دوفصلنامهٔ تخصصی حقوق قراردادها و فناوری‌های نوین، دورهٔ دوم، شمارهٔ ۳، بهار و تابستان ۱۴۰۰، صفحهٔ ۲۴۷-۲۶۵

ارزیابی رویکرد پیشگیری ریسک‌مدار از مخاطرات جنایی ارزهای مجازی

عارف خلیلی پاجی[۱]

تاریخ دریافت: ۱۴۰۰/۸/۱۰ تاریخ پذیرش: ۱۴۰۰/۹/۱۰

نوع مقاله: پژوهشی

چکیده

پدیده‌های فناورانه، با وجود ایجاد سهولت در زندگی بشر، دربردارندهٔ چالش‌هایی از ابعاد اقتصادی و اجتماعی‌اند. ازاین‌رو، کنکاش پیرامون چالش‌ها و یافتن راه‌هایی برای کاهش مخاطرات احتمالی و واقعی آن‌ها همواره یکی از پرسش‌های اساسی بشر بوده است. نمونهٔ بارز پدیده‌های فناورانه ارز مجازی است که در کنار تمامی مزایا و کارکردهای مثبت، بسترساز تحول و نوآوری در ارتکاب برخی جرایم شده است. امری که با گسترش محیط مجرمانه به فراتر از مرزهای جغرافیاییِ هر کشور، فرایند جهانی‌شدن بزهکاری را تسریع کرده و تأثیرات چشمگیری بر آن داشته است. ازاین‌رو، کنش‌گران نظام عدالت کیفری، بنابر وظایف ذاتی خود، باید با تنظیم نظام پاسخ‌گذاری مطلوب، تا حد امکان به مهار ظرفیت‌های جنایی این فناوری بپردازند. بی‌تردید، مانند سایر حوزه‌های پاسخ‌گذاری در برابر جرم، در این زمینه نیز پاسخ‌گذاری کنشی در اولویت اقدام قرار دارد؛ امری که مورد توجه جدی گروه ویژهٔ اقدام مالی اف‌ای‌تی‌اف نیز قرار گرفته است. این گروه، در چارچوب رویکرد ریسک‌مدار خود در برابر پولشویی، بر گزینش رویکرد پیشگیری ریسک‌مدار از مخاطرات ارزهای مجازی تأکید دارد. امری که در پی آن است تا با شمول الزامات پیشگیری از پولشویی بر ارزهای مجازی، رویکرد پیشگیری ریسک‌مدار را بر این فناوری تسری دهد. بااین‌حال، ارزیابی رویکرد اخیر حاکی از آن است که صرف اتکا به آن فاقد

۱. دانش‌آموختهٔ دکتری حقوق کیفری و جرم‌شناسی، دانشکدهٔ حقوق دانشگاه شهید بهشتی؛ arefkhalilipaji@gmail.com

اثربخشی لازم بوده و وجود برخی چالش‌ها مانع توفیق کامل آن شده است. امری که در پژوهش حاضر با نگاهی توصیفی و تحلیلی مورد ارزیابی قرار می‌گیرد تا ابعاد گوناگون آن آشکار شود.
واژگان کلیدی: ارزهای مجازی، پیشگیری ریسک‌مدار، گروه ویژهٔ اقدام مالی

مقدمه

پدیدهٔ مجرمانه همواره یکی از مهم‌ترین دغدغه‌های جوامع در تاریخ حیات بشری بوده و بخشی از تمرکز جوامع در دوره‌های گوناگون بر تلاش برای مهارکردن آن بوده است. امری که در آغاز بر محور رویکردهای واکنشی و کیفری استقرار می‌یافت و کیفر، به‌منزلهٔ تنها پاسخ به بزهکار در نگاهی پسینی مدنظر قرار می‌گرفت. با گذشت زمان ضعف‌ها، ناکارآمدی و عدم کفایت این رویکرد، انتقاداتی را برانگیخت و نظر کنش‌گران نظام عدالت کیفری را به سوی اتخاذ تدابیر کنشی/ پیشگیرانه جلب کرد. در این چارچوب، ضرورت اتخاذ تدابیر پیشینی برای اجتناب از هزینه‌های گزاف ناشی از ارتکاب جرم و آثار مخرب دیگر جرم بر اجتماع، به تهیه و تدوین برنامه‌ها و سیاست‌هایی با اهداف پیشگیری از جرم منجر شد تا در پرتو آن تا حد امکان رویکردی منسجم و منطبق بر نیازهای روز جوامع شکل گیرد. جوامعی که از گذر صنعتی‌شدن درگیر طیف وسیعی از مخاطرات‌اند؛ مخاطراتی که غالباً از تغییر سبک زندگی نشئت می‌گیرد و توسعهٔ فناوری سبب گسترش و ایجاد تنوع در آن‌ها شده است. امری که به تعبیر برخی اندیشمندان به شکل‌دهی «جوامع مخاطره‌آمیز» منجر شده است (بک، ۱۳۸۸).

در این چارچوب، پیشگیری از بزهکاری نیز جهت خاصی یافته است و تلاش برای کاهش مخاطرات احتمالی که ممکن است به بزهکاری یا بزه‌دیدگی منجر شود به اولویت راهبردی رویکردهای پیشگیرانه تبدیل شده است. در این دیدگاه، پیشگیری اجتماعی از اولویت خارج می‌شود و با اتخاذ رویکرد ریسک‌مدار سیاست جنایی، غالباً از ابزارهای پیشگیری فنی–وضعی متناسب با منطق اصل هدفمندی مدیریت ریسک استفاده می‌شود. امری که در دههٔ ۱۹۹۰، به‌موجب شکل‌گیری گفتمان «پیشگیری ریسک‌مدار»،[۱] سرآغاز تحولی در گفتمان پیشگیری از جرم شد که در قلمرو جرم‌شناسی آغاز به رشد کرد

۱. Risk–Based Prevention

(Farrington, 2002, p.10-16). ایدهٔ این رویکرد وام‌دار بخش سلامت عمومی است که در مقابله با برخی بیماری‌ها مورد توجه قرار گرفت. اندیشهٔ محوری این گفتمان بر این گزاره استوار است که باید عوامل اساسی ریسک ارتکابِ جرم شناسایی و با اتخاذ روش‌های مشخص خنثی شوند (نجفی ابرندآبادی، ۱۳۸۸). در این چارچوب، عامل ریسک متغیری است که از احتمال بالای وقوع جرم خبر می‌دهد؛ امری که یا درحال حاضر وجود دارد یا احتمال به‌وجودآمدن آن هست (Loeber et al., 2008, p.99).

از جمله مخاطراتی که در این ساختار از حیث پیشگیرانه مورد توجه قرار می‌گیرد، مخاطرات جنایی ارزهای مجازی[1] است. ارزهای مجازی ابزار نوین فناورانه‌ای است که ریسک‌های جدید و متنوعی دارد. ازاین‌رو، مانند سایر مخاطرات، تلاش برای پیشگیری

۱. ارز مجازی عنوانی عام برای برخی ابزارهای فناورانه با ویژگی‌ها و کارکردهای پول یا ابزارهای مبادله است. برخی از مصادیق ارزهای مجازی را می‌توان ارزهای مبتنی بر فناوری رمزنگاری دانست که با عناوینی چون «رمزارز (Crypto-Currency)»، «ارز رمزپایه» و «رمزینه ارز» در نوشتگان فارسی به‌کار می‌رود. این فناوری برآمده از فضای مجازی است و در بستر این فضا معنا می‌یابد. ارزهای مجازی در یک دسته‌بندی و بر مبنای قابلیت تبدیل‌پذیری به سایر ارزهای مجازی یا پول‌های ملی/ فیات (Fiat Currency) به دو دستهٔ «قابل تبدیل» و «غیرقابل تبدیل» تقسیم می‌شوند. ارزهای مجازی غیرقابل تبدیل، به لحاظ سامانه‌ای، امکانی برای تبدیل به سایر ارزها یا پول‌ها ندارند. نمونهٔ بارز این‌گونه از ارزها پول‌ها یا سکه‌هایی است که در بازی‌های رایانه‌ای یا موبایلی کسب می‌شوند و فقط امکان هزینه‌شدن در همان بازی را دارند و اصطلاحاً به آن‌ها «سکهٔ بازی Game coins» گفته می‌شود. این ارزها صرفاً به‌صورت متمرکز و در بستر همان فضایِ به‌خصوص قابلیت استفاده دارند. بر این اساس، یک نهاد مرکزی (برای مثال سازندهٔ بازی) برای طی مراحل بازی اقدام به انتشار این ارزها می‌کند و دفتر کل مشتمل بر اطلاعات آن‌ها، نیز نزد آن نهاد نگه‌داری می‌شود. ای-گُلد (E-Gold) معروف‌ترین مثال از این دسته ارزها است. بااین‌حال، با توجه به گسترش اقبال عمومی از یک بازی رایانه‌ای و اهمیت سکه‌ها و پول‌های کسب شده در آن برای طی مراحل، همواره امکان خرید و فروش این امتیازات در خارج از فضای بازی وجود دارد. این امر نیز تغییری در ماهیت این‌گونه ارزها ایجاد نمی‌کند و هم‌چنان این موارد به عنوان ارزهای مجازی غیرقابل تبدیل شناخته می‌شوند ("Virtual Currencies, Guidance for A Risk-Based Approach," FATF, Paris, Last Accessed on 16, December, 2020, https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf). در مقابلِ ارز مجازی غیرقابل تبدیل، ارز مجازی «قابل تبدیل» قرار می‌گیرد. این‌گونه ارزها امکان تبدیل به پول‌های ملی و برعکس و نیز قابلیت خرید کالا و خدمات حقیقی یا مجازی را دارند. این دسته از ارزهای مجازی نمونه‌ای بارز و پیشرو از پول‌های مجازی‌اند که خود به دو دستهٔ متمرکز و غیرمتمرکز تقسیم می‌شوند (Kotane, 2018, p. 63). منظور از ارز مجازی قابل‌تبدیلِ متمرکز آن است که انتشار و کنترل ارز توسط نهادی مرکزی صورت می‌گیرد. بر این اساس، سازنده و کنترل‌کنندهٔ ارز مشخص است و طبیعتاً آن ارز براساس پروتکل‌های سازنده یا سازندگان قابلیت استفاده دارد. اگر ایجاد و مدیریت این دسته از ارزها بر اساس رمزنگاری صورت پذیرد، آن‌ها نیز در زمرهٔ رمزارزها قرار می‌گیرند. در مقابل، ارز مجازیِ قابل‌تبدیلِ غیرمتمرکز اشاره به ارزی دارد که انتشار و کنترل آن توسط یک نهاد مرکزی صورت نمی‌گیرد، بلکه چرخش آن ارز توسط کلیهٔ افراد حاضر در شبکه با به‌کارگیری علم رمزگذاری خلق و مدیریت می‌شود. ازاین‌رو، به ارز مجازی قابل‌تبدیلِ غیرمتمرکز «رمزینه ارز» یا «ارز رمزنگاری‌شده» یا «رمزارز» گفته می‌شود؛ زیرا تمام فرایندهای آن، یعنی انتشار/ خلق، مبادله و تأیید تراکنش‌ها، قابلیت انجام توسط تک‌تک کاربران بر اساس الگوریتم‌های ریاضی و رمزنگاری را دارد.

از تحقق بزه بر مبنای آن در اولویت سیاست‌گذاران قرار دارد؛ زیرا ویژگی‌های منحصربه‌فرد این فناوری کشف جرم یا شناسایی بزهکار را بسیار سخت خواهد کرد؛ به‌همین دلیل تمرکز اولیه تا حد امکان باید بر پیشگیری از ارتکاب جرم واقع شود.

بی‌تردید گروه ویژهٔ اقدام مالی اف‌ای‌تی‌اف (FATF) برجسته‌ترین جایگاه را در ترویج گفتمان پیشگیری ریسک‌مدار از مخاطرات جنایی ارزهای مجازی دارد. در ژوئن ۲۰۱۹، این گروه با انتشار سندی[۱] تبیین کرد که چگونه الزامات این نهاد باید در رابطه با دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن اعمال شود، تا این فناوری نیز در چارچوب رویکرد ریسک‌مدار سیاست جنایی در برابرِ پولشویی قرار گیرد. در این راستا، اولویت موردتأکیدِ این گروه، اقدامات پیشگیرانه است که در منطق رویکرد ریسک‌مدار به کشورها ارائه می‌شود.

با وجود این، اتخاذ تدابیر پیشگیرانه در برابر مخاطرات ارزهای مجازی آسان نیست. زیرا نخست، تحول در این فناوری و پویایی آن همواره به شکل‌گیری ابهامات جدی در هرگونه سیاست‌گذاری پیرامون آن منجر می‌شود. توسعهٔ کمّی و کیفی ارزهای مجازی و افزایش شمار ابزارهای فناورانهٔ مرتبط[۲] با آن موجب تنوع در به‌کارگیری و خلاقیت در شگردهای بزهکارانه بر مبنای آن شده است. دوم، سیاست‌گذاری در این عرصه غالباً زمان‌بر و منفعلانه و همراه با چالش‌های عینی است و هم‌زمان با تحولات فنی پیش نمی‌رود. سوم، اتخاذ هر رویکرد پیشگیرانه‌ای مستلزم شناسایی و تقویت سیاست‌های

---

۱. See “Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers,” FATF, Paris, Rights, Last Accessed on 16, December, 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

۲. بیش از ۵۱۰۰ دارایی رمزنگاری‌شده با بازاری به ارزش ۲۵۰میلیون دلار در آغاز سال ۲۰۲۰ شناسایی شده است (Available at: “coin market cap,” Last Accessed on 16, December, 2020, https://coinmarketcap.com) که قانونی یا غیرقانونی وجود دارند. بیشتر فعالیت‌های قانونی درخصوص دارایی‌های مجازی، به‌ویژه درخصوص رمزارزها، در صرافی‌های رمزارزی صورت می‌پذیرد که هدف عمده کسب سود با سرمایه‌گذاری در چنین دارایی‌هایی است. فعالیت‌های غیرقانونی غالباً با خرید و فروش کالا یا خدمات غیرقانونی در بسترِ رویِ تاریک وب، یعنی دارک نت Dark Net ، با ارتکاب اعمالی چون پولشویی، جلوگیری از کنترل سرمایه با اقداماتی چون فرار مالیاتی، حملات باج‌افزاری و سرقت محقق می‌شود. در موارد اخیر، رمزارزها بیشتر به‌عنوان ابزار پرداخت به‌کار می‌روند. نکتهٔ قابل توجه این است که تقریباً نیمی از کل معاملات سالانهٔ بیت‌کوین، مطابق تحقیقات گروهی از محققان که از الگوریتم خاصی برای تحلیل داده‌های معاملات استفاده کرده‌اند، مربوط به فعالیت‌های غیرقانونی است. ازآنجاکه بازار رمزارزها هنوز هم با ارزشی حدود ۱۵۹میلیون دلار، یعنی حدود ۶۳ درصد، تحت سلطهٔ بیت‌کوین قرار دارد، این نکته بسیار قابل توجه است.

کارآمد و حذف اقدامات بی‌اثر است. ازاین‌رو، اگرچه جرم‌شناسی پیشگیری و به‌خصوص گونهٔ پیشگیری وضعی را می‌توان یکی از تحول‌پذیرترین شاخه‌های جرم‌شناسی دانست(Clarke, 2005, p.79)، اما باید توجه داشت که در چارچوب مدیریت ریسک پیوند اصل هدفمندی و اولویت‌بندی با اقدامات وضعی به علت این‌که مخاطرات با سرعتی شگرف، روزآمد و متحول می‌شوند و تغییر در نوع و آماج اقدامات با چنین سرعتی ممکن نیست، کار پیچیده‌ای خواهد بود.

بر این اساس، پرسشی که باید به آن پاسخ داده شود این است که آیا اساساً رویکرد پیشگیری ریسک‌مدار در برابر مخاطرات ارزهای مجازی در مدل ارائه‌شدهٔ گروه ویژهٔ اقدام مالی را می‌توان رویکردی مؤثر و کارآمد تلقی کرد؟ این امر مستلزم آن است که ابتدا منطق پیشگیری ریسک‌مدار در برابر ارزهای مجازی مورد بازخوانی قرار گیرد و سپس با توجه به برخی واقعیت‌ها علل عدم توفیق کامل آن بررسی شود. امری که در پژوهش حاضر با روشی توصیفی و تحلیلی و با استفاده از منابع موجود کتابخانه‌ای و اینترنتی مورد توجه قرار گرفته است. ازاین‌رو، در قسمت اول از مقالهٔ حاضر، منطق پیشگیری ریسک‌مدار در برابر مخاطرات ارزهای مجازی و در قسمت دوم، چالش‌های مؤثر بر اثربخشی رویکرد پیشگیری ریسک‌مدار از مخاطرات ارزهای مجازی ارزیابی و تحلیل شده است.

۱. منطق پیشگیری ریسک‌مدار در برابر مخاطرات ارزهای مجازی

منطق رویکرد ریسک‌مدار بر سه مؤلفهٔ اساسی استوار است. نخست، احتمالی‌بودن ریسک؛ دوم، جهانی‌بودن ریسک و سوم، قابل ارزیابی بودن ریسک. بی‌تردید، خاستگاه مدیریت ریسک الگوهای آماری است و مفهوم احتمال در این چارچوب نقشی برجسته دارد. پیوند ریسک و احتمال پیوندی ناگسستنی است، به‌طوری‌که می‌توان احتمالی‌بودن را ویژگی ذاتی ریسک یاد کرد. امری که با شدت‌گرفتن امنیت‌گرایی و تمایل جامعه به برقراری امنیت و تأکید بر عبارت «ریسک‌های بالقوه»، تأکید بیشتر بر احتمالی‌بودن ریسک را اقتضا دارد (قناد و اکبری، ۱۳۹۶، ص ۳۹). آینده‌محوری که در نهاد احتمال قرار دارد به نشانه‌گذاری ریسک با احتمال زیاد یا احتمال کم منجر می‌شود که در هرحال، نمایان‌گر

پیوند ریسک و احتمال است. امری که به‌عنوان مشخصهٔ پست‌مدرنیته در بیان ویژگی‌های ریسک شناخته می‌شود و آن را با مفهوم جهانی‌شدن نیز پیوند زده است.

جهانی‌شدن، با وجود برخورداری از مزایای بی‌شمار، پیامدهای منفی نیز در پی داشته است. امری که سبب شده عموم مردم ریسک‌ها را تجربه کنند. اگرچه سطح تجربه، بسته‌به عوامل گوناگون و میزان فقر و برخورداری افراد، متفاوت است، برخی ریسک‌ها جدا از چنین دسته‌بندی‌هایی با گسترهٔ جهانی بر عموم مردم تأثیرگذارند (Kemshall, 2003, p. 46). ازاین‌رو، گستردگی را می‌توان خاصیت ریسک دانست که دامنهٔ شمول آن را فراتر از مرزها و جدا از طبقه، ثروت و جنسیت گسترانیده است. ازاین‌رو، محور اساسی جهانی‌شدن ریسک گستردگی و بدون مرز شدن مخاطرات است؛ امری که امکان کنترل آن را در سطح ملی در عمل نشدنی می‌سازد. بااین‌حال، دو مؤلفهٔ اخیر مانع از سنجش‌پذیری، اندازه‌گیری و ارزیابی ریسک نمی‌شوند. در این چارچوب، با ارزیابی احتمالات موجود و نگاه به آینده و حوادثی غیرقطعی می‌توان با به‌کارگیری برخی ابزارها، به ارزیابی سطح ریسک[1] پرداخت (دنی، ۱۳۹۳، ص۴۳).

بر این اساس، منطق پیشگیری ریسک‌مدار بر پیشگیری از مخاطرات جنایی ارزهای مجازی نیز تسری یافته است. ازاین‌رو، مطابق مؤلفهٔ نخست، ارزهای مجازی دربردارندهٔ ریسک وقوع جرم‌اند؛ ابزاری فناورانه که از قابلیت استفاده در جرم برخوردار است. بی‌تردید، در مرحلهٔ ارزیابی ریسک این امر مورد پذیرش قرار می‌گیرد. حال پرسش اساسی این است که احتمال وقوع جرم در این موارد در چه موقعیت‌هایی یا توسط چه اشخاصی بالا ارزیابی می‌شود. در واقع، احتمالی‌بودن ریسک در این زمینه از دو بعد قابل بررسی است: احتمال وقوع جرم با استفاده از این فناوری، و احتمال وقوع جرم با استفاده از این فناوری توسط شخص معین یا در موقعیت‌های معین. در واقع، در هر دو بعد مزبور ضروری است که سنجش احتمال صورت پذیرد؛ امری که تأثیر مستقیمی در رویکرد پیشگیری ریسک‌مدار دارد؛ زیرا پویایی ریسک مستلزم پویایی اقدامات و تدابیر پیشگیرانه است. در این مفهوم، پیشگیری ریسک‌مدار رویکردی هدفمند و دارای اولویت است. زمانی که احتمال وقوع جرم در شخص یا موقعیتی زیاد شود، تدابیر و اقدامات پیشگیرانه

۱. Risk Assessment

نیز درخصوص آن شخص یا موقعیت افزایش می‌یابد و با کاهش احتمال وقوع جرم، تدابیر و اقدامات پیشگیرانه نیز کاهش می‌یابد. این امر به‌وضوح در تدابیر مربوط به «شناسایی مشتری» مشاهده می‌شود.[1]

مطابق مؤلفهٔ دوم، شناخت ویژگی جهانی‌بودن از دو طریق در اتخاذ اقدامات و تدابیر پیشگیرانه در برابر مخاطرات ارزهای مجازی اثرگذار است. از یک سو، شناخت ویژگی جهانی‌بودنِ قلمرو ریسک در ارزیابی و سنجش میزان ریسک، چه از نظر اشخاص و چه از نظر موقعیت‌ها، تأثیر بسیاری دارد. در این راستا، می‌توان به ترسیم وضعیت مخاطرات جنایی ارزهای مجازی در سراسر جهان دست یافت و نقاط کور را کاهش داد. از سوی دیگر، جهانی‌بودنِ 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.

مطابق مؤلفهٔ سوم، قابلیت ارزیابی ریسک از چند نظر اهمیت دارد.[2] نخست، ارزیابی ریسک با به‌کارگیری ابزارهای آماری با توجه به وضعیت اشخاص و موقعیت‌ها، سطح و میزان ریسک را مشخص می‌کند. طبیعتاً ارزیابی ریسک اولیه ترسیم‌کنندهٔ مخاطرات جنایی است. در این چارچوب، ارزیابی ریسک اولیه میزان ریسک بخش‌ها و اشخاص را از حیث قابلیت ارتکاب جرم با استفاده از ارزهای مجازی فراهم می‌سازد. دوم، ارزیابی ریسک مبنایی برای اولویت‌بندی به‌منظور اتخاذ تدابیر پیشگیرانهٔ ریسک‌مدار را فراهم

---

۱. یکی از مهم‌ترین اقدامات در چارچوب فرایند پیشگیری ریسک‌مدار از مخاطرات ارزهای مجازی، اقدامات مربوط به شناسایی مشتری است. این اقدام از طیف گسترده‌ای برخوردار است و اثربخشی آن نیازمند توجه به جزئیات خاصی است. امری که در اسناد بین‌المللی نیز مورد توجه قرار گرفته است. برای نمونه، بند «ب» از پارگراف ۱ مادهٔ ۱۸ کنوانسیون مبارزه با تأمین مالی تروریسم یکی از وظایفی که برای کشورها در جهت پیشگیری از جرم تأمین مالی تروریسم مقرر می‌دارد شناسایی اشخاصی است که ظن ارتباط آن‌ها با فعالیت‌های مجرمانه وجود دارد. مشابه چنین مقرره‌ای در پارگراف ۱ از مادهٔ ۱۴ کنوانسیون سازمان ملل متحد در برابر فساد وجود دارد. این امر در توصیه‌های گروه ویژهٔ اقدام مالی نیز مورد توجه قرار گرفته است. توصیهٔ شماره ۱۰ کشورها و نهادهای موظف به اجرای توصیه‌ها را مکلف کرده تا فرایند شناسایی کامل مشتری را مطابق توصیه‌های گروه ویژه اقدام مالی و الزامات قانونی ملی طراحی نمایند. افزودنی است مطابق بند ۳۳ مادهٔ ۱ آیین‌نامهٔ قانون مبارزه با پولشویی ۱۳۹۸ شناسایی عبارت از: «فرایند دریافت و بررسی مستمر اطلاعات ارباب‌رجوع، مرتبط با احراز هویت و ارزیابی خطر (ریسک) پولشویی و تأمین مالی تروریسم. سطوح شناسایی شامل سه سطح ساده، معمول و مضاعف است.».

۲. در علوم جنایی و در چارچوب رویکرد جرم‌شناسی اثباتی و تحققی، تحت تأثیر کلیت علوم اثباتی دنیا قلمرویی قابل محاسبه محسوب می‌شود که در آن هرچیزی از قابلیت محاسبه و سنجش‌پذیری برخوردار است (Brown, 1995, p.112).

می‌سازد. در واقع، نتایج این ارزیابی است که اولویت‌ها را تعیین می‌کند و کنش‌گران را قادر می‌سازد تا به‌صورتی هدفمند تدابیر و اقدامات لازم را در پیش گیرند. سوم، پس از ارزیابی ریسک و اتخاذ تدابیر پیشگیرانه بر اساس آن، سنجش کارآمدی اقدامات امکان‌پذیر می‌شود تا تأثیر اتخاذ تدابیر بر میزان ریسک، کاهش یا افزایش آن سنجیده شود. بر این اساس، اگر ارزیابی ریسک اولیه نشان از بالابودن ریسک ارتکاب جرم در حوزهٔ بانکی باشد و در جهت کاهش آن تدابیر شناسایی مضاعف تجویز شود، ارزیابی بعدی نشان خواهد داد که تدبیر مذکور تا چه میزان در کاهش سطح ریسک مؤثر بوده است. افزون‌براین، میزان سطح ریسک در ارزیابی بعدی در تشدید یا تخفیف تدابیر پیشگیرانه نیز مؤثر است.[۱]

بدین‌سان، به‌طور اختصاری منطق پیشگیری ریسک‌مدار در برابر مخاطرات ارزهای مجازی با شناسایی احتمال استفاده از این فناوری در ارتکاب جرم با گستره‌ای جهانی که از قابلیت ارزیابی برخوردار است، در تلاش است تا با به‌کارگیری برخی اقدامات و تدابیر، ریسک مجرمانهٔ این فناوری را کاهش دهد.

۱. یکی از ویژگی‌هایی که برای ریسک می‌توان درنظر گرفت غیرقابل پیش‌بینی بودن آن است. امری که درخصوص ریسک در جامعهٔ مخاطره‌آمیز مورد پذیرش قرار گرفته است. بااین‌حال، با تأکید بر غیرقابل پیش‌بینی بودن و اتفاقی‌بودن ریسک‌ها، سامانه‌های سنجش و ارزیابی آن‌ها نیز افزایش قابل‌توجه‌ای یافته است. در واقع، آنچه در اینجا در نگاه اول متعارض به‌نظر می‌رسد این است که چطور ریسک هم‌زمان می‌تواند غیرقابل پیش‌بینی اما سنجش پذیر باشد. شاید پاسخ اولیه به این تعارض این باشد که پیش‌بینی مربوط به «زمان وقوع» است و سنجش مربوط به «میزان وقوع» است. یعنی شاید زمان وقوع ریسک‌ها چندان قابل پیش‌بینی نباشد اما پس از وقوع، میزان آن را با توجه به ابزارهایی می‌توان تعیین کرد. این برداشت صحیح است اما پاسخ به تعارض مزبور صرفاً منحصر در آن نیست. افزون‌بر مورد فوق، باید دانست که غیرقابل پیش‌بینی بودن زمانی است که دیدگاهی نسبت به یک موضوع خاصی وجود ندارد و امری به‌طور ابتدایی رخ می‌دهد. برای نمونه، تا پیش از معرفی ارزهای مجازی و شروع استفاده از آن، طبیعتاً پیش‌بینی درخصوص ریسک استفاده از آن معنا پیدا نمی‌کرد اما با معرفی و توسعه و شکل‌گیری درک وجود ریسک در ساختار آن، میزان ریسک آن مورد سنجش و ارزیابی قرار خواهد گرفت و حتی درخصوص میزان آن پیش‌بینی‌هایی هم صورت می‌پذیرد (صیقل، ۱۳۹۷، ص۴۴). برای نمونه، در سال ۲۰۱۴، گروه ویژهٔ اقدام مالی در سند خود تأکید کرد که ارزهای مجازی ابزارهای نوظهوری هستند که در آینده از حیث پولشویی و تأمین مالی تروریسم بسیار بحث‌برانگیز خواهند بود. در این سند از این فنناوری به‌عنوان دروازهٔ جدیدی در تنظیم‌گری ابزارهای مالی یاد شده است. با وجود این، چون در این بند در مقام بیان ویژگی‌های ریسک ارزهای مجازی در چارچوب بایسته‌های پاسخ‌گذاری کنشی در برابر مخاطرات آن هستیم، در عمل غیرقابل پیش‌بینی بودن موضوعیت نمی‌یابد.

۲. چالش‌های مؤثر بر اثربخشی رویکرد پیشگیری ریسک‌مدار از مخاطرات ارزهای مجازی

ریسک در رویکرد پیشگیری ریسک‌مدار از دو بعد مورد توجه قرار می‌گیرد: ریسک اشخاص و ریسک موقعیت‌ها. بر این اساس، ارزیابی ریسک نیز متوجه اشخاص و موقعیت‌ها است تا با ترسیم وضعیت ریسک، تدابیر کنشی لازم اتخاذ شود. بر این اساس، اگرچه برخی اقدامات بر موقعیت‌ها تمرکز می‌کنند تا با موقعیت‌زدایی مانع از وقوع جرم شوند، اما اصلِ اولویت‌بندی و هدفمندی پیشگیری ریسک‌مدار بر ریسک اشخاص تمرکز می‌کند و مطابق آن است که اقدامات لازم اتخاذ و منابع تخصیص می‌یابد. باید توجه داشت که مرز باریکی بین اتخاذ تدابیر وضعی در رویکرد پیشگیری وضعی در معنای عام و رویکرد پیشگیری ریسک‌مدار وجود دارد (خانعلی‌پور واجارگاه، ۱۳۹۰، ص ۱۵). در پیشگیری وضعی، اقدامات مشخص‌شده بدون اولویت‌بندی خاصی به‌صورت عمومی اختصاص می‌یابد. بر این اساس، ممکن است اقدامات حسب مورد بر آماج جرم، بزه‌دیده یا اموال اثر بگذارد یا سبب ایجاد محدودیت بر بزهکار شود.[۱] اما زمانی که از پیشگیری ریسک‌مدار سخن می‌گوییم، نخست ریسک مشخصی مدنظر قرار دارد؛ دوم، اقدامات بر اساس ارزیابی ریسک اولویت‌بندی می‌شود؛ سوم، تدابیر موقعیت‌مدار به‌صورت عمومی اجرا می‌شوند و در نهایت، اقدامات خاص برای اشخاص پرریسک اتخاذ می‌شود. بر این اساس، پیشگیری ریسک‌مدار اگرچه از تدابیر پیشگیری وضعی استفاده می‌کند، اما روش منظم و خاص خود را در استفاده از این تدابیر دارد. ازاین‌رو، هدف نهایی شخص‌محور شدن تدابیر اتخاذی برحسب احتمال وقوع جرم از ناحیهٔ اشخاص است. امری که با توجه به ویژگی‌های ریسک ارزهای مجازی و امکاناتی که به کاربرانِ با اندیشهٔ مجرمانه می‌دهد با دشواری‌های زیادی همراه است.

به لحاظ نظری، فرایند مذکور مطلوب تلقی می‌شود. ابتدا برخی تدابیر عمومی مدنظر قرار می‌گیرد؛ برای مثال، ضرورت اخذ مجوز و ثبت‌نام برای ارائه‌دهندگان خدمات ارزهای مجازی و شناسایی آن‌ها به‌عنوان یکی از اشخاص موظف به رعایت الزامات رویکرد ریسک‌مدار، موظف‌شدن این اشخاص به انجام برخی الزامات مانند ایجاد

۱. برای نمونه، برخی اقدامات برای حفظ امنیت خودرو یا منزل از سوی مالک صورت می‌پذیرد تا مانع از وقوع سرقت از خودرو یا لوازم منزل شود یا برای یک کودک محافظ قرار داده می‌شود تا مورد بزه‌دیدگی واقع نشود یا با تعیین محدودهٔ رفت‌وآمد برای برخی اشخاص تلاش می‌شود مانع از تکرار جرم توسط آن‌ها شوند.

ساختارهای نظارتی، شناسایی مشتری، ارائهٔ گزارش عملیات مشکوک و... . سپس، اشخاص موظف مکلف به ارزیابی ریسک دوره‌ای می‌شوند تا بر اساس آن اقدامات پیشگیرانه را بر اساس منطق هدفمندی و اولویت‌بندی اعمال کنند. این الزامات از طیفی حداقلی تا حداکثری برخوردار است، به‌گونه‌ای که ریسک زیاد مستلزم اقدامات بیشتر و ریسک کم مستلزم اقدامات کمتر خواهد بود. بااین‌حال، در عمل و در مقام ارزیابی نمی‌توان این رویکرد را تاکنون در حوزهٔ ارزهای مجازی چندان موفق محسوب کرد. امری‌که از چند حیث قابل توجه است.

۲-۱. تحول در روند استفادهٔ مجرمانه از ارزهای مجازی

ماهیت فناورانهٔ ارزهای مجازی زمینه‌ساز تسریع در تحولات ارتکاب جرم با استفاده از ظرفیت این فناوری شده است. امری که به‌طور مشخص در ارتکاب پولشویی قابل بررسی است. چنین سرعتی در تحولات در کنار کندی پوشش توصیه‌های گروه ویژهٔ اقدام مالی در سطح جهانی، اساساً این پرسش را ایجاد می‌کند که آیا می‌توان بر مخاطرات جنایی این فناوری فائق آمد یا خیر. بر این اساس، بررسی روند اصلی در زمینهٔ ارزهای مجازی درخصوص ریسک پولشویی از ژوئن ۲۰۱۹ دربردارندهٔ نکات قابل تأملی است. در این چارچوب، نتیجهٔ برخی تحقیقات حاکی از آن است که حدود ۱۳ درصد از پولشویی‌ها در حوزهٔ دارایی‌های مجازی با استفاده از بستر کیف پول‌هایی رخ می‌دهد که حفاظت‌های مضاعفی را درخصوص حریم خصوصی ارائه می‌کنند و از قابلیت‌هایی چون «کوین جوین»[۱] برخوردارند (Houben & Snyers, 2018, p.109). بر این اساس، داده‌های شرکت تحلیلی الیپتیک[۲] نشان می‌دهد که استفادهٔ بزهکاران از چنین کیف پول‌هایی توسط مجرمان از سال ۲۰۱۹ تا به حال رشدی چشمگیر داشته است.[۳] در واقع، با یک تغییر رویه در پولشویی از طریق ارزهای‌مجازی، به‌ویژه بیت‌کوین، روبه‌روایم. پیش از این، استفاده از روش میکسینگ[۴] محبوب‌ترین گزینهٔ پولشویان برای پولشویی درآمدهای

۱. Coin Join

۲. Elliptic

۳. "https://cryptopotato.com/13-of-bitcoins-money-laundering-transactions-happened-through-privacy-wallets/", (Last Accessed on 16, December, 2020)

۴. Mixing

مجرمانه محسوب می‌شد. میکسینگ روشی است که در آن، با استفاده از ابزارهایی به نام میکسر، تلاش می‌شود که رد ارزهای مورداستفاده تا حد امکان گم شود. با استفاده از این ابزار، کشف کیف پول مبدأ در عمل بسیار دشوار می‌شود. بااین‌حال، وجود برخی مخاطرات در استفاده از میکسر، مانند موفقیت‌های به‌دست‌آمده توسط نهادهای اجرای قانون در رهگیری مبدأ تراکنش‌ها، منجر به آن شده که بزهکاران به استفاده از کیف پول‌های حریم خصوصی محور روی آورند. این کیف پول‌ها، با فراهم‌آوردن امکاناتی چون استفاده از شبکهٔ ناشناس TOR[1] یا روش‌هایی نظیر کوین جوین، به کاربران کمک می‌کنند تا مبدأ تراکنش خود را مخفی کنند.

کوین جوین روشی است که در آن تراکنش‌هایی با چندین طرف دیگر ایجاد می‌شود. با استفاده از این روش، تقریباً امکان شناسایی مبدأ ارسال نامشخص باقی می‌ماند. این روش از سال ۲۰۱۹ تاکنون با استقبال زیادی به‌ویژه از سوی بزهکاران روبه‌رو شده است و انتظار می‌رود با توجه به مزایای آن برای بزهکاران میزان پولشویی در بستر آن افزایش یابد. ازاین‌رو، سرعت تحولات در روند استفادهٔ مجرمانه از ارزهای مجازی را می‌توان به‌عنوان یکی از چالش‌های موجود در مقام ارزیابی رویکرد پیشگیری ریسک‌مدار مورد اشاره قرار داد. امری که از سرعتی به مراتب بیشتر نسبت به سرعت تطبیق‌پذیری کشورها با الزامات مربوط به پیشگیری ریسک‌مدار برخوردار است. بررسی سیر تحولات ارزهای مجازی از سال ۲۰۱۹ تا کنون از یک سو و سرعت تطبیق‌پذیری کشورها با الزامات مندرج در سند سال ۲۰۱۹ گروه ویژهٔ اقدام مالی، نشانگر سرعت بسیار کم تطبیق‌پذیری کشورها است. امری که به موجب ارزیابی دوازده‌ماههٔ[2] گروه مزبور در ژوئن سال ۲۰۲۰ به‌وضوح مورد تأکید قرار گرفته است. برای نمونه، یکی از موضوعاتی که به‌طور جدی بررسی شد این است که آیا حوزه‌های قضایی متعهد به اجرای توصیه‌های گروه ویژهٔ اقدام مالی، الزامات جدید درخصوص دارایی‌های مجازی را به قوانین و مقررات ملی

۱. Tor در اصل شبکهٔ توزیع رایانه‌ای است که آدرس IP واقعی کاربر را پنهان می‌کند و به‌همین علت هویت کاربران شبکه را با مسیریابی ارتباطات/ معاملات ازطریق چندین رایانه در سراسر جهان از شناسایی مصون می‌سازد و آن‌ها را در چندین لایهٔ رمزگذاری‌شده قرار می‌دهد.

۲. "12-month Review Virtual Assets and VASPs," FATF, Paris, France, Last Accessed on 16, December, 2020, www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html

خود وارد کرده‌اند یا خیر.[۱] افزون‌براین، ازآنجاکه مسئلهٔ نظارت یکی از کلیدی‌ترین بخش‌های توصیه‌های گروه ویژهٔ اقدام مالی محسوب می‌شود، محور مهم دیگر بررسی مزبور این است که آیا ناظران اجرای تدابیر در ارتباط با ارزهای مجازی توسط کشورها و چارچوب‌های نظارتی لازم مشخص شده‌اند یا خیر. در واقع، بسیار مهم است که وضعیت کشورهایی که فعالیت دارایی‌های مجازی را در قلمرو خود مجاز شمرده‌اند درخصوص الزاماتی چون صدور مجوز و ثبت برای ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی مشخص شود.[۲] در این بخش، ارزیابی حاکی از آن است که در میان ۳۸ کشور شرکت‌کننده در این ارزیابی، ۲۴ کشور هنوز فاقد رژیم مناسب برای ارائه‌دهندگان خدمات مربوط به ارزهای مجازی‌اند و تعداد قابل‌توجهی از کشورها هنوز برخوردار از رژیم نظارتی مناسبی در این زمینه نیستند.[۳] ازاین‌رو، در مقام ارزیابی رویکرد پیشگیری ریسک‌مدار، سرعت نه‌چندان مطلوب تطبیق‌پذیری با الزامات رویکرد پیشگیری ریسک‌مدار همسو با سرعت تحولات در روند استفاده مجرمانه از ارزهای مجازی، به یکی از چالش‌های مهم در اثربخشی آن تبدیل شده است.

۲-۲. عدم تأثیر الزامات پیشگیرانه بر بخش‌های غیررسمی

حتی اگر تطبیق‌پذیری کشورها به‌طور کامل صورت پذیرد، الزامات موجود فقط پوشش‌دهندهٔ بخش‌های رسمی است و همچنان قابلیت‌های منحصربه‌فرد برخی از اقسام ارزهای مجازی، مانند بیت‌کوین، بازارهای غیررسمی و مجرمانهٔ آن را خارج از دایرهٔ نظارت دولت‌ها قرار می‌دهد. در واقع، تلاش برای ایجاد ساختار و مقررات‌گذاری، از جمله ارائهٔ الزامات پیشگیرانه، صرفاً معطوف به بخش‌های رسمی می‌شود. بدیهی است، زمانی‌که از رویکرد پیشگیری ریسک‌مدار در برابر پولشویی سخن به‌میان می‌آید، الزاماتی مانند استانداردهای گروه ویژهٔ اقدام مالی بسیار مؤثر و کارآمد است. زیرا، هدف نهایی ایجاد مانع برای ورود پول‌های با منشأ مجرمانه به بخش اقتصاد رسمی و قانونی است. در این دیدگاه، سلب امکان استفاده از درآمدهای مجرمانه عاملی برای انصراف از ارتکاب

۱. Ibid.

۲. Investigating the impact of global stablecoins," BIS, Last Accessed on 16, October, 2019, www.bis.org/cpmi/publ/d187.pdf

۳. '12-month Review Virtual Assets and VASPs," FATF, Op. Cit, P.8.

جرم منشأ تلقی می‌شود. اما آیا می‌توان انتظار داشت چنین رویکردی درخصوص ارزهای مجازی نیز کارایی داشته باشد؟ پاسخ به این پرسش زمانی امکان‌پذیر است که به «نظریهٔ جایگزینی» در ساختار ارزهای مجازی جهان‌روا توجه شود (شاملو و خلیلی پاجی، ۱۳۹۹). مطابق این دیدگاه، هدف غایی ارزهای مجازی تبدیل‌شدن به جایگزینِ نظام پولی و مالی موجود است. بر این اساس، این فناوری با کارکرد پولی خود از نهادهای واسطه‌ای مانند بانک‌ها بی‌نیاز است و فضای اختصاصی خود را به کاربران ارائه می‌دهد. ازاین‌رو، کاربران در چارچوب این فناوری بدون احتیاج به ساختارهای پولی موجود می‌توانند فعالیت کنند. به این دلیل، ورود درآمدهای مجرمانه به نهادهای پولی رسمی دیگر به‌عنوان اولویت بزهکاران تلقی نمی‌شود. درواقع، سازوکار ارزهای مجازی به‌گونه‌ای است که آن را می‌توان بخشی موازی با اقتصاد رسمی و نهادهای موجود در آن، مانند بانک‌ها، به‌شمار آورد. امری که در چارچوب شکل‌گیری بازارهای مجرمانه بر پهنهٔ رویِ تاریک وب، دارک نت،[۱] به‌وضوح قابل مشاهده است.[۲]

دارک نت به کاربران اجازه می‌دهد تا در اینترنت جست‌وجو کنند، درحالی‌که با مسیریابی اتصالات توسط سرورهای پروکسی شخص ثالث و مسدودکردن آدرس آی‌پی[۳] کاربر، از آن‌ها دربرابر نظارت و تحلیل ترافیک محافظت می‌کند (Weimann, 2016, p. 40-44). مجلهٔ *وایرد*[۴] تخمین می‌زند که دارک نت بیش از ۰/۱ درصد از اینترنت را شامل نمی‌شود. بااین‌حال، به‌دلیل ناشناس‌بودن و امنیتی که دارک نت فراهم می‌کند، اغلب توسط مجرمان سایبری برای فعالیت‌های‌غیرقانونی مورد استفاده قرار می‌گیرد. گزارش‌ها حاکی از آن است که ۵۷ درصد

۱. Dark Web

۲. سه نوع وب‌سایت اینترنتی وجود دارد. نخست، وب سطحی (Surface Web)؛ وب‌سایت‌هایی که به‌عنوان بخشی از وب‌سطحی شناخته می‌شوند، به‌دلیل نمایه‌دارشدن آن‌ها از طریق موتورهای جست‌وجو در دسترس‌اند. وب‌سایت‌های دیگر که از طریق مرورگرهای استاندارد وب قابل دسترسی‌اند ولی توسط موتورهای جست‌وجو قابل دسترسی نیستند به‌عنوان بخشی از وب عمیق (Deep Web) طبقه‌بندی می‌شوند و توسط موتورهای جست‌وجو نشان‌داده نمی‌شوند. ردهٔ نهایی، دارک نت است که با وب‌سایت سطحی و وب عمیق تفاوت دارد؛ برخلاف وب‌سایت‌های موجود در وب سطحی، وب‌سایت‌هایی که به‌عنوان بخشی از دارک نت طبقه‌بندی می‌شوند، از طریق موتورهای جست‌وجوی معمولی قابل جست‌وجو نیستند. تمایز دارک نت از وب عمیق نیز از نحوهٔ دسترسی به آن‌ها شکل می‌گیرد.

۳. IP

۴. Wired

محتوای دارک نت غیرقانونی است؛ مانند پورنوگرافی، مراودات مالی‌غیرقانونی، فروش موادمخدر و سلاح، پولشویی و ارتباطات تروریستی (Wechsler, 2021).

برای خرید محصولات یا دریافت خدمات که در دارک نت وجود دارد، وجود یک ارز مجازی، مانند بیت‌کوین، ضروری است. زیرا «از فناوری نظیربه‌نظیر/ شخص‌به‌شخص استفاده می‌کند که برای کار، احتیاج به هیچ مقام مرکزی یا بانکی ندارد؛ کاربر معاملات را مدیریت می‌کند و صدور بیت‌کوین‌ها به‌صورت جمعی توسط شبکه انجام می‌شود. بیت‌کوین منبع باز است؛ طراحی آن عمومی است؛ هیچ‌کس صاحب یا کنترل‌کنندهٔ بیت‌کوین نیست و همه می‌توانند با آن کارکنند... بیت‌کوین قابلیت‌های استفادهٔ هیجان‌انگیزی دارد که سیستم‌های پرداخت دیگر از آن محروم هستند.».[۱] بیت‌کوین به‌دلیل سه مزیت عمده به خریداران و فروشندگان در بازارهای دارک نت ارائه می‌شود. نخست، **خطر کمتر برای کاربران**. معاملات بیت‌کوین امن و غیرقابل برگشت‌اند و حاوی اطلاعات حساس یا شخصی/ هویتی مشتری نیستند. این کار از کاربران در برابر خسارات ناشی از تقلب یا بازپرداخت‌های جعلی محافظت می‌کند. آن‌ها به‌راحتی می‌توانند به بازارهای جدیدی راه یابند که در آن یا کارت‌های اعتباری در دسترس نیستند یا نرخ تقلب به‌طور غیرقابل قبولی بالا است. نتایج این امر عبارت است از هزینه‌های کمتر انتقال، دسترسی به بازارهای بزرگ‌تر و هزینه‌های مادی و غیرمادی اداری کمتر. دوم، **امنیت و کنترل**، کاربران بیت‌کوین بر معاملات خود کنترل کامل دارند. پرداخت‌های بیت‌کوین را می‌توان بدون اطلاعات شخصی مرتبط با معامله انجام داد. این کار در برابر سرقت هویت از کاربر محافظت می‌کند. کاربران بیت‌کوین همچنین می‌توانند از ارزهای خود با استفاده از خدمات پشتیبانی مضاعف و رمزگذاری حفاظت بیشتری کنند. سوم، **شفافیت**؛ تمامی اطلاعات مربوط به عرضهٔ پول بیت‌کوین در بلاک‌چین برای هر کسی، جهت تأیید و استفاده، در هر زمانی در دسترس است. هیچ فرد یا سازمانی نمی‌تواند پروتکل بیت‌کوین را کنترل یا دست‌کاری کند، زیرا از طریق رمزنگاری ایمن‌سازی شده است. این کار اجازه می‌دهد تا هستهٔ بیت‌کوین کاملاً شفاف و قابل پیش‌بینی باشد.

۱. Available at: Bitcoin.org, https://bitcoin.org/en/. (Last Accessed on 14, February, 2020).

بیت‌کوین،امنیت و ناشناسی‌ای را فراهم می‌کند که کارت‌های اعتباری فاقد آن‌اند؛ هیچ دنبالهٔ کاغذی وجود ندارد، هیچ ارتباطی با بانک‌ها ندارد و مهم‌تر از همه، توسط نهادهای اجرای قانون قابل کنترل نیست. بیت‌کوین مانند پول نقد است، اما ازآنجاکه مجازی است، نیازی به حضور اشخاص ثالث در فرایند کاربری ندارد. این امر موجب می‌شود اشخاص برای خرید محصولات غیرقانونی از مجرمان راحت‌تر باشند. در مجموع، بیت‌کوین هم برای کاربری‌های مشروع و هم برای تبهکاران امنیت گسترده‌ای فراهم می‌کند و اطمینان لازم را برای تسهیل معاملات در جهان زیرزمینی ایجاد می‌کند.

بدین‌سان، حتی اگر الزامات گروه ویژهٔ اقدام مالی در چارچوب رویکرد پیشگیری ریسک‌مدار توسط کشورها به‌طور کامل عملیاتی شود، همچنان قسمت اصلی مخاطرات جنایی ارزهای‌مجازی که مربوط به بخش غیررسمی است ادامه خواهد داشت. امری که بی‌شک بزرگ‌ترین چالش پیشِ روی رویکرد پیشگیری ریسک‌مدار در برابر مخاطرات ارزهای مجازی است.

نتیجه‌گیری

ارز مجازی نمونهٔ نوین از تحولات فناوری است که به‌واسطهٔ ویژگی‌های منحصربه‌فرد خود کارکرد گسترده‌ای در وقوع بزهکاری در سطح جهانی دارد. این ویژگی‌ها، افزون‌بر ایجاد برخی تحولات مفهومی، گسترهٔ وسیعی از جذابیت‌های مجرمانه را ایجاد کرده که بیش‌ازپیش کوچ مجرمان به فضای مجازی را سرعت بخشیده است. امری که به افزایش ریسک بزهکارانهٔ ارزهای مجازی منجر شده و اقدام به اتخاذ سیاست جنایی مناسب را در برابر آن اجتناب‌ناپذیر کرده است.

بی‌تردید، اهمیت موضوع پیشگیری از جرم پاسخ‌گذاری کنشی در برابر فناوری ارزهای مجازی را تبدیل به اولویت سیاست جنایی کرده است. امری که در چارچوب رویکرد ریسک‌مدار گروه ویژهٔ اقدام مالی در برابر پولشویی با پوشش الزامات پیشگیری ریسک‌مدار بر مخاطرات جنایی ارزهای مجازی در سطح ملی و فراملی در دستور کار قرار گرفته است. ازاین‌رو، مطابق منطق رویکرد پیشگیری ریسک‌مدار و با تأکید بر مؤلفه‌هایی چون احتمالی‌بودن، جهانی‌بودن و قابل ارزیابی‌بودن ریسک ارزهای مجازی، راهنمای مفصلی توسط گروه مزبور خطاب به کشورها منتشر شده است تا در پرتو آن به

شکل منسجمی تدابیر پیشگیرانه مدنظر قرار گیرد. بااین‌حال، از یک سو، ارزیابی تدابیر مزبور و روند اجرای آن‌ها توسط کشورها و از سوی دیگر، سرعت تحولات فناورانهٔ ارزهای مجازی، گواه آن است که رویکرد پیشگیری ریسک‌مدار به‌تنهایی نمی‌تواند رویکردی کامل و مطلوب در جهت مهار مخاطرات جنایی ارزهای مجازی محسوب شود. ازاین‌رو، چاره‌اندیشی پیرامون حل این معضل ضروری است تا بتوان، با اتخاذ برخی رویکردهای مکمل، ضعف‌های موجود را برطرف کرد. امری که بی‌تردید نیازمند پژوهش‌های عمیق‌تر و بیشتری پیرامون ارزهای مجازی است.

بررسی منابع موجود حاکی از آن است که یکی از مکمل‌هایی که توسط برخی نهادهای بین‌المللی و کشورهای پیشرو مدنظر قرار گرفته، توسعهٔ رمزارزهای باثبات با پشتوانهٔ پول‌های ملی یا برخی دارایی‌های با ارزش مانند طلا یا نفت است. در این چارچوب، توسعهٔ رمزارزهای باثبات تا حد زیادی به مدیریت ویژگی گمنامی این فناوری منجر خواهد شد. امری که در کنار تدابیر اتخاذی در چارچوب رویکرد پیشگیری ریسک‌مدار، در کاهش مخاطرات رمزارزهای جهان‌روا، بدون پشتوانه و بدون نیاز به مرجع ناظر و مرکزی تأثیرگذار خواهد بود.

منابع

بک، اولریش (۱۳۸۸). *جامعه در مخاطره جهانی*. ترجمهٔ محمدرضا مهدی. تهران: انتشارات کویر، چاپ اول.

خانعلی‌پور واجارگاه، سکینه (۱۳۹۰). *پیشگیری فنی از جرم*. تهران: نشر میزان، چاپ اول.

دنی، دیوید (۱۳۹۳). *ریسک و جامعه*. ترجمهٔ صالح کاشانی محمدی. تهران: انتشارات پژوهشکده بیمه، چاپ اول.

شاملو، باقر و خلیلی پاجی، عارف (۱۳۹۹). «چالش‌های حقوقی-اقتصادی ارزهای مجازی برای نظام‌های سیاسی در پرتو نظریه جایگزینی». فصلنامهٔ علمی *رهیافت‌های سیاسی و بین‌المللی*، دورهٔ ۱۲، شمارهٔ ۱، ص ۱۲۵-۱۵۲.

صیقل، یزدان (۱۳۹۷). *مطالعه حقوقی-جرم‌شناختی جرم در جامعه مخاطره‌آمیز*. رسالهٔ دکتری، تهران: دانشگاه شهید بهشتی.

قناد، فاطمه و اکبری، مسعود (۱۳۹۶). «امنیت‌گرایی سیاست جنایی». *پژوهش حقوق کیفری*، دورهٔ ۵، شمارهٔ ۱۸، ص ۳۹-۶۷.

نجفی ابرندآبادی، علی حسین (۱۳۸۸). «کیفرشناسی نو – جرم‌شناسی نو؛ درآمدی بر سیاست‌جنایی مدیریتی خطرمدار». *تازه‌های علوم جنایی*. تهران: انتشارات میزان.

BIS. "Investigating the impact of global stablecoins," October 2019, www.bis.org/cpmi/publ/d187.pdf

Brown, P.(1995)."Popular Epidemiology, Toxic Waste and Social Movements". in *Medicine, Health and Ris*k, edited by J. Gabe. Oxford: Blackwell. 67-83.

Clarke, R. V. (2005). "Seven Misconceptions of Situational Crime Prevention." in *Handbook of Crime Prevention and Community Safety*, edited by N. Tilley. Cullompton, UK: Willan Publishing.

Farrington, D. P. (2002). "Criminology". *Criminal Behaviour and Mental Health, 12*, 59-76.

FATF, *12-month Review Virtual Assets and VASPs*, FATF, Paris, France, 2020: www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html

FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, FATF, Paris, 2019, www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html

FATF, *Virtual Currencies, Guidance for A Risk-Based Approach, Paris*, 2015: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf

FATF, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, June 2001, www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

Houben, R., & Snyers, A. (2018). *Cryptocurrencies and blockchain: legal context and implications for financial crime, money laundering and tax evasion*. European Parliament study. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf).

Kemshall, H. (2003). *Understanding risk in criminal justice*, UK: Open University Press.

Kotane, I. (2018). "Concept of Virtual Currencies in Modern Economies" *Latgale National Economy Research*, *1*(10), 63-76.

Loeber, R., Farrington, D. P., Stouthamer-Loeber, M. E., & White, H. R. E. (2008). *Violence and Serious Theft:Development and Predictionfrom Childhood to Adulthood*. New York: Routledge.

Wechsler, P. (2021). ""Dark web" gives cover to criminals". Issue: Cybersecurity. http://businessresearcher.sagepub.com/sbr-1775-98146-2715485.

Weimann, G. (2016). "Terrorist migration to the dark web". *Perspectives on Terrorism*, *10*(3), 40–44.

Evaluation of Risk-based Prevention Approach to Criminal Risks of Virtual Currencies

Aref Khalili Paji[۱]

Abstract

Technological phenomena, despite facilitating human life, pose challenges of economic and social dimensions. Therefore, exploring challenges and finding ways to reduce their potential and real risks has always been one of the fundamental human questions. A clear example is the technological phenomena of virtual currency, which, along with all the benefits and positive functions, has paved the way for change and innovation in committing some crimes. This has accelerated the process of globalization of crime and has had a significant impact on the criminal environment by extending beyond the geographical borders of a country. Therefore, the actors of the criminal justice system, according to their inherent duties, should control the criminal capacities of this technology as much as possible by setting up an optimal response system. Undoubtedly, like other areas of crime response, action response is a priority in this area. This has also been the focus of the FATF Financial Action Task Force. Within the framework of its risk-oriented approach to money laundering, the group emphasizes the selection of a risk-averse approach to the risks of virtual currencies. It seeks to extend the risk-based prevention approach to this technology, including the requirements for preventing money laundering on virtual currencies. However, the evaluation of the recent approach shows that relying on it alone is not effective enough and the existence of some challenges has prevented its full success. This is evaluated in the present study with a descriptive and analytical look to reveal its various dimensions.

Keywords: Virtual Currencies, Risk Prevention, Financial Action Task Force.

۱ Ph.D. in Criminal Law and Criminology, Faculty of Law, Shahid Beheshti University, Tehran, Iran; arefkhalilipaji@gmail.com