Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

مسئولیت کیفری هوش مصنوعی از دیدگاه حقوق جزا و جرم‌شناسی

فاطمه معبودیان کارشناسی‌ارشد حقوق جزا و جرم‌شناسی دانشگاه آزاد ساری

فصلنامه علمی فقه و حقوق نوین

Print ISSN: ۲۷۱۷- ۱٤٦۹
Online ISSN: ۲۷۱۷ – ۱٤۷۷

ISC.SID.NOORMAGZ.MAGIRAN
GOOGLESCHOLAR.ENSANI
www.jaml .ir

سال ۱۴۰۴، سال ششم، شماره ۲۳،
صفحات ۲۰-۱

چکیده

فناوری‌های نوین، شرایطی را برای نوسازی اشکال مختلف روابط اجتماعی با استفاده از فناوری‌های واقعیت مجازی و متاورس ایجاد نموده است که تنظیم روابط حقوقی را فراتر از قواعد سنتی، ایجاب می‌کند و توسعه و به‌روزرسانی قوانین در حوزه مسئولیت‌های قانونی متاورس ضروری است. متاورس به عنوان جامعه الکترونیکی آینده، هنوز مرزهای قانونی مشخصی ندارد و وظیفه حقوق‌دانان تعیین اختیارات قانونی برای محیط‌های واقعیت مجازی می‌باشد. جامعه بایستی در خصوص امکان‌سنجی و ضرورت تنظیم مقررات متاورس به این پرسش‌ها پاسخ دهد که در متاورس چه جرایمی قابل ارتکاب است و جرم‌شناسی در این حوزه چه ملاحظاتی را در بر می‌گیرد و چگونه می‌توان با جرایم ارتکابی در فضای واقعیت مجازی برخورد کرد؟ در این پژوهش به پاسخ این پرسش‌ها پرداخته می‌شود. رویکرد پژوهش توصیفی - تحلیلی می‌باشد و گردآوری مطالب به شیوه کتابخانه‌ای صورت می‌گیرد.

واژگان کلیدی: واقعیت مجازی، متاورس، جرم‌شناسی، حقوق کیفری.

طبقه‌بندی JEL: فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Criminal liability of artificial intelligence from the perspective of criminal law and criminology

Scientific Journal of Modern Jurisprudence and Law

Print ISSN: ۲۷۱۷- ۱٤٦۹
Online ISSN: ۲۷۱۷ - ۱٤۷۷

Profile in ISC,SID, Noormags, Magiran, Ensani, GoogleScholar
www.jaml .ir

Year ۲۰۲۵و Sixth year ,Issue ۲۳

Pages ۱-۲۰

fatemeh mobudian Master's degree in Criminal Law and Criminology, Sari Azad University

Abstract

New technologies have created conditions for the modernization of various forms of social relations using virtual reality and metaverse technologies, which require the regulation of legal relations beyond traditional rules, and the development and updating of laws in the field of legal responsibilities of the metaverse is essential. The metaverse, as the electronic society of the future, does not yet have clear legal boundaries, and it is the duty of lawyers to determine legal powers for virtual reality environments. Society must answer these questions regarding the feasibility and necessity of regulating the metaverse: what crimes can be committed in the metaverse, what considerations does criminology include in this area, and how can crimes committed in the virtual reality space be dealt with? This research will answer these questions. The research approach is descriptive-analytical, and the collection of materials is done in a library manner.

Keywords: Virtual reality, metaverse, criminology, criminal law.

JEL Classification: **Jurisprudence - Law - Criminal and Criminology - International Law - Private Law**

مقدمه

دنیای واقعیت مجازی دیگر تخیلی نیست و دنیای بدون مرزهای فیزیکی به واقعیت تبدیل شده است و افراد می‌توانند با استفاده از جهان واقعیت مجازی، بازی کنند، کار کنند و در فعالیت‌های دیگر شرکت کنند و رؤیاهای خود را به اشتراک بگذارند. این فناوری تجربه‌ای فراگیر داشته و حتی با فناوری‌های جدیدتر قابلیت‌های لمسی را نیز ایجاد کرده است. در این حوزه ممکن است جرایم مالی؛ مانند سرقت و کلاهبرداری، جرایم علیه اشخاص مانند آزار و اذیت، توهین و جرایم جنسی مانند تجاوز و... رخ دهد. در این جهان‌ها جرایم با آسیب جسمی روبرو نیست، اما به دلیل ارتباط به گیرنده‌های مغزی، آسیب روحی و روانی می‌باشد؛ همچنین احتمال ضررهای مالی نیز وجود دارد، اما در این خصوص جرم‌انگاری دقیقی صورت نگرفته است. [۱]

جرایم در متاورس می‌تواند شامل حملات فیزیکی سایبری علیه زیرساخت‌های حیاتی و همچنین سرقت اموال مجازی/فرهنگی سه‌بعدی، تجاوز به فضاهای مجازی خصوصی و سرقت از آواتارها باشد که عدم استانداردسازی و قابلیت همکاری و ماهیت فرامرزی جهان‌های مجازی که حوزه‌های قضایی متعدد را در بر می‌گیرند، موجب پیچیدگی مضاعف می‌گردد. در واقع، پلیس ممکن است با صحنه‌های جرم مجازی روبرو شود که در آن هیچ مدرک فیزیکی برای جمع‌آوری وجود ندارد و فقط تعاملات دیجیتالی شامل دارایی‌های مجازی مانند ارزهای دیجیتال و توکن‌های غیرقابل‌تعویض وجود دارد؛ بنابراین شواهد می‌توانند به‌راحتی ناپدید شوند یا تغییریافته به نظر برسند. این فضاها فرصت‌هایی را برای افزایش جرایم فراهم می‌کند و چالش‌هایی را برای اجرای قانون ایجاد می‌کند و بایستی اطمینان حاصل شود که مجریان قانون چالش‌های این فضا را درک می‌کنند و آماده پاسخگویی مؤثر می‌باشند. [۲]

در این حوزه صلاحیت رسیدگی الکترونیکی فرامرزی باید ایجاد شود. تنظیم روابط اجتماعی و حقوقی واقعیت مجازی باید با تمرکز بر هدف اصلی، تعریف واضح در خصوص وضعیت حقوقی متاورس، موضوعات و اشیاء الکترونیکی، ایجاد حقوق، وظایف و مسئولیت‌های آنها و برای تعریف انواع مختلف روابط بین موجودیت‌های مجازی، سوژه‌ها و اشیاء در یک متاورس در زمینه‌های فرامرزی صورت گیرد. در این زمینه پیش‌بینی قانون کیفری و جرم‌شناسی این حوزه، ضروری است و هنجارها و جرایم و مجازات‌های قابل‌اعمال بایستی تعیین گردد. تشکیل حوزه قضایی الکترونیکی برای رسیدگی به جرایم متاورس و توسعه یک قانون کیفری در خصوص متاورس یک موضوع چالش‌برانگیز علمی و حقوقی در جهان کنونی است. متاورس فضایی را ایجاد نموده است که انسان‌ها از آواتارها (نماد شخصیت الکترونیکی) استفاده می‌کنند و هویت مجازی ممکن است با هویت واقعی متفاوت باشد؛ بنابراین باید قوانینی تدوین شود که روابط اجتماعی الکترونیکی و مجازی را تنظیم نموده و از رفتارها و هنجارهای مخرب جلوگیری گردد.

۲-چیستی متاورس و آواتارها و تاریخچه آن

متاورس،[1] به همگرایی فضای فیزیکی و مجازی اشاره دارد که از طریق رایانه قابل‌دسترسی است و توسط فناوری‌های فراگیر؛ مانند واقعیت مجازی، واقعیت افزوده و واقعیت ترکیبی فعال می‌شود. این دنیای مجازی سه‌بعدی که توسط طرفداران به عنوان تکرار بعدی اینترنت توصیف می‌شود، به عنوان فضایی پایدار، جمعی و مشترک تصور می‌شود که در آن تصاویر دیجیتالی خودمان، یا آواتارها، آزادانه از تجربه‌ای به تجربه دیگر حرکت می‌کنند و هویت و دارایی‌های پولی ما را با خود می‌برند. آواتارها، نماد سه‌بعدی اشخاص در متاورس می‌باشند که می‌تواند ظاهری متفاوت با آن‌ها داشته باشد که از طریق آن با محیط متاورس ارتباط برقرار می‌کنند. دیدگاه‌های دنیای دیجیتال موازی که در آن انسان‌ها می‌توانند زندگی را به شیوه‌هایی مشابه و غیرممکن در دنیای واقعی تجربه کنند، جدید نیستند و به قبل از اینترنت برمی‌گردند، اما مفهوم واقعیت ترکیبی فیزیکی و دیجیتالی در دهه‌های اخیر با پیشرفت‌های فناوری، از پذیرش تقریباً جهانی تلفن‌های همراه و گسترش اینترنت پرسرعت گرفته تا بازی‌های محبوبی مانند پوکمون گو ملموس‌تر شد. سرمایه‌گذاری سنگین صنعت در فناوری‌های فعال‌کننده فراجهت، رشد بازی‌های ویدئویی آنلاین، پیشرفت‌هایی در هوش مصنوعی و تسریع کار از راه دور و اجتماعی شدن ناشی از همه‌گیری COVID-۱۹ باعث نوآوری بیشتر در فناوری و افزایش پذیرش زندگی آنلاین توسط کاربران شد. در نوامبر ۲۰۲۱، فیس‌بوک نام خود را متا تغییر داد و سرمایه‌گذاری ۱۰ میلیارددلاری برای توسعه تجربیات مجازی را اعلام کرد و علاقه‌مندان را بر آن داشت که متاورس را به عنوان رابط محاسباتی جدید دنیا معرفی کنند. بیل گیتس با پیش‌بینی این که جلسات از صفحه نمایش به متاورس طی دو یا سه سال آینده منتقل می‌شود، وارد این عرصه شد. هر چند هیاهو زودرس بود. در اواخر سال ۲۰۲۲، تقریباً زمانی که ChatGPT توجه جهان را به خود جلب کرد و حباب متاورس ظاهر شد. زیان‌های مالی به دنبال آن، به ویژه زیان عملیاتی ۱۳.۷ میلیارد دلاری متا در بخش آزمایشگاه‌های واقعیت برای سال ۲۰۲۲ به طور کلی رخ داد. مایکروسافت کارمندان بخش‌های مختلف خود را اخراج کرد، زیان‌های مالی موجب کاهش به‌کارگیری این فناوری شد، اما متاورس برای مشاغل مهم است و اجزای آن در حال افزایش است، زیرا گرافیک و قابلیت‌های واقعیت مجازی و واقعیت افزوده، تقویت شده توسط هوش مصنوعی، به‌سرعت بهبود می‌یابد. توسعه فناوری جدیدی مانند ردیابی چشم که از حسگرها برای نظارت و ضبط حرکات چشم استفاده می‌کند، تجارب بصری را جذاب‌تر می‌کند. طبق گزارش‌ها در ژوئن ۲۰۲۳، بازار تجارت متاورس از خانه و غذا گرفته تا تناسب اندام و پوشاک را در تجارت الکترونیک پوشش می‌دهد و پیش بینی می‌گردد که بازار متاورس در سال ۲۰۲۴ به ارزش ۷۴.۴ میلیارد دلار می‌رسد و پیش‌بینی می‌کند که تا سال ۲۰۳۰، با رشد سالانه ۳۸ درصدی، به ۵۰۷.۸ میلیارد دلار با بیش از ۲.۶ میلیارد کاربر خواهد رسید. نویسنده نیل استفنسون در سال ۱۹۹۲ در رمان

[1] metaverse

علمی-تخیلی خود Snow Crash (سقوط برف) کلمه متاورس را ابداع کرد تا محیط مجازی سازی شده‌ای را توصیف کند که در آن افراد تا حدی بر اساس مهارت فنی آواتارهای خود موقعیت کسب می‌کردند. علاوه بر محبوبیت مفهوم آواتارهای دیجیتال، گفته می‌شود که تصویر این رمان از دنیای سه‌بعدی شبکه‌ای بر برنامه‌های وب واقعی از جمله Google Earth و NASA World Wind تأثیر گذاشته است. رمان دیگری که متاورس را محبوب کرد، «یک بازیکن آماده» اثر ارنست کلین بود که در سال ۲۰۱۱ منتشر شد و بعدها توسط استیون اسپیلبرگ به فیلم تبدیل شد. این تصویر آینده‌ای را به تصویر می‌کشد که در آن مردم با ورود به دنیای مجازی که با استفاده از هدست واقعیت مجازی و دستکش‌های لمسی که حس لامسه را ارائه می‌دهند، به آن دسترسی پیدا می‌کنند، از مشکلات دنیای واقعی فرار می‌کنند. چنین بازخورد لمسی همچنین تبدیل به یک مفهوم فراجهانی کلیدی شد. گذشته از داستان‌های تخیلی، فناوری‌های اساسی که از یک متاورس واقعی پشتیبانی می‌کنند، به دهه ۱۹۶۰ برمی‌گردد. میراث متاورس شامل دو موج تبلیغاتی دیگر است که به کلی فراموش شده‌اند، اولین مورد در اوایل دهه ۲۰۰۰ رخ داد، زمانی که استفاده از جامعه مجازی پیشگام Second Life پس از رشد اولیه به ثمر رسید و دومی در سال ۲۰۱۰ زمانی که اولین هدست‌های VR که دروازه‌ای به فراجهان باز نمود. تیم برنرز لی، دانشمند کامپیوتر بریتانیایی، اولین وب سرور، مرورگر و ویرایشگر منبع باز را در اواخر دهه ۱۹۸۰ و اوایل دهه ۱۹۹۰ ایجاد کرد و شبکه جهانی وب را اختراع کرد، شبکه‌ای مرتبط از صفحات وب، گرافیک و سایر رسانه‌ها که اطلاعات را قابل دسترسی و ناوبری می کند. به طور کلی می‌توان متاورس را یک شبکه انبوه مقیاس‌پذیر و قابل تعامل از جهان‌های مجازی سه‌بعدی ارائه‌شده در زمان واقعی تعریف نمود که می‌تواند به طور همزمان و مداوم توسط تعداد بسیار نامحدودی از افراد تجربه شود. متاورس با حس حضور فردی و با تداوم داده‌ها مانند هویت، تاریخچه، حقوق، اشیاء، ارتباطات و پرداخت‌ها عمل می‌کند. لورن لوبتسکی، مدیر ارشد کمپانی بین در یک سخنرانی، متاورس را دامنه‌ای از برنامه‌های کاربردی دانست که فضایی پویا، باز و قابل تعامل دارد و بسیار شبیه به اینترنت اما به صورت سه بعدی است. متاورس یک اکوسیستم دیجیتالی است که بر اساس انواع مختلف فناوری سه بعدی مجازی، نرم افزارهای دیگر و ابزارهای مالی غیرمتمرکز مبتنی بر بلاک چین ساخته شده است. متاورس یک واقعیت فراوجهی و ترکیبی از جهان واقعی و مجازی است. هدست‌ها کاربران را قادر می‌سازد تا با محیط مجازی به گونه‌ای تعامل کنند که واقعیت را آن گونه که از طریق حواس ما درک می شود، درک کنند و می‌توانند شامل دستکش، جلیقه و حتی لباس‌های ردیابی تمام بدن و... باشند که تعامل واقعی‌تری را با محیط مجازی امکان پذیر می کنند. تفاوت بین اینترنت و متاورس این است که اینترنت شبکه‌ای متشکل از میلیاردها کامپیوتر، میلیون‌ها سرور و سایر دستگاه‌های الکترونیکی است. پس از آنلاین شدن، کاربران اینترنت می‌توانند با یکدیگر ارتباط برقرار کنند، وب‌سایت‌ها را مشاهده کرده و با آن‌ها تعامل داشته باشند و کالاها و خدمات را خریداری کرده و بفروشند. لازم به ذکر است، متاورس با اینترنت رقابت نمی‌کند، بلکه بر روی آن ساخته می شود. در حالی که اینترنت عمدتاً برای مرور استفاده می شود، متاورس تجربه غوطه ورتری را ارائه می‌دهد که در آن افراد می‌توانند تا حدی در فضاهای مجازی «زندگی» کنند. رشد اینترنت خدمات بسیاری را ایجاد کرده است که در حال شکل دادن به متاورس

هستند. فناوری‌های واقعیت مجازی خاص، ابزاری را برای تعامل با پلتفرم‌های چندجهانی گسترده‌تر فراهم می‌کنند. به عنوان مثال، به سازمان‌ها اجازه می‌دهد نمایش‌های مجازی از دستگاه‌های فیزیکی، ماشین‌ها یا فرآیندها ایجاد کنند و شرکت‌ها می‌توانند از متاورس برای شبیه سازی مسائل مختلف استفاده کنند. به عنوان مثال طراحان و شرکت‌های ساخت و ساز می‌توانند نمونه‌های اولیه شبیه سازی شده بسازند تا از هزینه ایجاد نمونه‌های فیزیکی جلوگیری کنند. سازمان‌ها می‌توانند با استفاده از متاورس کارکنان خود را تمرین دهند تا از بلایای طبیعی در تمرین‌ها در امان باشند. در مراقبت‌های پزشکی و مدیریت درد و... نیز متاورس کارایی دارد. در خصوص آماده سازی فضانوردان، انتقال دانش سازمانی و آموزش مهارت‌های خاص و بازآفرینی صحنه جرم و... نیز که در دنیای فیزیکی بسیار پرهزینه یا دشوار است، متاورس به عنوان یک قابلیت برجسته ظاهر خواهد شد. هوش مصنوعی، اینترنت اشیا، تکنولوژی واقعیت توسعه یافته و واقعیت ترکیبی و بلاک چین و سایر فناوری‌های نوین در متاورس کارایی دارند. لازم به ذکر است که بلاک چین یک فناوری کلیدی است که زیرساخت برنامه‌های غیرمتمرکز و ارزهای دیجیتال را فراهم می کند. قابلیت همکاری سیستم‌های مختلف را قادر به تبادل و استفاده از اطلاعات می‌کند، در حالی که سازگاری بین پلتفرمی تضمین می‌کند که برنامه‌ها می‌توانند بر روی دستگاه‌ها یا پلتفرم‌های مختلف اجرا شوند. انتظار می‌رود که متاورس به‌عنوان یک دنیای دیجیتال کاملاً غوطه‌ور و بهم پیوسته که در آن کاربران می‌توانند به طور یکپارچه با یکدیگر و اشیاء دیجیتالی در زمان واقعی تعامل داشته باشند، جایگاهی کلیدی در وب ۳.۰ اشغال کند. متاورس به بسیاری از اصول مشابه، از جمله کنترل بیشتر کاربر، متکی است و احتمالاً بسیاری از فناوری‌های پیشرفته مانند بلاک چین و هوش مصنوعی را به کار خواهد گرفت. یکی از جنبه‌های مثبت، یک متاورس غوطه‌ور این است که انسان را قادر می‌سازد به جایی برود که قبلاً هرگز قادر به رفتن نبوده است، از جمله فضاهای بیرونی و ارتباطات اجتماعی آنلاین نیز می‌تواند بسیار غنی‌تر شود. [۳] از سوی دیگر، چالش‌هایی مانند تسهیل ارتکاب برخی از جرایم و جرم انگاری آن‌ها که موضوع پژوهش حاضر است از نقاط منفی این تکنولوژی می باشد.

۳. پتانسل وقوع جرایم در متاورس

رشد متاورس و انقلاب تکنولوژیکی و عصر فراجهانی که امروزه در حال شکل‌دادن به فضای اجتماعی جدید است، روابط و نظام‌های حقوقی را با چالش‌های جدید مواجه ساخته است که نیازمند نوآوری و بهبود دکترین حقوقی برای رسیدگی به موارد جدید می‌باشد. [۴] دیدگاه عمل‌گرایانه در این زمینه ایجاد قوانینی جزایی در حوزه متاورس است، چرا که با قوانین سنتی نمی‌توان روابط پیچیده این حوزه را تنظیم کرد. دیجیتالی‌شدن زمینه بروز فرایندهایی را ایجاد کرده است که می‌تواند مخرب باشد و بر حقوق بشر تأثیر منفی داشته باشد؛ در این زمینه نیاز به قوانینی فراملی در محیط‌های واقعیت مجازی می‌باشد. [۵] در مورد اینکه چگونه متاورس ممکن است بر فرصت جرم از منظر نظری تأثیر بگذارد، باید رویکرد فعالیت معمول را در نظر گرفت و این یک تئوری زیست‌محیطی است که بیان می‌کند زمانی که مجرم با انگیزه در غیاب سرپرستی توانا با یک هدف مناسب مواجه می‌شود، جرم بیشتر رخ می‌دهد. [۶]

نگهبانان توانا، به پلیس یا نگهبانان امنیتی محدود نمی‌شوند، بلکه شامل هر کسی یا هر چیزی است که می‌تواند برای بازدارندگی متخلفان یا محافظت از یک هدف بالقوه اقدام کند. به‌عنوان‌مثال کسانی که دارای اختیار قانونی برای اعمال کنترل بر یک مکان (هرچند تعریف شده) هستند و می‌توانند با طراحی فضاهایی برای ایمن‌تر کردن آنها یا آموزش کارکنان نقش مهمی ایفا کنند. تغییر در هر یک از شرایط زیست‌محیطی توصیف شده (به‌عنوان‌مثال، در دسترس بودن اهداف مناسب) بر احتمال وقوع جرم تأثیر می‌گذارد. برخلاف دنیای فیزیکی، فعالیت در محیط‌های آنلاین موجود محدود به فضا نیست که باعث افزایش تحرک مجرمان، اهداف و نگهبانان می‌شود و احتمال تعامل آنها را تغییر می‌دهد. متاورس انواع تعاملات ممکن را نیز گسترش می‌دهد؛ بنابراین، متاورس این پتانسیل را دارد که به طور قابل‌ملاحظه‌ای فعالیت‌های معمول افراد خاص و همچنین کاربران را شکل دهد، در نتیجه بر فرصت جرم در مقیاس وسیع تأثیر می‌گذارد. البته جرم به همین سادگی زمانی رخ نمی‌دهد و بر اساس دیدگاه انتخاب منطقی، بستگی به ادراک مجرم از خطر، تلاش و پاداش درگیر در جرم دارد. [۷]

متاورس ممکن است وقوع جرم را تسهیل کند، مگر اینکه استراتژی‌های مدیریت مکان کافی اجرا شود یا سرپرستی غیررسمی در کاهش احتمال وقوع جرم مؤثر باشد، (مثلاً، اگر دیگران در موقعیت‌هایی که احتمال وقوع جرم وجود دارد مداخله کنند، ممکن است احتمال وقوع جرایم بسیار کاهش یابد.) اگرچه عدم قطعیت زیادی در مورد جنایات واقعی وجود دارد که می‌تواند در متاورس رخ دهد، اما پیش بینی تهدیدات احتمالی در حال حاضر مهم است؛ بنابراین انجام این کار می‌تواند به ذینفعانی مانند پلیس، تنظیم‌کننده‌ها، دولت‌ها و ارائه‌دهندگان خدمات کمک کند تا برای آنچه ممکن است پیش بیاید آماده شوند و به طور ایده‌آل با چنین تهدیداتی پیش از ظهور جرم‌های جدید مقابله کنند. [۸]

تشکیل رویه اجرای قانون، و مقررات واحد در زمینه متاورس، ایجاد انجمن فناوری، مؤسسه برق و مهندسین الکترونیک، سازمان بین‌المللی برای استانداردسازی، اتحادیه مخابرات بین‌المللی، کنسرسیوم زمین فضایی باز، انجمن متاورس امریکا و مجمع جهانی اقتصاد از نمونه اقداماتی است که برای ایجاد هنجارهای حقوقی قابل‌اعمال در محیط‌هایی مجازی با همکاری دانشمندان و حقوق‌دانان کشورهای دیگر انجام شده است. [۹] بدون اجرای مؤثر قانون چالش‌های فراوانی برای مجریان قانون ایجاد می‌گردد و به علت محدودیت در شناسایی مجرمان و برخی از جرایم جدید، قانون گذاری در این حوزه پیچیده‌تر خواهد بود. واقعیت مجازی به طور بالقوه زندگی روزمره ما را تغییر می‌دهد و نحوه تعامل و... با محیط اطراف تحت تأثیر قرار می‌گیرد. [۱۰]

جرم‌شناسی جرایم در متاورس به بررسی ابعاد مختلفی از رفتارهای مجرمانه در فضای واقعیت مجازی می‌پردازد، از جمله شناسایی و طبقه‌بندی انواع جرایم دیجیتال که در متاورس رخ می‌دهد، از جمله کلاهبرداری، هک، آزار و اذیت آنلاین و... مطالعه رفتارهای مجرمانه و انگیزه‌های آن‌ها، به‌ویژه در محیط‌های مجازی که ممکن است متفاوت از دنیای واقعی باشد، یکی از اهداف جرم‌شناسی در این حوزه می‌باشد. بررسی تأثیرات اجتماعی و فرهنگی جرایم در متاورس بر روی کاربران و جامعه و تحلیل قوانین موجود و نیاز به تدوین قوانین جدید برای مقابله با جرایم در متاورس و بررسی روش‌های پیشگیری از وقوع جرم و مدیریت بحران‌های مرتبط با جرایم در متاورس

از دیگر اهداف جرم‌شناسی در این حوزه می‌باشد. با توجه به عدم وجود قوانین مشخص برای رسیدگی به جرایم در متاورس این موضوع موجب ایجاد سردرگمی‌هایی در دادرسی کیفری و پیگیری جرایم گردیده است. با توجه به اینکه کاربران معمولاً ناشناس هستند، این موضوع شناسایی مجرمان را دشوارتر می‌کند. تکنولوژی‌های نوظهور مانند بلاک‌چین و واقعیت مجازی می‌توانند پیچیدگی‌هایی را ایجاد کنند که جرم‌شناسی را برای محققان حقوق کیفری دشوارتر می‌سازد؛ همچنین با توجه به ماهیت جهانی بودن متاورس و عبور فعالیت‌های مجرمانه از مرزهای ملی، چالش‌هایی برای جرم‌شناسی در این حوزه ایجاد گردیده است. با پیشرفت سریع فناوری، نوع و شیوه‌های جرایم نیز تغییر می‌کند و نیاز به به‌روزرسانی مداوم قوانین کیفری می‌باشد .با توجه به این ابعاد و چالش‌ها، مطالعه جرم‌شناسی در متاورس یک حوزه تحقیقاتی جدید و مهم است که نیازمند توجه ویژه‌ای است.

در این فضا کاربران انسانی قادرند که اشیا و املاکی را خریداری و تملک کنند، به‌عنوان‌مثال زمین بخرند، خانه بسازند و کسب‌وکار داشته باشند، فعالیت جنسی داشته باشند و ازدواج کنند و سایر فعالیت‌هایی که در زندگی واقعی امکان‌پذیر است، در دنیای واقعیت مجازی محقق می‌گردد، بنابراین متاورس فقط یک بازی ساده نیست و کاربران زیادی در سراسر جهان آن را تجربه می‌کنند و این تجربه همه‌جانبه و مانند زندگی ثانویه می‌باشد. [۱۱] این فضا به علت پیشرفت‌های خود دارای پتانسیل اقتصادی بالا در جهت سرمایه‌گذاری شرکت‌های خصوصی می‌باشد و به یکی از اشکال اصلی به‌کارگیری اینترنت در آینده تبدیل خواهد شد. متاورس به کاربران امکان تجربه‌ای فراگیر می‌دهد که این تجربه برخلاف بقیه بازی‌ها پایدار است و با خروج از بازی از بین نمی‌رود و پلتفرم جهانی است و فراتر از مرزها عمل می‌کند. [۱۲] این پلتفرم‌ها به دلیل به‌کارگیری فناوری‌های سمعی - بصری و لمسی درک جدیدی از واقعیت مجازی را برای کاربران محقق می‌سازند. [۱۳]

متاورس سؤالات زیادی را در حوزه حقوق مالکیت فکری، حقوق قراردادها، حقوق جزا و جرم‌شناسی و سایر حوزه‌های حقوق ایجاد کرده است. بی شک در فضای متاورس جرایمی رخ می‌دهد و یکی از اساسی‌ترین پرسش‌هایی که سیاست‌گذاران و مجریان قانون مجبور به پاسخگویی آن می‌باشند، نحوه برخورد با مجرمان در متاورس و جرم‌انگاری در این فضا می‌باشد. در این زمینه قوانین با خلأهایی مواجه می‌باشند. چالش‌های جرم‌شناسی در متاورس شامل، عدم وجود قوانین مشخص می‌باشد، چرا که در بسیاری از کشورها هنوز قوانین خاصی برای رسیدگی به جرایم مالی در متاورس ندارند. این موضوع باعث می‌شود که پیگرد قانونی مجرمان دشوار باشد و امکان اعمال مجازات محدود شود. ناشناسی کاربران در متاورس، شناسایی و پیگرد مجرمان را بسیار دشوار می‌کند. این امر باعث می‌شود که مجرمان احساس امنیت بیشتری کنند و دست به اقداماتی بزنند که در دنیای واقعی ممکن است، انجام ندهند. فناوری‌های نوینی مانند بلاک‌چین و واقعیت مجازی ممکن است فهم و تحلیل فعالیت‌های مجرمانه را برای محققان و مقامات قضایی دشوار کند. همچنین، تغییرات سریع در این فناوری‌ها باعث می‌شود که دانش موجود سریعاً منسوخ شود و نیاز به‌روزرسانی باشد. لازم به ذکر است، متاورس یک فضای جهانی است و فعالیت‌های مجرمانه ممکن است از مرزهای ملی عبور کند. این موضوع نیازمند همکاری بین‌المللی است که معمولاً با چالش‌هایی همراه است. در این راستا، جرایم مالی در متاورس می‌توانند

تأثیرات منفی بر روی سلامت روانی کاربران داشته باشند. آسیب‌هایی مانند افسردگی و اضطراب ناشی از کلاهبرداری‌ها و سرقت‌ها می‌تواند به مشکلات اجتماعی منجر شود. عدم آگاهی کاربران از خطرات موجود در متاورس و روش‌های محافظت از خود، می‌تواند آن‌ها را مستعد وقوع جرایم کند؛ بنابراین، آموزش و آگاهی‌بخشی به کاربران یکی از چالش‌های مهم است.

در این زمینه در جهت تحقق عدالت و ایجاد نظم در جامعه جهانی بایستی جرم‌انگاری و نظرپردازی صورت گیرد و اصل آزادی فردی در متاورس موجب آسیب به حقوق دیگران نشود، اگر چه منجر به آسیب واقعی به کاربران نشده باشد. بایستی بررسی نمود که در حیطه واقعیت مجازی رفتار مجرمانه موجب آسیب درون فعالیت مجازی است یا آسیب فراتر از مجازی نیز رخ می‌دهد؟ به‌عنوان‌مثال در فضاهایی که کشتن کاربران مجاز می‌باشد و کاربران به این موضوع رضایت می‌دهند، هیچ جرم کیفری محقق نشده است. [۱۴]

همان‌طور که بیان گردید به‌احتمال زیاد در متاورس آسیب فیزیکی رخ نمی‌دهد، بلکه آسیب‌ها اقتصادی و روانی است، در جرم‌انگاری نیز این موضوع لحاظ گردد. در برخی از موارد فضای متاورس اجازه برخی از رفتارها را می‌دهد اگر چه در واقعیت در برخی از کشورها جرم‌انگاری شده باشد، به‌عنوان‌مثال در متاورس ممکن است افراد قادر به مصرف مواد مخدر یا الکل باشند و یا فضای متاورس را آلوده سازند، در حالی که این موارد مجرمانه نیست. از سوی دیگر بخری از جرایم قابل‌تحقق نیست، مانند تقلب در انتخابات، مهاجرت غیرقانونی و چندهمسری و... اما برخی جرایم در متاورس احتمالاً مجرمانه تلقی می‌گردد، مانند زنا که از نظر تئوری ممکن است، رخ دهد و موجب ناراحتی کاربران گردد. به‌عنوان‌مثال زمانی که یک آواتار اقدام به اذیت و آزار جنسی کاربران دیگر می‌کنند، به عنوان جرایم جنسی یا حداقل جرایم علیه اشخاص قابل جرم‌انگاری است؛ همچنین ارسال تصاویر ناخواسته جنسی و فیلم‌های پورن به سایر کاربران می‌تواند برچسب زده شود و قابل پیگرد باشد؛ این موارد به‌احتمال زیاد شامل هک یا جنایت سایبری خواهد بود. برخی دیگر از جرایم در متاورس قابل‌تحقق نیستند، به عنوان مثال آدم‌ربایی در متاورس غیرممکن است، چرا که کاربران می‌توانند به‌سادگی از سیستم خارج شوند، اما ایجاد مزاحمت و ترسی که رخ می‌دهد می‌تواند موجب سلب آسایش کاربران دیگر گردد؛ بنابراین جرم توهین و تهدید نیز در متاورس قابل‌تحقق است؛ بنابراین جرایم قابل‌تحقق در متاورس به چند گروه جرایم مالی، جنایات جنسی، سایر جنایات علیه اشخاص تقسیم می‌گردند.

همان‌طور که بیان گردید، آواتارها نمایش ناملموسی از کاربران روی پلتفرم‌ها هستند، از جمله تصاویر ثابت، نمایش‌های مصور یا نمایش‌های انسان‌نما. آواتارهای کاربران در متاورس به عنوان یک نقطه دسترسی عمل می‌کنند. این آواتارها همچنین ماسکی را برای کمک به تعامل، انتشار اطلاعات و وحدت فرهنگی درک شده در اختیار کاربران قرار می‌دهند. در متاورس، آواتارها می‌توانند در دعواهایی درگیر شوند که در دنیای فیزیکی، نقض قانون جرم یا قانون کیفری است. یکی از استفاده‌های مخرب بالقوه افترا است. ایجاد آواتار تحت پوشش شخصیت دیگری غیرقانونی نیست، اما می‌تواند شخصیت را نادرست معرفی کند و به بی‌اعتمادی، نارضایتی و مزاحمت برای سایر کاربران منجر شود. اگر چه بخشی از اقدامات ممکن است به عنوان بخشی از فرهنگ بازی

قابل‌قبول باشد (مانند سرقت، و تیراندازی در بازی‌های تیراندازی اول‌شخص و...) اما بایستی این رفتارها از رفتارهای مجرمانه متمایز گردد. همان‌طور که بیان گردید، آواتارها کاربران را قادر می‌سازند تا هویت‌هایی ایجاد کنند که ممکن است با هویت خود در دنیای فیزیکی متفاوت باشد و به آنها اجازه می‌دهد که رفتار خود را به دلیل ناشناس بودن نسبی تغییر دهند و افراد را قادر می‌سازند تا به روش‌هایی عمل کنند که در دنیای آفلاین ممکن یا قابل‌قبول نباشد؛ بنابراین، ناشناس ماندن آواتار در متاورس، می‌تواند فرهنگ کاهش مسئولیت‌پذیری را القا کند و به بازیگران اجازه سوءاستفاده بدهد. [۱۵]

نسبت دادن مسئولیت قانونی به یک آواتار و کاربر آن دشوار است، به‌ویژه ازآنجایی‌که آواتارها ممکن است دارای قابلیت‌های هوش مصنوعی باشند، اگرچه توسط یک انسان یا مجموعه‌ای از انسان‌ها برنامه‌ریزی شده‌اند، اما چنین آواتارهایی همچنین از تعاملات یاد می‌گیرند و با گذشت زمان، مسئولیت‌پذیری منتسب به یک کاربر را با هر تعاملی منتشر می‌کنند. این شخصیت حقوقی را می‌توان از طریق ثبت‌نام اعطا کرد و هر فردی فقط یک آواتار را در متاورس ثبت می‌کند. آواتارها می‌توانند انواع مختلفی از جنایات و جنایات را فراتر از تعامل کاربر با کاربر مرتکب شوند. به‌عنوان‌مثال، متاورس می‌تواند به عنوان یک پلتفرم برای آواتارها برای فروش دارایی‌های معنوی دزدیده شده از خارج از متاورس عمل کند. در متاورس، هویت جنبه‌ای از انسانیت است که دارای ارزش خواهد بود. چه از نظر فرهنگی، اجتماعی، یا هر جنبه دیگری از هویت که فرد ممکن است با آن هماهنگ شود، این موضوع در درجه اول شامل هویت فردی می‌شود. افترا و سرقت هویت می‌تواند منجر به ارتکاب جرم و مسئولیت برای کسانی شود که از هویت خود سوءاستفاده می‌کنند. در متاورس نگرانی در مورد هویت و بازنمایی افزایش یافته است، زیرا هیچ راهی برای تأیید هویت مجازی بدون عبور از خطوط حریم خصوصی داده‌ها وجود ندارد؛ بنابراین، برای محدود کردن سرقت هویت و از دست دادن حریم خصوصی داده‌ها در این زمینه، پلتفرم‌ها باید مداخله کنند. ایجاد فرایندهای ثبت و ثبت آواتار (برای تبدیل آواتارها به تعهدات قراردادی و دائمی) یکی از راه‌های به چالش کشیدن این موضوع است. آزار و اذیت جنسی و سرقت هویت، احتمالاً در متاورس بدتر خواهد شد. در متاورس، آزار و اذیت می‌تواند شامل سرقت مالکیت معنوی، تصاویر شخصی برای جعل باشد. [۱۶] جرایمی دیگر شامل جرایم مالی از قبیل کلاهبرداری، سرقت، پول‌شویی در متاورس قابل‌تحقق است؛ حملات به بلاک‌چین و دارایی‌های دیجیتال برای سرقت یکی از انواع جرایم علیه اموال می‌باشد. [۱۷]

جرایم مالی در متاورس به‌دلیل ویژگی‌های خاص این فضا، مانند ناشناس بودن، عدم وجود قوانین مشخص و فناوری‌های نوین، به‌طور فزاینده‌ای در حال افزایش است. انواع کلاهبرداری مانند، ارائه فرصت‌های سرمایه‌گذاری جعلی در پروژه‌های متاورس که در واقع وجود ندارند. فروش کالاها یا خدمات مجازی که وجود ندارند، ایجاد وب‌سایت‌ها یا اپلیکیشن‌های جعلی برای سرقت اطلاعات شخصی و مالی کاربران از اشکال کلاهبرداری می‌باشد. سرقت نیز در این فضا شامل سرقت هویت دیجیتال و دسترسی غیرمجاز به حساب‌های کاربری و استفاده از هویت دیگران برای انجام فعالیت‌های مجرمانه و سرقت دارایی‌های دیجیتال از کیف پول‌های دیجیتال کاربران می‌باشد. پولشویی نیز در متاورس به دلیل وجود ارزهای دیجیتال و ناشناس بودن تراکنش‌ها، به

راحتی قابل انجام است. استفاده از ارزهای دیجیتال برای انتقال پول‌های حاصل از فعالیت‌های غیرقانونی به حساب‌های قانونی و بهره‌برداری از پلتفرم‌هایی که نظارت کمی بر روی تراکنش‌ها دارند، فرصت را برای پولشویی در این فضا ایجاد نموده است.

بازیگران مخرب می‌توانند به عنوان دلال دارایی‌های دیجیتال ظاهر گردند و با هدف سرقت یا کلاهبرداری از اموال مالکان سوءاستفاده کنند. [۱۸] نقض حق نسخه‌برداری مطالب و نرم‌افزارها نیز می‌تواند حق نسخه‌برداری را نقض کند و موجب استفاده مجدد از داده‌ها و کلاهبرداری گردد. [۱۹] سرقت هویت نیز برای جعل اطلاعات مانند جعل اطلاعات عابر بانک مجازی در جهت دسترسی به اطلاعات برای سود مالی نیز یکی از جرایم در حوزه متاورس می‌باشد. [۲۰] انواع کلاهبرداری نیز در متاورس قابل‌تحقق است، شامل توسعه زمین جعلی، کلاهبرداری با جعل اطلاعات و... [۲۱] پولشویی و استفاده از دارایی‌های غیرقانونی و تمیز نمودن آن و تملک دارایی‌ها مانند ارزهای رمزنگاری شده در متاورس، زمین و دارایی‌های مجازی نیز قابل‌تحقق است. [۲۲] سرقت فیزیکی حسگرها و هدست‌ها نیز توسط کاربران دیگر برای به‌دست‌آوردن اطلاعات و دارایی‌های دیجیتال یکی از انواع جرایم در این حوزه می‌باشد. [۱۸]

جرایم علیه کودکان در متاورس یکی از نگرانی‌های جدی در دنیای دیجیتال امروز است. این جرایم شامل انواع مختلفی از رفتارهای غیرقانونی می‌شوند که می‌توانند تأثیرات منفی عمیقی بر روی کودکان و نوجوانان داشته باشند. انواع جرایم شامل پورنوگرافی کودکان می‌باشد؛ این نوع جرم شامل تولید، توزیع و مشاهده محتوای جنسی غیرقانونی با مشارکت کودکان است. در متاورس، این محتوا می‌تواند به‌راحتی به اشتراک گذاشته شود و دسترسی به آن برای مجرمان آسان‌تر باشد. مجرمان می‌توانند با استفاده از هویت‌های جعلی یا پروفایل‌های جذاب، به دنبال کودکان باشند و سعی کنند با آن‌ها ارتباط برقرار کنند. این نوع ارتباط می‌تواند منجر به سوءاستفاده یا فریب کودکان شود. کودکان ممکن است در معرض آزار و اذیت‌های آنلاین قرار بگیرند که می‌تواند شامل توهین، تهدید یا قلدری باشد. این رفتارها می‌توانند تأثیرات روانی جدی بر روی کودکان داشته باشند. در این راستا، با توجه به اینکه بخشی از کاربران در متاورس را کودکان تشکیل می‌دهند، جرایمی مانند پورنوگرافی کودکان نیز چالش‌برانگیز است و کودکان نیز می‌توانند درگیر فعالیت‌های جنسی غیرمجاز شوند و مورد سوءاستفاده واقع شوند. [۲۳] استفاده از اطلاعات کاربران مانند داده‌های زیستی و ردیابی شده برای اخاذی و سوءاستفاده از آن‌ها نیز امکان‌پذیر است. [۲۴]

در اواخر سال ۲۰۲۱، نینا پاتل، یکی از بنیانگذاران و معاون تحقیقات متاورس، در مورد تجربه خود از آزار جنسی در مکان‌های متاورس نوشت. پاتل گزارش داد که چگونه آواتار او توسط سه تا چهار آواتار مرد، مورد آزار و اذیت کلامی و جنسی قرار گرفت و آنها نیز عکس‌های این حادثه را گرفتند و بعداً با او به اشتراک گذاشتند. او نوشت: «تا حدودی، پاسخ فیزیولوژیکی و روانی من طوری بود که انگار در واقعیت اتفاق افتاده است.» به نظر می‌رسد که پاتل تنها نیست. مرکز مقابله با نفرت دیجیتال دریافته است که کاربران واقعیت مجازی متاورس، از جمله کودکان، هر هفت دقیقه یک بار در طول ۱۲ ساعت در معرض رفتارهای توهین آمیز آنلاین قرار می‌گیرند. این شامل قرار گرفتن در معرض محتوای جنسی، قلدری، آزار و اذیت و سوء استفاده جنسی و تهدید به خشونت

است. ۴۹ درصد از زنان مورد بررسی حداقل یک تجربه آزار جنسی را هنگام استفاده از محصولات واقعیت مجازی گزارش کردند. متاورس فقط یک بازی نیست که در آن با قرار دادن یک هدست واقعیت مجازی، بتوان ابرقهرمان بودن را تجربه نمود، بلکه یک جهان موازی است که به کسانی که در آن هستند اجازه می‌دهد تا همان کارهایی را که در زندگی واقعی انجام می‌دهند (دیدار با دوستان، کار، رفتن به رویدادهای موسیقی زنده و قرار ملاقات‌ها) و موارد دیگر انجام دهند و تجربه کنند، بدون نیاز به پا گذاشتن به بیرون. هدف متاورس ایجاد دنیای مجازی است که به اندازه دنیایی که در حال حاضر در آن زندگی می‌کنیم احساس واقعی داشته باشد و این فناوری به طور مداوم برای تسهیل این امر در حال توسعه است. این موضوع شامل ابزارهای نوآورانه است که به ما امکان می‌دهد لمس، حرکت حسی و حتی حس بویایی مجازی را تجربه کنیم. در راستای ارتقای امنیت، پاسخ فیسبوک به شکایت پاتل افزودن یک ویژگی ایمنی (حباب) بود که از یک آواتار در برابر رفتار ناخواسته سایر آواتارها محافظت می‌کند. در حالی که دیدن مواجهه با عواقب قانونی نقض تعهدات رفتاری در متاورس می‌تواند کارایی بیشتری داشته باشد، اما متاورس هنوز به این مرحله نرسیده است. لایحه ایمنی آنلاین برای دومین بار در ۱۹ آوریل ۲۰۲۲ در مجلس عوام قرائت شد. هدف از این لایحه اطمینان از وجود سیستم‌هایی در پلتفرم‌های آنلاین است که با محتوای غیرقانونی و مضر سروکار دارند. این لایحه چهار جرم جدید را معرفی می‌کند: جرم ارتباطی مبتنی بر آسیب، جرم ارتباطی نادرست، جرم ارتباطی تهدیدآمیز و جرم فلش سایبری. به شرطی که بتوان فردی را که پشت یک آواتار آزاردهنده قرار دارد شناسایی کرد، نباید مانعی برای اعمال چنین قوانینی در فرافضا وجود داشته باشد. به راحتی می‌توان دید که چگونه، در موقعیت‌هایی مشابه با شرایطی که پاتل تجربه کرده، ممکن است یک جرم آزار و اذیت مرتکب شود و بایستی این رفتارها قابلیت پیگرد قانونی داشته باشد. لازم به ذکر است، قانون پاسخ آسانی به جرایم تماسی، مانند تجاوز جنسی، زمانی که در فضای مجازی انجام شده است، ندارد. برای انجام جرایم تماسی، سطحی از تعامل فیزیکی لازم است، در حالی که در فضای واقعیت مجازی اثبات لمس به طور قابل توجهی مشکل سازتر است و بدون شک نیاز سازوکارهای قانونی برای مقابله با آزار و اذیت جنسی است. در اوایل سال ۲۰۲۲ فیلسوف دیوید کالمرز استدلال کرد که تجربیات در دنیای مجازی، از جمله تعاملات اجتماعی عبارتند از: "به اندازه واقعیت واقعی، فقط متفاوت"، بنابراین، منطقی است که انتظار داشته باشیم تجربه‌ای مانند تجاوز جنسی، توسط دادگاه‌ها صرفاً به این دلیل که در دنیای مجازی رخ داده است، رد نشود. در این خصوص به دلیل ماهیت فرامرزی بودن مشکل تعیین صلاحیت مطرح می‌گردد و بایستی سازوکارهای قانونی در این خصوص در نظر گرفته شود به نحوی که گستره قانون قابل اعمال فرامرزی باشد. [۲۵]

با اینکه فعالیت‌های جنسی می‌تواند از اعمال روزمره در متاورس باشد، اما تجاوز و ارائه تصاویر جنسی مخرب و اشتراک آن‌ها یا سوءاستفاده از فعالیت‌های جنسی کاربران در متاورس و یا استفاده از زور و... نیز بایستی جرم‌انگاری گردد، چرا که به دلیل استفاده از لباس‌های لمسی و تجهیزات غوطه‌ور، این آسیب‌ها به ویژه برای کودکان و نوجوانان شدیدتر است و امکان بهره‌کشی جنسی آواتارهای کاربران آسیب‌پذیر می‌تواند موجب ناامنی در فضای متاورس گردد. [۲۶]

حملات سایبری افراد فیزیکی برای آسیب‌رساندن به کاربران و آزار و اذیت آن‌ها در پلتفرم‌های متاورس بایستی مورد تعقیب قرار گیرد. [۲۷] تحریک به خودآزاری و اجبار به کار کودکان و برده داری مدرن نیز در فضای دیجیتال قابل تحقق می‌باشد و بایستی سازوکارهایی در جهت جلوگیری از سوءاستفاده از کاربران پیش بینی گردد. طبق اجماع کارشناسان و تحقیقات صورت گرفته حدود یک سوم تهدیدها در متاورس مربوط به جرایم مالی شامل حملات پیچیده به بلاک چین‌ها، سرقت دارایی‌های مجازی، کلاهبرداریو جعل و فرار مالیاتی و پولشویی بوده است. همچنین طیف وسیعی از تجاوزات جنسی نیز در این فضا رخ می‌دهد و متاورس نیز به دلیل فناوری لباس‌های لمسی فرصت وقوع جرم را تسهیل کرده است و قربانیان آسیب پذیر تر می‌باشند.

۴-راهکارهای کاهش جرایم در متاورس

با توجه به چالش‌های مطرح شده و انواع جرایم قابل‌تحقق بایستی سیاست‌گذاران در این حوزه اقدام به وضع قوانین و مقررات واضحی بنمایند تا حقوق مالکیت و حقوق خصوصی اشخاص رعایت گردد. همان‌طور که بیان گردید در متاورس جرایم می‌تواند شامل دزدی، خراب‌کاری اموال، آتش‌زدن، توهین و تهدید و جرایم علیه اشخاص و کودکان باشد.

جرایم جنسی نیز یکی از چالش برانگیزترین جرایم در متاورس می‌باشد که تأثیرات روانی زیادی در پی دارد و ایمنی کاربران را با چالش‌هایی مواجه می‌سازد. [۲۸] کاهش جرایم علیه کودکان و دیگر کاربران در متاورس نیازمند رویکردی چندجانبه است که شامل همکاری میان قانون‌گذاران، شرکت‌های فناوری، خانواده‌ها و کاربران می‌باشد. قانون‌گذاران باید قوانینی خاص برای متاورس و فضای دیجیتال ایجاد کنند که شامل تعریف دقیق جرایم، مجازات‌ها و روش‌های پیگیری باشد و این قوانین باید به طور خاص به حفاظت از کودکان و نوجوانان توجه داشته باشند. چون متاورس یک فضای جهانی است، نیاز به همکاری بین‌المللی برای مقابله با جرایم فراملی وجود دارد و کشورها باید توافق‌نامه‌هایی برای تبادل اطلاعات و همکاری در تحقیقات جنایی امضا کنند. قانون‌گذاران باید قوانین سخت‌گیرانه‌ای برای حفاظت از داده‌های شخصی کاربران وضع کنند. توسعه قوانین مرتبط با مالکیت دیجیتال و حقوق مرتبط با آن می‌تواند به حفاظت از آثار و محتواهای تولید شده توسط کاربران کمک کند. برگزاری برنامه‌های آموزشی برای کودکان، والدین و معلمان درباره خطرات متاورس و نحوه مواجهه با آن‌ها می‌تواند به افزایش آگاهی کمک کند. اجرای کمپین‌های آگاهی عمومی در مورد حقوق کاربران و نحوه گزارش جرایم آنلاین می‌تواند به کاهش آسیب‌ها در این حوزه کمک کند. توسعه ابزارهای نظارتی و فیلترینگ محتوا که بتوانند محتوای نامناسب را شناسایی و مسدود کنند، می‌تواند به کاهش جرایم علیه اطفال کمک کند .ایجاد سیستم‌های آسان و ایمن برای گزارش جرایم و رفتارهای غیرقانونی علیه کودکان به کاربران این امکان را می‌دهد که به‌راحتی تخلفات را گزارش کنند. ایجاد دسترسی به خدمات مشاوره و پشتیبانی روان‌شناختی برای کودکانی که قربانی جرایم آنلاین شده‌اند، می‌تواند به بهبود وضعیت روانی آن‌ها کمک کند؛ همچنین، تشکیل شبکه‌های حمایتی برای والدین و خانواده‌ها به‌منظور تبادل تجربیات و راهکارها می‌تواند مفید باشد. در نتیجه، کاهش جرایم علیه کودکان و دیگر کاربران در متاورس نیازمند تلاش مشترک میان قانون‌گذاران، شرکت‌های فناوری، خانواده‌ها و خود کاربران است. با اتخاذ رویکردهای جامع و چندجانبه، می‌توان به ایجاد

فضایی امن‌تر و سالم‌تر در دنیای دیجیتال کمک کرد. در این زمینه بایستی سیاست‌گذاران درک عمیقی از وضعیت متاورس و انواع رفتارهایی که موجب آسیب به کاربران می‌گردد باشد و محققان از طریق پرسش‌نامه، مصاحبه و اقدامات روان‌شناختی اقدام به جمع‌آوری اطلاعات برای جرم‌انگاری این رفتارها در این فضاها نمایند؛ بنابراین بایستی بررسی شود که آیا آسیب روانی گستره زیادی دارد و موجب کاهش استقبال از فضای واقعیت مجازی می‌گردد یا خیر. چرا که چنین رفتارهایی می‌تواند منجر به آسیب به سلامت روانی و مادی کاربران گردد و حریم خصوصی آن‌ها را نیز نقض کنند؛ بنابراین، جرایم جنسی و تجاوز در متاورس می‌تواند به شکل‌های مختلفی رخ دهد و چالش‌های متعددی را به همراه داشته باشد. در متاورس، کاربران می‌توانند به صورت ناشناس با یکدیگر تعامل کنند. این ناشناس بودن ممکن است برخی افراد را به سوءاستفاده از دیگران ترغیب کند. برخی از افراد ممکن است هویت‌های جعلی ایجاد کنند تا به‌راحتی به قربانیان نزدیک شوند و از آن‌ها سوءاستفاده کنند. وجود محتواهای نامناسب یا تحریک‌آمیز در محیط‌های مجازی می‌تواند زمینه‌ساز رفتارهای جنسی غیرمجاز باشد. در واقعیت مجازی، کاربران می‌توانند تجربه‌های عمیق‌تری از تعاملات اجتماعی داشته باشند. این می‌تواند به رفتارهای غیرقانونی مانند تجاوز و آزار و اذیت جنسی منجر شود. بسیاری از پلتفرم‌های متاورس فاقد نظارت کافی بر رفتار کاربران هستند و این موضوع می‌تواند به افزایش جرایم جنسی کمک کند. بسیاری از کشورها هنوز قوانین خاصی برای مقابله با جرایم جنسی در فضای دیجیتال ندارند که این موضوع می‌تواند منجر به عدم برخورد مناسب با این نوع جرایم شود. قربانیان ممکن است به دلیل عدم وجود سازوکارهای حمایتی، از گزارش جرایم خود ترس داشته باشند و این موضوع می‌تواند مانع از دریافت کمک و حمایت مناسب شود. با توجه به اینکه مسئولیت پلتفرم‌های متاورس در قبال رفتار کاربران و حفظ امنیت آن‌ها هنوز به طور کامل مشخص نیست، این چالش می‌تواند به عدم پاسخگویی منجر شود. بسیاری از کاربران ممکن است از خطرات موجود در متاورس آگاهی کافی نداشته باشند و این موضوع می‌تواند آن‌ها را در معرض خطر قرار دهد. در برخی موارد، زنان و اقلیت‌های جنسی ممکن است بیشتر از دیگران هدف جرایم جنسی قرار گیرند که این موضوع نیازمند توجه ویژه به مسائل عدالت اجتماعی است. در نتیجه جرایم جنسی و تجاوز در متاورس یک چالش جدی است که نیازمند ایجاد قوانین مشخص، افزایش آگاهی عمومی و توسعه ابزارهای نظارتی می‌باشد که می‌تواند به کاهش این نوع جرایم کمک کند و فضایی امن‌تر برای همه کاربران فراهم آورد.

همان‌طور که در مقدمه بحث و قسمت چیستی متاورس بیان گردید، متاورس تجربه زندگی ثانویه و غوطه‌ور را ارائه می‌دهد که می‌تواند خدمات زیادی در بخش‌های صنعتی، پزشکی، نظامی و پلیسی، آموزشی و... ارائه دهد، اما مانند تمام محصولات جدید این فناوری نیز می‌تواند پتانسیل وقوع جرایم را افزایش دهد و محیط سه‌بعدی و همه‌جانبه متاورس و مبادله زیاد ارزهای دیجیتال، موجب تسهیل وقوع جرایم به ویژه جرایم مالی می‌گردد و موجب افزایش مقیاس و تنوع کلاهبرداری و سرقت و تأمین مالی تروریسم می‌گردد. از سوی دیگر ایجاد تجربیات زنده با به‌کارگیری هدست‌ها و لباس‌های لمسی، پتانسیل جرایم جنسی را نیز افزایش داده است که یکی از آسیب‌پذیرترین گروه در این پلتفرم کودکان می‌باشند که دست‌یافتنی‌تر بوده و امکان جرایم علیه آن‌ها آسان‌تر است. با توجه به پتانسیل‌های متاورس بایستی تعیین گردد که کدام

جرایم رتبه‌بندی بالاتری در متاورس داشته و کدام یک بایستی اولویت سیاست‌گذاران برای جرم‌انگاری و جرم‌شناسی با هدف جلوگیری از وقوع این جرایم قرار گیرد. ناشناس ماندن آواتارها یکی از چالش‌هایی است که موجب می‌گردد شناسایی آن‌ها دشوارتر شده و فضای ایجاد جرم را آسان‌تر نموده است، عدم وجود کنترل‌کننده‌های مرکزی نیز موجب تسهیل وقوع جرم می‌گردد؛ بنابراین مجرمان با بررسی احتمال دستگیری و سنجش پاداش به‌دست‌آمده از جرم، تصمیم به ارتکاب جرایم می‌گیرند. در این زمینه علاوه بر حفظ حریم خصوصی بایستی نظارت صورت گیرد تا فضای متاورس امن باشد و بین ایجاد امنیت و حفظ حریم خصوصی تعادل ایجاد شود. همان‌طور که بیان گردید تأثیرات وقوع بسیاری از جرایم ممکن است در دنیای واقعی نیز باشد، مانند کلاهبرداری، سرقت و... بنابراین جای تعجب نیست اگر راهبردهای جلوگیری از جرایم مالی در صدر برنامه‌های پیشگیری قرار گیرد.

فرصت‌های انواع کلاهبرداری‌ها در متاورس امکان‌پذیر خواهد بود، اما ازآنجایی‌که اشکال دیگری از مالکیت (به‌عنوان‌مثال، کالاهای مجازی، زمین مجازی) در متاورس وجود خواهد داشت که با به‌کارگیری بلاک‌چین‌های (احتمالاً غیرقانونی) که فاقد کنترل‌کننده مرکزی برای نظارت بر فعالیت هستند، ثبت می‌شود. فرصت‌های جرایم مالی (از جمله پولشویی) به طور قابل‌توجهی افزایش می‌یابد و ازآنجایی‌که انتظار می‌رود متاورس یک محیط چندکاربره باشد، این موضوع ممکن است تخلف را در مقیاسی بزرگ‌تری از آنچه امروز می‌بینیم تسهیل کند. کاهش جرایم مالی؛ مانند سرقت و کلاهبرداری در متاورس نیازمند رویکردهای چندجانبه و همکاری بین‌المللی است. کاربران باید با خطرات موجود در متاورس آشنا شوند. برگزاری وبینارها، کارگاه‌ها و تولید محتوای آموزشی می‌تواند به افزایش آگاهی کاربران کمک کند. پیاده‌سازی فناوری‌های رمزنگاری پیشرفته، احراز هویت چندعاملی و سیستم‌های نظارتی می‌تواند به کاهش جرایم مالی کمک کند. ایجاد و اجرای قوانین مشخص برای فعالیت‌های اقتصادی در متاورس، به ویژه در زمینه‌های مالی، می‌تواند به جلوگیری از کلاهبرداری‌ها کمک کند. توسعه پلتفرم‌های متاورس با استانداردهای امنیتی بالا و نظارت بر فعالیت‌های کاربران، می‌تواند به کاهش جرایم مالی کمک کند؛ همچنین، ایجاد سیستم‌های گزارش‌دهی آسان برای کاربران به‌منظور اطلاع‌رسانی درباره فعالیت‌های مشکوک و پیگیری سریع این گزارش‌ها و همکاری بین کشورها و سازمان‌های بین‌المللی برای مقابله با جرایم مالی در متاورس، به ویژه در زمینه تبادل اطلاعات و بهترین شیوه‌ها می‌تواند منجر به کاهش این جرایم گردد. استفاده از الگوریتم‌های هوش مصنوعی برای شناسایی الگوهای مشکوک و پیش‌بینی فعالیت‌های کلاهبردارانه، تشویق کاربران به رفتارهای اخلاقی و مسئولانه در فضای متاورس و ایجاد فرهنگ احترام به حقوق دیگران می‌تواند به کاهش جرایم مالی کمک کند و محیطی امن برای کاربران ایجاد کند.

کاهش جرایم مالیاتی در متاورس نیز نیازمند رویکردهای جامع و استفاده از فناوری‌های نوین است؛ ایجاد سیستم‌های مالی شفاف که تمامی تراکنش‌ها را ثبت و قابل پیگیری کند. این امر می‌تواند شامل استفاده از بلاک‌چین برای ثبت تراکنش‌ها باشد. برگزاری دوره‌های آموزشی برای کاربران و کسب‌وکارها در مورد قوانین مالیاتی مرتبط با فعالیت‌های آنها در متاورس و تدوین و اجرای قوانین مالیاتی روشن و دقیق برای فعالیت‌های اقتصادی در متاورس، به‌ویژه در زمینه

خریدوفروش دارایی‌های دیجیتال و به‌کارگیری هوش مصنوعی برای شناسایی الگوهای مشکوک و پیش‌بینی رفتارهای مالیاتی غیرقانونی و ایجاد نهادهای نظارتی بر فعالیت‌های مالی در متاورس و توسعه نرم‌افزارهای گزارش‌دهی درآمدها و هزینه‌ها و محاسبه مالیات و حمایت از نوآوری‌ها و کسب‌وکارهای نوین توسط دولت می‌تواند به کاهش جرایم مالیاتی کمک شایان توجهی نماید.

کاهش جرایم پولشویی در متاورس نیازمند رویکردهایی می‌باشد که شامل شفافیت در تراکنش‌ها می‌باشد، به‌نحوی‌که استفاده از فناوری بلاک‌چین برای ثبت و پیگیری تمامی تراکنش‌ها به‌گونه‌ای که قابل‌دسترسی و شفاف باشد. این امر می‌تواند به شناسایی فعالیت‌های مشکوک کمک کند. پیاده‌سازی فرایندهای شناسایی مشتری برای کاربران جدید، به ویژه در پلتفرم‌های مالی و تجاری که شامل جمع‌آوری اطلاعات هویتی و مالی کاربران می‌باشد می‌تواند به شفافیت تراکنش‌ها کمک کند؛ استفاده از ابزارهای تحلیل داده و هوش مصنوعی برای شناسایی الگوهای غیرعادی در تراکنش‌ها که ممکن است نشان‌دهنده فعالیت‌های پولشویی باشد و ایجاد نهادهای نظارتی که به طور مستمر بر فعالیت‌های اقتصادی در متاورس نظارت کنند و به شناسایی و بررسی موارد مشکوک بپردازند از دیگر راهکارهای کاهش پولشویی می‌باشد؛ برگزاری دوره‌های آموزشی برای کاربران و کسب‌وکارها درباره خطرات پولشویی و روش‌های شناسایی آن و تدوین و اجرای قوانین و مقررات خاص برای فعالیت‌های اقتصادی در متاورس که شامل جرایم پول‌شویی نیز باشد می‌تواند به کاهش این جرایم کمک شایان توجهی نماید. طراحی پلتفرم‌هایی با امنیت بالا و استفاده از روش‌های رمز نگاری شده برای شفافیت تراکنش‌ها و طراحی قراردادهای هوشمند می‌تواند منجر به کاهش این جرایم گردد.

از دیدگاه تئوری بررسی گردید که هر جرایمی تا چه حدی محتمل خواهد بود، با این حال، اینکه پتانسیل واقعی بروز جرایم چقدرخواهند بود، بستگی به این دارد که استفاده از متاورس چقدر در همه‌جا گسترش یابد و چه کسانی از آن استفاده کنند و برای چه اهدافی از آن استفاده شود. به دلیل ماهیت در حال ظهور آن، در حال حاضر در این موارد عدم اطمینان وجود دارد. با توجه به اینکه متاورس می‌تواند فرصت وقوع جرم را تسهیل کند، اینکه کدام بازیگران بیشتر درگیر خواهند شد برای طراحی سازوکار نظارتی و امنیتی و وضع مقررات حائز اهمیت است.

در بسیاری از موارد در دنیای فیزیکی، برای جلوگیری از تضاد در تقلب و تضعیف مالی، شخصیت حقوقی یک شرکت به عنوان مجزا از مالک تلقی می‌شود.، تشخیص آواتارها از کاربران آنها ضروری خواهد بود، به ویژه در مواردی که آواتارها توسط برنامه نویسان برای اهداف تجاری ایجاد می‌شوند. مهم است که اقدامات این آواتارها، حتی اگر مبتنی بر هوش مصنوعی باشد، بدون اینکه لزوماً برنامه نویس را مقصر بدانیم، پاسخگو بدانیم. [۲۹]

حفاظت از متاورس مستلزم سازوکارهایی جهت حفاظت از داده‌ها و حریم خصوصی، حقوق مالکیت، پرداخت مالیات و نظارت بر ایجاد هویت‌های چندگانه می‌باشد، چنین مقرراتی باید حریم خصوصی و امنیت را متعادل کنند، کارشناسانی در خصوص نظارت بر فعالیت‌ها به ویژه جرایم جنسی علیه کودکان برای گزارش‌دهی و هشدار وجود داشته باشند، تا از وقوع این جرایم جلوگیری شود چرا که فرا فضایی بودن

متاورس ممکن است ارتکاب جرایمی مانند جرایم مذکور در این نوشتار را آسان‌تر کند و استفاده از آواتارها ممکن است به پنهان‌کردن فعالیت مجرم کمک کند. ترکیب فیزیکی - مجازی ممکن است به این معنی باشد که اثرات این جرایم (مانند جنایات ناشی از نفرت، آزار و اذیت، و تعقیب) محدود به تأثیرگذاری بر قربانیان در دنیای مجازی نیست، بلکه ممکن است آنها را در زمینه‌های دنیای واقعی نیز تحت تأثیر قرار دهد. در حالی که بسیاری از جرایم فوق، قابل‌تحقق می‌باشند، انگیزه سایر اشکال جرم به‌وضوح مالی است، به طور کلی‌تر، در این زمینه نیاز به شناسایی نقش‌ها و مسئولیت‌های ذی‌نفعان و افراد وجود خواهد داشت و بررسی این موضوع که آیا مدل‌های نظارتی کنونی کارایی لازم را دارند یا خیر. بایستی ابر کنترل‌کننده‌هایی در این زمینه پیش‌بینی گردند که مانند مدیران یا نگهبانان نقش حراست از فضای متاورس را ایفا کنند و بازیگران مخرب را از فعالیت ممنوع کنند و اطمینان حاصل کنند که متاورس با قوانین و مقررات مطابقت دارند و رویه‌هایی برای ایمن نمودن پرداخت‌ها و رمزنگاری‌های قوی در نظر گرفته شود تا جرایم مالی به حداقل برسد. تکنیک‌هایی برای شناسایی موارد سوءاستفاده جنسی از کودکان در نظر گرفته شود و بازارهای قابل‌اعتماد برای خریدوفروش دارایی‌های مجازی تعیین گردند. [۳۰]

نتیجه‌گیری

تبلیغات زیادی در مورد متاورس وجود دارد و سرمایه‌گذاری زیادی روی آن انجام می‌گردد، این پژوهش با بررسی تسهیل وقوع جرایم و شناسایی تهدیدات جنایی که متاورس ممکن است وقوع آن‌ها را تسهیل کند و جرم‌شناسی آن‌ها در تلاش برای ارائه راهکارهایی جهت افزایش امنیت این فضا بوده است. رفتارهای مجرمانه در متاورس می‌تواند شامل تقلب و کلاهبرداری باشد شامل، کلاهبرداری‌های مالی، فیشینگ و فروش کالاهای جعلی یا غیرواقعی می‌شود. هکرها ممکن است سعی کنند به حساب‌های کاربران نفوذ کنند و اطلاعات شخصی یا دارایی‌های دیجیتال را سرقت کنند. جمع‌آوری غیرمجاز اطلاعات شخصی کاربران یا نقض حریم خصوصی آن‌ها نیز یکی دیگر از اشکال جرایم در فضای متاورس می‌باشد. خراب‌کردن یا تخریب دارایی‌های دیجیتال دیگران، مانند آثار هنری یا ساختمان‌ها در محیط‌های مجازی نیز امکان‌پذیر است. رفتارهای آزاردهنده، تهدیدآمیز یا توهین‌آمیز نسبت به دیگر کاربران نیز از اشکال دیگر جرایم در این حوزه می‌باشد. فروش مواد مخدر، سلاح، یا سایر کالاهای غیرقانونی در محیط‌های واقعیت مجازی، انتشار محتوای مستهجن، تجاوز، تأمین مالی تروریسم و جاسوسی، جرایم مالیاتی و... نیز از دیگر جرایمی است که در فضای متاورس قابل‌تحقق است و این رفتارهای مجرمانه می‌توانند تبعات قانونی و اجتماعی جدی داشته باشند و نیاز به نظارت و مدیریت مناسب دارند. کاهش جرایم در متاورس نیازمند رویکردی جامع و چندجانبه است که به بررسی ابعاد مختلف این فضا و چالش‌های آن می‌پردازد.

قوانین و مقررات باید به طور خاص برای متاورس طراحی شوند. این قوانین باید شامل مجازات‌های سنگین برای جرایم جنسی، کلاهبرداری، هک و سایر رفتارهای غیرقانونی باشند. همکاری بین کشورها برای ایجاد یک چارچوب قانونی جهانی نیز ضروری است .ایجاد سیستم‌های نظارتی که به کاربران اجازه دهند رفتارهای مشکوک را گزارش کنند، می‌تواند به شناسایی سریع جرایم کمک کند. این سیستم‌ها باید به طور مداوم به‌روزرسانی شوند و پاسخگویی سریع به گزارش‌ها را

تضمین کنند. استفاده از فناوری‌های پیشرفته برای شناسایی و مسدودکردن محتوای غیر مناسب، به‌ویژه برای کودکان، می‌تواند به کاهش دسترسی به محتوای خطرناک کمک کند. این فناوری‌ها باید به طور مداوم به‌روز شوند تا با محتوای جدید مقابله کنند. برگزاری کارگاه‌ها و دوره‌های آموزشی می‌تواند به افزایش آگاهی عمومی کمک کند. استفاده از سیستم‌های احراز هویت قوی برای شناسایی کاربران واقعی و جلوگیری از ایجاد حساب‌های جعلی می‌تواند به کاهش جرایم کمک کند. این مکانیزم‌ها باید شامل تأیید هویت یا تأیید دو مرحله‌ای باشند. ایجاد محیط‌های مجازی امن که در آن‌ها کودکان و نوجوانان بتوانند بدون ترس از آزار و اذیت فعالیت کنند، ضروری است. این محیط‌ها باید شامل ابزارهای نظارتی و کنترل والدین باشند. ارائه راهکارهای حفظ حریم خصوصی قوی به کاربران، به‌ویژه کودکان، می‌تواند کنترل بیشتری بر روی اطلاعات شخصی آنان فراهم کند. این گزینه‌ها باید شامل تنظیمات مربوط به‌اشتراک‌گذاری اطلاعات و تعامل با دیگر کاربران باشد. همکاری با سازمان‌های حقوق بشری و نهادهای اجتماعی برای توسعه سیاست‌های مؤثر در زمینه حفاظت از حقوق کودکان و دیگر گروه‌های آسیب‌پذیر ضروری است. با توجه به پیچیدگی‌های متاورس و چالش‌های جدیدی که در این فضا ایجاد می‌شود، نیاز است که اقدامات پیشگیرانه و واکنش‌های سریع مورد توجه قرار گیرند. در نهایت، ایجاد یک فضای امن و سالم در متاورس مستلزم همکاری همه‌جانبه بین کاربران، شرکت‌ها، دولت‌ها و سازمان‌های غیردولتی است و تنها با یک رویکرد جامع و همگرا می‌توان از پتانسیل‌های مثبت متاورس بهره‌برداری کرده و خطرات آن را کاهش داد.

سپاسگزاری

از معاونت محترم پژوهشی به خاطر حمایت معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود.

از آقای دکتر عبدالله علیزاده به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.

از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.

نگارندگان بر خود لازم می‌دانند از آقای دکتر محمد رسول آهنگران به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

منابع

منابع:

۱-Kashmir Hill, *This Is Life in the Metaverse*, N.Y. TIMES (Oct. ۷, ۲۰۲۲), **https://www.nytimes.com/۲۰۲۲/۱۰/۰۷/technology/metaverse-facebook-horizon-worlds.html [https://perma.cc/U٦٥G-LVQ٨]**

۲-https://www.interpol.int/en/News-and-**Events/News/۲۰۲٤/Grooming-radicalization-and-cyber-attacks-INTERPOL-warns-of Metacrime#:~:text=Contributing%۲۰towards%۲۰a%۲۰secure%۲Dby,and%۲۰robbery%۲۰from%۲۰an%۲۰avatar.**

۳-https://www.techtarget.com/whatis/feature/The-**metaverse-explained-Everything-you-need-to-know**

۴-Aynur Aydın (۲۰۲۳). Tree-dimensional law metaverse law. **Available at: https://www.researchgate.net/publication/۳٦٨٤٦٩٢٩٧_THREE-DIMENSIONAL_LAW_METAVERSE_LAW**

۵- ristova, I. B., Baranov, O. A., Dz'oban, O. P., & Beliakov, K. I. **(۲۰۱۹). Legal Liability for Offenses in the Information Sphere**

۱۵– Mary Anne Franks, "Unwilling Avatars: Idealism and **Discrimination in Cyberspace," Columbia Journal of Gender and Law, Vol. ۲۰, October ۲۱, ۲۰۰۹, https://ssrn.com/abstract=۱۳۷٤٥۳۳**

۱۶– B.C. Cheong, "Avatars in the Metaverse: potential legal **issues and remedies," International Cybersecurity Law Review, June ۷, ۲۰۲۲, https://doi.org/۱۰,۱۳٦٥/s٤۳٤۳۹-۰۲۲-۰۰۰٥٦-۹**

۱۷– Annison, T. (۲۰۲۲). Elliptic Metaverse Report ۲۰۲۲ – The **Future of Financial Crime in the Metaverse: Fighting Crypto-crime in Web۳,۰. Elliptic. https://www.elliptic.co/hubfs/Crime%۲۰in%۲۰the%۲**۰Metaverse٪۲۰۲۰۲۲٪۲۰final.pdf〉 . Accessed on **۱۲/۰۸/۲۰۲۲.Google Scholar**

۱۸– Huq, N., Reyes, R., Lin, P., & Swimmer, M. (۲۰۲۲). Metaverse **or metaworse? Cybersecurity Threats Against the Internet of Experiences. Trend Micro Research. https://documents.trendmicro.com/assets/white_papers /wp-metaverse-or-metaworse-cybersecurity-threats-against-the-internet-of-experiences.pdf. Accessed on ۳۱/۰۸/۲۰۲۲.**

Google Scholar

۱۹– S. Goossens, C. Morgan, C. Kuru, F. Ji, D.J. Cespedes, **Protecting intellectual property in the metaverse, Intellectual Property & Technology Law Journal, ۳۳ (۹) (۲۰۲۱), pp. ۱۱-۱٦.Google Scholar**

۲۰– ell, C. (۲۰۲۲, Mar. ۲۸). The metaverse is coming. Here are **the cornerstones for securing it. Official Microsoft Blog. 〈 https://blogs.microsoft.com/blog/۲۰۲۲/۰۳/۲۸/the-metaverse-is-coming-here-are-the-cornerstones-for-securing-it/〉 . Accessed on ۱۲/۰۸/۲۰۲۲.**

Google Scholar

۲۱– S. Banaeian Far, A. Imani Rad Applying digital twins in **metaverse: User interface, security and privacy challenges Journal of Metaverse, ۲ (۱) (۲۰۲۲), pp. ۸-۱٦.**

View in ScopusGoogle Scholar

۲۲– Pinnock, B. (۲۰۲۲, Jul. ۲۶). The metaverse will not be **immune to cyber threats. The Mail & Guardian. 〈 https://mg.co.za/opinion/۲۰۲۲–۰۷-۲٦-the-metaverse-will-not-be-immune-to-cyber-threats/〉 . Accessed on ۱۲/۰۸/۲۰۲۲.**

and the Basics of Information Tort Law: A Monograph, ۳٤٤ p. ISBN ۹۷۸-٦۱۷-٦۹۷-۱۰۰-۹.

۶– L.E. Cohen, M. Felson, Social change and crime rate **trends: A routine activity approach, American Sociological Review (۱۹۷۹), pp. ٥۸۸-٦۰۸, View at publisherCrossrefGoogle Scholar**

۷– D.B. Cornish, R.V. Clarke, Understanding crime **displacement: An application of rational choice theorym Criminology, ۲٥ (٤) (۱۹۸۷), pp. ۹۳۳-۹٤۸, View at publisher.**

۸– C. Craig, Risk management in a policy environment: The **particular challenges associated with extreme risks, Futures, ۱۰۲ (۲۰۱۸), pp. ۱٤٦-۱٥۲.**

۹– Donets, A. G. (۲۰۲۲). Doctrinal view on the issues of legal **regulation of virtual worlds, "metaverse" private law doctrine: traditions and modernity. Proceedings of the XX Scientifc and Practical Conference dedicated to the ۱۰۰th anniversary of Doctor of Law, Professor, Corresponding Member of the Ukrainian SSR Academy of Sciences, Rector of Kharkiv Law Institute (۱۹٦۲–۱۹۸۷ pp.). P. ۳–۷.**

۱۰– VIRTUAL WORLD, REAL CHALLENGES, *supra* note ۲, at ۱۰. **South Korea is currently pioneering the metaverse for public service delivery. Danny Park, *South Korea Launches Online Metaverse Replica of Capital City Seoul to Improve Public Services*, FORKAST (Jan. ۱۷, ۲۰۲۳, ٤:۰٥ PM),https://forkast.news/headlines/south-korea-metaversecapital-city-seoul [https://perma.cc/BY٦Q-٥۴□□].**

۱۱– Bettina M. Chin, Note, *Regulating Your Second Life: **Defamation in Virtual Worlds*, ۷۲ BROOK. L. REV. ۱۳۰۳, ۱۳۰۹ (۲۰۰۷).**

۱۲– Casey Newton, *Mark in the Metaverse*, VERGE (July ۲۲, ۲۰۲۱, ۱۰:۰۰ AM), **https://www.theverge.com/۲۲٥۸۸۰۲۲/mark-zuckerberg-facebook-ceo-metaverse-interview[https://perma.cc/٦۹۲Z-HXYK]**

۱۳– Was Virtually 'Groped' in Meta's VR Metaverse, *N.Y. **POST, https://nypost.com/2021/12/17/woman-claims-she-was-virtually-groped-in-meta-vrmetaverse [https://perma.cc/AYG9-CVX7] (Dec. 17, 2021, 3:35 PM)***

۱۴–https://www.bbc.com/news/blogs–trending–۴۷۴۸۴۳۹۷[https://perma.cc/A٥SS–۴L۲A]

Google Scholar

۲۳– Reed, N., & Joseff, K. (۲۰۲۲). Kids and the Metaverse: What **Parents, Policymakers, and Companies Need to Know.**

https://www.commonsensemedia.org/sites/default/files/featured-content/files/metaverse-white-paper.pdf. Accessed ۱۲/۰۸/۲۰۲۲.

Google Scholar

۲۴–Buck, L., & McDonnell, R. (۲۰۲۲). Security and Privacy in the **Metaverse: The Threat of the Digital Human. ACM CHI Conference on Human Factors in Computing Systems. Session: SSPXR - Novel Challenges of Safety, Security and Privacy in Extended Reality, Online.Google Scholar**

۲۵–
https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/the-metaverse-virtual-offences-real-world-penalties

۲۶– Allen, C., & McIntosh, V. (۲۰۲۲). Safeguarding the **metaverse: A guide to existing and future harms in virtual reality (VR) and the metaverse to support UK immersive technology policymaking.**

〈
https://www.theiet.org/impactsociety/factfiles/information-technology-factfiles/safeguarding-the-metaverse/〉 . Accessed on ۱۲/۰۸/۲۰۲۲.

Google Scholar

۲۷– Di Pietro, R., & Cresci, S. (۲۰۲۱). Metaverse: Security and **Privacy Issues. ۲۰۲۱ Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA),Google Scholar**

۲۸–https://www.vox.com/the–**bigidea/۲۰۱۸/۱/۲/۱٦۸٤۰۲۹٤/groping-sexual-assault-franken-law-punishment[https://perma.cc/۹٦F٥-۸UPG].**

۲۹– https://www.orfonline.org/research/crime–and–**punishment-in-the-metaverse-a-primer**

۳۰–
https://www.sciencedirect.com/science/article/pii/S۰۰۱٦۳۲۸۷۲۴۰۰۰۲۱۱