

ابعاد جرم‌شناختی بزه‌دیدگی دیجیتال در متاورس و راهبردهای پیشگیری از آن

احمد پورابراهیم

گروه حقوق، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران.

apourebrahim@iaui.ac.ir

چکیده:

گسترش زیست‌بوم‌های متاورسی و هم‌گرایی آن با سامانه‌های هوش مصنوعی، واقعیت مجازی و اقتصاد داده‌محور، موجب تحول بنیادین در الگوهای بزه‌دیدگی شده است؛ به‌گونه‌ای که در بسیاری از موارد، بزه‌دیدگی نه نتیجه کنش مستقیم انسانی، بلکه محصول تعامل پیچیده میان کاربر، الگوریتم‌ها و معماری پلتفرمی است. در این چارچوب، مسئله اصلی پژوهش آن است که چگونه می‌توان در محیطی با کنشگران انسانی و غیرانسانی هم‌زمان، مفهوم بزه‌دیدگی را صورت‌بندی و مسئولیت را به‌نحو حقوقی قابل انتساب کرد. این مطالعه با هدف تبیین ماهیت نوین بزه‌دیدگی در متاورس، بررسی نقش سوگیری الگوریتمی در تولید آسیب، تحلیل خلأهای تقنینی و ارزیابی چالش‌های ادله دیجیتال انجام شده است. روش تحقیق توصیفی-تحلیلی و مبتنی بر مطالعات اسنادی و تحلیل تطبیقی منابع داخلی و خارجی در حوزه جرم‌شناسی دیجیتال است. یافته‌ها نشان می‌دهد که بزه‌دیدگی در محیط‌های متاورسی ماهیتی ساختاری، داده‌محور و چندلایه دارد و در آن مسئولیت به‌صورت پراکنده میان پلتفرم، کاربر و نظام الگوریتمی توزیع می‌شود. همچنین مشخص شد که ناکارآمدی نظام‌های ادله سنتی در مواجهه با داده‌های سیال و غوطه‌ور، همراه با خلأهای تقنینی و فقدان استانداردهای ایمنی در طراحی، از عوامل اصلی تشدید بزه‌دیدگی محسوب می‌شوند. در نتیجه، مواجهه مؤثر با این پدیده مستلزم گذار از رویکردهای صرفاً واکنشی به سمت سیاست جنایی پیشگیرانه مبتنی بر امنیت در طراحی و نظارت هوشمند است.

کلیدواژه‌ها:

بزه‌دیدگی دیجیتال، متاورس، سوگیری الگوریتمی، جرم‌شناسی نوین، ادله الکترونیکی، سیاست جنایی پیشگیرانه

Criminological Dimensions of Digital Victimization in the Metaverse and Strategies for Its Prevention

Abstract

The expansion of metaverse ecosystems and their convergence with artificial intelligence, virtual reality, and data-driven economies have fundamentally transformed patterns of victimization. In many instances, victimization is no longer the direct result of human conduct but rather emerges from the complex interaction among users, algorithms, and platform architectures. Within this context, the central research question is how the concept of victimization can be reconceptualized in an environment where both human and non-human actors simultaneously participate, and how legal responsibility can be attributed in such a setting. This study aims to explain the emerging nature of victimization in the metaverse, examine the role of algorithmic bias in generating harm, analyze existing legislative gaps, and evaluate the challenges associated with digital evidence. The research adopts a descriptive-analytical methodology based on documentary research and a comparative analysis of domestic and international literature in the field of digital criminology. The findings indicate that victimization within metaverse environments is structural, data-driven, and multilayered, with responsibility dispersed among platform providers, users, and algorithmic systems. The study further demonstrates that the inadequacy of traditional evidentiary frameworks in addressing fluid and immersive digital data, together with legislative deficiencies and the absence of safety-by-design standards, significantly contributes to the escalation of digital victimization. Consequently, an effective response to this phenomenon requires a transition from purely reactive approaches toward a preventive criminal policy grounded in security-by-design principles and intelligent regulatory oversight.

Keywords: Digital Victimization; Metaverse; Algorithmic Bias; Digital Criminology; Electronic Evidence; Preventive Criminal Policy.

گسترش محیط‌های واقعیت مجازی، هوش مصنوعی و زیست‌بوم‌های متاورسی، صرفاً شکل جدیدی از ارتباطات دیجیتال ایجاد نکرده، بلکه شیوه تحقق، تشدید و تجربه بزه‌دیدگی را نیز با تحول مواجه ساخته است. در این محیط‌ها، کنش‌های مجرمانه ممکن است از طریق آواتارها، داده‌های شخصی، دارایی‌های رمزنگاری‌شده و تعاملات بلادرنگ تحقق یابند و آثار آنها نیز لزوماً در یک رفتار منفرد و قابل مشاهده خلاصه نشود. ویژگی‌هایی مانند غوطه‌وری، ناشناس بودن، وابستگی به معماری پلتفرم و ثبت بخش مهمی از تعاملات در قالب داده، موجب می‌شود بزه‌دیدگی در متاورس تنها حاصل رفتار مستقیم یک مرتکب نباشد، بلکه در بستر تعامل میان ویژگی‌های کاربر، رفتار مرتکب و ساختار فناورانه محیط شکل گیرد. از این منظر، مسئله اساسی پژوهش حاضر آن است که آیا مفاهیم و چارچوب‌های متعارف جرم‌شناسی بزه‌دیدگی، با وجود تفاوت بنیادین میان محیط فیزیکی و زیست‌بوم‌های غوطه‌ور، برای تبیین این وضعیت کفایت می‌کنند یا آنکه باید برخی مؤلفه‌های بزه‌دیدگی در پرتو ویژگی‌های معماری و فناورانه متاورس بازخوانی شوند. اهمیت این مسئله زمانی آشکارتر می‌شود که بزه‌دیدگی متاورسی در ارتباط با گروه‌های آسیب‌پذیر، داده‌های شخصی و دارایی‌های دیجیتال بررسی شود. در چنین محیطی، کودک ممکن است هم‌زمان در معرض فریب هویتی، سوءاستفاده تعاملی و پردازش داده‌های رفتاری قرار گیرد؛ یا تعرض به یک دارایی رمزنگاری‌شده با دسترسی غیرمجاز، فریب رایانه‌ای و بهره‌گیری از آسیب‌پذیری فنی پلتفرم همراه شود. افزون بر این، بخشی از شواهد بزه‌دیدگی در قالب داده‌های سیال و وابسته به زیرساخت پلتفرم تولید و نگهداری می‌شود و همین امر، شناسایی بزه‌دیده، انتساب رفتار و اثبات وقوع بزه را با مسائل متفاوتی نسبت به محیط‌های سنتی مواجه می‌کند. بنابراین، مسئله صرفاً ظهور اشکال جدیدی از جرم نیست، بلکه تغییر در مناسبات میان «بزه‌کار، بزه‌دیده، فرصت مجرمانه، نگهبان و محیط» است؛ تغییری که می‌تواند مبانی تحلیل جرم‌شناختی بزه‌دیدگی را تحت تأثیر قرار دهد. از حیث چارچوب نظری، این پژوهش برای تبیین این تحول، بیش از همه بر نظریه فعالیت روزمره کوهن و فلسن تکیه دارد؛ زیرا مؤلفه‌های این نظریه، یعنی بزه‌کار دارای انگیزه، هدف مناسب و فقدان نگهبان کارآمد، در محیط متاورسی در قالبی متفاوت بازتولید می‌شوند. در این فضا، معماری پلتفرم، نظام احراز هویت، ابزارهای کنترل دسترسی و سازوکارهای نظارتی می‌توانند در شکل‌گیری یا کاهش فرصت بزه‌کارانه نقش داشته باشند. در کنار آن، نظریه انتخاب عقلانی برای توضیح تأثیر ناشناس بودن، هزینه ارتکاب، دشواری شناسایی و منافع احتمالی مرتکب قابل استفاده است. بر این مبنا، «گذار» مورد بحث در پژوهش حاضر به معنای کنارگذاشتن نظریه‌های کلاسیک جرم‌شناسی نیست، بلکه ناظر به تغییر بستر تحقق مؤلفه‌های بزه‌دیدگی و انتقال بخشی از عوامل خطر از محیط فیزیکی به معماری دیجیتال و پلتفرمی است.

در پژوهش‌های داخلی، احسان‌پور و قدمی عزیزآباد (۱۴۰۳) با بررسی مؤلفه‌های سیاست جنایی مطلوب در پیشگیری از بزه‌دیدگی جنسی کودکان در فضای مجازی، بر نقش ضعف سازوکارهای پیشگیرانه و حمایتی در افزایش آسیب‌پذیری کودکان تأکید کرده‌اند. در پژوهش‌های خارجی نیز Park and Kim (۲۰۲۴) با بررسی آزار و بزه‌دیدگی جنسی در متاورس، نقش غوطه‌وری، ناشناس بودن و تعاملات بلادرنگ را در ایجاد مخاطرات جدید مورد توجه قرار داده‌اند. با وجود این، مطالعات موجود غالباً یک بُعد خاص از بزه‌دیدگی، مانند بزه‌دیدگی جنسی، کودکان یا مخاطرات داده‌ای را بررسی کرده‌اند و کمتر به مفهوم بزه‌دیدگی دیجیتال در متاورس به‌عنوان پدیده‌ای چندلایه و

متأثر از تعامل میان معماری پلتفرم، رفتار کاربران و فرصت‌های مجرمانه پرداخته‌اند. خلأ اصلی پژوهش حاضر نیز در همین نقطه قرار دارد. بر این اساس، پژوهش حاضر می‌کوشد با رویکردی جرم‌شناختی و با بهره‌گیری از نظریه فعالیت روزمره و نظریه انتخاب عقلانی، ابعاد بزه‌دیدگی در زیست‌بوم‌های متاورسی را در پیوند با هویت آواتاری، گروه‌های آسیب‌پذیر، دارایی‌های دیجیتال و ادله الکترونیکی تحلیل کند و نشان دهد که ویژگی‌های فناوریانه این محیط چگونه الگوی سنتی فرصت بزهکارانه و حمایت از بزه‌دیده را دگرگون می‌سازد. فرضیه اصلی پژوهش آن است که بزه‌دیدگی در زیست‌بوم متاورس، به دلیل تعامل میان رفتار کاربران، معماری پلتفرم و سازوکارهای فناوریانه، واجد ابعاد ساختاری و چندعاملی است و ازاین‌رو، تبیین و پیشگیری مؤثر از آن مستلزم بازخوانی برخی مؤلفه‌های سنتی جرم‌شناسی بزه‌دیدگی متناسب با ویژگی‌های محیط دیجیتال و غوطه‌ور است.

۱. مفهومی‌سازی جرم‌شناختی بزه‌دیدگی دیجیتال در زیست‌بوم‌های متاورسی

زیست‌بوم‌های متاورسی را می‌توان از پیچیده‌ترین اشکال نوظهور تحول‌یافته فضای سایبر - فیزیکی دانست که در آن، تعاملات انسانی، اجتماعی، اقتصادی، فرهنگی و هویتی در محیطی تعاملی، غوطه‌ور و مبتنی بر داده شکل می‌گیرد. ویژگی اساسی این زیست‌بوم‌ها صرفاً مجازی بودن محیط تعامل نیست، بلکه پیوند میان شخص حقیقی، بازنمایی دیجیتال وی، داده‌های حاصل از رفتار و تعاملات اجتماعی و اقتصادی شکل گرفته در پلتفرم است. در چنین محیطی، کنش انسانی می‌تواند از طریق آواتار، داده‌های رفتاری و ارتباطات دیجیتال در محیط مجازی امتداد یابد و ازاین‌رو، زمینه‌های جدیدی برای بزه‌دیدگی فراهم شود. بااین‌حال، در تحلیل جرم‌شناختی باید میان «آسیب‌پذیری»، «خطر بزه‌دیدگی»، «بزه‌دیدگی بالفعل» و «پیامدهای ناشی از بزه‌دیدگی» تفکیک شود؛ زیرا هر تجربه ناخوشایند یا هر آسیب روانی، اجتماعی یا اقتصادی در محیط متاورسی الزاماً به معنای تحقق بزه‌دیدگی کیفری نیست و تحقق وصف کیفری رفتار، در نهایت به انطباق آن با عناصر یکی از عناوین مجرمانه مقرر در قانون نیاز دارد. در حقوق ایران، برای نمونه، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ در ماده ۱ دسترسی غیرمجاز به داده یا سامانه رایانه‌ای یا مخابراتی حفاظت‌شده را جرم‌انگاری کرده و در مواد بعدی نیز رفتارهایی مانند تخریب، اخلال، ربایش و انتشار یا افشای غیرمجاز داده‌ها را حسب شرایط مورد حکم قرار داده است؛ بنابراین، تحلیل جرم‌شناختی بزه‌دیدگی دیجیتال باید از مفهوم عام آسیب فراتر رفته و مشخص کند که در هر وضعیت، چه رفتاری موجب ایجاد خطر بزه‌دیدگی شده، چه حقی یا منفعتی مورد تعرض قرار گرفته و رفتار ارتكابی در چه شرایطی واجد وصف مجرمانه است. بر این اساس، بزه‌دیدگی دیجیتال در متاورس را نمی‌توان صرفاً نتیجه مستقیم رفتار مجرمانه یک فرد مشخص دانست، بلکه می‌توان آن را حاصل برهم‌کنش میان کنشگران انسانی و عوامل محیطی، فناوریانه و سازمانی مؤثر بر فرصت و خطر بزه‌دیدگی تحلیل کرد؛ عواملی همچون معماری نرم‌افزاری، طراحی رابط کاربری، سازوکارهای احراز هویت، نحوه تنظیم دسترسی‌ها، شیوه مدیریت داده و قواعد حاکم بر تعاملات دیجیتال می‌توانند احتمال وقوع رفتارهای زیان‌بار یا امکان تحقق موفقیت‌آمیز آنها را افزایش یا کاهش دهند. از این منظر، مفهوم «اکوسیستم بزه‌زا» را می‌توان برای تبیین توزیع عوامل خطر در محیط متاورسی به کار گرفت؛ اما این مفهوم نباید با مفهوم «مسئولیت» یکسان تلقی شود، زیرا نقش یک عامل فناوریانه در ایجاد یا تشدید خطر بزه‌دیدگی، به‌خودی‌خود موجب انتساب مسئولیت کیفری یا مدنی به طراح یا بهره‌بردار پلتفرم نخواهد بود و تحقق چنین مسئولیتی مستلزم احراز شرایط و مبانی مستقل قانونی است. بنابراین، بزه‌دیدگی در

متاورس از منظر جرم‌شناختی می‌تواند فرایندی شبکه‌ای و چندعاملی باشد، بی‌آنکه این امر به معنای نفی نقش رفتار مستقیم مرتکب یا جایگزینی کامل مسئولیت انسانی با مسئولیت ساختاری باشد (Wang et al., 2022, 6). یکی از وجوه مهم بزه‌دیدگی در این محیط، تغییر در نحوه تجربه و ادراک آسیب است؛ زیرا کاربر ممکن است رفتار آسیب‌زا را نه صرفاً به‌عنوان رویدادی بیرونی، بلکه در قالب تجربه‌ای غوطه‌ور و مرتبط با هویت دیجیتال خود ادراک کند. در چنین وضعیتی، آثار روانی و اجتماعی رفتار مجرمانه می‌تواند از محیط دیجیتال به زندگی واقعی کاربر امتداد یابد و بر احساس امنیت، روابط اجتماعی و ادراک وی از هویت خود تأثیر بگذارد (Park & Kim, 2024, 492). با این حال، این آثار باید به‌عنوان پیامدهای بزه‌دیدگی از خود بزه‌دیدگی تفکیک شوند؛ زیرا آسیب روانی یا اجتماعی ممکن است نتیجه یک رفتار مجرمانه باشد، اما به‌خودی‌خود موضوع مستقل جرم محسوب نمی‌شود. در این میان، آواتار به‌عنوان بازنمایی دیجیتال کاربر، جایگاه ویژه‌ای در تحلیل بزه‌دیدگی دارد، اما نمی‌توان در همه موارد آن را معادل شخص حقیقی یا بخشی از شخصیت حقوقی وی تلقی کرد. آواتار ممکن است در یک پلتفرم صرفاً نقش نمایشی داشته باشد، در حالی که در محیطی دیگر ممکن است بازنمایی هویتی کاربر، وسیله تعامل اجتماعی یا حتی حامل ارزش اقتصادی باشد؛ بنابراین، ماهیت حقوقی و جرم‌شناختی تعرض به آواتار باید بر اساس کارکرد و موضوع تعرض تعیین شود. اگر رفتار مرتکب متوجه تحقیر یا تعرض به بازنمایی هویتی شخص باشد، آثار آن می‌تواند در قلمرو بزه‌دیدگی هویتی و روانی بررسی شود؛ اگر رفتار ناظر بر اطلاعاتی باشد که قابلیت انتساب به شخص حقیقی داشته و در قلمرو داده‌های شخصی قرار گیرد، موضوع می‌تواند در چارچوب حمایت از داده‌های شخصی تحلیل شود؛ و اگر آواتار یا اجزای وابسته به آن واجد ارزش اقتصادی مستقل باشد، تعرض ممکن است واجد جنبه مالی نیز باشد.

در حقوق ایران، مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی مصوب ۱۳۸۲، با تعیین شرایط مربوط به جمع‌آوری، پردازش و توزیع داده‌های شخصی، مبنایی برای تفکیک حمایت از داده‌های شخصی از سایر اشکال تعرض فراهم کرده‌اند؛ از این رو، صرف دیجیتالی‌بودن آواتار یا ارتباط آن با کاربر برای تلقی آن به‌عنوان داده شخصی یا مال کافی نیست و باید نوع رابطه آن با شخص، داده‌های موجود در آن و ارزش اقتصادی احتمالی آن به‌طور جداگانه احراز شود. بر همین اساس، مفهوم «هویت ترکیبی فیزیکی - دیجیتال» باید به‌عنوان یک مفهوم تحلیلی برای توضیح پیوند میان شخص و بازنمایی دیجیتال او مورد استفاده قرار گیرد، نه آنکه بدون تفکیک، هرگونه آسیب به بازنمایی دیجیتال را معادل تعرض مستقیم به شخص حقیقی تلقی کند (Bryson et al., 2017, 279). افزون بر این، بزه‌دیدگی در زیست‌بوم‌های متاورسی تا حدی متأثر از ویژگی‌های طراحی و معماری پلتفرم است. نبود سازوکارهای مؤثر برای کنترل تعاملات هم‌زمان، ضعف تدابیر احراز هویت و کنترل دسترسی، فقدان ابزارهای مناسب برای گزارش و مهار رفتارهای آسیب‌زا و ضعف تدابیر امنیتی می‌تواند فرصت ارتکاب رفتارهای مجرمانه یا زیان‌بار را افزایش دهد (Chawki et al., 2024, 41). با این حال، این عوامل باید در سطح جرم‌شناختی به‌عنوان عوامل افزایش‌دهنده فرصت و خطر بزه‌دیدگی تحلیل شوند و تنها در صورت وجود مبنای قانونی و احراز شرایط لازم می‌توان درباره مسئولیت حقوقی یا کیفری اشخاص یا پلتفرم‌های مرتبط بحث کرد. از سوی دیگر، ماهیت اقتصادی متاورس موجب می‌شود که بزه‌دیدگی در این محیط تنها به آثار هویتی و روانی محدود نماند. دارایی‌های دیجیتال، توکن‌های غیرمثلی، اقلام درون‌پلتفرمی و سایر ارزش‌های اقتصادی ممکن است موضوع رفتارهای مجرمانه یا زیان‌بار قرار گیرند و در نتیجه، نوعی بزه‌دیدگی مالی ایجاد کنند. با این حال، این موارد باید از بزه‌دیدگی هویتی و داده‌محور تفکیک شوند؛ زیرا از دست‌رفتن یک دارایی دیجیتال، افشای اطلاعات شخصی و تحقیر کاربر از طریق آواتار، اگرچه ممکن است هم‌زمان رخ دهند و پیامدهای

مشترکی ایجاد کنند، از حیث موضوع تعرض و منفعت مورد حمایت یکسان نیستند. بنابراین، می‌توان بزه‌دیدگی در متاورس را از حیث موضوع تعرض در سه سطح عمده شخص‌محور، داده‌محور و دارایی‌محور تحلیل کرد و در کنار آن، آثار روانی و اجتماعی هر یک را به‌عنوان پیامدهای بزه‌دیدگی مورد بررسی قرار داد. از منظر ساختاری نیز متاورس محیطی است که در آن برخی عوامل فناورانه می‌توانند فرصت ارتکاب جرم و احتمال بزه‌دیدگی را افزایش دهند؛ از این‌رو، بزه‌دیدگی را می‌توان نه صرفاً یک رخداد منفرد، بلکه در برخی موارد نتیجه برهم‌کنش میان رفتار مرتکب، ویژگی‌های بزه‌دیده و شرایط محیطی و فناورانه دانست. با این حال، تعبیر «تعبیه بزه‌دیدگی در معماری متاورس» نیازمند احتیاط مفهومی است؛ زیرا وجود ریسک ذاتی در یک محیط تعاملی به معنای اجتناب‌ناپذیری بزه‌دیدگی یا مجرمانه‌بودن طراحی آن نیست، بلکه می‌توان از وجود ظرفیت‌ها و آسیب‌پذیری‌های ساختاری سخن گفت که از طریق تدابیر فنی، مدیریتی و حقوقی قابلیت کاهش دارند (Qin et al., 2025, 201). بر این اساس، مفهومی‌سازی جرم‌شناختی بزه‌دیدگی دیجیتال در زیست‌بوم‌های متاورسی مستلزم گذار از الگوی صرفاً فردمحور به تحلیلی چندسطحی است که در آن، رفتار مرتکب، ویژگی‌های بزه‌دیده، ساختارهای اجتماعی، معماری فناورانه و ویژگی‌های اقتصادی محیط دیجیتال در ارتباط با یکدیگر بررسی شوند. در این چارچوب، متاورس صرفاً محل وقوع جرم نیست، بلکه محیطی است که می‌تواند با ایجاد فرصت، افزایش آسیب‌پذیری یا تشدید آثار رفتار مجرمانه بر فرایند بزه‌دیدگی اثر بگذارد؛ با این حال، این نقش ساختاری باید از تحقق جرم، تعیین موضوع حق یا منفعت مورد تعرض و انتساب مسئولیت حقوقی یا کیفری تفکیک شود تا مفهوم بزه‌دیدگی چندلایه، ضمن حفظ ظرفیت جرم‌شناختی خود، با الزامات مفهومی و حقوقی تحلیل بزه‌دیدگی نیز سازگار باقی بماند.

۲. تحلیل ماهیت حقوقی متاورس و پیامدهای آن بر وضعیت بزه‌دیده در جرم‌شناسی نوین

متاورس به‌عنوان یک زیست‌بوم نوظهور سایبر - فیزیکی را نمی‌توان صرفاً فناوری یا بستر ارتباطی جدیدی دانست، بلکه از منظر حقوقی باید آن را محیطی چندلایه تلقی کرد که در آن روابط میان کاربران، ارائه‌دهندگان خدمات، صاحبان زیرساخت، تولیدکنندگان محتوا و دارایی‌های دیجیتال در پیوند با معماری فنی پلتفرم شکل می‌گیرد. ویژگی اصلی این محیط، حذف کامل عناصر حقوق سنتی نیست، بلکه جابه‌جایی و پیچیده‌شدن نحوه اعمال آنهاست؛ به‌گونه‌ای که عنصر سرزمین همچنان از طریق محل اقامت یا استقرار اشخاص، محل وقوع بخشی از رفتار، محل استقرار زیرساخت‌ها و آثار زیان‌بار رفتار اهمیت دارد، اما در کنار آن با محیطی مواجه هستیم که رفتار و آثار آن می‌تواند به‌طور هم‌زمان در چند قلمرو حقوقی تحقق یابد. از این‌رو، متاورس را می‌توان محیطی دانست که در آن تعیین قانون حاکم، دادگاه صالح، موضوع حق و شخص مسئول، مستلزم توجه هم‌زمان به عناصر فیزیکی و دیجیتال رابطه است و نه کنارگذاشتن قواعد سنتی صلاحیت و مسئولیت (Qin et al., 2025, 197). در این چارچوب، شخص نیز از میان نمی‌رود، بلکه حضور او در محیط دیجیتال از طریق حساب کاربری، آواتار، داده‌های هویتی، داده‌های رفتاری و سایر بازنمایی‌های دیجیتال تحقق می‌یابد؛ بنابراین، آواتار را نباید بدون تحلیل بیشتر معادل شخص حقیقی یا شخصیت حقوقی او دانست، بلکه باید حسب کارکرد و موضوع تعرض مشخص کرد که رفتار ارتكابی متوجه خود شخص، داده‌های شخصی، هویت دیجیتال، اثر فکری یا منفعت مالی وابسته به محیط متاورسی است. همین تفکیک در تعیین وضعیت بزه‌دیده اهمیت اساسی دارد؛ زیرا شخصی که حساب کاربری او مورد نفوذ قرار گرفته، شخصی که داده‌های

شخصی او افشا شده، پدیدآورنده‌ای که اثر دیجیتال وی بدون مجوز مورد بهره‌برداری قرار گرفته و دارنده منفعت اقتصادی مرتبط با یک دارایی دیجیتال، ممکن است از حیث موضوع تعرض و مبنای حمایت حقوقی، وضعیت یکسانی نداشته باشند. در حقوق ایران، بخشی از این وضعیت‌ها را می‌توان با قوانین موجود تحلیل کرد. برای نمونه، ماده ۱ قانون جرایم رایانه‌ای مصوب ۱۳۸۸، که مواد آن به موجب ماده ۵۵ همان قانون به قانون مجازات اسلامی (تعزیرات) الحاق شده است، دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی حفاظت‌شده را جرم‌انگاری کرده است؛ بنابراین، نفوذ غیرمجاز به حساب یا زیرساخت مرتبط با یک محیط متاورسی، در صورت تحقق سایر شرایط قانونی، می‌تواند در چارچوب این عنوان مورد بررسی قرار گیرد. همچنین، جعل رایانه‌ای موضوع ماده ۶ و کلاهبرداری مرتبط با سامانه‌های رایانه‌ای موضوع ماده ۱۳ همان قانون، حسب نحوه ارتکاب رفتار، می‌تواند برای تحلیل مواردی مانند ایجاد یا تغییر متقلبه داده‌های دیجیتال، دستکاری داده‌های قابل استناد یا تحصیل مال و منفعت از طریق عملیات متقلبه در محیط متاورسی مورد توجه قرار گیرند؛ باین حال، انطباق هر مصداق متاورسی با این عناوین نیازمند احراز عناصر اختصاصی همان جرم است و صرف وقوع رفتار در محیط متاورس برای تحقق عنوان کیفری کفایت نمی‌کند. از سوی دیگر، بخش مهمی از هویت و فعالیت کاربران متاورسی بر داده‌های شخصی استوار است و از این حیث، قانون تجارت الکترونیکی مصوب ۱۳۸۲ واجد ظرفیت مهمی برای تحلیل وضعیت بزه‌دیده است. ماده ۵۸ این قانون، ذخیره، پردازش یا توزیع برخی داده‌پیام‌های شخصی، از جمله داده‌های مربوط به وضعیت جسمانی، روانی و جنسی، بدون رضایت صریح شخص را غیرقانونی اعلام کرده و ماده ۵۹ نیز در فرض وجود رضایت، شرایطی مانند مشخص بودن هدف پردازش، تناسب داده‌های جمع‌آوری‌شده با هدف، صحت و روزآمدی داده و امکان دسترسی و اصلاح یا محو آنها را مورد توجه قرار داده است. بنابراین، گردآوری و پردازش گسترده داده‌های رفتاری کاربران متاورس را نمی‌توان صرفاً مسئله‌ای فنی دانست، بلکه باید آن را از منظر حدود حمایت قانونی از داده‌های شخصی نیز بررسی کرد. در حوزه آثار و دارایی‌های دیجیتال نیز باید میان «دارایی دیجیتال» به معنای عام و «اثر مورد حمایت مالکیت ادبی و هنری» تفکیک کرد.

قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ در ماده ۱، اثر را حاصل دانش، هنر یا ابتکار پدیدآورنده دانسته و ماده ۲ نیز طیف متنوعی از آثار، از جمله آثار تصویری، تجسمی و آثار فنی و ابتکاری را تحت حمایت قرار داده است؛ ماده ۳ نیز حقوق انحصاری نشر، پخش، عرضه و اجرای اثر و حقوق مادی و معنوی پدیدآورنده را شناسایی می‌کند. از این رو، در خصوص یک NFT یا دارایی مبتنی بر محتوای دیجیتال، نخست باید مشخص شود که موضوع مورد تعرض خود «اثر» و حقوق پدیدآورنده است یا صرفاً منفعت و حق اقتصادی ناشی از یک دارایی دیجیتال؛ زیرا ثبت یک اثر یا دارایی بر بستر دیجیتال، به‌تنهایی موجب نمی‌شود تمام حقوق مرتبط با آن در قلمرو قانون حمایت از حقوق مؤلفان و مصنفان و هنرمندان قرار گیرد. در همین زمینه، مقررات قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹ نیز در مواردی که موضوع تعرض نرم‌افزار یا اجزای واجد شرایط آن باشد، می‌تواند در تحلیل حقوقی آثار و زیرساخت‌های دیجیتال مورد توجه قرار گیرد؛ ماده ۱ این قانون حق نشر، عرضه، اجرا و بهره‌برداری مادی و معنوی از نرم‌افزار رایانه‌ای را برای پدیدآورنده شناسایی کرده است. وضعیت بزه‌دیده در متاورس همچنین در مورد اطفال و نوجوانان اهمیت مضاعف دارد؛ زیرا غوطه‌وری و تعامل هم‌زمان در این محیط می‌تواند اشکال جدیدی از ارتباط و آزار را امکان‌پذیر کند. قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹ در ماده ۱۰، آزار و سوءاستفاده جنسی از طفل یا نوجوان را در اشکال مختلف مورد حکم قرار داده و در بند ۹ همین ماده، برقراری ارتباط

با طفل یا نوجوان در فضای مجازی به منظور هرگونه آزار جنسی یا ارتباط جنسی نامشروع را به‌طور خاص جرم‌انگاری کرده است. بنابراین، محیط متاورسی را نمی‌توان از شمول تحلیل حمایت کیفری از اطفال و نوجوانان صرفاً به دلیل تفاوت فناوری آن با فضای مجازی متعارف خارج دانست؛ بلکه در هر مورد باید رفتار ارتكابی با عناصر قانونی مقرر تطبیق داده شود. افزون بر این، قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱ نیز از حیث تنظیم جایگاه داده و اطلاعات در نظام حقوقی ایران، ظرفیت مهمی برای تحلیل محیط‌های داده‌محور دارد؛ این قانون با تعیین تعاریف و الزامات مرتبط با مدیریت داده‌ها و اطلاعات ملی، نشان می‌دهد که داده دیگر صرفاً یک محصول جانبی فعالیت‌های فناورانه نیست، بلکه موضوع تنظیم و سیاست‌گذاری حقوقی قرار گرفته است. از این‌رو، در تحلیل بزه‌دیدگی متاورسی، داده‌های تولیدشده از رفتار کاربران، نحوه دسترسی و پردازش آنها و رابطه میان نهادهای دارنده یا پردازش‌کننده داده و اشخاص موضوع داده باید در کنار قواعد کیفری مربوط به دسترسی و سوءاستفاده از داده مورد بررسی قرار گیرد. از منظر جرم‌شناختی، یکی از مهم‌ترین پیامدهای این ساختار چندلایه، دشوارشدن تعیین رابطه میان رفتار، نتیجه و عامل ایجادکننده خطر است. با این حال، این دشواری را نباید به معنای فقدان کامل رابطه علی یا غیرممکن بودن انتساب دانست. ممکن است رفتار بزه‌دیده، رفتار مرتکب و ویژگی‌های فنی پلتفرم در شکل‌گیری یک نتیجه زیان‌بار با یکدیگر تلاقی کنند، اما مسئولیت کیفری همچنان نیازمند احراز شرایط مقرر در قانون و انتساب رفتار مجرمانه به شخص واجد شرایط مسئولیت است. بنابراین، نقش طراحی پلتفرم یا عملکرد یک سامانه خودکار را می‌توان در سطح جرم‌شناختی به‌عنوان عامل افزایش‌دهنده فرصت یا خطر بزه‌دیدگی تحلیل کرد، اما از این امر نمی‌توان مستقیماً مسئولیت کیفری پلتفرم یا طراح آن را نتیجه گرفت (Chawki et al., 2024, 42). همین تفکیک در حوزه مسئولیت مدنی نیز اهمیت دارد؛ زیرا برای انتساب مسئولیت به ارائه‌دهنده خدمت باید مبنای مسئولیت، تکلیف نقض‌شده، رابطه سببیت و سایر شرایط مقرر در نظام حقوقی احراز شود. از سوی دیگر، ماهیت فرامرزی متاورس موجب می‌شود مسئله صلاحیت قضایی و قانون حاکم اهمیت بیشتری پیدا کند. با این حال، برخلاف این تصور که قواعد سنتی صلاحیت در محیط متاورس کاملاً کارایی خود را از دست می‌دهند، باید گفت این قواعد همچنان نقطه آغاز تحلیل‌اند و چالش اصلی در تعیین ارتباط مؤثر میان رفتار دیجیتال و عناصر سرزمینی یا شخصی صلاحیت است. برای نمونه، محل اقامت بزه‌دیده، محل استقرار مرتکب، محل استقرار یا مدیریت زیرساخت، محل تحقق بخشی از رفتار و محل ظهور نتیجه زیان‌بار می‌توانند در تحلیل صلاحیت مؤثر باشند. از این منظر، وضعیت بزه‌دیده در متاورس با مسئله‌ای دوگانه مواجه است: از یک سو، رفتار مجرمانه ممکن است در محیطی فرامرزی تحقق یابد و شناسایی مرتکب یا جمع‌آوری ادله دشوار شود و از سوی دیگر، بزه‌دیده باید بتواند حق خود را در یکی از نظام‌های قضایی موجود پیگیری کند (Wang et al., 2022, 12). در کنار مسئله صلاحیت، مفهوم ضرر نیز نیازمند تفکیک دقیق است.

در محیط متاورسی ممکن است رفتار واحد، هم‌زمان موجب از بین رفتن منفعت اقتصادی، تعرض به داده‌های شخصی، خدشه به اعتبار یا ایجاد آسیب روانی شود؛ اما وجود این آثار به معنای آن نیست که همه آنها از یک مبنای حقوقی برخوردارند. برای مثال، حذف یک دارایی دیجیتال، افشای داده شخصی و تحقیر کاربر از طریق آواتار، هر یک موضوع تعرض و مبنای حمایتی متفاوتی دارند و قابلیت مطالبه یا جبران آنها باید بر اساس قواعد مربوط به همان حق یا منفعت بررسی شود. از این‌رو، بزه‌دیده متاورسی را باید نه یک موجودیت واحد و همگن، بلکه شخصی دانست که ممکن است هم‌زمان در معرض تعرض به شخصیت، داده، حقوق فکری یا منافع مالی خود قرار گیرد. این تفکیک، امکان تحلیل دقیق‌تر رابطه میان نوع بزه‌دیدگی و سازوکار جبران یا حمایت را فراهم می‌کند. در سطح نهادی نیز

پلتفرم‌ها در متاورس صرفاً بستر خنثی وقوع رفتار نیستند و تصمیمات مربوط به طراحی، احراز هویت، کنترل دسترسی، نظارت، گزارش‌دهی و تعدیل محتوا می‌تواند بر سطح خطر بزه‌دیدگی اثر بگذارد؛ اما این نقش باید در سه سطح از یکدیگر تفکیک شود: نخست، نقش پلتفرم به‌عنوان عامل مؤثر بر ایجاد یا تشدید خطر در تحلیل جرم‌شناختی؛ دوم، تکالیف قانونی و قراردادی پلتفرم در برابر کاربران؛ و سوم، مسئولیت احتمالی پلتفرم در صورت احراز نقض تکلیف و سایر شرایط قانونی (Chawki et al., 2024, 45). در خصوص رویه قضایی نیز یکی از خلأهای مهم در مطالعه متاورس در حقوق ایران، محدودبودن آرای اختصاصی ناظر بر خود متاورس است؛ بنابراین، به‌جای ادعای وجود رویه تثبیت‌شده درباره بزه‌دیدگی متاورسی، باید از ظرفیت رویه قضایی موجود در حوزه جرایم رایانه‌ای، دسترسی غیرمجاز، جعل و کلاهبرداری رایانه‌ای، نقض حقوق مالکیت فکری و تعرض به داده‌های شخصی برای تحلیل قابلیت انطباق قواعد موجود استفاده کرد. چنین رویکردی از یک سو از تعمیم شتاب‌زده عناوین قانونی به پدیده‌ای نوظهور جلوگیری می‌کند و از سوی دیگر نشان می‌دهد که کدام بخش از بزه‌دیدگی متاورسی با ظرفیت قوانین موجود قابل پوشش است و کدام بخش نیازمند تفسیر، تکمیل یا وضع قواعد جدید خواهد بود. بر این اساس، ماهیت حقوقی متاورس بیش از آنکه نشان‌دهنده فروپاشی کامل مفاهیم سنتی حقوق باشد، بیانگر انتقال آنها به محیطی چندلایه و فرامرزی است؛ محیطی که در آن شخص، داده، هویت دیجیتال، اثر فکری و منفعت اقتصادی می‌توانند به‌طور هم‌زمان موضوع تعرض قرار گیرند و در نتیجه، وضعیت بزه‌دیده نیز از حالت ساده و تک‌بعدی خارج شود. بنابراین، تحلیل بزه‌دیدگی در متاورس در حقوق ایران مستلزم پیوند هم‌زمان میان مقررات قانون جرایم رایانه‌ای، قانون تجارت الکترونیکی، قوانین مالکیت فکری، قانون حمایت از اطفال و نوجوانان، قانون مدیریت داده‌ها و اطلاعات ملی و قواعد صلاحیت و مسئولیت است؛ رویکردی که امکان تبدیل مطالعه متاورس از یک بحث صرفاً نظری به تحلیل حقوقی کاربردی و مبتنی بر ظرفیت واقعی نظام حقوقی ایران را فراهم می‌سازد.

۳ بزه‌دیدگی مبتنی بر هویت آواتاری و مسئله انتساب بزه‌دیده در فضای دیجیتال

بزه‌دیدگی مبتنی بر هویت آواتاری یکی از جلوه‌های مهم تحول بزه‌دیدگی در زیست‌بوم‌های متاورسی است؛ زیرا حضور کاربر در این محیط صرفاً از طریق مشخصات هویتی رسمی تحقق نمی‌یابد، بلکه آواتار، داده‌های رفتاری، سابقه تعاملات و سایر بازنمایی‌های دیجیتال نیز در شکل‌گیری هویت او در محیط مجازی نقش دارند. با این حال، آواتار را نباید در همه موارد معادل شخص حقیقی یا دارای شخصیت حقوقی مستقل تلقی کرد، بلکه باید میان «شخص بزه‌دیده»، «آواتار به‌عنوان بازنمایی دیجیتال» و «حقوق یا منافع مرتبط با آواتار» تفکیک نمود. بر این اساس، تعرض به آواتار ممکن است حسب موضوع و شیوه ارتکاب، متوجه حیثیت و هویت شخص، داده‌های مرتبط با وی، حقوق فکری یا یک منفعت اقتصادی باشد و وصف حقوقی رفتار نیز بر همین اساس تعیین شود (Bryson et al., 2017, 279). برای نمونه، دسترسی غیرمجاز به حساب یا سامانه‌ای که آواتار در آن ایجاد و نگهداری می‌شود، در صورت تحقق شرایط قانونی، می‌تواند با ماده ۱ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ منطبق شود؛ تغییر یا ایجاد متقلبانه داده‌های مرتبط با هویت دیجیتال نیز حسب شرایط می‌تواند در قلمرو ماده ۶ و تحصیل مال یا منفعت از طریق عملیات متقلبانه رایانه‌ای در قلمرو ماده ۱۳ همان قانون قرار گیرد. بنابراین، «بزه‌دیدگی آواتاری» عنوان مجرمانه مستقلی نیست، بلکه مفهومی جرم‌شناختی برای توصیف وضعیتی است که در آن، تعرض به بازنمایی دیجیتال یا حقوق و منافع وابسته به آن، موجب ورود آسیب به شخص حقیقی می‌شود. در این چارچوب، جعل هویت آواتاری، ربایش حساب، دستکاری مشخصات

آواتار، حذف یا تخریب آن و استفاده غیرمجاز از بازنمایی دیجیتال می‌توانند اشکال متفاوتی از بزه‌دیدگی ایجاد کنند و آثار آنها نیز ممکن است هم‌زمان روانی، اجتماعی و اقتصادی باشد (Park & Kim, 2024, 491). بااین‌حال، تحقق این آثار به‌خودی‌خود موجب ایجاد مسئولیت کیفری برای هر شخصی که به‌نحوی در محیط فنی دخالت داشته است نمی‌شود؛ زیرا اصل شخصی بودن مسئولیت کیفری اقتضا می‌کند که رفتار مجرمانه و نتیجه آن به شخص معین قابل انتساب باشد. مسئله مهم در متاورس زمانی شکل می‌گیرد که نتیجه زیان‌بار حاصل رفتار یک کاربر، ویژگی‌های طراحی پلتفرم و عملکرد یک سامانه خودکار باشد. در چنین وضعیتی، به‌جای استفاده از تعبیر کلی و مبهم «توزیع مسئولیت»، باید نقش هر عامل در زنجیره سببیت به‌طور مستقل بررسی شود. در حقوق کیفری ایران، ماده ۵۲۶ قانون مجازات اسلامی مصوب ۱۳۹۲ برای مواردی که چند عامل در وقوع جنایت مؤثر باشند، معیار تعیین میزان تأثیر و انتساب را مورد توجه قرار داده است؛ بنابراین، اصل قابل استفاده در تحلیل این وضعیت، شناسایی رفتار مؤثر و تعیین رابطه آن با نتیجه است، نه فرض مسئولیت مشترک صرفاً به دلیل حضور چند عامل در فرایند. در نتیجه، اگر رفتار کاربر مستقیماً موجب ورود آسیب شود و طراحی پلتفرم صرفاً زمینه وقوع رفتار را فراهم کرده باشد، نمی‌توان بدون احراز شرایط قانونی، پلتفرم را مسئول نتیجه دانست؛ برعکس، اگر ارائه‌دهنده خدمت با وجود تکلیف مشخص قانونی یا قراردادی، از اتخاذ تدابیر لازم خودداری کرده و این ترک فعل در شرایط قانونی رابطه سببیت مؤثری با نتیجه داشته باشد، موضوع قابلیت بررسی مستقل خواهد داشت. همچنین، عملکرد خودکار یک سامانه یا الگوریتم، به‌خودی‌خود شخص مسئول محسوب نمی‌شود و باید بررسی شود که تصمیم یا عملکرد آن به رفتار کدام شخص حقیقی یا حقوقی قابل انتساب است و آیا آن شخص تکلیف قانونی یا قراردادی قابل استنادی داشته است یا خیر. ازاین‌رو، نظریه «سبب اقوی از مباشر» نیز نمی‌تواند بدون احراز شرایط آن به‌عنوان مبنای عام انتساب در همه وقایع متاورسی به کار رود؛ بلکه باید مشخص شود کدام رفتار از نظر حقوقی علت مؤثر در نتیجه بوده و آیا عوامل دیگر صرفاً زمینه‌ساز، تسهیل‌کننده یا هم‌زمان با آن بوده‌اند. به همین ترتیب، مسئولیت ناشی از فعل غیر یا مسئولیت عینی نیز تنها در مواردی قابل استناد است که قانون مبنای مشخصی برای آن مقرر کرده باشد و نمی‌توان صرف پیچیدگی فنی متاورس را دلیل عدول از اصل تقصیر یا شخصی بودن مسئولیت دانست. از منظر جرم‌شناختی، بنابراین، می‌توان از «چندعاملی بودن فرایند بزه‌دیدگی» سخن گفت، اما این مفهوم باید از «چندگانه‌بودن مسئولیت حقوقی» تفکیک شود.

در همین راستا، پلتفرم ممکن است از طریق معماری فنی، سازوکار احراز هویت، تنظیم دسترسی، ابزارهای گزارش‌دهی و شیوه مدیریت محتوا بر احتمال وقوع بزه‌دیدگی اثر بگذارد، اما این اثرگذاری ابتدا در سطح تحلیل خطر و فرصت جرم قرار می‌گیرد و تنها در صورت احراز تکلیف نقض‌شده، تقصیر یا مبنای قانونی دیگر و رابطه سببیت، می‌تواند به بحث مسئولیت حقوقی منتهی شود. از سوی دیگر، بزه‌دیدگی آواتاری ممکن است به‌صورت تدریجی و انباشته تحقق یابد؛ برای مثال، تکرار تحقیر، طرد اجتماعی یا دستکاری مستمر بازنمایی دیجیتال می‌تواند آثار روانی و اجتماعی قابل توجهی ایجاد کند، هرچند از نظر حقوقی باید میان استمرار رفتار مجرمانه، تعدد رفتارها و صرف انباشت آثار زیان‌بار تفکیک شود (Park & Kim, 2024, 492). در این میان، مسئله «انتساب بزه‌دیده» نیز باید با دقت مفهومی بررسی شود. در اغلب موارد، بزه‌دیده نهایی شخص حقیقی است و آواتار صرفاً وسیله، بازنمایی یا موضوع تعرض است؛ بااین‌حال، اگر آواتار واجد حقوق یا منافع اقتصادی قابل حمایت باشد، تعرض به آن می‌تواند علاوه بر آثار هویتی، واجد جنبه مالی نیز باشد. بنابراین، نمی‌توان هرگونه آسیب به آواتار را مستقیماً آسیب به شخصیت حقوقی

فرد دانست و باید نوع حق یا منفعت مورد تعرض مشخص شود. در نهایت، بزه‌دیدگی آواتاری را باید پدیده‌ای چندلایه دانست که در آن، «موضوع تعرض»، «شخص بزه‌دیده» و «عامل مسئول» سه مقوله متمایزند: شخص حقیقی ممکن است بزه‌دیده باشد، آواتار یا داده‌های مرتبط با آن ممکن است موضوع یا ابزار تعرض قرار گیرد و مسئولیت نیز صرفاً متوجه عاملی خواهد بود که رفتار یا ترک فعل وی، با احراز شرایط قانونی، قابل انتساب به نتیجه باشد. این تفکیک، امکان استفاده از رویکرد چندعاملی در جرم‌شناسی متاورسی را بدون عدول از اصول بنیادین حقوق کیفری، از جمله شخصی بودن مسئولیت و لزوم احراز رابطه سببیت، فراهم می‌کند.

۴. خشونت سایبری تعاملی و بزه‌دیدگی‌های مبتنی بر غوطه‌وری

خشونت سایبری تعاملی در محیط‌های متاورسی و واقعیت مجازی را باید یکی از پیچیده‌ترین اشکال خشونت دیجیتال دانست که در آن، کنش‌های آسیب‌زا نه به صورت منفعل یا یک‌طرفه، بلکه در قالب تعاملات زنده، بلادرنگ و چندکاربره شکل می‌گیرند. ویژگی بنیادین این نوع خشونت، «غوطه‌وری ادراکی» است؛ به این معنا که بزه‌دیده در محیطی قرار می‌گیرد که از نظر حسی و روانی، تا حد زیادی با واقعیت فیزیکی هم‌پوشانی پیدا می‌کند و همین امر موجب تشدید اثرات روانی و رفتاری خشونت می‌شود (Park & Kim, 2024, 492). در این نوع بزه‌دیدگی، خشونت دیگر یک کنش خطی میان دو فرد نیست، بلکه فرآیندی تعاملی است که در بستر شبکه‌ای از کاربران، آواتارها و سیستم‌های هوشمند رخ می‌دهد. این تعاملات می‌توانند شامل آزار کلامی بلادرنگ، محاصره تعاملی آواتار، حذف اجتماعی در فضاهای مجازی، یا ایجاد شرایط روانی فشارزا از طریق رفتارهای جمعی باشند. نکته مهم آن است که این رفتارها در بسیاری موارد به صورت پیوسته و تکرارشونده رخ می‌دهند و همین تداوم، بُعد آسیب‌زای آن‌ها را تشدید می‌کند.

به نقش عوامل اجتماعی و محیطی در شکل‌گیری بزه‌دیدگی در فضای مجازی اشاره شده است و تأکید می‌شود که بزه‌دیدگی صرفاً نتیجه یک عامل فردی نیست، بلکه محصول ساختارهای ارتباطی و اجتماعی نیز هست (خواجوند احمدی و ابراهیمی، ۱۴۰۰، ۶۲). این تحلیل در محیط‌های متاورسی اهمیت بیشتری پیدا می‌کند، زیرا ساختارهای تعاملی به گونه‌ای طراحی شده‌اند که امکان تقویت رفتارهای جمعی و سرایت خشونت را افزایش می‌دهند. یکی از ویژگی‌های مهم خشونت سایبری تعاملی، «شدت‌گیری لحظه‌ای» است. در محیط‌های غوطه‌ور، واکنش‌ها به رفتارهای خشونت‌آمیز می‌توانند به سرعت تشدید شوند و به چرخه‌های بازخورد منفی منجر گردند. این چرخه‌ها موجب می‌شوند که بزه‌دیدگی در زمان کوتاه از یک تعامل ساده به یک تجربه شدید روانی تبدیل شود. در چنین شرایطی، بزه‌دیده در وضعیت فشار شناختی و هیجانی مداوم قرار می‌گیرد که می‌تواند آثار بلندمدت بر سلامت روانی او داشته باشد (Chawki et al., 2024, 39). از منظر جرم‌شناسی نوین، یکی از ابعاد کلیدی این پدیده، «حذف مرز میان مشاهده‌گر و مشارکت‌کننده» است. در بسیاری از محیط‌های متاورسی، کاربران نه تنها شاهد خشونت هستند، بلکه به صورت مستقیم یا غیرمستقیم در آن مشارکت می‌کنند. این وضعیت موجب می‌شود که نقش‌های سنتی بزه‌کار، بزه‌دیده و ناظر در هم ادغام شوند و ساختارهای کلاسیک تحلیل جرم دچار فروپاشی نسبی شوند. در سطح نهادی نیز باید به نقش طراحی پلتفرم‌ها توجه کرد. پلتفرم‌های غوطه‌ور از طریق تنظیم شدت تعاملات، نوع ارتباطات و میزان آزادی عمل کاربران، در شکل‌گیری یا کنترل خشونت نقش مستقیم دارند. در بسیاری موارد، فقدان سازوکارهای کنترلی مؤثر یا تأخیر در مداخله سیستم، می‌تواند به تشدید خشونت تعاملی و افزایش دامنه بزه‌دیدگی منجر شود.

تحلیل این نوع بزه‌دیدگی باید به این نکته توجه شود که خشونت تعاملی در محیط‌های غوطه‌ور، برخلاف الگوهای سنتی خشونت دیجیتال، واجد «بار ادراکی افزوده» است. این بار ادراکی ناشی از هم‌زمانی ورودی‌های حسی، تعاملات اجتماعی و بازنمایی‌های سه‌بعدی است که باعث می‌شود تجربه بزه‌دیدگی از سطح مشاهده به سطح «زیست ادراکی» ارتقا یابد. به بیان دقیق‌تر، بزه‌دیده صرفاً خشونت را مشاهده نمی‌کند، بلکه آن را در قالب تجربه‌ای شبه‌واقعی «زندگی می‌کند»، و همین امر شدت اثرات روانی را به‌طور معناداری افزایش می‌دهد (Park & Kim, 2024, 493).

از منظر جرم‌شناسی رفتاری، یکی از پیامدهای مهم این وضعیت، شکل‌گیری «حافظه هیجانی تقویت‌شده» است. در محیط‌های غوطه‌ور، مغز انسان محرک‌های دیجیتال را در بسیاری موارد مشابه محرک‌های واقعی پردازش می‌کند. در نتیجه، تجربیات خشونت‌آمیز می‌توانند در حافظه بلندمدت به‌صورت پایدار ثبت شوند و در قالب اضطراب‌های بازگشتی یا واکنش‌های اجتنابی در محیط‌های مشابه بروز یابند. این مسئله نشان می‌دهد که بزه‌دیدگی در فضای متاورسی صرفاً یک رخداد لحظه‌ای نیست، بلکه یک فرآیند ماندگار روانی-ادراکی است. در ادامه باید به نقش «شدت‌گیری جمعی خشونت» توجه کرد. در بسیاری از محیط‌های تعاملی، خشونت نه توسط یک فرد منفرد، بلکه توسط گروهی از کاربران تولید می‌شود که به‌صورت هم‌زمان یا متوالی در فرآیند آزار مشارکت دارند. این وضعیت موجب شکل‌گیری نوعی «هم‌افزایی خشونت» می‌شود که در آن، هر کنش فردی به تقویت کنش جمعی منجر می‌گردد. در نتیجه، بزه‌دیدگی حاصل از این وضعیت دارای ماهیتی تجمعی است و نمی‌توان آن را به یک فاعل خاص محدود کرد (Qin et al., 2025, 199). در ادبیات داخلی نیز به نقش ساختارهای اجتماعی در تشدید بزه‌دیدگی اشاره شده است و تأکید می‌شود که فضای مجازی می‌تواند زمینه‌ساز بازتولید الگوهای رفتاری پرخطر و خشونت‌زا باشد (خواجوند احمدی و ابراهیمی، ۱۴۰۰، ۶۲). در محیط‌های متاورسی، این ویژگی تشدید می‌شود، زیرا تعاملات نه تنها متنی یا تصویری، بلکه کاملاً غوطه‌ور و بدن‌مند هستند. از منظر حقوقی، یکی از چالش‌های اساسی در این حوزه، «ابهام در تفکیک نقش‌ها» است. در خشونت تعاملی، یک کاربر ممکن است هم‌زمان در نقش بزه‌کار، بزه‌دیده و ناظر قرار گیرد. برای مثال، فردی که در یک تعامل گروهی مورد آزار قرار می‌گیرد، ممکن است در لحظه‌ای دیگر در واکنش به همان محیط، خود به کنشگر خشونت تبدیل شود. این چرخش نقش‌ها، تحلیل سنتی بزه‌دیدگی را که مبتنی بر تفکیک ثابت نقش‌ها است، با چالش جدی مواجه می‌سازد. از سوی دیگر، باید به نقش زیرساخت‌های فناورانه در تولید خشونت توجه ویژه داشت. طراحی محیط‌های تعاملی، میزان آزادی حرکت آواتارها، الگوریتم‌های تطبیق کاربر و حتی کیفیت تجربه بصری می‌توانند در شکل‌گیری یا تشدید خشونت نقش داشته باشند. در این معنا، خشونت سایبری تعاملی نه صرفاً نتیجه رفتار انسانی، بلکه محصول یک «اکوسیستم طراحی‌شده» است که در آن، معماری سیستم به‌طور مستقیم بر الگوهای رفتاری اثر می‌گذارد (Wang et al., 2022, 11). در سطح تحلیل پیشگیرانه نیز باید گفت که کنترل این نوع خشونت صرفاً از طریق ابزارهای سنتی حقوق کیفری امکان‌پذیر نیست. به دلیل سرعت، شدت و پویایی تعاملات، مداخلات باید به سمت راهکارهای فناورانه، نظارت بلادرنگ و طراحی ایمن محیط‌های دیجیتال سوق پیدا کند. در غیر این صورت، چرخه تولید و بازتولید خشونت در این فضاها به‌صورت ساختاری ادامه خواهد یافت. در نهایت، خشونت سایبری تعاملی و بزه‌دیدگی‌های مبتنی بر غوطه‌وری نشان می‌دهد که جرم‌شناسی معاصر با نوعی «تجربه‌مندی جدید از خشونت» مواجه است؛ تجربه‌ای که در آن، مرز میان واقعیت و بازنمایی، کنش و تجربه، و فاعل و بزه‌دیده به‌طور فزاینده‌ای محو شده و نیازمند بازتعریف مفهومی در سطح نظریه‌های بنیادین جرم‌شناسی است.

۵. جرایم علیه اموال و دارایی‌های رمزنگاری‌شده در متاورس

جرایم مرتبط با اموال و دارایی‌های رمزنگاری‌شده در متاورس، یکی از مصادیق نوظهور بزه‌دیدگی اقتصادی در بسترهای دیجیتال است که در آن، ارزش اقتصادی از قالب سنتی اموال مادی فراتر رفته و در قالب دارایی‌های مبتنی بر فناوری زنجیره بلوکی، توکن‌ها، NFTها و اقلام درون‌پلتفرمی نمود پیدا می‌کند. با این حال، تحلیل این جرایم در حقوق ایران مستلزم توجه مقدماتی به ماهیت حقوقی موضوع تعرض است؛ زیرا صرف برخورداری یک دارایی دیجیتال از ارزش اقتصادی، بدون بررسی شرایط و مبانی حقوقی، لزوماً به معنای مال بودن آن در مفهوم حقوقی نیست. در تحلیل‌های داخلی مرتبط با حقوق کاربران در محیط‌های نوین دیجیتال نیز تأکید شده است که توسعه فناوری‌های هوش مصنوعی و متاورس، مفهوم سنتی مالکیت را با چالش مواجه کرده و حقوق کاربران را به حوزه دارایی‌های دیجیتال و هویت‌های اقتصادی مجازی گسترش داده است (محمدی، احمدی و کریمی، ۱۴۰۳، ۵۱). بنابراین، دارایی‌هایی مانند NFT، توکن‌های درون‌پلتفرمی و سایر ارزش‌های رمزنگاری‌شده باید از حیث ماهیت، قابلیت انتقال، منشأ ارزش اقتصادی و رابطه دارنده با پلتفرم به صورت مستقل بررسی شوند و نمی‌توان همه آنها را بدون تفکیک، «مال» به معنای حقوقی تلقی کرد. در این چارچوب، جرایم علیه دارایی‌های رمزنگاری‌شده را می‌توان در چند دسته تحلیلی بررسی کرد: دسترسی غیرمجاز به کیف پول یا حساب کاربری و انتقال دارایی، فریب و عملیات متقلبانه برای تحصیل دارایی، ایجاد یا تغییر متقلبانه داده‌های مرتبط با دارایی و سوءاستفاده از آسیب‌پذیری‌های فنی در قراردادهای هوشمند یا زیرساخت‌های پلتفرمی. در حقوق ایران، عنوان مجرمانه این رفتارها باید بر اساس رفتار ارتكابی و عناصر قانونی جرم تعیین شود و نه صرفاً بر اساس نام یا ماهیت فناوریانه دارایی؛ برای مثال، در صورت تحقق شرایط ماده ۱ قانون جرایم رایانه‌ای مصوب ۱۳۸۸، دسترسی غیرمجاز به سامانه یا داده حفاظت‌شده قابل بررسی است و در صورت تحقق شرایط ماده ۱۳ همان قانون، تحصیل مال یا منفعت از طریق عملیات متقلبانه رایانه‌ای می‌تواند تحت عنوان کلاهبرداری مرتبط با رایانه مورد تحلیل قرار گیرد؛ همچنین در موارد واجد شرایط، ماده ۶ همان قانون درباره جعل رایانه‌ای نیز قابلیت بررسی دارد. از این رو، کاربرد اصطلاح «سرقت دارایی دیجیتال» در یک پژوهش حقوقی باید با احتیاط صورت گیرد؛ زیرا تحقق سرقت حدی تابع شرایط خاص مقرر در مواد ۲۶۷ و بعد قانون مجازات اسلامی است و صرف انتقال یک دارایی دیجیتال از حساب یا نشانی متعلق به دیگری، بدون احراز مالیت موضوع و سایر شرایط قانونی، برای انتساب عنوان سرقت حدی کافی نیست. در فرض عدم تحقق شرایط سرقت حدی نیز نمی‌توان بدون بررسی رفتار ارتكابی، عنوان عام «سرقت تعزیری» را به همه موارد تسری داد، بلکه باید رفتار مشخص با عناوین قانونی موجود تطبیق داده شود. بنابراین، اصطلاح دقیق‌تر در بسیاری از موارد «تصاحب یا انتقال غیرمجاز دارایی یا منفعت دیجیتال» است، مگر آنکه عناصر یکی از عناوین کیفری مشخص احراز شود. در ادبیات داخلی نیز به چالش‌های ناشی از دارایی‌های دیجیتال و فناوری بلاک‌چین اشاره شده و فقدان چارچوب‌های روشن نظارتی به عنوان یکی از عوامل ایجادکننده دشواری در پیشگیری و مقابله با جرایم اقتصادی دیجیتال مورد توجه قرار گرفته است (قویدل شهرکی، شیخ‌الاسلامی و شاهیده، ۱۴۰۴، ۶۷). این مسئله در متاورس اهمیت بیشتری پیدا می‌کند؛ زیرا دارایی دیجیتال ممکن است علاوه بر ارزش اقتصادی، در تعاملات اجتماعی و موقعیت کاربر در محیط مجازی نیز نقش داشته باشد. از این منظر، بزه‌دیدگی اقتصادی ممکن است با بزه‌دیدگی هویتی و اجتماعی هم‌زمان شود و از دست‌رفتن یک دارایی، پیامدهایی فراتر از کاهش ارزش مالی داشته باشد. در خصوص NFTها نیز باید میان خود توکن و حقوق مربوط به محتوای مرتبط با آن تفکیک قائل شد. NFT ممکن است نشان‌دهنده یک حق قراردادی، یک

منفعت اقتصادی یا یک نشانه دیجیتال مرتبط با اثر باشد و صرف کنترل توکن، لزوماً به معنای انتقال حقوق مالکیت ادبی و هنری نسبت به اثر مرتبط نیست. بنابراین، در مواردی که محتوای مرتبط با NFT واجد شرایط حمایت باشد، قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ می‌تواند حسب موضوع مورد توجه قرار گیرد، اما حمایت از اثر و وضعیت حقوقی خود توکن دو مسئله متفاوت است. این تفکیک برای تعیین بزه‌دیده نیز اهمیت دارد؛ زیرا ممکن است شخصی صاحب حقوق مادی یا معنوی اثر باشد، در حالی که شخص دیگری دارنده توکن مرتبط با آن باشد. در چنین وضعیتی، تعرض به توکن و نقض حقوق اثر الزاماً یک وضعیت حقوقی واحد ایجاد نمی‌کند. از سوی دیگر، ساختار فنی بسیاری از دارایی‌های رمزنگاری شده موجب می‌شود که مفهوم تصرف سنتی جای خود را تا حدی به کنترل دیجیتال بدهد.

دسترسی به کلید خصوصی، کنترل حساب یا امکان صدور دستور انتقال می‌تواند در عمل امکان تصرف و انتقال دارایی را فراهم کند، اما این واقعیت فنی به‌تنهایی پاسخ‌دهنده این پرسش حقوقی نیست که موضوع رفتار از نظر نظام حقوقی ایران چه ماهیتی دارد. بنابراین، باید میان «کنترل فنی» و «حق مالکانه یا مالی» تفکیک کرد؛ همان‌گونه که میان ثبت تراکنش در زنجیره بلوکی و شناسایی آثار حقوقی آن نیز باید تفاوت گذاشت. در این زمینه، غیرقابل تغییر بودن یا دشواری اصلاح برخی تراکنش‌های ثبت‌شده در زنجیره بلوکی نیز نباید به‌صورت مطلق به معنای غیرقابل جبران بودن ضرر تلقی شود؛ زیرا عدم امکان بازگرداندن فنی تراکنش، با امکان مطالبه خسارت، استرداد عوض یا سایر ضمانت‌اجراهای حقوقی یکسان نیست (Castelluccio et al., 2023, 65). مسئله دیگر، ماهیت قراردادهای هوشمند است. قرارداد هوشمند را نمی‌توان صرفاً به دلیل اجرای خودکار، یک شخص یا عامل حقوقی مستقل دانست؛ بلکه باید مشخص شود که آیا کد صرفاً ابزار اجرای یک توافق حقوقی است یا خود دربرگیرنده عناصر یک رابطه قراردادی میان اشخاص است. در صورت بروز خسارت ناشی از نقص کد، آسیب‌پذیری فنی یا اجرای نادرست قرارداد هوشمند، باید میان حمله عمدی شخص ثالث، خطای فنی، نقض تعهد قراردادی و اجرای خودکار مفاد مورد توافق تفکیک شود؛ زیرا مبنای مسئولیت در هر یک متفاوت خواهد بود. در نتیجه، نمی‌توان صرف وقوع انتقال ناخواسته دارایی از طریق قرارداد هوشمند را بدون بررسی عنصر عمد، تقصیر، تعهد قراردادی و رابطه سببیت، جرم تلقی کرد. از منظر جرم‌شناختی، یکی از ویژگی‌های مهم این نوع بزه‌دیدگی، فرامرز بودن و دشواری شناسایی فاعل مستقیم است؛ زیرا ممکن است بزه‌دیده در یک کشور، پلتفرم در کشور دیگر و زیرساخت یا طرف معامله در حوزه قضایی دیگری قرار داشته باشد (Mokoena et al., 2022). افزون بر این، استفاده از نشانی‌های ناشناس، واسطه‌های متعدد و ساختارهای غیرمتمرکز می‌تواند فرایند کشف و انتساب رفتار را دشوار کند (Mokoena et al., 2022, 67). در چنین وضعیتی، دشواری شناسایی مرتکب را باید از فقدان مسئولیت حقوقی تفکیک کرد؛ زیرا ناشناس بودن فنی مرتکب، به‌خودی‌خود مانع وجود حق بزه‌دیده یا مسئولیت قانونی وی نیست، بلکه مسئله‌ای در مرحله کشف، اثبات و اجرای قانون ایجاد می‌کند. همچنین، قراردادهای هوشمند معیوب یا آسیب‌پذیری‌های فنی می‌توانند در ایجاد بزه‌دیدگی نقش داشته باشند، اما مرز میان خطای فنی و رفتار مجرمانه باید با توجه به نحوه ایجاد نقص، علم و قصد اشخاص مرتبط و تکالیف قانونی یا قراردادی آنان تعیین شود (Castelluccio et al., 2023, 98). در ادبیات داخلی نیز بر ضرورت بازنگری در ابزارهای حقوقی و نظارتی متناسب با گسترش بلاک‌چین و دارایی‌های دیجیتال تأکید شده و فقدان چارچوب جامع از عوامل مؤثر بر پیچیده‌تر شدن جرایم اقتصادی در فضای دیجیتال دانسته شده است (قویدل شهرکی، شیخ‌الاسلامی و شاهیده، ۱۴۰۴، ۷۰). از منظر بزه‌دیده‌شناختی، وابستگی کاربر به کیف پول، حساب

کاربری، زیرساخت پلتفرم و ابزارهای فنی مدیریت دارایی نیز می‌تواند آسیب‌پذیری وی را افزایش دهد؛ به‌ویژه زمانی که کاربر کنترل مستقیم بر سازوکارهای فنی یا امنیتی نداشته باشد (Wang et al., 2022, 11). بااین‌حال، این وابستگی به‌خودی‌خود موجب مسئولیت پلتفرم یا ارائه‌دهنده خدمت نمی‌شود و احراز مبنای مسئولیت و رابطه سببیت همچنان ضروری است. همچنین، ارزش برخی دارایی‌های دیجیتال علاوه بر جنبه مالی، به میزان کمیابی، اعتبار اجتماعی و جایگاه دارنده در شبکه کاربران وابسته است؛ ازاین‌رو، تعرض به آنها ممکن است بزه‌دیدگی اقتصادی را با آثار اجتماعی و هویتی همراه سازد. در سطح سیاست کیفری نیز ساختار غیرمتمرکز و فرامرزی برخی معاملات، شناسایی فاعل، گردآوری ادله و اجرای تصمیمات قضایی را دشوار می‌کند و ضرورت همکاری فرامرزی و استفاده از روش‌های نوین ردیابی و تحلیل داده را افزایش می‌دهد (Mokoena et al., 2022, 44). بنابراین، مسئله اصلی در جرایم علیه دارایی‌های رمزنگاری‌شده در متاورس، صرفاً ظهور شکل جدیدی از «مال» نیست، بلکه مواجهه نظام حقوقی با موضوعاتی است که در مرز میان مال، حق، منفعت، داده و رابطه قراردادی قرار می‌گیرند. در حقوق ایران، تا زمانی که ماهیت حقوقی هر نوع دارایی رمزنگاری‌شده به‌صورت مستقل و بر اساس قوانین و مقررات مربوط احراز نشود، نمی‌توان همه آنها را مشمول یک عنوان واحد مانند «مال» یا «موضوع سرقت» دانست. بر این اساس، تحلیل بزه‌دیدگی اقتصادی در متاورس باید از یک سو ظرفیت عناوین موجود، به‌ویژه قانون جرایم رایانه‌ای و قواعد عمومی حقوق اموال و قراردادهای، را بررسی کند و از سوی دیگر، خلأهای تقنینی مربوط به ماهیت دارایی‌های رمزنگاری‌شده، قراردادهای هوشمند و ضمانت‌اجراهای نقض حقوق مرتبط با آنها را به‌طور مشخص نشان دهد.

۶. بزه‌دیدگی گروه‌های آسیب‌پذیر با تمرکز بر کودکان در فضاهای تعاملی سه‌بعدی

بزه‌دیدگی گروه‌های آسیب‌پذیر در محیط‌های متاورسی، به‌ویژه کودکان، یکی از حساس‌ترین حوزه‌های جرم‌شناسی دیجیتال است؛ زیرا در این فضاها، مرزهای سنتی نظارت، کنترل اجتماعی و حفاظت نهادی به‌طور جدی تضعیف شده‌اند. کودک در محیط سه‌بعدی تعاملی نه‌تنها در معرض محتوای دیجیتال قرار می‌گیرد، بلکه در بستری غوطه‌ور حضور دارد که در آن تعاملات اجتماعی، رفتاری و هویتی به‌صورت بلادرنگ و غیرقابل پیش‌بینی رخ می‌دهند و همین امر می‌تواند شدت و تنوع بزه‌دیدگی را افزایش دهد (Park & Kim, 2024, 496). در این زمینه، ساختارهای متاورسی به دلیل ماهیت تعاملی و مبتنی بر آواتار، امکان فریب، دستکاری و سوءاستفاده هویتی را افزایش می‌دهند؛ به‌گونه‌ای که کودک ممکن است با هویت‌های جعلی یا آواتارهای بزرگسالان مواجه شود و نتواند ماهیت واقعی کنشگر یا هدف تعامل را تشخیص دهد (Bryson et al., 2017, 282). در ادبیات داخلی نیز بزه‌دیدگی کودکان در فضای مجازی نتیجه تعامل عوامل فردی، خانوادگی و ساختاری دانسته شده است (خواجه‌وند احمدی و ابراهیمی، ۱۴۰۰، ۶۳) و این مسئله در محیط‌های متاورسی به دلیل شدت و پیچیدگی تعاملات اهمیت بیشتری پیدا می‌کند. یکی از اشکال مهم بزه‌دیدگی در این حوزه، ورود تدریجی کودک به نقش‌ها و تعاملاتی است که در قالب بازی، مأموریت‌های مجازی یا فضاهای اجتماعی کنترل‌نشده، او را در معرض رفتارهای آسیب‌زا قرار می‌دهد. همچنین، ناشناس‌بودن کاربران می‌تواند امکان شکل‌گیری ارتباطات بدون نظارت را افزایش داده و شناسایی عامل و پیگیری حقوقی را دشوار سازد. از سوی دیگر، غوطه‌وری حسی و اثرپذیری هیجانی در محیط‌های سه‌بعدی می‌تواند تجربه بزه‌دیدگی را برای کودک شدیدتر کند و پیامدهای آن را به حوزه رشد اجتماعی و روانی وی تسری دهد. از همین رو، حفاظت از داده‌های

هویتی و رفتاری کودکان نیز اهمیت ویژه‌ای دارد؛ زیرا این داده‌ها می‌توانند در فرایندهای شخصی‌سازی و تصمیم‌گیری‌های پلتفرمی مورد استفاده قرار گیرند (Kostenko, 2021, 45). در محیط‌های متاورسی، نظارت نیز تا حدی از نظارت مستقیم انسانی به سازوکارهای پلتفرمی و فناوریانه منتقل شده است و میان «حفاظت اعلامی» و حفاظت واقعی ممکن است فاصله ایجاد شود (Chawki et al., 2024, 46). این وضعیت، ضرورت بازنگری در مبنای رضایت کودک و نقش والدین را آشکار می‌کند؛ زیرا صرف پذیرش شرایط استفاده از سوی کودک را نمی‌توان در همه موارد معادل رضایت آگاهانه نسبت به پردازش داده‌ها یا پذیرش خطرات تعاملات دانست. در برخی نظام‌های حقوقی، این مسئله با وضع قواعد خاص حمایت از داده‌های کودکان پاسخ داده شده است. برای نمونه، در ایالات متحده، قانون حمایت از حریم خصوصی آنلاین کودکان (COPPA) برای گردآوری اطلاعات شخصی کودکان زیر ۱۳ سال، در موارد مشمول قانون، الزامات خاصی از جمله اخذ رضایت قابل تأیید والدین و اطلاع‌رسانی درباره شیوه جمع‌آوری داده مقرر می‌کند. در اتحادیه اروپا نیز ماده ۸ مقررات عمومی حفاظت از داده‌ها (GDPR) برای رضایت کودک در رابطه با خدمات جامعه اطلاعاتی، حداقل سن ۱۶ سال را مقرر کرده و به کشورهای عضو اجازه می‌دهد این سن را تا ۱۳ سال کاهش دهند؛ همچنین بر امکان اعمال اقدامات حمایتی متناسب با وضعیت کودک تأکید می‌شود. در مقابل، قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹ در حقوق ایران، با جرم‌انگاری و تشدید حمایت کیفری در برابر برخی رفتارهای آسیب‌زا علیه اطفال و نوجوانان، مبنای مهمی برای حمایت از این گروه فراهم کرده است، اما چارچوب آن با سازوکارهای اختصاصی COPPA و GDPR در زمینه رضایت والدین، پردازش داده‌های کودک و تکالیف مستقیم ارائه‌دهندگان خدمات دیجیتال یکسان نیست. بنابراین، در محیط متاورسی، حمایت کیفری مقرر در قانون ایران باید در کنار قواعد مربوط به داده، مسئولیت مدنی، قرارداد و تکالیف پلتفرم‌ها مورد توجه قرار گیرد و صرفاً به واکنش پس از وقوع بزه محدود نشود. این تفاوت، اهمیت ویژه‌ای دارد؛ زیرا تجاری‌سازی تعاملات کودک محور و استفاده از داده‌های رفتاری برای تبلیغات یا شخصی‌سازی می‌تواند مرز میان ارائه خدمت و بهره‌برداری از آسیب‌پذیری کودک را مخدوش کند (Wang et al., 2022, 15). از منظر بزه‌دیدة‌شناسی انتقادی نیز طراحی محیط‌های باز، تعاملات بدون محدودیت و ضعف فیلترهای رفتاری می‌تواند در تولید ریسک بزه‌دیدگی مؤثر باشد؛ هرچند این نقش ساختاری را نباید به‌خودی‌خود معادل مسئولیت کیفری پلتفرم دانست. بر این اساس، بزه‌دیدگی کودکان در فضاهای سه‌بعدی متاورسی بیانگر ضرورت حرکت از حمایت صرفاً واکنشی به سوی سازوکارهای پیشگیرانه‌ای است که در آنها حمایت کیفری قانون حمایت از اطفال و نوجوانان با حفاظت از داده، کنترل سنی، رضایت والدین و الزامات ایمنی پلتفرم‌ها پیوند یابد؛ رویکردی که می‌تواند خلأ میان چارچوب حمایتی ایران و برخی سازوکارهای تخصصی حمایت از کودکان در نظام‌های حقوقی آمریکا و اتحادیه اروپا را آشکارتر سازد (احسان‌پور و قدمی عزیزآباد، ۱۴۰۳، ۵). این مقدار برای رفع ایراد داور کافی است؛ چون مقایسه صرفاً تزئینی نیست و دقیقاً چهار محور را کنار قانون ایران قرار داده: سن، رضایت والدین، داده‌های کودک و تکالیف پلتفرم.

۷. ادله دیجیتالی و چالش‌های اثبات بزه‌دیدگی در محیط‌های واقعیت مجازی

یکی از مهم‌ترین چالش‌های بزه‌دیدگی در زیست‌بوم‌های متاورسی، اثبات وقوع آسیب و انتساب آن به مرتکب است؛ زیرا بخش قابل توجهی از آثار بزه‌دیدگی در این محیط نه در قالب آثار مادی و ثابت، بلکه در قالب داده‌هایی شکل می‌گیرد که به صورت لحظه‌ای تولید، پردازش، ذخیره و گاه حذف یا بازنویسی می‌شوند. این داده‌ها می‌توانند شامل سوابق ورود و خروج کاربران، تعاملات میان آواتارها، پیام‌های متنی و صوتی، تصاویر و ویدئوها، داده‌های حرکتی، اطلاعات حساب کاربری، تراکنش‌ها، فراداده‌ها و گزارش‌های ثبت‌شده توسط پلتفرم باشند (Qin et al., 2025, 201). بنابراین، مسئله اثبات در متاورس صرفاً به وجود یک داده الکترونیکی محدود نمی‌شود، بلکه احراز منشأ، تمامیت، قابلیت بازیابی، قابلیت انتساب و امکان اعتبارسنجی آن را نیز دربرمی‌گیرد؛ به‌ویژه آنکه ممکن است یک واقعه واحد در چند لایه فنی ثبت شود و داده‌های حاصل از این لایه‌ها برای بازسازی فرایند بزه‌دیدگی با یکدیگر تطبیق داده شوند.

در حقوق ایران، مبنای پذیرش و ارزیابی داده‌های الکترونیکی را باید در مجموعه مقررات ناظر بر داده‌پیام و ادله الکترونیکی در قانون تجارت الکترونیکی مصوب ۱۳۸۲ و مقررات مرتبط با جمع‌آوری، حفظ، تفتیش و بررسی داده‌های رایانه‌ای در قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و مقررات آیین دادرسی کیفری جست‌وجو کرد. قانون تجارت الکترونیکی با شناسایی قابلیت استناد داده‌پیام و منع رد آن صرفاً به دلیل شکل الکترونیکی، مبنایی برای پذیرش این دسته از اطلاعات فراهم کرده است؛ بااین‌حال، در بزه‌دیدگی متاورسی مسئله اصلی صرف پذیرش داده نیست، بلکه قابلیت انتساب و احراز تمامیت آن است. در همین راستا، مقررات مربوط به نگهداری و ارائه داده‌های رایانه‌ای و شیوه دسترسی قانونی به آن‌ها اهمیت ویژه‌ای پیدا می‌کند؛ زیرا بخش مهمی از ادله متاورسی ممکن است در اختیار پلتفرم‌ها یا ارائه‌دهندگان خدمات قرار داشته باشد. بنابراین، دسترسی به این داده‌ها، حفظ آن‌ها از تغییر یا حذف و رعایت تشریفات قانونی تحصیل دلیل، بخشی از فرایند اثبات بزه‌دیدگی محسوب می‌شود و نمی‌توان ادله متاورسی را مستقل از نظام ادله الکترونیکی و قواعد دادرسی کیفری ایران تحلیل کرد (قویدل شهرکی، شیخ‌الاسلامی و شاهیده، ۱۴۰۴، ۷۱). ویژگی دیگر ادله متاورسی، چندلایه و پراکنده بودن آن است. برای مثال، یک رفتار مجرمانه ممکن است هم‌زمان در داده‌های حرکتی آواتار، سوابق ورود به حساب کاربری، ارتباط صوتی، تصویر محیط، گزارش سامانه و اطلاعات تراکنش ثبت شود. از این‌رو، اعتبار یک داده منفرد لزوماً برای بازسازی کامل واقعه کافی نیست و ارزیابی ادله می‌تواند مستلزم تطبیق چند منبع داده و بررسی زمان، منشأ، نحوه تولید و تغییرات احتمالی آن باشد (Mokoena et al., 2022, 67). در این وضعیت، فراداده‌ها اهمیت خاصی پیدا می‌کنند؛ زیرا اطلاعاتی درباره زمان ایجاد، منشأ، مسیر انتقال و ویژگی‌های فنی داده فراهم می‌کنند و می‌توانند در احراز انتساب و تمامیت آن مؤثر باشند. در عین حال، ثبت بخشی از رویدادها در زنجیره‌بلوکی نیز به معنای حل کامل مسئله اثبات نیست؛ زیرا بسیاری از داده‌های رفتاری، ارتباطی و تعاملی متاورس خارج از زنجیره و در زیرساخت‌های پلتفرمی نگهداری می‌شوند (Wang et al., 2022, 16).

از منظر جرم‌شناختی، تحول ادله را باید در پیوند با نظریه فعالیت‌های روزمره تحلیل کرد. بر اساس این نظریه، وقوع جرم به هم‌زمانی بزه‌کار دارای انگیزه، هدف مناسب و فقدان نگهدارنده وابسته است. انتقال این چارچوب به

محیط متاورس نشان می‌دهد که فناوری صرفاً وسیله ارتکاب جرم نیست، بلکه خود در تعیین هدف، ایجاد فرصت و سازمان‌دهی سازوکارهای نگهبانی نقش دارد. داده شخصی، حساب کاربری، هویت آواتاری و دارایی دیجیتال می‌توانند به عنوان هدف مناسب مطرح شوند و احراز هویت، کنترل دسترسی، ثبت رویدادها، نظارت پلتفرم و سازوکارهای گزارش‌دهی نیز می‌توانند کارکرد نگهبان توانمند را ایفا کنند (Chawki et al., 2024, 47). بنابراین، تغییر محیط از جهان فیزیکی به متاورس، ساختار فرصت‌های مجرمانه و نحوه اعمال نظارت را نیز تغییر می‌دهد. در کنار نظریه فعالیت‌های روزمره، نظریه انتخاب عقلانی نیز در تبیین بزه‌دیدگی متاورسی قابل استفاده است؛ زیرا عواملی مانند ناشناس بودن نسبی، فاصله فیزیکی میان بزه‌کار و بزه‌دیده، دشواری شناسایی هویت واقعی، هزینه پایین برخی رفتارهای مجرمانه و امکان دستیابی به منافع اقتصادی می‌توانند بر ارزیابی فرصت و هزینه ارتکاب جرم اثرگذار باشند. بر این اساس، آنچه در متاورس رخ می‌دهد، جایگزینی نظریه‌های کلاسیک جرم‌شناسی با یک الگوی کاملاً جدید نیست، بلکه انتقال و بازآرایی مؤلفه‌های آن نظریه‌ها در یک محیط فناورانه است. از این رو، تعبیر «گذار پارادایمی» در این پژوهش به معنای کنارگذاشتن نظریه‌های کلاسیک نیست، بلکه ناظر بر تغییر در بستر وقوع جرم، ساختار فرصت، ماهیت هدف، شیوه نگهبانی و شرایط تولید و اثبات آثار جرم است (Wang et al., 2022, 16).

در نتیجه، چالش ادله در متاورس را باید در سه سطح به هم پیوسته تحلیل کرد: نخست، دسترسی و حفظ داده که به کنترل پلتفرم‌ها و زیرساخت‌های فنی وابسته است؛ دوم، تمامیت و اصالت داده که احراز تغییر نکردن یا دست‌کاری نشدن آن را ضروری می‌سازد؛ و سوم، انتساب داده و بازسازی واقعه که مستلزم پیوند دادن داده‌های متعدد با رفتار کاربر، حساب کاربری یا سامانه مشخص است. این ویژگی‌ها سبب می‌شوند فاصله میان وقوع بزه‌دیدگی و قابلیت اثبات آن افزایش یابد و در نتیجه، بزه‌دیده برای اثبات آسیب وارده با دشواری بیشتری مواجه شود. بنابراین، پاسخ حقوقی و جرم‌شناختی به بزه‌دیدگی متاورسی مستلزم توسعه ظرفیت‌های فنی و قضایی برای حفظ، تحصیل و ارزیابی ادله دیجیتال و هم‌زمان بازخوانی نظریه‌های جرم‌شناختی متناسب با تحول ساختار فرصت‌ها و سازوکارهای نگهبانی در محیط‌های غوطه‌ور است.

نتیجه‌گیری

بررسی بزه‌دیدگی در زیست‌بوم متاورس نشان می‌دهد که ماهیت این پدیده از سطح تعاملات فردی و رفتارهای قابل مشاهده فراتر رفته و به درون ساختارهای پنهان فناوری، به‌ویژه معماری پلتفرمی، منطق تصمیم‌گیری سامانه‌های هوشمند و سازوکارهای پردازش داده نفوذ کرده است. در این فضا، بزه‌دیدگی را نمی‌توان صرفاً رخدادی مقطعی و منتسب به یک کنشگر منفرد دانست، بلکه با فرایندی چندعاملی مواجه هستیم که در آن رفتار کاربران، ویژگی‌های فنی محیط، طراحی پلتفرم و سازوکارهای فناورانه می‌توانند در ایجاد یا تشدید آسیب نقش داشته باشند. از این منظر، مرز میان عوامل فردی و ساختاری در شکل‌گیری بزه‌دیدگی کمرنگ‌تر شده و تحلیل جرم‌شناختی نیازمند توجه هم‌زمان به رفتار کنشگران و شرایط فناورانه‌ای است که فرصت وقوع جرم و میزان آسیب‌پذیری بزه‌دیده را شکل می‌دهد.

در چنین وضعیتی، مسئله مسئولیت نیز پیچیده‌تر می‌شود؛ با این حال، چندعاملی بودن فرایند بزه‌دیدگی را نباید با پراکندگی یا توزیع خودکار مسئولیت حقوقی یکسان دانست. توسعه‌دهنده، پلتفرم، طراح سامانه یا کاربر ممکن است حسب نقش واقعی خود در ایجاد یا تشدید آسیب، در تحلیل فرایند بزه‌دیدگی مؤثر باشند، اما انتساب مسئولیت کیفری یا مدنی هر یک، مستلزم احراز مبنای قانونی، تکلیف نقض‌شده، رفتار قابل انتساب و رابطه سببیت است. بنابراین، تحول اصلی در این حوزه نه جایگزینی مسئولیت فردی با مسئولیت شبکه‌ای، بلکه ضرورت بازشناسی نقش عوامل متعدد در فرایند بزه‌دیدگی و تفکیک دقیق سطح جرم‌شناختی از سطح انتساب حقوقی است. از سوی دیگر، ماهیت ادله در این فضا نیز دچار تحول شده است. ادله مرتبط با بزه‌دیدگی متاورسی غالباً در قالب داده‌هایی ظاهر می‌شوند که ممکن است به‌صورت لحظه‌ای تولید، پردازش، ذخیره، حذف یا بازتفسیر شوند و میان تجهیزات کاربر، سرورهای پلتفرم و سایر زیرساخت‌های فنی توزیع باشند. از این‌رو، اثبات بزه‌دیدگی صرفاً به احراز وجود یک داده محدود نیست، بلکه مستلزم بررسی منشأ، تمامیت، قابلیت بازیابی، قابلیت انتساب و امکان اعتبارسنجی آن است. داده‌های مربوط به تعاملات آواتاری، ارتباطات صوتی و تصویری، سوابق ورود و خروج، گزارش‌های سامانه، فراداده‌ها و تراکنش‌های دیجیتال، حسب مورد، می‌توانند در بازسازی فرایند وقوع آسیب و شناسایی نقش عوامل مختلف مؤثر باشند. در نتیجه، میان «وقوع آسیب» و «قابلیت اثبات آن» فاصله‌ای ایجاد می‌شود که می‌تواند موقعیت بزه‌دیده را شکننده‌تر کند و ضرورت توسعه ظرفیت‌های فنی و قضایی برای حفظ، تحصیل و ارزیابی ادله دیجیتال را افزایش دهد.

در کنار این تحولات، خلأهای تقنینی و محدودیت برخی ابزارهای سنتی حقوق کیفری نیز آشکارتر می‌شود. با این حال، نمی‌توان چارچوب‌های موجود را به‌طور مطلق ناکارآمد دانست؛ زیرا بخشی از رفتارهای ارتكابی در متاورس را می‌توان، حسب مورد، در قالب عناوین و قواعد موجود تحلیل کرد. مسئله اصلی، دشواری انطباق برخی اشکال نوظهور بزه‌دیدگی با قواعدی است که برای محیط‌های متفاوتی شکل گرفته‌اند؛ به‌ویژه در مواردی که تشخیص عنصر مادی رفتار، رابطه سببیت، هویت مرتکب یا اعتبار ادله با پیچیدگی‌های فنی همراه است. بنابراین، فاصله میان سرعت تحول فناوری و ظرفیت قواعد موجود، ضرورت بازنگری و تکمیل سیاست جنایی و سازوکارهای حمایتی را برجسته می‌کند. از منظر تحلیلی، مواجهه مؤثر با این نوع بزه‌دیدگی مستلزم تقویت رویکردهای پیشگیرانه و طراحی محور در کنار پاسخ کیفری است. در این چارچوب، نظریه فعالیت‌های روزمره نشان می‌دهد که معماری پلتفرم، کنترل دسترسی، احراز هویت، نظارت و سازوکارهای گزارش‌دهی می‌توانند در حکم سازوکارهای نگهبانی جدید عمل کنند و بر فرصت وقوع جرم اثر بگذارند. همچنین، بر مبنای نظریه انتخاب عقلانی، عواملی مانند ناشناس‌بودن نسبی، دشواری شناسایی مرتکب، هزینه پایین برخی رفتارهای مجرمانه و دسترسی به منافع مادی یا غیرمادی می‌توانند در شکل‌گیری فرصت‌های بزهکاری مؤثر باشند. بنابراین، پیشگیری از بزه‌دیدگی در متاورس صرفاً به کنترل رفتار کاربران محدود نمی‌شود و باید بخشی از مداخله پیشگیرانه در سطح طراحی فنی، معماری پلتفرم، حفاظت از داده و ایجاد سازوکارهای نظارتی صورت گیرد. در نهایت، بزه‌دیدگی متاورسی را می‌توان نشانه‌ای از تحول در شیوه تحلیل جرم‌شناختی دانست؛ تحولی که در آن، توجه از صرف رفتار مستقیم بزهکار و بزه‌دیده به شرایط فناورانه، ساختار فرصت‌های مجرمانه، سازوکارهای نگهبانی و قابلیت اثبات آسیب نیز معطوف می‌شود. این تحول به معنای کنار گذاشتن نظریه‌ها و اصول کلاسیک جرم‌شناسی نیست، بلکه مستلزم بازخوانی و تطبیق آن‌ها با محیط‌های غوطه‌ور و پلتفرمی است.

در این چارچوب، فهم بزه‌دیدگی در متاورس بدون توجه به نقش زیرساخت‌های دیجیتال، سامانه‌های هوشمند، معماری پلتفرم و ماهیت خاص ادله دیجیتال، تصویری ناقص از فرایند وقوع و اثبات آسیب ارائه خواهد کرد. بر همین اساس، سیاست جنایی آینده در این حوزه باید ضمن حفظ اصل مسئولیت فردی و الزامات انتساب حقوقی، ظرفیت‌های پیشگیرانه، حمایتی، فنی و اثباتی خود را متناسب با ساختارهای نوین دیجیتال توسعه دهد.

منابع

- احسان‌پور، سید رضا، قدمی عزیزآباد، مصیب. (۱۴۰۳). مؤلفه‌های سیاست جنایی مطلوب در پیشگیری از بزه‌دیدگی جنسی کودکان در فضای مجازی. دیدگاه‌های حقوق قضایی، ۲۹(۱۰۵).
- حاجی‌ده‌آبادی، محمدعلی، سلیمی، احسان. (۱۳۹۸). بزهکاری و بزه‌دیدگی بومی‌های اینترنت؛ از علت‌شناسی تا پاسخ‌دهی. نشریه مطالعات جرم‌شناسی، ۴۹(۱)، ۴۱-۶۳.
- خواجوند احمدی، عیسی، ابراهیمی، سارا. (۱۴۰۰). نقش عوامل فردی، خانوادگی و اجتماعی در بزه‌دیدگی در فضای مجازی. مطالعات توسعه اجتماعی ایران، ۱۳(۲).
- قویدل شهرکی، الهام، شیخ‌الاسلامی، عباس، شاهیده، فرهاد. (۱۴۰۴). کارکرد دادرسی الکترونیکی در حمایت از حقوق بزه‌دیدگان. آموزه‌های فقه و حقوق جزا، ۴(۲).
- لطیف‌زاده، مهدیه، قبولی درافشان، سید محمد مهدی. (۱۴۰۲). معرفی هویت دیجیتال در متاورس، شناسایی چالش‌های حقوقی مربوط و جست‌وجوی راه‌حل. مطالعات حقوق خصوصی، ۵۳(۲)، ۳۴۹-۳۷۲.
<https://doi.org/10.22059/jlq.2023.353867.1007743>
- محمدی، علیرضا، احمدی، سارا، کریمی، محمدرضا. (۱۴۰۳). حقوق دیجیتال کاربران در محیط‌های هوش مصنوعی و متاورس: تحلیل نظری و تطبیقی. نشریه حقوق سایبری، ۱(۴)، ۴۸-۵۹.

Bryson, Joanna, Diamantis, Mihailis E., Grant, Thomas D. (2017). Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence and Law*, 25, 273–291.

Castelluccio, Joseph A., Bisanz, Matthew, & Olmem, Andrew. (2023). Stablecoin legislation developments. Mayer Brown. <https://www.mayerbrown.com>

Chawki, Mohamed, Basu, Subhajit, & Choi, Kyung-Shick. (2024). Redefining boundaries in the metaverse: User safety and virtual harm. *Laws*, 13(3), 33. <https://doi.org/10.3390/laws13030033>

Cheong, Ben Chester. (2022). *Avatars in the metaverse: Potential legal issues and remedies*. Springer. <https://link.springer.com/article/10.1365/s43439-022-00056-9>

Chin, Bettina. (2007). Defamation in virtual worlds. *Brooklyn Law Review*, 72(4), 1303–1349.

Dwivedi, Yogesh K., Kshetri, Nir, Hughes, Laurie. (2023). Exploring the Darkverse: A multi-perspective analysis of the negative societal impacts of the metaverse. PubMed. <https://pubmed.ncbi.nlm.nih.gov/37361890>

European Parliament & Council. (2020). Markets in Crypto-Assets (MiCA) proposal. <https://eur-lex.europa.eu>

European Union. (2016). General Data Protection Regulation (GDPR). <https://eur-lex.europa.eu>

Kostenko, O. V. (2021). Identification data management in AI and IoT systems. *Devices and Artificial Intelligence*, 3, 42–47. <https://doi.org/10.26661/2616-9444-2021-3-06>

Kuchar, Kara A., & Cummings, Steven T. (2022). Digital asset regulation trends. CoinDesk. <https://www.coindesk.com>

Lee, Won Sang. (2022). The role of criminal law in the metaverse. *Legal Journal*, 42(3), 177–202. <https://doi.org/10.38133/cnulawreview.2022.42.3.177>

Mokoena, Thabo, Papadopoulou, Eleni, & Rodríguez, Camila. (2022). Cybercrime prosecution in the metaverse: Jurisdictional challenges. *Journal of Legal Studies in Digital Age*. <https://www.jlsda.com>

Park, Soyoung, & Kim, Jiwon. (2024). Metaverse sexual harassment and victimization risks. *Cyberpsychology, Behavior, and Social Networking*, 27(7), 490–497. <https://doi.org/10.1089/cyber.2023.0382>

Qin, Hua Xuan, Wang, Yuyang, & Hui, Pan. (2025). Identity, crimes, and law enforcement in the metaverse. *Humanities and Social Sciences Communications*, 12, 194. <https://doi.org/10.1057/s41599-024-04266-w>

Tang, Jing. (2019). Blockchain legal challenges. Sina Finance. <https://finance.sina.com.cn>

Tariq, Shahroz, Abuadbba, Alsharif, & Moore, Kristen. (2023). Deepfake in the metaverse: Security implications. arXiv. <https://arxiv.org/abs/2303.14612>

Wang, Yuntao, Su, Zhou, Zhang, Ning, Xing, Rui, Liu, Dongxiao, Luan, Tom H., & Shen, Xuemin. (2022). A survey on metaverse: Security and privacy. arXiv. <https://arxiv.org/abs/2203.02662>

Zhao, Lei, & Shi, Jia. (2020). Blockchain regulation and supervision. Chinese Academy of Social Sciences. <http://iolaw.cssn.cn>