Comparative Studies in Jurisprudence, Law, and Politics

Transformation of the Concept of "Property" in Iranian and Japanese Criminal Law and Its Impact on the Protection of Digital Assets

1. Rasool Moradi Emamgheisi: PhD Student, Department of Law, Na.C., Islamic Azad University, Najafabad, Iran
2. Yasin Saeedi*: Department of Law, Isf.C., Islamic Azad University, Isfahan, Iran.
Email: Yasinsaeedi@iau.ac.ir (Corresponding Author)
3. Razie Ghasemi: Department of Law, Ti.C., Islamic Azad University, Tiran, Iran

ABSTRACT

This study aims to comparatively examine the transformation of the concept of "property" in Iranian and Japanese criminal law and to analyze its impact on the criminal-law protection of digital assets in the metaverse. The principal research question is: What differences exist between the Iranian and Japanese legal systems in their understanding of the concept of "property," and how do these differences affect the manner in which digital assets in the metaverse are protected under criminal law? The findings indicate that, in Japan, there is a more pronounced tendency to recognize digital assets as property, which has contributed to strengthening criminal-law safeguards against offenses such as theft, fraud, and forgery committed within the metaverse. By contrast, in Iran, due to a restrictive interpretation of the concept of "property" and the absence of explicit statutory provisions, an adequate legal framework for the criminal protection of such assets has not yet been established. This study employs a descriptive-analytical method with a comparative approach and draws upon library-based sources, domestic and international legal instruments, and the legal practices of the two countries. The results may contribute to the formulation of legislative reform proposals in Iran and to the enhancement of criminal-law protection for digital assets in the metaverse.

Keywords: *transformation of the concept of property, criminal law, Iran, Japan, digital assets, metaverse, criminal-law protection, cybercrime.*

How to cite: Moradi Emamgheisi, R., Saeedi, Y., & Ghasemi, R. (2027). Transformation of the Concept of "Property" in Iranian and Japanese Criminal Law and Its Impact on the Protection of Digital Assets. *Comparative Studies in Jurisprudence, Law, and Politics*, *9*(3), 1-16.

© 2027 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Submit Date: 30 March 2026
Revise Date: 14 September 2026
Accept Date: 21 September 2026
Initial Publish Date: 12 October 2026
Final Publish Date: 23 August 2027

پژوهش‌های تطبیقی فقه، حقوق و سیاست

تحول مفهوم «مال» در حقوق کیفری ایران و ژاپن و تأثیر آن بر حمایت از دارایی‌های دیجیتال

۱. رسول مرادی امام‌قیسی: دانشجوی دکتری، گروه حقوق، واحد نجف‌آباد، دانشگاه آزاد اسلامی، نجف‌آباد، ایران
۲. یاسین صعیدی*: گروه حقوق، واحد اصفهان (خوارسگان)، دانشگاه آزاد اسلامی، اصفهان، ایران. پست الکترونیک: Yasinsaeedi@iau.ac.ir (نویسنده مسئول)
۳. راضیه قاسمی: گروه حقوق، واحد تیران، دانشگاه آزاد اسلامی، تیران، ایران

چکیده

هدف این پژوهش بررسی تطبیقی تحول مفهوم «مال» در حقوق کیفری ایران و ژاپن و تحلیل تأثیر آن بر حمایت کیفری از دارایی‌های دیجیتال در متاورس است. سؤال اصلی پژوهش این است که چه تفاوت‌هایی در برداشت از مفهوم «مال» میان دو نظام حقوقی ایران و ژاپن وجود دارد و این تفاوت‌ها چگونه بر نحوه حمایت کیفری از دارایی‌های دیجیتال در متاورس اثرگذار است؟ یافته‌های پژوهش نشان می‌دهد که در ژاپن گرایش به شناسایی دارایی‌های دیجیتال به عنوان مال مشهودتر است و این امر موجب تقویت ضمانت‌های کیفری در قبال جرایمی همچون سرقت، کلاهبرداری و جعل در فضای متاورس شده است. در حالی که در ایران به دلیل تفسیر محدود از مفهوم «مال» و فقدان قوانین صریح، بستر مناسبی برای حمایت کیفری از این نوع دارایی‌ها وجود ندارد. روش تحقیق در این مقاله به صورت توصیفی ـ تحلیلی و با رویکرد تطبیقی است که از منابع کتابخانه‌ای، قوانین داخلی و بین‌المللی و رویه‌های حقوقی دو کشور استفاده شده است. نتایج پژوهش می‌تواند به ارائه راهکارهای اصلاحی برای قانون‌گذاری در ایران و ارتقای حمایت کیفری از دارایی‌های دیجیتال در متاورس منجر شود.

واژگان کلیدی: *تحول مفهوم مال، حقوق کیفری، ایران، ژاپن، دارایی‌های دیجیتال، متاورس، حمایت کیفری، جرایم سایبری.*

نحوه استناددهی: مرادی امام‌قیسی، رسول.، صعیدی، یاسین.، و قاسمی، راضیه. (۱۴۰۶). تحول مفهوم «مال» در حقوق کیفری ایران و ژاپن و تأثیر آن بر حمایت از دارایی‌های دیجیتال. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۹(۳)، ۱۶-۱.

© ۱۴۰۶ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

تاریخ ارسال: ۱۰ فروردین ۱۴۰۵
تاریخ بازنگری: ۲۳ شهریور ۱۴۰۵
تاریخ پذیرش: ۳۰ شهریور ۱۴۰۵
تاریخ چاپ اولیه: ۲۰ مهر ۱۴۰۵
تاریخ چاپ نهایی: ۱ شهریور ۱۴۰۶

مقدمه

تحولات پرشتاب فناوری‌های نوین، به‌ویژه در عرصه دارایی‌های دیجیتال و متاورس، موجب بروز دگرگونی‌های اساسی در نظام‌های حقوقی و به‌ویژه در قلمرو حقوق کیفری شده است. متاورس به‌عنوان بستری نوین برای تعاملات انسانی و اقتصادی، مفاهیمی چون مالکیت، دارایی و حق بهره‌مندی را به سطحی جدید منتقل کرده است. در این بستر، اشیاء دیجیتال نه‌تنها ارزش اقتصادی دارند، بلکه به‌عنوان «اموال» نوظهور، در معرض تهدیدهای کیفری متعددی همچون کلاهبرداری، سرقت، جعل و پول‌شویی قرار می‌گیرند. در نتیجه، بازاندیشی در مفهوم «مال» در حقوق کیفری و میزان شمول آن بر دارایی‌های دیجیتال ضرورتی انکارناپذیر یافته است.

در ایران، قوانین کیفری سنتی و حتی قانون جرایم رایانه‌ای مصوب ۲۰۰۹، نتوانسته‌اند پاسخی کافی به پرسش‌های نوپدید درباره ماهیت دارایی‌های دیجیتال و نحوه حمایت کیفری از آن‌ها بدهند. برداشت محدود از مفهوم «مال» در حقوق کیفری ایران سبب شده است که بسیاری از بزه‌دیدگان فضای متاورس امکان احقاق حق و برخورداری از حمایت مؤثر را نداشته باشند. در مقابل، ژاپن با بهره‌گیری از قوانین مرتبط با جرایم سایبری و مقررات ناظر بر دارایی‌های رمزنگاری‌شده، تلاش کرده است مفهوم «مال» را با تحولات فناوری هماهنگ کند و با این رویکرد، بستر حقوقی کارآمدتری برای حمایت کیفری از دارایی‌های دیجیتال فراهم ساخته است.

با وجود اهمیت این موضوع، بررسی تطبیقی تحول مفهوم «مال» در حقوق کیفری ایران و ژاپن تاکنون کمتر مورد توجه پژوهش‌های داخلی قرار گرفته است. تحقیقات موجود عمدتاً بر حقوق ایران و تا حدودی اتحادیه اروپا متمرکز بوده و ژاپن، با وجود پیشرفت‌های چشمگیرش در تنظیم مقررات دارایی‌های دیجیتال و برخورد با جرایم سایبری، کمتر در کانون توجه پژوهشگران ایرانی قرار گرفته است. از سوی دیگر، متاورس به‌عنوان پدیده‌ای نوظهور، هنوز در ابتدای راه خود قرار دارد و در ادبیات حقوقی کشور نیز بحث‌های جدی و نظام‌مند درباره ابعاد کیفری آن صورت نگرفته است. از این رو، ضرورت دارد پژوهشی جامع، با تکیه بر مطالعه تطبیقی، به بررسی تأثیر تحول مفهوم «مال» بر حمایت کیفری از دارایی‌های دیجیتال در متاورس بپردازد و راهکارهای اصلاحی برای نظام حقوقی ایران ارائه دهد.

نوآوری این مقاله در دو محور اصلی است: نخست، تمرکز بر ژاپن به‌عنوان نظام حقوقی‌ای که در ادبیات داخلی کمتر بدان پرداخته شده و می‌تواند الگوی مفیدی برای ایران باشد؛ دوم، پرداختن به متاورس به‌عنوان عرصه‌ای کاملاً جدید که مباحث حقوق کیفری سنتی را با چالش‌های بی‌سابقه‌ای روبه‌رو ساخته است. این نوآوری‌ها مقاله حاضر را از پژوهش‌های پیشین متمایز کرده و آن را به منبعی ارزشمند برای غنای مباحث نظری و اصلاح قوانین کیفری ایران در حوزه دارایی‌های دیجیتال بدل می‌سازد.

۱- مفهوم مال در حقوق سنتی

در حقوق سنتی، «مال» به چیزی اطلاق می‌شود که دارای ارزش اقتصادی بوده، قابلیت اختصاص یافتن به شخص معین را داشته باشد و نیازهای مادی یا معنوی انسان را برآورده سازد. فقهای اسلامی نیز در تعریف مال، معیارهایی همچون منفعت عقلایی، قابلیت بقا و امکان تصرف مشروع را مورد توجه قرار داده‌اند (Ayoubi, 2024). بدین ترتیب، اموالی همچون زمین، مسکن، حیوانات، محصولات کشاورزی و به‌طور کلی اشیاء محسوس و قابل لمس، مصادیق اصلی مال در حقوق سنتی محسوب می‌شوند. در حقوق مدنی ایران نیز، مال معمولاً به اشیاء مادی و دارایی‌های قابل دادوستد محدود شده است و از این رو، ارزش‌گذاری بر اشیاء غیرملموس چندان رایج نبوده است.

ضرورت بازاندیشی در مفهوم مال در پرتو فناوری‌های نوین (ارتباط با دارایی‌های دیجیتال و متاورس)

در حقوق کنونی، مفهوم مال دیگر صرفاً به اشیاء مادی و محسوس محدود نمی‌شود، بلکه شامل هر آن چیزی است که دارای ارزش اقتصادی و قابلیت دادوستد باشد. هرچند قانون مدنی ایران تعریفی صریح از «مال» ارائه نداده است، اما با بررسی مواد مختلفی چون ۱۲۱۷، ۱۲۱۴، ۹۴۶ و ۸۷۲ می‌توان دریافت که قانون‌گذار، مال را در معنای گسترده آن در نظر گرفته است؛ به‌گونه‌ای که هم اموال مادی (مانند زمین و منقولات) و هم حقوق مالی (مانند طلب، حق سرقفلی و سهام) در این مفهوم می‌گنجند. به تعبیر کاتوزیان، حق مالی امتیازی است که نظام حقوقی هر کشور برای تأمین نیازهای مادی افراد به آن‌ها اعطا می‌کند (Katouzian, 2006). بنابراین، در حقوق مدنی معاصر، «مال» هم شامل دارایی‌های عینی و ملموس است و هم شامل حقوق و امتیازات غیرمادی با ارزش اقتصادی.

در حقوق کیفری نیز تحول مشابهی رخ داده است. در گذشته، «مال» صرفاً به اشیاء فیزیکی و ملموس اطلاق می‌شد و جرایمی چون سرقت، کلاهبرداری یا خیانت در امانت تنها ناظر بر اموال مادی بودند. اما با گسترش مناسبات اقتصادی و ظهور دارایی‌های اعتباری و غیرملموس، قانون‌گذار و رویه قضایی ناگزیر از پذیرش مفهوم گسترده‌تر مال شدند. امروزه اوراق بهادار، سهام، مطالبات و حتی داده‌های الکترونیکی و اطلاعات مالی، در زمره اموال قابل حمایت کیفری قرار گرفته‌اند. این تحول نشان می‌دهد که مفهوم سنتی مال در حقوق کیفری نیز دچار دگرگونی شده و زمینه برای پذیرش دارایی‌های نوینی چون دارایی‌های دیجیتال و متاورس فراهم شده است.

پیشرفت‌های فناوری در عرصه دیجیتال، به‌ویژه ظهور دارایی‌های دیجیتال و محیط‌های نوینی مانند متاورس، نشان داده است که تعریف سنتی و حتی کنونی «مال» در حقوق موجود، پاسخگوی همه نیازهای نوین نیست (Fairfield, 2022). دارایی‌هایی نظیر رمزارزها، توکن‌های غیرقابل تعویض [NFTs] و دارایی‌های مجازی در متاورس، واجد ارزش اقتصادی واقعی‌اند و قابلیت دادوستد، انتقال و حتی مصادره یا سرقت را دارند، اما از آنجا که فاقد ماهیت فیزیکی هستند، در قالب سنتی مال به‌سختی می‌گنجند. این شکاف میان واقعیت‌های نوین اقتصادی و چارچوب‌های حقوقی سنتی، ضرورت بازاندیشی در مفهوم مال را آشکار می‌سازد. از منظر حقوق کیفری نیز، پذیرش این نوع دارایی‌ها به‌عنوان «مال» اهمیت بسزایی دارد؛ زیرا بدون این بازتعریف، حمایت کیفری از اشخاص در برابر جرایمی مانند سرقت هویت دیجیتال، کلاهبرداری اینترنتی یا ربایش دارایی‌های مجازی با دشواری مواجه می‌شود. بنابراین، بازاندیشی در مفهوم مال نه‌تنها پاسخی به تحولات فناوری است، بلکه ضرورتی برای کارآمدی نظام‌های حقوقی و کیفری در عصر دیجیتال به شمار می‌رود.

۲- بررسی تطبیقی حقوق ایران و ژاپن در تحول مفهوم مال

تحول مفهوم «مال» در پرتو فناوری‌های نوین، از جمله دارایی‌های دیجیتال و مجازی، یکی از مهم‌ترین چالش‌های حقوق کیفری معاصر است. در حالی که در گذشته، مال به اشیاء مادی و محسوس محدود بود، امروزه دارایی‌هایی مانند رمزارزها، توکن‌های غیرقابل تعویض و سایر دارایی‌های دیجیتال جایگاه ویژه‌ای در مبادلات اقتصادی و اجتماعی پیدا کرده‌اند. همین امر سبب شده است که نظام‌های حقوقی مختلف برای حمایت کیفری از این دارایی‌ها، ناگزیر از بازتعریف و گسترش مفهوم سنتی مال شوند. بررسی تطبیقی نظام‌های حقوقی می‌تواند نشان دهد که چگونه کشورها به‌طور متفاوت با این چالش مواجه شده‌اند و چه راهکارهایی را برای تأمین حمایت کیفری کارآمد در برابر جرایم نوین برگزیده‌اند. در این میان، ایران و ژاپن دو نمونه قابل توجه به شمار می‌آیند. در ایران، هرچند قانون جرایم رایانه‌ای (۲۰۰۹) برخی از ابعاد حمایت کیفری از داده‌ها و اطلاعات را پیش‌بینی کرده است، اما هنوز جایگاه دقیق دارایی‌های دیجیتال به‌عنوان «مال» در حقوق کیفری با چالش‌های مفهومی و تفسیری روبه‌روست. در مقابل، ژاپن با بهره‌گیری از قوانین پیشرفته در حوزه جرایم سایبری و مقررات مربوط به

دارایی‌های رمزنگاری‌شده، گام‌هایی در جهت شناسایی گسترده‌تر این نوع دارایی‌ها برداشته است. بنابراین، مقایسه تطبیقی این دو نظام حقوقی می‌تواند نقاط ضعف و قوت هر یک را آشکار ساخته و چشم‌انداز مناسبی برای اصلاح و بازاندیشی در حقوق کیفری ایران فراهم آورد.

جایگاه دارایی‌های دیجیتال در حقوق کیفری ایران (قانون جرایم رایانه‌ای و چالش‌های مفهومی)

در حقوق کیفری ایران، هنوز تعریف روشنی از «دارایی‌های دیجیتال» وجود ندارد و قانون‌گذار بیشتر بر حمایت از «داده‌ها و سامانه‌های رایانه‌ای» تمرکز کرده است. قانون جرایم رایانه‌ای مصوب ۲۰۰۹، برخی رفتارها مانند دسترسی غیرمجاز، شنود داده‌ها، جعل و کلاهبرداری رایانه‌ای را جرم‌انگاری کرده است، اما این مقررات بیشتر ناظر به حمایت از محرمانگی، تمامیت و صحت داده‌ها هستند تا شناسایی «دارایی دیجیتال» به‌عنوان «مال». به بیان دیگر، این قانون با اینکه زمینه حمایت کیفری از فضای سایبری را فراهم کرده است، اما در خصوص اینکه آیا دارایی‌های دیجیتال همانند رمزارزها یا دارایی‌های متاورسی قابلیت شمول در عنوان «مال» را دارند یا خیر، سکوت دارد. این وضعیت موجب بروز چالش‌های مفهومی و تفسیری در محاکم شده است. در مواردی، دادگاه‌ها برای حمایت از بزه‌دیدگان، تلاش کرده‌اند با تفسیر موسع از مفاهیمی همچون «اموال»، «وجوه» یا «حقوق مالی» به دارایی‌های دیجیتال نیز شمول بدهند، اما این رویه یکنواخت و کافی نیست. از منظر کیفری، تا زمانی که دارایی‌های دیجیتال به‌صراحت در تعریف «مال» یا در قوانین حمایتی مستقل وارد نشوند، حمایت کامل و کارآمد از صاحبان این دارایی‌ها دشوار خواهد بود. به همین دلیل، یکی از چالش‌های اصلی نظام حقوقی ایران، بازاندیشی در تعریف مال و ایجاد پیوند روشن میان مفاهیم سنتی حقوق کیفری و واقعیت‌های نوین اقتصادی و دیجیتال است. به‌عنوان مثال، در حقوق ایران، توقیف ارزهای دیجیتال به‌عنوان یکی از مصادیق نوین و پیچیده دارایی‌ها، با چالش‌های قابل توجهی همراه است. قوانین موجود، به‌ویژه قانون اجرای احکام مدنی و قانون نحوه اجرای محکومیت‌های مالی، در اصل برای اموال فیزیکی یا دارایی‌های مالی سنتی طراحی شده‌اند. با این حال، قواعد کلی این قوانین، مانند ماده ۶۲ قانون اجرای احکام مدنی، ظرفیت‌هایی برای شمول دارایی‌های نوین نیز دارند (Gholami et al., 2023)؛ زیرا طبق این ماده، هر مالی که قابلیت تملک و انتقال داشته باشد، می‌تواند موضوع توقیف قرار گیرد. بر این اساس، ارزهای دیجیتال به دلیل ارزش اقتصادی و قابلیت انتقال، به‌صورت تفسیری موسع، می‌توانند در زمره اموال قابل توقیف قرار گیرند.

با وجود این ظرفیت قانونی، اجرای توقیف ارزهای دیجیتال در عمل با موانع فنی و نهادی روبه‌رو است. ارزهای دیجیتال ممکن است در صرافی‌های آنلاین بین‌المللی مانند Binance یا Coinbase نگهداری شوند که در بسیاری موارد خارج از دسترس مستقیم محاکم داخلی هستند. همچنین، نگهداری ارز دیجیتال در کیف‌پول‌های دیجیتال (سخت‌افزاری یا نرم‌افزاری) شناسایی و توقیف آن را دشوارتر می‌سازد. بر اساس مقررات، بار اثبات مالکیت و معرفی محل نگهداری دارایی دیجیتال بر عهده محکوم‌له است (Banaei Oskouei & Jalali, 2022). در صورت ارائه مستندات کافی، دادگاه می‌تواند از صرافی مربوطه استعلام کند و دستور توقیف صادر نماید. با این حال، به دلیل ماهیت غیرمتمرکز فناوری بلاکچین و پیچیدگی تعاملات مالی دیجیتال، نیاز به همکاری مؤثر میان نهادهای قضایی، بانک مرکزی و پلتفرم‌های مالی به‌وضوح احساس می‌شود. این امر نشان می‌دهد که علی‌رغم وجود بسترهای حقوقی، بازنگری و اصلاح قوانین برای پوشش صریح دارایی‌های دیجیتال امری اجتناب‌ناپذیر است.

جایگاه دارایی‌های دیجیتال در حقوق کیفری ژاپن (قوانین سایبری و رمزنگاری‌شده و تفسیر گسترده از مال)

در حقوق کیفری ژاپن، دارایی‌های دیجیتال از جایگاه ویژه‌ای برخوردار شده‌اند، زیرا مقنن این کشور با درک اهمیت اقتصادی و خطرات ناشی از جرایم سایبری، تلاش کرده است با ابزارهای قانونی جدید، آن‌ها را در زمره اموال مورد حمایت کیفری قرار دهد (Lyaskalo, 2023).

اگرچه قانون مدنی ژاپن دارایی‌های رمزنگاری‌شده را به‌طور صریح در زمره اموال سنتی قرار نمی‌دهد و آن‌ها را بیشتر به‌عنوان «ادعا علیه صرافی‌های رمزنگاری‌شده» تفسیر می‌کند، اما در عمل رویه قضایی و قوانین کیفری تفسیر گسترده‌تری ارائه داده‌اند. در نتیجه، در صورت وقوع جرایمی همچون کلاهبرداری، سرقت یا سوءاستفاده از رمزارزها، دادگاه‌ها این دارایی‌ها را مشمول حمایت کیفری از مال دانسته و امکان تعقیب کیفری مرتکبان را فراهم ساخته‌اند. این رویکرد نشان می‌دهد که مفهوم «مال» در حقوق کیفری ژاپن دیگر محدود به دارایی‌های مادی نیست و دارایی‌های دیجیتال نیز تحت شمول آن قرار می‌گیرند.

از منظر تقنین، قانون خدمات پرداخت (Payment Services Act – PSA) و قانون ابزارهای مالی و مبادلات (Financial Instruments and Exchange Act – FIEA) نقش کلیدی در تنظیم جایگاه کیفری دارایی‌های دیجیتال دارند. PSA با تعریف «دارایی رمزنگاری‌شده» و الزام صرافی‌ها به ثبت و رعایت الزامات امنیتی، شرایطی را ایجاد کرده که تخلفات مرتبط با صرافی‌ها و جرایم علیه دارایی‌های دیجیتال قابل پیگیری کیفری باشد (Harata, 2025). در مقابل، FIEA با شناسایی رمزارزها به‌عنوان ابزار مالی و الزام شرکت‌ها به ثبت به‌عنوان ارائه‌دهنده خدمات مالی، امکان برخورد کیفری با تخلفات در فرآیند عرضه یا دادوستد رمزارزها را فراهم می‌کند. بدین ترتیب، در ژاپن دو بستر قانونی مکمل به‌طور هم‌زمان عمل می‌کنند: یکی برای ساماندهی فعالیت‌های بازار و دیگری برای تضمین حمایت کیفری از سرمایه‌گذاران و کاربران.

علاوه بر این، تجربه‌های عملی ژاپن در پرونده‌های بزرگ مانند ورشکستگی صرافی Mt.Gox یا حملات سایبری به صرافی Coincheck نشان داده است که دادگاه‌ها با تفسیر موسع از مفهوم مال، دارایی‌های دیجیتال را مشمول توقیف و مصادره قرار داده‌اند (Kavaloski, 2024). در این پرونده‌ها، ارزهای دیجیتال به‌عنوان دارایی‌های ارزشمند و قابل انتقال تلقی شده‌اند که می‌توانند موضوع جرم واقع شوند یا به‌عنوان اموال حاصل از جرم توقیف گردند. همین رویه عملی، همراه با قوانین تقنینی، سبب شده است که ژاپن یکی از پیشروترین نظام‌های حقوقی در شناسایی و حمایت کیفری از دارایی‌های دیجیتال باشد؛ رویکردی که تفاوت آشکاری با حقوق ایران دارد که همچنان بیشتر بر تفسیر موسع از قواعد عمومی اتکا دارد.

۳- چالش‌های حمایت کیفری از دارایی‌های دیجیتال در متاورس

با گسترش متاورس و ورود دارایی‌های دیجیتال به محیط‌های مجازی، نظام‌های کیفری ایران و ژاپن با چالش‌های نوینی مواجه شده‌اند. در ایران، ابهام در شناسایی ماهیت حقوقی دارایی‌های دیجیتال یکی از مسائل اصلی است؛ زیرا قوانین موجود بیشتر بر دارایی‌های فیزیکی یا مالی سنتی تمرکز دارند و دارایی‌های متاورسی در آن‌ها به‌طور صریح تعریف نشده‌اند. این امر باعث شده که مالکیت، توقیف و پیگیری کیفری دارایی‌های دیجیتال با دشواری مواجه شود و تفسیر موسع قوانین مدنی و کیفری برای پوشش این دارایی‌ها ضروری باشد. در مقابل، ژاپن با ترکیب قانون مدنی، قانون خدمات پرداخت [PSA] و قانون ابزارهای مالی و مبادلات [FIEA] تلاش کرده است چارچوب روشنی برای شناسایی دارایی‌های دیجیتال ایجاد کند؛ هرچند هنوز برخی ابهامات حقوقی درباره دسته‌بندی دقیق مال دیجیتال در متاورس باقی است، اما وجود مقررات تخصصی، امکان پیگیری کیفری و حمایت از مالک را نسبت به ایران آسان‌تر کرده است. مسئله دیگر در هر دو کشور، صلاحیت قضایی و تعیین مسئولیت کیفری در متاورس است. در ایران، به دلیل فقدان قوانین صریح درباره جرایم فراملی دیجیتال و مسئولیت پلتفرم‌ها، تعیین مرجع صالح و مسئولیت کاربران و ارائه‌دهندگان خدمات دشوار است و این خلأ می‌تواند به فرار مجرمان و ناکارآمدی نظام کیفری منجر شود. در ژاپن، اگرچه قوانین تخصصی صرافی‌ها و دارایی‌های رمزنگاری‌شده وجود دارد و دادگاه‌ها سابقه رسیدگی به جرایم سایبری و

توقیف دارایی‌های دیجیتال را دارند، اما همچنان مواردی که بازیگران و دارایی‌ها در قلمروهای مختلف جغرافیایی قرار دارند، چالش‌های صلاحیت و تعیین مسئولیت را به همراه دارد. بنابراین، در هر دو کشور، حمایت کیفری کامل از دارایی‌های دیجیتال در متاورس نیازمند بازتعریف ماهیت حقوقی دارایی‌ها، ایجاد چارچوب‌های مسئولیت مشخص و تدوین مقررات تطبیقی برای رسیدگی به جرایم فراملی است.

ابهام در شناسایی ماهیت حقوقی دارایی‌های دیجیتال (اموال فیزیکی یا طبقه‌بندی جدید حقوقی)

با گسترش ارزهای دیجیتال و دارایی‌های رمزنگاری‌شده، فرصت‌های جدیدی برای ارتکاب جرائم مالی مانند پول‌شویی، تأمین مالی تروریسم و سایر فعالیت‌های غیرقانونی ایجاد شده است. ویژگی‌های منحصربه‌فرد این دارایی‌ها، از جمله ناشناس بودن، غیرمتمرکز بودن و فراملیتی بودن، باعث شده که سیستم‌های حقوقی و نظارتی سنتی با چالش‌های جدی مواجه شوند. در این زمینه، اگرچه نظام‌های حقوقی داخلی به‌تنهایی قادر به پاسخگویی کامل نیستند و استفاده از چارچوب‌ها و اسناد بین‌المللی ضروری است (Ghavamipour Sarashkeh & Mahmoudi, 2024)، اما باید در خصوص قانون‌گذاری پویاتر باشند. چه اینکه قوانین موجود عمدتاً برای دارایی‌های فیزیکی یا مالی سنتی طراحی شده‌اند و هنوز تعریفی روشن از اموال دیجیتال یا مجازی ارائه نشده است. این ابهام باعث شده که شناسایی مالکیت، تعیین حقوق و تکالیف کیفری و نظارتی مرتبط با ارزهای دیجیتال با دشواری مواجه شود و زمینه بروز جرائم مالی مانند فرار مالیاتی، پول‌شویی و سایر تخلفات اقتصادی را فراهم آورد (Akhlaghdoost & Faghih Habibi, 2024). چالش‌های امنیتی و اقتصادی ناشی از این عدم شفافیت می‌تواند نقض حقوق شهروندی، از جمله مواد ۳۴، ۳۵، ۷۱ و ۱۱۸ منشور حقوق شهروندی را به دنبال داشته باشد و حفاظت قانونی از افراد در معاملات داخلی و بین‌المللی را با مشکل روبه‌رو سازد. برای رفع این ابهام، ضروری است قوانین و مقررات داخلی بازنگری و با ویژگی‌های منحصربه‌فرد دارایی‌های دیجیتال هماهنگ شوند. ایجاد طبقه‌بندی جدید حقوقی برای دارایی‌های دیجیتال، تعریف دقیق اموال مجازی و تعیین چارچوب مسئولیت کیفری، امکان پیشگیری و پیگیری تخلفات را فراهم می‌کند. نهادهایی مانند سازمان امور مالیاتی، شورای عالی مبارزه با پول‌شویی، شورای عالی فضای مجازی، پلیس فتا و قوه قضائیه با همکاری دانشگاه‌ها و مراکز پژوهشی می‌توانند سازوکارهای قانونی و نظارتی جامع طراحی کنند تا از سوءاستفاده کلاهبرداران جلوگیری شود و تهدیدهای اقتصادی تبدیل به فرصت‌هایی برای رونق اقتصادی و افزایش امنیت مالی کشور گردد. این در حالی است که اقدامات قابل توجهی انجام نشده است.

با این وجود، در ژاپن، قانون ممنوعیت دسترسی غیرمجاز به رایانه‌ها (UCAL) به‌طور صریح اقدامات هکری و دسترسی بدون اجازه به سیستم‌های رایانه‌ای را جرم‌انگاری کرده است (Katagiri, 2021). طبق این قانون، هرگونه دسترسی به یک رایانه تحت کنترل مدیر سیستم بدون اجازه، اعم از وارد کردن شناسه کاربری دیگران یا دور زدن کنترل‌های امنیتی، به‌عنوان «دسترسی غیرمجاز» تلقی می‌شود و مجازات آن حبس تا سه سال یا جریمه تا یک میلیون ین است. این چارچوب قانونی به‌وضوح نشان می‌دهد که ژاپن سعی دارد مالکیت و کنترل سیستم‌های رایانه‌ای را به رسمیت بشناسد و فعالیت‌های هکری را تحت پیگرد کیفری قرار دهد (Mosechkin, 2024). برای مثال، هک یک صرافی رمزارز یا ورود غیرمجاز به شبکه بانکی بدون اجازه، مشمول این قانون خواهد بود و دادگاه‌ها مجاز به صدور حکم کیفری علیه مرتکبان هستند. علاوه بر دسترسی غیرمجاز، جرائم سایبری دیگری مانند حملات انکار سرویس (DoS) و فیشینگ نیز تحت قوانین کیفری ژاپن جرم‌انگاری شده‌اند. ماده ۲۳۴-۲ قانون جزا، ایجاد اختلال در عملکرد رایانه‌های مورد استفاده در کسب‌وکار دیگران از طریق دستورات نادرست یا وارد کردن اطلاعات جعلی را جرم می‌داند و مجازات آن حبس تا پنج سال یا جریمه تا یک میلیون ین است. همچنین، فیشینگ به‌عنوان جعل هویت مدیر سیستم و درخواست غیرمجاز اطلاعات کاربری، طبق مواد ۴ و ۷ UCAL قابل تعقیب کیفری است و حداکثر

مجازات حبس یک سال یا جریمه ۵۰۰ هزار ین برای آن تعیین شده است. این مقررات نشان می‌دهد که ژاپن به‌صراحت مسئولیت کیفری کاربران، مجرمان سایبری و حتی سازمان‌های ارائه‌دهنده خدمات آنلاین را برای حفظ امنیت اطلاعات و جلوگیری از سوءاستفاده‌ها مشخص کرده است.

در زمینه بدافزارها و برنامه‌های مخرب رایانه‌ای، قانون جزا ژاپن «رکوردهای دستوری نامناسب» را جرم‌انگاری کرده است که شامل ویروس‌ها، باج‌افزارها، تروجان‌ها و سایر بدافزارها می‌شود. ایجاد، ارائه یا انتشار این رکوردها بدون توجیه قانونی مجازات تا سه سال حبس یا جریمه تا ۵۰۰ هزار ین دارد. یک مثال مهم قضایی در این زمینه، پرونده استخراج رمزارز از طریق برنامه جاسازی‌شده در وب‌سایت در سال ۲۰۲۲ است. دادگاه عالی ژاپن متهم را تبرئه کرد، زیرا هرچند برنامه بدون اطلاع کاربران اجرا شده و منابع رایانه آن‌ها را مصرف کرده بود، ولی از نظر دادگاه اجتماعی غیرمجاز تلقی نشد و مشابه نمایش تبلیغات پاپ‌آپ بدون رضایت کاربران بود (Collins, 2022). این پرونده نشان می‌دهد که تفسیر قانونی در ژاپن علاوه بر اعمال قانون، نیازمند ارزیابی جنبه اجتماعی و مشروعیت رفتار سایبری نیز هست. بر این اساس، قوانین UCAL و قانون جزا، دسترسی غیرمجاز به این دارایی‌ها، دستکاری در کیف‌پول‌ها، استخراج غیرمجاز رمزارز و انتشار بدافزار در محیط‌های متاورسی را مشمول تعقیب کیفری قرار می‌دهند. با این حال، همانند پرونده استخراج رمزارز در وب‌سایت، قضات ژاپنی همواره نیاز به بررسی مشروعیت اجتماعی و تأثیر رفتار کاربران بر دیگران دارند که نشان می‌دهد در زمینه دارایی‌های دیجیتال و متاورس، تعادل میان نوآوری فناوری و حفاظت قانونی از کاربران و دارایی‌ها همچنان یک چالش حقوقی مهم است.

با این وجود، علی‌رغم پیشرفت ژاپن در قانون‌گذاری، می‌توان گفت که در زمینه دارایی‌های دیجیتال و متاورس، ایران و ژاپن هر دو با چالش‌های مشابهی مواجه‌اند؛ هرچند رویکردها و چارچوب‌های قانونی متفاوت است. در ژاپن، قوانین UCAL و قانون جزا دسترسی غیرمجاز به دارایی‌های دیجیتال، انتشار بدافزار، استخراج غیرمجاز رمزارز و دستکاری آیتم‌های مجازی در متاورس را جرم‌انگاری کرده و هم‌زمان بر تحلیل مشروعیت اجتماعی و اثر اقدامات بر دیگر کاربران تأکید دارد، همان‌طور که پرونده استخراج رمزارز بدون اطلاع کاربران نشان داد. در ایران نیز با رشد ارزهای دیجیتال و متاورس، فقدان تعریف دقیق از ماهیت حقوقی این دارایی‌ها، ابهامات مالکیت و مسئولیت کیفری را تشدید کرده است و جرائم مالی مانند پول‌شویی، فرار مالیاتی و سوءاستفاده از دارایی‌های مجازی نیازمند بازنگری قوانین، ایجاد طبقه‌بندی جدید حقوقی و تقویت نهادهای نظارتی همچون شورای عالی فضای مجازی، پلیس فتا و قوه قضائیه است. ترکیب این چارچوب‌ها در هر دو کشور نشان می‌دهد که حفاظت کیفری از دارایی‌های دیجیتال و محیط‌های متاورسی نیازمند تعادل میان نوآوری فناوری، امنیت اقتصادی و حقوق شهروندان است، به‌گونه‌ای که هم توسعه بازارهای دیجیتال تسهیل شود و هم ریسک سوءاستفاده و جرائم سایبری به حداقل برسد.

مسائل صلاحیت قضایی و تعیین مسئولیت کیفری در متاورس (کاربران، ارائه‌دهندگان خدمات و دولت‌ها)

جرایم سایبری به دلیل ماهیت فراملی و تکنولوژیک خود، نیازمند چارچوب‌های قانونی بین‌المللی هستند. تاکنون هیچ معاهده جهانی کامل و یکتایی برای تعریف و رسیدگی به جرایم سایبری وجود ندارد و به همین دلیل جامعه بین‌المللی به تدابیر منطقه‌ای و چندجانبه مانند کنوانسیون بوداپست ۲۰۰۱ متوسل شده است. این کنوانسیون، با مشارکت کشورهای اروپایی، ایالات متحده، ژاپن، کانادا و آفریقای جنوبی، نقطه عطفی در ایجاد هماهنگی حقوقی و ارائه الگوی همکاری بین‌المللی برای مقابله با جرایم سایبری به شمار می‌رود (Bucaj & Idrizaj, 2025). این چارچوب‌ها امکان پیشگیری، تعقیب و مجازات مجرمان سایبری را در سطح فراملی فراهم می‌کنند و با توجه به پیچیدگی و سرعت تحول تهدیدات دیجیتال، ضرورت به‌روزرسانی و گسترش آن‌ها آشکار است.

در ژاپن، قوانین متعددی مسئولیت کیفری و حقوقی در فضای سایبری و حفاظت از دارایی‌های دیجیتال را تنظیم می‌کنند و در عین حال تلاش دارند بین نوآوری فناوری و امنیت کاربران تعادل برقرار کنند. سرقت الکترونیکی، از جمله دسترسی غیرمجاز به اسرار تجاری توسط کارکنان فعلی یا سابق، تحت قانون پیشگیری از رقابت ناعادلانه جرم‌انگاری شده است؛ به‌طور مثال، اگر کارمندی بدون اجازه به اطلاعات محرمانه شرکت دسترسی پیدا کند یا از آن برای کسب منفعت نادرست استفاده کند، ممکن است به حبس تا ۱۰ سال یا جریمه تا ۲۰ میلیون ین محکوم شود (ماده ۲۱). همچنین، قوانین حق مؤلف، هرگونه بارگذاری یا دانلود غیرمجاز محتوای دیجیتال دارای کپی‌رایت را مجازات می‌کند و فروش یا تولید ابزارهای دور زدن حفاظت کپی‌رایت نیز جرم است (مواد ۱۱۹ و ۱۲۰-۲) (Imamura, 2025).

فعالیت‌هایی مانند تست نفوذ بدون اجازه نیز به‌عنوان دسترسی غیرمجاز تلقی شده و مجازات کیفری دارد، مگر اینکه توسط نهاد ملی فناوری اطلاعات و ارتباطات ژاپن (NICT) انجام شود (Bendiek & Schulze, 2021). علاوه بر آن، هرگونه اقدام که امنیت، محرمانگی، یکپارچگی یا دسترسی به سیستم‌ها و داده‌ها را تهدید کند، مانند ارائه کد شناسایی کاربران به افراد ثالث، مجازات حبس یا جریمه دارد (مواد ۵ و ۱۲ UCAL). این قوانین قابلیت اعمال فراملی نیز دارند، به‌طوری که اقدامات انجام‌شده خارج از ژاپن می‌تواند تحت تعقیب قانونی قرار گیرد (ماده ۱۴ UCAL) (Arnell & Kawai, 2023).

در سطح حفاظت سایبری و دارایی‌های دیجیتال در متاورس، چارچوب‌های قانونی شامل قانون اساسی سایبری (BAC)، قانون کسب‌وکار مخابراتی (TBA) و قانون حفاظت از اطلاعات شخصی (APPI) است. این قوانین مسئولیت دولت، اپراتورها و کسب‌وکارها را برای پیشگیری، شناسایی و مدیریت حملات سایبری تعیین می‌کنند و همکاری بین بخش دولتی و خصوصی را تقویت می‌کنند. برای مثال، پروژه ACTIVE و دستورالعمل‌های MIC اجازه می‌دهند که ISPها با اطلاع‌رسانی به کاربران یا مسدودسازی ارتباطات، تهدیدهای سایبری را کاهش دهند، بدون اینکه قوانین محرمانگی ارتباطات را نقض کنند (Shin, 2022). در نتیجه، ژاپن با این چارچوب‌ها تلاش می‌کند امنیت دارایی‌های دیجیتال و تعاملات در متاورس را تضمین کند، هم‌زمان که نوآوری و توسعه فناوری دیجیتال محدود نشود.

در ایران، قوانین مرتبط با دارایی‌های دیجیتال و متاورس در حال تحول هستند. در سال ۲۰۱۸، بانک مرکزی ایران با استناد به نگرانی‌های مربوط به پول‌شویی و تأمین مالی تروریسم، فعالیت‌های مرتبط با رمزارزها را ممنوع اعلام کرد (Aghaei Toogh & Naser, 2021). اما در سال ۲۰۱۹، با تشدید تحریم‌ها و کاهش ارزش ریال، دولت به‌تدریج این ممنوعیت را کاهش داد و رمزارزها را به‌عنوان ابزاری برای مقابله با تحریم‌ها و تقویت اقتصاد دیجیتال پذیرفت. در ژانویه ۲۰۲۵، بانک مرکزی ایران چارچوب سیاستی و نظارتی جدیدی را برای رمزارزها تصویب کرد که شامل صدور مجوز برای صرافی‌ها و نظارت بر تطابق با قوانین ضدپول‌شویی و مالیات می‌شود (Khajevand, 2024). در این چارچوب، صرافی‌ها موظف به ارائه اطلاعات کاربران به بانک مرکزی هستند. همچنین، در سال ۲۰۲۴، بانک مرکزی ایران برنامه‌ای را برای مسدودسازی تراکنش‌های رمزارز به ریال و بالعکس از طریق وب‌سایت‌ها در ایران اجرا کرد. در ژانویه ۲۰۲۵، بانک مرکزی شروع به باز کردن مجدد درگاه‌های پرداخت رمزارز برای صرافی‌ها با استفاده از API دولتی کرد.

در زمینه متاورس، در ایران هنوز چارچوب‌های قانونی مشخصی وجود ندارد. با این حال، پژوهش‌ها نشان می‌دهند که در فقه امامیه، اکثر فقها معاملات مبتنی بر توکن‌ها و رمزارزها را باطل یا غیرمجاز می‌دانند. با این وجود، برخی از حقوق‌دانان معتقدند که با توجه به تحولات اقتصادی و سیاسی، مفهوم مالکیت در تجارت معاصر دیگر محدود به اشیاء فیزیکی نیست و دارایی‌های دیجیتال در متاورس می‌توانند از منظر حقوقی

معتبر باشند. این دیدگاه بر این اساس استوار است که انتقال دارایی در متاورس، مشابه تحویل فیزیکی، منجر به خروج آن از مالکیت فروشنده و ورود به دارایی خریدار می‌شود.

در زمینه صلاحیت قضایی و مسئولیت کیفری در متاورس، با توجه به ماهیت جهانی و بی‌مرز این فضا، چالش‌هایی در تعیین صلاحیت قضایی و مسئولیت کیفری وجود دارد. در پرونده‌های واقعی، مانند حمله سایبری به صرافی Nobitex در ایران در سال ۲۰۲۵ که منجر به سرقت ۹۰ میلیون دلار شد، مسائل مربوط به مسئولیت کیفری و صلاحیت قضایی پیچیده‌تر می‌شود (Mosechkin, 2024). در این حمله، گروهی با انگیزه‌های سیاسی به صرافی حمله کردند و وجوه سرقت‌شده را به آدرس‌هایی مرتبط با سپاه پاسداران منتقل کردند. این حادثه نشان‌دهنده چالش‌های موجود در پیگیری و محاکمه جرایم در فضای متاورس است. بر این مبنا، در نهایت، ایران در حال توسعه چارچوب‌های قانونی برای دارایی‌های دیجیتال و متاورس است، اما هنوز با چالش‌هایی در زمینه تطابق با فقه امامیه و مسائل بین‌المللی مواجه است. توسعه قوانین و مقررات شفاف و هماهنگ با استانداردهای بین‌المللی می‌تواند به ایجاد فضایی امن و قانونی برای فعالیت‌های دیجیتال در ایران کمک کند.

براساس آنچه آوردیم، به نظر می‌رسد که می‌توان گفت یکی از تفاوت‌های اساسی میان حقوق کیفری ایران و ژاپن در زمینه حمایت از دارایی‌های دیجیتال، در برداشت از مفهوم «مال» نهفته است. همچنین، در حقوق ایران، «مال» همچنان بر پایه معیارهای سنتی چون قابلیت لمس، ارزش اقتصادی محسوس و قابلیت دادوستد مادی تعریف می‌شود و این برداشت موجب شده دارایی‌های دیجیتال در متاورس غالباً تحت حمایت کیفری قرار نگیرند، مگر آنکه بتوان آن‌ها را ذیل عناوین سنتی چون «داده» یا «اسناد الکترونیکی» جای داد. در مقابل، حقوق ژاپن با رویکردی پویا و متناسب با تحولات فناوری، دارایی‌های رمزنگاری‌شده و سایر اشکال اموال دیجیتال را به‌عنوان «مال» تلقی کرده و با وضع قوانین ویژه، زمینه حمایت کیفری از آن‌ها را فراهم ساخته است. این تفاوت در نگرش باعث شده در ژاپن امکان تعقیب کیفری جرایم متاورسی همچون سرقت، کلاهبرداری و پول‌شویی فراهم باشد، حال آنکه در ایران فقدان چنین رویکردی موجب خلأ قانونی و آسیب‌پذیری کاربران شده است. بنابراین، می‌توان گفت که اصلاح و توسعه مفهوم «مال» در حقوق کیفری ایران و هماهنگ‌سازی آن با واقعیت‌های فناوری‌های نوین، شرط ضروری برای حمایت مؤثر از دارایی‌های دیجیتال در متاورس است.

نتیجه‌گیری

پژوهش حاضر با هدف بررسی تطبیقی تحول مفهوم «مال» در حقوق کیفری ایران و ژاپن و تأثیر آن بر حمایت از دارایی‌های دیجیتال در متاورس، نشان داد که بسترهای نوین فناوری، چالش‌های بی‌سابقه‌ای را برای نظام‌های حقوقی ایجاد کرده‌اند. متاورس به‌عنوان محیطی فرامرزی و مجازی، پرسش‌های مهمی را در خصوص مالکیت و حمایت کیفری از دارایی‌های دیجیتال مطرح کرده است. در این میان، مهم‌ترین چالش، تعیین ماهیت حقوقی دارایی‌های دیجیتال و میزان انطباق آن‌ها با مفهوم «مال» در حقوق کیفری است.

یافته‌های تحقیق بیانگر آن است که نظام حقوقی ایران، به‌واسطه تفسیر سنتی از «مال» و اتکای صرف به قانون جرایم رایانه‌ای ۲۰۰۹، نتوانسته است از دارایی‌های دیجیتال به نحو مؤثر حمایت کند. این محدودیت سبب شده بسیاری از بزه‌دیدگان متاورس در برابر جرایمی چون کلاهبرداری و سرقت، از ابزارهای کافی برای احقاق حق برخوردار نباشند. در مقابل، ژاپن با پذیرش گسترده‌تر دارایی‌های دیجیتال در قالب «مال» و تصویب مقررات خاص درباره دارایی‌های رمزنگاری‌شده و جرایم سایبری، توانسته است حمایت کیفری کارآمدتری ارائه دهد. این امر نشان می‌دهد که رویکرد ژاپن، به دلیل پویایی و انعطاف در پذیرش واقعیت‌های نوین، الگوی مناسبی برای اصلاح قوانین ایران به شمار می‌آید.

از سوی دیگر، بررسی موضوع نشان داد که مسئله صلاحیت قضایی و تعیین مسئولیت کیفری در متاورس نیز یکی از موانع جدی در مسیر حمایت از دارایی‌های دیجیتال است. متاورس به دلیل فقدان مرزهای جغرافیایی روشن، پیچیدگی‌های زیادی در تعیین محل وقوع جرم و شناسایی مرتکبان ایجاد می‌کند. تجربه ژاپن در تدوین مقررات هماهنگ با تعهدات بین‌المللی و مشارکت در اسناد چندجانبه، نمونه‌ای موفق از تلاش برای غلبه بر این مشکل است؛ در حالی که ایران در این حوزه همچنان با خلأهای قابل توجهی روبه‌روست.

بنابراین، نتیجه کلی این تحقیق آن است که ایران برای حمایت کیفری مؤثر از دارایی‌های دیجیتال در متاورس، نیازمند بازتعریف مفهوم «مال» در قوانین کیفری و تدوین مقررات جامع و به‌روز در حوزه جرایم سایبری است. این اصلاح باید با الهام از تجربیات موفق کشورهایی چون ژاپن و اتحادیه اروپا، اما متناسب با نیازها و شرایط بومی کشور صورت گیرد. بدین ترتیب، می‌توان از یک سو امنیت حقوقی و اقتصادی کاربران ایرانی در فضای متاورس را تضمین کرد و از سوی دیگر، با کاهش خلأهای قانونی، زمینه سوءاستفاده مجرمان سایبری را محدود ساخت. بر این مبنا، این پژوهش روشن می‌سازد که تحول مفهوم «مال» نه‌تنها یک ضرورت نظری برای هماهنگی حقوق با فناوری‌های نوین است، بلکه یک الزام عملی برای تضمین عدالت کیفری و حمایت از حقوق کاربران در دنیای دیجیتال به شمار می‌رود.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

The rapid development of digital technologies has transformed conventional legal understandings of property, ownership, economic value, and criminal protection, particularly in relation to digital assets and emerging virtual environments such as the metaverse. The metaverse has created a technologically mediated space in which users acquire, transfer, exchange, and exploit digital objects possessing measurable economic value, including cryptocurrencies, non-fungible tokens, virtual land, digital collectibles, platform-based entitlements, and other tokenized assets. These developments have exposed the limitations of traditional legal concepts that were originally constructed around tangible and physically transferable objects. In classical legal doctrine, property was generally associated with materiality, economic utility, exclusivity, transferability, and the possibility of possession, whereas contemporary digital assets may satisfy most economic and functional characteristics of property without possessing a physical form. Modern legal scholarship has therefore increasingly emphasized the need to distinguish physical embodiment from economic and proprietary value and to recognize that digitally represented interests may constitute legally protectable property where they are transferable, identifiable, exclusive, and economically valuable (Ayoubi, 2024; Fairfield, 2022). This conceptual transformation is particularly significant in criminal law because offenses such as theft, fraud, embezzlement, unlawful appropriation, forgery, money laundering, and unauthorized access traditionally presuppose either the existence of property or interference with a legally recognized proprietary interest. If digital assets remain outside the legal category of property, victims of offenses involving virtual assets may encounter difficulties in obtaining effective criminal protection. Consequently, the central question addressed in this study is

how the concept of "property" has evolved in Iranian and Japanese criminal law and how differences between these two legal systems affect the criminal-law protection of digital assets in the metaverse. The study adopts a descriptive-analytical and comparative approach, drawing upon legal doctrine, statutory frameworks, cybercrime legislation, regulatory instruments governing cryptocurrencies and digital assets, and relevant scholarly analyses of digital property and cybercriminality. The comparison between Iran and Japan is particularly instructive because both systems have been exposed to the challenges of digitalization, yet they have responded differently to the legal classification, regulation, and criminal protection of emerging digital assets.

In Iranian law, the concept of property has historically been influenced by civil-law doctrine and Islamic jurisprudential understandings of economic value, rational benefit, lawful appropriation, and transferability. Although the Iranian Civil Code does not provide a comprehensive statutory definition of property, Iranian legal doctrine has traditionally understood property in a broad sense as encompassing material objects and certain economically valuable rights. Katouzian's conception of financial rights as legally recognized privileges serving material interests illustrates that Iranian private law is not theoretically confined to tangible objects (Katouzian, 2006). Nevertheless, the criminal-law treatment of property has historically remained more closely connected to conventional categories of tangible assets and traditional forms of financial value. This creates considerable difficulty when criminal offenses concern cryptocurrencies, virtual assets, tokenized rights, or property existing solely within digital platforms. Iran's Computer Crimes Law of 2009 criminalizes conduct such as unauthorized access, illegal interception, computer-related forgery, data interference, and computer fraud, but its primary focus is the protection of information systems, data integrity, confidentiality, and the security of electronic communications rather than the explicit recognition of digital assets as "property." As a result, courts and legal scholars may need to rely upon expansive interpretations of existing concepts such as property, funds, financial rights, data, or electronic documents in order to provide legal protection for digitally represented value. Similar interpretive problems arise in the enforcement of judgments involving cryptocurrencies. Iranian scholarship has argued that cryptocurrencies may potentially fall within the scope of attachable property because they possess economic value and are transferable, even though the existing enforcement framework was originally designed for conventional assets (Gholami et al., 2023). However, practical enforcement remains difficult when cryptocurrencies are held in decentralized wallets, anonymous addresses, or foreign exchanges. Questions regarding proof of ownership, identification of digital wallets, asset control, and judicial access to exchange records further complicate attachment and confiscation procedures (Banaei Oskouei & Jalali, 2022). Iranian scholarship has also emphasized that regulatory uncertainty regarding virtual currencies may affect economic security and citizens' rights, particularly where unclear legal classifications limit the effectiveness of judicial protection, regulatory supervision, taxation, and anti-money-laundering mechanisms (Aghaei Toogh & Naser, 2021; Akhlaghdoost & Faghih Habibi, 2024). These problems demonstrate that, despite the functional economic characteristics of digital assets, Iranian law still lacks a fully articulated and unified legal doctrine recognizing such assets as property for all purposes of criminal protection.

The Japanese legal framework presents a comparatively more adaptive response to the emergence of digital assets, although Japanese law also preserves distinctions between traditional property law and newer regulatory categories. Japan has developed an increasingly specialized legal framework for cryptocurrencies, cybercrime, electronic transactions, and digitally mediated financial activities. The Payment Services Act and the Financial Instruments and Exchange Act provide important

regulatory structures governing crypto-assets, financial intermediaries, exchange services, and certain forms of tokenized financial activity. These developments demonstrate a legislative willingness to regulate economically valuable digital assets on the basis of their actual function within markets rather than solely through traditional doctrines of corporeal property. Scholarly analyses of digital financial assets similarly indicate that contemporary criminal-law classification increasingly depends on the economic function, transferability, technological structure, and legally protected interest represented by an asset rather than on physical possession alone (Lyaskalo, 2023). The Japanese approach is also supported by a more developed cybercrime framework addressing unauthorized access, interference with computer systems, malware, phishing, and related conduct. The Act on Prohibition of Unauthorized Computer Access criminalizes access to protected systems without authorization, while the Japanese Penal Code contains provisions addressing interference with computers used in business and the creation or dissemination of malicious computer instructions. These rules provide indirect but important protection for digital assets by criminalizing technological methods used to obtain, manipulate, or disrupt them (Katagiri, 2021; Mosechkin, 2024). Japan's legal treatment of digitally mediated conduct also reflects a broader institutional approach to cybersecurity, combining criminal law, administrative regulation, private-sector compliance, and technological security standards. Research on Japanese cyber-security measures has shown that public authorities, telecommunications operators, and service providers play complementary roles in protecting networks and preventing cyberattacks (Shin, 2022). Moreover, Japanese law demonstrates a broader capacity to adapt existing legal categories to technologically complex circumstances, including transnational conduct and digital copyright infringements (Harata, 2025; Imamura, 2025). Although digital assets may not always be conceptually identical to conventional tangible property, the combined effect of specialized regulation, cybercrime legislation, financial regulation, and judicial interpretation creates a stronger legal environment for protecting virtual economic interests than is presently available under Iranian law.

The comparative analysis becomes particularly important in the context of the metaverse because digital property in immersive and decentralized environments generates forms of criminal conduct that challenge conventional concepts of possession, territorial jurisdiction, identity, and proprietary control. Digital assets in virtual environments may be stored on centralized servers, blockchains, digital wallets, or hybrid technological infrastructures, and the user who economically controls an asset may be located in a different jurisdiction from the platform, service provider, blockchain validator, or alleged offender. The recognition of such assets as legally protected property is therefore closely connected with broader questions concerning cybercrime jurisdiction, criminal attribution, platform responsibility, and international cooperation. Cryptocurrency and tokenized assets have already become relevant to organized crime, illicit transfers, fraud, money laundering, and other forms of digital criminality, which demonstrates that legal systems cannot effectively combat these offenses without defining the protected economic interest with sufficient clarity (Collins, 2022). International legal scholarship has consequently emphasized the need for more coherent frameworks for cybercrime cooperation and harmonization, particularly because national criminal laws remain fragmented and digital offenses often cross territorial boundaries (Buçaj & Idrizaj, 2025). International regulatory initiatives concerning cryptocurrency crime likewise stress the importance of coordination among states, financial institutions, exchanges, law-enforcement bodies, and supervisory authorities (Ghavamipour Sarashkeh & Mahmoudi, 2024; Kavaloski, 2024). The metaverse intensifies these challenges because criminal conduct may involve virtual environments that are neither territorially fixed nor subject to a single legal authority. A stolen or fraudulently transferred

digital asset may move between wallets and exchanges located in multiple jurisdictions within minutes, while offenders may conceal their identities through pseudonymous accounts, privacy-enhancing tools, decentralized networks, or intermediary platforms. Japan's greater integration into international cybercrime and digital regulation frameworks gives it stronger institutional capacity to address some of these problems, although jurisdictional and attribution difficulties remain. Comparative studies of international and Japanese criminal law demonstrate that questions of extraterritorial jurisdiction, attribution, and cross-border enforcement remain central even in more technologically developed legal systems (Arnell & Kawai, 2023; Harata, 2025). Iran faces similar challenges but with a less developed statutory framework specifically addressing digital assets and metaverse-related criminality, thereby increasing reliance on traditional rules whose application to decentralized virtual environments may be uncertain.

Another major finding concerns the distinction between criminalizing interference with computer systems and recognizing the economic object of that interference as legally protected property. This distinction is essential because a legal system may criminalize unauthorized access to a computer or digital wallet without necessarily providing a coherent proprietary framework for the digital asset obtained through such access. In Iran, cybercrime provisions may punish unauthorized access, fraud, data manipulation, or related conduct, but uncertainty remains regarding whether cryptocurrencies, NFTs, virtual items, or other metaverse assets independently constitute property capable of being stolen, confiscated, attached, or restored to victims. This uncertainty may limit both substantive criminal liability and post-conviction remedies. Iranian scholarship on the legal legitimacy of digital assets in the metaverse has therefore emphasized the importance of recognizing their juridical value and of adapting traditional property concepts to contemporary digital transactions (Khajevand, 2024). Similar research concerning the transformation of property in the digital environment suggests that the defining characteristics of property should increasingly be understood in functional rather than purely physical terms (Ayoubi, 2024). By contrast, the Japanese regulatory environment is more conducive to treating digital assets as legally significant economic interests because financial regulation, cybercrime legislation, and platform obligations operate together. Japan's experience also illustrates that criminal-law responses to cyber conduct cannot rely solely on formal technological definitions but may require judicial assessment of the social legitimacy, harmfulness, and context of digital behavior. This approach is particularly relevant to emerging practices such as unauthorized cryptomining, malicious scripts, phishing, digital credential theft, and virtual asset manipulation (Collins, 2022; Mosechkin, 2024). At the same time, comparative analysis indicates that both legal systems must address the responsibilities of intermediaries, exchanges, platform operators, users, and state authorities. Effective protection requires not only substantive criminal prohibitions but also rules concerning evidence preservation, asset tracing, confiscation, restitution, compliance obligations, cross-border cooperation, and institutional cybersecurity. International analyses of cyber attribution and sanctions further demonstrate that identifying the responsible actor behind technologically sophisticated attacks remains difficult even where specialized cyber frameworks exist (Bendiek & Schulze, 2021). Therefore, the transformation of the concept of property should be understood as one component of a broader restructuring of criminal-law protection in digital environments.

In conclusion, the comparative findings demonstrate that the evolution of the concept of property has direct consequences for the effectiveness of criminal protection in digital environments. Iranian law retains sufficient doctrinal flexibility to recognize economically valuable non-physical interests, but its criminal-law framework has not yet developed a clear and comprehensive classification of

digital assets as protected property. This creates uncertainty in cases involving theft, fraud, unlawful transfer, confiscation, restitution, and other offenses relating to cryptocurrencies, tokenized assets, and virtual property in the metaverse. Japan has responded more systematically by combining specialized regulation of crypto-assets, cybercrime legislation, financial-market rules, cybersecurity obligations, and broader interpretations of legally protected digital interests. The principal lesson for Iranian criminal law is therefore not the mechanical transplantation of Japanese legislation but the need to modernize the legal concept of property in a manner consistent with the functional characteristics of digital assets. A reformed framework should expressly recognize economically valuable, identifiable, transferable, and controllable digital assets as potential objects of criminal-law protection, while distinguishing among different technological and legal categories where necessary. It should also clarify the conditions governing seizure, confiscation, restitution, evidentiary proof, jurisdiction, and the liability of users and service providers. Such reform would reduce interpretive inconsistency, improve legal certainty, strengthen the position of victims, and provide courts with clearer tools for addressing offenses committed in increasingly complex virtual environments. More broadly, the comparison indicates that the criminal-law concept of property must remain responsive to technological transformation if legal systems are to preserve the substantive values traditionally protected by property offenses, including economic security, individual autonomy, lawful possession, transactional trust, and protection against unlawful appropriation. The evolution of property from a predominantly material concept toward a technologically neutral and functionally defined legal interest is therefore not merely a theoretical development, but an essential condition for maintaining effective criminal justice in the digital age.

References

Aghaei Toogh, M., & Naser, M. (2021). Virtual currency policymaking: The tension between societal security and the fundamental rights of the people. *Administrative Law*, *8*(26), 9-28.

Akhlaghdoost, A., & Faghih Habibi, A. (2024). Effects of virtual currencies on economic security and citizens' rights in Iran. *Legal Research*, *23*(60), 37-70.

Arnell, P., & Kawai, T. (2023). International Crimes in United Kingdom and Japanese Law and Practice. *Nihon University Comparative Law*, *39*, 89-103.

Ayoubi, S. (2024). *The transformation of attitudes toward property in the digital environment* University of Mazandaran].

Banaei Oskouei, M., & Jalali, S. H. (2022). Requirements for issuing an enforcement writ for a dishonored check through the court. *Legal Research*, *21*(52), 479-516.

Bendiek, A., & Schulze, M. (2021). *Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, Bundestag Hack and the attack on the OPCW* (SWP Research Paper, Issue.

Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024.

Collins, J. (2022). *Crypto, crime and control. Cryptocurrencies as an enabler of organized crime*.

Fairfield, J. A. (2022). Tokenized: The law of non-fungible tokens and unique digital property. *Ind. LJ*, *97*, 1261.

Ghavamipour Sarashkeh, M., & Mahmoudi, A. (2024). Legal frameworks and international efforts to combat cryptocurrency crimes: An approach based on international instruments. *Research and Development in Criminal Law and Criminology*, *1*(1), 288-314.

Gholami, Y., Javadi, M., & Moghaddasi, M. (2023). Enforcement of civil judgments against cryptocurrencies. *Judiciary Law Journal*, *87*(121), 283-306.

Harata, H. (2025). The Extraterritorial Application of Statutes and Regulations: Japan. In *Extraterritoriality in Comparative Perspective* (pp. 229-263). Brill Nijhoff.

Imamura, T. (2025). Copyright and Streaming in Japan. In *Copyright Law and Streaming* (pp. 585-598). Brill Nijhoff.

Katagiri, N. (2021). From cyber denial to cyber punishment: What keeps Japanese warriors from active defense operations? *Asian Security*, *17*(3), 331-348.

Katouzian, N. (2006). *Introductory course in civil law: Property and ownership* (13 ed.). Mizan.

Kavaloski, M. (2024). A Global Crypto Code of Conduct: Crafting an Internationally Centralized Regulatory Body for a Decentralized Asset. *Vand. J. Transnat'l L.*, *57*, 301.

Khajevand, M. (2024). The Juridical and Legal Legitimacy of Digital Assets in the Metaverse. *Legal Studies in Digital Age*, *3*(4), 115-123.

Lyaskalo, A. N. (2023). Financial Assets in Digital Form and How They Influence Classification of Crime. *Legal Issues in the Digital Age*(4), 48-67.

Mosechkin, I. (2024). Unauthorized access to computer information: The empirical study of characteristics of victims and their victimization. *Russian Law Journal*, *12*(2), 1098-1109.

Shin, S. (2022, 2022/12). *A Study on 5G Security Activities in Japan* International Symposium on Mobile Internet Security, Singapore.