابر آن اتخاذ کنیم.

۱-۲. ماهیت فنی دارایی های مجازی

دارایی مجازی عنوانی عام برای برخی ابزارهای فناوریانه با ویژگی ها و کارکردهای پول یا ابزارهای مبادله است. برخی از مصادیق این فناوری را می توان ارزهای مبتنی بر فناوری رمزنگاری دانست که با عناوینی چون «رمزارز»، «ارز رمز پایه» و «رمزین ارز» در نوشتگان فارسی استفاده می شود. این فناوری برآمده از فضای مجازی است و در بستر این فضا معنا می یابد (Soleimanipour et al., 2016, p. 173). دارایی های مجازی در یک دسته بندی و بر مبنای قابلیت تبدیل شدن به سایر دارایی های مجازی یا پول های ملی به دو دسته «قابل تبدیل» و «غیرقابل تبدیل» تقسیم می شوند. دارایی های مجازی غیرقابل تبدیل به لحاظ سامانه ای، امکانی برای تبدیل به سایر ارزها یا پول ها ندارند. نمونه بارز این گونه از دارایی، پول ها یا سکه هایی است که در بازی های رایانه ای یا موبایلی کسب می شوند و فقط امکان هزینه شدن در همان بازی را دارند و اصطلاحاً به آن ها «سکه بازی» می گویند (Khalili Paji, 2022a, p. 16).

۱. توصیه شماره ۱۵ گروه ویژه اقدام مالی: «کشورها و نهادهای مالی باید ریسک های پول شویی و تأمین مالی تروریسم را که ممکن است درباره موضوعات زیر به وجود آید شناسایی و ارزیابی کنند: الف) توسعه محصولات جدید و شیوه های کسب و کار جدید از جمله سازوکارهای جدید برای تحویل کالا؛ ب) استفاده از فناوری های جدید یا در حال توسعه در خصوص محصولات جدید یا قدیم. در مورد نهادهای مالی، باید این ارزیابی از ریسک، قبل از راه اندازی محصولات جدید، شیوه های کسب و کار و یا استفاده از فناوری های جدید یا در حال توسعه انجام شود. نهادهای مزبور باید تدابیر مناسبی را برای مدیریت و کاهش آن ریسک ها اتخاذ کنند. به منظور مدیریت و کاهش ریسک های مربوط به دارایی مجازی، کشورها باید اطمینان حاصل کنند که ارائه دهندگان خدمات مربوط به دارایی مجازی در راستای اهداف مبارزه با پول شویی و تأمین مالی تروریسم مشمول مقررات می باشند و دارای مجوز بوده یا ثبت شده اند و به منظور پایش و اطمینان از پایبندی آن ها به تدابیر مرتبط مطالبه شده در توصیه های گروه ویژه اقدام مالی تحت نظامات مؤثرند.

در مقابل دارایی مجازی غیرقابل تبدیل، دارایی مجازی قابل تبدیل قرار می‌گیرد. این گونه دارایی‌ها امکان تبدیل شدن به پول‌های ملی و برعکس و نیز قابلیت خرید کالا و خدمات حقیقی یا مجازی را دارند. این دسته از دارایی‌های مجازی، نمونه‌ای بارز و پیشرو از پول‌های مجازی هستند که خود به دو دسته متمرکز و غیرمتمرکز تقسیم می‌شوند (Kotane, 2018, p. 63).

دارایی مجازی قابل تبدیل متمرکز آن است که انتشار و کنترل آن از طریق یک نهاد مرکزی صورت می‌گیرد و سازنده و کنترل‌کننده آن مشخص است. در مقابل، دارایی مجازی قابل تبدیل غیرمتمرکز، مانند بیت‌کوین، قابلیت استخراج، خلق یا تولید به دست کاربران براساس الگوریتم‌های ریاضی و رمزنگاری را دارد؛ از این رو به آن‌ها «رمزینه ارز» یا «ارز رمزنگاری شده» یا «رمزارز» گفته می‌شود. نمونه بارز این ارزها بیت‌کوین است که با استفاده از فناوری دستگاه‌های استخراج تولید می‌شوند. استخراج ارز از فرایند مشخصی مبتنی بر الگوریتم‌های ریاضی برخوردار است (Dawood, 2019, p. 759).

۱-۳. ماهیت حقوقی دارایی‌های مجازی

بررسی همه‌جانبه ابعاد و انواع دارایی‌های مجازی به‌منزله پدیده‌ای نوین و در حال گسترش امری ضروری است. از میان ابعاد گوناگون، شناسایی ماهیت حقوقی دارایی‌های مجازی در تدوین و تنظیم قوانین و مقررات شایسته، عنصری اساسی است. در واقع، می‌توان کارکرد دارایی‌های مجازی را از لحاظ مبانی حقوقی و اقتصادی مشابه با پول دانست که می‌توانند در مبادلات پذیرفته شوند؛ اما این مسئله مستلزم شناسایی و تصدیق دولت‌هاست.

با وجود این، گفتنی است چهار دیدگاه عمده در نظام‌های حقوقی درباره ماهیت حقوقی دارایی‌های مجازی مطرح شده است: ۱) دارایی مجازی در قالب پول؛ ۲) دارایی مجازی در قالب اوراق بهادار؛ ۳) دارایی مجازی در قالب کالا؛ ۴) دارایی مجازی در قالب یکی از اقسام اموال (Mafi & Rameshi, 2022, p. 2).

شناسایی ماهیت دارایی‌های مجازی، بسته به ساختار فنی آن‌ها، متفاوت است و از این رو نمی‌توان ماهیتی یکسان برای تمامی دارایی‌های مجازی قائل بود؛ بنابراین این تقسیم‌بندی می‌تواند ناشی از تنوع ماهیتی این دارایی‌ها باشد. ارزهای مجازی را می‌توان به رمزارز ملی، رمزارزهای با پشتوانه، کوین‌ها و توکن‌ها تقسیم‌بندی کرد.

رمزارز ملی توسط دولت‌ها خلق و کنترل می‌شوند؛ لذا کاملاً رمزارز محسوب نمی‌شوند. در مقابل، کوین‌ها، که با نام‌های رمزارزهای بین‌المللی یا جهان‌روا نیز خوانده می‌شوند، نمونه اجزای ارزهای غیرمتمرکزند. این رمزارزها توسط هیچ نهاد مرکزی‌ای صادر و کنترل نمی‌شوند؛ بلکه عملیات صدور توسط همین افراد تأیید و ثبت می‌شود (Nouri et al., 2021, p. 352).

علاوه بر این می‌توان برخی از رمزارزها را با مفهوم اوراق بهادار تطبیق داد. برای مثال، توکن‌هایی که در یک عرضه اولیه منتشر می‌شوند ممکن است جنبه سرمایه‌گذاری داشته باشند که در این حالت، شرکت عرضه‌کننده توکن دارندگان را در سود حاصل از فعالیت نوآورانه‌ای که خلق توکن و فروش آن به هدف تحقق این فعالیت انجام شده است، شریک می‌کند (Hacker & Thomale, 2018, p. 13).

یکی دیگر از رویکردهایی که در خصوص ماهیت حقوقی دارایی مجازی وجود دارد، مال محسوب کردن دارایی‌های مجازی است. برخی از حقوق‌دانان معتقدند: «مال به چیزی گفته می‌شود که از نظر اقتصادی ارزش مبادله داشته باشد و بتواند مورد دادوستد قرار گیرد» (Emami, 2008, p. 22).

«مال» تا پیش از تصویب قانون مبارزه با پول‌شویی، در قوانین ایران تعریف مشخصی نداشت. باین حال بند «ب» ماده ۱ قانون مبارزه با پول‌شویی اصلاحی ۱۳۹۷ و بند «۳۲» ماده «۱» آیین‌نامه اجرایی قانون مبارزه با پول‌شویی «مال را هر نوع دارایی، وجوه یا منابع اقتصادی اعم از مادی یا غیرمادی، محسوس یا غیرمحسوس، منقول یا غیرمنقول، نقد یا غیرنقد، مشروع یا غیرمشروع و هر نوع منفعت یا امتیاز مالی یا وجوه اعم از نقد و غیرنقد و همچنین کلیه اسناد قانونی مبین حق اعم از کاغذی یا الکترونیکی نظیر اسناد تجاری، سهام، یا اوراق بهادار» تعریف کرده

است. به نظر می‌رسد با پذیرش عرفی دارایی های مجازی به منزله اموال غیرمادی، می‌توان قائل به مال بودن دارایی های مجازی شد. با این حال، ضروری است قانون‌گذار بسته به ماهیت و کارکرد دارایی های مجازی به عنوان پول، دارایی یا اوراق بهادار، انواع آن‌ها را شناسایی کند و وضعیت حقوقی مبادلات هریک را مشخص سازد.

درخصوص ماهیت حقوقی دارایی های مجازی در نظام حقوقی ایران طی سال‌های اخیر، نظر واحدی وجود نداشته است. بخشی از این امر به دلیل سیاست ممنوع‌سازی استفاده از این فناوری بوده است. براین اساس در جلسه سی‌ام شورای عالی مبارزه با پول‌شویی در تاریخ ۱۳۹۶/۱۰/۹ به کارگیری ابزار بیت‌کوین و سایر ارزهای مجازی در تمام مراکز پولی و مالی کشور، به جهت قابلیت آن در ارتکاب پول‌شویی و تأمین مالی تروریسم ممنوع اعلام شد. با این حال با گذشت بیش از یک سال از مصوبه مذکور، بانک مرکزی ایران رویکرد واقع‌بینانه‌تری در قبال ارزهای مجازی اتخاذ کرد. براین اساس معاونت فناوری های نوین بانک مرکزی جمهوری اسلامی ایران، اقدام به انتشار پیش‌نویس سند «الزامات و ضوابط فعالیت‌ها در حوزه رمزارزها در کشور» مورخ ۱۳۹۷/۱۱/۰۸ را با هدف بررسی و ارائه نظرات متخصصان و صاحب‌نظران منتشر کرد که قرار بود پس از انجام اصلاحات احتمالی و با تصویب شورای پول و اعتبار جهت اجرا ابلاغ شود. سند مذکور اقدام به ارائه تعریفی از ارزهای مجازی به منزله یک نوع دارایی مالی بر بستری دیجیتال، غیرمتمرکز و شفاف پرداخت و آن را در چهار دسته ارزهای جهان‌روا، رمزارزهای بانک مرکزی، رمزارز منطقه‌ای و رمزارز حاصل از عرضه سکه یا توکن قرار داد. با وجود این، به دلیل فقدان طی تشریفات قانونی برای تصویب این سند، این سند هیچ‌گاه به مرحله اجرا درنیامد.

رویکرد دیگر در تعیین ماهیت دارایی های مجازی، تلاش برای ارز خارجی محسوب کردن این فناوری بوده است. قانون‌گذار در لایحه اصلاحی قانون مبارزه با قاچاق کالا و ارز در سال ۱۳۹۹، تلاش کرد به تصویب تبصره ۷ ماده ۲ مکرر الحاقی بپردازد که مقرر می‌داشت: «تمامی رمزارزها (ارزهای رقمی) در حکم ارز موضوع این قانون هستند و جرایم، تخلفات، ضمانت اجراها و نیز تمامی احکام و مقررات مربوط به ارز در این قانون در مورد آن‌ها نیز اجرا می‌شود.» امری که از متن نهایی مصوبه حذف شد.

در نهایت قانون جدید بانک مرکزی که در آذرماه ۱۴۰۲ ابلاغ شد به اختلافات در این زمینه پایان داد و با به کارگیری عبارت «رمزپول» در بند «ض» مقرر داشت: «رمزپول نوعی پول رقمی دیجیتال رمزنگاری شده است که در بستر پایگاه داده اشتراکی به صورت متمرکز (با محوریت بانک مرکزی) یا غیرمتمرکز ایجاد و به صورت غیرمتمرکز مبادله می‌شود.» از این رو، به نظر می‌رسد سیاست‌گذاران ایرانی به ماهیت پولی این فناوری توجه کرده‌اند.

۴-۱. ظرفیت های جنایی دارایی های مجازی

ماهیت جرایم، به‌ویژه جرایم اقتصادی و مالی، طی فرایند جهانی شدن تغییراتی را به خود دیده است؛ به گونه‌ای که امروزه «سازمان‌یافتگی»، «فرامرزی بودن» و «اتخاذ سازوکارهای پیچیده برای ارتکاب» از جمله ویژگی های مهم این دسته از جرایم است. از نظر ویژگی های ساختاری، بزه جهانی بیشتر اوقات با مشخصاتی همچون نبود تمرکز، انعطاف‌پذیری، قابلیت انطباق، به کارگیری فناوری های نوین و گستردگی شبکه توصیف می‌شوند (Rotman, 2001, p. 5).

در این میان، ترکیب دارایی های مجازی با برخی فناوری های دیگر در بستر فضای مجازی، موجبات توسعه ظرفیت های مجرمانه را پدید آورده‌اند که بارزترین ثمره آن، انعطاف‌پذیری در هویت است. این امر بدین معناست که اطلاعات مشخصی از کاربران این فناوری (فرستنده، گیرنده و استخراج‌کننده) وجود ندارد یا این اطلاعات لزوماً با اطلاعات هویت واقعی آن‌ها منطبق نیست. در واقع آن‌ها نه تنها از هویت های جعلی استفاده می‌کنند، بلکه مکرراً هویت خود را نیز تغییر می‌دهند (Safari et al., 2019, p. 231)، امری که در کنار ناشناس ماندن معاملات مبتنی بر این فناوری، نظارت بر تراکنش‌ها را مشکل می‌سازد. در واقع، به دلیل فقدان یک نهاد ناظر، امر ردیابی منشأ عواید با دشواری مواجه می‌شود. نبود نهاد مرکزی کنترل‌کننده و همچنین عدم شناسایی کاربران از بُعد دیگری نیز شایان توجه است. این بُعد، امکان اتحاد فراملی برای

ارتکاب جرم است. بررسی‌ها نشان می‌دهد متهمان برخی پرونده‌های مربوط به دارایی‌های مجازی در کشورهای مختلف مانند آمریکا و تایلند ساکن بوده‌اند و از راه دور در انجام فعالیت‌های مجرمانه با استفاده از ارزهای مجازی با یکدیگر مشارکت داشته‌اند (Kethineni et al., 2018, p. 149).

وجود این ویژگی‌ها، نظر مرتکبان پول‌شویی را به منظور پاک‌نمایی عواید مجرمانه به خود جلب کرده است. در واقع، مرتکبان پول‌شویی استفاده از دارایی‌های مجازی را بستری امن برای دستیابی به اهداف خود، یعنی پنهان کردن منشأ عواید و ناشناس ماندن زنجیره معاملات می‌دانند.

۲. شمول الزامات نظام مبارزه با پول‌شویی بر دارایی‌های مجازی؛ از ضرورت تا شیوه شمول

دارایی‌های مجازی در کنار تمام خصیصه‌های مثبت خود، دربردارنده چالش‌هایی در نظام عدالت کیفری است. امری که مخاطرات آن در عرصه اقتصاد ملی و فراملی، نیاز به ارائه راهکاری ایمن برای پیشگیری و مقابله با آن را اجتناب‌ناپذیر ساخته است.

۲-۱. مفهوم نظام مبارزه با پول‌شویی

در دهه‌های گذشته، تصویب شمار بسیاری از اسناد بین‌المللی حول محور پیشگیری و مقابله با پول‌شویی، اهمیت مبارزه با این جرم را به سبب آثار زیان‌بار آن در ابعاد داخلی و بین‌المللی آشکار ساخته است؛ از این رو مبارزه با پول‌شویی همواره یکی از اهداف اساسی دولت‌ها در چهارچوب سیاست جنایی بوده است. بررسی رویکردهای پیشگیرانه و مقابله‌ای در زمینه پول‌شویی حاکی از تحولات درخور توجهی در این عرصه است. روند مقابله با پول‌شویی همیشه یکسان نبوده و تحولاتی را پشت‌سر گذاشته تا از مفهوم سنتی خود به مفهومی نوین، یعنی شکل‌گیری نظام پیشگیری و مقابله با پول‌شویی، تبدیل شود^۱.

در واقع، ابعاد فراملی و سازمان‌یافتگی پول‌شویی، اثرات نامطلوب آن بر جامعه و نحوه عملکرد پول‌شویان، که منابع ناشی از جرم را طی فرایندی مخفی می‌کردند، کشورها را برآن داشت که واکنش سخت‌تری در برابر این‌گونه مجرمان داشته باشند و در برخی موارد از قواعد سنتی عدول کنند (Paknahad, 2014, p. 81)، امری که با گسترش فضای مجازی و استفاده از دارایی‌های مجازی وارد ابعاد جدیدی شده است. بدین ترتیب و با توجه به شرایط پیش‌آمده، دیگر صرف جرم‌انگاری پول‌شویی برای مقابله با این جرم، کافی به نظر نمی‌رسد؛ بلکه برپایه آموزه‌های مدیریت ریسک، نیازمند نظامی دقیق و یکپارچه‌ای هستیم که ضمن جرم‌انگاری مؤثر و کیفرگذاری بازدارنده، تدابیری برای پیشگیری در حوزه‌های مختلف ارائه دهد، امری که در چهارچوب نظام مبارزه با پول‌شویی معنا پیدا می‌کند.

۲-۲. رویکرد گروه ویژه اقدام مالی به دارایی‌های مجازی

گروه ویژه اقدام مالی (FATF) نهادی بین‌الدولی است که از سال ۱۹۸۹ توسط کشورهای عضو گروه هفت^۲ تشکیل شده و به‌طور تخصصی فعالیت خود را آغاز کرده است. نخستین مأموریت و هدف گروه ویژه، وضع قواعدی در راستای پیشگیری و مبارزه با پول‌شویی بوده است. این مأموریت تا بدین‌جا ختم نشد و به‌تدریج کارویژه‌های دیگری در محدوده اقدامات این گروه قرار گرفت؛ به‌ویژه پس از وقوع حملات یازده

۱. در ابتدا کشورها پول‌شویی را جرم مستقلی قلمداد نمی‌کردند؛ بلکه برخی آن را نتیجه جرایم منشأ به حساب آورده و بر این نظر بودند که مصادره و توقیف اموال ناشی از آن جرایم برای مبارزه با پول‌شویی کفایت می‌کند. این تفکر از آن ناشی می‌شود که پول‌شویی را تنها تداوم جرم اولیه‌ای می‌دانستند که مجرم برای گریز از مجازات به آن دست می‌زند.

براساس دیدگاه دیگر، جرم پول‌شویی شکلی از معاونت و تسهیل در امر جرم منشأ است. براساس این نظریه اشخاصی مجازات می‌شوند که قصد پنهان کردن منبع نامشروع مال یا اخلال در تحقیق و رسیدگی در مورد منبع، ضبط، مصادره یا توقیف درآمد حاصل از جرم را دارند. دیدگاه دیگری که می‌توان آن را دیدگاه غالب دانست، معتقد است هرگونه معامله روی اموال یا دارایی‌ها با آگاهی از اینکه مال مورد نظر از فعالیت‌های مجرمانه به دست آمده، برای تحقق جرم پول‌شویی کافی است (جزایری، ۱۳۸۲، ص ۱۲۰).

۲. در سال ۱۹۷۵، شش کشور صنعتی جهان شامل فرانسه، آلمان (غربی)، ایتالیا، ژاپن، بریتانیا و آمریکا، یک گروه بین‌المللی مالی تحت عنوان گروه شش (G6) را تشکیل دادند که یک سال پس از آن، با پیوستن کشور کانادا به این گروه، گروه مزبور به گروه هفت (G7) تغییر نام یافت. سپس در سال ۱۹۹۷ با اضافه شدن روسیه به این دسته از کشورها، گروه هشت نامیده شد؛ البته درحال حاضر این گروه بعضاً همان گروه هفت نیز نامیده می‌شود.

سپتامبر، مبارزه با تأمین مالی تروریسم نیز به اهداف و مأموریت های این گروه افزوده شد. همچنین با افزایش تنش در حوزه های هسته ای، ممانعت از تأمین مالی اشاعه سلاح های کشتار جمعی نیز در دستور کارگروه ویژه قرار گرفت.

گروه ویژه اقدام مالی به دارایی های مجازی به منزله دسته ای که ریسک ارتکاب جرم و به ویژه پول شویی در آن ها بالا ارزیابی می شود، توجه نشان داده است و تلاش کرده در توصیه های خود، به لزوم اهمیت شناسایی، تنظیمگری و ارزیابی میزان ریسک ارزهای مجازی توسط کشورها بپردازد.

گروه ویژه اقدام مالی در ژوئن ۲۰۱۴ سند مربوط به «ارزهای مجازی: تعاریف و ریسک های بالقوه پول شویی و تأمین مالی تروریسم و پاسخ ها» (FATF, 2014) را منتشر کرد و ضمن آن به ظهور ارزهای مجازی و سازوکار مربوط به پرداخت آن ها به عنوان یک روش نوین انتقال ارزش، از طریق اینترنت پرداخت. این گروه در ماه ژوئن سال ۲۰۱۵ نیز به موجب راهنمای مربوط به «رویکرد ریسک مدار در برابر ارزهای مجازی» (FATF, 2015) به ارزیابی ریسک مجرمانه ارزهای مجازی به ویژه در حوزه پول شویی و تأمین مالی تروریسم پرداخت.

راهنمای سال ۲۰۱۵ بر این نکته تمرکز داشت که ارزهای مجازی دروازه نظام تنظیمگری مالی سنتی به سوی یک نظام نوین تنظیمگری است، امری که به تدریج توسعه یافت و در نتیجه آن، در سال های اخیر، فضای دارایی های مجازی با افزایش ناگهانی رمزارزها، گمنام سازها، پلتفرم های غیر متمرکز و صرافی ها و دیگر ابزارها و خدماتی که قابلیت کاهش شفافیت و افزایش تداخل جریان های مالی را دارند و نیز ظهور مدل های تجاری مجازی یا فعالیت های چون عرضه سکه های اولیه، که در بر دارنده ریسک کلاهبرداری و دست کاری بازار است، روبه رو شده است (Khalili Paji, 2022a, p. 70).

گسترش مصادیق ارزهای مجازی و خدمات ناشی از آن، به افزایش ریسک در این دسته منجر شد و گروه ویژه اقدام مالی را بر آن داشت تا با روزآمد کردن توصیه های خود، اقدامات پیشگیرانه را به نحو مطلوب تری در این حوزه بگمارد. چنان که در اکتبر سال ۲۰۱۸ گروه ویژه اقدام به تعریف دو واژه جدید «دارایی های مجازی» و «ارائه دهندگان خدمات مربوط به دارایی های مجازی» و اصلاح توصیه شماره ۱۵ خود کرد. هدف از اعمال این تغییرات، ارائه رهنمودی به دولت ها است تا نسبت به سیاست گذاری در حوزه ارائه دهندگان خدمات دارایی های مجازی، در این چهارچوب مشخص اقدام کنند و از این رهگذر رویکردی منسجم میان کشورها، که همانا رویکردی ریسک مدار است، به کار گرفته شود. بر این اساس، گروه ویژه اقدام مالی در ژوئن ۲۰۱۹ با افزودن یک یادداشت تفسیری به توصیه شماره ۱۵، کشورها را ملزم کرده علاوه بر الزام ارائه کنندگان خدمات مربوط به دارایی مجازی به انجام اقداماتی نظیر (شناسایی مشتری، ثبت سوابق، ارائه گزارش های مشکوک و...)، نسبت به پیگیری اخذ مجوز و ثبت آن ها اقدام کنند تا زمینه پیشگیری و مقابله با پول شویی و تأمین مالی تروریسم بیش از پیش فراهم شود.

بنابراین، رویکرد گروه ویژه اقدام مالی به ارزهای مجازی را می توان در چند گام تبیین کرد. نخست آن که قسم کلی تری از رمزارزها، یعنی دارایی های مجازی، را به رسمیت شناخت؛ دوم آن که رویکردی مبتنی بر ریسک را در حوزه دارایی های مجازی عرضه کرد و در آخر این اصول را به منزله الگویی در سطوح ملی و فراملی معرفی کرد.

۲-۳. شیوه شمول نظام مبارزه با پول شویی بر دارایی های مجازی

دارایی های مجازی قابلیت استفاده در طیف وسیعی از جرایم را دارند، اما مهم ترین آن پول شویی است. دلیل اهمیت مبارزه با پول شویی آن است که پیشگیری و مقابله با این جرم به کاهش وقوع جرایم منشأ نیز منجر خواهد شد. در واقع، اگر این مبارزه به حدی تکامل یابد که امکان تطهیر درآمدهای حاصل از اعمال ناقض قانون از مرتکبان سلب شود، عملاً ارتکاب جرم منشأ بی فایده خواهد بود (Siah-Bidi Kermanshahi & Sales moyyed, 2016, p. 22).

ازاین‌رو، گروه ویژه اقدام مالی با تسری قوانین مبارزه با پول‌شویی بر دارایی‌های مجازی و همسوساختن دولت‌ها در اتخاذ این رویکرد، تلاش کرده به‌طور مؤثری از ریسک ارتکاب پول‌شویی در این دسته پیشگیری کند. بااین‌حال، موفقیت در این امر از سویی در گرو شناسایی قانونی دارایی‌های مجازی و از سوی دیگر مستلزم به‌رسمیت شناختن فعالیت‌های ارائه‌دهندگان خدمات مجازی است.

هم‌اکنون در برخی از کشورها، وضعیت قانونی دارایی‌های مجازی کاملاً مشخص نیست و منطقه‌ای خاکستری محسوب می‌شوند؛ ازاین‌رو، نخستین گام ضروری برای دولت‌ها، شناسایی دارایی‌های مجازی و قانونی‌سازی ابعاد گوناگون آن است. اهمیت این امر از آن‌روست که دارایی‌های مجازی برای تحت شمول قرارگرفتن مقررات مبارزه با پول‌شویی، می‌باید در دایره یک شی ارزشمند، خواه پول یا مال، قرار گیرند. در این راستا، بند «ب» ماده ۱ قانون مبارزه با پول‌شویی اصلاحی ۱۳۹۷ و بند ۳۲ ماده ۱ آیین‌نامه اجرایی قانون مبارزه با پول‌شویی ۱۳۹۸، مال را هر نوع دارایی، وجوه یا منابع اقتصادی اعم از مادی یا غیرمادی، محسوس یا غیرمحسوس تعریف کرده‌اند. بااین‌حال، با تصویب قانون جدید بانک مرکزی دیگر تردیدی بر شمول قانون مبارزه با پول‌شویی بر این فناوری نیست.

گام بعدی دولت‌ها، مطابق با الزامات گروه ویژه اقدام مالی، شناسایی نهادهای ارائه‌دهنده دارایی‌های مجازی است. این دسته اشخاصی هستند که یک یا چند فعالیت ذیل را به نمایندگی از اشخاص دیگر انجام می‌دهند: ۱. مبادله بین ارزهای مجازی و فیات؛ ۲. مبادله بین یک یا چند نوع دارایی مجازی؛ ۳. نقل و انتقال دارایی‌های مجازی؛ ۴. نگه‌داری یا اداره دارایی‌های مجازی یا ابزارهایی که امکان کنترل دارایی‌های مجازی را دارند؛ ۵. مشارکت و ارائه خدمات مالی مربوط به ایجاب به‌منظور فروش یا فروش دارایی‌های مجازی (FATF, 2019).

در این راستا، یکی از گام‌های مثبتی که اخیراً برداشته شده، افزودن مشاغلی به لیست مشاغل غیرمالی است که به ارائه خدمات دارایی‌های مجازی می‌پردازند. در تاریخ ۱۴۰۱/۰۷/۰۴ مرکز اطلاعات مالی در نامه‌ای، درخصوص تعیین مصادیق مشاغل غیرمالی، با توجه به بررسی نتیجه جلسات وزارتخانه صمت با محوریت اهمیت جریان‌های نقدی مشکوک و احتمال انجام آن در گروه مشاغل غیرمالی، نظر نهایی خود را پیرامون فهرست نهایی مصادیق مشاغل غیرمالی منطبق بر مفاد قانون و آیین‌نامه اجرایی ماده ۱۴ الحاقی قانون مبارزه با پول‌شویی اعلام کرد. متعاقب این نامه در تاریخ ۱۴۰۱/۰۷/۱۲ وزارتخانه صمت، فهرست نهایی مشاغل غیرمالی را منتشر کرد که مزایع بزرگ و متوسط استخراج رمزارزها، خدمات کیف پول متولی رمزارزها و مبادلات رمزنگاری فیات در این دسته قرار دارد.

این اقدام گامی بلند در راستای تنظیمگری و شمول مقررات ضد پول‌شویی بر این دسته از مشاغل خواهد بود. وزارت صمت مطابق با تبصره ماده «۱۴۹»^۱ قانون مبارزه با پول‌شویی، اختیار تعیین مصادیق جدید مشاغل غیرمالی را دارد. طبیعی است این اختیار صرفاً به مواردی محدود است که قلمرو آن را قانون‌گذار شناسایی کرده باشد؛ ازاین‌رو با توجه به تصویب قانون جدید بانک مرکزی و به‌خصوص ماده ۵۹ آن و ایجاد تکلیف برای این نهاد در تنظیمگری صرافی‌ها و ارائه‌دهندگان خدمات مربوط می‌توان اتخاذ این رویکرد را مثبت ارزیابی کرد. بااین‌حال، درصورت پذیرش رویکرد فوق، همچنان درخصوص ضوابط این اشخاص، سازوکار ثبت و دریافت مجوز آن‌ها مقرر قانونی خاصی وجود ندارد؛ ازاین‌رو ضروری است با تهیه دستورالعملی چهارچوب ایجاد و فعالیت این اشخاص تعیین شود و با شمول ضوابط و الزامات مبارزه با پول‌شویی بر آن‌ها زمینه برای کاهش مخاطرات پول‌شویی دارایی‌های مجازی فراهم شود.

۳. سیاست جنایی در برابر مخاطرات پول‌شویی دارایی‌های مجازی

در عصر حاضر، حوزه فناوری‌های نوین مجازی/سایبری از جمله مهم‌ترین حوزه‌هایی است که توجه قانون‌گذاران و سیاست‌گذاران را جلب کرده است. اتخاذ رویکردی منسجم و سازنده در قبال دارایی‌های مجازی به‌گونه‌ای که به نفی و انفعال نسبت به دارایی‌های مجازی منجر نباشد، ضروری است؛ ازاین‌رو دولت‌ها در تلاش‌اند با رویکردی منطقی و کارا نسبت به مقررگذاری پیرامون دارایی‌های مجازی اقدام کنند.

۱. وزارت صنعت، معدن و تجارت مکلف است با همکاری مرکز، سایر مصادیق مشاغل غیرمالی را با توجه به بند «ث» ماده یک قانون ظرف سه ماه پس از تصویب آیین‌نامه تعیین و در بازه زمانی سه تا پنج سال به‌روزرسانی کند.

سابقه ناکام تقنینی شناسایی رمزارز در قوانین ایران، به قانون قاچاق کالا و ارز در سال ۱۳۹۹ به تبصره ۷ ماده ۲ مکرر الحاقی بازمی گردد. مطابق با این تبصره «تمامی رمزارزها (ارزهای رقومی) در حکم ارز موضوع این قانون هستند و جرایم، تخلفات، ضمانت اجراها و نیز تمامی احکام و مقررات مربوط به ارز در این قانون در مورد آن ها نیز اجرا می شود.» این تبصره در آخرین نسخه اصلاحی توسط مجلس شورای اسلامی حذف شد و تا مدت زمان زیادی، وضعیت قانونی این فناوری مشخص نبود. سرانجام قانون بانک مرکزی جمهوری اسلامی که در جلسه علنی روز سه شنبه ۱۴۰۲/۰۳/۳۰ مجلس شورای اسلامی تصویب شد؛ خط بطلانی بر تمامی شبهات سابق کشید و آشکارا تکلیف قانونی دارایی های مجازی را مشخص کرد و آن ها را به رسمیت شناخت. بند «ض» ماده یک این قانون به تعریف «رمز پول» پرداخته و مقرر می دارد: «رمز پول نوعی پول رقومی دیجیتال رمزنگاری شده است که در بستر پایگاه داده اشتراکی به صورت متمرکز (با محوریت بانک مرکزی) یا غیرمتمرکز ایجاد و به صورت غیرمتمرکز مبادله می شود.» باین حال، مهم تر از شناسایی قانونی، تعیین تکلیف نهاد تنظیمگر در این حوزه است. مطابق ماده ۵۹ این قانون، مسئولیت انحصاری ابلاغ دستورالعمل های مورد نیاز در حوزه نظام های پرداخت، فناوری های نوین مالی مرتبط با ابزارهای پرداخت و رمزپول و همچنین نهادهای فعال در این حوزه ها برعهده بانک مرکزی است. نهادهای فعال در زمینه های یادشده «اشخاص تحت نظارت» بانک مرکزی تلقی شده و تأسیس و فعالیت آن ها منوط به اخذ مجوز از بانک مرکزی است. همچنین این نهادها موظف اند حسب درخواست بانک مرکزی، کلیه اطلاعات و آمار و اسناد خود را به ترتیب مدنظر بانک مرکزی در اختیار آن بانک قرار دهند.

در واقع، وجود ظرفیت های جنایی در دارایی های مجازی و همچنین ماهیت پویای فضای مجازی و نفوذ آن در مناسبات سیاسی و اقتصادی و امنیتی اولویت و توجه قانون گذاران را به مقررگذاری در این حوزه برانگیخته است. براین اساس، سیاست گذاران جنایی در راستای تنظیمگری و مقررات گذاری درخصوص جنبه های مختلف بزهکاری، از جمله بزهکاری فناوری، اقدام به سیاست گذاری در سطح سیاست جنایی تقنینی می کنند که نقشی راهبردی در تعیین برنامه های کلان پیشگیرانه و مقابله ای در برابر پدیده مجرمانه دارد.

۳-۱. پیشگیری از مخاطرات جنایی دارایی های مجازی

با گذشت زمان و با تأثر از پدیده های نوظهور، الزامات عملی و دیدگاه های نظری، مفهوم جرم تغییر پیدا کرده است. وقوع روزافزون ریسک های مختلف در قلمروهای اجتماعی و زیستی، به طرح نظریه جامعه مخاطره آمیز در ادبیات جامعه شناسی از سوی الریش بک منجر شد (Beck, 1992). رویکرد مدیریت ریسک جرم و نظارت بر مجرمان بالقوه و بالفعل به منزله سیاست جنایی نوین با تأکید بر وضعیت پیش جنایی و عوامل خطر جرم نزد بزهکار، در پی نظارت و کنترل بر بزهکاران، بزه دیدگان و آماج جرم از گذر تقویت و حفاظت از آن هاست. این به معنای تغییر بنیادین گفتمان امنیت مدار به جای تأکید اخلاق گراست (Rigakas, 2012, p. 25).

پیش دستی مدنظر در نظم حقوقی جدید، بر این باور است که پیشگیری از وقوع جرایم بزرگ از طریق ترس از مجازات و سیاست بازدارندگی نه تنها کارآمد و مؤثر نبوده و به پیشگیری از وقوع آن ها منجر نخواهد شد، بلکه تنها با کشف و شناسایی اعمال ارتكابی در مراحل نخستین (پیش جرم) و خفه کردن این جرایم در نطفه و اتخاذ اقدامات زودهنگام می توان و باید مانع از تحقق مقاصد مدنظر تصمیم گیران و برنامه ریزان و مرتکبان این گونه جرایم شد (Esmaili, 2016, p. 305).

استفاده روزافزون از دارایی های مجازی با توجه به ظرفیت های مجرمانه آن، راه را برای مرتکبان پولشویی هموار ساخته و در عوض، مجریان عدالت کیفری را در تعقیب آنان ناکام باقی گذاشته است. بی گمان مبارزه مؤثر با جرایم اقتصادی و به ویژه پولشویی نیز جز از رهگذر اقدامات پیشگیرانه محقق نخواهد شد.

ازاین رو، ضروری است به منظور پیشگیری از پولشویی در حوزه دارایی های مجازی، در سطح ملی و فراملی اقداماتی صورت گیرد؛ بنابراین گروه ویژه اقدام مالی به عنوان گروهی فراملی، بنیان توصیه های خود را بر پیشگیری قرار داده است و از کشورها خواسته تا مطابق با ریسک موجود و اولویت های خود، به اجرای توصیه ها بپردازند.

جهانی‌بودن قلمرو ریسک نیاز به همسانی تدابیر ملی را به‌منظور کاهش مخاطرات برجسته می‌سازد و این فهم مشترک را ایجاد می‌کند که بدون همسانی در اتخاذ تدابیر، در عمل هرگونه تدبیر پیشگیرانه‌ای ناقص و ناکارآمد تلقی می‌شود (Khalili Paji, 2022b, p. 253). توصیه شماره یک گروه ویژه با تأکید بر شناسایی و ارزیابی ریسک مربوط به پول‌شویی دارایی‌های مجازی، کشورها را به اتخاذ رویکردی مبتنی بر ریسک راهنمایی کرده است. اتخاذ چنین رویکردی مستلزم تخصیص مرجع یا سازوکاری برای هماهنگی فعالیت‌ها به‌منظور ارزیابی ریسک و اختصاص منابع به‌صورت مؤثر با هدف کاهش ریسک است.

اقتضای رویکرد ریسک‌مدار، توزیع و نظارت بر منابع، متناسب با سطح و ماهیت خطرات شناخته شده است. در واقع، کشورها باید در مواردی که ریسک ارتکاب جرم بیشتر ارزیابی می‌شود برای تقویت اقدامات خود برای مدیریت و کاهش ریسک بکوشند و به‌همین ترتیب، در مواردی که ریسک وقوع جرم کمتر است، اقدامات ساده‌تری را اتخاذ کنند.

یکی از مهم‌ترین ویژگی‌های این رویکرد، پویایی آن است. کشورها برای موفقیت در اتخاذ این رویکرد، باید همواره به ماهیت پویا و تغییرپذیر دارایی‌های مجازی توجه کنند. در واقع یکی از ویژگی‌های رویکرد ریسک‌مدار، پویایی آن است که در طول زمان و متناسب با مخاطرات جدید، منابع خود را مطابق با اولویت پیش‌آمده، بر آن معطوف می‌سازد. در این موارد، نیازی به وجود اطمینان از ریسک نیست؛ بلکه صرف احتمال وقوع جرم کافی است. تکیه بر رویکرد ریسک‌مدار نه تنها سبب ارزیابی واقع‌بینانه‌تری از تهدیدات پول‌شویی می‌شود، بلکه با تمرکز منابع بر فعالیت‌های پرریسک از هدررفت منابع نیز جلوگیری می‌کند.

بدین ترتیب، گروه ویژه اقدام مالی از رهگذر شناسایی ارائه‌دهندگان خدمات دارایی‌های مجازی، آن‌ها را به‌منزله یکی از گروه‌های پرریسک شناسایی کرده و از کشورها خواسته تا الزاماتی که برای پیشگیری از پول‌شویی ضروری است؛ مانند شناسایی مشتری، گزارش عملیات مشکوک، نگهداری سوابق و...، بر این دسته از مشاغل نیز بار شود.

بنابراین به‌منظور مدیریت ریسک ارزهای مجازی راهکاری موقعیت‌مدار، به‌واسطه شناسایی مشارکت‌کنندگان و نگهداری سوابق هویتی و معاملاتی آن‌ها می‌تواند تا حد زیادی راهگشا باشد. بدین ترتیب زمانی که کاربر از مشخص بودن هویت خود آگاه است و می‌داند عملکردش ثبت و ضبط می‌شود، ریسک ارتکاب عمل مجرمانه کاهش می‌یابد. البته این امر منوط به آن است که مشارکت‌کنندگان در فرایند دارایی‌های مجازی در محدوده محیط نظارتی اقدام به عملیات کنند که در این راستا می‌توان به احراز هویت به‌واسطه یک شناسه اجباری هنگام افتتاح حساب و نظارت مستمر بر حساب ارزهای مجازی، به‌ویژه زمانی که تراکنش‌ها از مبلغ معینی فراتر می‌رود، اشاره کرد (Shamloo & Khalili Paji, 2019: 267).

در ایران نیز شناسایی ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی ذیل عنوان مشاغل غیرمالی سبب می‌شود با شمول قوانین و مقررات پول‌شویی، فعالیت‌های مرتبط با این فناوری در چهارچوب برنامه‌های ضدپول‌شویی به عنوان سامانه‌ای جامع رصد و بررسی شود. مطابق با ماده ۷ قانون مبارزه با پول‌شویی اصلاحی ۱۳۹۷، اشخاص مشمول موظف به انجام اقدامات ذیل هستند: الف) احراز هویت و شناسایی مراجعان؛ ب) ارائه گزارش و اسناد و مدارک به مرکز اطلاعات مالی؛ پ) ارائه گزارش عملیات بیش از میزان مصوب شورا یا عملیات مشکوک به مرکز اطلاعات مالی؛ ت) نگهداری سوابق مربوط به شناسایی مشتری و معاملات حداقل به مدت پنج سال؛ ث) تدوین معیارهای کنترل داخلی و آموزش مدیران.

تکالیف فوق تماماً بر ارائه‌دهندگان خدمات دارایی‌های مجازی نیز بار خواهد شد. درحال حاضر، ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی، که وزارت صمت معرفی کرده، به مصادیق موجود مشاغل غیرمالی، در بند «ث» ماده یک اضافه شده و مشمول الزامات ضد پول‌شویی قرار گرفته‌اند. امری که به‌موجب ماده ۵۹ قانون جدید بانک مرکزی نیز با ذکر عبارت «اشخاص تحت نظارت» بر آن تأکید شده است. به این الزامات در آیین‌نامه اجرایی قانون مبارزه با پول‌شویی مصوب ۱۳۹۸ به‌طور مفصل‌تری اشاره شده است. بااین حال، شناسایی ارائه‌دهندگان خدمات دارایی‌های مجازی به‌تنهایی کافی نیست و ضروری است دستورالعملی درخصوص تأسیس، فرایند اخذ مجوز، نظارت

مستمر و برخی الزامات دیگر متناسب با ماهیت فنی دارایی های مجازی صادر شود و همچنین با ایجاد بسترها و سامانه هایی بتوانیم هویت کاربران و زنجیره معاملات را بازشناسیم.

برای نمونه می توان به «دستورالعمل اجرایی تأسیس، فعالیت و نظارت بر صرافی ها» مصوب مرداد ۱۳۹۳ اشاره کرد. در این دستورالعمل به طور خاص، مقررات مربوط به تشکیل و طرز کار و ضمانت اجراهای مرتبط مشخص شده است. براین اساس، پس از مشخص شدن متولی تدوین و تصویب دستورالعمل، باید به دستورالعملی مشابه درخصوص ارائه دهندگان خدمات مربوط به دارایی های مجازی پرداخت. برای مثال، یکی از وظایف موجود به موجب بند «ت» ماده ۷ برای اشخاص موظف، نگهداری سوابق مربوط به شناسایی ارباب رجوع، مالک، سوابق حساب ها، عملیات و معاملات داخلی و خارجی حداقل به مدت پنج سال است. در چنین مواردی باید سازوکار نگهداری مختص ارائه دهندگان خدمات مربوط به دارایی های مجازی مشخص شود.

۲-۳. مداخله کیفری درخصوص مخاطرات جنایی دارایی های مجازی

نباید از نظر دور داشت که اقدامات پیشگیرانه همواره مؤثر نیستند و در صورت عدم مهار جرم در این مرحله، به جایگزینی پاسخ های کیفری نیاز خواهیم داشت. تدابیر واکنشی به تناسب ماهیت متفاوت ریسک و اثرپذیری متفاوت آن ها، طیفی از پاسخ های مدنی، انضباطی و کیفری را دربر می گیرند. بنابراین، پیشگیری باید زمینه ای باشد برای استفاده احتمالی از مجازات. به عبارت دیگر، تأثیر پیشگیری بدون وجود دورنمای مجازات و عدالت کیفری اندک و محدود است؛ بدین سان که اگر پیشگیری شکست بخورد، جامعه باید بداند که خلع سلاح نیست و سلاحی به نام کیفر دارد.

در واقع، اگرچه تدابیر پیشگیرانه تا حد زیادی از وقوع پولشویی جلوگیری می کند؛ اما نمی تواند به طور قطعی مانع از ارتکاب جرم شود؛ ازاین رو همواره ناگزیر از اعمال تدابیر واکنشی خواهیم بود. براین اساس، تدابیر کنشی و واکنشی دو رکن اصلی سیاست جنایی به شمار می روند که هریک بدون دیگری کارایی و تأثیر لازم را نخواهند داشت.

درعین حال، مداخله کیفری از طریق جرم انگاری پیرامون ریسک های دارایی های مجازی از چالش برانگیزترین جنبه مداخلات است. این امر سبب شده دولت ها درک درستی از دارایی های مجازی یا مخاطرات آن نداشته باشند و در نتیجه از حیث مقررگذاری در حوزه جنایی نتوانند ادله توجیهی ارائه دهند.

اما به تدریج و با افزایش کاربرد این فناوری، ابعاد پنهان تجاری آن، که دربردارنده برخی مخاطرات است، آشکار شد. در این مرحله در وهله نخست، مداخله غیرکیفری و تلاش برای تنظیمگری مدنظر قرار گرفت. بااین حال، مجموع ریسک های شناسایی شده، اعم از ریسک های تجاری و جنایی، مداخله کیفری به واسطه شمول برخی قوانین کیفری و جرم انگاری برخی اعمال مرتبط با این فناوری را اجتناب ناپذیر کرد، امری که از آن به عنوان مکمل مداخلات غیرکیفری، یعنی به رسمیت شناختن جنبش جرم انگاری به نام حمایت از حقوقی که جدیداً به رسمیت شناخته شده است، یاد می شود (Delmas Marti, 2018, p. 477).

مطابق با توصیه شماره «۳» گروه ویژه اقدام مالی، کشورها ملزم‌اند پول‌شویی را براساس کنوانسیون وین و کنوانسیون پالرمو جرم‌انگاری کنند. بدین‌سان قانون مبارزه با پول‌شویی اصلاحی ۹۷ در بند «الف» و «ب» و «پ» ماده «۲»^۱ خود به تعریف پول‌شویی پرداخته که با جرم پول‌شویی در ماده «۶» کنوانسیون پالرمو^۲ مطابقت دارد.

براین‌اساس، با به‌رسمیت شناختن دارایی‌های مجازی به‌منزله مال یا کالا می‌توان به این امر قائل بود که هنگامی که اثبات شود این اموال درآمد حاصل از جرم هستند، بدون نیاز به محکومیت دارنده به ارتکاب جرم منشأ، محکومیت وی با وجود سایر شرایط (علم به مجرمانه‌بودن منشأ) برای تحقق عنوان پول‌شویی کفایت می‌کند (Laurent Chiton et al., 2012, p. 17).

علاوه‌بر شمول مقررات پول‌شویی بر رمزارزها، ضروری است نقض مقررات مبارزه با پول‌شویی به‌منزله جرم خاص نیز توجیه شود. براین‌اساس، با قرارگرفتن ارائه‌دهندگان خدمات دارایی‌های مجازی ذیل عنوان مشاغل غیرمالی، الزامات خاص این حوزه و ضمانت اجرای عدم انجام آن‌ها نیز بر این دسته بار خواهد شد.

در واقع، شمول قوانین و مقررات مربوط به پول‌شویی بر دارایی‌های مجازی نه‌تنها از حیث این‌که آن‌ها می‌توانند موضوع جرم پول‌شویی واقع شوند، بر نظام جرم‌انگاری تأثیر نمی‌گذارد، بلکه در این چهارچوب جرم نقض مقررات مبارزه با پول‌شویی درحکم جرایمی خاص نیز مدنظر است. زمانی که رمزارزها و ارائه‌دهندگان خدمات مربوط به رمزارزها مشمول قوانین مبارزه با پول‌شویی قرار گرفتند، الزامات خاص این حوزه و ضمانت اجرای عدم انجام آن‌ها نیز بر این فناوری بار خواهد شد.

برای مثال، فصل پنج از آیین‌نامه مبارزه با پول‌شویی مصوب ۱۳۹۸، در باب شناسایی مشتری، مقرر می‌دارد که اشخاص مشمول مکلف‌اند پیش از برقراری هرگونه تعامل کاری، رویه‌های شناسایی مقتضی را انجام دهند و ریسک تعاملات کاری ارباب رجوع را براساس مقررات مبارزه با پول‌شویی و تأمین مالی تروریسم، طبقه‌بندی کنند و متناسب با ریسک هریک از مشتریان، رویه‌های شناسایی را در سه سطح ساده و معمول و مضاعف به اجرا گذارند.

تبصره ۲ ماده ۵۰ بیان می‌دارد: «اشخاص مشمول مکلف‌اند نگهداری و استمرار در ارائه خدمات پایه را به‌صورت بی‌نام و یا با هویت مجهول یا جعلی و همچنین انجام هرگونه تراکنش و معاملات الکترونیکی بی‌نام یا غیرقابل ردیابی را متوقف کنند.» به نظر می‌رسد در این خصوص باید سازوکاری فراهم شود تا ارائه‌دهندگان خدمات دارایی‌های مجازی بتوانند شناسه دیجیتال طرفین مبادله را با اطلاعات دقیق هویت کاربر تطبیق دهند تا درنتیجه آن، زنجیره نقل و انتقال مبادلات نیز رصد شود.

همچنین اشخاص مشمول مکلف‌اند مطابق با قانون مبارزه با پول‌شویی و آیین‌نامه آن، معاملات و عملیات مشکوک را به مرکز اطلاعات مالی ارائه دهند و سوابق مشتری را برای مدت زمان خاصی نزد خود نگاه دارند. براین‌اساس، اگر یک نهاد مالی یا غیرمالی مظنون شود به این‌که وجوهی از فعالیت‌های مجرمانه به‌دست آمده و ادله منطقی برای ظن خود داشته باشد، باید به‌طور قانونی ملزم شود که در اسرع وقت، ظن خود را به مرکز اطلاعات مالی گزارش دهد. براین‌اساس، کشورها باید اطمینان حاصل کنند که ارائه‌دهندگان خدمات مربوط به رمزارزها، اقدام به چنین گزارشی می‌کنند. انجام‌ندادن هریک از این موارد یا سهل‌انگاری در اجرای آن‌ها، این اشخاص را از ضمانت اجرای خاص تبصره ماده ۷ قانون مبارزه با پول‌شویی اصلاحی ۱۳۹۷ برخوردار خواهد کرد.

۱. ماده «۲» بیان می‌دارد: «پول‌شویی عبارت است از: الف- تحصیل، تملک، نگهداری یا استفاده از عواید حاصل از ارتکاب جرایم با علم به منشأ مجرمانه آن‌ها. ب- تبدیل، مبادله یا انتقال عوایدی به‌منظور پنهان یا کتمان‌کردن منشأ مجرمانه آن با علم به این‌که به‌طور مستقیم یا غیرمستقیم از ارتکاب جرم به‌دست آمده یا کمک به مرتکب جرم منشأ به‌نحوی که وی مشمول آثار و تبعات قانونی ارتکاب آن جرم نشود. پ- پنهان یا کتمان‌کردن منشأ، منبع، محل، نقل و انتقال، جابه‌جایی یا مالکیت عوایدی که به‌طور مستقیم یا غیرمستقیم درنتیجه جرم تحصیل شده باشد.»
۲. ماده ۶ کنوانسیون پالرمو عبارت است از: ۱. تبدیل یا انتقال اموال به‌منظور مخفی کردن یا تغییر ظاهر منشأ غیرقانونی آنها یا کمک به شخصی که در ارتکاب جرم منشأ مشارکت داشته است، به منظور فرار از عواقب قانونی عملش با علم به اینکه اموال مزبور عواید حاصل از جرم است؛ ۲. مخفی کردن یا تغییر ظاهر، ماهیت، منشأ، محب، موقعیت، جابه‌جایی یا مالکیت یا حقوق متعلق به اموال با آگاهی از آنکه اموال مزبور عواید حاصل از جرم است.

نتیجه گیری

دارایی های مجازی از چند بُعد در نظام عدالت کیفری قابلیت بررسی دارد. این امر زمانی که قرار است در چهارچوب مفهوم سیاست جنایی بررسی شود از گستره درخور ملاحظه ای برخوردار خواهد شد. در این راستا، باید دید که در دو حوزه تدابیر کنشی / پیشینی و تدابیر واکنشی / پسینی با توجه به ظرفیت های جنایی دارایی های مجازی چه ترکیبی از سیاست جنایی باید مورد توجه قرار گیرد. امری که پیش شرط آن شناسایی دقیق نیم رخ جنایی و ظرفیت های مجرمانه این فناوری است تا در پرتو آن، مجموعه مداخلات اثرگذار سیاست جنایی از گذر ترکیبی از مداخلات کیفری و غیرکیفری و پیشگیرانه مدنظر قرار گیرد.

اول در حوزه تدابیر واکنشی / پسینی ابتدا با ترسیم نیم رخ جنایی و تعیین ظرفیت های مجرمانه دارایی های مجازی باید بررسی کرد که ضروری است تدابیر و اقدامات این حوزه بر چه مبنایی استوار شود. آیا این حوزه نیازمند مداخلات کیفری است یا صرف تنظیمگری حقوقی و پاسخ گذاری های غیرکیفری کفایت می کند؟ یا باید ترکیبی از تدابیر کیفری و غیرکیفری را مدنظر قرار داد؟

بی تردید این فضا از حیث کیفری در بر دارنده ظرفیت های احتمالی و واقعی در ایجاد تغییر کمی و کیفی و مصداقی و مفهومی جرایم است؛ از این رو، پاسخ به پرسش های مهمی همچون این که دارایی های مجازی چه تغییراتی در کمیت و کیفیت جرائم ایجاد می کند؟ میزان ارتکاب جرم با استفاده از این فناوری تا چه اندازه افزایش خواهد داشت؟ چه انواع جدیدی از جرم، که از نظر ماهوی با جرائم فعلی مرتبط با اینترنت، هوش مصنوعی و ... متفاوت اند، به وجود خواهد آمد؟ آیا جرائمی که در دنیای واقعی قابل ارتکاب هستند، با استفاده از دارایی های مجازی نیز قابلیت اجرا دارند یا مداخله کیفری در این فضا مستلزم جرم انگاری گونه های جدیدی از رفتارهای خاص این فضا است؟ بخش مهمی از توجیه مداخله کیفری در این زمینه و گونه های آن است. همچنین، پاسخ گذاری کیفری در این حوزه و شناسایی ضمانت اجرای کیفری نیز از اهمیت برخوردار است. پرسش هایی مانند کارآمدی مجازات های موجود یا ضرورت اتخاذ رویکردهای نوین پاسخ گذاری کیفری بر مبنای مؤلفه های بنیادین دارایی های مجازی از مهم ترین پرسش هایی است که در کار بست بسته های سیاست جنایی بر مبنای ترکیبی از تدابیر و اقدامات از اهمیت بسیاری برخوردار است که در بعد واکنش کیفری قابل بررسی است. با این حال، ضرورت مداخله کیفری نافی لزوم اتخاذ پاسخ های غیرکیفری در چهارچوب نظام تنظیمگری این فناوری نیست. بخش درخور توجهی از تنظیم روابط درخصوص این فناوری می تواند بر مبنای اقدامات صنفی، اداری و مدنی استوار شود. امری که اصل کمینه حقوق کیفری نیز مؤید آن است.

دوم در حوزه اقدامات کنشی / پیشینی نیز ظرفیت های جنایی دارایی های مجازی و کارکردهای مجرمانه آن ممکن است اثرگذار باشد. در این چهارچوب نیز ترکیبی از تدابیر و اقدامات سیاست جنایی قابلیت طرح دارد. از یک سو، تدابیر پیشگیرانه بر محور آموزه های جرم شناسی پیشگیری در سطح پیشگیری موقعیت مدار و اجتماعی در مهار جرایم احتمالی با این فناوری اثرگذار است و از سوی دیگر، تدابیر حقوقی و کیفری پیشگیرنده از گذر جرم انگاری های منطبق با عدالت کیفری پیش دستانه می تواند با تحقق بازدارندگی به واسطه توسعه جرم انگاری جرایم مانع و قراردادن ضمانت اجرای حقوقی - کیفری برای تدابیر پیشگیرانه زمینه ساز مهار جرایم مهم این حوزه باشد. در واقع، در حوزه اقدامات کنشی / پیشینی نیز با اتخاذ بسته ای ترکیبی از تدابیر سیاست جنایی می توان با مدنظر قراردادن مفهوم پیشگیری جرم شناختی و بازدارندگی، با استفاده از تدابیر کیفری و غیرکیفری، به هدف مهار بزه کاری و مدیریت ریسک جرم این فناوری دست یافت. بدین سان، در صورتی که رویکرد سیاست جنایی در برابر مخاطرات پول شویی دارایی های مجازی موارد مذکور را مدنظر قرار دهد، می توان به نتایج مفید ناشی از اجرای آن خوش بین بود.

منابع

- اس.سیمپسون، سالی، ویزبرد، دیوید (۱۳۹۳). جرم‌شناسی جرایم یقه‌سفیدان. ترجمه حمیدرضا دانش ناری و آزاده صادقی، تهران: انتشارات مجد.
- اسماعیلی، محمد (۱۳۹۶). عدالت پیشگیرنده: مهار جرم در بستر نظام حقوقی. مجله مطالعات حقوق کیفری و جرم‌شناسی، ۴(۲)، ۲۹۷-۳۲۶. <https://doi.org/10.22059/JQCLCS.2018.239944.1232>
- امامی، سیدحسین (۱۳۸۷). حقوق مدنی. ج ۱، تهران: کتابفروشی اسلامیه.
- پاک‌نهاد، امیر (۱۳۹۴). سیاست جنایی ریسک‌مدار. تهران: میزان.
- جزایری، مینا (۱۳۸۲). جرم پول‌شویی به‌عنوان یک جرم مستقل. مجموعه‌سخنرانی‌ها و مقالات همایش بین‌المللی مبارزه با پول‌شویی. تهران: نشر وفاق.
- خلیلی پاجی، عارف (۱۳۹۸). امکان‌سنجی تأمین مالی تروریسم در پرتو ارزش‌های مجازی. مجموعه‌مقالات همایش بین‌المللی ابعاد حقوقی - جرم‌شناختی تروریسم. تهران: انتشارات دانشگاه علامه طباطبائی.
- خلیلی پاجی، عارف (۱۴۰۱). ارزش‌های مجازی؛ جهانی‌شدن بزهکاری و سیاست‌جنایی. تهران: میزان.
- خلیلی پاجی، عارف (۱۴۰۰). ارزیابی رویکرد پیشگیری ریسک‌مدار از مخاطرات جنایی ارزش‌های مجازی. دوفصل‌نامه تخصصی حقوق قراردادها و فناوری‌های نوین، ۲(۳)، ۲۴۵-۲۶۷. [HTTPS://DOI.ORG/10.22133/CLJ.2021.313012.1066](https://doi.org/10.22133/CLJ.2021.313012.1066)
- دل‌ماس مارتی، می‌ری (۱۳۹۸). نظام‌های بزرگ سیاست جنایی. ترجمه علی حسین نجفی ابرندآبادی. تهران: میزان.
- ریگاکاس، جورج اس. (۱۳۹۲). جامعه خطر و جرم‌شناسی سنجشی: جنبه‌هایی برای یک گفتمان انتقادی. ترجمه افشین عبداللهی. فصل‌نامه بین‌المللی پلیس، ۴(۱۳)، ۱۵۷-۱۷۲.
- سلیمانی‌پور، محمد مهدی، سلطانی‌نژاد، حامد و پورمطهر، مهدی (۱۳۹۶). بررسی فقهی پول مجازی. فصل‌نامه تحقیقات مالی اسلامی، ۶(۲)، ۱۶۷-۱۹۲. <https://doi.org/10.30497/IFR.2017.2002>
- سیاه‌بیدی کرمانشاهی، سعید و ثالث موید، احمدعلی (۱۳۹۶). حقوق کیفری اقتصادی پول‌شویی. تهران: میزان.
- شاملو، باقر و خلیلی پاجی، عارف (۱۳۹۹). سیاست‌گذاری جنایی ریسک‌مدار در برابر فناوری ارزش‌های مجازی، فصل‌نامه مجلس و راهبرد، ۲۷(۱۰۳)، ۲۴۷-۲۷۸.
- صفاری، علی، صابری، راضیه و خلیلی پاجی، عارف (۱۳۹۹). کارکردهای مجرمانه ارزش‌های مجازی: تحلیل جرم‌شناختی و راهکارهای پیشگیرانه. دوفصل‌نامه دانشنامه حقوق اقتصادی، ۲۷(۱۸)، ۲۵۰-۲۲۳. <https://doi.org/10.22067/lowecon.2020.48879.0>
- اسکات، پل آلن، مک‌دونل، جان، لارنت چیتن، پیترو و موس، سدريک و مندرپز، امیل (۱۳۹۲). پیشگیری از پول‌شویی و تأمین مالی تروریسم؛ راهنمای عملی برای ناظران بانکی. ترجمه مریم کشتکار. تهران: تاش.
- مافی، همایون و رامشی، میثم (۱۴۰۱). ماهیت حقوقی دارایی مجازی. فصل‌نامه تحقیقات حقوقی دانشکده حقوق دانشگاه شهیدبهبشتی. ۲۶(۱۰۳)، ۱۵۷-۱۸۰. <https://doi.org/10.52547/JLR.2022.228887.2319>

- نوری، فاطمه، کوشا، ابوطالب و خادمان، محمود (۱۴۰۰). شناسایی ماهیت حقوقی رمزارزها با تحلیل ساختاری آنها در نظام حقوقی ایران. *مجله حقوقی دادگستری*، ۸۵(۱۱۵)، ۳۷۲-۳۴۹. <https://doi.org/10.22106/rlj.2021.137039.3698>
- Beck, U. (1992). *Risk society: Towards a new modernity* (Vol. 17). sage.
- Bershidsky, L. (2017). Bitcoin and the Value of Financial Freedom. Bloomberg. December, 20. at <https://www.Bloomberg.com/view/articles/2017-12-20/bitcoin-and-the-value-of-financial-freedom>
- Dawood, O. A., Hammadi, O. I., & Mohammed, F. M. (2019). Secure symmetric block cipher design for encrypting the bitcoin wallets in cryptocurrencies applications. *J. Comput. Sci*, 15(5), 758-768. <https://doi.org/10.3844/jcssp.2019.758.768>
- FATF (2019). Guidance for a Risk-Based Approach for Virtual Assets and Virtual Asset Service Providers. Archived at :<https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf>
- FATF (2014). Virtual Currencies Key Definitions and Potential AML/CFT Risks. <http://www.fatfgafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>
- FATF (2015). Guidance for A Risk-Based Approach Guidance for A Risk-Based Approach Virtual Currencies: <http://www.fatfgafi.org/media/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>
- Hacker, P., & Thomale, C. (2018). Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU financial law. *European Company and Financial Law Review*, 15(4), 645-696. <https://doi.org/10.1515/ecfr-2018-0021>
- Kethineni, S., Cao, Y., & Dodge, C. (2018). Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes. *American Journal of Criminal Justice*, 43, 141-157. <https://doi.org/10.1007/s12103-017-9394-6>
- Kotane, I. (2018). Concept of Virtual Currencies in Modern Economies. *Latgale National Economy Research*, 1(10), 63-76. <https://doi.org/10.17770/lner2018vol1.10.3605>
- Ritzer, G. (2007). *The Globalization of Nothing* Thousand Oaks. Forge Press.
- Rotman, E. (2001). The Globalization of Criminal Violence. *Cornell Journal of Law and Public Policy*, 10(1), 1-42.
- Viano, E. C. (2008). Globalization and transnational crime: New links, new perspectives. *Int'l Annals Criminology*, 46, 81. https://doi.org/10.1007/978-1-4939-2471-4_1

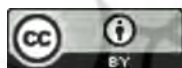
[In Persian]

- Delmas Marti, M. (2018). *The Great Systems of Criminal Politics*. translated by Ali Hossein Najafi Abrandabadi. second edition. Tehran: Mizan.
- Emami, S. H. (2008). *Civil Rights* (Vol. 1). Tehran: Islamia Bookstore.
- Smaili, M. (2016). Proactive justice: Curbing crime in the framework of the legal system. *Journal of Criminal Law and Criminology Studies*, 4(2), 297-326. <https://doi.org/10.22059/JQCLCS.2018.239944.1232>
- Jazayeri, M. (2012). *The crime of money laundering as an independent crime: A collection of lectures and articles of the international conference on combating money laundering* (1st ed.). Tehran: Vefagh Publications.
- Khalili Paji, A. (2021). Evaluation of the risk-based approach to prevent the criminal risks of virtual currencies. *Specialized Two-Quarterly Journal of Contract Law and New Technologies*, 2(3), 245- 267. <https://doi.org/10.22133/CLJ.2021.313012.1066>
- Khalili Paji, A. (2022a). Evaluation of a Risk-Based Preventive Approach to the Criminal Risks of Virtual Currencies. *Contracts and New Technologies Law*, 2(3), 245-267. <https://doi.org/10.22133/CLJ.2021.313012.1066>
- Khalili Paji, A. (2022b). *Virtual Currencies: The Globalization of Crime and Criminal Policy* (in Persian). Tehran: Mizan.
- Laurent Chatain, P., McDowell, J., Mousset, C., Allan Schott, P., Does de Willebois, E. (2012). *Prevention of Money Laundering and Terrorist Financing: A practical guide for bank supervisors*. (M. Keshtkar, Trans.). Tehran: Tash.
- Mafi, H., & Ramashi, M. (2023). The Legal Nature of Virtual Assets. *Law Research Journal of Shahid Beheshti University Law School*, 26(103), 157-180. <https://doi.org/10.52547/JLR.2022.228887.2319>
- Nouri, F., Kosha, A., & Khadiman, M. (2021). Identifying the legal nature of cryptocurrencies with their structural analysis in Iran's legal system. *Judiciary Journal*, 85(115), 349-372. <https://doi.org/10.22106/jlj.2021.137039.3698>
- Pak Nahad, A. (2014). *Risk-based criminal policy* (2nd ed.). Tehran: Mizan.
- Rigakas, G. S. (2012). Risk Society and Quantitative Criminology: Aspects for a Critical Discourse (translated by A. Abdullahi). *International Police Quarterly*, 4(13), 157- 172.
- S. Simpson, S., & Weisburd, D. (2009). *Criminology of white-collar crimes* (translated by H. R. Danesh-Nari & A. Sadeghi, 2013). Tehran: Majd Publications.
- Safari, A., Saberi, R., & Khalili Paji, A. (2019). Criminal functions of virtual currencies: Criminological analysis and preventive solutions. *Bi-quarterly encyclopedia of economic law*, 27(18), 223-250. <https://doi.org/10.22067/lowecon.2020.48879.0>

- Shamloo, B., & Khalili Paji, A. (Autumn 2019). Risk-based criminal policy against virtual currency technology. *Majlis and Strategy Quarterly*, 27(103), 247-278.
- Siah-Bidi Kermanshahi, S., & Sales moyyed, A. A. (2016). *Economic Criminal Law of Money Laundering* (1st ed.). Tehran: Mizan Publications.
- Soleimanipour, M. M., Soltaninejad, H., & Pourmathar, M. (2016). Jurisprudence review of virtual money. *Islamic Financial Research Quarterly*, 6(2), 167-192. <https://doi.org/10.30497/IFR.2017.2002>

COPYRIGHTS

©2025 by the authors. Published by University of Science and Culture. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY 4.0) <https://creativecommons.org/licenses/by/4.0/>



پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی