Iranian Journal of Public Policy
2025 , Vol. 11 , No. 1 , 56-72
Online ISSN: 2538-5089
Home Page: jppolicy.ut.ac.ir

RESEARCH ARTICLE

Feasibility Study of the Realization of the Idea of Meta Criminal Law with an Approach to the Metaverse

Mahdi Karimi

Assistant Professor of Law, Faculty of Law and Social Sciences, University of Payam e Noor, Tehran, Iran

Corresponding Author's Email: m.karimi342@pnu.ac.ir

https://doi.org/10.22059/jppolicy.2025.101190

Received: 27 July 2024
Accepted: 30 September 2024

ABSTRACT

With the emergence of new technologies and the expansion of virtual spaces, criminal law has faced new challenges. The author suggests creating a new branch titled "Meta Criminal Law" and proposes that legislators at national and international levels establish the substantive and procedural aspects of this field based on a criminal policy framework. The article examines the concept of meta criminal law, the opportunities and necessity of its formation, and its role in combating crimes in cyberspace. Using an analytical-descriptive method and library studies, it analyzes the current situation and future of meta criminal law. The article addresses the threats that could form the basis of criminal behaviors in the metaverse space and emphasizes that despite concerns about crime formation in the metaverse, there are inherent capabilities in the metaverse that can be used across a broad spectrum, including a criminal policy ranging from meta-criminal trials to the social rehabilitation of criminals and even virtual imprisonment.

Keywords:. Metaverse, Meta Criminal Law, Virtual Reality, Virtual Crimes, Virtual Legal Laboratories.

Citation: Karimi, Mahdi (2025). Feasibility Study of the Realization of the Idea of Meta Criminal Law with an Approach to the Metaverse. *Iranian Journal of Public Policy,* 11 (1), 56-72.
DOI: https://doi.org/10.22059/jppolicy.2025.101190

Published by University of Tehran.

فصلنامه سیاستگذاری عمومی

دوره ۱۱، شماره ۱، بهار ۱۴۰۴. صفحات ۷۲-۵۶

شاپا الکترونیکی: ۵۰۸۹ - ۲۵۳۸

آدرس سایت: jppolicy.ut.ac.ir

مقاله پژوهشی

امکان‌سنجی تحقق ایده حقوق متاکیفری با رویکردی بر متاورس

مهدی کریمی

استادیار حقوق، دانشکده حقوق و علوم اجتماعی، دانشگاه پیام نور، تهران، ایران

رایانامه: m.karimi342@pnu.ac.ir

تاریخ دریافت: ٦ مرداد ١٤٠٣
تاریخ پذیرش: ٩ مهر ١٤٠٣

https://doi.org/10.22059/jppolicy.2025.101190

چکیده

با ظهور فناوری‌های نوین و گسترش فضاهای مجازی، حقوق کیفری با چالش‌های جدیدی مواجه شده است. نویسنده پیشنهاد می‌کند شاخه جدید تحت عنوان حقوق متاکیفری ایجاد شود و قانون‌گذاران در عرصه ملی و بین‌المللی جنبه‌های ماهوی و شکلی این رشته را بر مبنای یک سیاست کیفری پایه‌گذاری نمایند. مقاله به بررسی مفهوم حقوق متاکیفری فرصت‌ها و ضرورت شکل‌گیری و نقش آن در مقابله با جرائم در فضای مجازی می‌پردازد و با استفاده از روش تحلیلی-توصیفی و مطالعات کتابخانه‌ای به تحلیل وضعیت موجود و آینده حقوق متاکیفری می‌پردازد. بر این اساس، تهدیدهایی که می‌تواند مبنای رفتارهای مجرمانه در فضای متاورس باشد مورد توجه قرار گرفته و تأکید می‌شود علی‌رغم نگرانی‌هایی که در زمینه متاورس برای شکل‌گیری جرایم وجود دارد، قابلیت‌هایی در ذات متاورس هست که می‌توان از آنها در طیفی گسترده مشتمل بر یک سیاست کیفری از محاکمات متاکیفری تا بازاجتماعی‌کردن مجرمین و حتی حبس مجازی استفاده کرد.

واژگان کلیدی: متاورس، حقوق متاکیفری، واقعیت مجازی، جرایم مجازی، چهرک ، آزمایشگاه‌های حقوقی مجازی.

استناد: کریمی، مهدی (۱۴۰۴). امکان‌سنجی تحقق ایده حقوق متاکیفری با رویکردی بر متاورس. *فصلنامه سیاستگذاری عمومی*، ۱۱ (۱)، ۷۲-۵۶.
DOI: https://doi.org/10.22059/jppolicy.2025.101190

ناشر: دانشگاه تهران.

مقدمه

علی‌رغم نقدهای مطرح شده در خصوص متاورس[1]، این موضوع همچنان یکی از مباحث داغ در میان صاحب‌نظران و رسانه‌ها به شمار می‌رود. برخلاف نسل قبلی طرح‌های مبتنی بر اینترنت، متاورس به طور چشمگیری مورد توجه نویسندگان مختلفی قرارگرفته‌است. در جامعه مدرن دنیای فیزیکی دیگر تنها عرصه منحصر به فرد فعالیت‌های انسانی نیست بلکه تحت تأثیر پیشرفت‌های فناوری، تغییرات مهمی در تلاش‌های انسانی ایجاد شده است. به مدد فضای مجازی می‌توانیم اکثر قریب به اتفاق فعالیت‌هایی که در دنیای فیزیکی پیش از این انجام می‌دادیم، اکنون در این قلمرو انجام دهیم. این امر بر تطبیق‌پذیری و دامنه بالقوه فعالیت‌های انسانی در حوزه دیجیتال دلالت می‌کند. این فعالیت‌ها در فضای مجازی، چالش‌های حقوقی و پیامدهای گوناگون برای حقوق کیفری به همراه دارد. لذا حقوق کیفری به شکلی ویژه می بایستی به آن‌ها پاسخ دهد(Brenner, 2012: 58) نیاز برای ایجاد قوانین و چارچوب‌های قانونی حاکم بر استفاده و عملکرد متاورس و قانونمند کردن آن امری اجتناب‌ناپذیر است و اقدامات نظارتی را ایجاب می‌کند، عوامل مختلفی مانند ملاحظات اخلاقی، ایمنی کاربران، نگرانی‌های مربوط به حریم خصوصی، پیامدهای اقتصادی و تأثیرات بالقوه اجتماعی می‌توانند بر این امر تأکید کنند. متاورس طیف وسیعی از فعالیت‌های دیجیتال را گردهم آورده است که کاربر می‌تواند مجموعه متنوعی از آنها را تجربه کند.این فعالیت‌ها می‌تواند شامل تجربیات واقعیت مجازی[2]، واقعیت افزوده[3]، تعاملات اجتماعی آنلاین، تجارت دیجیتال، بازی، جلسات مجازی و سایر اشکال تعامل دیجیتال باشد. تنوع روابط اجتماعی در متاورس و افزایش تعداد کاربران، دسته جدیدی از خطرات و تهدیدها را برای انسان به همراه دارد و حقوق و آزادی‌های آنها را به خطر می‌اندازد. در حال حاضر، حقوق کیفری بر جرائمی تمرکز دارند که در دنیای واقعی و فیزیکی رخ می‌دهند. همچنین قوانین مرتبط با جرائم رایانه‌ای و فضای مجازی بیشتر بر جرائمی متمرکز هستند که از طریق رایانه و اینترنت انجام می‌شوند. کاربران فضای مجازی متاورس بسیار آسیب‌پذیر و شکننده هستند. این آسیب‌پذیری ناشی از چند عامل است که دو مورد بارز و مهم آن عبارت‌اند از: انواع رفتارهای جدید جرایم سایبری که با ویژگی‌های قلمرو واقعیت مجازی و واقعیت افزوده سازگار شده‌اند و فقدان قوانین، مقررات و چارچوب‌های حقوقی لازم. در عصر حاضر با گسترش روزافزون فناوری‌های دیجیتال و ظهور فضاهای مجازی مانند متاورس، مفهوم جرم و مجازات با چالش‌های جدی روبرو شده است(Jathavedan, 2022: 69) . حقوق متاکیفری، به عنوان شاخه‌ای نوظهور از حقوق کیفری، به دنبال پاسخگویی به این چالش‌ها و تنظیم روابط حقوقی در فضای مجازی است. این حوزه، که در تقاطع حقوق کیفری وفناوری اطلاعات قرار دارد، با مسائل پیچیده‌ای مواجه است که نیازمند بررسی دقیق و جامع می‌باشد. در این راستا این مقاله به دنبال پاسخگویی به سؤالات زیر است: ۱. حقوق متاکیفری چگونه می‌تواند با چالش‌های ناشی از جرائم در فضای مجازی و متاورس مقابله کند؟ ۲. آیا مفاهیم سنتی جرم و مجازات در فضای متاورس قابل اعمال هستند؟ ۳- تهدیدهای ناظر بر حقوق متاکیفری با توجه به گذار از مفاهیم سنتی حقوق جزا چیست و چگونه شکل می‌گیرند؟ ۴- فرصت‌ها و ضرورت شکل‌گیری حقوق متاکیفری چیست؟ بر اساس مطالعات اولیه و بررسی ادبیات موجود، فرضیه‌های زیر مطرح می‌شوند: ۱. حقوق متاکیفری نیازمند تدوین اصول و قواعد جدیدی است که متناسب با ماهیت فضای مجازی و متاورس باشد. ۲. اعمال مفاهیم سنتی جرم و مجازات در فضای متاورس بدون تغییرات اساسی امکان‌پذیر نیست و نیاز به بازتعریف دارد. ۳- تهدیدهای ناظر بر حقوق متاکیفری در طیف وسیع وگستره‌ای از متاورس شکل می‌گیرند. ۴- حقوق متاکیفری فرصت‌های بی‌شمار و عدیده

1. Metaverse
2. (VR) Virtual Reality

واقعیت مجازی این امکان را می‌دهد تا با استفاده از دستگاه‌های الکترونیکی مانند هدست‌های واقعیت مجازی، کنترل‌کننده‌ها و دستکش در یک محیط سه بعدی مصنوعی تعامل داشته باشید

3. (AR) Augmented Reality

واقعیت افزوده (AR) تعامل بین یک تجربه مجازی و دنیای واقعی را توصیف می کند. این محیط واقعی را با تصاویر، انیمیشن یا متن بهبود می بخشد. می‌توان آن را از طریق عینک‌های هوشمند AR، تبلت‌ها و گوشی‌های هوشمند تجربه کرد

ای را فراروی نظام عدالت کیفری همانند محاکمات متاکیفری تا بازاجتماعی‌کردن مجرمین و حتی حبس مجازی قرار می‌دهد و این فرصت‌ها مبانی ضروری شکل‌گیری حقوق متا کیفری را توجیه می‌کند.

مفهوم حقوق متاکیفری، اگرچه جدید است، اما ریشه در مطالعات پیشین در زمینه حقوق سایبری و جرائم رایانه‌ای دارد. در دهه ۱۹۹۰، با گسترش اینترنت، اولین مطالعات جدی در مورد جرائم سایبری آغاز شد. کتاب جرائم کامپیوتری و امنیت سایبری (Grabosky& Smith,1998:125) یکی از اولین آثار جامع در این زمینه بود که به بررسی چالش‌های حقوقی ناشی از فناوری‌های نوین پرداخت. در اوایل قرن ۲۱، با پیشرفت فناوری‌های وب ۲,۰ و شبکه‌های اجتماعی، مفهوم هویت دیجیتال و جرائم مرتبط با آن مورد توجه قرار گرفت. مقاله هویت دیجیتال و چالش‌های حقوقی(67: 2007, Wall) آن به بررسی این موضوع پرداخت و زمینه را برای مطالعات بعدی در حوزه حقوق متاکیفری فراهم کرد. با ظهور ارزهای دیجیتال و فناوری بلاک‌چین، مطالعات جدیدی در زمینه جرائم مالی در فضای مجازی شکل گرفت. کتاب حقوق کیفری در عصر بلاک‌چین (Muharem , 2018 : 72) به بررسی چالش‌های حقوقی ناشی از این فناوری‌ها پرداخت و مفاهیم اولیه حقوق متا کیفری را مطرح کرد. مقاله سیاست جنایی ایران در فضای سایبر به بررسی سیاست جنایی ایران با حلول فضاهای مجازی پرداخته است(Mahdavi sabet & Mordi, 2017: 101) . در سال‌های اخیر، با مطرح شدن مفهوم متاورس، مطالعات در این زمینه شتاب بیشتری گرفته است. مقاله چالش‌های حقوقی متاورس (Lee,et al, 2022:234) به بررسی جنبه‌های مختلف حقوقی در فضای متاورس پرداخته و ضرورت تدوین قوانین جدید را مطرح کرده است مقاله مسائل حقوقی نوظهور در فضای سه بعدی متاورس (Lalalizadeh, 2023, 86) به جنبه های حقوقی متاورس پرداخته است. موضوع دیگری که در ادبیات حقوق متاکیفری مورد توجه قرار گرفته، استفاده از هوش مصنوعی در پیشگیری و کشف جرائم است. کتاب هوش مصنوعی و عدالت کیفری به بررسی جنبه‌های مختلف استفاده از هوش مصنوعی در سیستم عدالت کیفری پرداخته و چالش‌های اخلاقی و حقوقی آن را مورد بحث قرار داده است (Bryden 2024 : 48) . با توجه به گسترش روزافزون فعالیت‌های انسانی در فضای مجازی و ظهور پدیده‌هایی مانند متاورس، اهمیت مطالعه و تدوین قوانین متناسب با این فضا بیش از پیش آشکار می‌شود. حقوق متاکیفری به عنوان یک حوزه نوظهور، می‌تواند نقش مهمی در تنظیم روابط حقوقی و مقابله با جرائم در فضای مجازی ایفا کند. تشکیل شاخه جدیدی از حقوق کیفری که بتواند پاسخگوی تمام این ضروریات باشد امری لازم به نظر می‌رسد. با توجه به قابلیت های متاورس و ضرورت پاسخگویی حقوق کیفری به مقتضیات فوق الذکر تشکیل رشته حقوق متا کیفری توسط نویسنده پیشنهاد شده است. بدیهی است که در این راستا پرداختن به جنبه‌های گوناگون این رشته، توجه به فرصت‌هایی که می‌تواند در گستره این الزامات در اختیار اندیشمندان قرار دهد و از سویی دیگر ذکر طیف گسترده‌ای از تهدیدهایی که با آن مواجه است و برخی از آنها منحصر به فضای متاورس و دنیای دیجیتال هستند ضروری است. پیش از بیان تهدیدها، فرصت‌ها و ضرورت مذکور در خصوص حقوق متا کیفری در ابتدا به برخی مفاهیم اشاره می‌کنیم.

واژه شناسی متاورس

اصطلاح متاورس از پیشوند یونانی"متا" (*meta* اصطلاح یونانی به معنای فراتررفتن) و پسوند "ورس" (مخفف *Universe* به معنای "جهان") ترکیب شده است. این اصطلاح به یک دنیای تولید شده توسط رایانه اشاره دارد که با یک سیستم ارزشی سازگار و سیستم اقتصادی مستقل توصیف شده است و به طور پیچیده‌ای با دنیای فیزیکی در ارتباط است (Wang, et al ,2022 :340) به عبارت دیگر متاورس به طیف گسترده‌ای از فناوری‌هایی اطلاق می‌شود که هدف آنها ادغام ارتباطات اجتماعی دنیای واقعی با نوآوری‌های عصر دیجیتال است(Zhou, et al, 2022:46) . اصطلاح متاورس اولین‌بار در رمان علمی- تخیلی ضد آرمان شهر

سال ۱۹۹۲ نوشته نیل استفنسون [۱] با عنوان «سقوط برف»[۲] به کار رفته است. این کتاب جهانی را توصیف می‌کند که در آن دولت‌ها جای خود را به شرکت‌ها داده‌اند، اقتصاد جهانی سقوط کرده است، در حالی که شهروندان با دسترسی به دنیای مجازی از طریق هدست از این واقعیت تلخ فرار می‌کنند. درچنین محیطی، انسان‌ها از طریق آواتارهای[۳] خود می‌توانند در قلمرو دیجیتال وقت بگذارنند و مالکیت مجازی داشته باشند و با آواتارهای دیگر افراد ارتباط برقرار کنند. این آینده ضدآرمان شهر که نویسنده تصور کرده است، با اساس پیدایش و توسعه متاورس در دنیای واقعی مطابقت ندارد. بلکه با افزایش دیجیتالی‌شدن و پیدایش فناوری‌ها و نوآوری‌های متعدد جدید مانند دارایی‌های رمزنگاری شده[۴] و بلاک‌چین[۵]، که به آن‌ها "وب ۳/۰" می‌گویند، شکل گرفته است. اصطلاح متاورس یک پلتفرم واقعیت توسعه‌یافته[۶] در نظر گرفته می‌شود که شامل طیف گسترده‌ای از تجربیات و تعاملات مجازی است و فراتر از واقعیت فیزیکی است و خطوط بین دنیای دیجیتال و فیزیکی را محو می‌کند و در حال حاضر با چندین چالش از جمله مسائل مربوط به ویروس‌ها و ناتوانی در اعمال محدودیت‌های سنی برای کاربران به دلیل وجود بازی‌های مجازی زیادی در متاورس مواجه است. علاوه بر این، رشد کاربران و شرکت‌ها، این فضای مجازی را به شدت شلوغ کرده و در نتیجه تنظیم و برنامه‌ریزی آینده آن، دشوار گردیده است (Carissoli,et al , 2022 :63) .

متاورس و حقوق کیفری

با توجه به خطراتی که کاربران در متاورس با آن روبرو هستند، ضروری است که قبل از اینکه این فناوری به طور گسترده در زندگی ما نفوذ کند، سریعاً درباره قوانین و مقرراتی که باید در این فضاهای مجازی اعمال شوند، بحث و تصمیم‌گیری کنیم. این کار به منظور محافظت از کاربران و ایجاد یک محیط امن و قانونمند در متاورس است. به نظر می‌رسد، اعمال قوانین کیفری دنیای واقعی در فضای متاورس به سه شرط بستگی دارد: الف) اراده طراحان و مالکان پلتفرم متاورس از طریق برنامه‌ها و الگوریتم‌هایی که توسط ایشان ایجاد شده: به عبارت دیگر، شرایط و ضوابط تعیین‌شده برای استفاده از پلتفرم بخشی از چارچوب حقوقی محسوب می‌شود که طراحان و توسعه‌دهندگان متاورس با اعمال نظر خود از طریق کدنویسی، تعیین‌کننده قوانین و محدودیت‌های حاکم بر این فضا هستند(Lee, 2024 :101) ب) نوع یکسان‌بودن عمل: منظور این است که آیا رفتار مجرمانه‌ای که در فضای مجازی

1. Neal Stephenson
2. Snow Crash
3. Avatar

چهرک یا آواتار، از زبان سانسکریت گرفته شده است. آنجا अवतार (آواتارا) به معنای "نزول" است که به نزول یک خدا به کره زمین اشاره دارد. آواتارها تصاویری هستند که کاربران در اینترنت و به خصوص در تالار گفتگو برای پروفایل خود استفاده می‌کنند. کاربران عموما از آواتار خود در شبکه های اجتماعی، بازی‌های کامپیوتری و فضای مجازی استفاده می‌کنند. این تصویر جایگزین تصویر واقعی فرد می باشد و افراد در صورتی از آن استفاده می‌کنند که تمایلی به انتشار تصویر واقعی خود نداشته باشند.

4. Cryptocurrency Assets

به دارایی‌های دیجیتال یا مجازی اشاره دارد که از رمزنگاری برای امنیت استفاده می‌کنند و در شبکه‌های غیرمتمرکز، معمولاً مبتنی بر فناوری بلاک چین، کار می‌کنند. این دارایی‌ها نمایش دیجیتال یا مجازی ارزش هستند و می توانند به عنوان وسیله مبادله، واحد حساب یا ذخیره ارزش مورد استفاده قرار گیرند. بیت کوین، اتریوم و سایر آلتکوین ها نمونه‌هایی از دارایی‌های رمزنگاری هستند. آنها توسط هیچ مقام مرکزی، مانند یک دولت یا موسسه مالی کنترل نمی شوند، که آنها را غیرمتمرکز می کند و اغلب با سطح بالایی از شفافیت و امنیت مشخص می‌شود.

5. Blockchain

اصطلاح "بلاک چین" به یک فناوری دفتر کل دیجیتال غیرمتمرکز و توزیع شده اشاره دارد. این سیستمی است از ثبت اطلاعات به گونه ای که تغییر، هک یا تقلب سیستم را دشوار یا غیرممکن می کند. یک بلاک چین از زنجیره ای از بلوک ها تشکیل شده است که هر بلوک حاوی لیستی از تراکنش ها است. این تراکنش ها از طریق هش های رمزنگاری ایمن شده و به هم مرتبط می شوند و یک زنجیره را تشکیل می دهند. فناوری بلاک چین در ابتدا برای پشتیبانی از ارزهای رمزنگاری شده مانند بیت کوین طراحی شد و به عنوان دفتر کل عمومی برای همه تراکنش ها عمل می‌کرد. با این حال، کاربردهای آن فراتر از ارزهای دیجیتال به صنایع مختلف از جمله مالی، مدیریت زنجیره تامین، مراقبت‌های بهداشتی و غیره گسترش یافته است.

6. (XR) Extended Reality

واقعیت توسعه‌یافته، به اختصار (XR)، یک اصطلاح جامع برای فناوری‌هایی است که دنیای واقعی را با یک شبیه‌سازی کامپیوتری جایگزین یا تقویت می‌کنند. این شامل سه فناوری همه جانبه واقعیت مجازی (Virtual Reality) (VR)، واقعیت افزوده (Augmented Reality) (AR) و واقعیت ترکیبی (Mixed Reality) (MR) است.

انجام می‌شود، شبیه و مشابه اعمالی است که معمولاً در دنیای واقعی به عنوان جرم شناخته می‌شوند یا خیر؟ در این زمینه، اصل قانونی‌بودن جرم[1] دخالت حقوق کیفری در این حوزه را محدود می‌کند. زیرا اَعمال انجام شده در قلمرو مجازی با اَعمال انجام شده در دنیای واقعی به سختی قابل مقایسه هستند و اِعمال حقوق کیفری در مواردی که هیچ چارچوب قانونی از قبل برای تعریف اَعمال انجام شده وجود ندارد، محدود می‌شود. در این راستا اگر اَعمال ارتکابی در فضای مجازی همان جرایم دنیای واقعی باشد، تحت قوانین موجود قرار می‌گیرد واگر متفاوت باشند، نیاز به قانون‌گذاری جدید در این حوزه است. ج) ایجاد یک نتیجه در دنیای واقعی: منظور این است که برای اینکه یک رفتار در فضای مجازی بتواند به عنوان جرم تلقی شود، باید پیامدی در دنیای واقعی داشته باشد. باید یک ارتباط و پیوند بین دنیای مجازی و دنیای واقعی وجود داشته باشد. در واقع باید بین نتیجه حاصله در دنیای واقعی با رفتار ارتکابی در فضای متاورس رابطه سببیت وجود داشته باشد تا یک رفتار مجازی بتواند به عنوان جرم طبقه‌بندی شود. با توجه به تمام این ملاحظات، برخی رفتارهای مجازی که به وضوح زیان‌آور یا خطرناک هستند، از جمله تجاوز مجازی، تخریب مجازی، قتل مجازی در حال حاضر نمی‌توانند در الگویی که توسط قواعد سنتی جرم‌انگاری ارائه شده است قرار گیرند (Brassel,2022 :54)علاوه بر این، قابل ذکر است که رشد و گسترش انواع خاصی از اَعمال مجرمانه توسط کاربران پلتفرم‌ها ومحققان مشاهده شده است مانند سرقت و آسیب‌رساندن دارایی‌های رمزنگاری‌شده. به عنوان مثال، الیپتیک[2] نشان داده است که قبلاً فعالیت‌های غیرقانونی در مورد دارایی‌های مورد استفاده در متاورس وجود داشته است از این فعالیت‌های غیرقانونی، ۹۹/۵٪ شامل سرقت ارزهای دیجیتال بوده است[3] . بدیهی است، این موارد نیازمند دخالت حقوق کیفری هستند و لیکن در حال حاضر، این امر از طریق اِعمال قوانین کیفری که عمدتاً برای جرائم ارتکابی در واقعیت مادی و فیزیکی، تعریف شده‌اند، محقق می‌گردد. در متاورس و دنیاهای مجازی آن، هنوز نمی‌توانیم در مورد اشخاص بحث کنیم زیرا از نظر قانونی، آواتارها وجود متمایز و جدا از افراد دنیای واقعی که آنها را کنترل می‌کنند، لحاظ نمی‌شوند. آنها صرفاً بیانگر هویت مجازی کاربران بوده و هنوز وجود مستقل قانونی ندارند بدین جهت حقوق متاکیفری با طیف گسترده‌ای از تهدیدات خاص که منحصردر فضای متاورس هستند مواجه می‌باشد که به شرح زیر طبقه بندی می‌شوند (Wang Su, et al,2022:319) .

تهدیدهای حقوق متاکیفری

جرائم سایبری پیشرفته

الف) سرقت هویت دیجیتال[4]: در متاورس، هویت دیجیتال افراد شامل آواتارها، حساب‌های کاربری، و دارایی‌های مجازی آنهاست. مجرمان ممکن است با استفاده از تکنیک‌های پیشرفته هک، فیشینگ یا مهندسی اجتماعی این هویت‌ها را سرقت کنند. آنها می‌توانند از این هویت‌های دزدیده شده برای دسترسی به اطلاعات شخصی، انجام معاملات غیرقانونی، یا حتی اخاذی استفاده کنند. این نوع سرقت می‌تواند پیامدهای جدی مالی و روانی برای قربانیان داشته باشد سرقت هویت در فضای مجازی (متاورس): منجر به از دست دادن آواتارها، دارایی دیجیتال، اطلاعات شخصی کاربر می‌گردد(Brown, 2024: 21).

ب) کلاهبرداری‌های پیچیده: کلاهبرداران در متاورس از فناوری‌های پیشرفته مانند هوش مصنوعی و واقعیت مجازی برای ایجاد طرح‌های فریبنده استفاده می‌کنند. این می‌تواند شامل ایجاد پروژه‌های سرمایه‌گذاری جعلی، فروش املاک مجازی غیرموجود، یا حتی ایجاد رویدادهای واقعیت مجازی ساختگی باشد. پیچیدگی این کلاهبرداری‌ها و ماهیت غوطه‌ور متاورس می‌تواند تشخیص واقعیت از فریب را برای کاربران دشوار کند. تهدید علیه مالکیت افراد بر روی دارایی‌ها و سرمایه‌گذاری‌های دیجیتالی خود مانند

1. "Nullum Crimen Sine Lege"

۲. Elliptic یک شرکت نرم‌افزاری امنیت سایبری است که بر روی تشخیص و پایش فعالیت‌های غیرقانونی مرتبط با ارزهای دیجیتال و بلاک‌چین تمرکز دارد.

3. Elliptic Metaverse Report, 2022, URL:https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf, accessed: 14.02.2023

4. Identity Theft

رمز ارزها، توکن‌های غیرقابل جایگزین و دیگر دارایی‌های باارزش در فضای مجازی مهمترین این‌گونه تهدیدها هستند (Alawadhi, 2024, 28).

پ) هک‌کردن اشیاء مجازی: در متاورس اشیاء مجازی می‌توانند ارزش قابل توجهی داشته باشند. هکرها ممکن است سعی کنند این اشیاء را دست‌کاری کنند، مثلاً با تغییر ویژگی‌های یک NFT [1] گران‌قیمت یا دسترسی غیرمجاز به ساختمان‌های مجازی خصوصی. این می‌تواند منجر به از دست رفتن دارایی‌ها، نقض حریم خصوصی یا حتی خرابکاری در رویدادها و تجربیات مجازی شود (Bertazzolo, 2023).

نقض حریم خصوصی

الف) جاسوسی دیجیتال: در متاورس هر تعامل، حرکت و حتی نگاه کاربر می‌تواند ردیابی و ثبت شود. جاسوسان دیجیتال ممکن است از این داده‌ها برای جمع‌آوری اطلاعات حساس استفاده کنند. این می‌تواند شامل الگوهای رفتاری، ترجیحات شخصی و حتی اطلاعات مالی باشد. برای مثال، یک جاسوس می‌تواند با تحلیل الگوهای خرید یک کاربر در متاورس، اطلاعات ارزشمندی درباره وضعیت مالی یا عادات شخصی او به دست آورد (Wang et al, 2022, 323).

ب) ردیابی بیومتریک: دستگاه‌های واقعیت مجازی و واقعیت افزوده اغلب داده‌های بیومتریک مانند حرکات چشم، الگوهای حرکتی و حتی ضربان قلب را جمع‌آوری می‌کنند. سوء استفاده از این داده‌ها می‌تواند پیامدهای جدی داشته باشد. برای مثال، الگوهای حرکت چشم می‌توانند برای تشخیص بیماری‌های خاص استفاده شوند

آزار و اذیت مجازی

الف) زورگویی سایبری پیشرفته[2]: در متاورس، زورگویی سایبری می‌تواند اشکال پیچیده‌تری به خود بگیرد. مهاجمان می‌توانند از آواتارهای خود برای محاصره، تهدید یا تحقیر قربانیان استفاده کنند. این تجربه می‌تواند به دلیل ماهیت غوطه‌ور واقعیت مجازی بسیار واقعی و آسیب‌زا باشد.

ب) تجاوز مجازی: این شکل خاص از آزار شامل نقض عمدی حریم شخصی و فضای مجازی یک کاربر بدون رضایت اوست. اگرچه فیزیکی نیست، اما می‌تواند آسیب روانی جدی ایجاد کند (El Asam & Muthanna, 2016, 136). برای مثال، یک آواتار ممکن است به فضای شخصی آواتار دیگری وارد شود و حرکات نامناسب انجام دهد. قربانیان ممکن است احساس ناتوانی و آسیب‌پذیری شدیدی را تجربه کنند.

پ) استاکینگ [3]در متاورس: این پدیده به رفتار آزاردهنده، تهدیدآمیز در متاورس اشاره دارد که در آن یک فرد سالکر به طور مداوم و ناخواسته فرد دیگری را در فضاهای مجازی تعقیب و آزار می‌دهد. در متاورس، این رفتار می‌تواند شامل موارد زیر باشد: تعقیب مداوم، نظارت مستمر، ارسال پیام‌های ناخواسته، ایجاد مزاحمت در تجربیات مجازی مانند خراب‌کردن تجربه‌های قربانی در فضاهای مجازی مانند رویدادها یا بازی‌ها. استاکرها[4] در متاورس می‌توانند قربانیان خود را در تمام فضاهای مجازی تعقیب کنند (Haber, 2024, 4). آنها ممکن است از ابزارهای ردیابی پیشرفته برای دنبال‌کردن حرکات قربانی در سراسر پلتفرم‌های مختلف

1. Non-Fungible Token
به معنای "توکن غیرقابل معاوضه" است. این اصطلاح به یک نوع دارایی دیجیتال منحصر به فرد اشاره دارد که با استفاده از فناوری بلاکچین ایجاد و مدیریت می‌شود
2. Cyberbullying
به معنای آزار و اذیت، تهدید، تحقیر یا ارعاب دیگران با استفاده از تکنولوژی و فضای مجازی است مانند ارسال پیام‌های تهدیدآمیز یا توهین‌آمیز، انتشار اطلاعات خصوصی یا شایعات در مورد فرد، ایجاد پروفایل‌های جعلی برای تمسخر دیگران، استفاده از عکس‌ها یا ویدیوهای شخصی برای تهدید یا شرمسار کردن افراد، محروم کردن عمدی افراد از گروه‌های آنلاین
3. Stalking
4. Stalker

استفاده کنند. این می‌تواند منجر به احساس ناامنی مداوم و استرس شدید برای قربانی شود، حتی در فضایی که قرار بود امن و سرگرم‌کننده باشد.

جرائم مالی

الف) پولشویی دیجیتال: متاورس با اقتصاد پیچیده و ارزهای مجازی خود، می‌تواند به بستری مناسب برای پولشویان تبدیل شود. مجرمان می‌توانند از معاملات پیچیده دارایی‌های مجازی، خرید و فروش NFTها یا توکن های غیر قابل معاوضه، حتی کازینوهای مجازی برای پنهان کردن منشأ پول‌های نامشروع استفاده کنند. پیچیدگی و ماهیت فراملی این معاملات، ردیابی و مقابله با آنها را برای مقامات قانونی دشوار می‌کند.

ب) کلاهبرداری در معاملات مجازی: این می‌تواند شامل فروش املاک مجازی غیرموجود، ارائه خدمات جعلی یا حتی ایجاد ارزهای دیجیتال تقلبی باشد. برای مثال، یک کلاهبردار ممکن است یک جزیره زیبا در متاورس را به فروش بگذارد، پول را دریافت کند و سپس ناپدید شود بدون اینکه هرگز مالکیت را منتقل کند(Chung,2024 :63).

نقض حقوق مالکیت معنوی

الف) کپی غیرمجاز اشیاء و طراحی‌های مجازی: در متاورس، طراحان و هنرمندان می‌توانند اشیاء، لباس‌ها و حتی فضاهای منحصر به فردی خلق کنند. کپی غیرمجاز این آثار می‌تواند به راحتی و در مقیاس بزرگ انجام شود. برای مثال، یک طراح ممکن است ساعت‌ها صرف خلق یک لباس منحصر به فرد برای آواتارها کند، اما یک متخلف می‌تواند در عرض چند ثانیه آن را کپی و به صورت انبوه توزیع کند.

ب) سرقت ایده‌های خلاقانه: در محیط باز و تعاملی متاورس، ایده‌های نوآورانه می‌توانند به راحتی مشاهده و کپی شوند. برای مثال، یک کارآفرین ممکن است یک مفهوم جدید برای یک فضای اجتماعی مجازی ارائه دهد، اما قبل از اینکه بتواند آن را به طور کامل توسعه دهد، دیگران ممکن است ایده را بدزدند و اجرا کنند.

تهدیدهای امنیتی

الف) حملات فیشینگ[1] پیشرفته: فیشینگ یک نوع حمله سایبری است که هدف آن فریب افراد برای افشای اطلاعات حساس مانند نام‌های کاربری، رمزهای عبور، اطلاعات کارت اعتباری یا سایر داده‌های شخصی است. در متاورس، حملات فیشینگ می‌توانند بسیار پیچیده‌تر شوند. مهاجمان ممکن است محیط‌های مجازی کاملاً واقعی ایجاد کنند که شبیه بانک‌ها یا سایر مؤسسات معتبر هستند. کاربران ممکن است فریب بخورند و اطلاعات حساس خود را در این محیط‌های به ظاهر امن وارد کنند. تصور کنید یک کاربر وارد یک «شعبه بانک مجازی» می‌شود که در واقع یک تله فیشینگ پیچیده است.

ب) آسیب‌پذیری‌های سیستمی: زیرساخت‌های پیچیده متاورس می‌تواند آسیب‌پذیری‌های جدیدی ایجاد کند. برای مثال، یک نقص در پروتکل انتقال داده واقعیت مجازی می‌تواند به هکرها اجازه دهد به جریان داده‌های حسی کاربران دسترسی پیدا کنند. این می‌تواند منجر به سرقت اطلاعات حساس یا حتی دستکاری تجربیات حسی گردد(Thompson, 2024 :78) .

تهدیدها علیه دنیای فیزیکی و جامعه انسانی

آخرین گروه از تهدیدهای در فضای متاورس که به نظر می‌رسد مهم‌ترین دسته به دلیل ارتباطات آشکاری که میان واقعیت مجازی وافزوده و دنیای واقعی برقرار می‌کند، تهدیدهای علیه دنیای فیزیکی و جامعه انسانی است که به شرح زیر می‌توان در مورد آنها توضیح داد. این گروه شامل تهدیدهایی علیه ایمنی شخصی افراد می‌تواند باشد (به عنوان مثال، یک فرد می‌تواند واقعیت

1. Phishing

مجازی را به گونه‌ای دستکاری کند که محدوده‌های فیزیکی تعریف شده در سخت‌افزار آن وسیله بازنشانی شود، در نتیجه، کاربر آن وسیله در فضای مجازی بدون اطلاع به سمت یک پله، خیابان شلوغ یا سایر مکان‌های خطرناک فیزیکی هدایت شود و دچار سوانح گوناگون شود) و همچنین شامل تهدیدهای علیه امنیت و زیرساخت‌های کلیدی کشورها نیز می‌شود، به این صورت که هکرها از طریق شنود نرم‌افزارها یا بهره‌برداری از آسیب‌پذیری‌های سیستم‌ها در فضای مجازی می‌توانند به زیرساخت‌های ملی و حیاتی چون برق، آب، نفت و گاز دسترسی پیدا کنند و از این طریق با حملات بدافزاری آن‌ها را مورد هدف قرار دهند (Wang, 2024: 122). در رابطه با پیچیدگی تهدیدها و خطرات فضای مجازی که در بالا ارائه شد، ضرورت ایجاد یک چارچوب حقوقی کیفری مناسب برای حمایت از کاربران دنیاهای مجازی، حقوق و آزادی‌های آن‌ها امری اجتناب ناپذیر است.

ضرورت تشکیل حقوق متا کیفری در نظام عدالت کیفری

ایجاد شاخه‌های جدید حقوقی به طور کلی و یک شاخه جدید از حقوق جزا – به نام حقوق متا کیفری– که منحصراً در واقعیت‌های متاورس کاربرد داشته باشد، ایده‌ای است که پذیرش و اجرای آن در عمل دشوار است. با این حال، طراحی صرف یک شاخه جدید حقوقی برای متاورس کافی نیست. بلکه نیاز به طراحی یک نظام کاملاً جدید وجود دارد تا این قوانین را اجرا کند و مجرمانی را که مرتکب متا جرایم می‌شوند، مجازات نماید. در اصل، حقوق متا کیفری شامل توسعه مجموعه‌ای از اصول، قوانین و مقررات قانونی است که به فعالیت‌های مجرمانه، جرایم و مسائل منحصر به فرد در محیط های مجازی می‌پردازد. این می‌تواند شامل جرائمی مانند سرقت مجازی، کلاهبرداری مجازی، آزار و اذیت یا هر فعالیت غیرقانونی دیگری باشد که ممکن است در متاورس رخ دهد. اجرای شاخه جدید حقوق جزا مستلزم بررسی دقیق عوامل مختلف از جمله تعریف و شناسایی جرایم مجازی، تعیین صلاحیت قضایی و ایجاد رویه‌های قانونی مناسب برای اجرا است. چالش‌های مرتبط با اجرای قوانین در فضای مجازی جایی که مفاهیم حقوقی سنتی ممکن است به طور مستقیم اعمال نشوند، پذیرش و اجرای این ایده را در عمل ممکن می‌سازد. در اصل، در مورد یک تحول بالقوه در سیستم حقوقی می‌توانیم حدس بزنیم که در آن پرونده های جنایی، ارائه شواهد و اجرای مجازات‌ها کاملاً در محدوده دیجیتال متاورس رخ می‌دهد. این ایده، منعکس کننده ادغام مداوم فناوری‌های مجازی و دیجیتال در جنبه‌های مختلف زندگی انسان از جمله حوزه حقوقی آن است. استفاده از عباراتی مانند محاکمات متا جنایی دلالت بر دیدگاهی آینده نگر دارد که در آن فرآیندهای قانونی از مرزهای فیزیکی فراتر می‌روند و به بخشی جدایی‌ناپذیر از تجربه واقعیت مجازی تبدیل می‌شوند. آیا روزی فرا خواهد رسید که محاکم متاکیفری داشته باشیم که در آن‌ها صرفاً شواهد مجازی در فضای مجازی ارائه شود و مجازات‌ها در زندان‌های مجازی اجرا گردد؟ این احتمالاً مسیر طبیعی توسعه خواهد بود. در این مسیر طبیعی مبانی ضروری شکل گیری حقوق متا کیفری را می توانیم پیش‌بینی کنیم. با گسترش روزافزون فناوری‌های واقعیت مجازی و متاورس، فضایی جدید برای تعاملات انسانی شکل گرفته است. این فضا، که از دنیای فیزیکی متمایز است، نیازمند قوانین و مقررات خاص خود می‌باشد(sina, et al,2009 :67). حقوق متاکیفری می‌تواند چارچوب قانونی لازم برای مدیریت رفتارهای مجرمانه در این فضای نوظهور را فراهم کند. این امر بیانگر تحول در فضای مجازی است. با توجه به ماهیت متفاوت جرایم در فضای متاورس از جرایم دنیای واقعی مانند، سرقت اموال مجازی، آزار و اذیت در فضای مجازی، یا حتی جرایمی که هنوز تعریف نشده‌اند حقوق متاکیفری می‌تواند این چالش‌های جدید را شناسایی کرده و راهکارهای قانونی مناسب ارائه دهد. از سوی دیگر با افزایش حضور افراد در فضای متاورس، حفاظت از حقوق آنها اهمیت بیشتری می‌یابد. حقوق متا کیفری می‌تواند چارچوبی برای حمایت از حریم خصوصی، امنیت و حقوق مالکیت معنوی کاربران در فضای مجازی ایجاد کند. استفاده از فناوری‌های واقعیت مجازی در دادگاه‌ها می‌تواند به بازسازی صحنه جرم و درک بهتر وقایع کمک کند. حقوق متا کیفری می‌تواند قوانین و رویه‌های لازم برای استفاده از این فناوری‌ها در روند دادرسی را تعیین کند. با تدوین قوانین متا کیفری، می‌توان چارچوب‌های پیشگیرانه برای جلوگیری از وقوع جرم در فضای متاورس ایجاد کرد. این امر می‌تواند شامل آموزش کاربران، نظارت بر فعالیت‌های مشکوک و ایجاد سازوکارهای امنیتی

باشد.حقوق متا کیفری می‌تواند مجازات‌های متناسب با جرایم ارتکابی در فضای متاورس را تعریف کند. این می‌تواند شامل مجازات‌های مجازی مانند محدودیت دسترسی به فضاهای خاص در متاورس یا حتی زندان‌های مجازی باشد از آنجا که فضای متاورس مرزهای جغرافیایی را درمی‌نوردد، ایجاد یک چارچوب حقوقی بین‌المللی برای رسیدگی به جرایم فراملی ضروری است (Lalalizadeh, 2023, 70). متاورس و فناوری‌های نوین، مرز بین واقعیت و دنیای مجازی را مبهم کرده‌اند. این فضای جدید ترکیبی از واقعیت افزوده، واقعیت مجازی و اینترنت اشیاء (IoT)[1] است. در چنین محیطی، تعاملات انسانی، معاملات تجاری و حتی هویت‌های شخصی می‌توانند اشکال پیچیده‌ای به خود بگیرند. برای مثال، یک فرد ممکن است چندین آواتار با شخصیت‌های متفاوت در متاورس داشته باشد. این پیچیدگی نیاز به متخصصانی دارد که نه تنها درک عمیقی از مفاهیم حقوقی داشته باشند، بلکه با جنبه‌های فنی و اجتماعی این فضای نوظهور نیز آشنا باشند (Moradi berelian, 2022, 392) . متخصصان حقوق متا کیفری باید درک عمیقی از فناوری‌های زیربنایی متاورس داشته باشند. این شامل آشنایی با بلاکچین، هوش مصنوعی، یادگیری ماشین و سیستم‌های توزیع‌شده است. آن‌ها باید بتوانند پیامدهای حقوقی پیشرفت‌های فناورانه را پیش‌بینی و تفسیر کنند. برای مثال، اگر یک الگوریتم هوش مصنوعی در متاورس تصمیمی بگیرد که منجر به آسیب به یک کاربر شود، چه کسی مسئول است؟ یا چگونه می‌توان قراردادهای هوشمند را از نظر حقوقی تنظیم و اجرا کرد؟ با گسترش خلاقیت‌های دیجیتال در متاورس، قوانین سنتی کپی‌رایت نیاز به بازنگری و توسعه دارند. برای مثال، چگونه می‌توان از یک طرح سه‌بعدی در متاورس محافظت کرد؟ یا اگر یک هوش مصنوعی اثر هنری خلق کند، مالکیت معنوی آن متعلق به چه کسی است؟ متخصصان حقوق متاکیفری باید بتوانند قوانین مالکیت معنوی را با واقعیت‌های فضای مجازی تطبیق دهند. رشد اقتصادهای مبتنی بر ارزهای دیجیتال و دارایی‌های مجازی در متاورس نیازمند چارچوب‌های قانونی جدید است. این شامل مقررات مربوط به معاملات مالی در متاورس، مالیات بر دارایی‌های مجازی و نحوه تنظیم بازارهای مالی در این فضا می‌شود(khalili bagi,et al, 2022: 68). متخصصان حقوق متاکیفری باید بتوانند سیستم‌های مالی سنتی را با واقعیت‌های اقتصاد دیجیتال تطبیق دهند. در مجموع، رشته حقوق متاکیفری نه تنها به پرکردن خلأ قانونی در فضای متاورس کمک می‌کند، بلکه می‌تواند پیشران توسعه قوانین و مقررات برای آینده فناوری باشد. متخصصان این رشته نقش کلیدی در شکل دادن به آینده تعاملات انسانی، تجارت، و حکمرانی در عصر دیجیتال خواهند داشت. در نتیجه، ایجاد و تشکیل حقوق متاکیفری نه تنها یک ضرورت، بلکه یک فرصت برای پیش‌بینی و مدیریت چالش‌های حقوقی آینده در عصر دیجیتال است(cuartas, 2022 :47). این شاخه جدید از حقوق می‌تواند به ایجاد یک فضای مجازی امن، عادلانه و قانونمند کمک کند، در حالی که زمینه را برای نوآوری و پیشرفت در این عرصه فراهم می‌سازد.

فرصت‌های تحقق حقوق متا کیفری در نظام عدالت کیفری

ما هم‌اکنون با برخورد دو جهان از نظر فرآیند کیفری روبرو هستیم، زیرا متاورس می‌تواند با موفقیت در بررسی پرونده‌های جنایی از واقعیت فیزیکی مورد استفاده قرار گیرد. اگرچه نگرانی‌هایی در مورد استفاده از فناوری‌های واقعیت مجازی در نظام عدالت کیفری فعلی وجود دارد، لیکن این فقط آغاز راه است. تصور دادگاه‌های کیفری مجازی که شامل ارائه مدارک مجازی در فضای مجازی بوده و مجازات‌ها در زندان‌های مجازی اجرا خواهند شد امر دور از ذهنی نیست، بدینگونه متاورس بینشی همه جانبه در مورد چگونگی وقوع جرم، در دنیای فیزیکی ارائه می‌دهد. انتظار می‌رود با پیشرفت فناوری در آینده نزدیک، شاهد افزایش چشمگیر و فزاینده‌ای در به‌کارگیری واقعیت مجازی در حوزه‌ی قضایی و دادرسی‌های کیفری و به عبارتی محاکم متاکیفری باشیم. این می‌تواند به سطح جدیدی از ارائه و تجزیه و تحلیل شواهد و همچنین چالش‌های بالقوه از نظر قابل قبول بودن شواهد مجازی در دادگاه منجر شود. در چین، ارائه مدارک در دادگاه‌های کیفری با استفاده از فناوری‌های واقعیت مجازی از سال ۲۰۱۸ مجاز شده

1. Internet of Things

این مفهوم به شبکه‌ای از دستگاه‌های فیزیکی متصل به هم اشاره دارد که می‌توانند داده‌ها را جمع‌آوری، تبادل و عمل کنند.

است (Nafarette,2018 :83) به عبارتی در نظام حقوقی چین، پذیرش مدارک و شواهدی که از طریق فناوری واقعیت مجازی تولید شده‌اند، در دادگاه‌های کیفری از چندین سال پیش مورد تأیید بوده و به عنوان شواهد و مدارک معتبر پذیرفته می‌شوند علاوه بر این، ابتکارات واقعی دانشمندان برای ترویج استفاده گسترده از واقعیت مجازی به منظور تسهیل روند دادرسی کیفری و کشف حقیقت، حداقل از ۱۶ سال پیش وجود داشته است. مزیت دیگر این است که واقعیت مجازی می‌تواند در آموزش افراد شاغل در قوه قضائیه یا حتی در فرآیند اصلاح و تربیت محکومان به منظور توان‌بخشی و بازاجتماعی‌کردن آنها و بازگشت ایشان به جامعه مورد استفاده قرار گیرد (Bailenson,et al, 2006 :246) اما استفاده گسترده از محیط‌های مجازی فراگیر مانند متاورس، امکانات و کاربردهای منحصر به فردی را در این سیستم فراهم می‌کند به این معنا که کارکنان و مجریان سیستم عدالت کیفری می‌توانند با استفاده از متاورس، کنترل و نظارت کامل بر واکنش‌ها و رفتار افرادی که با آنها سر و کار دارند، داشته باشند. اهم فرصت‌هایی که حقوق متاکیفری می‌تواند در اختیار محققین و نظام عدالت کیفری قرار دهد به شرح زیر است:

۵-۱- حقوق متاکیفری می‌تواند به عنوان یک ابزار پیش‌بینی برای شناسایی روش‌های احتمالی در جرایم دیجیتال آینده عمل کند. با مطالعه و تحلیل الگوهای رفتاری در فضای متاورس، متخصصان حقوق متاکیفری می‌توانند طرح‌های مختلف را پیش‌بینی کرده و راهکارهای قانونی مناسب را قبل از وقوع مشکلات جدی طراحی کنند. با مطالعه دقیق رفتارهای کاربران در فضای متاورس، می‌توان الگوهای رفتاری مشخصی را شناسایی کرد. این الگوها می‌توانند نشان‌دهنده روند احتمالی در جرایم آینده باشند. بررسی ساختار فنی متاورس می‌تواند به شناسایی نقاط ضعف احتمالی کمک کند که ممکن است مورد سوءاستفاده مجرمان قرار گیرند. متعاقب داده‌های جمع‌آوری شده و بر اساس آنها می‌توان سناریوها و طرح‌های مختلفی را برای جرایم احتمالی آینده تدوین کرد و مبتنی بر طرح‌های پیش‌بینی شده فوق می‌توان راهکارهای قانونی و فنی مناسب را برای پیشگیری از وقوع جرایم طراحی کرد. این رویکرد پیش‌بینانه می‌تواند به ایجاد یک چارچوب حقوقی منعطف و کارآمد برای مقابله با جرایم دیجیتال در فضای متاورس کمک کند و امنیت کاربران را در این محیط جدید افزایش دهد(Mahmoudi & Sadeghi, 2022: 62).

۵-۲- حقوق متاکیفری می‌تواند زمینه‌ساز ایجاد آزمایشگاه‌های حقوقی مجازی شود. آزمایشگاه‌های حقوقی مجازی در حوزه حقوق متاکیفری بسیار نوآورانه و کاربردی است. در این آزمایشگاه‌ها، قوانین و مقررات پیشنهادی می‌توانند در محیط‌های شبیه‌سازی شده آزمایش شوند تا اثربخشی و پیامدهای احتمالی آنها قبل از اجرا در دنیای واقعی ارزیابی شود. این آزمایشگاه‌ها می‌توانند محیطی مشابه متاورس را با تمام پیچیدگی‌ها و تعاملات آن شبیه‌سازی کنند. این امر امکان بررسی دقیق‌تر تأثیر قوانین پیشنهادی را فراهم می‌کند. قوانین و مقررات پیشنهادی می‌توانند در این محیط مجازی اجرا شوند تا اثربخشی و پیامدهای احتمالی آنها مشاهده شود. این امر به قانونگذاران اجازه می‌دهد تا نقاط ضعف و قوت قوانین را قبل از اجرای واقعی شناسایی کنند. آزمایشگاه‌های حقوقی مجازی با استفاده از الگوریتم‌های هوش مصنوعی، می‌تواند رفتار کاربران را در واکنش به قوانین جدید شبیه‌سازی کند(Cuartas, 2022:95) و بدین ترتیب به پیش‌بینی واکنش‌های احتمالی جامعه به قوانین جدید کمک کند. در این آزمایشگاه‌ها می‌توان سناریوها و طرح های مختلف را آزمود. مثلاً می‌توان تأثیر یک قانون را در شرایط مختلف اقتصادی، اجتماعی یا فرهنگی بررسی کرد. این آزمایشگاه‌ها می‌توانند محلی برای همکاری متخصصان حقوقی، فناوری اطلاعات، جامعه‌شناسی و روانشناسی باشند تا دیدگاه‌های مختلف در تدوین قوانین لحاظ شود. آنها می‌توانند به شناسایی پیامدهای ناخواسته احتمالی قوانین جدید کمک کنند که ممکن است در شرایط واقعی قابل پیش‌بینی نباشند. با توسل به این آزمایشگاه‌ها می‌توان قوانین را در مقیاس‌های مختلف آزمایش کرد تا از کارآمدی آنها در شرایط مختلف اطمینان حاصل شود. ایجاد چنین آزمایشگاه‌هایی می‌تواند به تدوین قوانین کارآمدتر و مناسب‌تر برای فضای متاورس منجر شود و ریسک اجرای قوانین ناکارآمد را کاهش دهد.

۵-۳- توسعه سیستم‌های هوش مصنوعی حقوقی: با ایجاد حقوق متاکیفری، امکان توسعه سیستم‌های هوش مصنوعی تخصصی برای تحلیل و پیش‌بینی روند و فرآیند جرم در فضای دیجیتال فراهم می‌شود. این سیستم‌ها می‌توانند به شناسایی سریع الگوهای جدید جرم و ارائه راهکارهای پیشگیرانه کمک کنند. توسعه سیستم‌های هوش مصنوعی حقوقی در حوزه حقوق متاکیفری

می‌تواند تحولی عظیم در مدیریت و پیشگیری از جرائم دیجیتال ایجاد کند. سیستم‌های هوش مصنوعی می‌توانند حجم عظیمی از داده‌های مربوط به فعالیت‌های کاربران در فضای متاورس را تحلیل کنند. این تحلیل می‌تواند الگوهای پنهان را که ممکن است نشان‌دهنده فعالیت‌های مجرمانه باشند، شناسایی کند. این سیستم‌ها می‌توانند به قضات و وکلا در درک بهتر پرونده‌های پیچیده مربوط به جرائم دیجیتال کمک کنند و اطلاعات لازم را در اختیار آنها قرار دهند. با تحلیل مداوم اثربخشی قوانین موجود، هوش مصنوعی می‌تواند پیشنهادهایی برای بهبود و به‌روزرسانی قوانین ارائه دهد. سیستم‌های هوش مصنوعی می‌توانند در شناسایی و تأیید هویت کاربران در فضای متاورس کمک کنند که این امر می‌تواند به کاهش جرائم مرتبط با هویت جعلی منجر شود. هویت دیجیتال افراد را مدیریت کند. با بررسی تراکنش‌های مالی و تحلیل رفتار مالی در متاورس، هوش مصنوعی می‌تواند الگوهای مشکوک مانند پولشویی یا کلاهبرداری را شناسایی کند (Ghazi & Shabazi, 2021: 502) . توسعه چنین سیستم‌هایی می‌تواند به ایجاد یک محیط امن‌تر و قانونمندتر در فضای متاورس کمک کند و ابزاری قدرتمند برای مقابله با جرائم دیجیتال در اختیار مقامات قضایی و قانونگذاران قرار دهد.

۵-۴- توسعه مدل‌های ریسک و ارزیابی تهدید: با استفاده از داده‌های جمع‌آوری شده در فضای متاورس، حقوق متاکیفری می‌تواند به توسعه مدل‌های پیشرفته ارزیابی ریسک و تهدید کمک کند. این مدل‌ها می‌توانند به پیش‌بینی و مدیریت بهتر خطرات احتمالی در فضای دیجیتال کمک کنند. توسعه مدل‌های ریسک و ارزیابی تهدید در حوزه حقوق متاکیفری می‌تواند نقش مهمی در پیشگیری و مدیریت جرایم در فضای متاورس ایفا کند. این مفهوم را می‌توان به شکل زیر گسترش داد: این مدل‌ها می‌توانند از طیف وسیعی از داده‌ها و جمع‌آوری داده‌های جامع در متاورس استفاده کنند، از الگوهای رفتاری کاربران، تراکنش‌های مالی، تعاملات اجتماعی و فعالیت‌های مشکوک را می‌توان نام برد. با استفاده از تکنیک‌های پیشرفته یادگیری ماشینی، این مدل‌ها می‌توانند الگوهای رفتاری مرتبط با فعالیت‌های مجرمانه را شناسایی و تحلیل کنند. مدل‌های ارزیابی ریسک می‌توانند نقاط ضعف و آسیب‌پذیری‌های سیستمی در متاورس را شناسایی کنند که ممکن است مورد سوءاستفاده مجرمان قرار گیرند. با تحلیل داده‌های تاریخی و الگوهای جاری، این مدل‌ها می‌توانند روند آینده جرایم در متاورس را پیش‌بینی کنند. این مدل‌ها می‌توانند به صورت بلادرنگ فعالیت‌های کاربران را ارزیابی کرده و هشدارهای لازم را در مورد رفتارهای مشکوک صادر کنند. با استفاده از الگوریتم‌های پیچیده، این مدل‌ها می‌توانند سطوح مختلف تهدید را برای انواع مختلف فعالیت‌ها در متاورس تعیین کنند. مدل‌ها می‌توانند بر اساس ویژگی‌های خاص هر کاربر یا هر بخش از متاورس، ارزیابی‌های ریسک شخصی‌سازی شده ارائه دهند. با بررسی ارتباطات و تعاملات کاربران در متاورس، این مدل‌ها می‌توانند شبکه‌های مجرمانه احتمالی را شناسایی کنند. مدل‌ها می‌توانند سیستم‌هایی برای ارزیابی اعتبار و قابلیت اعتماد کاربران در متاورس ایجاد کنند، که می‌تواند به کاهش ریسک تعاملات مخرب کمک کند. این مدل‌ها می‌توانند سناریوهای مختلف تهدید را شبیه‌سازی کنند تا آمادگی سیستم‌ها و کاربران برای مقابله با آنها افزایش یابد. مدل‌های ارزیابی ریسک می‌توانند تأثیر قوانین و مقررات جدید بر کاهش یا افزایش ریسک‌های امنیتی را ارزیابی کنند. بر اساس الگوهای شناسایی شده، این مدل‌ها می‌توانند هشدارهای پیش‌دستانه در مورد تهدیدهای احتمالی صادر کنند. با شناسایی مناطق پرخطر در متاورس، این مدل‌ها می‌توانند به تخصیص بهینه منابع امنیتی کمک کنند و قادر هستند به شناسایی و ارزیابی ریسک‌های جدید و نوظهور که با پیشرفت فناوری ظهور می‌کنند، یاری رسانند (Mirashrafi, 2022, 387) . مدل‌ها می‌توانند الگوهای مشکوک در تراکنش‌های مالی در متاورس را شناسایی کرده و موجب جلوگیری از پولشویی و کلاهبرداری شوند. توسعه چنین مدل‌هایی می‌تواند زمینه ایجاد یک محیط امن‌تر در متاورس را فراهم کرده و ابزارهای قدرتمندی برای پیشگیری و مدیریت جرایم در اختیار مقامات قانونی و مدیران پلتفرم‌ها قرار دهد. همچنین، این مدل‌ها می‌توانند به توسعه سیاست‌های حقوقی و امنیتی موثرتر و متناسب با چالش‌های خاص فضای متاورس یاری رسانند.

۵-۵- ایجاد سیستم‌های هشدار زودهنگام: با تحلیل الگوهای رفتاری در متاورس، حقوق متاکیفری می‌تواند به طراحی سیستم‌های هشدار زودهنگام برای شناسایی فعالیت‌های مشکوک یا بالقوه خطرناک کمک کند. این سیستم‌ها می‌توانند به

پیشگیری از جرایم قبل از وقوع آنها کمک کنند. ایجاد سیستم‌های هشدار زودهنگام در حوزه حقوق متاکیفری می‌تواند نقش مهمی در پیشگیری از جرایم و افزایش امنیت در فضای متاورس ایفا کند. این سیستم‌ها می‌توانند به صورت بلادرنگ رفتار کاربران را در متاورس تحلیل کنند. با استفاده از الگوریتم‌های پیشرفته یادگیری ماشینی، می‌توان الگوهای رفتاری غیرعادی یا مشکوک را سریعاً شناسایی کرد. سیستم‌های هشدار زودهنگام می‌توانند الگوهای رفتاری که معمولاً با فعالیت‌های مجرمانه مرتبط هستند را شناسایی کنند. این می‌تواند شامل تغییرات ناگهانی در الگوهای تعامل، فعالیت‌های مالی غیرعادی، یا تلاش‌های مکرر برای دسترسی به اطلاعات حساس باشد. با بررسی ارتباطات و تعاملات کاربران، این سیستم‌ها می‌توانند شبکه‌های مشکوک یا گروه‌های با رفتار غیرعادی را شناسایی کنند(Brown, 2022 :76). این می‌تواند به کشف زودهنگام فعالیت‌های سازمان‌یافته مجرمانه کمک کند. با استفاده از مدل‌های پیش‌بینی‌کننده این سیستم‌ها می‌توانند احتمال وقوع رفتارهای خاص را در آینده تخمین بزنند و به پیشگیری از جرایم قبل از وقوع آنها کمک کند. سیستم‌های هشدار می‌توانند هشدارهایی در سطوح مختلف صادر کنند. از هشدارهای کم‌اهمیت برای رفتارهای مشکوک تا هشدارهای فوری برای تهدیدهای جدی. این سیستم‌ها می‌توانند محتوای تولید شده توسط کاربران را تحلیل کنند تا موارد نامناسب، خشونت‌آمیز یا غیرقانونی را شناسایی کنند. سیستم‌های هشدار زودهنگام می‌توانند تلاش‌های نفوذ به سیستم‌ها یا حملات سایبری را در مراحل اولیه شناسایی کنند.و قادر هستند الگوهای غیرعادی در تراکنش‌های مالی را که ممکن است نشان‌دهنده پولشویی یا کلاهبرداری باشد، شناسایی کنند.

۵-۶- توسعه پروتکل‌های امنیتی پیشرفته: حقوق متاکیفری می‌تواند به توسعه پروتکل‌های امنیتی پیشرفته برای محافظت از داده‌ها و حریم خصوصی کاربران در فضای متاورس کمک کند. این پروتکل‌ها می‌توانند به پیش‌بینی و مقابله با تهدیدات امنیتی آینده کمک کنند. توسعه پروتکل‌های امنیتی پیشرفته در حوزه حقوق متاکیفری می‌تواند نقش کلیدی در حفاظت از داده‌ها و حریم خصوصی کاربران در فضای متاورس ایفا کند. این مهم به اشکال گوناگون گسترش می یابد. پروتکل‌های امنیتی جدید می‌توانند از الگوریتم‌های رمزنگاری پیشرفته استفاده کنند که حتی در برابر حملات کوانتومی آینده مقاوم باشند. این می‌تواند شامل استفاده از رمزنگاری هومومورفیک باشد که امکان پردازش داده‌های رمزگذاری شده را بدون نیاز به رمزگشایی فراهم می‌کند. پروتکل‌های جدید می‌توانند از روش‌های احراز هویت چند عاملی پیشرفته استفاده کنند که شامل عوامل بیومتریک، رفتاری و حتی عوامل مبتنی بر موقعیت در متاورس می باشد استفاده از فناوری‌های مبتنی بر بلاکچین برای ایجاد سیستم‌های مدیریت هویت غیرمتمرکز که به کاربران کنترل بیشتری بر داده‌های شخصی خود می‌دهد پروتکل‌هایی برای محافظت از داده‌های حسی جمع‌آوری شده توسط دستگاه‌های واقعیت مجازی و افزوده، مانند داده‌های حرکتی یا بیومتریک. پروتکل‌هایی که امکان مدیریت دسترسی پویا و ظریف به داده‌ها و منابع را بر اساس زمینه، موقعیت و سطح اعتماد در متاورس فراهم می‌کنند. پروتکل‌هایی که از هوش مصنوعی برای پیش‌بینی و شناسایی تهدیدات امنیتی بالقوه استفاده می‌کنند و به طور خودکار اقدامات دفاعی را اجرا می‌کنند. پروتکل‌هایی برای حفاظت از اطلاعات مکانی کاربران در متاورس، با استفاده از تکنیک‌هایی مانند مبهم‌سازی مکانی یا رمزنگاری مکانی et , (shaahbadian al,2023:134). توسعه چنین پروتکل‌های امنیتی پیشرفته‌ای می‌تواند به ایجاد یک محیط امن و قابل اعتماد در متاورس کمک کند. این پروتکل‌ها نه تنها از داده‌ها و حریم خصوصی کاربران محافظت می‌کنند، بلکه می‌توانند به پیش‌بینی و مقابله با تهدیدات امنیتی آینده نیز کمک کنند. همچنین، این پروتکل‌ها می‌توانند به ایجاد اعتماد بیشتر در میان کاربران و تسهیل پذیرش گسترده‌تر متاورس کمک کنند. در نهایت، توسعه این پروتکل‌ها باید با چارچوب‌های قانونی و اخلاقی مناسب همراه باشد تا اطمینان حاصل شود که امنیت و حریم خصوصی با حقوق و آزادی‌های اساسی کاربران در تعادل است.

۵-۷- ایجاد سیستم‌های خودتنظیم‌کننده: حقوق متاکیفری می‌تواند زمینه‌ساز ایجاد سیستم‌های خودتنظیم‌کننده در فضای متاورس شود. این سیستم‌ها می‌توانند به طور خودکار قوانین و مقررات را بر اساس تغییرات محیطی و رفتاری تنظیم کنند، که به مدیریت پویای چالش‌های حقوقی کمک می‌کند. سیستم‌های خودتنظیم‌کننده قادرند خود را با شرایط متغیر تطبیق دهند. در زمینه قانونی، این به معنای ایجاد قوانینی است که می‌توانند به طور خودکار و پویا با تغییرات محیط مجازی سازگار شوند آنها قادر هستند

قوانین را بر اساس الگوهای رفتاری کاربران و تغییرات در محیط مجازی به روز کنند. برای مثال، اگر نوع جدیدی از تخلف در متاورس رایج شود، سیستم می‌تواند به طور خودکار قوانین جدیدی برای مقابله با آن ایجاد کند.با توجه به ماهیت در حال تغییر فناوری و تعاملات در متاورس، این سیستم‌ها می‌توانند بدون نیاز به دخالت مستقیم انسان در هر مورد.به سرعت به مسائل حقوقی جدید پاسخ دهند(latifzadeh, et al, 2023 : 349) . این رویکرد می‌تواند به ایجاد یک محیط امن‌تر و منصفانه‌تر در متاورس کمک کند، جایی که قوانین به طور مداوم با نیازهای جامعه مجازی تطبیق می‌یابند.

۵-۸- ایجاد سیستم‌های نظارتی هوشمند: با استفاده از فناوری‌های پیشرفته مانند یادگیری ماشین و پردازش زبان طبیعی، حقوق متاکیفری می‌تواند به ایجاد سیستم‌های نظارتی هوشمند کمک کند. این سیستم‌ها می‌توانند به طور مداوم فعالیت‌های کاربران را تحلیل کرده و الگوهای مشکوک را شناسایی کنند. استفاده از فناوری‌های پیشرفته در چارچوب حقوق متاکیفری پتانسیل لازم برای ایجاد سیستم‌های نظارتی هوشمند در فضای متاورس را دارد. این سیستم‌ها از هوش مصنوعی و الگوریتم‌های پیشرفته برای نظارت، تحلیل و ارزیابی فعالیت‌های کاربران در محیط متاورس استفاده می‌کنند و به طور پیوسته فعالیت‌های کاربران را بررسی می‌کنند و تحلیل مداوم دارد. از سوی دیگر، قادر به تشخیص الگوهای رفتاری غیرعادی یا مشکوک هستند و توانایی احتمال وقوع تخلفات را پیش‌بینی کنند. تعاملات کاربران، معاملات مالی و تجاری، محتوای تولید شده توسط کاربران الگوهای حرکتی و رفتاری آواتارها انواع فعالیت‌های قابل نظارت توسط این سیستم ها هستند این سیستم‌ها باید با قوانین حفاظت از داده‌ها و حریم خصوصی در سراسر جهان مطابقت داشته باشند. با جمع‌آوری داده‌های بیشتر و یادگیری از تجربیات، آنها می‌توانند به طور مداوم بهبود یابند و دقیق‌تر شوند. ایجاد چنین سیستم‌هایی می‌تواند به ایجاد یک محیط امن‌تر و قانونمندتر در متاورس کمک کند، اما همزمان باید با دقت طراحی و اجرا شوند تا از حقوق و آزادی‌های اساسی کاربران محافظت شود. این موارد نشان می‌دهند که چگونه ایجاد و تشکیل حقوق متاکیفری می‌تواند فرصت‌های جدیدی برای پیش‌بینی و مدیریت چالش‌های حقوقی آینده در عصر دیجیتال فراهم کند. با توسعه این شاخه جدید از حقوق، ما می‌توانیم به طور پیش‌فعال با مسائل نوظهور در فضای دیجیتال مواجه شویم و راه‌حل‌های نوآورانه‌ای برای حفظ امنیت، عدالت و حقوق افراد در دنیای مجازی ارائه دهیم.

در بررسی ضرورت تشکیل حقوق متا کیفری با توجه به نظام حقوقی ایران، نکات ذیل حائز اهمیت است:

۵-۹- مبانی نظری و ساختاری: نظام حقوقی ایران مبتنی بر فقه اسلامی و قوانین موضوعه است. حقوق متا کیفری می‌تواند با تلفیق رویکردهای فقهی و مدرن، چارچوبی جامع‌تر برای تحلیل و مواجهه با پدیده مجرمانه ایجاد کند. این حوزه از حقوق کیفری، به دنبال پاسخگویی به چالش‌های نوظهور در عرصه جرم‌شناسی و حقوق کیفری است.

۵-۱۰- پیچیدگی‌های جرایم نوین: با توجه به گسترش فناوری و تحولات اجتماعی، نظام کیفری ایران با انواع جدیدی از جرایم مواجه است که نیازمند رویکردی فراتر از برخورد سنتی هستند. جرایم سایبری، اقتصادی و سازمان‌یافته، ضرورت نگاه متا کیفری را آشکار می‌سازند. در نظام حقوقی اسلام و ایران، مفاهیمی مانند تعزیر و اصلاح مجرم از اهمیت ویژه‌ای برخوردار است. حقوق متا کیفری می‌تواند این رویکرد را با مطالعات علمی و روانشناختی تقویت کند.

۵-۱۱- پیشگیری از جرم: در فقه اسلامی، پیشگیری از جرم اهمیت بسیاری دارد. حقوق متا کیفری با نگاهی میان‌رشته‌ای، می‌تواند راهکارهای پیشگیرانه مؤثرتری را شناسایی و ارائه دهد. این رویکرد می‌تواند نقش مؤثری در کاهش بازگشت مجرمان به چرخه بزهکاری و ارتقای عدالت ترمیمی ایفا کند. حقوق متا کیفری می‌تواند به بازنگری مداوم در سیاست‌های کیفری کمک کرده و راهکارهای پیشگیرانه و درمانی را جایگزین رویکردهای سنتی و صرفاً تنبیهی سازد. در نهایت، تشکیل حقوق متا کیفری در نظام حقوقی ایران، ضرورتی انکارناپذیر است که می‌تواند به ارتقای کارآمدی نظام عدالت کیفری و ایجاد جامعه‌ای امن‌تر و عادلانه‌تر کمک کند.

نتیجه‌گیری

حقوق متاکیری فرصت‌های متعددی را در عرصه دیجیتال ایجاد می‌کند. یکی از مهم‌ترین این فرصت‌ها، ایجاد دادگاه‌های کیفری مجازی که شامل ارائه مدارک مجازی در فضای مجازی بوده و مجازات‌ها در زندان‌های مجازی اجرا خواهند شد می‌باشد ، بدینگونه متاورس بینشی همه‌جانبه در مورد چگونگی وقوع جرم، در دنیای فیزیکی ارائه می‌دهد فرصت دیگر این است که واقعیت مجازی می‌تواند در آموزش افراد شاغل در قوه قضائیه یا حتی در فرآیند اصلاح و تربیت محکومان به منظور توانبخشی و بازاجتماعی‌کردن آنها و بازگشت ایشان به جامعه مورد استفاده قرار گیرد. ایجاد چارچوب‌های قانونی جدید برای محافظت از حقوق کاربران در فضای مجازی است. این چارچوب‌ها می‌توانند شامل قوانین مربوط به حفاظت از داده‌های شخصی، حقوق مالکیت دیجیتال و حق دسترسی به اطلاعات باشند. به عنوان مثال، می‌توان قوانینی را تدوین کرد که به کاربران اجازه می‌دهد کنترل بیشتری بر داده‌های شخصی خود در پلتفرم‌های آنلاین داشته باشند. علاوه بر این، حقوق متاکیری می‌تواند تعاملات اقتصادی در دنیای دیجیتال را تسهیل کند. این امر از طریق ایجاد قوانین شفاف برای قراردادهای هوشمند، مبادلات ارزهای دیجیتال، و تجارت الکترونیک امکان‌پذیر می‌شود. افزایش شفافیت در مبادلات آنلاین نیز یکی دیگر از فرصت‌های مهم است. با تدوین قوانین مناسب، می‌توان الزاماتی را برای شرکت‌های فناوری ایجاد کرد تا نحوه استفاده از الگوریتم‌ها و داده‌های کاربران را به صورت شفاف‌تر اعلام کنند. این امر می‌تواند به افزایش اعتماد کاربران و کاهش سوءاستفاده‌های احتمالی منجر شود. در کنار فرصت‌ها، تهدیدهای قابل توجهی نیز در حوزه حقوق متاکیری وجود دارد. یکی از مهم‌ترین این تهدیدها، احتمال نقض حریم خصوصی است. با گسترش فناوری‌های جمع‌آوری داده و هوش مصنوعی، خطر سوءاستفاده از اطلاعات شخصی افزایش می‌یابد. هک‌کردن اشیاء مجازی، در متاورس هر تعامل، حرکت و حتی نگاه کاربر می‌تواند ردیابی و ثبت شود. جاسوسان دیجیتال ممکن است از این داده‌ها برای جمع‌آوری اطلاعات حساس استفاده کنند. چالش‌های مربوط به مالکیت معنوی در فضای مجازی نیز از دیگر تهدیدهای مهم است. با توجه به سهولت کپی و انتشار محتوا در اینترنت، حفاظت از حقوق مؤلفان و هنرمندان دشوارتر شده است. این مسئله به ویژه در مورد محتواهای تولید شده توسط هوش مصنوعی پیچیده‌تر می‌شود، زیرا تعیین مالکیت و حقوق مربوط به این محتواها چالش‌برانگیز است. مسئله هویت دیجیتال و امنیت اطلاعات نیز از دیگر تهدیدهای جدی در این حوزه است. با افزایش تعاملات آنلاین، خطر سرقت هویت و کلاهبرداری‌های اینترنتی افزایش می‌یابد. همچنین، حملات سایبری و نقض امنیت داده‌ها می‌تواند منجر به افشای اطلاعات حساس شخصی و مالی شود. ضرورت توجه به حقوق متاکیری با توجه به گسترش روزافزون فناوری‌های دیجیتال و افزایش تعاملات در فضای مجازی، بیش از پیش احساس می‌شود. یکی از مهم‌ترین ضرورت‌ها، نیاز به تدوین قوانین جامع و به‌روز است. قوانین فعلی در بسیاری از کشورها برای مواجهه با چالش‌های دنیای دیجیتال کافی نیستند و نیاز به بازنگری و به‌روزرسانی دارند. به عنوان مثال، قوانین مربوط به حفاظت از داده‌ها باید با توجه به پیشرفت‌های اخیر در زمینه هوش مصنوعی و یادگیری ماشینی به‌روز شوند. ایجاد سازوکارهای نظارتی مؤثر نیز از دیگر ضرورت‌های این حوزه است. با توجه به پیچیدگی و سرعت تغییرات در فضای دیجیتال، نیاز به نهادهای نظارتی تخصصی که توانایی درک و واکنش سریع به تحولات فناوری را داشته باشند، احساس می‌شود. این نهادها باید قادر باشند تعادلی بین حمایت از حقوق کاربران و تشویق نوآوری در صنعت فناوری ایجاد کنند. آموزش عمومی در زمینه حقوق و مسئولیت‌های دیجیتال نیز یکی دیگر از ضرورت‌های مهم است. در متاورس، طراحان و هنرمندان می‌توانند اشیاء، لباس‌ها و حتی فضاهای منحصر به فردی خلق کنند. کپی غیرمجاز این آثار می‌تواند به راحتی و در مقیاس بزرگ انجام شود. حقوق متا کیفری می‌تواند چارچوبی برای حمایت از حریم خصوصی، امنیت و حقوق مالکیت معنوی کاربران در فضای مجازی ایجاد کند. استفاده از فناوری‌های واقعیت مجازی در دادگاه‌ها می‌تواند به بازسازی صحنه جرم و درک بهتر وقایع کمک کند. حقوق متاکیفری می‌تواند قوانین و رویه‌های لازم برای استفاده از این فناوری‌ها در روند دادرسی را تعیین کند. با تدوین قوانین متاکیفری، می‌توان چارچوب‌های پیشگیرانه برای جلوگیری از وقوع جرم در فضای متاورس ایجاد کرد. این امر می‌تواند شامل

آموزش کاربران، نظارت بر فعالیت‌های مشکوک و ایجاد سازوکارهای امنیتی باشد.حقوق متا کیفری می‌تواند مجازات‌های متناسب با جرایم ارتکابی در فضای متاورس را تعریف کند. این می‌تواند شامل مجازات‌های مجازی مانند محدودیت دسترسی به فضاهای خاص در متاورس یا حتی زندان‌های مجازی باشد از آنجا که فضای متاورس مرزهای جغرافیایی را درمی‌نوردد، ایجاد یک چارچوب حقوقی بین‌المللی برای رسیدگی به جرایم فراملی ضروری است. پیشنهاد می‌شود که تحقیقات آینده بر روی تأثیرات اجتماعی–اقتصادی حقوق متاکیری متمرکز شوند. این می‌تواند شامل بررسی تأثیر قوانین جدید بر نوآوری در صنعت فناوری، تغییرات در الگوهای مصرف دیجیتال، و تأثیر بر بازار کار باشد. همچنین، مطالعه روش‌های نوآورانه برای حل اختلافات در فضای مجازی، مانند استفاده از هوش مصنوعی در داوری آنلاین، می‌تواند راهگشا باشد. در نهایت، باید تأکید کرد که حقوق متاکیری فراتر از یک موضوع صرفاً حقوقی است و ابعاد اخلاقی و اجتماعی گسترده‌ای دارد. توجه به این حوزه و تلاش برای توسعه آن، می‌تواند زمینه‌ساز ایجاد یک فضای مجازی امن‌تر، عادلانه‌تر و پویاتر برای همه کاربران باشد. این امر مستلزم تعهد مستمر به حفظ ارزش‌های انسانی در عصر دیجیتال و انعطاف‌پذیری در برابر تغییرات سریع فناوری است.

References

1-Alawadhi, Ibtesam Mohammed. "Future Cybercrimes in the Metaverse: A Comprehensive Forecast." Forecasting Cyber Crimes in the Age of the Metaverse. IGI Global, 2024. 24-32. DOI: 10.4018/979-8-3693-0220-0.ch002

2-Bailenson, J. N., Blascovich, J., Beall, A. C., & Noveck, B. Law & Policy, 28, no. 2 (2006): 246-270, DOI:10.1111/j.1467-9930.2006.00226.x

3-Bertazzolo, Giacomo. NFTS IN THE DIGITAL AGE: CYBERSECURITY RISKS AND AI-POWERED SMART CONTRACT SOLUTION. Diss. Politecnico di Torino, 2023

4- Brassel, J. Murder in the Metaverse could be a real crime, 2022, URL: https://www.beyondgames.biz/21556/murder-in-the-metaverse-could-be-a-real-crime/ accessed: 14.02.2023.

5- Brenner, S.W. Cybercrime and the Law: Challenges, Issues, and Outcomes, Northeastern University Press, Boston: 2012

6-Bryden, Sarah (2024). Artificial Intelligence and Criminal Justice . Oxford: Oxford University Press

7-Brown, A. B. Monetizing platforms: The challenges of revenue generation. Journal of Business Strategy, 45, no. 3(2022): 12-34. https://doi.org/10.5555/5555555

8-Brown, M. Examining Privacy Risks and Challenges in the Metaverse. Journal of Privacy and Security, Vol. 4, no. 2(2024): 15-30 doi:10.1080/23738871.2024.1998573

9-Carissoli, C., Villani, V., & Riva, G. Does the Metaverse need Minority Report-style “precrime” algorithms? Risks for privacy violation. Annual Review of Cybertheory and Telemedicine, 20, no. 1(2022): 63-68.

10- Chung, S. The Problems with Trying to Apply Real-World Laws in the Virtual Metaverse, 2022, URL: https://abovethelaw.com/2022/02/the-problems-with-trying-to-applyreal-world-laws-in-the-virtual-metaverse/, accessed: 14.02.2023

11-Cuartas, V. The metaverse: A critical approach to a legal definition. Computer Law & Security Review, 47, (2022): 105680. https://doi.org/10.1016/j.clsr.2022.105680

12- El Asam, Aiman, and Muthanna Samara. "Cyberbullying and the law: A review of psychological and legal challenges." Computers in Human Behavior 65 (2016): 127-141.

13-Elliptic Metaverse Report, 2022, URL: https://www.elliptic.co/hubfs/Crime%20in%20the%20Metaverse%202022%20final.pdf, accessed: 14.02.2023

14-Ghazi, Emadeddin & Shahbazi, Hadiseh. The Role of Artificial Intelligence in Financial Management (Necessities, Applications and Challenges). Proceedings of the 7th International Conference on Management and Industry, pp. 502-509. [In Persian]

15-Grabosky, Peter N. and Smith, Russell G. (1998), Crime in the Digital Age, Controlling Telecommunications and Cyberspace Illegalities. New Brunswick, NJ: Transaction Publishers, New York, 1st Edition

16-Haber, Eldar. "The criminal metaverse." Indiana Law Journal 99.3 (2024): 4

17-Jathavedan, S. The Buzz Around the ‘Metaverse’, 2022, URL: https://www.khuranaandkhurana.com/2022/10/12/metaverse-blurred-lines-forcriminal-law/, accessed: 14.02.2023

18-Khalili Baji, Aref & Shamloo, Bagher (2021). Criminalization in the Field of Cryptocurrencies. Criminal Law Doctrines, 18(21), 29-68. [In Persian]

15-Lal Alizadeh, Mohsen (2023). Emerging Legal Issues in the Three-Dimensional Space of Metaverse. Civil Law Knowledge, 23, 68-96. [In Persian]

19-Latifzadeh, Mahdieh & Ghabooli Dorafshan, Seyed Mohammad Mehdi (2023). Introducing Digital Identity in the Metaverse, Identifying Related Legal Challenges and Seeking Solutions. Private Law Studies, 2, 349-372[In Persian]

20 -Lee, C.H. Threats to metaverse economy. Journal of Virtual Economies, 145, no. 67(2024): 101-114. https://doi.org/10.2000/987-654321

21-Lee, Jennifer, Smith, Michael, and Johnson, Sarah (2022). "Legal Challenges in the Metaverse". Journal of Cyber Law, 15(3), pp. 234-251

22-Mahdavi Sabet, Mohammad Ali & Moradi, Ghasem (2017). Iran's Criminal Policy in Cyberspace. Social Sciences Studies, Winter 2017, 3(4), 97-102. [In Persian]

23-Mahmoudi, Mohsen & Sadeghi, Salar (2022). Metaverse and Its Impact on Lifestyle. Virtual Space Legal Studies, 45-62. [In Persian]

24-Mirashrafi, Amir Hossein (2022). Scientific Analysis of the Metaverse World and Its Future Perspective. New Approaches in Islamic Studies, 12, 387-404[In Persian].

25-Moradi Berlian, Mehdi (2022). An Introduction to the Legal Consequences and Challenges of the Metaverse. Legal Research Quarterly: Law and Technology Special Issue, 25, 363-392. [In Persian]

26- Muharem Kianieff, (2018). Criminal Law in the Age of Blockchain, London, Routledge.

27- Nafarette, J. Chinese Courtroom Uses VR to Revisit Crime Scene, 2018, URL: https://vrscout.com/news/chinese-courtroom-vr-crime-scene/, accessed: 14.02.2023

28-Shah Abadian, Ahad, Haddadi, Mohammad Hassan & Marzi Alamdari, Jebreil (2023). Examining E-commerce Opportunities in the Metaverse. Journal of Islamic Marketing Research, 1, 119-134. [In Persian]

29-Sina, Soghra, Afshar, Fatemeh & Hasanzadeh, Zeinab (2010). Computer Damages and Crimes in the Virtual World. Mazandaran Police Knowledge, Summer 2010, 1(1) [In Persian]

30 -Thompson, M. K. Threats to metaverse network. Journal of Emerging Technologies, 123, no. 45 (2024): 78-91. https://doi.org/10.1000/123-456789

31-Wall, David S. (2007). "Digital Identities and Cybercrime". In Yvonne Jewkes and Majid Yar (eds.), Handbook of Internet Crime. Cullompton, Devon: Willan Publishing, pp. 67-87

32 -Wang, S. Threats to physical world and human society. International Journal of Mixed Reality, 156, no. 78(2024): 122-135. https://doi.org/10.3000/111-222333

33-Wang, Yuntao, et al. "A survey on metaverse: Fundamentals, security, and privacy." IEEE Communications Surveys & Tutorials 25.1 (2022): 319-352. DOI: 10.1109/COMST.2022.3202047

34-Wang, Y., Su, Z., Zhang, N., Xing, R, Liu, D., Luan, T.H., & Shen, X. A Survey on Metaverse: Fundamentals, Security, and Privacy, IEEE Communications Surveys & Tutorials, 25, (2022): 319-352, DOI: 10.1109/COMST.2022.3202047

35- Zhou, Z., Bandari, R., Kong, J., Qian, H., & Roy, S. The Metaverse - A survey. Computers & Graphics, 2022. 104904.