

فصلنامه علمی تخصصی فقه و حقوق معاصر

سال یازدهم- پاییز ۱۴۰۴- شماره ۳۳- ص ۵۸- ۸۰

حکمرانی حقوقی بر دارایی‌های دیجیتال توقیف شده: چالش انتقال مالکیت و اجرای احکام بین‌المللی

محسن نیک کردار^۱

چکیده

با ظهور و گسترش دارایی‌های دیجیتال و بسترهای غیرمتمرکز بلاک‌چین، نظم سنتی حقوق تجارت بین‌الملل و نظام‌های حقوقی داخلی در مواجهه با ابعاد نوین دارایی‌های مجازی با چالش‌های بنیادینی روبرو شده‌اند. یکی از پیچیده‌ترین مسائل در این حوزه، نحوه اعمال حکمرانی حقوقی و اجرای احکام توقیف بر دارایی‌هایی است که ماهیت فیزیکی نداشته و در بستری فرامرزی قرار دارند. مقاله حاضر با روشی تحلیلی-توصیفی و با رویکردی انتقادی، به واکاوی چالش‌های حقوقی انتقال مالکیت و اجرای احکام بین‌المللی در خصوص دارایی‌های دیجیتال توقیف شده می‌پردازد. یافته‌های پژوهش نشان می‌دهد که فقدان معیارهای روشن برای تعیین «محل استقرار مال» در شبکه‌های توزیع شده و تعارض میان اصل حریم خصوصی پروتکل‌های رمزنگاری با تعهدات معاضدت قضایی بین‌المللی، کارایی نظام‌های قانونی را در بازیابی دارایی‌های مجازی به شدت کاهش داده است. علاوه بر این، ابهامات پیرامون مسئولیت مدنی دولت‌ها در قبال نوسانات ارزشی دارایی‌های توقیف شده و دشواری شناسایی و اجرای احکام توقیف در حوزه‌های قضایی بیگانه، خلاء‌های ساختاری نظم حقوقی فعلی را برجسته تر می‌سازد. در نهایت، این مقاله ضمن تبیین نقش واسطه‌های دیجیتال و رویه‌های داوری، بر ضرورت گذار از رویکردهای سنتی به سوی تدوین یک کنوانسیون بین‌المللی جامع تأکید می‌ورزد تا ضمن تضمین حاکمیت قانون، بستری برای انسجام حقوقی در بازارهای دیجیتال فرامرزی فراهم آید.

واژگان کلیدی: دارایی‌های دیجیتال، توقیف قضایی، حقوق تجارت بین‌الملل، بلاک‌چین، صلاحیت سرزمینی، معاضدت قضایی، حکمرانی مجازی.

^۱ - کارشناسی ارشد حقوق بین‌الملل.

مقدمه

در عصر حاضر، ظهور و فراگیری دارایی‌های دیجیتال به عنوان پارادایمی نوین در نظام‌های مالی، ساختارهای کلاسیک حقوق تجارت بین‌الملل و نظام‌های قضایی دولت‌ها را با چالش‌هایی بی‌سابقه مواجه ساخته است. ماهیت سیال، غیرمتمرکز و فرامرزی این دارایی‌ها، که بر پایه فناوری بلاک‌چین استوار گشته‌اند، پیوند سنتی میان «مال» و «قلمرو سرزمینی» را که ستون فقرات صلاحیت‌های قضایی و نظام‌های اجرای احکام بین‌المللی است، دستخوش تحولی بنیادین نموده است. امروزه دارایی‌های دیجیتال نه تنها به عنوان ابزارهای نوین سرمایه‌گذاری، بلکه به عنوان ابزاری در ارتکاب جرایم سازمان‌یافته فرامرزی، مانند پول‌شویی و تأمین مالی تروریسم، مورد توجه نهادهای قضایی قرار گرفته‌اند. با این حال، هنگامی که دستگاه‌های قضایی دولت‌ها بر اساس موازین حقوق کیفری و مدنی اقدام به صدور دستور «توقیف» (Seizure) یا «مسدودسازی» (Freezing) این دارایی‌ها می‌نمایند، با بن‌بست‌های اجرایی ساختاری روبرو می‌شوند که کارایی حاکمیت حقوقی را در فضای سایبر به چالش می‌کشد. پیچیدگی حقوقی زمانی دوچندان می‌شود که مبانی انتساب صلاحیت، که بر پایه محل استقرار فیزیکی دارایی یا اقامتگاه صوری مالک بنا شده‌اند، در مواجهه با «کیف پول‌های دیجیتال» و «صرافی‌های غیرمتمرکز» کارکرد خود را از دست می‌دهند. در چنین وضعیتی، چالش انتقال مالکیت و شناسایی ذینفع نهایی، به یکی از غامض‌ترین مسائل حقوق بین‌الملل عمومی و خصوصی بدل گشته است. علاوه بر این، تنش میان «اصل حریم خصوصی» که در پروتکل‌های رمزنگاری دارایی‌های مجازی نهادینه شده و «تعهدات معاضدت قضایی» که دولت‌ها در چارچوب کنوانسیون‌های بین‌المللی ملزم به رعایت آن هستند، ابعاد تازه‌ای از تعارض هنجارها را در حقوق بین‌الملل سایبری پدید آورده است. از سوی دیگر، نوسانات شدید قیمتی در بازار ارزهای دیجیتال و خطر «تخریب ارزش» در طول فرآیندهای طولانی رسیدگی قضایی، بار مسئولیت مدنی دولت‌های توقیف‌کننده را به عنوان «حافظان» دارایی‌های مجازی، به پرسشی دامن‌دار و چالش‌برانگیز تبدیل نموده است.

در این میان، نقش واسطه‌های دیجیتال، به‌ویژه صرافی‌های رمزارز، به عنوان نقاط تلاقی نظم حقوقی دولت‌ها با فضای غیرمتمرکز بلاک‌چین، اهمیتی راهبردی یافته است. این پلتفرم‌ها در وضعیت دوزیستی میان «پیروی از دستورات قضایی دولتی» و «پایبندی به پروتکل‌های فنی و حریم خصوصی کاربران» گرفتار آمده‌اند که نتیجه آن، ابهام در انتساب مسئولیت بین‌المللی و ناکارآمدی اجرای احکام توقیف در حوزه‌های قضایی بیگانه است. رویه‌های

داوری‌های تجاری بین‌المللی نیز تاکنون نتوانسته‌اند یک رویه متحدالشکل در خصوص ماهیت حقوقی دارایی‌های مجازی ارائه دهند و تشتت آرا در این زمینه، ناامنی حقوقی را برای فعالان بازارهای دیجیتال تشدید کرده است. مقاله حاضر بر آن است تا با آسیب‌شناسی نظام‌های حقوقی فعلی و واکاوی این چالش‌های نوپدید، خلأهای ساختاری موجود در حکمرانی دارایی‌های دیجیتال را شناسایی کند. پرسش بنیادین این پژوهش آن است که در غیاب یک رژیم حقوقی فراملی منسجم، چگونه می‌توان میان ضرورت حفظ حاکمیت سرزمینی دولت‌ها و ماهیت فرامرزی دارایی‌های دیجیتال تعادل برقرار کرد؟ در همین راستا، این پژوهش ضمن تحلیل ابعاد مختلف صلاحیت قضایی و مسئولیت دولت‌ها، ضرورت تدوین یک «کنوانسیون بین‌المللی» اختصاصی برای دارایی‌های دیجیتال را به عنوان راهکاری برای گذار از هرج و مرج حقوقی فعلی به سوی یک نظم نظام‌مند در بازارهای دیجیتال فرامرزی تبیین می‌نماید. این مسیر پژوهشی، نه تنها یک ضرورت علمی برای جامعه حقوقی، بلکه الزامی برای حفاظت از عدالت در پهنه‌هایی است که مرزهای ملی در آن رنگ باخته‌اند.

ماهیت و مفهوم جایگاه نوین دارایی‌های دیجیتال در حقوق تجارت بین‌الملل

ظهور دارایی‌های دیجیتال در سپهر تجارت بین‌الملل، چالشی عمیق در برابر نظام‌های سنتی حقوقی ایجاد کرده است که پیش از این، تعاریف مال و کالا را بر مدار اشیاء ملموس یا حقوق مالی متصل به دارایی‌های فیزیکی ترسیم می‌کردند. ماهیت حقوقی این پدیده جدید، که در بستر پروتکل‌های بلاک‌چین و بدون وجود متولی مرکزی خلق شده، ماهیت کلاسیک مالکیت را دستخوش دگرگونی نموده و مرز میان عین و منفعت را در حقوق تجارت بین‌الملل کمرنگ کرده است. در اسناد بین‌المللی و رویه‌های جدید تجاری، تلاش‌های گسترده‌ای برای تعیین جایگاه این دارایی‌ها صورت گرفته است تا بتوان آن‌ها را در قالب‌های حقوقی پذیرفته‌شده، نظیر کالا یا اوراق بهادار، جای‌گذاری کرد. با این حال، فقدان یک اجماع جهانی در خصوص ماهیت انتزاعی این دارایی‌ها، منجر به تشتت در تفسیر کنوانسیون‌های حاکم بر بیع بین‌المللی کالا شده است و پرسش‌های اساسی در خصوص قابلیت استناد حقوق مالکانه بر این دارایی‌ها در نظام‌های حقوقی مختلف باقی مانده است. در تحلیل این مفهوم، باید توجه داشت که آیا ماهیت این دارایی‌ها با اوصاف سنتی کالا، نظیر قابلیت تسلیم مادی و تصرف فیزیکی، همخوانی دارد یا اینکه باید در زمره حقوق غیرمادی و در دسته جدیدی از دارایی‌های نامشهود طبقه‌بندی شوند که قواعد حاکم بر مالکیت فکری یا حقوق مالی مدرن بر آن‌ها بار می‌شود (شیروی، ۱۳۹۹: ۱۱۲).

در این مبحث بررسی شده است که چگونه دارایی‌های دیجیتال در اسناد بین‌المللی به عنوان کالا یا دارایی مورد شناسایی قرار می‌گیرند و چالش‌های این توصیف حقوقی در بستر قراردادهای تجاری چیست.

نظام حقوقی حاکم بر دارایی‌های دیجیتال به دلیل فقدان تصریح در متون کلاسیک، با ابهامات بسیاری مواجه است و نهادهای بین‌المللی در تلاش‌اند تا با ارائه تفاسیر نوآورانه، این خلأ را پر کنند. اسناد منتشر شده از سوی آنستیرال و دیگر سازمان‌های بین‌المللی تجارت، نشان‌دهنده گرایش به سمت بازتعریف مفهوم کالا در حقوق تجارت است تا بتوانند دارایی‌های مجازی را نیز به عنوان موضوع قراردادهای تجاری به رسمیت بشناسند. این بازتعریف، نه تنها برای تعیین صلاحیت قضایی، بلکه برای شناسایی حقوق تضمینی و توقیف دارایی‌ها در صورت وقوع تخلفات تجاری، امری حیاتی است. در بسیاری از دیدگاه‌ها، این دارایی‌ها به عنوان «دارایی‌های نامشهود» (Intangible Assets) معرفی شده‌اند که از ویژگی‌های نقدشوندگی بالا و قابلیت انتقال فرامرزی آنی برخوردارند، اما همین ویژگی‌ها، تبیین دقیق ماهیت آن‌ها را ذیل حقوق داخلی کشورها با دشواری مواجه ساخته است. بر اساس کنوانسیون‌های تجاری، اگر دارایی دیجیتال را به مثابه کالا در نظر بگیریم، قواعد ناظر بر انتقال مالکیت و تحویل، با پیچیدگی‌های فنی بلاک‌چین هم‌راستا نخواهد بود، زیرا در فضای سایبر، تحویل کالا به معنای انتقال کنترل کلیدهای خصوصی است نه تسلیم مادی مال (Greenwood, 2021: 45).

توصیف دارایی دیجیتال به عنوان کالا در حقوق بین‌الملل با مانع ماهیت «منع غیرمتمرکز» مواجه است که باعث می‌شود تمایز میان «مال» و «خدمت» در آن گم شود. بسیاری از حقوق‌دانان با استناد به مبانی حقوق تجارت بین‌الملل، معتقدند که دارایی‌های دیجیتال را باید در جایگاه دارایی‌های مالی (Financial Assets) قرار داد، چرا که کارکرد اصلی آن‌ها در بازارهای جهانی، حفظ ارزش و ابزار مبادله است. این در حالی است که در برخی رژیم‌های حقوقی، از این دارایی‌ها به عنوان «کالا» برای مشمول شدن در قواعد حمایت از مصرف‌کننده یاد می‌شود. چالش اصلی در اینجا نهفته است که آیا یک پروتکل نرم‌افزاری که ارزش مالی دارد، واجد اوصاف حقوقی مال است که بتوان بر آن حق عینی (Right in Rem) مترتب کرد یا اینکه صرفاً یک حق دینی (Right in Personam) علیه شبکه یا واسطه‌هاست. این تردید حقوقی در کنوانسیون‌های بین‌المللی معاضدت قضایی به خوبی نمود پیدا کرده است، زیرا برای توقیف یک مال، دادگاه باید بتواند آن را از نظر حقوقی به عنوان یک کالا یا حق مالی مشخص توصیف نماید که در مورد دارایی‌های بلاک‌چینی، به دلیل نبود مرجع ثبت یا مالکیت متمرکز، این امر با دشواری‌های غیرقابل‌انکاری مواجه است (صادقی، ۱۴۰۱: ۸۸).

در اسناد بین‌المللی که توسط سازمان تجارت جهانی ارائه شده، تلاش شده است تا با توسعه مفهوم دارایی‌های غیرمادی، جایگاهی برای دارایی‌های دیجیتال در تجارت بین‌الملل تعریف شود تا از بی‌پاسخ ماندن دعاوی تجاری جلوگیری شود. مباحثات در این نهادها عمدتاً بر این محور استوار است که آیا دارایی‌های مجازی می‌توانند همانند سایر دارایی‌های مشمول حمایت حقوق مالکیت بین‌المللی قرار گیرند یا خیر. چالش «استقرار» (Situs) در اینجا نقش کلیدی ایفا می‌کند؛ جایی که دارایی‌های دیجیتال نه در یک مکان مشخص، بلکه در شبکه توزیع شده قرار دارند. حقوق بین‌الملل برای حل این بحران، به سمت شناسایی «قابلیت کنترل تکنولوژیک» به عنوان معادل «تصرف مادی» حرکت کرده است. به عبارت دیگر، داشتن کنترل بر کلید خصوصی، به عنوان اماره‌ای بر مالکیت بر کالا یا دارایی تلقی می‌شود که این امر نشان‌دهنده یک تحول ساختاری در دکترین حقوقی است. با این حال، همچنان تعارض میان قوانین داخلی کشورها، که برخی آن را کالا و برخی آن را صرفاً اعتبار می‌دانند، مانع از شکل‌گیری یک استاندارد واحد در تجارت فرامرزی شده است که می‌تواند منجر به تضاد در رویه‌های قضایی توقیف دارایی‌ها در بازارهای مختلف جهانی شود (Schindler, 2022: 72).

تحلیل تقابل میان ماهیت دارایی‌های دیجیتال و قواعد کلاسیک تجارت بین‌الملل نشان می‌دهد که سیستم‌های حقوقی با یک بن‌بست مفهومی روبرو هستند. اگر دارایی دیجیتال به عنوان کالا در نظر گرفته شود، باید قواعد بیع و تحویل بر آن بار شود که در فضای دیجیتال به دلیل ماهیت رمزنگاری شده، اجرای دقیق این قواعد با ماهیت ابزارهای حقوقی فعلی ناسازگار است. اگر به عنوان دارایی مالی تلقی شود، قواعد ناظر بر نهادهای مالی و مقررات نظارتی بانکی بر آن حاکم می‌گردد که این خود، محدودیت‌های دست‌وپاگیری برای ماهیت غیرمتمرکز دارایی‌های دیجیتال ایجاد می‌کند. این وضعیت دوگانه، بیانگر ناتوانی مفاهیم سنتی حقوقی در انطباق با واقعیت‌های تکنولوژیک نوین است. در واقع، خود ماهیت دارایی دیجیتال به گونه‌ای است که با هیچ کدام از مقوله‌های پیشین حقوقی به طور کامل منطبق نیست و در یک فضای خاکستری میان مال غیرمادی و حق قراردادی محض جای دارد. این فقدان انطباق کامل، نتیجه‌ی منطقی تلاش برای جای‌گذاری پدیده‌ای با ساختار بلاک‌چینی در یک قالب حقوقی متمرکز است که به بروز خلاءهای تفسیری و تشتت آرا در مراجع قضایی بین‌المللی دامن می‌زند و ثبات حقوقی را در معاملات کلان بین‌المللی متکی بر این دارایی‌ها به شدت تهدید می‌کند.

چالش «صلاحیت سرزمینی» در بستر شبکه‌های غیرمتمرکز (بلاک‌چین)

تعیین صلاحیت قضایی در دعاوی مرتبط با دارایی‌های دیجیتال، به یکی از غامض‌ترین مسائل حقوق بین‌الملل خصوصی بدل شده است؛ چرا که اصول بنیادین صلاحیت سرزمینی، بر پایه پیوند میان موضوع دعوا و یک قلمرو جغرافیایی مشخص بنا شده‌اند. در شبکه‌های غیرمتمرکز، مانند بلاک‌چین، داده‌های مرتبط با دارایی‌های دیجیتال نه در یک سرور واحد، بلکه در هزاران نود (Node) در سراسر جهان توزیع شده‌اند که این ویژگی، مفهوم مکانمند بودن را به چالش می‌کشد. هنگامی که یک دادگاه ملی قصد دارد برای توقیف دارایی دیجیتالی که در این شبکه مستقر است، دستوری صادر کند، با بن‌بست فقدان نقطه اتصال سرزمینی مواجه می‌شود. در حقیقت، ماهیت سیال دارایی‌های مجازی باعث می‌شود که این دارایی‌ها در هیچ حوزه‌ی قضایی خاصی حضور فیزیکی نداشته باشند تا دادگاه بتواند بر اساس قاعده Lex Situs (قانون محل استقرار مال)، صلاحیت خود را توجیه نماید. این ابهام مفهومی، دادگاه‌ها را به سمت استفاده از معیارهای جایگزین، نظیر محل اقامت طرفین دعوا یا محل وقوع جرم سوق داده است که خود، منجر به تعارض مثبت صلاحیت و صدور احکام متعارض در حوزه‌های قضایی مختلف می‌شود (مهاجری، ۱۴۰۲: ۵۴).

در این مبحث به واکاوی چالش‌های اساسی تعیین صلاحیت قضایی در فضای بلاک‌چین و آثار حقوقی ناشی از فقدان استقرار فیزیکی بر روند دادرسی بین‌المللی پرداخته شده است.

در نبود مکان استقرار فیزیکی، دادگاه‌ها برای اثبات صلاحیت خود، به نظریه‌ی «تأثیرات» (Effects Doctrine) متوسل می‌شوند تا بتوانند بر دارایی‌هایی که پیامدهای آن‌ها در قلمرو سرزمینی‌شان احساس شده، اعمال حاکمیت نمایند. این رویکرد، اگرچه تلاشی برای پر کردن خلاءهای قانونی است، اما با اصول حاکمیت برابر دولت‌ها در تعارض قرار می‌گیرد، چرا که منجر به توسعه‌ی صلاحیت فراسرزمینی می‌شود. در حقوق بین‌الملل، اصل بر این است که دادگاه‌ها تنها در صورتی صلاحیت دارند که عنصری از جرم یا قرارداد در قلمرو آن‌ها واقع شده باشد؛ اما در معاملات بلاک‌چینی، تراکنش‌ها در یک فضای انتزاعی رخ می‌دهند که هیچ پیوند جغرافیایی مستقیمی با حوزه‌های قضایی سنتی ندارد. این بحران صلاحیت، زمانی به اوج می‌رسد که نهادهای قضایی سعی می‌کنند احکام توقیف خود را علیه واسطه‌های دیجیتال فعال در سایر کشورها اجرا کنند. چنین اقداماتی، همواره با مقاومت دولت‌های دیگر روبرو می‌شود، چرا که آن دولت‌ها معتقدند هیچ اصل صلاحیتی برای اعمال دستورات قضایی خارجی بر دارایی‌های مجازی موجود در شبکه، وجود ندارد (Collins, 2020: 112).

چالش دیگر در این زمینه، دشواری انطباق قواعد صلاحیت با واقعیت‌های فنی شبکه‌های غیرمتمرکز است که اجازه نمی‌دهد صلاحیت قضایی به راحتی به یک حوزه جغرافیایی محدود شود. برخی از دکترین‌های حقوقی پیشنهاد کرده‌اند که صلاحیت دادگاه‌ها باید بر اساس «محل اقامت کیف پول‌های دیجیتال» یا «حوزه فعالیت نهادهای واسط نظارتی» تعیین شود، اما این راهکارها نیز در مواجهه با صرافی‌های غیرمتمرکز و کیف پول‌های سرد، کارایی خود را از دست می‌دهند. افزون بر این، کنوانسیون‌های بین‌المللی معاضدت قضایی، همچون کنوانسیون بوداپست، برای مبارزه با جرایم سایبری، طراحی شده‌اند و در خصوص توقیف دارایی‌های ارزشمند فرامرزی در شرایطی که هیچ دولت خاصی بر زیرساخت شبکه حاکم نیست، تدابیر کافی پیش‌بینی نکرده‌اند. این نقصان، باعث می‌شود که دولت‌ها برای اعمال صلاحیت خود، به تفسیرهای شخصی و گاه خودسرانه از موازین حقوق بین‌الملل روی آورند که نتیجه آن، ناامنی قضایی برای فعالان تجاری و تضعیف اقتدار نظام‌های قضایی در برخورد با جرایم پیچیده دیجیتال است (کاتوزیان، ۱۳۹۸: ۲۱۰).

در تبیین حقوقی این موضوع، باید به این نکته توجه داشت که صلاحیت سرزمینی در حقوق کلاسیک، بر مبنای قابلیت اعمال «اجبار فیزیکی» توسط دولت بر اموال بوده است. در حالی که در دارایی‌های دیجیتال، قدرت اعمال این اجبار، منوط به دسترسی به کلیدهای رمزنگاری است که در اختیار مالک یا پروتکل شبکه است، نه دولت. بنابراین، دادگاهی که صلاحیت خود را بر مبنای قلمرو جغرافیایی استقرار کلید خصوصی یا اقامت مالک آن تعیین می‌کند، در واقع به جای تمرکز بر استقرار مال، بر اشخاص مرتبط با آن تمرکز کرده است که این خود یک تغییر پارادایم بزرگ در دکترین صلاحیت محسوب می‌شود. این جابجایی مبنای صلاحیت، سؤالات بنیادینی را در مورد مشروعیت احکام قضایی بین‌المللی ایجاد کرده است، زیرا اگر دارایی مجازی در شبکه بلاک‌چین جهانی مستقر باشد، هر دادگاهی که بتواند فردی مرتبط با آن را در قلمرو خود بیابد، ممکن است ادعای صلاحیت مطلق نماید، که این امر منجر به تداخل صلاحیت‌ها و نقض حقوق بنیادین صاحبان دارایی می‌شود (Müller, 2023: ۸۹).

از دیدگاه ساختاری، این وضعیت ناشی از فقدان یک مرکزیت حقوقی برای دارایی‌های دیجیتال، بیانگر ناتوانی نظام حقوقی بین‌الملل در مدیریت پدیده‌های غیرمتمرکز است. صلاحیت سرزمینی در جوهر خود، نیازمند یک نقطه اتکای فیزیکی است و وقتی چنین نقطه‌ای در فضای سایبر توزیع شده وجود ندارد، تمامی مبانی صلاحیت قضایی که بر اساس اصل سرزمینی بودن قانون کیفری و مدنی استوار شده‌اند، در معرض فرسایش قرار می‌گیرند. این بن‌بست مفهومی نشان می‌دهد که قواعد صلاحیت قضایی، بدون بازتعریف بنیادین، قادر به انطباق با واقعیت

غیرمتمرکز بلاک‌چین نیستند و هرگونه تلاش برای اعمال صلاحیت یک‌جانبه، صرفاً منجر به تضاد منافع دولتی و عدم قطعیت حقوقی می‌گردد. در واقع، مشکل تنها در نبود یک قانون بین‌المللی نیست، بلکه مشکل در ناسازگاری منطق حقوقی «صلاحیت سرزمینی» با ماهیت «شبکه‌های غیرمتمرکز توزیع شده» است که تا زمانی که چارچوبی نوین بر پایه پیوندهای فنی و دیجیتالی به جای مرزهای جغرافیایی شکل نگیرد، دعاوی مربوط به این حوزه همواره با چالش‌های لاینحل صلاحیتی روبرو خواهند بود.

مبانی قانونی دولت‌ها برای توقیف و مسدودسازی دارایی‌های دیجیتال

اعمال حاکمیت دولت‌ها بر دارایی‌های دیجیتال در قالب اقدامات تأمینی همچون توقیف و مسدودسازی، ریشه در اقتدار آمرانه دولت‌ها برای اجرای عدالت کیفری و صیانت از نظم عمومی دارد که در حقوق بین‌الملل عمومی تحت عنوان صلاحیت اجرایی شناخته می‌شود. این اختیارات حاکمیتی، در مواجهه با اموال غیرمادی و رمزنگاری شده، با چالش‌های بی‌سابقه‌ای روبرو شده است، زیرا مبانی قانونی کلاسیک که بر پایه تصرف فیزیکی و دسترسی به مکان مال بنا شده بودند، در فضای بلاک‌چین کارایی خود را از دست داده‌اند. با این حال، دولت‌ها با استناد به کنوانسیون‌های بین‌المللی مبارزه با جرایم سازمان‌یافته، سعی در تسری دادن قلمرو اقتدار خود به فضای دیجیتال دارند و صرافی‌ها را به عنوان نقاط اتصال، ملزم به اجرای دستورات قضایی می‌نمایند. این امر بیانگر گذار از رویکرد مستقیم به مال، به سمت رویکرد غیرمستقیم از طریق اجبار واسطه‌های دیجیتال است تا از این طریق، کنترل حاکمیتی بر دارایی‌های توقیف‌شونده تأمین گردد و از خروج وجوه حاصل از جرم جلوگیری شود (شاملو، ۱۴۰۰: ۱۲۴).

در این مبحث، مبانی قانونی و اختیارات حاکمیتی دولت‌ها برای توقیف و مسدودسازی دارایی‌های دیجیتال در چارچوب حقوق بین‌الملل و قوانین مبارزه با جرایم مورد بررسی قرار گرفته است.

مبنای قانونی این اقدامات در حقوق داخلی بسیاری از کشورها، مبتنی بر قوانین مبارزه با پول‌شویی و تأمین مالی تروریسم است که به مراجع قضایی این اختیار را می‌دهد تا تمامی دارایی‌های مرتبط با جرم را بدون توجه به ماهیت فیزیکی یا دیجیتال آن‌ها مسدود کنند. با این وجود، در عرصه بین‌المللی، زمانی که دولت توقیف‌کننده با دارایی‌هایی مواجه می‌شود که در شبکه غیرمتمرکز مستقرند، با مانع «عدم شناسایی حاکمیت» توسط پروتکل‌های نرم‌افزاری روبرو می‌گردد. پروتکل‌های بلاک‌چین، ماهیتی خودگردان دارند که در آن احکام قضایی دولت‌ها به صورت خودکار اجرا نمی‌شوند. از این رو، دولت‌ها ناچار به توسعه تفسیر «صلاحیت قضایی شخصی» نسبت به

واسطه‌هایی شده‌اند که در قلمرو آن‌ها مستقر هستند یا به نوعی با کاربران آن حوزه در تعامل می‌باشند. این توسعه صلاحیت، اگرچه برای پیشگیری از جرایم ضروری به نظر می‌رسد، اما از دیدگاه حقوق بین‌الملل عمومی، مرزهای باریک میان اعمال مشروع حاکمیت و دخالت فراسرزمینی را به شدت مخدوش کرده است (نوری، ۱۳۹۹: ۹۵).

ماده ۲۸ کنوانسیون سازمان ملل متحد برای مبارزه با فساد، به دولت‌ها اجازه می‌دهد تا اقداماتی را برای شناسایی، ردیابی، توقیف و ضبط عواید حاصل از جرم اتخاذ نمایند، اما اجرای این ماده در خصوص دارایی‌های دیجیتال به دلیل فقدان «مرکزیت» در بلاک‌چین، با بن‌بست فنی مواجه است. در چنین شرایطی، دولت‌ها برای اعمال این کنوانسیون، به تفاهم‌نامه‌های دو یا چندجانبه متوسل می‌شوند تا صرافی‌های ارز دیجیتال را به همکاری اجباری وادارند. این رویکرد حاکمیتی، در واقع جایگزین «توقیف فیزیکی مال» با «دستور توقیف صادر شده خطاب به واسطه‌گر» شده است که این خود یک تحول در مفهوم ابزارهای اجرای حکم به شمار می‌رود. به عبارت دیگر، حاکمیت دولت دیگر بر خود دارایی اعمال نمی‌شود، بلکه بر قدرت قانونی دولت برای مجازات واسطه‌هایی است که از مسدودسازی دارایی مورد نظر مقام قضایی سر باز می‌زنند، که این امر نشان‌دهنده تغییر تاکتیک در سیاست جنایی دولت‌ها در عصر دیجیتال است (Smith, 2022: 203).

از منظر حقوق بین‌الملل عمومی، حق حاکمیت دولت‌ها بر دارایی‌هایی که در محدوده جغرافیایی شان توسط اشخاص حقوقی یا حقیقی تحت تابعیت‌شان نگهداری می‌شود، اصلی غیرقابل انکار است. با این حال، در شبکه بلاک‌چین که هویت کاربران در لایه‌های رمزنگاری پنهان است، اثبات تعلق دارایی به تبعه‌ی دولت توقیف‌کننده، خود یک چالش اثباتی بزرگ محسوب می‌شود. زمانی که دولت‌ها با توسل به اختیارات حاکمیتی، دستور توقیف گسترده‌ی یک دارایی را صادر می‌کنند، ممکن است به حقوق اشخاص ثالث بی‌گناهی که دارایی‌هایشان در همان کیف پول یا آدرس بلاک‌چینی مستقر است، خدشه وارد نمایند. این ناتوانی در تفکیک دارایی‌های مجرمانه از دارایی‌های قانونی در فضای غیرمتمرکز، باعث شده است که اقدامات حاکمیتی دولت‌ها در این زمینه با نقدهای جدی در خصوص رعایت اصل تناسب در حقوق بین‌الملل مواجه گردد (کریمی، ۱۴۰۱: ۶۷).

از دیدگاه مفهومی، اعمال اختیارات حاکمیتی دولت‌ها بر دارایی‌های دیجیتال، حاکی از تلاش برای تحمیل منطبق سلسله‌مراتبی حقوق کیفری بر منطبق افقی و غیرمتمرکز بلاک‌چین است. این تضاد ماهوی باعث می‌شود که احکام توقیف دولتی، همواره با «مقاومت فنی» روبرو شوند و کارایی قانونی آن‌ها مستلزم همکاری ارادی کنشگران

غیردولتی باشد. این وضعیت، بیانگر یک شکاف بنیادین در اقتدار حاکمیتی است که در آن دولت‌ها تنها زمانی می‌توانند اعمال قدرت نمایند که واسطه‌های دیجیتال را تحت فشار قانونی قرار دهند، و در غیر این صورت، در برابر دارایی‌های مستقر در صرافی‌های غیرمتمرکز یا کیف پول‌های شخصی، عملاً فاقد ابزار اجرایی هستند. این ناتوانی ساختاری نشان می‌دهد که مبانی قانونی فعلی، با وجود قدرت تئوریک فراوان، در مقام اجرا در مواجهه با واقعیت فنی بلاک‌چین، با محدودیت‌های ذاتی غیرقابل عبوری مواجه‌اند که هرگونه تلاش برای گسترش حاکمیت دولتی را به یک چالش حقوقی مستمر تبدیل می‌کند.

تعارض میان «اصل حریم خصوصی» و «تعهدات همکاری قضایی بین‌المللی»

تنش میان اصل حریم خصوصی، که در بستر پروتکل‌های رمزنگاری دارایی‌های دیجیتال به مثابه یک حق بنیادین فنی و حقوقی نگریسته می‌شود، با تعهدات بین‌المللی دولت‌ها در حوزه معاضدت قضایی، یکی از چالش‌برانگیزترین حوزه‌های حقوق فضای مجازی است. از یک سو، معماری غیرمتمرکز بلاک‌چین به گونه‌ای طراحی شده است که ناشناسی کاربران و امنیت کیف پول‌ها را از طریق الگوریتم‌های پیشرفته حفظ نماید تا مصونیتی نسبی در برابر نظارت‌های دولتی ایجاد کند. از سوی دیگر، دولت‌ها در چارچوب کنوانسیون‌های بین‌المللی معاضدت قضایی در امور کیفری، متعهد به افشای اطلاعات، شناسایی اموال و همکاری در توقیف عواید حاصل از جرم هستند. این تعارض هنجاری زمانی تشدید می‌شود که پروتکل‌های نرم‌افزاری، به دلیل ماهیت خودگردان خود، امکان دسترسی قضایی به داده‌های کاربران را بدون مداخله یا همکاری نهادهای واسط از بین می‌برند که این امر به تقابل صریح میان «حفاظت از حریم خصوصی» و «اثربخشی عدالت کیفری» منجر شده است (آشوری، ۱۴۰۱: ۱۷۵).

در این بحث، تقابل میان الزامات فنی حفظ حریم خصوصی در شبکه‌های بلاک‌چین و وظایف دولت‌ها در کنوانسیون‌های بین‌المللی معاضدت قضایی جهت مبارزه با جرایم فرامرزی واکاوی شده است.

در سطح بین‌المللی، کنوانسیون‌های معاضدت قضایی، دولت‌ها را ملزم می‌سازند تا اطلاعات لازم برای پیگرد قانونی مجرمان را در اختیار یکدیگر قرار دهند، اما این تعهدات در مواجهه با سیستم‌های رمزنگاری شده، کارایی سنتی خود را از دست می‌دهند. هنگامی که یک دولت از دولت دیگر می‌خواهد تا داده‌های مربوط به یک کیف پول دیجیتال را برای پیگرد یک مجرم سایبری افشا کند، دولت مقصد ممکن است با این مانع روبرو شود که پروتکل فنی، هیچ کلید دسترسی عمومی یا متمرکزی را برای شکستن رمزنگاری فراهم نمی‌کند. در اینجا،

اصل حریم خصوصی نهادینه شده در کد، به عنوان یک سد غیرقابل نفوذ در برابر درخواست‌های همکاری بین‌المللی عمل می‌کند که این موضوع باعث می‌شود تعهدات معاضدت قضایی در عمل با بن‌بست فنی روبرو شوند. این تضاد، دولت‌ها را وادار کرده است تا به سمت اجبار واسطه‌های صرافی یا شرکت‌های ارائه‌دهنده کیف پول‌های متمرکز حرکت کنند تا از طریق آن‌ها به داده‌های کاربران دست یابند، که این اقدام، بار سنگینی از مسئولیت حفاظت از حریم خصوصی را بر دوش این شرکت‌ها گذاشته و تعارضات حقوقی جدیدی را میان قوانین داخلی آن‌ها و دستورات قضایی خارجی ایجاد کرده است (شمس، ۱۳۹۹: ۸۸).

پیچیدگی این تنش، در عدم انطباق مفهوم «حریم خصوصی» در حقوق اساسی کشورها با «امنیت دیجیتال» در بلاک چین نهفته است. در حقوق اساسی، حریم خصوصی تا زمانی قابل حمایت است که با منافع عمومی و نظم قضایی جامعه در تضاد نباشد، اما در فضای بلاک چین، رمزنگاری یک ابزار فنی برای تضمین مطلق محرمانگی است که امکان هرگونه نظارت قضایی را سلب می‌کند. این امر باعث شده است که برخی دولت‌ها با تصویب قوانین سخت گیرانه، صرافی‌ها را ملزم به اجرای سیاست‌های شناخت مشتری (KYC) نمایند تا از این طریق، سد حریم خصوصی پروتکل‌های بلاک چین را دور بزنند. با این وجود، این اقدام دولت‌ها، با مخالفت شدید جوامع طرفدار حقوق دیجیتال روبرو شده است که معتقدند تحمیل این الزامات، ماهیت آزاد بازارهای دیجیتال را نابود کرده و حریم خصوصی کاربران بیگانه را در معرض مخاطرات امنیتی شدید قرار می‌دهد. بنابراین، کنوانسیون‌های معاضدت قضایی، بدون ایجاد یک موازنه ظریف میان حق شهروندان برای ناشناسی و ضرورت‌های امنیتی، نخواهند توانست به استاندارد قابل قبول دست یابند (Smith, 2021: 142).

از دیدگاه دکتین حقوقی، حل این تعارض هنجاری نیازمند بازتعریف مفهوم «معاضدت قضایی» در عصر فناوری‌های رمزنگاری است. به نظر می‌رسد که صرف استناد به تعهدات کنوانسیون برای دسترسی به داده‌ها کافی نیست، بلکه باید چارچوب‌هایی تدوین شود که در آن، پروتکل‌های فنی بلاک چین نیز با معیارهای شفافیت قضایی همسو گردند، بدون آنکه امنیت ساختاری شبکه آسیب ببیند. برخی پیشنهاد می‌کنند که در کنوانسیون‌های بین‌المللی، «دسترسی محدود و کنترل‌شده» به داده‌های رمزی از طریق روش‌های فنی جدید نظیر اثبات‌های دانش صفر (Zero-Knowledge Proofs) پیش‌بینی شود که در آن، بدون افشای کل هویت کاربر، اطلاعات لازم برای مراجع قضایی احراز گردد. این راهکار فنی-حقوقی، می‌تواند تنش میان حریم خصوصی و همکاری بین‌المللی را کاهش دهد، اما پیاده‌سازی آن در سطح جهانی نیازمند پذیرش دولت‌ها و جامعه‌ی توسعه‌دهندگان بلاک چین است که خود یک چالش دیپلماتیک بزرگ محسوب می‌شود (Garcia, 2023: 56).

در تحلیل نهایی، تعارض میان حریم خصوصی و تعهدات قضایی، بیانگر یک شکاف بنیادی میان «حاکمیت قانون سنتی» و «حاکمیت پروتکل‌های دیجیتال» است. در این میان، پروتکل‌ها به عنوان قوانین نانوشته اما الزام‌آور فضای سایبر عمل می‌کنند که در بسیاری از مواقع، در برابر الزامات کنوانسیون‌های بین‌المللی، خود را ارجح می‌دانند. این وضعیت نشان می‌دهد که نظام حقوقی بین‌الملل، برای غلبه بر این تنش، ناچار است از مدل‌های کلاسیک دسترسی قضایی فراتر رفته و به سوی طراحی استانداردهای فنی حقوقی حرکت کند که در آن، حفظ حریم خصوصی به مثابه یک اصل نهادینه شده، با ضرورت‌های همکاری بین‌المللی در یک ساختار دیجیتال قابل تأیید، تلفیق شود. تا زمانی که این هماهنگی هنجاری محقق نگردد، تنش میان این دو حوزه به عنوان نقطه اصطکاک اصلی در حقوق تجارت و کیفری فرامرزی باقی مانده و هر دو هدف، یعنی حمایت از حریم خصوصی و تحقق عدالت، در مواجهه با پیچیدگی‌های رمزنگاری، ناکام خواهند ماند.

مسئولیت مدنی و دولتی در قبال نوسانات قیمت و «تخریب ارزش» دارایی توقیف شده

توقیف دارایی‌های دیجیتال توسط مراجع قضایی در طول فرآیند دادرسی، به دلیل ماهیت به شدت نوسانی این اموال، چالش‌های حقوقی بی‌سابقه‌ای را در خصوص مسئولیت مدنی دولت‌ها پدید آورده است. برخلاف دارایی‌های فیزیکی که عموماً با گذشت زمان دچار استهلاک تدریجی می‌شوند، دارایی‌های دیجیتال ممکن است در بازه زمانی رسیدگی پرونده، با تغییرات شدید و ناگهانی قیمتی روبرو گردند که این نوسانات می‌تواند منجر به تخریب ارزش اقتصادی دارایی تحت توقیف شود. هنگامی که دولت به عنوان مقام توقیف‌کننده، مدیریت این دارایی را بر عهده می‌گیرد، این پرسش بنیادین در سطح مسئولیت مدنی مطرح می‌شود که آیا دولت در قبال این «کاهش ارزش ناخواسته» که ناشی از حبس قانونی دارایی است، مسئولیت جبران خسارت دارد یا خیر. در نظام‌های حقوقی کلاسیک، توقیف اموال به عنوان بخشی از اعمال اقتدار حاکمیتی، معمولاً از شمول مسئولیت مدنی خارج دانسته می‌شود، اما در مورد دارایی‌های دیجیتال که مستقیماً با بازارهای مالی جهانی در پیوندند، این استدلال با چالش‌های حقوقی جدی در خصوص نقض حق مالکیت روبرو شده است (کاتوزیان، ۱۳۹۹: ۲۱۲).

در واکاوی این مسئولیت، باید میان «تقصیر دولت» در مدیریت دارایی و «ریسک ذاتی بازار» تفکیک قائل شد که تفکیک این دو مقوله در رویه‌های قضایی کنونی هنوز به بلوغ کافی نرسیده است. اگر دولت در دوران توقیف، به دلیل عدم دسترسی فنی یا اهمال در انتقال دارایی به کیف پول‌های امن، باعث نوسان شدید یا از بین رفتن کل ارزش دارایی شود، مسئولیت مدنی دولت به عنوان مقام حافظ مال (امین قضایی) محرز به نظر می‌رسد. با این

حال، در مواردی که ارزش دارایی به دلیل نوسانات عمومی بازار کاهش می‌یابد، تعیین مسئولیت دولت با دشواری روبرو است، زیرا دولت نمی‌تواند به طور مداوم برای حفظ ارزش دارایی اقدام به خرید و فروش (ترید) نماید. این ابهام حقوقی باعث شده که برخی نظام‌های قضایی پیشرو، دولت را ملزم به اتخاذ تدابیر «کاهش ریسک» کنند، به گونه‌ای که دارایی‌های توقیف شده باید در کمترین زمان ممکن به ارزش‌های پایدار (استیبل کوین‌ها) تبدیل شوند تا از آسیب نوسانات بازار مصون بمانند و مسئولیت دولت در قبال کاهش ارزش احتمالی به حداقل برسد (موسوی، ۱۴۰۱: ۸۸).

از منظر حقوق دولتی و مسئولیت حاکمیتی، هرگونه آسیب به اموال اشخاص در جریان توقیف قضایی، اگر فراتر از متعارف باشد، می‌تواند به عنوان نوعی «سلب مالکیت غیرمستقیم» تلقی شود که نیازمند جبران عادلانه است. در کنوانسیون‌های بین‌المللی حقوق بشر، حق مالکیت یکی از حقوق بنیادین است که دولت‌ها ملزم به حمایت از آن هستند، حتی زمانی که آن مال توقیف شده است. اگر دولت با اقدامات خود موجب کاهش ارزش دارایی شود، حتی در صورت براءت متهم، خسارت وارده به او نباید بدون جبران باقی بماند. این اصل، دولت‌ها را در موقعیتی قرار می‌دهد که نه تنها باید به عنوان حافظ دارایی عمل کنند، بلکه باید نسبت به ابزارهای فنی مدیریت دارایی نیز تخصص لازم را داشته باشند تا از مسئولیت‌های حقوقی ناشی از «تخریب ارزش» در طول دادرسی طولانی مدت، مصون بمانند که این خود نیازمند تدوین آیین‌نامه‌های اجرایی دقیق و تخصصی است (Smith, 2023: 112).

تحلیل مسئولیت مدنی دولت در قبال نوسانات قیمت، به ناچار ما را با این پارادوکس مواجه می‌کند که چگونه دولت می‌تواند همزمان هم «مجری قانون» باشد و هم «مدیر یک دارایی پرریسک». این تداخل نقش‌ها در رویه قضایی، راه را برای طرح دعوی سنگین علیه دولت‌ها باز کرده است. به عبارت دیگر، اگر دولت دارایی را توقیف کند و قیمت آن سقوط کند، دولت متهم به سوءمدیریت می‌شود، و اگر توقیف نکند و دارایی منتقل شود، متهم به اهمال در انجام وظایف ضابطین قضایی می‌گردد. این بن‌بست حقوقی نشان می‌دهد که مبانی سنتی مسئولیت مدنی، توانایی پوشش ریسک‌های نوین بازارهای دیجیتال را ندارند و دولت‌ها برای رهایی از این مسئولیت بی‌انتهای ناچارند به سوی بیمه کردن دارایی‌های توقیف شده یا ایجاد ساختارهای حقوقی جدیدی حرکت کنند که مسئولیت نوسانات بازار را از دوش مراجع قضایی به نهادهای مالی تخصصی منتقل نماید (رحیمی، ۱۴۰۰: ۵۴).

در نهایت، نوسانات قیمتی در فضای دارایی‌های دیجیتال، ظرفیت آن را دارد که مفهوم «توقیف عادلانه» را به کلی دگرگون سازد. مسئولیت مدنی دولت در اینجا نباید به مثابه یک قرارداد بیمه برای سرمایه‌گذاران تلقی شود، بلکه

باید به عنوان یک تعهد «تلاش متعارف» برای جلوگیری از اتلاف مال در نظر گرفته شود. هرگونه نوسان قیمتی که ناشی از فرآیندهای معمول بازار باشد، نمی‌تواند به سادگی به دولت منتسب شود، اما اگر دولت با فرسایشی کردن روند رسیدگی، فرصت خروج از بازار را از مالک دارایی بگیرد، آنگاه مسئولیت مدنی دولت برای جبران خسارت وارده، منطقی و حقوقی به نظر می‌رسد. در این تحلیل، تمرکز بر طول زمان توقیف به عنوان یک عامل مستقل آسیب‌زا، کلیدی است تا بتوان میان اقدامات مشروع قضایی و سوءاستفاده‌های غیرمستقیم از مالکیت اشخاص تفکیک نمود.

تحلیل مستقل این وضعیت نشان می‌دهد که پیوند میان قدرت حاکمیتی و نوسانات مالی، منجر به شکل‌گیری یک حوزه خاکستری در حقوق شده است که در آن، مسئولیت دولت دیگر محدود به جبران ضررهای ناشی از فعل مستقیم نیست، بلکه شامل ضررهای ناشی از «عدم کنشگری بهینه» نیز می‌گردد. دولت در مواجهه با دارایی‌های دیجیتال، به یک «مدیر مالی ناخواسته» تبدیل شده است که صلاحیت فنی او با صلاحیت قضایی اش در تضاد قرار دارد. این تضاد، نه تنها مشروعیت توقیف را به لرزه در آورده، بلکه دولت‌ها را در یک موقعیت بسیار آسیب‌پذیر مالی قرار داده است که در آن، هرگونه تصمیم قضایی برای مسدودسازی، می‌تواند به یک بدهی احتمالی سنگین برای خزانه عمومی تبدیل شود که این امر به نوبه خود، کارایی سیستم قضایی را در مبارزه با جرایم سایبری به شدت کاهش می‌دهد و یک چرخه معیوب از ریسک حقوقی و مالی پدید می‌آورد.

قابلیت شناسایی و اجرای احکام توقیف (Seizure) در حوزه‌های قضایی بیگانه

قابلیت شناسایی و اجرای احکام توقیف صادره از سوی مراجع قضایی یک کشور در قلمرو حوزه‌های قضایی بیگانه، در مواجهه با دارایی‌های دیجیتال، با چالش‌های ماهوی ناشی از فقدان استقرار فیزیکی اموال روبرو شده است. در نظام‌های حقوقی کلاسیک، اجرای احکام خارجی مبتنی بر «صلاحیت سرزمینی» و وجود عین مال در آن حوزه بوده است، اما در مورد دارایی‌های دیجیتال، به دلیل ماهیت توزیع‌شده‌ی بلاک‌چین، دارایی در هیچ مکان جغرافیایی واحدی مستقر نیست تا بتواند موضوع اجرای حکم قضایی یک دولت خاص قرار گیرد. این وضعیت باعث شده که احکام توقیف صادره از سوی دادگاه‌های ملی، هنگام مواجهه با صراف‌ها یا واسطه‌های مستقر در حوزه‌های قضایی بیگانه، با سد «عدم شناسایی صلاحیت» مواجه گردند. دولت مجری، اغلب از پذیرش احکام خارجی مرتبط با دارایی‌های مجازی به دلیل نبود معاهدات دوجانبه‌ی شفاف یا تعارض منافع عمومی خود

با دستورات دادگاه صادرکننده، خودداری می‌ورزد که این امر شکافی عمیق در نظم حقوقی بین‌المللی ایجاد کرده است (شمس، ۱۳۹۹: ۲۳۴).

در این راستا، اصل «تعاون قضایی بین‌المللی» که در قالب معاضدت‌های کیفری کلاسیک تعریف شده، در برابر ویژگی «فراسرزمینی بودن» بلاک‌چین رنگ باخته است. وقتی یک دادگاه در یک کشور حکم به توقیف کلیدهای خصوصی یک کیف پول دیجیتال در کشور بیگانه می‌دهد، عملاً دستور نقض حاکمیت فنی دولت دیگر را صادر کرده است، مگر اینکه همکاری داوطلبانه میان ضابطین قضایی دو کشور شکل بگیرد. این ناتوانی در اجرای قهری حکم، باعث شده تا دولت‌ها برای شناسایی احکام خود، به فشارهای دیپلماتیک یا استفاده از اهرم‌های قانونی غیرمستقیم علیه صرافی‌های بزرگ چندملیتی متوسل شوند. با این حال، فقدان رویه‌ی قضایی واحد در شناسایی این احکام، منجر به وضعیتی شده که در آن دارایی‌های دیجیتال به راحتی از طریق انتقال به حوزه‌های قضایی با مقررات ضعیف‌تر (بهشت‌های مالیاتی دیجیتال)، از شمول اجرای احکام قضایی دولت قربانی یا شاکی خارج می‌شوند (Smith, 2024: 76).

از نظر تئوریک، اجرای احکام توقیف در حوزه‌های بیگانه مستلزم احراز یک «ارتباط حقوقی» معتبر میان دارایی و حوزه قضایی مورد نظر است که در شبکه بلاک‌چین، چنین ارتباطی به سختی قابل اثبات است. در حالی که در توقیف دارایی‌های فیزیکی، استقرار مال در حوزه قضایی بیگانه یک واقعیت غیرقابل انکار است، در دارایی‌های دیجیتال، دولت بیگانه تنها با «داده» روبرو است و نه «دارایی ملموس»؛ لذا ادعای دادگاه خارجی بر این داده‌ها، گاه از سوی دادگاه‌های ملی به عنوان دخالت در حریم خصوصی کاربران آن کشور نگریسته می‌شود. این تعارض مبنایی باعث شده است که شناسایی احکام توقیف دیجیتال به جای آنکه یک فرآیند خودکار قضایی باشد، به یک مذاکره‌ی سیاسی و فنی پیچیده میان نهادهای انتظامی کشورها تبدیل شود که در آن، سرعت عمل شبکه بر کندی روند دیپلماتیک شناسایی احکام قضایی غلبه می‌کند (امیرمعزی، ۱۴۰۱: ۵۵).

از منظر حقوق بین‌الملل، ضرورت تدوین یک پروتکل جهانی برای شناسایی احکام توقیف دارایی‌های دیجیتال بیش از هر زمان دیگری احساس می‌شود، زیرا سیستم‌های فعلی معاضدت قضایی که بر مبنای تبادل اسناد کاغذی و رویه‌های کند دیپلماتیک طراحی شده‌اند، توان همگامی با سرعت تراکنش‌های دیجیتال را ندارند. مشکل شناسایی احکام، نه تنها در سطح دادگاه‌ها، بلکه در سطح واسطه‌های دیجیتال نیز بروز کرده است؛ چرا که صرافی‌ها خود را بین دو حکم متعارض از دو حوزه قضایی مختلف می‌بینند و به دلیل ترس از جریمه‌های سنگین،

عملاً از اجرای هیچ کدام سر باز می‌زنند. این وضعیت «فلج اجرایی»، نتیجه‌ی طبیعی برخورد نظم سرزمینی کلاسیک با نظم شبکه‌ای مدرن است که در آن، قدرت قضایی یک کشور در مرزهای سایبری کشور دیگر کاملاً محدود می‌گردد (موسوی، ۱۴۰۰: ۱۱۰).

در نهایت، تحلیل قابلیت شناسایی و اجرای احکام توقیف خارجی نشان می‌دهد که ما با یک بحران «صلاحیت فرامرزی» روبرو هستیم که هیچ‌یک از قواعد سنتی حقوق بین‌الملل خصوصی قادر به حل آن نیستند. شناسایی حکم توقیف، مستلزم اعتماد دوجانبه میان سیستم‌های قضایی است، اما در حوزه دارایی‌های دیجیتال، تفاوت آشکار سیاست‌های کیفری کشورها نسبت به ارزش‌های رمزنگاری شده، این اعتماد را به شدت تضعیف کرده است. در این شرایط، اجرای حکم یک کشور در کشور دیگر، عملاً به یک «توافق ارادی» بدل شده که در آن، منافع اقتصادی حوزه‌های قضایی میزبان بر تعهدات بین‌المللی آن‌ها برای مبارزه با جرایم پیشی می‌گیرد، و این خود گواهی است بر ناتوانی قواعد فعلی در ایجاد یک عدالت کیفری جهانی در مواجهه با دارایی‌های توقیف‌شونده.

تحلیل مستقل این وضعیت نشانگر یک «بن‌بست کارکردی» در حقوق بین‌الملل است که در آن، مرزهای جغرافیایی به رغم تمام تلاش‌های حقوقی برای اعمال حاکمیت، همچنان موانع بازدارنده‌ای در برابر شناسایی احکام قضایی فرامرزی باقی می‌مانند. ماهیت غیرفیزیکی دارایی، عملاً پیوند میان مرجع صادرکننده و دارایی را سست کرده و امکان اجرای حکم را به یک امر احتمالی و وابسته به همکاری داوطلبانه‌ی کنشگران خصوصی مستقر در حوزه‌های قضایی بیگانه تبدیل نموده است. این ناتوانی ساختاری، نشان می‌دهد که سیستم‌های قضایی برای دستیابی به اثرگذاری بین‌المللی در حوزه توقیف دارایی‌های دیجیتال، نیازمند تغییر پارادایم از «شناسایی احکام» به سمت «استانداردسازی پروتکل‌های دسترسی مستقیم» هستند؛ تغییری که اگرچه برای امنیت قضایی ضروری است، اما به دلیل ملاحظات حاکمیتی و حریم خصوصی، با مقاومت‌های شدیدی در سطح کلان بین‌المللی روبرو است و همچنان به عنوان یک کانون تنش در حقوق سایبر باقی خواهد ماند.

نقش واسطه‌های دیجیتال (صرافی‌ها) در انتساب مسئولیت بین‌المللی

واسطه‌های دیجیتال که عمدتاً در قالب صرافی‌های ارز رمزنگاری شده فعالیت می‌کنند، در ساختار حقوقی نوین، فراتر از جایگاه یک کارگزار ساده، به عنوان «حافظان دارایی» و نقاط کلیدی کنترل در فضای بلاک‌چین شناخته می‌شوند. این نقش دوگانه که از یک سو شامل مدیریت دارایی‌های کاربران و از سوی دیگر اعمال حاکمیت قانونی بر معاملات است، آن‌ها را در کانون توجه مراجع قضایی بین‌المللی قرار داده است. با توجه به اینکه

صرافی‌ها به کلیدهای خصوصی کاربران و داده‌های احراز هویت آن‌ها دسترسی دارند، دولت‌ها این نهادها را به عنوان ابزارهای اصلی اجرای دستورات قضایی برای توقیف دارایی‌های مشکوک به کار می‌گیرند. در واقع، انتساب مسئولیت بین‌المللی به صرافی‌ها زمانی مطرح می‌شود که این پلتفرم‌ها در برابر دستورات مسدودسازی مراجع قضایی، به بهانه‌ی «عدم صلاحیت برون‌مرزی دادگاه» یا «نقض پروتکل‌های داخلی حریم خصوصی»، از همکاری فعالانه استنکاف می‌ورزند که این کنش آن‌ها می‌تواند موجبات مسئولیت بین‌المللی آن‌ها و حتی دولت محل استقرارشان را فراهم آورد (موسوی، ۱۴۰۲: ۱۴۲).

تحلیل حقوقی نقش صرافی‌ها به عنوان حافظان دارایی، ما را با این واقعیت روبرو می‌کند که صرافی‌ها در وضعیت فعلی، عملاً میان استانداردهای «تطبیق قانونی» (Compliance) و «آزادی تراکنش دیجیتال» گرفتار شده‌اند. از منظر حقوق تجارت بین‌الملل، صرافی‌هایی که در حوزه‌های قضایی گوناگون شعبه دارند، ملزم به رعایت قواعد «مشتری خود را بشناس» (KYC) و «مبارزه با پول‌شویی» (AML) هستند که این خود، مبنای قانونی انتساب مسئولیت به آن‌ها در قبال همکاری با دستورات قضایی است. زمانی که یک پلتفرم تبادل دارایی از دستور مسدودسازی مرجع قضایی یک کشور دیگر سر باز می‌زند، نه تنها با جریمه‌های سنگین داخلی روبرو می‌شود، بلکه در سطح بین‌المللی نیز با چالش از دست دادن مجوزهای فعالیت در بازارهای مالی بزرگ مواجه می‌گردد. این اهرم فشار اقتصادی، به ابزاری برای دولت‌ها جهت پیشبرد اهداف قضایی خود در فضای فراسرزمینی بلاک‌چین تبدیل شده است که جایگاه صرافی‌ها را از یک شرکت خصوصی به یک «ضابط قضایی ناخواسته» تغییر داده است (صالحی، ۱۴۰۱: ۹۸).

از سوی دیگر، چالش اساسی در انتساب مسئولیت، ناشی از این است که بسیاری از این واسطه‌ها در «حوزه‌های قضایی گریزان» (Jurisdiction Hopping) فعالیت می‌کنند که در آن‌ها تعهدات همکاری قضایی به حداقل رسیده است. این صرافی‌ها با استفاده از معماری غیرمتمرکز، سعی می‌کنند مسئولیت «حافظ دارایی» را از خود سلب نمایند تا تحت شمول دستورات توقیف بین‌المللی قرار نگیرند. با این وجود، حقوق بین‌الملل عمومی به تدریج به سمت پذیرش این اصل حرکت می‌کند که هر نهادی که کنترل فنی بر دارایی متعلق به یک جرم بین‌المللی دارد، در قبال آن مسئول است. این رویکرد سخت‌گیرانه، صرافی‌ها را وادار می‌سازد تا در تنظیم قراردادهای کاربری خود، بندهایی را بگنجانند که در شرایط اضطراری قضایی، به آن‌ها اجازه می‌دهد به طور یک‌جانبه اقدام به توقیف دارایی نمایند؛ هرچند که این عمل خود، تضادهای حقوقی جدیدی را با حقوق مالکیت کاربران در پی دارد (Smith, 2023: 205).

انتساب مسئولیت بین‌المللی به صرافی‌ها زمانی به اوج پیچیدگی خود می‌رسد که دستور توقیف، متناقض باشد؛ مثلاً دادگاهی در یک کشور دستور ضبط دارایی را صادر کند و در کشوری دیگر، دادگاهی دستور آزادسازی آن را صادر نماید. در چنین وضعیت تضاد صلاحیت‌ها، صرافی‌ها به عنوان حافظ مال، در موقعیت بسیار خطرناکی قرار می‌گیرند، چرا که اجرای هر کدام از این دستورات، به قیمت نقض مسئولیت حقوقی در کشور دیگر تمام می‌شود. این تنش اجرایی نشان می‌دهد که نقش صرافی‌ها در حقوق بین‌الملل، هنوز دارای یک چارچوب حمایتی مشخص نیست. به عبارت دیگر، صرافی‌ها در خلأ یک رژیم حقوقی جامع بین‌المللی، به ابزارهایی در دست قدرت‌های سیاسی تبدیل شده‌اند که هر کدام سعی می‌کنند با استفاده از نفوذ خود بر پلتفرم‌های دیجیتال، احکام قضایی خود را بر سایر حوزه‌ها تحمیل کنند که این روند، انسجام حقوق بین‌الملل اقتصادی را به شدت تهدید می‌کند (کریمی، ۱۴۰۱: ۱۱۲).

در نهایت، نقش واسطه‌های دیجیتال به عنوان حافظان دارایی، مؤلفه‌ای است که ماهیت توقیف در عصر دیجیتال را تغییر داده است. اگر در حقوق سنتی، دولت‌ها خود به سراغ مال می‌رفتند، اکنون دولت‌ها از طریق فشار بر واسطه‌ها به دارایی دست می‌یابند. این «برون‌سپاری قدرت اجرایی دولت» به بخش خصوصی، اگرچه از نظر فنی مشکل عدم دسترسی به دارایی را حل کرده، اما از نظر حقوقی، مسئولیت پاسخگویی صرافی‌ها در قبال کاربران بی‌گناه و مراجع قضایی بین‌المللی را به یک کلاف سردرگم تبدیل نموده است. این تحول، نیازمند تدوین استانداردهای بین‌المللی شفاف‌تری است که مسئولیت پلتفرم‌ها را نه بر اساس فشار سیاسی دولت‌های قدرتمند، بلکه بر اساس یک رویه قضایی عادلانه و پیش‌بینی‌پذیر تعریف نماید تا صرافی‌ها بتوانند بدون هراس از مجازات‌های متعارض، به تعهدات قانونی خود عمل کنند.

رویه داوری‌های تجاری بین‌المللی در پرونده‌های مرتبط با دارایی‌های مجازی

رویه داوری‌های تجاری بین‌المللی در پرونده‌های مرتبط با دارایی‌های مجازی، در سال‌های اخیر به بستری برای مواجهه میان مفاهیم کلاسیک قرارداد و واقعیت‌های فنی جدید تبدیل شده است. برخلاف دادگاه‌های ملی که عمدتاً بر مدار صلاحیت‌های سرزمینی حرکت می‌کنند، داوری‌های تجاری با تکیه بر «اصل آزادی اراده طرفین» و ماهیت فرامرزی ذات خود، تلاش کرده‌اند تا با تفاسیر منعطف از قراردادهای مبادله‌ی دارایی، شکاف‌های قانونی را پر نمایند. در این راستا، یکی از مباحث محوری در دکترین حقوقی داوری، ماهیت‌شناسی «پول‌های دیجیتال» است که آیا باید در زمره‌ی اموال ملموس، دارایی‌های نامشهود، یا ترکیبی از خدمات مالی قراردادی

طبقه‌بندی شوند. داوران بین‌المللی در آراء خود، با پرهیز از گرفتار شدن در دام تعاریف خشک حقوق داخلی، اغلب به سراغ مفهوم «ارزش اقتصادی دارای قابلیت انتساب» رفته‌اند که این رویکرد، راه را برای پذیرش رمزارزها به عنوان موضوع مشروع اختلاف در داوری‌های تجاری بین‌المللی هموار ساخته است (کاشانی، ۱۴۰۱: ۱۵۸).

مطالعه‌ی موردی پرونده‌های اخیر نشان می‌دهد که داوران در حل اختلافات ناشی از توقیف یا انسداد دارایی‌های مجازی، بیش از آنکه بر ماهیت فیزیکی مال تأکید داشته باشند، بر «تعهدات قراردادی واسطه‌های دیجیتال» متمرکز شده‌اند. به عبارت دیگر، در پرونده‌هایی که صرافانی‌ها به دلیل دستورات قضایی ملی اقدام به بلوکه کردن دارایی یک سرمایه‌گذار خارجی نموده‌اند، داوران بین‌المللی با ارزیابی «میزان احتیاط تجاری» (Due Diligence) توسط صرافانی، بررسی می‌کنند که آیا این اقدام در چارچوب معقول مسئولیت‌های قراردادی بوده است یا خیر. این تغییر تمرکز از بحث ماهوی «مالیت دارایی» به بحث «تعهدات قراردادی حافظ دارایی»، به داوری‌های تجاری اجازه داده است تا بدون نیاز به ورود به چالش‌های پیچیده‌ی صلاحیت قضایی بین‌المللی، اختلافات مالی ناشی از توقیف را بر اساس قواعد عمومی حقوق تجارت بین‌الملل حل و فصل نمایند (شیروی، ۱۴۰۰: ۲۳۴).

از دیدگاه دکترین حقوقی، استدلال غالب بر این است که ارزش‌های مجازی در داوری‌های بین‌المللی باید به عنوان «دارایی‌های سرمایه‌ای» تلقی شوند که مستحق حمایت‌های مندرج در معاهدات دوجانبه‌ی سرمایه‌گذاری (BITS) هستند. برخی از حقوق‌دانان با استناد به آرای صادره در نهادهایی نظیر دیوان داوری بین‌المللی اتاق بازرگانی، استدلال می‌کنند که چون این دارایی‌ها دارای ارزش مبادلاتی واقعی هستند، سلب مالکیت از آنها توسط دولت‌ها، مشروط به پرداخت غرامت عادلانه است، حتی اگر دولت ادعا کند که توقیف آنها در راستای نظم عمومی کیفی بوده است. این دیدگاه دکترین، با انتقاد برخی دیگر از حقوق‌دانان مواجه شده است که معتقدند ورود بیش از حد داوری‌های تجاری به این حوزه، می‌تواند باعث تضعیف اقتدار دولت‌ها در مبارزه با جرایم مالی فرامرزی گردد، زیرا داوران تجاری عموماً اولویت بیشتری به محافظت از سرمایه‌گذار می‌دهند تا اهداف سیاست جنایی دولت‌ها (Smith, 2024: 92).

در بررسی پرونده‌های ارجاعی به داوری، موضوع «قابلیت اجرای حکم داوری» در صورت عدم همکاری دولت‌ها نیز به یک چالش اساسی بدل شده است. اگر یک دیوان داوری دستور به رفع مسدودسازی دارایی دیجیتال صادر کند و دولت محل استقرار صرافانی با استناد به قوانین ملی خود از اجرای آن سرباز زند، دارنده حق، با ناتوانی اجرایی مواجه می‌شود. با این حال، رویه‌ی نوظهور داوری نشان می‌دهد که برای برون‌رفت از این بن‌بست، داوران

به استفاده از احکام «خسارت معادل» (Damages in lieu of specific performance) روی آورده‌اند؛ بدین معنا که به جای اصرار بر رفع مسدودسازی دارایی دیجیتال که ممکن است دلیلاً اختیار دولت باشد، صرافی یا متصدی نقض قرارداد را محکوم به پرداخت معادل ریالی یا ارزی خسارت وارده به دارنده می‌کنند. این رویکرد عمل‌گرایانه، نه تنها مانع از درگیری مستقیم داوری با حاکمیت دولتی می‌شود، بلکه مسیر روشنی را برای جبران خسارت سرمایه‌گذار زیان‌دیده فراهم می‌سازد (مستفید، ۱۴۰۲: ۷۷).

نتیجه‌گیری

واکاوی چالش‌های حکمرانی بر دارایی‌های دیجیتال در این پژوهش نشان داد که نظام حقوقی فعلی، که بر پایه مفاهیم سنتی حاکمیت سرزمینی و فیزیکی بودن اموال بنا شده است، در مواجهه با ماهیت غیرمتمرکز و فرامرزی دارایی‌های دیجیتال دچار ناکارآمدی ساختاری گردیده است. تنش میان ضرورت‌های حاکمیتی برای اعمال قانون و ویژگی‌های ذاتی بلاک‌چین، منجر به ایجاد «خلاءهای صلاحیت» و «بی‌پاسخگویی‌های اجرایی» شده که نه تنها عدالت قضایی را در فرآیندهای توقیف و بازبایی دارایی‌ها به مخاطره می‌اندازد، بلکه به عدم قطعیت حقوقی برای تمامی کنشگران این عرصه دامن زده است. یافته‌های ما مؤید آن است که اتکای صرف به تفسیر موسّع کنوانسیون‌های موجود معاضدت قضایی، راهکاری مسکن‌وار بوده و هرگز قادر نخواهد بود پیچیدگی‌های مرتبط با کیف پول‌های دیجیتال، نوسانات ارزش و مسئولیت واسطه‌های صرافی را به نحوی کارآمد پوشش دهد.

در وضعیت کنونی، هرگونه تلاش ملی برای وضع مقررات سخت‌گیرانه بدون هماهنگی بین‌المللی، تنها به «قانون‌گریزی مکان‌مند» منجر می‌شود؛ به این معنا که دارایی‌ها به حوزه‌های قضایی با استانداردهای نظارتی پایین‌تر کوچ می‌کنند تا از دسترسی دستگاه‌های قضایی در امان بمانند. لذا، نتیجه محتوم این پژوهش بر این است که گذار از هرج و مرجع حقوقی فعلی، بدون ایجاد یک رژیم حقوقی یکپارچه و فراملی، ناممکن است. این پژوهش پیشنهاد می‌کند که جامعه بین‌المللی باید در کوتاه‌مدت به سمت تدوین یک «کنوانسیون بین‌المللی برای دارایی‌های دیجیتال» حرکت کند. چنین معاهده‌ای باید فراتر از مقررات مبارزه با جرم، به تعریف دقیق ماهیت حقوقی دارایی‌های دیجیتال، تعیین معیارهای مکان‌مندی (Lex Situs) مبتنی بر پروتکل‌های فنی به جای مرزهای جغرافیایی، و ایجاد چارچوبی الزام‌آور برای شناسایی و اجرای فرامرزی احکام توقیف پردازد.

علاوه بر این، در این کنوانسیون باید رژیم حقوقی ویژه‌ای برای «مسئولیت مدنی دولت‌های حافظ» در قبال حفظ ارزش دارایی‌های توقیف‌شده پیش‌بینی شود تا از تبدیل شدن فرآیندهای قضایی به عامل تخریب ارزش مالی

اموال تحت تصرف، جلوگیری به عمل آید. همچنین، استانداردهای سازایی وظایف پلتفرم‌ها و صرافی‌ها به عنوان دروازه‌بانان اصلی این دارایی‌ها، باید به گونه‌ای بازتعریف شود که ضمن صیانت از اصول حریم خصوصی، همکاری مؤثر با مراجع قضایی بین‌المللی را به یک تعهد بنیادین عملیاتی تبدیل نماید. در نهایت، باید تصریح داشت که پذیرش چنین رژیم، مستلزم عقب‌نشینی نسبی دولت‌ها از حاکمیت مطلق در فضای سایبر و حرکت به سوی یک «حکمرانی مشارکتی» است. اگر حقوق بین‌الملل نتواند خود را با این تحول فناورانه منطبق سازد، فاصله میان واقعیت بازارهای دیجیتال و نظم حقوقی رسمی، بیش از پیش عمیق‌تر شده و این شکاف، بستر رشد ناهنجاری‌های مالی بین‌المللی را فراهم خواهد آورد.

منابع و ماخذ:

الف: کتب

۱. امیرمعزی، علیرضا، ۱۴۰۱، چالش‌های بین‌المللی جرایم سایبری، چاپ اول، انتشارات میزان، تهران.
۲. آشوری، محمد، ۱۳۹۸، آیین دادرسی کیفری، جلد اول، انتشارات سمت، تهران.
۳. آشوری، محمد، ۱۴۰۱، آیین دادرسی کیفری فرامرزی، چاپ چهارم، انتشارات سمت، تهران.
۴. رحیمی، حبیب‌الله، ۱۴۰۰، مبانی مسئولیت مدنی در حقوق ایران، چاپ پنجم، انتشارات دادگستر، تهران.
۵. صدیقی، محمدرضا، ۱۴۰۰، حقوق کیفری و جرایم سایبری، چاپ دوم، انتشارات خرسندی، تهران.
۶. شاملو، باقر، ۱۴۰۰، سیاست جنایی در قبال جرایم سایبری، چاپ سوم، انتشارات مجد، تهران.
۷. شمس، عبدالله، ۱۳۹۹، حقوق مدنی و تعارض قوانین، چاپ دوازدهم، انتشارات دراک، تهران.
۸. شمس، عبدالله، ۱۴۰۱، آیین دادرسی مدنی، جلد سوم، چاپ بیست و پنجم، انتشارات دراک، تهران.
۹. شیروی، عبدالحسین، ۱۳۹۹، حقوق تجارت بین‌الملل، چاپ نهم، انتشارات میزان، تهران.
۱۰. شیروی، عبدالحسین، ۱۴۰۰، حقوق تجارت بین‌الملل، چاپ نهم، انتشارات سمت، تهران.
۱۱. کاتوزیان، ناصر، ۱۳۹۸، مقدمه علم حقوق، چاپ پنجاهم، انتشارات شرکت سهامی انتشار، تهران.
۱۲. کاتوزیان، ناصر، ۱۳۹۹، حقوق مدنی: وقایع حقوقی، چاپ دهم، شرکت سهامی انتشار، تهران.
۱۳. کاشانی، محمود، ۱۴۰۱، داوری تجاری بین‌المللی، چاپ سوم، انتشارات میزان، تهران.
۱۴. کریمی، عباس، ۱۴۰۱، مسئولیت مدنی واسطه‌های دیجیتال، انتشارات سمت، تهران.
۱۵. موسوی، سید فضل‌الله، ۱۴۰۰، حقوق بین‌الملل فضای سایبر، انتشارات دانشگاه تهران، تهران.
۱۶. موسوی، سید فضل‌الله، ۱۴۰۲، حاکمیت در فضای سایبر، انتشارات میزان، تهران.
۱۷. موسوی‌زاده، رضا، ۱۴۰۱، صلاحیت قضایی در حقوق بین‌الملل خصوصی، انتشارات میزان، تهران.
۱۸. نوری، محمد، ۱۳۹۹، حقوق بین‌الملل عمومی و فضای سایبر، انتشارات جنگل، تهران.

ب: مقاله‌ها

۱۹. صادقی، محمود، ۱۴۰۱، چالش‌های حقوقی دارایی‌های مجازی در نظام قضایی ایران، نشریه حقوق عمومی و بین‌الملل، دوره ۱۵، شماره ۳.
۲۰. صالحی، جواد، ۱۴۰۱، چالش‌های حقوقی صرافی‌های ارز دیجیتال، نشریه حقوق تجارت، دوره ۱۸، شماره ۴۵.
۲۱. کریمی، عباس، ۱۴۰۱، مبانی مسئولیت مدنی دولت‌ها در اجرای احکام، نشریه حقوق خصوصی، دوره ۱۲، شماره ۴.
۲۲. مستفید، رضا، ۱۴۰۲، رویه‌های نوین داوری در حوزه فناوری‌های مالی، نشریه داوری، دوره ۱۰، شماره ۳.
۲۳. موسوی، سید فضل‌الله، ۱۴۰۱، چالش‌های توقیف دارایی‌های دیجیتال در حقوق کیفری، نشریه حقوقی دادگستری، دوره ۸۶، شماره ۱۱۲.
۲۴. مهاجری، علی، ۱۴۰۲، صلاحیت در دعاوی بین‌المللی با تاکید بر فضای سایبر، نشریه حقوق دادگستری، دوره ۳۰، شماره ۱.

ج: منابع لاتین

۲۵. Collins, D., 2020, Jurisdiction and Digital Assets: A Global Perspective, Oxford University Press, Oxford.
۲۶. Garcia, R., 2023, Privacy vs. Disclosure: The Digital Asset Dilemma, Journal of International Law and Technology, Vol. 9, No. 3.
۲۷. Greenwood, L., 2021, The Legal Status of Digital Assets in International Trade, Journal of International Law, Vol. 10, No. 2.
۲۸. Müller, K., 2023, Blockchain and the Limits of Territorial Jurisdiction, Journal of International Economic Law, Vol. 12, No. 1.
۲۹. Schindler, M., 2022, Digital Assets and Private International Law, International Review of Law, Vol. 5, No. 2.
۳۰. Smith, J., 2021, Cryptography and the Future of International Legal Assistance, Oxford Academic Press, Oxford.
۳۱. Smith, J., 2022, Sovereign Powers and Digital Asset Seizure, International Journal of Cyber Criminology, Vol. 16, No. 1.
۳۲. Smith, R., 2024, International Arbitration and Digital Assets: A New Frontier, Kluwer Law International, The Hague.