

بایسته‌های شمول قانون مبارزه با پولشویی بر دارایی‌های مجازی؛ در پرتو توصیه‌های گروه ویژه اقدام مالی FATF

عارف خلیلی پاجی^۱

دکتری حقوق جزا و جرم‌شناسی، دانشکده

حقوق دانشگاه شهید بهشتی

امیرحسین نیازپور^۲

استادیار گروه حقوق جزا و جرم‌شناسی،

دانشکده حقوق دانشگاه شهید بهشتی

تاریخ پذیرش: ۱۴۰۰/۰۶/۰۲

تاریخ دریافت: ۱۴۰۰/۰۲/۱۰

چکیده

دارایی‌های مجازی به‌عنوان یک ابزار فن‌آورانه با برخورداری از کارکردهای اقتصادی، نظر بزه‌کاران را نیز به خود جلب کرده است. به‌گونه‌ای که ویژگی‌های منحصر به فرد این فن‌آوری زمینه‌ساز تحولات قابل توجهی در روش و شگرد ارتکاب برخی از انواع جرائم شده است. از این رو ضرورت مهار مخاطرات جنایی این فن‌آوری، اتخاذ تدابیر و اقداماتی را در برابر آن اجتناب‌ناپذیر ساخته است. در این راستا، گروه ویژه اقدام مالی FATF به‌عنوان یک گروه فراملی نقش بارزی را ایفا می‌کند. آنچه در رویکرد این گروه مدنظر قرار دارد پوشش قواعد مبارزه با پولشویی بر این فن‌آوری است تا در چارچوب آن، زمینه مهار مخاطرات دارایی‌های مجازی فراهم گردد. از این رو، توصیه به کشورها جهت پوشش قواعد ملی مبارزه با پولشویی در دستور کار این گروه قرار گرفته است. با این حال، پوشش قواعد مزبور مستلزم رعایت الزاماتی است و تا زمانی که نتوان به تحقق آن‌ها پرداخت، نمی‌توان منتظر نتایج مثبت این تدابیر و اقدامات ماند. در

*- نوع مقاله: پژوهشی

1- Arefkhalilipaji@gmail.com

۲- نویسنده مسئول: a_niazpour@sbu.ac.ir

DOI: 10.22067/LOWECON.2022.70831.1052

نوشتار حاضر با روش توصیفی و تحلیلی به بررسی بایدهای شمول قانون مبارزه با پولشویی در ایران بر دارایی‌های مجازی پرداخته می‌شود تا در پرتو توصیه‌های گروه ویژه اقدام مالی، راهکارهای تحقق آن‌ها ارائه گردد. در این راستا، دستاورد این پژوهش، لزوم شناسایی قانونی دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن است تا زمینه لازم جهت مقرر کردن گذاری و تنظیم‌گری پیرامون ابعاد گوناگون این فن-آوری فراهم گردد.

کلیدواژه‌ها: دارایی‌های مجازی، رمز ارزها، پولشویی، گروه ویژه اقدام مالی، رویکرد ریسک‌مدار.

مقدمه

دارایی‌های مجازی بازنمایی دیجیتال (رقومی) از یک ارزش با قابلیت معامله و انتقال و با هدف سرمایه‌گذاری و پرداخت به صورت غیرمتمرکز و شفاف است. نمونه بارز این دارایی‌ها، رمز ارزها است که بر بستر زنجیره بلوک (بلاک‌چین)^۱ مبتنی بر علم رمزنگاری موجودیت دارد. گذشت بیش از یک دهه از معرفی، انتشار و توسعه رمز ارزها به‌عنوان یکی از اقسام دارایی‌های مجازی^۲ سبب شده تا در کنار تلاش‌های ملی، در سطح فراملی نیز ابعاد گوناگون آن به‌موجب برخی اسناد و رهنمودها مورد توجه قرار گیرد. نمونه بارز چنین رویکردهایی را می‌توان در چارچوب فعالیت‌های گروه ویژه اقدام مالی FATF^۳ جست که با ارائه نسخه‌ای ویژه، به شکل دهی

۱- واژه بلاک‌چین Blockchain ترکیبی از دو کلمه بلوک Block و زنجیره Chain است. این فن‌آوری در حقیقت زنجیره‌ای از بلوک‌ها است. بلاکچین به زنجیره‌ای از بلاک‌ها اطلاق می‌شود که در بردارنده اطلاعاتی هستند. این فن‌آوری برای نخستین بار در سال ۱۹۹۱ توسط گروهی از پژوهش‌گران و به‌منظور زمان‌بندی اسناد دیجیتال بکار گرفته شد. در واقع در این کارکرد، بلاک‌چین به عنوان یک دفتر اسناد رسمی به کار برده شد تا امکان تغییر تاریخ یا دست بردن در اطلاعات موجود امکان نداشته باشد. با این حال بلاک‌چین تا پیش از سال ۲۰۰۹ و بکارگیری آن در ایجاد بیت‌کوین توسط ساتوشی ناکاموتو از کاربرد محدودی برخوردار بود (Yaga, 2018: 15).

۲- بیش از ۵۱۰۰ دارایی رمزنگاری شده با بازاری به ارزش ۲۵۰ میلیون دلار در آغاز سال ۲۰۲۰ شناسایی شده است (Available at: "coinmarketcap", Last modified July 15, 2021, <https://coinmarketcap.com>) که به صورت قانونی یا غیرقانونی وجود دارند. بیشتر فعالیت‌های قانونی در خصوص دارایی‌های مجازی، به ویژه در خصوص رمز ارزها، در صرافی‌های رمز ارزی صورت می‌پذیرد که هدف عمده کسب سود با سرمایه‌گذاری در چنین دارایی‌هایی است.

3- Financial Action Task Force

تنظیم‌گری ابعاد گوناگون حقوقی و کیفی دارایی‌های مجازی پرداخته است. این امر به‌عنوان یک ضرورت عملی از فهم این نکته نشأت می‌گیرد که اگرچه فن‌آوری‌های نوظهور و خدمات مرتبط با آن، منجر به ایجاد سهولت در زندگی شهروندان شده و به‌واسطه ویژگی‌های نوآورانه تحولات مثبتی را در عرصه‌های اقتصادی پدید آورده‌اند، اما از قابلیت ایجاد موقعیت‌های مجرمانه جدید برای بزه‌کاران جهت تطهیر درآمدهای مجرمانه و یا تأمین مالی فعالیت‌های مجرمانه نیز برخوردارند (Shamloo and Khalili Paji, 2020 [b]: 65-96, Najafi, 2009). از این رو است که گروه ویژه اقدام مالی در چارچوب توجه به ریسک‌های مجرمانه در ارتباط با پولشویی، با نگاهی ویژه به حوزه فن‌آوری‌های نوظهور تلاش کرده است تا به پوشش آن‌ها در چارچوب رویکرد ریسک‌مدار بپردازد.

در این راستا، رویکرد ریسک‌مدار در برابر مخاطرات دارایی‌های مجازی از مؤلفه‌هایی برخوردار شده است: نخست؛ این رویکرد ذیل رویکرد ریسک‌مدار در برابر پولشویی قرار می‌گیرد که در نتیجه فعالیت گروه ویژه اقدام مالی به شکل منسجمی ارائه شده است. آخرین ویرایش قابل توجه این توصیه‌نامه‌ها تحت‌عنوان «استانداردهای بین‌المللی در مبارزه با پولشویی و تأمین مالی تروریسم» مربوط به سال ۲۰۱۲ است که در قالب توصیه‌های چهل‌گانه منتشر شد.^۱ مطابق توصیه شماره ۱ این گروه «ارزیابی ریسک‌ها و اتخاذ رویکرد مبتنی بر ریسک»^۲ توسط کشورها ضرورت دارد.^۳ دوم؛ پولشویی در رویکرد اتخاذی گروه ویژه اقدام مالی صرفاً در معنای یک جرم خاص دیده نمی‌شود. در واقع، برخلاف رویکرد سنتی به پولشویی به‌عنوان یک جرم نتیجه، در رویکرد

گروه ویژه اقدام مالی یک سازمان بین‌الدولی است که در سال ۱۹۸۹ با ابتکار گروه ۷ (در حال حاضر گروه ۸) با توجه به توسعه سیاست‌های مبارزه با پولشویی تأسیس شد. وظایف این سازمان در سال ۲۰۰۱ به‌حوزه مبارزه با تأمین مالی تروریسم گسترش یافت و بعدها منع توسعه تسلیحات کشتار جمعی نیز به وظایف سازمانی آن افزوده شد (FATF, 2021:7).
۱- افزودنی است نسخه منتشر شده این توصیه‌ها در سال ۲۰۲۱ به‌طور جزئی ویرایش شده است.

2- Risk-Based Approach (RBA)

۳- کشورها باید ریسک‌هایی را که در ارتباط با پولشویی و تأمین مالی تروریسم با آنها مواجه هستند، شناسایی، ارزیابی و بررسی نمایند. براساس این گونه ارزیابی‌ها، کشورها باید با بکارگیری رویکرد ریسک‌مدار، اطمینان پیدا کنند اقداماتی را که برای پیشگیری از پولشویی و تأمین مالی تروریسم یا کاهش میزان وقوع این جرائم انجام می‌دهند با ریسک‌های شناسایی شده، تناسب داشته باشد (Werle, 2017: 42).

جدید، پولشویی، یک ابزار مؤثر با دو کارکرد پیشگیرانه و کشف جرم معرفی می‌شود.^۱ سوم؛ آنچه گروه ویژه اقدام مالی در تلاش است تا به‌عنوان یک مدل و الگوی کارآمد جهانی در برابر مخاطرات جنایی ارائه نماید از حیث ملی بسیار منعطف است. در این راستا، اگرچه اصول و رهنمودهای اجرایی به‌طور کامل به کشورها ارائه شده اما هر کشوری از این ابزار با توجه به ویژگی‌های تقنینی، قضایی، اجرایی و نیازهای داخلی خود بهره می‌برد.^۲

بدین‌سان، رویکرد ریسک‌مدار در اجرای مؤثر استانداردهای بین‌المللی مبارزه با پولشویی^۳ گروه ویژه اقدام مالی، به‌طور فعال بر خطرات مربوط به فن‌آوری‌های نوظهور در این زمینه پرداخته است. در این راستا، گروه ویژه اقدام مالی به‌موجب برخی اسناد در چند گام رویکرد خود در برابر دارایی‌های مجازی را تبیین کرده است. نخست آنکه، از نگاه به رمز ارزها به‌عنوان یک ارز/پول گذر کرده و قسم کلی‌تری، با عنوان دارایی‌های مجازی را که یکی از انواع آن رمز ارزها

۱- بدین‌سان، تلاش می‌شود با کنترل پول، کاهش هزینه‌های جرم برای نظام پولی و مالی و افزایش خطر ارتکاب جرم برای بزهکاران به مدیریت ریسک هدف‌مند در این حوزه و انسداد روزه‌ها پرداخته شود تا ابتدا از وقوع جرائم مالی-اقتصادی پیشگیری شود و سپس در صورت وقوع جرم، سریعاً کشف شود (Shamloo and Khalili Paji, 2020 [a]). در این چارچوب از حیث کیفری نیز جرم‌انگاری پیش‌دستانه به عنوان مکمل رویکردهای پیشگیرانه مورد توجه قرار می‌گیرد.

۲- برای نمونه، گروه ویژه اقدام مالی به‌موجب سند سال ۲۰۱۹ خود چارچوب اجرایی رویکرد ریسک‌مدار سیاست جنایی در برابر مخاطرات جنایی ارزهای مجازی را ارائه کرده است. با این حال هر کشوری باید با سنجش میزان ریسک واقعی و احتمالی این فن‌آوری برای نظام پولی و مالی خود در راستای تحقق رویکرد ریسک‌مدار و به واسطه ابزارهای اجرایی آن، اقدامات و راهبردهایی را اتخاذ نماید. از این‌رو، سنجش و بررسی ریسک ارزهای مجازی در سطح ملی، ترسیم مخاطرات جنایی و تنظیم سیاست در هر کشوری با الهام و استفاده از سیاست ریسک‌مدار ممکن است متفاوت از سایر کشورها باشد. اگرچه هدف نهایی استقرار رویکرد ریسک‌مدار است.

۳- تصویب کنوانسیون سازمان ملل متحد برای مبارزه با جنایات سازمان‌یافته فراملی- پالرمو ۲۰۰۰، به‌عنوان جامع‌ترین سند حقوقی جهانی در حوزه مقابله با بزهکاری سازمان‌یافته یکی از نمونه‌ها برجسته همکاری‌های بین‌المللی است که بنا بر ضرورت همکاری‌ها در بعد جهانی و بکارگیری سیاست جنایی متناسب با آن تصویب شد. به‌موجب ماده ۱ کنوانسیون مزبور، هدف این کنوانسیون عبارت از ارتقاء همکاری‌ها جهت پیشگیری و مقابله مؤثرتر با جرائم سازمان‌یافته فراملی است. یکی از این جرائم، جرم پولشویی است. این جرم از این جهت که دارای ارتباط مستقیمی با سایر جرائم جهانی است در ماده ۶ کنوانسیون پالرمو مورد توجه قرار گرفته است و مطابق آن دولت‌های عضو متعهد شده‌اند که نسبت به جرم‌انگاری پولشویی در قوانین ملی خود اقدام نمایند. دیگر اقدام جامعه جهانی در زمینه مبارزه با فساد- مالی و اداری، تصویب کنوانسیون سازمان ملل متحد برای مبارزه با فساد- مریدا ۲۰۰۳ است که به‌عنوان اولین سند حقوقی بین‌المللی با هدف پیشگیری و مبارزه با عمده‌ترین مظاهر فساد مالی و اداری تدوین و تصویب شد (Mireille Delmas, 2014: 98).

هستند معرفی کرده است. دوم؛ گروه ویژه اقدام مالی تلاش کرده تا چارچوب کلی اتخاذ رویکرد ریسک‌مدار در تنظیم‌گری دارایی‌های مجازی را به‌موجب سند سال ۲۰۱۹ تشریح کند و سوم؛ اصول اساسی تنظیم‌گری در این حوزه را جهت الگوبرداری در سطوح ملی یا فراملی بیان دارد (FATF, 2019: 5).

بر این اساس، آنچه در رویکرد گروه ویژه اقدام مالی مدنظر قرار دارد شمول قوانین ملی مبارزه با پولشویی بر مخاطرات دارایی‌های مجازی است. با توجه به این که تطبیق کشورها با استانداردهای این گروه عملاً الزامی است^۱، آن‌ها باید در چارچوب قوانین ملی خود اقدامات لازم را به عمل آورند. بی‌تردید، کشور ایران نیز از این امر مستثنا نیست. از این‌رو، در نوشتار حاضر تلاش می‌شود با رویکردی توصیفی و تحلیلی ابتدا به فرآیند تکوین رویکرد ریسک‌مدار گروه ویژه اقدام مالی در زمینه دارایی‌های مجازی پرداخته شود، سپس بایدها و آثار شمول قانون مبارزه با پولشویی اصلاح شده در ۱۳۹۷ بر دارایی‌های مجازی مورد بررسی قرار گیرد.

۱. فرآیند تکوین رویکرد ریسک‌مدار گروه ویژه اقدام مالی در زمینه دارایی‌های مجازی

گروه ویژه اقدام مالی در ژوئن ۲۰۱۴ سند مربوط به «ارزهای مجازی: تعاریف و ریسک‌های بالقوه پولشویی و تأمین مالی تروریسم و پاسخ‌ها» (FATF, 2014: 12) را منتشر کرد و ضمن آن به ظهور ارزهای مجازی و سازوکار مربوط به پرداخت آن‌ها به‌عنوان یک روش نوین انتقال ارزش، از طریق اینترنت پرداخت. این گروه در ماه ژوئن سال ۲۰۱۵، نیز به‌موجب راهنمای مربوط به «رویکرد ریسک‌مدار در برابر ارزهای مجازی» (FATF, 2015) به‌عنوان بخشی از رویکرد مقدماتی در برابر ریسک پولشویی و تأمین مالی تروریسم در ارتباط با ابزارها و خدمات نوظهور 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 در سال-های اخیر، فضای دارایی‌های مجازی را در بردارنده طیف جدیدی از ابزارها و خدمات، مدل‌های تجاری، فعالیت‌ها و تعاملاتی از جمله تراکنش‌های دارایی‌های مجازی کرده است که ارزهای

۱- در صورت عدم همکاری، کشورها بر ریسک محسوب شده و تحت اقدامات مقابله‌ای موضوع توصیه شماره ۱۹ گروه ویژه اقدام مالی قرار خواهند گرفت.

مجازی نیز به عنوان بخشی از آن محسوب می‌شود. در واقع توسعه مصداقی ابزارهای مبتنی بر فن-آوری رمزنگاری^۱ منجر به ایجاد آشکال گوناگونی از دارایی‌ها بر پایه این فن‌آوری و به تبع آن برخی ابزارهای فن‌آورانه مرتبط و مشاغل، مانند ارائه‌دهندگان خدماتی چون تبدیل و صرافی‌های دارایی‌ها و ارزها، شده است.^۲

از این رو، با توجه به توسعه ابزارها و خدمات و معرفی انواع جدیدی از ارائه‌دهندگان خدمات در این فضای مجازی، گروه ویژه اقدام مالی نیاز به ارائه توضیحات تکمیلی در مورد به کارگیری استانداردهای خود در خصوص رویکرد ریسک‌مدار در برابر پولشویی را در زمینه فن‌آوری‌های جدید و ارائه‌دهندگان آن ضروری دانست. به‌طور خاص در اکتبر سال ۲۰۱۸، گروه مزبور به تعریف دو واژه جدید «دارایی‌های مجازی» و «ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی» و روزآمد کردن توصیه شماره ۱۵^۳ خود پرداخت. هدف از اعمال این تغییرات از یک سو، آشکار کردن کاربرد توصیه‌های گروه ویژه اقدام مالی در خصوص فعالیت‌های مربوط به دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن است تا شرایط را برای ایجاد چارچوب تنظیم‌گری در خصوص این ارائه‌دهندگان فراهم سازد و از سوی دیگر، به کشورها جهت کاهش

1- Encryption/Cryptography

۲- بدین سان، فضای دارایی‌های مجازی با افزایش ناگهانی رمزارزها، گمنام‌سازها، پلتفرم‌های غیرمتمرکز و صرافی‌ها و دیگر ابزارها و خدماتی که قابلیت کاهش شفافیت و افزایش تداخل جریان‌های مالی را دارند و نیز ظهور مدل‌های تجاری مجازی یا فعالیت‌های چون عرضه سکه‌های اولیه (Initial Coin Offerings (ICOs)) که در بردارنده ریسک کلاهبرداری و دستکاری بازار است رو به رو شده است. امری که زمینه‌ساز شکل‌گیری فن‌آوری‌های مالی غیرقانونی نوین و توسعه آنها نیز شده که با افزایش استفاده از سامانه‌های مجازی انجام معاملات را با اهدافی مجرمانه به شیوه‌های آسان، ارزان و امن ارائه می‌کنند.

۳- توصیه اصلاحی شماره ۱۵ بیان می‌دارد: «کشورها و مؤسسات مالی باید ریسک‌های پولشویی و تأمین مالی تروریسم که در ارتباط با: الف. عرضه محصولات جدید و نیز رویه‌های جدید مورد استفاده در مشاغل از جمله سازوکارهای جدید برای تحویل کالا؛ و ب. استفاده از فن‌آوری‌های جدید یا در حال توسعه برای محصولات جدید و محصولات قبلی، بروز پیدا می‌کنند را مورد شناسایی و ارزیابی قرار دهند. در مورد مؤسسات مالی، این نوع ریسک باید پیش از عرضه محصولات جدید، اعمال رویه‌های جدید کسب و کار و یا استفاده از فن‌آوری‌های جدید یا در حال توسعه، انجام شود. مؤسسات مالی باید برای مدیریت و کاهش این گونه ریسک‌ها، تدابیر مناسب اتخاذ کنند.

برای مدیریت و کاهش ریسک‌های ناشی از دارایی‌های مجازی، کشورها باید اطمینان حاصل کنند که ارائه‌دهندگان خدمات دارایی مجازی برای اهداف ضد پولشویی و ضد تأمین مالی تروریسم مجوز خواهند گرفت، ثبت می‌شوند و مشمول سامانه‌های مؤثر برای نظارت و اطمینان از رعایت اقدامات مرتبط با توصیه‌های گروه ویژه اقدام مالی قرار می‌گیرند».

مخاطرات پولشویی و تأمین مالی تروریسم مرتبط با دارایی‌های مجازی کمک نماید. در این راستا، در ژوئن ۲۰۱۹، گروه ویژه اقدام مالی با روزآمد کردن سند سال ۲۰۱۵ و افزودن یک یادداشت تفسیری به توصیه شماره ۱۵ (FATF, 2019: 15) تلاش کرد تا به تشریح این امر پردازد که چگونه الزامات این نهاد باید در رابطه با دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن اعمال شود. در این چارچوب، هدف این است تا زمینه برای تحقق رویکرد ریسک-مدار، با الزاماتی چون ضرورت اخذ مجوز، اتخاذ تدابیر پیشگیرانه همچون شناسایی مشتری، ثبت سوابق و ارائه گزارش‌های مشکوک، نظارت و کنترل و برخی الزامات مهم دیگر مانند همکاری-های بین‌المللی فراهم شود. امری که با توجه به کارکردهای اقتصادی ارزهای مجازی از منظر این گروه در تلاش است تا رویکرد تنظیم‌گری آن را تبیین نماید (FATF, 2019: 15).

بر این اساس از یک سو، تلاش جهت ایجاد در کی صحیح در خصوص مقررات‌گذاری و پاسخ‌گذاری‌های نظارتی در مورد دارایی مجازی و ارائه‌دهندگان خدمات مربوط به آن در میان مقامات ملی و از سوی دیگر، اشخاص خصوصی که تمایل به ورود در این حوزه‌ها را دارند مدنظر قرار دارد تا با الزامات مربوط به مبارزه با پولشویی و تأمین مالی تروریسم و چگونگی اعمال مؤثر این الزامات در این زمینه آشنا شوند (Ibid). در این چارچوب، آنچه در وهله اول باید تبیین شود، این نکته است که چگونه دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن مشمول توصیه‌های گروه ویژه اقدام مالی قرار می‌گیرند. امری که به واسطه تعریف دارایی‌های مجازی، ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی و بیان مثال‌هایی از فعالیت‌های مرتبط با دارایی مجازی در سند مزبور، مورد توجه قرار گرفته است و می‌توان از آن به‌عنوان پیش شرط لازم برای اعمال توصیه‌ها در این زمینه یاد کرد.

سپس توصیف کارکرد توصیه‌های گروه ویژه اقدام مالی به کشورها و مقامات صالح و همچنین به ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی و سایر اشخاص موظف درگیر در فعالیت دارایی‌های مجازی، شامل نهادهای مالی از قبیل بانک‌ها و چگونگی اعمال توصیه‌ها در این

۱- سند سال ۲۰۱۹ روزآمد شده سند سال ۲۰۱۵ با عنوان رویکرد ریسک‌مدار FATF به ارزهای مجازی است. نک:

<http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html>

حوزه اهمیت می‌یابد. در این چارچوب، نگاه گروه ویژه اقدام مالی این است که تمامی توصیه‌ها به طور مستقیم در خصوص خطرات پولشویی دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن کاربرد دارد؛ اگرچه در توصیه‌ها به طور صریح از این دارایی‌ها و ارائه‌دهندگان خدمات مرتبط با آن نامی برده نشده است. در واقع، از دیدگاه این گروه، می‌توان ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی را مشمول مشاغل و حرفه‌های غیرمالی معین^۱ مذکور در توصیه‌های خود دانست^۲ که موظف به اجرای الزامات مبارزه با پولشویی هستند.

پس از توجیه شمول توصیه‌های گروه ویژه اقدام مالی بر دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن، راهنمای مزبور اقدام به تشریح جزئیات طیف وسیعی از الزامات مربوط به دارایی‌های مجازی و ارائه‌دهندگان آن می‌نماید. این امر به وضوح روشن می‌سازد که مفهوم وجوه و ارزش در توصیه‌های گروه ویژه اقدام مالی (به‌عنوان مثال اموال، درآمدها، وجوه و سایر دارایی‌ها) شامل دارایی مجازی نیز می‌شوند. در نتیجه کشورها باید اقدامات لازم را ذیل توصیه‌های گروه ویژه اقدام مالی در خصوص دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی به عمل آورند.

در این راستا، راهنمای مذکور، الزامات ثبت نام و صدور مجوز برای ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی را تشریح می‌کند، به‌ویژه نحوه تعیین اینکه این عمل در کدام کشور یا کشورها باید انجام شود، برای نمونه در جایی که این دارایی‌ها ایجاد شده باشند یا قلمرو ملی که در آن مورد معامله قرار می‌گیرند. با این حال، هر حوزه قضایی می‌تواند الزام به ثبت نام یا دریافت مجوز را در قلمرو خود الزامی نماید.^۳ در این زمینه، تأکید راهنما بر این است که مقامات

1- Designated Non-Financial Businesses and Professions (DNFBPs)

^۲ این امر با توجه به توصیه شماره ۲۲ گروه ویژه اقدام مالی و توصیف و تشریح مشاغل و حرفه‌های غیرمالی معین قابل استنباط است (FATF, 2021: 19).

^۳ بر این اساس، کشورها باید اقدامات و سازوکارهای لازم جهت دریافت مجوز فعالیت توسط صرافی‌ها/ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی را فراهم سازند. امری که می‌تواند در عمل منجر به ایجاد انضباط در فعالیت این اشخاص شود. برای نمونه، تا مدت‌ها استفاده از خدمات صرافی بایننس binance به عنوان بزرگترین صرافی فعال در عرصه دارایی‌های مجازی، نیازمند احراز هویت از جانب کاربران نبود. با این حال، اعمال برخی قواعد بر صرافی‌ها، این صرافی را ناگزیر ساخته تا جهت مواجه نشدن با ضمانت اجراهای مشخص شده، جهت ادامه فعالیت، احراز هویت کاربران را پیش شرط ارائه خدمات به

ملی باید اقدام به شناسایی اشخاص حقیقی یا حقوقی که در نقل و انتقال دارایی، بدون ثبت نام و دریافت مجوز، فعال هستند بپردازد. این امر زمانی قابل اعمال خواهد بود که دارایی‌های مجازی در سطح ملی مورد پذیرش قرار گیرند و سپس چنین محدودیت‌هایی بر آنها اعمال شود.^۱

۲. بایدها و آثار شمول قانون مبارزه با پولشویی در زمینه دارایی‌های مجازی

با توجه به رویکرد گروه ویژه اقدام مالی آنچه مدنظر این گروه قرار دارد شمول قوانین ملی مبارزه با پولشویی بر دارایی‌های مجازی است. از این رو ضروری است تا کشورها با انجام اصلاحاتی در قوانین خود به نحو مؤثری قواعد مبارزه با پولشویی را به دارایی‌های مجازی تسری دهند؛ امری که بی‌شک نیازمند مقدماتی است. به همین دلیل بررسی قانون مبارزه با پولشویی اصلاح شده ۱۳۹۷ از اهمیت برخوردار است تا مشخص شود جهت شمول این قانون بر دارایی‌های مجازی چه بایدهایی وجود خواهد داشت و آثار اجرای آنها چیست. در این راستا، نخست شناسایی ارزشهای مجازی به عنوان یک ارزش و دوم، شناسایی هنجارمندان ارائه‌دهندگان خدمات مربوط به دارایی‌هایی مجازی به عنوان بایدهای شمول قانون مبارزه با پولشویی در زمینه دارایی‌های مجازی و در نهایت آثار شمول این قانون بر فن آوری مذکور بررسی خواهد شد.

۲.۱- شناسایی دارایی‌های مجازی به عنوان یک ارزش

یکی از مهم‌ترین الزامات جهت شمول قوانین مبارزه با پولشویی بر دارایی‌های مجازی، قانونی-سازی ابعاد گوناگون این فن آوری است. بر این اساس، تا دارایی‌های مجازی از منطقه خاکستری

آنها نماید. نمونه دیگر، بررسی تراکنش‌های مشکوک به فعالیت‌های مجرمانه است که این صرافی به‌طور فعالی به رصد آنها می‌پردازد و مورد مشکوک را به اطلاع مقامات ذیصلاح می‌رساند. بنگرید: تاریخ مشاهده ۱۴۰۰/۰۹/۱۰

<https://academy.binance.com/en/articles/what-is-anti-money-laundering-aml>

۱- افزون بر این، راهنما به‌طور شفاف بیان می‌دارد که ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی و دیگر نهادهای درگیر در فعالیت دارایی‌های مجازی، باید تمام اقدامات پیشگیرانه ارائه‌شده در توصیه‌های ۱۰ تا ۲۱ گروه ویژه اقدام مالی را اعمال نمایند. راهنما توضیح می‌دهد که چگونه این وظایف باید در مورد دارایی‌های مجازی در پرتو توصیه ۱۰ به منظور شناسایی کامل مشتریان و با توجه به توصیه ۱۶ مبنی بر الزام دریافت، نگهداری، انتقال فوری و ایمن اطلاعات ضرورت یابد.

قانونی وارد حیطه قانون‌گذاری نشوند نمی‌توان قوانین و قواعد الزامی را بر آن‌ها بار کرد.^۱ از این رو، جهت آنکه دارایی‌های مجازی موضوع تعهدات مبارزه با پولشویی واقع شوند، قرار گرفتن آن‌ها در دایره کثی ارزشمند؛ خواه یک وجه یا مال، ضرورت دارد. در واقع، جرم پولشویی باید هر نوع مالی را صرف‌نظر از ارزش آن در برگیرد. امری که در توصیه شماره ۳ گروه ویژه اقدام مالی، با توجه به کنوانسیون پالرمو مورد توجه قرار گرفته است. جرم پولشویی در کنوانسیون پالرمو از یک سو، شامل تبدیل یا انتقال اموال به منظور مخفی کردن یا تغییر ظاهر منشأ غیر قانونی آن‌ها یا کمک به شخصی که در ارتکاب جرم منشأ مشارکت داشته است به منظور فرار از عواقب قانونی عملش با علم به این که اموال مزبور عواید حاصل از جرم است می‌شود. از سوی دیگر، این عنوان مواردی را در برمی‌گیرد که شامل مخفی نمودن یا تغییر ظاهر، ماهیت، منشأ، محل، موقعیت، جابه‌جایی یا مالکیت یا حقوق متعلق به اموال با آگاهی از آن که اموال مزبور عواید حاصل از جرم است. از این رو، ضروری است تا مفهوم مال شامل دارایی‌های مجازی نیز گردد و با اثبات این امر که این اموال؛ دارایی‌های مجازی، عوائد حاصل از جرم هستند، بدون نیاز به محکومیت دارنده به ارتکاب جرم منشأ، محکومیت دارنده با وجود سایر شرایط (مانند علم به مجرمانه بودن منشأ) برای تحقق عنوان پولشویی کفایت کند (Laurent, et al., 2017: 17). بدین ترتیب، با شمول عنوان مال، دارایی یا سرمایه بر دارایی‌های مجازی و از جمله ارزش‌های مجازی، تعهدات مربوط به مبارزه با پولشویی و تأمین مالی تروریسم به دارایی‌های مجازی گسترش می‌یابد.^۲ امری که بی‌تردید از پشتوانه نظری برخوردار است و در چارچوب مکاتب اقتصادی، به‌عنوان

۱- وضعیت قانونی دارایی‌های مجازی هنوز یک منطقه خاکستری به‌شمار می‌رود. اگرچه ممکن است برخی از اقسام آن مانند بیت‌کوین قابلیت تبدیل به ارزهای سنتی، مانند دلار آمریکا یا یورو را داشته باشد، اما هنوز در بسیاری از کشورهای به‌عنوان پول شناخته نشده است. بر این اساس، یکی از استدلال‌های اولبرایچ متهم ردیف اول در پرونده جاده ابریشم؛ به‌عنوان بزرگترین بازار برخط مجرمانه، در دفاع از خود در برابر اتهام به پولشویی، این بود که او در پولشویی دخالت نمی‌کند، زیرا معاملات در جاده ابریشم «معاملات مالی» نبودند. همچنین فیلا، صراف بیت‌کوین در بازار مزبور، استدلال کرد که رفتار وی انتقال غیرقانونی پول نقد نیست؛ زیرا بیت‌کوین پول نیست، بنابراین او فرستنده پول محسوب نمی‌شود (Saffari, et al., 2020: 233). Kethineni, et al., 2018:150.

۲- در این راستا، توصیه شماره ۵ گروه ویژه اقدام مالی نیز قابل توجه است. بر اساس این توصیه کشورها در مقام الزام به جرم-انگاری تأمین مالی تروریسم موظف شده‌اند تا هر نوع مالی را، چه از منشأ قانونی و چه از منشأ غیرقانونی برخوردار باشد،

مهم‌ترین بُعد، توجیه شده است. بر این اساس، ویژگی‌های دارایی‌های مجازی افرون‌بر آنکه این فن آوری را در شمار یک ارزش قرار می‌دهد، کارکرد پولی این فن آوری آن را در چارچوب نظریه جایگزینی^۱، به‌عنوان نسل جدیدی از پول مطرح کرده است. از این رو، به نظر می‌رسد تمایل عمومی جهت ورود به بازار دارایی‌های مجازی و کسب و ذخیره آن با اهداف سرمایه‌گذاری و تجارت و ذات ارزشمند فن آوران آن بحثی در خصوص ارزش این فن آوری باقی نگذارد. ضمن آنکه، مفهوم دارایی‌های مجازی صرفاً شامل یک یا چند نوع رمز ارز خاص نیست. این مفهوم و ضرورت مقرر گذاری پیرامون آن به مراتب گسترده‌تر از چند مصداق مشخص است. امری که شناسایی آن به‌عنوان یک ارزش را اجتناب‌ناپذیر می‌سازد.

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 در تعریفی نسبتاً مشابه، مال را هر نوع دارایی، وجوه یا منابع اقتصادی اعم از مادی یا غیرمادی، محسوس یا غیرمحسوس... تعریف کرده‌اند. در خصوص اینکه آیا دارایی‌های مجازی در چارچوب تعریف مذکور قرار می‌گیرد یا خیر از حیث حقوقی و فقهی اختلافاتی در کشور وجود دارد (Roshan, et al., 2019: 49-8). امری که می‌توانست با اصلاحات صورت گرفته در قانون مبارزه با قاچاق کالا و ارز در سال ۱۳۹۹ و شناسایی رمز ارزها به‌عنوان ارز خارجی پایانی بر تمامی اختلافات باشد. در این راستا، قانون‌گذار جهت شناسایی قانونی رمز ارزها در لایحه اصلاحی قانون مبارزه با قاچاق کالا و ارز در سال ۱۳۹۹ ابتدا تبصره ۷ ماده ۲ مکرر الحاقی را به تصویب رساند. این تبصره مقرر می‌داشت: «تمامی رمز ارزها (ارزهای رقمی) در حکم ارز موضوع این قانون هستند و جرائم، تخلفات، ضمانت اجراها و نیز تمامی احکام و مقررات مربوط به ارز در این قانون در مورد آن‌ها نیز اجرا می‌شود».

با این حال با توجه به برخی ایرادات شورای نگهبان، متن تبصره اصلاح شد. متن اصلاحی

موضوع این جرم قرار دهند. در واقع، هر مالی که برای تأمین مالی تروریسم اختصاص داده شد مشمول توصیه شماره ۵ می‌شود. بدین سان، دارایی‌های مجازی و از جمله ارزهای مجازی به عنوان یک مال یا ارزش، جدا از این که از منشاء قانونی به دست آمده‌اند یا از منشاء غیرقانونی، زمانی که جهت تأمین مالی تروریسم اختصاص داده شوند، مشمول تعهدات مبارزه با تأمین مالی تروریسم کشورها قرار خواهند گرفت.

۱- در این زمینه بنگرید: (Shamloo and Khalili Paji, 2020 [C])

مجلس مصوب ۱۴۰۰/۰۱/۲۴ که به شورای نگهبان ارسال شده به این شرح است: «رمز ارز (ارز رقومی) نوعی اسناد الکترونیکی موضوع بند «پ» ماده (۱) این قانون است که بر بستری دیجیتال (رقومی)، غیرمتمرکز و شفاف به نام زنجیره بلوک (بلاک چین) موجودیت می‌یابد و بدین لحاظ ارز محسوب و مشمول مقررات بندهای «پ»، «ت»، «ث»، «ج» و «چ» این ماده است.»

بر این اساس، قانون‌گذار بنا داشت با شناسایی رمز ارزها به‌عنوان ارز خارجی، آن‌ها را مشمول قوانین و مقررات ارزی کشور قرار دهد. امری که می‌توانست امکان شمول قوانین قاچاق ارز را در برخی فروض بر برخی اعمال مرتبط با رمز ارزها فراهم سازد. نقد این رویکرد خارج از حوصله نوشتار حاضر است اما باید توجه داشت که شناسایی قانونی این دارایی عملاً منجر به شمول قوانین مبارزه با پولشویی ایران بر این فن‌آوری می‌شود. جدا از انتقادات مربوط به شمول قوانین ارزی بر رمز ارزها و الحاق آن به قانون مبارزه با قاچاق کالا و ارز، ایراد دیگری که به تبصره مزبور وارد بود، توجه به رمز ارزها به جای توجه به دارایی‌های مجازی است. از این رو، افزون‌بر اینکه از حیث مکان‌یابی تقنینی، ایده‌آل‌ترین حالت ممکن الحاق چنین مقرره‌ای به قانون مبارزه با پولشویی است، رویکرد صحیح‌تر شناسایی دارایی‌های مجازی به جای صرف شناسایی رمز ارزها است؛ زیرا رمز ارزها مصداقی از دارایی‌های مجازی هستند و طبیعتاً شامل سایر مصادیق این دارایی‌ها نخواهند شد. نکته‌ای که عدم توجه به آن در عمل می‌تواند منجر به ایجاد خلأ قانونی در خصوص سایر مصادیق دارایی‌های مجازی شود. از این رو، قانون‌گذار می‌توانست در قانون مبارزه با پولشویی با ایجاد اصلاحاتی در بند «ب» ماده ۱، به دارایی‌های مجازی به‌عنوان مصداقی از مال تصریح نماید و سپس، آن را تعریف کند. با این وجود، حذف بی‌مقدمه تبصره مزبور در آخرین نسخه اصلاحات توسط مجلس شورای اسلامی، همچنان از حیث قانونی شناسایی این فن‌آوری را در یک برزخ رویکردی قرار داده است. بر این اساس، می‌توان با استفاده از این فرصت، با برطرف کردن مشکلات تعریف قانونی مزبور، تعریف پیشنهادی از دارایی‌های مجازی با توجه به سند گروه ویژه اقدام مالی را بدین شرح ارائه کرد: «دارایی مجازی بازنمایی دیجیتالی (رقومی) از ارزشی است که به‌صورت غیرمتمرکز و شفاف می‌تواند با هدف پرداخت یا سرمایه‌گذاری به‌صورت دیجیتالی مورد معامله قرار گیرد یا انتقال داده شود؛ از قبیل رمز ارزها که بر بستر زنجیره بلوک (بلاک چین) مبتنی بر علم رمزنگاری موجودیت دارند». طبیعی است مناسب‌ترین مکان تقنینی برای این مقرره نیز، همان‌طور که گذشت، قانون مبارزه با پولشویی است.

۲.۲- شناسایی هنجارمندانه ارائه‌دهندگان خدمات مربوط به دارایی‌هایی مجازی

هدف نهایی توصیه‌های گروه ویژه اقدام مالی، الزام کلیه دولت‌ها به اعمال استانداردهای خاص مربوط به مبارزه با پولشویی در خصوص نهادهای مالی و غیرمالی است. امری که تمامی اشخاصی که ذیل نهادهای مزبور قرار می‌گیرند شامل می‌شود. بر این اساس، جهت شمول قوانین مبارزه با پولشویی بر دارایی‌های مجازی افزون بر شناسایی قانونی این فن‌آوری، ضروری است تا نهادهای ارائه‌دهنده خدمات مربوط به آن نیز مورد شناسایی قرار گیرند. به‌طور کلی در خصوص فعالیت‌های مرتبط با دارایی‌های مجازی، نهادهای موظف به اجرای تعهدات مبارزه با پولشویی در چند دسته قرار می‌گیرند که تمامی آن‌ها مکلف‌اند در چارچوب رویکرد ریسک‌مدار، به اجرای توصیه‌های گروه ویژه اقدام مالی بپردازند. سه دسته از این نهادها؛ یعنی نهادهای مالی^۱، نهادهای غیرمالی^۲ و سازمان‌های غیرانتفاعی، در توصیه‌های چهارگانه گروه ویژه اقدام مالی مورد اشاره قرار گرفته است و دسته جدیدی تحت عنوان ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی نیز به‌موجب واژه‌نامه جدید گروه مزبور و اصلاح توصیه شماره ۱۵ و تفسیر نگاشته آن ایجاد شده است. در خصوص سه دسته اول اصول فعالیت مشخص است. این نهادها معمولاً در تمامی کشورها تعریف شده‌اند و قوانین و ضوابط خاص و مرتبط با آن‌ها در زمینه مبارزه با پولشویی وجود دارد. بر این اساس، چنانچه این نهادها بخواهند در حوزه دارایی‌های مجازی فعالیت داشته باشند باید

۱- در آیین‌نامه اجرایی قانون مبارزه با پولشویی مصوب ۱۳۹۸ از اصطلاح «مؤسسات مالی و اعتباری» به عنوان معادل Financial Institutions استفاده شده است؛ به نظر می‌رسد با توجه به این که اصطلاح «مؤسسات مالی و اعتباری» در حقوق ایران یک اصطلاح رایج بوده که شامل شرکت‌های لیزینگ، صرافی‌ها، بورس‌ها، بیمه‌ها، شرکت‌های ارائه دهنده خدمات پرداخت و غیره نمی‌شود و از طرفی عبارت Financial Institutions علاوه بر مؤسسات مالی و اعتباری، موارد مذکور را نیز در بر می‌گیرد. از این رو، بهتر است برای معادل‌سازی از واژه «نهادهای مالی» استفاده شود.

۲- در قانون مبارزه با پولشویی مصوب ۱۳۸۶ اصلاحی ۱۳۹۷ و آیین‌نامه اجرایی آن مصوب ۱۳۹۸ از اصطلاح «مشاغل غیر مالی» به عنوان معادل Designated Non-Financial Businesses And Professions (DNFBPs) استفاده شده است و شرکت‌های لیزینگ، صرافی‌ها و موارد دیگری که در زمره این اشخاص طبقه‌بندی نمی‌شوند، به اشتباه وارد مصادیق این تعریف شده و بالعکس موارد نظیر وکلا و حساب‌برسان که باید در این دسته طبقه‌بندی شوند، در تعریف ارائه شده قرار نمی‌گیرند. اگرچه ترجمه صحیح این عبارت «تجارت‌ها و حرفه‌های غیرمالی معین» است؛ اما به منظور سهولت در کاربرد آن در ادبیات مبارزه با پولشویی ایران به نظر می‌رسد عبارت «نهادهای غیر مالی» مناسب‌تر باشد، از این رو در این نوشتار از این معادل استفاده شده است.

تمامی الزامات مبارزه با پولشویی ملی را مطابق قوانین داخلی اعمال نمایند. در واقع، جهت انجام وظایف مربوطه توسط این سه دسته، صرف شناسایی قانونی دارایی‌های مجازی کفایت می‌کند. با این حال، گسترش استفاده از دارایی‌های مجازی منجر به ایجاد دسته‌ای جدید از ارائه‌دهندگان خدمات شده است که به‌طور تخصصی و حرفه‌ای در زمینه دارایی‌های مجازی و از جمله ارزش‌های مجازی فعالیت دارند. منظور از «ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی» نیز اشخاصی هستند که یک یا چند فعالیت ذیل را به نمایندگی از اشخاص دیگر انجام می‌دهند: ۱. مبادله بین دارایی‌های مجازی و ارزش‌های فیات (ملی)؛ ۲. مبادله بین یک یا چند نوع دارایی مجازی؛ ۳. نقل و انتقال^۱ دارایی‌های مجازی؛ ۴. نگهداری و 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).

باید توجه داشت که مطابق تعریف گروه ویژه اقدام مالی، دامنه تعریف شامل معاملات و فعالیت‌های اقتصادی مجازی-مجازی یا مجازی-فیات می‌شود. از این رو، بسته به فعالیت‌های مالی خاص آن‌ها، ارائه خدمات مالی مربوط به دارایی‌های مجازی شامل تبادلات دارایی‌های مجازی، خدمات انتقال، ارائه خدمات کیف پول ارزی، خدمات مربوط به صدور، ایجاد یا فروش دارایی‌های مجازی است.

هنگام تعیین این که یک فعالیت یا نهاد خاص در محدوده تعریف ارائه‌دهنده خدمات مرتبط با دارایی‌های مجازی قرار می‌گیرد و مشمول مقررات مربوط می‌شود یا خیر، دولت‌ها باید طیف گسترده‌ای از خدمات مختلف، دارایی‌ها یا مدل‌های تجاری که در ساختار دارایی‌های مجازی وجود دارند و به‌ویژه عملکرد آن‌ها یا فعالیت‌های مالی را که موجب تسهیل فعالیت‌های مرتبط می‌شوند را در نظر بگیرند (FATF, 2019).

بدین سان، کشورها باید بر روی رفتارهای مالی و فعالیت‌های مرتبط با دارایی‌های مجازی و فن آوری زیربنایی آن و چگونگی ایجاد خطرات پولشویی و تأمین مالی تروریسم (به‌عنوان مثال، ظرفیت افزایش ناشناس ماندن، گمنامی و کاهش شفافیت) از جانب آن تمرکز نمایند و در این

۱- در این زمینه، نقل و انتقال به معنای انجام یک معامله از طرف هر شخص حقیقی یا حقوقی در زمینه اموال مجازی است.

زمینه تدابیری اتخاذ کنند. از این رو، ضروری است تا ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی نیز به‌عنوان یکی از اشخاص مشمول قانون مبارزه با پولشویی-مشاغل غیرمالی- در بند «ث» ماده ۱ شناسایی شوند. با این حال، این امر پایان کار نخواهد بود. ضروری است تا ضوابط لازم برای این دسته از اشخاص نیز پس از مشخص شدن متولی، به‌موجب دستورالعمل‌های مربوط به تصویب برسد. برای نمونه می‌توان به «دستورالعمل اجرایی تأسیس، فعالیت و نظارت بر صرافی‌ها» مصوب مرداد ۱۳۹۳ اشاره کرد که به‌طور خاص، مقررات مربوط به تشکیل، طرز کار و ضمانت‌اجراه‌های مرتبط توسط صرافی‌های ارزی را مشخص کرده است. بر این اساس، پس از مشخص شدن متولی تدوین و تصویب دستورالعمل، باید اقدام به تصویب دستورالعملی مشابه در خصوص ارائه-دهندگان خدمات مربوط به دارایی‌های مجازی پرداخت.

۲.۳- آثار شمول قانون مبارزه با پولشویی بر دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن
بی‌تردید با شناسایی قانونی دارایی‌های مجازی به‌عنوان یک ارزش و ارائه‌دهندگان خدمات مربوط به آن به‌عنوان یکی از مشاغل غیرمالی مشمول قانون، طیف گسترده‌ای از الزامات موجود در قانون مبارزه با پولشویی اصلاحی ۱۳۹۷ و آیین‌نامه اجرایی ۱۳۹۸ این قانون بر آن‌ها بار خواهد شد. از این رو، چنین امری دارای آثاری خواهد بود.

بدیهی‌ترین اثر این است که با شمول عنوان مال بر دارایی‌های مجازی، حسب مورد امکان شمول عنوان «مال حاصل از جرم» مطابق بند «پ» ماده ۱ قانون مبارزه با پولشویی اصلاحی ۱۳۹۷ بر این فن‌آوری وجود خواهد داشت. بر این اساس، چنانچه این دارایی‌های به‌طور مستقیم یا غیرمستقیم از جرم منشأ به دست آیند مال حاصل از جرم محسوب می‌شوند و ارتکاب هر کدام از رفتارهای مادی موضوع ماده ۲ قانون مبارزه با پولشویی (مانند تبدیل، انتقال و...) می‌تواند با وجود سایر شرایط، اتهام پولشویی را در خصوص اعمال مرتبط با این اموال قابل طرح نماید.

بر این اساس، با شمول عنوان مال بر دارایی‌های مجازی افزون‌بر اینکه این فن‌آوری در زمره ارزش‌های موضوع جرم پولشویی قرار می‌گیرد، مشمول جرم نقض مقررات مبارزه با پولشویی نیز به‌عنوان جرمی خاص نیز قرار خواهد گرفت. بر این اساس، الزامات این حوزه و ضمانت‌اجرای عدم انجام آن بر ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی بار خواهد شد. این امر، در بردارنده طیف وسیعی از الزامات است که در برخی کشورها نیز از نمونه‌هایی برخوردار است. در

استرالیا، اشخاص درگیر در قرایندها مبادله دارایی‌های مجازی موظف به ثبت معاملات و سوابق آن (همچون مقدار فیات، مشخصات هویتی طرفین و...) هستند. از این رو، چنانچه این الزامات از سوی اشخاص موظف رعایت نشود آن‌ها با ضمانت اجراهای مشخص که در برخی موارد از جنس کیفری است روبه‌رو خواهند شد (Hughes, 2018: 12).

تکالیف مشابهی مانند مورد مذکور، مطابق ماده ۷ قانون مبارزه با پولشویی اصلاحی ۱۳۹۷ در ایران وجود دارد. اشخاص موضوع قانون مبارزه با پولشویی، همچون بانک‌ها، مکلف به انجام الزاماتی شده‌اند. این الزامات در یک نگاه کلی عبارت‌اند از شناسایی مشتری، نگهداری سوابق و ارائه گزارش عملیات مشکوک که عدم انجام این تکالیف در موارد مصرح، برای ناقضان قانون ضمانت اجراهایی (حسب مورد انفصال یا جزای نقدی) در پی خواهد داشت. در این راستا، شناسایی قانونی دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن‌ها، این نتیجه را در بردارد که تکالیف مزبور شامل آن‌ها نیز خواهد شد. برای نمونه، این اشخاص موظف‌اند چنانچه در انجام فعالیت‌های خود با موردی مشکوک مطابق بند «چ» ماده ۱ قانون مبارزه با پولشویی مواجه شوند مطابق بند «پ» ماده ۷ قانون مزبور اقدام به ارائه گزارش عملیات مشکوک^۱ به مرکز اطلاعات مالی نمایند. مرکز مزبور نیز موظف است مطابق بند «الف» ماده ۷ مکرر به بررسی این گزارش بپردازد و چنانچه احتمال قوی به ارتکاب جرم می‌دهد مطابق بند «پ» ماده مزبور، اقدام به ارسال گزارش‌ها در قالب اعلام جرم به مرجع قضایی نماید. نمونه دیگر از الزامات مربوط به گزارش‌دهی در ماده ۱۳۹ آیین‌نامه اجرایی قانون مبارزه با پولشویی آمده است. مطابق این ماده،

۱- مطابق تبصره بند «پ» ماده ۷ قانون مبارزه با پولشویی اصلاحی ۱۳۹۷: «معاملات و عملیات مشکوک شامل هر نوع معامله، دریافت یا پرداخت مال اعم از فیزیکی یا الکترونیکی یا شروع به آنها است که براساس اوضاع و احوالی مانند ارزش، موضوع یا طرفین آن برای انسان به طور متعارف ظن وقوع جرم را ایجاد کند؛ نظیر: ۱- معاملات و عملیات مالی مربوط به ارباب رجوع که به نحو فاحش بیش از سطح فعالیت مورد انتظار وی باشد. ۲- کشف جعل، اظهار کذب یا گزارش خلاف واقع از سوی مراجعان قبل یا بعد از آنکه معامله یا عملیات مالی صورت گیرد و نیز در زمان اخذ خدمات پایه. ۳- معاملات یا عملیات مالی که به هر ترتیب مشخص شود صوری یا ظاهری بوده و مالک شخص دیگری است. ۴- معاملات یا عملیات مالی که اقامتگاه قانونی هر یک از طرفین در مناطق پرخطر (از نظر پولشویی) واقع شده است. فهرست این مناطق توسط شورا مشخص می‌شود. ۵- معاملات یا عملیات مالی بیش از سقف مقرر در آیین‌نامه اجرایی. هر چند مراجعان، قبل یا حین معامله یا عملیات مزبور از انجام آن انصراف داده یا بعد از انجام آن بدون دلیل منطقی نسبت به فسخ قرارداد اقدام نمایند.»

کارکنان تحت امر اشخاص مشمول مکلف‌اند تمام تعاملات کاری بیش از سقف مقرر (خرد یا تجمیعی) را از قبیل تراکنش‌ها، انتقال وجه نقد و معاملاتی که ارباب‌رجوع وجه آن را روزانه به صورت نقدی پرداخت می‌کند، ثبت کنند و همراه با توضیحات ارباب‌رجوع که به تأیید وی رسیده است، به واحدهای مبارزه با پول‌شویی اطلاع دهند. واحدهای مذکور مکلف‌اند خلاصه برگه (فرم)‌های مربوط را در پایان هر هفته به‌نحوی که مرکز مشخص می‌سازد ارسال و اصل آن را به نحو کاملاً حفاظت‌شده نگهداری کنند.

به‌طور کلی، ارائه برخی گزارش‌ها، مانند گزارش عملیات مشکوک یکی از مهم‌ترین وظایف نهادهای مالی و غیرمالی به شمار می‌رود که در برخی اسناد بین‌المللی، مانند بند «ب» از پاراگراف ماده ۱۸ کنوانسیون مبارزه با تأمین مالی تروریسم، مورد اشاره قرار گرفته است. گروه ویژه اقدام مالی نیز به‌موجب توصیه‌های شماره ۲۰ و ۲۱ خود به ارائه گزارش عملیات مشکوک به‌عنوان یک الزام توجه داشته است. بر این اساس، چنانچه یک نهاد مالی در چارچوب فعالیت خود نسبت به وجوه یا اموالی مظنون شود که از فعالیت‌های بزه‌کارانه کسب شده یا مربوط به تأمین مالی تروریسم است، موظف خواهد بود تا ادله مربوط به ظن خود را در زمانی معقول به مرکز اطلاعات مالی^۱ گزارش دهد.

بی‌تردید افزون بر اجرای مقررات عام قانون مبارزه با پولشویی و آیین‌نامه آن، شناسایی قانونی ارائه‌دهندگان خدمات مذکور، مستلزم تهیه دستورالعمل مشخصی در خصوص تأسیس، فرایند اخذ مجوز و برخی دیگر از الزامات آن‌ها است. برای نمونه، یکی از وظایف موجود به‌موجب بند «ت» ماده ۷ برای اشخاص موظف، نگهداری سوابق مربوط به شناسایی ارباب‌رجوع، مالک، سوابق حساب‌ها، عملیات و معاملات داخلی و خارجی حداقل به مدت پنج سال است. بدیهی است در این زمینه باید سازوکار نگهداری مختص ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی مشخص شود. نمونه دیگر، که در موارد مشابه مطابق برخی دستورالعمل‌ها وجود دارد، سازوکار ثبت

۱- توصیه شماره ۲۹ گروه ویژه اقدام مالی به تشکیل واحد اطلاعات مالی به عنوان مرکز ملی دریافت و تحلیل اطلاعات اشاره دارد و از کشورها خواسته نسبت به ایجاد چنین نهادی اقدام نمایند. در ایران به موجب ماده ۷ مکرر قانون مبارزه با پولشویی اصلاحی سال ۱۳۹۷، در رویکردی مشابه با رویکرد سابق در آیین‌نامه اجرایی قانون مبارزه با پولشویی سال ۱۳۸۸، به تشکیل مرکز اطلاعات مالی اشاره شده است.

اطلاعات مربوط به معاملات است. در این چارچوب، می‌توان به سامانه «سنا» اشاره کرد. مطابق بند ۱-۱۴ دستورالعمل اجرایی مبارزه با پولشویی در صرافی‌ها مصوب ۱۳۹۰، سنا، «سامانه نظارت بر ارز» است که در بانک مرکزی مستقر بوده و صرافی‌ها موظف هستند، تمام عملیات صرافی و اطلاعات مربوط به شناسایی مشتری را در این سامانه ثبت کنند. مطابق ماده ۶ «مقررات ناظر بر عملیات ارزی صرافی‌ها» نیز کلیه صرافی‌ها موظف‌اند معاملات عمده را به صورت هم‌زمان در سامانه سنا ثبت نمایند. از این رو، زمانی می‌توان چنین تکلیفی را بر ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی بار کرد که مشابه چنین سامانه‌ای برای فعالیت‌های آن‌ها ایجاد شود. امری که با وجود مؤلفه‌های ضروری است. در واقع، مراکز ارائه‌دهنده خدمات مربوط به دارایی‌های مجازی باید مکلف شوند اطلاعات مربوط به معامله (میزان، مقدار، تاریخ و نرخ معامله)، اطلاعات هویتی معامله‌کنندگان و منشأ (دارا شدن از طریق استخراج یا طریق دیگر) یا محل مصرف دارایی مورد معامله را در سامانه نظارت دارایی‌های مجازی هم‌زمان با وقوع رویداد به ثبت برسانند. امری که می‌تواند تا حد امکان منجر به کاهش مخاطرات ناشی از ناشناختگی در فرایند فن‌آوری‌های مجازی گردد.

نتیجه‌گیری

بررسی رویکرد فراملی گروه ویژه اقدام مالی در پاسخ‌دهی به ریسک دارایی‌های مجازی نشان‌دهنده پذیرش رویکرد ریسک‌مدار در چارچوب برنامه‌های مقابله با پولشویی است. بر این اساس، کشورها تلاش می‌کنند با تحت شمول قوانین پولشویی قرار دادن دارایی‌های مجازی نسبت به کاهش مخاطرات مجرمانه این فن‌آوری اقدام نمایند. در این راستا، در ژوئن ۲۰۱۹، گروه ویژه اقدام مالی، به عنوان تخصصی‌ترین نهاد فراملی در زمینه پیشگیری و مقابله با پولشویی، به بهر روزآمد کردن دستورالعمل خود در مورد رویکرد ریسک‌مدار در برابر دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن پرداخت. دستورالعمل روزآمد شده در عمل‌الگویی پیش‌روی کشورها است تا در پرتو آن با اتخاذ برخی تدابیر و اقدامات، اصلاحات ضروری را در قوانین ضد پولشویی ملی اعمال نمایند و از گذر آن شرایط لازم جهت شمول الزامات مبارزه با پولشویی را بر دارایی‌های مجازی فراهم سازند. بی‌تردید، پیش شرط این امر، شناسایی قانونی دارایی‌های مجازی و

ارائه‌دهندگان خدمات مربوط به آن است؛ امری که در دستور کار بسیاری از کشورها قرار گرفته است.

در ایران نیز با توجه به کاربرد گسترده دارایی‌های مجازی، به‌ویژه رمز ارزها، طی سال‌های اخیر و ضرورت قانون‌مندی ابعاد گوناگون آن، تلاش‌هایی جهت وضع مقررات مربوط آغاز شده است. اگرچه این امر تاکنون به سرانجام مشخصی نرسیده اما جهت شمول دقیق قانون مبارزه با پولشویی، شناسایی قانونی دارایی‌های مجازی و ارائه‌دهندگان خدمات مربوط به آن که از کارکردی چون صرافی برخوردارند، همچنان مهم‌ترین نیاز کشور در این حوزه است؛ امری که با توجه به توصیه‌های گروه ویژه اقدام مالی از اهمیت فراوانی برخوردار است. بر این اساس، زمانی می‌توان مخاطرات جنایی رمز ارزها را به شکل مناسبی مهار کرد که چنین الزاماتی مدنظر قانون‌گذار قرار گیرد. اهمیت این امر زمانی دو چندان می‌شود که بدانیم با شناسایی قانونی ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی، جهت شمول قوانین مبارزه با پولشویی بر آن‌ها، وضع مقررات خاص در خصوص تأسیس، فعالیت و نظارت بر این اشخاص ضروری است. بر این اساس، گام نخست، تعریف ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی است. تعریف پیشنهادی این ارائه‌دهندگان با توجه به دستاوردهای این پژوهش به این شرح است: «ارائه‌دهندگان خدمات مربوط به دارایی‌های مجازی اشخاصی هستند که یک یا چند فعالیت از قبیل فعالیت‌های ذیل را به نمایندگی از اشخاص دیگر انجام می‌دهند: ۱. مبادله بین دارایی‌های مجازی و ارزهای فیات (ملی)؛ ۲. مبادله بین یک یا چند نوع دارایی مجازی؛ ۳. نقل و انتقال دارایی‌های مجازی؛ ۴. نگهداری و 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».

افزون بر این، همان‌طور که بیان شد، با توجه به ضرورت تدوین برخی مقررات خاص در حوزه دارایی‌های مجازی، ضروری است تا دستورالعملی با توجه به برخی موارد در دستور کار قرار گیرد. این دستورالعمل باید در بردارنده برخی نکات اساسی در خصوص ارائه‌دهندگان خدمات دارایی مجازی باشد. نخست آنکه، ضوابط اجرایی تأسیس این اشخاص را معین نماید. برای نمونه می‌توان پیشنهاد کرد که تأسیس مراکز ارائه‌دهنده خدمات مربوط به دارایی‌های مجازی، توسط مؤسسات اعتباری صرفاً در قالب شرکت سهامی خاص و توسط اشخاص حقیقی در قالب شرکت تضامنی امکان‌پذیر باشد. در هر دو صورت باید اخذ مجوز از مرجع ذی صلاح جهت ارائه خدمات

مربوط به دارایی‌های مجازی ضروری باشد. همچنین ضروری است که بر این نکته تأکید شود که مسئولیت صحت عملکرد پلتفرم مراکز و تضمین ملاحظات امنیتی آن بر عهده مراکز است؛ مراکز ارائه‌دهنده خدمات مربوط به دارایی‌های مجازی موظف‌اند به منظور انجام معاملات خود از سامانه برخط امن با تأیید مراجع ذیصلاح اقدام نمایند و مقرر شود که رعایت تکالیف مربوط به مشاغل غیرمالی موضوع بند «ث» ماده ۱ قانون مبارزه با پولشویی اصلاحی ۱۳۹۷ و آیین‌نامه اجرایی آن برای ارائه‌دهندگان خدمت فوق الزامی است. همچنین مناسب است بر این نکته نیز تأکید شود که مراکز مزبور می‌توانند خدمات مربوط به نگهداری دارایی‌های مجازی را در چارچوب کیف پول-های مجازی ارائه نمایند؛ با این شرط که تأمین امنیت این کیف پول‌ها با رعایت الزامات امنیتی ابلاغی از مراجع ذیصلاح بر عهده مراکز باشد.

علاوه بر این، برخی موارد دیگر نیز ضروری است در دستورالعمل مزبور مورد تأکید قرار گیرد. برای نمونه لازم است مراکز ارائه‌دهنده خدمات مربوط به دارایی‌های مجازی مکلف شوند اطلاعات مربوط به معامله (میزان، مقدار، تاریخ و نرخ معامله)، اطلاعات هویتی معامله‌کنندگان و منشأ (دارا شدن از طریق استخراج یا طریق دیگر) یا محل مصرف دارایی مورد معامله را در سامانه-ای مشخص همزمان با وقوع رویداد به ثبت برسانند و تمام وجوه مربوط به معاملات خود را صرفاً در حساب بانکی متعلق به مرکز که به بانک مرکزی معرفی شده است واریز و نگهداری نمایند.

References

- [1] BINANCE. (2021). What is Anti-Money Laundering (AML)?
<https://academy.binance.com/en/articles/what-is-anti-money-laundering-aml>
- [2] "coin market cap", Last modified July 15, 2021, <https://coinmarketcap.com>
- [3] Duncan Hughes, "ATO Creates Specialist Task Force to Tackle Cryptocurrency Tax Evasion," *FINANCIAL REVIEW* 25 (2018): 12.
<http://www.afr.com/news/policy/tax/ato-creates-specialist-task-force-to-tackle-cryptocurrency-tax-evasion-20180109-h0fyaz>,
archived at <https://perma.cc/VNY2-R6G3>.
- [4] FATF.(2014). "Virtual Currencies Key Definitions and Potential AML/CFT Risks"
<http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>
- [5] FATF. (2015). "Guidance for A Risk-Based Approach Guidance for A Risk-Based Approach Virtual Currencies", <https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf>

- [6] FATF. (2019). "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," FATF, Paris: www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html
- [7] FATF. (2021), "International Standards on Combating Money Laundering and The Financing of Terrorism & Proliferation", FATF, Paris: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf>
- [8] Kotane, IntaKotane .(2018). "Concept of Virtual Currencies in Modern Economies", *Rezekne Academy of Technologies*: 63-76.
- [9] Laurent, Peter and et al. (2017). Preventing Money Laundering and Terrorist Financing: A Practical Guide for Banking Supervisors, Translated by Maryam Keshtkar, Tehran, Tash.
- [10] Mireille Delmas, Marty. (2014). systems of criminal policy, Translated by Alihossein Najafi Abrandabadi, Tehran, Mizan. (In Persian)
- [11] Najafi Abrandabadi, Alihossein. (2009). New criminology-New criminology; An introduction to risk-based criminal policy, Criminal Science, Tehran, Mizan.Roshan, Mohammad Mozafari, Mostafa & Mirzaie, Hanieh. (2019). A Study of the Jurisprudential and Legal Status of Bitcoin, *Journal of Legal Research*, Volume 22, Number 87, pp. 49-78. (In Persian)
- [12] Saffari, Ali, Saberi, Razieh, Khalili Paji, Aref. (2020). Criminal Functions of Virtual Currencies: Criminological Analysis and Preventive Strategies, *Encyclopedia of Economic Law*, Volume 18, Number 27, pp. 223-250. (In Persian)
- [13] Shamloo, Baqir & Khalili Paji, Aref. (2020 [a]). Risk-based approach to criminal policy against money laundering, *Journal of Criminal Law*, Volume 1, Number 11, pp. 127-152. (In Persian)
- [14] Shamloo, Baqir & Khalili Paji, Aref. (2020 [b]). Virtualization of white-collar delinquency in the light of virtual currencies, *Legal Journal of Justice*, Volume 84, Number 110, pp. 41-73. (In Persian)
- [15] Shamloo, Baqir & Khalili Paji, Aref. (2020 [C]). Legal-Economic Challenges of Virtual Currencies on Political Systems in the Light of Alternative Theory, *Political and International Approaches*, Volume 12, Number 1, pp. 125-152. (In Persian)
- [16] Werle, Gerhard and Lovell Fernandez and Moritz Vormbaum . (2017). *Anti-Money Laundering: Socio-legal Perspectives on the Effectiveness of German Practices*. Berlin Springer Nature.
- [17] Yaga Dylan and others .(2018). *Blockchain Technology Overview*. U.S. Department of Commerce, National Institute of Standards and Technology Internal Report 8202.