مطالعات حقوق خصوصی

شاپا الکترونیکی: ۶۶۲۲-۲۵۸۸
دوره ۵۳، شماره ۲
تابستان ۱۴۰۲ (مقاله علمی پژوهشی)

Homepage: https://jlq.ut.ac.ir/

معرفی هویت دیجیتال در متاورس، شناسایی چالش‌های حقوقی مربوط به آن و جست‌وجوی راه‌حل*

مهدیه لطیف‌زاده[۱]، سید محمدمهدی قبولی درافشان[۲] ✉ **

۱. دانش‌آموختهٔ دکتری حقوق خصوصی، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران. رایانامه: m.latifzadeh@mail.um.ac.ir

۲. نویسندهٔ مسئول: دانشیار گروه حقوق خصوصی، دانشکدهٔ حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران. رایانامه: ghaboli@um.ac.ir

چکیده

متاورس فضای دیجیتالی سه‌بعدی است که برای افراد با ایجاد حسِ حضور، امکان تعامل و کسب تجارب مختلف را فراهم می‌کند. این دنیای مجازی که در حال حاضر فراوان استفاده می‌شود، بستری نوین نیست لیکن امروزه به‌دلیل توسعهٔ فناوری‌های مختلف، بیش‌ازپیش بر ابعاد مختلفی از زندگی اشخاص اثرگذار است. در این محیط، کاربران می‌توانند با ماهیت‌های دیجیتالی به نام آواتار، خودِ دیگری از هویتشان ارائه کنند و در قالب این هویت دیجیتال یا هویت مجازی با دیگران تعامل داشته باشند و به فعالیت بپردازند. در کنار مزایایی که این جهان دیجیتال به ارمغان آورده است، چالش‌های بسیاری را نیز ایجاد کرده است که از جملهٔ آنها چالش‌های حقوقی است. در واقع رونق متاورس، مسائل حقوقیِ مختلفی ازجمله چگونگی حمایت از هویت دیجیتالی اشخاص در متاورس را مطرح کرده است. این جستار با روشی توصیفی - تحلیلی، سعی کرده است ضمن تعریف هویت دیجیتال در متاورس به چالش‌های حقوقی مربوط به هویت‌های مجازی در این محیط و ارائهٔ راه‌حلی جهت پاسخ به معضلاتِ پیش رو، بپردازد. به موجب برآمد پژوهش، استفادهٔ موردی از برخی قوانین و مقررات خاص مانند مقررات اروپایی حفاظت از داده و قانون هوش مصنوعی اتحادیهٔ اروپا در کنار بهره‌مندی از فناوری بلاک‌چین با توجه به استفاده از نوع متناسب آن، می‌تواند در خصوص حمایت‌های مؤثر از هویت‌های دیجیتال کارامد باشد.

واژه‌های کلیدی: بلاک‌چین، حفاظت از داده، متاورس، هویت دیجیتال، هویت خودمختار.

---

* این اثر تحت حمایت مادی بنیاد ملّی نخبگان انجام شده است.

** **استناد:** لطیف زاده، مهدیه؛ سید محمدمهدی قبولی درافشان. (تابستان ۱۴۰۲) «معرفی هویت دیجیتال در متاورس، شناسایی چالش‌های حقوقی مربوط به آن و جست‌وجوی راه‌حل»، *مطالعات حقوق خصوصی*، ۵۳، ۲: ۳۴۹ - ۳۷۲.

DOI: 10.22059/JLQ.2023.353867.1007743

تاریخ دریافت: ۲۴ دی ۱۴۰۱، تاریخ بازنگری: ۱۶ خرداد ۱۴۰۲، تاریخ تصویب: ۷ تیر ۱۴۰۲، تاریخ انتشار: ۲۵ مرداد ۱۴۰۲.

ناشر: مؤسسه انتشارات دانشگاه تهران

۱. مقدمه

متاورس[۱] دنیای مجازی سه‌بعدی است که تاکنون در حوزهٔ بازی‌های مجازی رونق زیادی داشته است. با این حال، به لطف توسعهٔ فناوری‌های مختلف، متاورس ابعاد جدیدی یافته است تا بتواند فرصت‌هایی به‌اندازهٔ دنیای واقعی یا شاید بیشتر از آن در زمینه‌های مختلف زندگی روزمره از جمله توسعهٔ کسب‌وکار، نحوهٔ ارتباط اشخاص، فعالیت‌های علمی و... ارائه دهد (LÓPEZ & PERERA, 2022: 1). در واقع متاورس جهان دیجیتالی است که برای کاربران تعاملات چندبعدی را با دخیل کردن ادراک افراد فراهم می‌کند. کاربران در متاورس از طریق آواتارها[۲] (هویت دیجیتال یا هویت مجازی که انعکاسی از هویت فیزیکی کاربران هستند) با یکدیگر به شیوه‌های مختلف تعامل و ارتباط دارند. فعالیت‌های دنیای واقعی را می‌توان با استفاده از فناوری‌هایی مانند واقعیت افزوده (AR) و واقعیت مجازی[۳](VR)، بلاک‌چین[۴] و سایر ابزارهای فناوری در متاورس انجام داد (See. Dremliuga et al. , 2020: 76). این جهان دیجیتال

---

۱. متاورس‌ها انواع مختلفی دارند که مبتنی بر ساختارشان است. در برخی از انواع متاورس مسئولیتِ مدیریت تمام جنبه‌های مرتبط با این محیط از جمله مدیریت فعالیت‌های اقتصادی بین کاربران یا داده‌های تولیدشده با مرجعی مرکزی است. این متاورس‌ها «متمرکز» – centralized – نامیده می‌شوند. از سوی دیگر متاورس‌های «غیرمتمرکز» – Decentralized – وجود دارند که به‌جای متمرکز شدن فعالیت در یک مرکز واحد، عملکردها با استفاده از فناوری بلاک‌چین غیرمتمرکز می‌شوند. در این حالت متاورس‌ها به‌صورت غیرمتمرکز یا خودمختار – Decentralised autonomous organisation (DAO) – اداره می‌شوند. این نوع، ابزاری مفید برای اثرگذاری بیشتر افراد در محیط متاورس است(See. Gadekallu et al., 2022: 2 & See. Kane & Duranske, 2008: 12).

2. Avatars

3. Augmented Reality and Virtual Reality

واقعیت افزوده به فناوری اطلاق می‌شود که در آن عناصری از دنیای دیجیتال با دنیای واقعی ترکیب می‌شود. در این نوع از فناوری به نمایش عناصر دیجیتال در دنیای واقعی بسنده نمی‌شود؛ بلکه امکان ارتباط حسی بیشتر نیز وجود دارد ولی شخص به‌طور کامل از دنیای واقعی جدا نمی‌شود. عینک‌های هوشمند از اصلی‌ترین ابزارهای مورد استفاده در واقعیت افزوده هستند. کاربران این فناوری – بر خلاف واقعیت مجازی که یک محیط کاملاً مصنوعی ایجاد می‌کند – یک محیط واقعی را با اطلاعات ادراکی تولیدشده روی آن تجربه می‌کنند. در مقابل واقعیت مجازی یک محیط سه‌بعدی شبیه‌سازی‌شده است که کاربران را قادر می‌سازد تا به کاوش و تعامل با یک محیط مجازی نزدیک به واقعیت بپردازند. محیط با سخت‌افزار و نرم‌افزار رایانه ایجاد می‌شود. هرچه کاربران بیشتر در محیط واقعیت مجازی فرو روند – و محیط فیزیکی اطراف خود را مسدود کنند – باورپذیری بیشتری نسبت به این محیط اتفاق خواهد افتاد. تفاوت اصلی بین این دو فناوری این است که واقعیت مجازی یک شبیه‌سازی رایانه‌ای است. بدان‌معنی که واقعیت با یک جهان گرافیکی جایگزین می‌شود. با استفاده از سخت‌افزار مناسب، امکان تعامل کامل کاربر با دنیای دیجیتال وجود دارد. بنابراین تفاوت‌های مهمی نیز بین عینک‌های هوشمند واقعیت افزوده در مقایسهٔ عینک‌های واقعیت مجازی وجود دارد. سخت‌افزاری که برای واقعیت مجازی طراحی شده است، به دستگاه‌های حسی نیاز دارد تا حرکات دنیای واقعی را به یک واقعیت مدلسازی‌شده تبدیل کند. با استفاده از صفحهٔ نمایش، کاربر می‌تواند دنیای دیجیتال را درک کند و در آن تعامل داشته باشد. این امر به دو لنز بین کاربر و صفحهٔ نمایش نیاز دارد. آنها حرکت چشم را تفسیر می‌کنند و حرکت فرد را با دنیای واقعیت مجازی تطبیق می‌دهند (See. TeamViewer, 2022).

4. Blockchain

توضیح تفصیلی این فناوری در بند نهایی پژوهش خواهد آمد.

باوجود مزایای آشکار، پیچیدگی‌های مخصوص به خود را دارد و علوم مختلفی را درگیر کرده است. در این زمینه علم حقوق نیز با سؤالات متعددی روبه‌روست. با توجه بـه فراگیـری ایـن فناوری و تأثیر آن بر زندگی اشخاص، توجه به چالش‌های حقوقی متاورس، تلاش برای کنترل این محیط و حل مسائل مربوط به آن ضروری است. یکـی از ایـن مـوارد تبیـین چـالش‌هـای حقوقی مربوط به هویت در متاورس یعنی هویت دیجیتال یا هویت مجازی و مسائل مرتبط بـا آن ازجمله چگونگی حمایت حداکثری از هویت دیجیتال در متاورس است. به‌خصوص اینکـه توجه به چالش‌های حقوقی متاورس به‌طور کلی و پرداختن به مسائل حقوقی مربوط به هویت دیجیتال در این محیط در پژوهش‌های به زبان فارسی و در دامنهٔ نظام حقوقی ایـران- در ایـن خصوص منابع لاتین بسیار تـوجهی متعددنـد و بـه جنبـه‌هـای مختلفـی نـسبت بـه متـاورس پرداخته‌اند- بسیار محدود است. برای نمونه مقالات اندکی در این خصوص وجـود دارنـد کـه رویکرد و هدف آنها نیز با این پژوهش متفاوت است و خود این امر اهمیـت ایـن پـژوهش را پررنگ‌تر می‌کند. به‌طور مثال شاکری و جعفرپور (۱۴۰۱) در مقاله‌ای با عنوان «امکان‌سـنجی اعمال حقوق معنوی مؤلف تحت فناوری‌های نوین اطلاعات و ارتباطـات» در جهـت جریـان حقوق معنوی صاحبان اثر بر اساس فناوری‌هـای مختلـف بـه متـاورس نیـز اشـاره کـرده‌انـد. همچنین عاکفی قاضیانی و همکاران (۱۴۰۱) در مقالـه‌ای بـا عنـوان «متـاورس و چـالش‌هـای حقوقی در حوزهٔ حقوق اموال» به‌طور خاص بر مسائل حقوقی مربوط بـه مالیـت در متـاورس قلم زده‌اند. همان‌طورکه از عناوین و محتوای این مقالات روشن است، پژوهش حاضر کـه بـر هدف چگونگی حمایت از هویت در متاورس، تمرکز دارد، رویکرد و غایتی دیگر دارد. بـدین ترتیب در راستای نیل به هدف پژوهش، ابتدا هویت دیجیتال (مجـازی) در متـاورس تعریـف خواهد شد، سپس چالش‌های حقوقی مربوط به هویت‌های دیجیتالی مورد توجه قرار خواهنـد گرفت و در نهایت راه‌حل‌هایی با هدف حل معضلات حقـوقی پـیش رو جـست‌وجوخواهنـد شد.

۲. تبیین مفهوم و ماهیت شناسی هویت دیجیتال در متاورس

گام نخست و منطقی برای تحقیق در مورد یک موضوع، تعریف آن و شناسایی ماهیتِ موضوع مورد بحث است. بدین‌ترتیب در این بند ابتدا هویت دیجیتال در متاورس تعریف خواهد شـد، سپس ماهیت آن بررسی خواهد شد.

۲. ۱. تعریف هویت دیجیتال

هویت به معنای منحصربه‌فرد بودن یا فردیت شخص تعریف می‌شود و در جایی است که فـرد به‌عنوان شخصی خاص شناسایی شود یا قابل‌شناسایی باشد و بدین‌ترتیب از دیگران قابل تمییز

است (میرشکاری، ۱۳۹۶: ۷۱). شناسه‌های مختلفی که شناسایی یا قابلیت شناسایی را ایجاد می‌کنند، از جمله ویژگی‌های زیست‌سنجی[1] (اجزای چهره به‌خصوص عنبیهٔ چشم یا اثرانگشت)، نام، تصویر، صدا، شمارهٔ کارت شناسایی، داده‌های مکانی و... است که داده‌های شخصی[2] اشخاص حقیقی‌اند (See. Kavut, 2021: 532). با وجود متاورس آنچه امروزه قابل‌توجه است، تعریف هویت دیجیتالی اشخاص است. در این زمینه هویت در متاورس را می‌توان تقریباً کدی ژنتیکی مانند هویت زیست‌سنجی دانست. این یعنی اشخاص با استفاده از خود دیگر[3] در محیط متاورس حیات دارند. هویت‌های دیجیتال در متاورس ماهیتی منحصربه‌فرد دارند و بخشی جدایی‌ناپذیر از دنیای مجازی‌اند. این هویت‌ها می‌توانند اشکال مختلفی داشته باشند و مربوط به اشخاص حقیقی یا حقوقی باشند؛ بنابراین حتی یک کاربر می‌تواند در شرایط مختلف، هویت‌های دیجیتال متفاوتی داشته باشد (مانند هویت محل کار و هویت شخصی)، ولی در نهایت همهٔ آنها مرتبط با هویت واقعی کاربرند. هویت‌های دیجیتال را می‌توان با استفاده از توکن‌های غیرمثلی یا غیرقابل تعویض[4] (NFT) به‌دست آورد. دارایی‌های دیجیتال (توکن‌های غیرمثلی) نیز مانند هویت‌های دیجیتال از عناصر اصلی متاورس‌اند (Zhenlin et al. , 2017: 4&5).

هویت‌های دیجیتالی کاربران در قالب آواتارها بروز می‌کند. آواتارها، نمایش شخصیت اشخاص در متاورس هستند. درواقع فناوری‌های متاورس به کاربران این امکان را می‌دهد که آواتارهایی داشته باشند که نه‌تنها ظاهر فیزیکی فرد را دارند، بلکه حرکات و رفتارهای یک فرد را نیز بازسازی می‌کنند. این کار به‌سادگی با اسکن یک عکس و تبدیل آن به یک آواتار

1. Biological
2. Personal Data

مقررات عمومی حفاظت از دادهٔ اتحادیهٔ اروپا – The General Data Protection Regulation (GDPR) – جامع‌ترین بستر قانونی است که متضمن حمایت از داده‌های شخصی در جنبه‌های مختلفی است. این مقررات به حمایت از هویت و چگونگی حفاظت مناسب از داده‌های شخصی می‌پردازد که به‌طور کلی مربوط به هویت واقعی افراد است. دادهٔ شخصی از نگاه این مقررات به معنای هر اطلاعاتی است که مربوط به شخص حقیقی شناخته‌شده یا قابل‌شناسایی (شخص موضوع داده) است. یک فرد حقیقی قابل‌شناسایی کسی است که به‌طور مستقیم یا غیرمستقیم، به‌ویژه با ارجاع به یک شناسه ازجمله نام، شمارهٔ شناسایی، اطلاعات مکانی، شناسهٔ آنلاین یا به یک یا چند ویژگی مانند هویت فیزیکی، فیزیولوژیکی، روانی، اقتصادی، فرهنگی و اجتماعی آن فرد حقیقی، شناسایی شود (EUR-Lex, 2016: 33)

3. Alter Ego
4. Non-Fungible-Token

توکن‌های غیرقابل تعویض نوعی ابزار مجازی است که جزئی حیاتی برای متاورس محسوب می‌شود. در متاورس، NFT به‌عنوان بازنمایی از مالکیت دارایی‌ها عمل می‌کند. برای مثال، قطعات زمین مجازی در واقع NFT هستند. به دیگر سخن NFT ها دارایی‌های دیجیتالی‌اند که مبین اشیای درون متاورس‌اند. آنها اغلب به‌صورت آنلاین با استفاده از ارزهای رمزنگاری‌شده خریداری و معامله می‌شوند. قبل از جریان توکن‌های غیرقابل تعویض هیچ روش تضمینی برای تأیید مالکیت اشیای آنلاین وجود نداشت. بدین‌سبب می‌توان گفت توکن‌های غیرقابل‌تعویض نقش مهمی در اقتصاد متاورس ایفا می‌کنند (See. Belk, Humayun, & Brouard, 2022: 199).

سه‌بعدی امکان‌پذیر است. پیچیده‌ترین آواتارها، اشیای تصنعیِ بصری و شناختی‌انـد کـه مبـین حضور فرد در دنیای مجازی‌اند یـا آن چیـزی هـستند کـه کـاربر تمایـل دارد بـه‌نظـر برسـد. آواتارهای مجازی همچنین ممکن است نمایانگر اعمال کاربر، جنبـه‌هـای مختلـف شخـصیت کاربر یا موقعیت اجتماعی کـاربر در محـیط مجـازی باشـند. بـدین ترتیـب آواتارهـا نمایـشی واقع‌گرایانه از صاحب یا خلق‌کنندهٔ خود هستند یا حتی می‌تواننـد نمایـشی از شخـصی دیگـر (مانند یک بازیگر زنده یا فوت‌شده یا شخصیت تاریخی) یا یـک حیـوان یـا حتـی موجـودی افسانه‌ای باشند (Barfield & Blitz, 2018: 13). پس از آماده شدن آواتار، کـاربران مـی‌تواننـد بـا استفاده از ابزارهای واقعیت مجازی مانند عینک و... به متاورس دسترسـی داشـته باشـند. ایـن دستگاه‌های هوش مصنوعی دارای فناوری هستند که می‌توانند حرکات و رفتارهای کاربر را در زمان واقعی بازتولید کنند و تجربه را تا حد امکان واقعـی کننـد (See. Barfield, 2006: 658). بـا تبیین مفهوم هویت‌های دیجیتال برای حمایت‌های مناسب، شناسایی ماهیت این هویت‌هـا نیـز بسیار مهم است که در بند بعد بحث خواهد شد.

۲ .۲. شناسایی ماهیت هویت دیجیتال

با وجود تعاریف پیش‌گفته و تبیین مفهوم اصطلاحی هویت دیجیتال در منابع مختلف، این امـر هنوز به‌طور کامل درک نشده است. درواقع در زمان حـال بیـشتر افـراد مـی‌داننـد کـه هویـت دیجیتال دارند؛ لیکن ماهیت حقوقی آن، چگونگی عملکرد آن، پیامدهای مربوط به آن در حال حاضر و در آینده و لزوم وجود حمایت‌های قانونی نسبت به آن را بـه‌خـوبی درک نکـرده‌انـد (Sullivan, 2018: 723). هویت دیجیتالی باید از طریق بسترهای مربوطه حمایت شود. این وظیفهٔ قانونگذار، رویهٔ قضایی و دکترین حقـوقی اسـت کـه بـا توجـه ویـژه بـه هویـت دیجیتـال و چالش‌های مربوط به آن، برای اشخاص درکی جامع در زمینهٔ هویت دیجیتـالی‌شـان همچنـین حقـوق و تکـالیف مربـوط بـه آن ایجـاد کننـد (See. Naik & Jenkins, 2020: 1). در ایـن خصوص‌شناسایی ماهیت این هویت‌ها نیز ضروری است.

در این خصوص سؤال مرتبط این است که آیا اجزای هویت دیجیتـال را مـی‌تـوان جـزء داده‌های شخصی تلقی کرد و ماهیت آنها را مرتبط با داده‌های شخصی دانست. در مقام پاسـخ باید گفت زندگی متاورس مجازی است نه واقعی؛ بنابراین کسانی که مایل به تجربهٔ این دنیای دیجیتال هستند، باید یک آواتار ایجاد کنند. آواتارها می‌توانند به‌صـورت هـر ظـاهر دیجیتـالی باشند که کاربر انتخاب می‌کند، به‌طوری‌که ظاهر انتخابی کاربران حتی می‌تواند به شکل حیوان باشد، زیرا هیچ قاعده‌ای وجود ندارد که کاربران فقط به شکل انسان یا به‌صورت خاصی ظاهر شوند. بدین ترتیب هر کاربر می‌تواند هر شخصیت دیجیتالی که مـی‌خواهـد ایجـاد کنـد. ایـن

شخصیت دیجیتالی ممکن است شخصیت واقعی کاربر را شناسایی کند یا قابل‌شناسایی کند، درحالی‌که ممکن است این‌گونه نباشد. بدون شک اگر یک شخصیت دیجیتالی، یک فرد واقعی را در دنیای واقعی شناسایی کند یا قابل‌شناسایی کند، این امر، جزء داده‌های شخصی محسوب می‌شود. برای مثال در حال حاضر افراد می‌توانند جلساتی را در اتاق‌های جلسات مجازی با حضور شرکت‌کنندگان بسیاری (مانند جلسات مربوط به داوری‌های بین‌المللی) برگزار کنند. در نتیجه، دادهٔ شخصی تلقی شدن شخصیت‌های دیجیتالی برحسب مورد و با لحاظ شرایط خاص است. همان‌طور که بیان شد ممکن است هویت دیجیتالی مرتبط با شخصیت دنیای واقعی باشد. برای مثال، ترجیحات، رفتارها و... از یک کاربر می‌تواند نظارت و پردازش شود، تبلیغات بازاریابی مرتبط با داده‌های پردازش‌شده از متاورس ممکن است به کاربری ارسال شود که شخصیت دیجیتالی مرتبط با دنیای واقعی دارد. در صورت دادهٔ شخصی بودن اجزای هویت دیجیتال، جریان بسترهای قانونی مربوط به حریم خصوصی اطلاعاتی به‌طورکلی و حفاظت از داده‌های شخصی به‌طور خاص لازم است؛ لیکن چگونگی و دامنهٔ اعمال این قوانین و مقررات نیاز به بررسی دارد. درواقع ضرورت وجود حمایت‌های حقوقی برای داده‌های شخصی افراد که در محیط متاورس به‌صورت دیجیتالی درآمده‌اند، به‌ویژه برای محافظت از کاربرانی که اهلیت کامل ندارند – مانند کودکان – بر کسی پوشیده نیست؛ لیکن چگونگی حمایت از هویت دیجیتال به‌عنوان دادهٔ شخصی مستلزم بررسی تفصیلی است (See. Cheong, 2022: 491).

۳. بررسی چالش‌های حقوقی مربوط به هویت‌های دیجیتال

بررسی چالش‌های حقوقی مربوط به هویت در متاورس یعنی هویت دیجیتال یا هویت مجازی و مسائل مرتبط با آن ازجمله چگونگی حمایت حداکثری از هویت دیجیتال در متاورس، مسئله‌ای مهم است. همچنین بر مسئلهٔ چگونگی حمایت از هویت دیجیتال، فروعات مختلفی قابل تصور است. این موارد می‌تواند شامل چگونگی حمایت از هویت واحد در متاورس‌های متعدد یا هویت‌های چندگانه؛ شناسایی ویژگی‌های هویت دیجیتال؛ چگونگی تأمین امنیت هویت؛ امکان فروش یا اجاره هویت؛ حمایت از فرزند دیجیتالی و... باشد که توجه تفصیلی به آنها خود مجالی دیگر می‌طلبد. فارغ از این موارد، هویت‌های دیجیتال در متاورس به‌طور کلی با چالش‌های ذیل مواجه‌اند:

۳. ۱. چالش‌های مربوط به شخصیتِ هویت‌های دیجیتال

یکی از مسائل بسیار مهم نسبت به آواتارها چالش‌های حقوقی مربوط به شخصیت آنهاست. با توجه به اینکه هویت‌های دیجیتال با سرعت شایان توجهی هوشمندتر، رفتار آنها پیچیده‌تر و ظاهر آنها به‌طور روزافزون واقع‌گرایانه‌تر و شبه‌انسانی می‌شوند، بحث در خصوص اعطای شخصیت به آنها یا عدم آن بسیار مهم است. برآمده از قوانین فعلی این است که حقوق و تکالیف مربوط به مالک بوده و نه آواتار مجازی که فاقد شخصیت حقوقی است. در واقع مالک خواه شخص حقیقی یا حقوقی باشد، مسئول اعمال آواتار است و آواتار صرفاً به‌عنوان عامل[1] (نماینده) عمل می‌کند. بر اساس این دیدگاه، امری مهم مغفول می‌ماند و آن اینکه مهم نیست که یک هویت دیجیتال چقدر هوشمند باشد و آنها به‌نوعی شیء تحت مالکیت شخص هستند. بدین ترتیب اگر آواتار قراردادی منعقد کند، آن توافق، مالک را - با رعایت قواعد متعارف انعقاد قراردادها - و نه آواتار را متعهد می‌سازد و اگر آواتار مرتکب تخلف شود، مالک آن مسئول جبران هرگونه خسارت است. این در حالی است که آواتارهای مجازی هوشمندتر می‌شوند و می‌توانند اعمالی را مستقل از مداخلات انسانی ایجاد می‌کنند، بدین‌ترتیب این رویه ممکن است تغییر کند. در این حالت، خود آواتارها ممکن است به حمایت‌های حقوقی برای اقداماتی که به نفع یا ضررشان انجام می‌شود، نیاز داشته باشند. اگر هویت‌های دیجیتال همچنان هوشمندتر شوند و از سوی دیگر اشخاص زمان بیشتری را در متاورس صرف تعامل توسط آنها کنند، مسائل حقوقی مهمی به‌وجود می‌آیند (Barfield & Blitz, 2018: 16 & 41). برای نمونه هنگام استفاده از آواتارهایی که تحت کنترل کامل کاربران هستند، چالش‌هایی وجود دارد، ازجمله اینکه کاربران می‌توانند برخلاف عادات خود در تعاملات اجتماعی -در دنیای واقعی- رفتار کنند و می‌توان آواتارها را جایگزین کرد و به دلخواه تغییر داد و در نتیجه شفافیت رفتار اجتماعی را تحت تأثیر قرار داد (Dwivedi et al., 2022: 11). در مقابل با توسعهٔ آواتارهای مجازی که به‌طور روزافزون از مداخلات و تصمیم‌گیری انسانی مستقل‌تر می‌شوند و شروع به تشخیص الگوریتم‌های خود می‌کنند، چالش‌ها بیشتر می‌شود و به‌تبع، یافتن راه‌حل برای آنها نیز دشوارتر خواهد شد. بدین ترتیب باید در قوانین و مقرراتی جدید با رویکردی خاص روشن شود که چگونه باید با چنین ماهیت‌هایی برخورد شود؟ (See. Barfield & Blitz, 2018: 17). روشن است که متعاقب مسئلهٔ شخصیت هویت‌های دیجیتال در متاورس، مسائل مختلفی به‌دنبال خواهد آمد که بررسی تفصیلی آنها پژوهشی مستقل می‌طلبد.

1. Agent

۳. ۲. چالش‌های مربوط به چگونگی حفاظت از داده‌های شخصی

به‌تناسب این موضوع که در بسیاری از موارد اجزای هویت‌های دیجیتال را می‌توان دادهٔ شخصی دانست، باید به چگونگی حفاظت از داده‌ها و حریم خصوصی اطلاعاتی در متاورس نیز توجه شود. در این خصوص نیز چالش‌های متفاوتی مطرح است که در ذیل به برخی از آنها اشاره می‌شود:

– ضرورت وجود مبانی حقوقی برای پردازش[۱]: به دلیل ماهیت فراگیر بسترکارهای[۲] متاورس، داده‌های شخصی بیشتر جمع‌آوری می‌شوند. یک بسترکار متاورس که از طریق لباس لمسی قابل دسترسی است (ارائهٔ بازخورد لمسی به کاربر) می‌تواند اطلاعاتی در مورد کاربران و ویژگی‌های مختلف آنها از جمله عملکردهای بدن، احساسات و... فراهم کند. اطلاعات موجود در این بسترِ جدید برخلاف رسانه‌های اجتماعی متداول، شامل هر امر جزئی است (See. Singh, 2022: 2&3). همچنین کاربران شرکت‌کننده در متاورس احتمالاً برای مدت‌زمان طولانی در این محیط، حضور خواهند داشت، این امر بدین معناست که الگوهای رفتاری به‌طور مستمر نظارت خواهند شد و به متاورس و کسب‌وکارهای شرکت‌کننده در متاورس (فروشندگان کالا و خدمات) این امکان را می‌دهد تا بفهمند که چگونه بهترین خدمات را به کاربران به روشی فوق‌العاده هدفمند ارائه دهند. به دیگر سخن هدست‌ها و عینک‌های واقعیت مجازی که در متاورس رایج‌اند (البته ممکن است با شیء پیچیده‌تری مانند رابط‌های مستقیم الکترونیکی یا مغزی جایگزین شوند)، ظرفیت جمع‌آوری طیف گسترده‌ای از داده‌های حساس نسبت به فرد موردنظر را دارند تا جایی که این داده‌ها توسط متصدیان متاورس برای اطلاع از ماهیت کاربر یا تصمیم‌گیری در مورد آنها استفاده می‌شود (See. Dwivedi et al. , 2022: 8). بدین‌سبب الزامات قانونی بیشتری باید برای جواز پردازش داده در این محیط وجود داشته باشد. برای نمونه برای حمایت مناسب در محیط متاورس، کاربران به‌احتمال زیاد باید رضایت صریح را برای هر هدفی که از داده‌ها استفاده می‌شود، ابراز کنند (See. Mystakidis, 2022: 439). بدین‌سبب اگر قرار است که فردی با استفاده از فناوری تحلیل نگاه، مورد هدف تبلیغات قرار گیرد، برای قانونی بودن این تبلیغات، به اجازهٔ صریح او نیاز است و رضایت عمومی برای بازاریابی کافی نیست (See. Ning et al. , 2021: 21& 22). در واقع چگونگی رضایت به بازاریابی امری کلیدی در توسعهٔ متاورس برای جواز شیوه‌های جدیدی از بازاریابی است. درعین‌حال

---

۱. به‌طور کلی پردازش دادهٔ شخصی ممنوع است، مگر اینکه سبب خاصی برای پردازش وجود داشته باشد. این موارد که با عنوان مبانی حقوقی پردازش دادهٔ شخصی قابل اشاره‌اند، در بسترهای قانونی مربوطه از جمله در مادهٔ ۶ (۱) GDPR مقرر شده‌اند.

2. Platform

اینکه چگونه این رضایت باید ارائه شود، به این موضوع مربوط می‌شود که آیا متاورس یک مدل غیرمتمرکز[1] است یا به‌صورت متمرکز (به انواع متاورس ازجمله مدل متمرکز و غیرمتمرکز در پاورقی قسمت مقدمه اشاره شده است) جریان دارد (See. Madiega et al. , 2022: 5).

–لزوم حفاظت ویژه از داده‌های شخصی کودکان: در زمینهٔ حفاظت از داده‌ها در متاورس، کودکان باید به‌طور ویژه مورد توجه قرار گیرند؛ چراکه در مورد کودکان حساسیت بیشتری لازم است. قوانین حفاظت از داده بسیاری از کشورها، حفاظت ویژه‌ای را برای داده‌های شخصی کودکان فراهم می‌کند. در این زمینه ضرورت چنین حفاظتی در متاورس که محیطی فراتر از شبکه‌های اجتماعی متعارف و بسترهای آنلاین فعلی است، بر کسی پوشیده نیست. بدین‌علت شیوه‌های پیچیدهٔ تأیید سن، اعمال محدودیت‌های سنی و اجرای اقداماتی برای بازدارندگی کودکان از ارائهٔ داده‌های شخصی‌شان، عناصر ضروری حمایت مؤثر از کودکان در متاورس است که با تأمل و تغییر در قوانین حفاظت از دادهٔ موجود، میسر خواهد شد(See. Livingstone et al. , 2019: 4; See. Siibak & Mascheroni, 2021: 3&4).

–ضرورت توجه خاص به مسائل مربوط به نقض داده: مانند سایر برنامه‌های آنلاین، متاورس با چالش‌های معمول مانند مقابله با حوادث امنیت سایبری و نقض داده‌ها مواجه است. با این حال در متاورس، این نوع حملات ممکن است از طریق فرایندهای پیچیده و آواتارهای هک‌شده، شکل‌های پیش‌بینی‌ناپذیر داشته باشند. بدین دلیل شناسایی و کنترل کردن این حوادث، ممکن است بسیار دشوار باشد (Wang et al. , 2022: 9& 10). در این زمینه تعیین اینکه چه کسی مسئول امنیت داده‌هاست، چگونه می‌توان از وقوع نقض داده جلوگیری کرد و در صورت نقض داده، پیامدهای آن چگونه قابل‌کنترل است، بسیار مهم است. در این خصوص تعیین اینکه چه کسی کنترل‌کننده یا پردازنده[2] است، از جمله مسائلی است که نیاز به بررسی دارد (See. Bavana k. , 2022: 4).

به‌طور کلی چالش‌های مربوط به حفاظت از داده در متاورس بسیار مهم و گسترده است و در این خصوص مسئلهٔ چگونگی اعمال قوانین و مقررات مربوط به حفاظت از داده و حریم

1. Decentralised
2. Controller or Processor

کنترل‌کننده به معنای شخص حقیقی یا حقوقی، مرجع عمومی یا نهاد دیگری است که به‌تنهایی یا به‌طور مشترک با دیگران، اهداف و ابزار پردازش داده‌های شخصی را تعیین می‌کند (EUR-Lex, 2016: 33) . اگر یک شخص – اعم از حقیقی یا حقوقی– یا یک مرجع عمومی یا یک نهاد تصمیم بگیرد که چرا و چگونه داده‌های شخصی باید پردازش شوند، کنترل‌کننده داده است (Colcelli, 2019: 1031). پردازنده نیز به معنای شخص حقیقی یا حقوقی، مرجع عمومی یا نهاد دیگری است که از جانب کنترل‌کننده پردازش داده‌های شخصی را انجام می‌دهد. پردازنده داده‌های شخصی را فقط به نمایندگی از کنترل‌کننده پردازش می‌کند (EUR-Lex, 2016: 33).

خصوصی اطلاعاتی، نسبت به متاورس مطرح است. درواقع جریان چنین بسترهای قانونی اگرچه لازم است؛ لیکن کافی نیست و با توجه به ماهیت و خصایص ویژهٔ متاورس، قانونگذاران باید به تطبیق الزامات قانونی با این محیط، توجه ویژه کنند؛ چراکه این دنیای پیچیده برای کنترل، به قوانین خاص نیاز دارد. خلاصه اینکه این جهان مجازی به قانونگذاری واقعی نیاز دارد.

۴. تلاش برای کنترل متاورس و جست‌وجوی راه‌حل برای رفع چالش‌ها

با توجه به آنچه بیان شد، روشن است که در حال حاضر هیچ بستر قانونی خاصی برای کاهش خطرهای مربوط به متاورس به‌خصوص نسبت به هویت‌های دیجیتال وجود ندارد. این فقدان، شکاف بزرگی برای اعتماد و نیاز افراد به استفاده از فناوری‌های نوین از یک‌سو و لزوم حمایت‌های قانونی در مواجهه با آنها از سوی دیگر است. به دیگر سخن ضرورت قانونگذاری بدین دلیل است که بسترهای حقوقی موجود همچنان برای مقابله با چالش‌های مختلف ازجمله در مورد هویت دیجیتالی اشخاص در متاورس به روشی جامع، فاصله دارند به‌طوری‌که حقوق کاربران در معرض خطر است. بدین‌سبب ظهور متاورس به‌عنوان یک فناوری در حال توسعه، قوانین و مقررات فعلی را نیازمند بازنگری کرده همچنین قانونگذاران را ملزم به ورود به عرصه‌های جدیدی می‌کند که با پیچیدگی‌های فناوری مطابقت داشته باشند (See. Bernal Bernabe et al., 2019: 164934). با وجود خلأهای یادشده، به‌نظر می‌رسد قوانین عمومی که در مورد اینترنت اعمال می‌شود، از جمله برخی از الزامات مربوط به حقوق مالکیت فکری، حقوق قراردادها، قوانین مسئولیت مدنی و قوانین جزایی، در مورد متاورس نیز قابل اعمال هستند. البته چگونگی جریان قوانین و مقررات مختلف بر محیط متاورس باید بررسی شود و بسترهای قانونی موجود به‌صورت مطلق قابل جریان نیست. این امر بدین دلیل است که فناوری‌های نوین، موقعیت‌های پیش‌بینی‌نشده و جدیدی را نیز به‌همراه دارند که باید توسط چارچوب‌های قانونی مناسب مورد توجه قرار گیرند. همچنین با توجه به ماهیت خاص متاورس ممکن است بسترهای حقوقی و قانونی جدیدی که مختص موضوعات حقوقی مختلف‌اند نیز برای کنترل متاورس مناسب باشند. فارغ از بسترهای مذکور، بهره‌مندی از فناوری بلاک‌چین نیز می‌تواند برای کنترل متاورس مناسب باشد. بدین‌سبب در این بند ابتدا به بسترهای حقوقی و قانونی خاص پرداخته می‌شود و سپس در خصوص تأثیر استفاده از بلاک‌چین سخن به میان خواهد آمد.

۴. ۱. قانونمند کردن متاورس با استفاده از بسترهای حقوقی و قانونی خاص

فارغ از بسترهای حقوقی و قانونی عام که به‌دلیل نبود قانونی خاص برای متاورس می‌تواند بر این محیط دیجیتال، قابل اعمال باشند، ممکن است بسترهای قانونی جدیدی که مختص موضوعات حقوقی مختلف‌اند نیز برای کنترل متاورس مناسب باشند، از جمله موارد زیر:

– مقررات «هویت دیجیتال اتحادیهٔ اروپا»[1] در سال ۲۰۲۱ است. مقررات مذکور با هدف اثربخشی بیشتر و رفع کاستی‌های موجود در مقررات «تعیین هویت الکترونیکی و اعتمادبخشی به معاملات الکترونیکی در بازار داخلی اتحادیهٔ اروپا»[2] مصوب ژوئیهٔ ۲۰۱۴، پیشنهاد شده است. این مقررات پیشنهادی چند نوآوری مانند ارائهٔ کیف پول هویت دیجیتال اروپایی[3]، تعهدات جدید برای کشورهای عضو در مورد ابزارها و طرح‌های شناسایی الکترونیکی[4] و ادغام مجموعهٔ داده‌های شناسایی افراد را معرفی می‌کند. دامنهٔ خاص آن مربوط به عملیات پردازش داده‌های شخصی در خصوص شناسایی الکترونیکی و خدمات اعتماد الکترونیکی مانند ایجاد، تأیید و اعتبارسنجی، حفظ و مدیریت امضاهای الکترونیکی، مهرها، بایگانی اسناد الکترونیکی و... است (European Commission, n. d).

–به‌علاوه می‌توان از مقررات و قوانین مربوط به حفاظت از داده‌ها و حریم خصوصی اطلاعاتی (به‌دلیل ارتباط هویت دیجیتال با داده‌های شخصی که در بند پیشین بیان شد) مانند مقررات عمومی حفاظت از داده اتحادیه اروپا[5] عندالاقتضا بهره برد. البته در حقوق ایرانی هنوز مسئلهٔ مربوط به حمایت از داده‌ها قانونمند نشده است.[6] یادشدنی است، هدف قوانین و مقررات مربوط به حفاظت از داده‌های شخصی حمایت از اشخاص حقیقی نسبت به پردازش داده‌های شخصی‌شان است؛ چراکه حق بر داده‌ها از حقوق بشر و از مصادیق حقوق شهروندی است. از مهم‌ترین جنبه‌های حمایت از داده‌های شخصی بر اساس جامع‌ترین بستر قانونی در

1. European Digital Identity Regulation (EDIR) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281&from=EN
2. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910 (eIDAS)
3. European Digital Identity Wallet (EDIW)
4. Electronic Identification Schemes
5. https://eur-lex.europa.eu/legal-ontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
۶. البته در این خصوص پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» در تیرماه ۱۳۹۷ و طرح «حمایت و حفاظت از داده و اطلاعات شخصی» در شهریورماه ۱۴۰۰ مطرح شده است، پیش‌نویس مذکور در همین مرحله رها شده است و طرح مذکور نیز گزیده‌ای از پیش‌نویس سابق است. این طرح که با چند سال فاصله از ارائهٔ پیش‌نویس، در خصوص حمایت از دادهٔ شخصی و اشخاص موضوع داده، در مجلس وصول شده است؛ در محتوا نسبت به مواد استفاده‌شده از پیش‌نویس، تغییری نکرده و با عدم شفافیت و فقدان افزایش حمایت از دادهٔ شخصی و اشخاص موضوع داده، با همان کیفیتِ مقرر در پیش‌نویس، به حمایت از داده‌های شخصی و اشخاص موضوع داده، پرداخته است. اگرچه قانون مدیریت داده‌ها و اطلاعات ملی که در جلسهٔ علنی مجلس شورای اسلامی مورخ ۱۴۰۱/۰۶/۳۰ به تصویب رسیده است نیز وجود دارد؛ لیکن به‌نظر می‌رسد به‌دلیل اختصار و عدم توجه به جزئیات، راهگشا نباشد.

این خصوص یعنی مقررات عمومی حفاظت از داده اتحادیهٔ اروپا، وجود مبانی حقوقی پردازش است. به‌موجب مواد مربوطه، کنترل‌کننده‌ها باید مبنای حقوقی معتبر جهت پردازش داده‌های شخصی داشته باشند تا تصرف در داده‌های شخصی مجاز باشد. در صورت فقدان این مبانی، پردازش ممنوع و غیرقانونی است. همچنین به‌موجب مواد مختلفی از این مقررات، اشخاص موضوع داده از حقوق متعددی برخوردارند. این حقوق در راستای تحقق حمایت جامع از داده‌های شخصی و کنترل بیشتر افراد نسبت به داده‌های شخصی‌شان است. در مقابل اشخاص پردازش کنندهٔ داده (کنترل‌کننده و پردازنده) تعهدات مختلفی را در راستای حمایت از داده‌های شخصی دارند. تعهدات موجود در این مقررات به‌طور کامل برای کنترل‌کننده‌ها، به‌عنوان مسئول اصلی پردازش، وجود دارند. پردازنده‌ها نیز که به نمایندگی از کنترل‌کننده‌ها در خصوص پردازش عمل می‌کنند، ملزم به رعایت برخی از تعهدات موجود در این مقررات هستند. تصریح بر ضمانت اجراهای مختلف ازجمله ضمانت اجراهای مدنی و کیفری نیز از نکات مثبت این مقررات است (See. EUR-Lex, 2016). با توجه به وجود حمایت‌های قانونی چندجانبه برای داده‌های شخصی، جریان آنها نسبت به هویت‌های دیجیتال به قانونمند کردن وضعیت آواتارها در متاورس کمک شایانی خواهد کرد.

– همچنین ممکن است بتوان از برخی دیگر از پیش‌نویس‌های قانونی اتحادیهٔ اروپا (پیشنهاده) برای مواجهه با متاورس استفاده کرد. البته این موارد ممکن است تا رسیدن به مرحلهٔ نهایی و تبدیل به قانون، دستخوش تغییراتی شوند، لیکن می‌توان از مفاد مقرر در این بسترها برای چگونگی نظارت حقوقی و قانونی بر متاورس استفاده کرد. این موارد از جمله مقررات پیشنهادی پارلمان و شورای اروپا برای وضع قواعد یکسان در مورد هوش مصنوعی (قانون هوش مصنوعی) مورخ ۲۰۲۱[1] است. به‌نظر می‌رسد این مقررات پیشنهادی بتواند تأثیر قابل‌توجهی بر متاورس داشته باشد؛ چراکه متاورس با بهره‌مندی از هوش مصنوعی ویژگی‌های فنی خاص به خود گرفته است. این پیشنهاده برای محافظت از انسان در زمینهٔ تأثیر هوش مصنوعی – چه از طریق تعامل مستقیم بین انسان‌ها با هوش مصنوعی یا به‌طور مثال از طریق تصمیم‌گیری هوش مصنوعی که بر انسان‌ها تأثیر می‌گذارد – تدوین شده است (Bavana k. , 2022: 6). اتحادیهٔ اروپا در پیش‌نویس قانون هوش مصنوعی رویکرد انسان‌محور را نسبت به هوش مصنوعی انتخاب کرده است که می‌تواند تحولات ناخواسته را محدود کند (Madiega et al. , 2022: 6). از جمله هدف این مقررات پیشنهادی جلوگیری از خطرهایی است که فناوری‌های مبتنی بر هوش مصنوعی ایجاد می‌کنند – منوط به شرایطِ کاربرد و استفاده از

1.https://eur-lex.europa.eu/legal- content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

هوش مصنوعی- که ممکن است به منافع عمومی نیز آسیب برسانند. پیشنهادهٔ مذکور با تضمین سطح بالای حفاظت از منافع عمومی، توسعهٔ هوش مصنوعی را امن‌تر و قابل اعتماد می‌کند. همچنین به موجب این مقررات پیشنهادی فناوری‌های مبتنی بر هوش مصنوعی می‌توانند طوری طراحی شوند که در سطوح مختلفی به‌صورت مستقل عمل کنند (این امر و مطالبی از این قبیل می‌تواند در مورد اعطای شخصیت به هویت‌های دیجیتال در متاورس قابل استفاده باشد) (European Commission, 2021: 1& 2).

۴. ۲. حمایت‌های بیشتر با استفاده از فناوری بلاک‌چین

بلاک‌چین به‌عنوان یک فناوری ایمن و پرکاربرد می‌تواند برای حل چالش‌های حقوقی مربوط به هویت‌های دیجیتال در متاورس قابل استفاده باشد، لیکن با توجه به کاربردِ متفاوت انواع آن؛ اینکه استفاده از کدام نوع بلاک‌چین در جهت حل بهتر معضل‌های مربوط به هویت‌های دیجیتال، مناسب است با بررسی هر قسم روشن خواهد شد. بدین‌سبب در این بند ابتدا به معرفی مختصر این فناوری و انواع آن پرداخته می‌شود، سپس به تأثیر بهره‌مندی از بلاک‌چین در خصوص حمایت از هویت‌های دیجیتال و تفاوت استفاده از هر نوع نسبت به موضوع مورد بحث پرداخته خواهد شد.

۴. ۲. ۱. معرفی مختصر بلاک‌چین و انواع آن

فناوری‌های بلاک‌چین و دفتر کلِ (پایگاه اطلاعاتی) توزیع‌شده[1]، فرصت‌های جدیدی را برای محافظت از داده‌های کاربر از طریق هویت غیرمتمرکز[2] و سایر سازوکارهای حفظ حریم خصوصی، فراهم می‌کنند (Beduschi, 2019: 2). بلاک‌چین قطعه‌های مجزای (بلوک‌های) به‌هم مرتبط است که تأیید و رمزنگاری شده است و توسط دستگاه متصل به شبکه نگهداری می‌شود. فناوری بلاک‌چین یک پایگاه اطلاعاتی پیشرفته است که امکان به‌اشتراک‌گذاری شفاف داده‌ها را فراهم می‌کند و می‌تواند هر نوعی از داده‌ها را ذخیره کند. تفاوت اصلی بین پایگاه

1. Distributed Ledger Technology (DLT)

تعاریف مختلفی از فناوری دفتر کل(پایگاه اطلاعاتی) توزیع‌شده (DLT) وجود دارد، برخی از آنها محدودند، درحالی‌که برخی دیگر بسیار موسع‌اند و شامل مصادیق بسیاری می‌شوند. برخی تعاریف دیگر بین این فناوری و بلاک‌چین تفاوتی قائل نمی‌شوند. مطابق این تعاریف زنجیرهٔ بلوکی به‌عنوان یک دفتر کل (پایگاه اطلاعاتی) توزیع‌شده معرفی شده است که به‌طور مستقل داده‌ها را در هر بلوک حفظ می‌کند تا از دستکاری و تغییر محافظت شوند. بدین‌سبب می‌توان گفت هیچ تعریف ثابتی برای این فناوری وجود ندارد. موضوع چالش‌برانگیز این است که از یک سو، تعاریف گاه بسیار خاص، فنی و غیرقابل دسترس برای مخاطبان عام هستند، درحالی‌که از سوی دیگر، برخی تعاریف ساده و موسع‌اند، به‌طوری‌که هیچ تفاوت معناداری با تعاریف سنتی پایگاه داده ندارند (Rauchs et al., 2018: 19 & 20).

۲. توضیح آن به‌زودی خواهد آمد.

داده‌های سنتی با بلاک چین در نحوهٔ ساختاربندی و دسترسی به داده‌هاست. یک بلاک‌چین شامل برنامه‌هایی است که معمولاً در یک پایگاه داده انجام می‌شود، این امر مانند وارد کردن اطلاعات و دسترسی به آنها و ذخیرهٔ اطلاعات است، ولی این موارد در چند نسخه ذخیره می‌شوند و برای اعتبار باید همهٔ آنها باهم مطابقت داشته باشند. این بستر می‌تواند اطلاعات مربوط به تراکنش‌های مختلف را ثبت و ارتباطات ایمن در شبکه را فراهم کند. بلاک‌چین‌ها انواعی نیز دارند که به‌طور عمده به‌صورت عمومی (غیرمتمرکز) یا خصوصی(متمرکز) است (See. Alam, 2019: 153). بلاک‌چین عمومی، بلاک‌چینی است که در آن هر کسی می‌تواند آزادانه به فعالیت‌های اصلی شبکهٔ بلاک‌چین بپیوندد و در آن شرکت کند. در واقع هر کسی می‌تواند به فعالیت‌های جاری در شبکهٔ بلاک‌چین دسترسی داشته باشد و این امر به دستیابی به ماهیت خودگردان و غیرمتمرکز این بستر کمک می‌کند. با این حال، از منظر امنیتی باز یا غیرمتمرکز بودن این نوع از بلاک‌چین، چالشی منحصربه‌فرد است؛ چراکه یک سیستم کاملاً باز، تقریباً امنیت محیطی ندارد (See. Bird & Bird LLP, 2020b: 1 & 3; See. Huang et al., 2019: 356 & 357). در مقابل بلاک‌چین‌های خصوصی که اغلب به‌عنوان بلاک‌چین‌های مجاز هم شناخته می‌شوند، اغلب توسط یک سازمان (واسط مورد اعتماد) اجرا و اداره می‌شوند. از آنجایی که واسطه‌های مورد اعتماد، مسئولیت اجرای بلاک‌چین را بر عهده دارد، این موضوع را کنترل خواهند کرد که چه کسی می‌تواند به بلاک‌چین خصوصی دسترسی داشته باشد و همچنین می‌توانند نوع حقوق قابل دسترسی برای هر شرکت‌کننده را کنترل کنند. برای مثال، برخی شرکت‌کنندگان ممکن است محدود به مشاهدهٔ (برخی یا همه) داده‌های پایگاه اطلاعاتی (دفتر کل) باشند، درحالی‌که دیگران ممکن است اجازهٔ ارسال تراکنش‌های جدید برای ثبت در زنجیره‌های بلوکی را نیز داشته باشند (Bird & Bird LLP, 2020a: 1; See. Strehle, 2020: 3 & 4). فارغ از نوع بلاک‌چین، داده‌های موجود در این بستر قابل تغییر نیستند و داده‌های منتشرشده را نمی‌توان حذف کرد (See. Matsson, 2022: 43 & 44). این امر بلاک‌چین را به یک بستر تغییرناپذیر نسبت به فعالیت‌های گذشته تبدیل می‌کند (ویژگی تغییرناپذیری[1] بلاک چین) (Tijan et al., 2019: 2 & 3).

با توجه به مفهومی که از بلاک‌چین ارائه شد، می‌توان گفت محیط متاورس با فناوری بلاک‌چین به‌نحوی مطلوب قابل سازماندهی است. در واقع می‌توان از این فناوری در راستای حمایت بیشتر از افراد به‌ویژه نسبت به حریم خصوصی اطلاعاتی، حفاظت از داده و هویت

1. Immutability

البته این بستر به‌صورت مطلق در مقابل تغییر و آسیب مصون نیست و با اقداماتی مخرب ممکن است در بلوکی تغییر ایجاد شود. تغییر در یک بلوک سایر بلوک‌ها بعدی را نامعتبر می‌سازد.

دیجیتال (توجه به ارتباط هویت دیجیتال و دادهٔ شخصی مذکور در بند ۱ پژوهش) بهره جست. این امر بدین‌دلیل است که بلاک‌چین زمینهٔ حفاظت از حریم خصوصی و داده‌های شخصی را به‌طور مناسب فراهم می‌کند.

۴. ۲. ۲. اثرگذاری هریک از انواع بلاک‌چین بر چگونگی حمایت هویت‌های دیجیتال (متمرکز یا غیرمتمرکز کردن حریم خصوصی؟)

همان‌گونه‌که اشاره شد، بلاک‌چین برای حمایت مناسب از هویت‌های دیجیتال و پردازش ایمن داده‌های شخصی نیز قابل استفاده است (به ارتباط این موارد در بند نخست اشاره شد)، ولی در خصوص اینکه کدام‌یک از انواع بلاک‌چین، باید مورد توجه قرار گیرد، نظرهای متفاوتی وجود دارد.

الف) استفاده از بلاک‌چین عمومی (غیرمتمرکز): از یک منظر می‌توان مدل غیرمتمرکز (عمومی) بلاک‌چین را برای مسائل مربوط به حفاظت از داده و هویت دیجیتال در متاورس مورد توجه قرار داد. در مدل غیرمتمرکز خود کاربران داده‌هایشان را کنترل می‌کنند و تصمیم می‌گیرند که داده‌های مزبور چگونه می‌توانند به اشتراک گذاشته شوند. با این حال به‌دلیل تنش‌هایی بین بلاک‌چین و قوانین مربوط به حفاظت از داده به‌عنوان نمونه مقررات اروپایی حفاظت از داده (GDPR)، برخی الزامات حقوقی جدید باید مقرر شوند (Madiega et al. , 2022: 6). در این مسیر پرسش‌های مختلفی نیز وجود دارند که باید پاسخ آنها تبیین شود؛ از جمله اینکه کنترل‌کنندهٔ داده در بلاک‌چین کیست؟ آیا همهٔ افراد دخیل در بلاک‌چین، کنترل‌کننده‌اند؟ اگر چند کاربر به‌طور مشترک تصمیم بگیرند که عملیات پردازش را روی یک بلاک‌چین انجام دهند، چه اتفاقی رخ می‌دهد؟ آیا پردازنده‌های داده، به معنای مقررات اروپایی حفاظت از داده، در زنجیره‌های بلوکی وجود دارند؟ و سؤالات دیگری که باید به آنها توجه شود (Commission Nationale Informatique & Libertés, 2018: 1-3).

به دیگر سخن استفاده از بلاک‌چین‌های عمومی به معنای بهره‌مندی از هویت غیرمتمرکز[1] یا هویت خودمختار[2] در متاورس است. این امر یعنی با استفاده از بلاک‌چین، افراد می‌توانند بر هویت خود کنترل داشته و در مورد چگونگی به اشتراک‌گذاری هویتشان با دیگران استقلال داشته باشند. هویت‌های غیرمتمرکز یا هویت‌های خودمختار تجسمی از هویت‌های مستقل مبتنی بر بلاک‌چین هستند که می‌توان به‌وسیلهٔ آنها حریم خصوصی و امنیت داده‌های شخصی را به‌طور اساسی بهبود بخشید (Kondova & Erbguth, 2020: 344). در واقع کاربران می‌توانند دارایی به نام داده را ایمن کنند، تحت کنترل قرار دهند و تعیین کنند چه کسی به آنها دسترسی

1. Decentralized Identity (DID)
2. Self-Sovereign Identity (SSI)

داشته باشد. همچنین امنیت افراد هنگام تعامل با چند بستر کار با توجه به هویت‌های غیرمتمرکز افزایش می‌یابد. هویت‌های غیرمتمرکز که بر روی بلاک‌چین عمومی مستقر شده‌اند، ذاتاً ایمن‌تر از هویت‌های متمرکزند و بهتر می‌توان تمامیت داده را حفظ کرد. به‌طورکلی ذخیره‌سازی غیرمتمرکز از اجزای اصلی مدیریت داده‌ها برای هویتی ایمن است. زمانی‌که هویت‌ها صرفاً تحت کنترل کاربر باشد، هویت خودحاکمیتی در نظر گرفته می‌شود. این امر بدین معنی است که کاربر می‌تواند دسترسی به داده‌ها را کاملاً کنترل کند، بدون اینکه نگران دسترسی بدون اجازه باشد. درعین‌حال در چارچوب هویت غیرمتمرکز، امنیت نیز به عهدهٔ کاربر است (See. Heister & Yuthas, 2022: 7). افزون‌بر این اتحادیهٔ اروپا چارچوبی را برای مدیریت اشتراک‌گذاری داده و افزایش رضایتِ افراد از طریق سرویس‌های واسطه داده در قانون حاکمیت داده[1] برای متاورس‌های باز و غیرمتمرکز ارائه کرده است. این امر یعنی مدل‌های متاورس مبتنی بر بلاک‌چین عمومی و استانداردهای باز به‌طور قانونی مورد توجه قرار گرفته است تا محیط متاورس توسط خود کاربران به‌صورت مستقل و غیرمتمرکز[2] کنترل شود (Madiega et al. , 2022: 6). خلاصه اینکه می‌توان از طریق بلاک‌چین‌های عمومی و هویت‌های خودمختار یا غیرمتمرکز افراد را قادر ساخت تا داده‌های تحت مالکیت خود را کنترل کنند و بدین‌ترتیب حق حاکمیت بیشتری نسبت به داده‌هایشان داشته باشند (Heister & Yuthas, 2022: 1).

ب) **استفاده از بلاک‌چین خصوصی (متمرکز):** در این نوع از بلاک‌چین فقط به اشخاص خاصی اجازه داده می‌شود که در یک شبکهٔ بسته و محدود شرکت کنند. بدین‌علت برای کاربران فارغ از حقوق، محدودیت‌های خاصی نیز در شبکه وجود دارد و به صلاحدید متصدی دسترسی کامل یا محدود قابل اعمال است. در نتیجه، بلاک‌چین خصوصی ماهیت متمرکز دارد زیرا تنها به گروه محدودی مربوط می‌شود. در بلاک‌چین‌های خصوصی هویت شرکت‌کنندگان مشخص است و نمی‌توان به‌صورت ناشناس فعالیت کرد (Nuss et al. , 2018: 5& 6). سیستم متمرکزی که مدیریت شبکه را بر عهده دارد، در رأس شبکه قرار دارد. برای استفاده از این نوع بلاک‌چین، کاربران برای پیوستن به شبکه نیاز به مجوز دارند. همچنین تنها کاربران خاصی که به بلاک چین دسترسی دارند و درگیر تراکنش هستند، می‌توانند فعالیت‌های مربوطه در شبکه

1. European Data Governance Act
Regulation (Eu) 2022/868 Of The European Parliament And Of The Council Of 30 May 2022 On European Data Governance And Amending Regulation (Eu) 2018/1724 (Data Governance Act)
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868
قانون حاکمیت دادهٔ اروپا، اشتراک‌گذاری داده در کشورهای اتحادیهٔ اروپا را تسهیل می‌کند تا از ظرفیت داده‌ها به نفع شهروندان و مشاغل اتحادیهٔ اروپا استفاده کند (European Commission, 2022).

2. Decentralised autonomous organisations (DAOs)

را مشاهده کنند و هیچ شرکت‌کنندهٔ دیگری در بلاک‌چین نمی‌تواند به تراکنش‌های خصوصی دسترسی داشته باشد. اگرچه بلاک چین خصوصی مخاطبان محدودتری دارد، ولی ویژگی‌های مفید بسیاری دارد. این موارد ازجمله سرعت بیشتر و کارایی بالاتر است. این امر بدین دلیل است که بلاک‌چین خصوصی از منابع مورد نیاز استفاده می‌کند و بدین‌ترتیب کارامدتر است. همچنین حمایت از حریم خصوصی به دلایل توانایی محرمانه نگه‌داشتن داده‌ها تا حد زیادی قابل تحقق است. در بلاک‌چین‌های خصوصی به دلیل اینکه صرفاً تعداد کمی از کاربران به تراکنش‌های خاص دسترسی دارند، بی‌شک شبکه پایدارتر است و ازآنجایی‌که گره‌ها به هر گروه کاربری تخصیص داده می‌شوند، ثبات بالایی برای کاربران در شبکه فراهم می‌شود (See. Lai & Chuen, 2017: 153& 154).

با توجه به آنچه بیان شد شاید بتوان گفت بلاک‌چین‌های خصوصی یا مجاز برای پیاده‌سازی قوانین حفاظت از داده (برای نمونه GDPR) و حمایت از هویت‌های دیجیتال، مناسب‌تر از شبکه‌های عمومی و بدون مجوز است. این امر بدین‌دلیل است که شرکت‌کنندگان در شبکه‌های مجاز برای دیگران شناخته شده‌اند. درواقع در بلاک‌چین‌های مجاز، هویت شرکت‌کنندگان شناخته می‌شود و این امر حمایت از کاربران را ساده می‌کند (Ibáñez et al., 2018: 5). برای نمونه امکان تعریف روابط قراردادی و امکان تخصیص مناسب مسئولیت وجود دارد. همچنین این شبکه‌ها، بر خلاف شبکه‌های عمومی و بدون مجوز، به‌گونه‌ای طراحی شده‌اند که کنترل بر روی شبکه امکان‌پذیر است. برای مثال با داده‌ها به شیوه‌ای منطبق با قانون رفتار شود. همچنین نظارتی وجود دارد که کدام بازیگران به داده‌های شخصی مربوطه دسترسی دارند که در مورد بلاک‌چین‌های عمومی و غیرمجاز صدق نمی‌کند (Michèle, 2019: 101&102). خلاصه اینکه با جریان بلاک‌چین‌های خصوصی و مجاز به‌نظر می‌رسد مطلوب‌تر از بلاک‌چین‌های عمومی و بدون مجوز، بتوان الزامات قانونی را رعایت کرد.

۵. نتیجه

با توجه به معضلات حقوقی متاورس و اهمیت قانون‌مند نکردن این محیط از یکسو و از سوی دیگر فقدان بستر حقوقی مناسب برای کنترل متاورس و بی‌توجهی قانونگذاران در بسیاری از نظام‌های حقوقی به این مهم، کنترل متاورس با استفاده از بسترهای حقوقی موجود، امری ضروری است. در این زمینه استفاده از مفاد برخی قوانین و مقررات خاص می‌تواند این جهان بدون مرز را تا حدی کنترل کند. از جملهٔ این موارد، مقررات «هویت دیجیتال اتحادیه اروپا» در سال ۲۰۲۱ است. دامنهٔ خاص این مقررات پیشنهادی مربوط به پردازش داده‌های شخصی نسبت به شناسایی الکترونیکی است که می‌تواند برای حمایت مناسب از داده‌های شخصی و

آواتارها در متاورس کارامد باشد. همچنین می‌توان از برخی پیشنهاده‌های قانونی در حقوق اتحادیهٔ اروپا نیز استفاده کرد. البته این موارد ممکن است تا رسیدن به مرحلهٔ نهایی و قانونی شدن دستخوش تغییراتی شوند، لیکن می‌توان از نوع حمایت حقوقی مقرر در این بسترها برای چگونگی نظارت بر متاورس استفاده کرد. این موارد از جمله مقررات پیشنهادی پارلمان و شورای اروپا برای وضع قواعد یکسان در مورد هوش مصنوعی (قانون هوش مصنوعی) مورخ ۲۰۲۱ است. اتحادیهٔ اروپا در این پیش‌نویس، رویکرد انسان‌محور را نسبت به هوش مصنوعی انتخاب کرده است که می‌تواند تحولات ناخواسته را محدود کند. این امر در حالی است که به‌موجب این مقررات پیشنهادی، فناوری‌های مبتنی بر هوش مصنوعی می‌توانند طوری طراحی شوند که در سطوح مختلفی به‌صورت مستقل عمل کنند. افزون‌بر این توجه به بسترهای حقوقی و قانونی مربوط به حفاظت از داده‌های شخصی در هریک از نظام‌های حقوقی – به‌دلیل ارتباط هویت دیجیتال با داده‌های شخصی– نیز خالی از فایده نیست. این موارد از جمله مقررات اروپایی حفاظت از داده و سندهای حقوقی مربوط به داده‌های شخصی در نظام حقوقی ایران (پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» مورخ تیرماه ۱۳۹۷ و طرح «حمایت و حفاظت از داده و اطلاعات شخصی» مورخ ۱۴۰۰) است. از مهم‌ترین جنبه‌های حمایت به‌موجب این بسترها، وجود تعهدات مختلف برای اشخاص پردازش‌کنندهٔ داده و حقوق متعدد برای اشخاص موضوع داده است. این حقوق و تکالیف متقابل در راستای تحقق حمایت جامع از داده‌های شخصی و کنترل بیشتر افراد نسبت به داده‌های شخصی‌شان است. بدین‌سبب توجه به آنها در متاورس موجب جریان حمایت‌های حقوقی در این محیط است. همچنین می‌توان برای کنترل متاورس از فناوری بلاک‌چین استفاده کرد. هریک از انواع مختلف بلاک‌چین – که در این پژوهش به آنها اشاره شد– به نحوی می‌تواند از داده‌ها و هویت‌های موجود در متاورس حمایت کند. به‌طور مختصر استفاده از بلاک‌چین‌های عمومی (غیرمتمرکز) حاکمیت خود اشخاص بر هویت دیجیتالی را بیشتر می‌کند و به آنها هویت‌های خودمختار اعطا می‌کند و از سویی دیگر جریان بلاک‌چین‌های خصوصی (متمرکز) موجب دخالت بیشتر مراجع قانونی و حمایت‌های حقوقی نظام‌مند است. با توجه به ماحصل این پژوهش، به‌نظر می‌رسد استفاده از بلاک‌چین‌های خصوصی به‌دلیل امکان جریان دقیق‌تر قوانین و مقررات بر آن و توانایی نظارت نهادهای قانونی نسبت به آن – برای تحقق حمایت‌های حقوقی نسبت به هویت‌های دیجیتالی– مناسب‌تر باشد. با وجود این تصریح بر استفاده از کدام‌یک از انواع بلاک‌چین برای تحقق حمایتی جامع نسبت به هویت‌های دیجیتال، منوط به توجه ویژهٔ قانونگذار نسبت به ابعاد مختلف فناوری فراگیر متاورس است.

منابع

الف) فارسی

۱. پیش‌نویس لایحه‌ی «صیانت و حفاظت از داده‌های شخصی» منتشرشده در تیرماه ۱۳۹۷

۲. شاکری، زهرا؛ یاسمن جعفرپور (۱۴۰۱)، «امکان‌سنجی اعمال حقوق معنوی مؤلف تحت فناوری‌های نوین اطلاعات و ارتباطات». *حقوق فناوری‌های نوین*، ۳(۶)، ۱۵-۲۹. شناسه برنمود دیجیتالی: 10.22133/mtlj.2022.360779.1120

۳. طرح «الزام به انتشار داده و اطلاعات» اعلام وصول شده در مجلس مورخ آذرماه ۱۳۹۹

۴. عاکفی قاضیانی، موسی؛ سیدمصطفی میلانی؛ وحید عاکفی قاضیانی (۱۴۰۱)، «متاورس و چالش‌های حقوقی در حوزهٔ حقوق اموال». *حقوق فناوری‌های نوین*، ۳(۶)، ۱۴۳-۱۵۳. شناسه برنمود دیجیتالی: DOI: 10.22133/mtlj.2022.353672.1109

۵. قانون «مدیریت داده ها و اطلاعات ملی» مصوب ۱۴۰۱

۶. میر شکاری، عباس (۱۳۹۶).*حقوق شخصیت و حقوق مسئولیت مدنی در اتحادیه اروپا*، تهران: سهامی انتشار

ب) خارجی

7. Alam, Tanweer (2019). Blockchain and its Role in the Internet of Things (IoT). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 151–157. https://doi.org/10.32628/CSEIT195137
8. Barfield, Woodrow (2006). Intellectual property rights in virtual environments: considering the rights of owners, programmers and virtual avatars. *Akron Law Review*, *93*(3), 649–700. Accessed 20 October 2022, from ttps://law.bepress.com/cgi/viewcontent.cgi?article=4342&context=expresso
9. Barfield, Woodrow, and Marc Blitz (2018). *Research Handbook on the Law of Virtual and Augmented Reality*. Edward Elgar Publishing. https://doi.org/10.4337/9781786438591
10. Bavana k, (2022). "Privacy in the Metaverse" . *Jus Corpus Law Journal*, *2*(3), 1–11. Accessed 8 November 2022, from https://www.juscorpus.com/wp- content/uploads/2022/03/2.-K.-Bavana.pdf
11. Beduschi, Ana (2019). "Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights". *Big Data & Society*, *6*(2), 1–6. https://doi.org/10.1177/2053951719855091
12. Bernal Bernabe, Jorge, Jose Luis Canovas, Jose L. Hernandez-Ramos, Rafael Torres Moreno, and Antonio Skarmeta (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access*, *7*, 164908–164940. https://doi.org/10.1109/ACCESS.2019.2950872
13. Belk, Russell, Mariam Humayun, and Myriam Brouard (2022). Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web3 and Wild Markets. *Journal of Business Research*, 153, 198-205. https://doi.org/10.1016/j.jbusres.2022.08.031
14. Bird & Bird LLP. (2020a). *Private Blockchains* (pp. 1–4).
15. Bird & Bird LLP. (2020b). *Public Blockchains* (pp. 1–4).
16. Cheong, Ben Chester (2022). Avatars in the metaverse: potential legal issues and remedies. *International Cybersecurity Law Review*, *3*(2), 467–494. https://doi.org/10.1365/s43439-022-00056-9
17. Commission Nationale Informatique & Libertés. (2018). *Solutions for a responsible use of the blockchain in the context of personal data* (pp. 1–10).
18. Colcelli, Valentina (2019). Joint Controller Agreement Under GDPR. *Eu and Member States – Legal and Economic Issues*, 3, 1030–1047. https://doi.org/10.25234/eclic/9043
19. Dremliuga, Roman, Olga Dremliuga, and Andrei Iakovenko (2020). Virtual Reality: General Issues of Legal Regulation. *Journal of Politics and Law*, *13*(1), 75–81. https://doi.org/10.5539/jpl.v13n1p75
20. Dwivedi, Yogesh K., Laurie Hughes, Abdullah M. Baabdullah, Samuel Ribeiro-Navarrete, Mihalis Giannakis, Mutaz M. Al-Debei, Denis Dennehy, Bhimaraya Metri, Dimitrios Buhalis, Christy M. K. Cheung, Kieran Conboy, Ronan Doyle, Rameshwar Dubey, Vincent Dutot, Reto Felix, D. P. Goyal, Anders Gustafsson, Chris Hinsch, Ikram Jebabli, Marijn Janssen, Young-Gab Kim, Jooyoung Kim, Stefan Koos, David Kreps, Nir Kshetri, Vikram Kumar, Keng-Boon Ooi, Savvas Papagiannidis, Ilias O. Pappas, Ariana

Polyviou, Sang-Min Park, Neeraj Pandey, Maciel M. Queiroz, Ramakrishnan Raman, Philipp A. Rauschnabel, Anuragini Shirish, Marianna Sigala, Konstantina Spanaki, Garry Wei-Han Tan, Manoj Kumar Tiwari, Giampaolo Viglia, and Samuel Fosso Wamba (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management*, *66*, 1–55. https://doi.org/10.1016/j.ijinfomgt.2022.102542

21. EUR-Lex. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). *Official Journal of the European Union*, 1–88.
22. European Commission. (2021). Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts.
23. European Commission. (2022). *European Data Governance Act* . Accessed 26 May 2023, from https://digital-strategy.ec.europa.eu/en/policies/data-governance-act
24. European Commission. (n.d.). *European Digital Identity*. Accessed 29 June 2022, from https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
25. Gadekallu, Thippa Reddy, Thien Huynh-The, Weizheng Wang, Gokul Yenduri, Pasika Ranaweera, Quoc-Viet Pham, Daniel Benevides da Costa, and Madhusanka Liyanage (2022). Blockchain for the Metaverse: A Review. *Computer Science*, 1–17. https://doi.org/10.48550/arXiv.2203.09738
26. Heister, Stanton, and Kristi Yuthas (2022). How Blockchain and AI Enable Personal Data Privacy and Support Cybersecurity. In book: *Blockchain Potential in AI*. IntechOpen. https://doi.org/10.5772/intechopen.96999
27. Huang, Dijiang, Chun-Jen Chung, Qiuxiang Dong, Jim Luo, and Myong Kang (2019). Building private blockchains over public blockchains (PoP). *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, 355–363. https://doi.org/10.1145/3297280.3297317
28. Ibáñez, Luis-Daniel, Kieron O'Hara, and Elena Simperl (2018). *On Blockchains and the General Data Protection Regulation*. (pp. 1–13).
29. KAVUT, Sevgi (2021). The Digital Identities In The Context Of Blockchain and Artificial Intelligence. *Journal Of Selçuk Communication*, *14*(2), 529–548. https://doi.org/10.18094/josc.865641
30. Kondova, Galia, and Jörn Erbguth (2020). "Self-sovereign identity on public blockchains and the GDPR". *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, 342–345. https://doi.org/10.1145/3341105.3374066
31. Lai, Roy, and David LEE Kuo Chuen (2017). Blockchain–From Public to Private. *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2: ChinaTech, Mobile Security, and Distributed Ledger*, 145.
32. Livingstone, Sonia, Mariya Stoilova, and Rishita Nandagiri (2019). Children's data and privacy online Growing up in a digital age an evidence review. In *London School of Economics and Political Science* (pp. 1–57).
33. LÓPEZ, ARLOS ÁLVAREZ, and ÁNGEL CARRASCO PERERA (2022). *What is a metaverse?* (pp. 1–5).
34. Madiega, Tambiama, Polona Car, Maria Niestadt, and Louise van de Pol (2022). *Metaverse, Opportunities, risks and policy implications* (pp. 1–12).
35. Matsson, David (2022). GDPR, Blockchain & Personal data - The rights of the individual v. the integrity of Blockchain. In *Gothenburg University Publications Electronic Archive (GUPEA)* (pp. 1–64).
36. Michèle, finck (2019). *Blockchain and the general data protection regulation* (pp. 1–120).
37. Mystakidis, Stylianos (2022). Metaverse". *Encyclopedia*, *2*(1), 486–497. https://doi.org/10.3390/encyclopedia2010031
38. Naik, Nitin, and Paul Jenkins (2020). Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity. *Proceedings of 2020 7th IEEE International Conference on Behavioural and Social Computing, BESC 2020*, 1–6. https://doi.org/10.1109/BESC51023.2020.9348298
39. Ning, Huansheng, Hang Wang, Yujia Lin, Wenxi Wang, Sahraoui Dhelim, Fadi Farha, Jianguo Ding, and Mahmoud Daneshmand (2021). A Survey on Metaverse: the State-of-the-art, Technologies, Applications, and Challenges. In *Cornell University* (pp. 1–34). https://doi.org/10.48550/arxiv.2111.09673

40. Nuss, Martin, Alexander Puchta, and Michael Kunz (2018). Towards blockchain-based identity and access management for internet of things in enterprises. In *Trust, Privacy and Security in Digital Business: 15th International Conference, TrustBus 2018, Regensburg, Germany, September 5–6, 2018, Proceedings 15* (pp. 167-181)
41. Rauchs, Michel, Andrew Glidden, Brian Gordon, Gina C. Pieters, Martino Recanatini, François Rostand, Kathryn Vagneur, and Bryan Zheng Zhang (2018). Distributed ledger technology systems: A conceptual framework. *The Cambridge Centre for Alternative Finance (CCAF)* (pp. 1-97)
42. Siibak, Andra, and Giovanna Mascheroni (2021). Children's data and privacy in the digital age. In *CO:RE Short Report Series on Key Topics* (pp. 1–13).
43. Singh, Ramandeep (2022). *User Privacy Protection in the Emerging World of Metaverse* (pp. 1–7).
44. Strehle, Elias (2020). Public Versus Private Blockchains. In *Blockchain Research Lab* (pp. 1–8).
45.Sullivan, Clare (2018). Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review*, *34*(4), 723–731. https://doi.org/10.1016/j.clsr.2018.05.015
46. Tama, Bayu Adhi, Bruno Joachim Kweka, Youngho Park, and Kyung-Hyune Rhee (2017). A critical review of blockchain and its current applications. In *2017 International Conference on Electrical Engineering and Computer Science (ICECOS)* (pp. 109-113).
47. TeamViewer. (2022). *Augmented Reality vs Virtual Reality*. Accessed 25 May 2023, from https://www.teamviewer.com/en/augmented-reality-ar-vs-virtual-reality-vr/
48.Tijan, Edvard, Saša Aksentijević, Katarina Ivanić, and Mladen Jardas (2019). Blockchain Technology Implementation in Logistics. *Sustainability*, *11*(4), 1–13. https://doi.org/10.3390/su11041185
49.Wang, Yuntao, Zhou Su, Ning Zhang, Dongxiao Liu, Rui Xing, Tom H. Luan, and Xuemin Shen (2022). A Survey on Metaverse: Fundamentals, Security, and Privacy. In *Cornell University* (pp. 1–31).
50. Zhenlin, Huang, Chen Hao, and Ahmed (2017). *Metaverse digital identity white paper* (pp. 1–22).

Private Law Studies Quarterly

Homepage: https://jlq.ut.ac.ir/

Online ISSN: 2588-6622
Volume: 53, Issue:2
Summer 2023

Research Paper

Introducing Digital Identity in Metaverse, Identifying Related Legal Challenges and Solutions*

Mahdieh Latifzadeh[1], Sayyed Mohammad Mahdi Qabuli Dorafshan[2] **✉

1. PhD Graduated in Private Law, Faculty of Law and Political Science, Ferdowsi University of Mashhad, Mashhad, Iran.
Email: m.latifzadeh@mail.um.ac.ir
2. Corresponding Author: Associate Professor, Department of Private Law, Faculty of Law and Political Science, Ferdowsi University of Mashhad, Mashhad, Iran. Email: ghaboli@um.ac.ir

Abstract

Metaverse is a Three-dimensional (3D) virtual framework where users can communicate with each other and engage in various activities. Despite the advantages that have led to the development of Metaverse, this environment also has many legal challenges. Along with new opportunities, this virtual world has caused different legal problems. Among these problems are issues related to preserving the integrity of the physical and spiritual personality of people, as well as how to protect intellectual property rights and even material property rights of people. Regardless of the challenges, one of the most important concerns for users who are active in this virtual world is how to protect their digital identity and personal data in the metaverse. Explaining that people in the metaverse are in the form of avatars; Avatars are a representation of a person's personality in the metaverse and allow users to recreate not only their physical appearance but also their movements and behaviors. The use of avatars has created various challenges. One of the most important challenges is how to protect information privacy, specifically protecting personal data in the Metaverse, as well as the possibility of giving

*This article is supported by the National Elites Foundation.

** **How to Cite:** Latifzadeh, Mahdieh; Sayyed Mohammad Mahdi Qabuli Dorafshan. (2023, Summer) "Introducing Digital Identity in Metaverse, Identifying Related Legal Challenges and Solutions" *Private Law Studies Quarterly*, 53, 2: 349 – 372, DOI: https://doi.org/10.22059/JLQ.2023.353867.1007743
Manuscript received: 14 January 2023; final revision received: 6 June 2023; accepted: 28 June 2023, published online:16 August 2023

avatars personality. The stated issues are the main questions that this research has answered with a descriptive-analytical approach and the use of comparative studies.

Now there is no specific law for metaverse. Therefore, it is difficult to control this virtual world and the flow of legal protections for it, even though many people are related to Metaverse for various reasons and the lack of a legal framework is inappropriate and even dangerous. According to the above, the solution is to use related legal frameworks in the effective legal systems regarding Metaverse as well as the Iranian legal system. In other words, some provisions of related laws and regulations in the EU legal system can be used as an effective legal system for this issue. The European Digital Identity Regulation, as well as the legal related to artificial intelligence in this legal system, are among these matters. In addition, it is appropriate to pay attention to the legal frameworks related to the protection of personal data in each of the legal systems due to the connection between digital identity and personal data. In this regard, it is possible to use the European General Data Protection Regulation and the proposed documents related to personal data in Iranian law. Considering that one of the most important aspects of protection based on the previous frameworks is the existence of various obligations for controllers and processors and numerous rights for data subjects; It seems that the use of these obligations and rights in Metaverse will lead to legal protections in this environment.

blockchain technology can also be used to control the metaverse. Blockchain is a safe and widely used technology that is significant in various fields. Regarding the current discussion, blockchain can be used as a platform for realizing legal protection in the metaverse and monitoring it. Each of the different types of blockchain - mentioned in this research - controls the metaverse in a way and specifically protects personal data and identities in this environment. According to the results of this research, it seems that the use of private blockchains is more suitable due to the better implementation of laws and regulations on it, as well as the ability of legal institutions to monitor it. Of course, the use of this technology has also been evaluated in some legal systems, including the European Union, while this has not been achieved in Iranian law. For this reason, the Iranian legislator should - with the help of people who are experts in this technology - determine the legal opinion regarding which of the types of blockchain is more suitable for realizing comprehensive protection for digital identities in the metaverse.

Keywords: Blockchain, Data Protection, Metaverse, Digital Identity, Self-Sovereign Identity.

Declaration of conflicting interests
The author diclares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The authors received no financial support for the research, authorship, and/or publication of this article.