

The Legal Status of Health Data Protection in the Metaverse: A New Opportunity or a Threat to Patients' Privacy

Zahra Nanaei ^{1*}

1. Master's Student in International Trade Law, STe.C., Islamic Azad University, Tehran, Iran.

Received: 14 Feb 2026 **Revised:** 01 Mar 2026 **Accepted:** 01 Apr 2026 **Available Online:** 22 Jun 2026

Abstract: The rapid expansion of emerging technologies and the rise of the metaverse as a new generation of digital interaction have brought about profound transformations in the healthcare sector. Services such as telemedicine, virtual reality-based therapies, and virtual clinics are increasingly being developed and delivered within this environment. While these innovations offer significant opportunities to improve the quality of care and enhance access to healthcare services, they simultaneously involve the large-scale generation, processing, and exchange of patients' health data, giving rise to serious legal challenges. Health data, due to their personal, highly sensitive, and in some cases irreplaceable nature, enjoy the highest level of importance within legal systems, and any violation or misuse of such data may severely undermine human dignity and patients' right to privacy. Nevertheless, the metaverse, owing to its technical complexity, cross-border nature, lack of transparency in data ownership, and the weaknesses of digital informed consent mechanisms, faces substantial legal gaps and ambiguities in the protection of health data. This study adopts an analytical-descriptive methodology combined with a comparative approach to examine the legal framework governing health data protection in the metaverse, drawing on international instruments and selected national legal systems. The findings indicate that existing legal frameworks are insufficient to address the complexities of the metaverse, highlighting the inevitable need for the development of specific and up-to-date regulations to effectively safeguard patients' privacy in this emerging digital space.

Keywords: Metaverse, Health Data, Privacy, Patients' Rights, Telemedicine, Data Protection.

Please Cite This Article As: Nanaei, Z (2026). "The Legal Status of Health Data Protection in the Metaverse: A New Opportunity or a Threat to Patients' Privacy". *Iranian Health System Law*, 2(2): 1-15.

Copyright

This is an open access article distributed under CC BY 4.0 License.

© 2026 The Authors.

وضعیت حقوقی حفاظت از داده‌های سلامت در متاورس؛

فرصتی نوین یا تهدیدی برای حریم خصوصی بیماران

زهرا نعنایی*

۱. دانشجوی کارشناسی ارشد رشته حقوق تجارت بین‌الملل، واحد تهران جنوب، دانشگاه آزاد اسلامی، تهران، ایران.

تاریخ دریافت: ۱۴۰۴/۱۱/۲۵ تاریخ ویرایش: ۱۴۰۴/۱۲/۱۰ تاریخ پذیرش: ۱۴۰۵/۰۱/۱۲ تاریخ انتشار: ۱۴۰۵/۰۴/۰۱

چکیده:

گسترش فناوری‌های نوین و ظهور متاورس به عنوان نسل جدید تعاملات دیجیتال، تحولات عمیقی در حوزه سلامت ایجاد کرده است؛ به گونه‌ای که ارائه خدماتی مانند تله‌مدیسین، درمان‌های مبتنی بر واقعیت مجازی و کلینیک‌های مجازی به صورت فزاینده‌ای در این فضا در حال توسعه است. این تحولات، اگرچه فرصت‌های نوینی برای ارتقاء کیفیت و دسترسی به خدمات درمانی فراهم می‌کنند، اما هم‌زمان با تولید، پردازش و تبادل گسترده داده‌های سلامت بیماران، چالش‌های جدی حقوقی را نیز به همراه دارند. داده‌های سلامت به دلیل ماهیت شخصی، حساس و گاه غیرقابل جایگزین بودن، از بالاترین سطح اهمیت در نظام‌های حقوقی برخوردارند و هرگونه نقض یا سوءاستفاده از آن‌ها می‌تواند کرامت انسانی و حریم خصوصی بیماران را به طور جدی مخدوش سازد. با این حال، فضای متاورس به دلیل ویژگی‌هایی نظیر پیچیدگی فنی، ماهیت فرامرزی، نبود شفافیت در مالکیت داده‌ها و ضعف نظام رضایت آگاهانه دیجیتال، با خلأها و ابهامات حقوقی قابل توجهی در زمینه حفاظت از داده‌های سلامت مواجه است. پژوهش حاضر با بهره‌گیری از روش تحقیق تحلیلی-توصیفی و رویکرد تطبیقی، به بررسی وضعیت حقوقی حفاظت از داده‌های سلامت در متاورس در اسناد بین‌المللی و نظام‌های حقوقی منتخب پرداخته و چالش‌ها و پیامدهای آن را تحلیل می‌کند. نتایج پژوهش نشان می‌دهد که چارچوب‌های حقوقی موجود پاسخگوی پیچیدگی‌های متاورس نبوده و ضرورت تدوین مقررات خاص و روزآمد برای تضمین حریم خصوصی بیماران در این فضا امری اجتناب‌ناپذیر است.

کلمات کلیدی: متاورس، داده‌های سلامت، حریم خصوصی، حقوق بیماران، تله‌مدیسین، حفاظت از داده‌ها.

مقدمه

تحول دیجیتال در دهه‌های اخیر به یکی از مهم‌ترین محرک‌های تغییر در نظام‌های سلامت تبدیل شده است. استفاده گسترده از فناوری‌های اطلاعات و ارتباطات، ابتدا در قالب «سلامت الکترونیک» و با هدف بهبود مدیریت داده‌های پزشکی، تسهیل ارتباط میان بیمار و ارائه‌دهنده خدمات درمانی و افزایش کارایی نظام سلامت شکل گرفت. با این حال، پیشرفت‌های شتابان در حوزه‌هایی همچون واقعیت مجازی، واقعیت افزوده، هوش مصنوعی و بلاک‌چین، زمینه‌ساز گذار از سلامت الکترونیک سنتی به الگوهای نوینی از سلامت دیجیتال شده است که امروزه تحت عنوان «سلامت مبتنی بر متاورس» شناخته می‌شوند. متاورس با ایجاد محیط‌های سه‌بعدی تعاملی و فراگیر، امکان تجربه‌ای متفاوت از ارائه و دریافت خدمات درمانی را فراهم ساخته و مرزهای فیزیکی و زمانی مراقبت‌های سلامت را تا حد زیادی از میان برداشته است.

ظهور متاورس و نفوذ تدریجی آن در خدمات درمانی، اشکال نوینی از مراقبت پزشکی را پدید آورده است. کلینیک‌های مجازی که بیماران و پزشکان در آن‌ها از طریق آواتارهای دیجیتال با یکدیگر تعامل می‌کنند، درمان‌های روان‌شناختی مبتنی بر واقعیت مجازی برای اختلالاتی نظیر اضطراب، فوبیا و اختلال استرس پس از سانحه و نیز آموزش و توان‌بخشی بیماران در محیط‌های شبیه‌سازی شده، تنها نمونه‌هایی از کاربردهای رو به گسترش متاورس در حوزه سلامت به شمار می‌روند. این تحولات، ضمن افزایش دسترسی بیماران به خدمات تخصصی و کاهش هزینه‌ها، کیفیت تشخیص و درمان را نیز ارتقا می‌بخشند. با این حال، بهره‌گیری از چنین فناوری‌هایی مستلزم جمع‌آوری و پردازش حجم عظیمی از داده‌های سلامت است که خود پیامدهای حقوقی و اخلاقی قابل توجهی به همراه دارد.

داده‌های سلامت از حساس‌ترین انواع داده‌های شخصی محسوب می‌شوند و دامنه‌ای گسترده از اطلاعات زیستی، ژنتیکی، روانی و رفتاری افراد را در برمی‌گیرند. این داده‌ها نه تنها وضعیت جسمی و روانی فرد را آشکار می‌سازند، بلکه می‌توانند اطلاعاتی عمیق درباره سبک زندگی، ترجیحات شخصی و حتی آینده سلامت فرد ارائه دهند. در فضای متاورس، علاوه بر داده‌های پزشکی متعارف، داده‌های رفتاری حاصل از تعاملات کاربران، حرکات بدن، واکنش‌های هیجانی و الگوهای تصمیم‌گیری نیز به‌طور مستمر ثبت و تحلیل می‌شوند. همین امر حساسیت داده‌های سلامت را دوچندان کرده و خطر نقض حریم خصوصی، تبعیض، برچسب‌زنی و سوءاستفاده تجاری از اطلاعات بیماران را افزایش می‌دهد.

در چنین شرایطی، مسأله اصلی پژوهش حاضر این است که آیا چارچوب‌های حقوقی موجود توانایی حمایت مؤثر از حریم خصوصی بیماران و حفاظت از داده‌های سلامت آن‌ها را در فضای متاورس دارند یا خیر. قوانین و مقررات فعلی عمدتاً در بستر سلامت الکترونیک و فضای دیجیتال سنتی تدوین شده‌اند و کمتر به ویژگی‌های خاص متاورس، از جمله ماهیت فرامرزی، عدم تمرکز، نقش پررنگ شرکت‌های فناوری و پیچیدگی‌های فنی آن توجه داشته‌اند. از این رو، این تردید جدی وجود دارد که نظام‌های حقوقی موجود با چالش‌هایی بنیادین در مواجهه با سلامت مبتنی بر متاورس روبه‌رو باشند.

بر این اساس، سؤال اصلی پژوهش آن است که وضعیت حقوقی حفاظت از داده‌های سلامت در متاورس چگونه است و چه خلأها و چالش‌هایی در این زمینه وجود دارد؟ فرضیه پژوهش بر این مبنا استوار است که چارچوب‌های حقوقی کنونی، به‌رغم تأکید بر اصل حریم خصوصی و حمایت از داده‌های حساس، برای پاسخگویی به پیچیدگی‌های متاورس کفایت لازم را ندارند و نیازمند بازنگری و تدوین مقررات خاص و روزآمد هستند.

نوآوری این پژوهش در تمرکز بر پیوند میان متاورس و حقوق سلامت و بررسی انتقادی ظرفیت‌های حقوقی موجود در حمایت از داده‌های سلامت بیماران نهفته است؛ حوزه‌ای که هنوز در ادبیات حقوقی، به‌ویژه در نظام حقوقی ایران، کمتر مورد توجه قرار گرفته است. ضرورت انجام این پژوهش نیز از آنجا ناشی می‌شود که توسعه بی‌ضابطه فناوری‌های مبتنی بر متاورس در سلامت، بدون چارچوب حقوقی مناسب، می‌تواند پیامدهای جبران‌ناپذیری برای حریم خصوصی و کرامت انسانی بیماران به همراه داشته باشد. روش تحقیق در این مقاله به‌صورت تحلیلی - توصیفی و با بهره‌گیری از رویکرد تطبیقی انجام شده است. بدین منظور،

ضمن تحلیل مفاهیم و مبانی نظری مرتبط با داده‌های سلامت و حریم خصوصی، اسناد بین‌المللی و نظام‌های حقوقی منتخب مورد بررسی و مقایسه قرار گرفته‌اند تا در نهایت، تصویری روشن از وضعیت حقوقی حفاظت از داده‌های سلامت در متاورس و راهکارهای تقنینی مناسب ارائه شود.

۱- مبانی نظری

مبانی نظری هر پژوهش حقوقی، چارچوب مفهومی و تحلیلی لازم را برای فهم دقیق مسأله و ارزیابی یافته‌ها فراهم می‌سازد. در حوزه‌ای نوظهور همچون متاورس سلامت که در آن فناوری‌های پیشرفته با حقوق بنیادین انسان تلاقی پیدا می‌کند، تبیین مفاهیم پایه و نظریه‌های حاکم بر حفاظت از داده‌های سلامت و حریم خصوصی از اهمیتی دوچندان برخوردار است. بدون اتکا به مبانی نظری روشن، تحلیل وضعیت حقوقی داده‌های سلامت در متاورس و سنجش کفایت یا ناکارآمدی قواعد موجود امکان‌پذیر نخواهد بود. از این‌رو، در این بخش ابتدا به مفهوم‌شناسی اصطلاحات کلیدی و سپس به بررسی مهم‌ترین نظریه‌ها و اصول حقوقی مرتبط با حریم خصوصی، داده‌های سلامت و خودمختاری بیمار پرداخته می‌شود تا زمینه‌ای منسجم برای تحلیل‌های بعدی مقاله فراهم آید.

۱-۱- مفهوم‌شناسی

در این قسمت ابتدا به تبیین مفاهیمی که متغیرهای بحث را تشکیل می‌دهند پرداخته خواهد شد:

متاورس: متاورس به‌عنوان مفهومی میان‌رشته‌ای، هم‌زمان واجد ابعاد فنی و حقوقی است و صرفاً نمی‌توان آن را یک فناوری یا پلتفرم دیجیتال تلقی کرد. از منظر فنی، متاورس به محیطی مجازی، سه‌بعدی، تعاملی و پایدار اطلاق می‌شود که از طریق هم‌گرایی فناوری‌هایی نظیر واقعیت مجازی، واقعیت افزوده، هوش مصنوعی و بلاک‌چین، امکان حضور و تعامل هم‌زمان کاربران را فراهم می‌سازد. این فضا نه تنها بازنمایی دیجیتال واقعیت فیزیکی است، بلکه به تدریج به زیست‌جهانی مستقل با قواعد، اقتصاد و هویت‌های خاص خود تبدیل می‌شود. از منظر حقوقی، متاورس چالشی جدی برای مفاهیم سنتی قلمرو، صلاحیت و مسئولیت ایجاد می‌کند، زیرا روابط حقوقی در محیطی شکل می‌گیرند که نه کاملاً واقعی و نه صرفاً مجازی است و مرزهای جغرافیایی در آن کارکرد کلاسیک خود را از دست می‌دهند (Arora, 2024: 41). این ویژگی‌ها موجب می‌شود که متاورس به‌عنوان یک «فضای تنظیم‌گری نوین» نیازمند بازتعریف مفاهیم حقوقی موجود باشد (Brownsword, 2022: 118).

داده‌های سلامت: داده‌های سلامت به مجموعه‌ای از اطلاعات اطلاق می‌شود که به وضعیت جسمی، روانی یا ذهنی یک شخص حقیقی مربوط بوده و از طریق ارائه خدمات درمانی، تشخیصی یا مراقبتی تولید یا پردازش می‌شوند. این داده‌ها صرفاً محدود به سوابق پزشکی سنتی نیستند، بلکه شامل داده‌های تولیدشده توسط ابزارهای پوشیدنی، سامانه‌های هوشمند سلامت و محیط‌های دیجیتال تعاملی نیز می‌شوند. در بستر متاورس، داده‌های سلامت ماهیتی پویا و پیوسته پیدا می‌کنند و از طریق تعاملات کاربر با محیط مجازی به‌صورت لحظه‌ای تولید می‌شوند. همین پیوستگی و حجم بالای داده‌ها، تحلیل و پیش‌بینی وضعیت سلامت فرد را ممکن می‌سازد، اما در عین حال مرز میان مراقبت درمانی و نظارت دائمی را تضعیف می‌کند و پرسش‌های بنیادینی درباره حدود مشروع پردازش این داده‌ها مطرح می‌سازد (Bujosa Vadell & Mansour, 2024: 87).

داده‌های حساس شخصی: داده‌های حساس شخصی، زیرمجموعه‌ای از داده‌های شخصی هستند که افشای آن‌ها می‌تواند پیامدهای جدی برای حقوق و آزادی‌های اساسی افراد به همراه داشته باشد. داده‌های سلامت، داده‌های ژنتیکی و داده‌های روان‌شناختی در کانون این دسته قرار می‌گیرند، زیرا به جنبه‌هایی از هویت انسان مربوط می‌شوند که عمیقاً با شخصیت، شأن و آینده فرد گره خورده‌اند. در فضای متاورس، حساسیت این داده‌ها تشدید می‌شود، چراکه ترکیب داده‌های سلامت با داده‌های رفتاری و زیستی، امکان ترسیم پروفایل‌های دقیق و پیش‌بینی‌گر از کاربران را فراهم می‌کند. چنین وضعیتی خطر تبعیض، برچسب‌زنی و بهره‌برداری تجاری یا حتی سیاسی از داده‌های حساس را افزایش داده و ضرورت حمایت مضاعف حقوقی از این دسته داده‌ها را برجسته می‌سازد (Dean Armstrong et al., 2023: 152).

حریم خصوصی و کرامت انسانی: حریم خصوصی و کرامت انسانی مفاهیمی به هم پیوسته‌اند که در بطن نظام‌های حقوقی مدرن جایگاه بنیادین دارند. حریم خصوصی صرفاً به معنای مصونیت از مداخله غیرمجاز نیست، بلکه ناظر بر حق فرد در کنترل اطلاعات مربوط به خود و تعیین حدود دسترسی دیگران به آن‌هاست. کرامت انسانی نیز اقتضا می‌کند که انسان هرگز به ابزاری برای اهداف اقتصادی یا فناورانه تقلیل نیابد. در محیط متاورس سلامت که بدن و ذهن انسان به داده‌های قابل پردازش تبدیل می‌شوند، خطر شیء‌انگاری انسان افزایش می‌یابد. از این رو، حفاظت از حریم خصوصی داده‌های سلامت در این فضا نه تنها یک الزام فنی یا اداری، بلکه تجلی عملی احترام به کرامت انسانی است (Brownsword, 2022: 64).

رضایت آگاهانه دیجیتال: رضایت آگاهانه دیجیتال به عنوان یکی از ارکان مشروعیت پردازش داده‌های سلامت، در متاورس با چالش‌های مفهومی و عملی جدی مواجه است. رضایت در معنای حقوقی خود مستلزم آگاهی، اختیار و امکان عدول است، درحالی که معماری پیچیده پلتفرم‌های متاورسی، شرایط استفاده طولانی و غیر شفاف و پردازش‌های ثانویه داده‌ها، تحقق واقعی این عناصر را تضعیف می‌کند. در چنین فضایی، رضایت کاربر اغلب به یک اقدام صوری و از پیش طراحی شده تقلیل می‌یابد و بیش از آنکه بیان اراده آزاد باشد، نتیجه عدم توازن قدرت میان کاربر و ارائه‌دهنده خدمات است. این وضعیت نشان می‌دهد که مفهوم سنتی رضایت آگاهانه برای پاسخگویی به الزامات متاورس سلامت کافی نیست و نیازمند بازتعریف و تقویت هنجاری است (Arora, 2024: 133).

۱-۲- مبانی نظری حفاظت از داده‌های سلامت

در این قسمت به تبیین نظریات مرتبط با حریم خصوصی بیماران و فضای متاورس پرداخته خواهد شد:

نظریه حق بر حریم خصوصی: نظریه حق بر حریم خصوصی به عنوان یکی از بنیان‌های اساسی حفاظت از داده‌های سلامت، بر این فرض استوار است که هر فرد حق دارد حوزه‌ای مصون از مداخله غیرموجه دیگران، به‌ویژه در خصوص اطلاعات شخصی و حساس خود، داشته باشد. در بستر سلامت دیجیتال و به‌ویژه متاورس، این نظریه از سطح منع افشای اطلاعات فراتر رفته و به حق کنترل فعال فرد بر چرخه حیات داده‌های سلامت گسترش می‌یابد. داده‌های سلامت در محیط‌های متاورسی نه تنها بازتاب وضعیت جسمی یا روانی فرد هستند، بلکه بخشی از هویت دیجیتال او را نیز شکل می‌دهند و همین امر، نقض حریم خصوصی را به تعرضی مستقیم به شخصیت فرد تبدیل می‌کند. از این منظر، حمایت حقوقی از داده‌های سلامت در متاورس مستلزم بازتعریف دامنه حریم خصوصی و پذیرش این واقعیت است که تعرض به داده‌های سلامت، هم‌سنگ تعرض به تمامیت شخصی فرد در فضای فیزیکی است (Ross, 2025: 92).

نظریه مالکیت داده‌ها: نظریه مالکیت داده‌ها می‌کوشد با نسبت دادن نوعی حق مالکانه به داده‌های شخصی، از جمله داده‌های سلامت، زمینه‌ای برای کنترل حقوقی مؤثرتر آن‌ها فراهم کند. این نظریه در فضای متاورس سلامت اهمیت مضاعفی می‌یابد، زیرا داده‌ها به منبعی ارزشمند برای تحلیل‌های پیش‌بینی‌گر، توسعه الگوریتم‌های هوش مصنوعی و خلق ارزش اقتصادی تبدیل شده‌اند. نسبت دادن مالکیت داده‌ها به بیمار، امکان اعمال حق انتقال، محدودسازی یا حتی منع پردازش داده‌ها را فراهم می‌سازد، اما در عین حال با چالش‌هایی مانند ماهیت غیرمادی داده‌ها و نقش مشترک بازیگران متعدد در تولید آن‌ها مواجه است. در متاورس، داده‌های سلامت اغلب حاصل تعامل بیمار با پلتفرم‌ها و فناوری‌ها هستند و همین امر، مفهوم مالکیت انحصاری را با تردید مواجه می‌کند. با این حال، نظریه مالکیت داده‌ها به عنوان ابزاری تحلیلی، بر ضرورت شناسایی جایگاه برتر بیمار در تصمیم‌گیری درباره سرنوشت داده‌های سلامت تأکید دارد (Salami & Islam, 2025: 143).

نظریه امنیت اطلاعات: نظریه امنیت اطلاعات بر حفاظت فنی و سازمانی از داده‌ها تمرکز دارد و هدف آن جلوگیری از دسترسی غیرمجاز، افشا، تغییر یا نابودی داده‌هاست. در حوزه داده‌های سلامت، امنیت اطلاعات نه تنها یک الزام فنی، بلکه پیش‌شرط تحقق حقوق بنیادین بیماران محسوب می‌شود. در محیط متاورس که داده‌های سلامت در بسترهای غیرمتمرکز، مبتنی بر هوش مصنوعی و گاه بر فناوری بلاک‌چین پردازش می‌شوند، سطح تهدیدات امنیتی به‌طور چشمگیری افزایش می‌یابد. ضعف در امنیت داده‌ها می‌تواند به نقض گسترده حریم خصوصی و حتی آسیب‌های جسمی یا روانی بیماران منجر شود. از این رو، نظریه امنیت اطلاعات

در متاورس سلامت صرفاً به معنای اتخاذ تدابیر فنی نیست، بلکه مستلزم نهاده‌سازی اصل «امنیت پیش‌فرض و در طراحی» به‌عنوان یک تعهد حقوقی است (Bhattathiri, 2025: 201).

اصل خودمختاری بیمار: اصل خودمختاری بیمار یکی از اصول بنیادین حقوق سلامت است که بر حق فرد در تصمیم‌گیری آزادانه و آگاهانه درباره بدن، سلامت و داده‌های مرتبط با آن تأکید دارد. در متاورس سلامت، خودمختاری بیمار با چالش‌های تازه‌ای روبه‌رو می‌شود، زیرا تصمیم‌گیری درباره پردازش داده‌های سلامت اغلب در محیط‌هایی صورت می‌گیرد که پیچیدگی فنی آن‌ها از درک کاربران عادی فراتر است. الگوریتم‌های هوش مصنوعی، تصمیمات خودکار و توصیه‌های درمانی مبتنی بر داده‌های کلان می‌توانند به تدریج نقش اراده بیمار را کمرنگ کنند. حفظ خودمختاری بیمار در چنین فضایی مستلزم شفافیت در فرایندهای پردازش داده، امکان مداخله و اعتراض بیمار و جلوگیری از جایگزینی تصمیم انسانی با تصمیم فناورانه است. از این منظر، اصل خودمختاری نه تنها یک ارزش اخلاقی، بلکه معیاری برای سنجش مشروعیت نظام‌های سلامت مبتنی بر متاورس به شمار می‌رود (Vemula, 2025: 76).

۲- کاربرد متاورس در حوزه سلامت و داده‌های سلامت

ورود متاورس به حوزه سلامت، صرفاً به معنای استفاده از یک فناوری نوین نیست، بلکه نشان‌دهنده دگرگونی عمیق در شیوه ارائه خدمات درمانی و تولید و پردازش داده‌های سلامت است. در این فضا، تعاملات درمانی، آموزشی و مدیریتی در قالب محیط‌های مجازی فراگیر بازتعریف می‌شوند و داده‌های سلامت به عنصر محوری این تحولات بدل می‌گردند. بررسی کاربردهای متاورس در حوزه سلامت، از یک سو ظرفیت‌های آن برای ارتقاء کیفیت و دسترسی به خدمات درمانی را آشکار می‌سازد و از سوی دیگر، ابعاد تازه‌ای از چالش‌های حقوقی مرتبط با حفاظت از داده‌های سلامت را نمایان می‌کند.

۲-۱- مصادیق استفاده از متاورس در سلامت

تله‌مدیسین در متاورس بیانگر گذار از ارتباطات دوجانبه و محدود سلامت الکترونیک به تعاملات فراگیر، سه‌بعدی و هم‌زمان میان بیمار و ارائه‌دهنده خدمات درمانی است. در این فضا، ارتباط درمانی صرفاً مبتنی بر انتقال داده‌های پزشکی نیست، بلکه بر تجربه حضور مشترک در یک محیط مجازی استوار می‌شود که می‌تواند اعتماد، درک متقابل و دقت تشخیصی را افزایش دهد. با این حال، این سطح از تعامل مستلزم پردازش پیوسته داده‌های زیستی و رفتاری بیمار است و مرز میان مراقبت درمانی و پایش دائمی را تضعیف می‌کند. از منظر حقوقی، تله‌مدیسین متاورسی چالش‌هایی همچون تعیین مسؤولیت حرفه‌ای، امنیت داده‌ها و اعمال قوانین ملی در محیطی فرامرزی را برجسته می‌سازد و نشان می‌دهد که توسعه این شیوه درمانی بدون بازنگری در چارچوب‌های حمایتی داده‌های سلامت می‌تواند به تضعیف حقوق بیماران منجر شود (Marwood, 2025: 118).

درمان‌های روان درمانی مبتنی بر واقعیت مجازی یکی از مهم‌ترین و حساس‌ترین کاربردهای متاورس در حوزه سلامت به شمار می‌روند، زیرا مستقیماً با لایه‌های عمیق روان و هیجانات بیماران سروکار دارند. این درمان‌ها از طریق بازآفرینی موقعیت‌های کنترل‌شده، امکان مواجهه تدریجی با محرک‌های اضطراب‌زا یا آسیب‌زا را فراهم می‌کنند و از این جهت ظرفیت بالایی برای ارتقاء اثربخشی درمان دارند. در عین حال، داده‌های تولیدشده در این فرایندها شامل واکنش‌های هیجانی، الگوهای رفتاری و پاسخ‌های ناخودآگاه بیمار است که سطحی از حساسیت را ایجاد می‌کند که فراتر از داده‌های پزشکی متعارف است. تحلیل و ذخیره این داده‌ها در محیط‌های متاورسی، بدون تضمین‌های حقوقی کافی، می‌تواند به نقض حریم خصوصی روانی بیماران و حتی دست‌کاری غیرمجاز رفتار آنان منجر شود (Mallikarjunaiah, 2024: 203).

آموزش پزشکی و شبیه‌سازی‌های درمانی در متاورس امکان تمرین مهارت‌های بالینی در محیط‌هایی ایمن، تکرارپذیر و عاری از خطر برای بیماران واقعی را فراهم می‌کند. این شبیه‌سازی‌ها با استفاده از داده‌های واقعی یا شبه‌واقعی بیماران طراحی می‌شوند و می‌توانند دقت و آمادگی حرفه‌ای کادر درمان را به‌طور چشمگیری افزایش دهند. با این حال، استفاده از داده‌های سلامت در فرایندهای آموزشی، به‌ویژه زمانی که داده‌ها قابلیت بازشناسایی داشته باشند، پرسش‌هایی جدی درباره مشروعیت پردازش ثانویه

داده‌ها مطرح می‌سازد. در متاورس، مرز میان آموزش، پژوهش و درمان به‌طور فزاینده‌ای مبهم می‌شود و همین امر ضرورت تعریف قواعد شفاف برای استفاده آموزشی از داده‌های سلامت را برجسته می‌سازد (Meçik, 2024: 156).

کلینیک‌ها و بیمارستان‌های مجازی به‌عنوان تجلی نهادی متاورس سلامت، ساختارهای سنتی ارائه خدمات درمانی را به چالش می‌کشند. این نهادها می‌توانند به‌صورت کاملاً دیجیتال فعالیت کرده و مجموعه‌ای از خدمات تشخیصی، درمانی و پیگیری را در یک فضای مجازی یکپارچه ارائه دهند. در چنین محیطی، داده‌های سلامت بیماران نه تنها ابزار درمان، بلکه زیرساخت اصلی عملکرد کل نظام درمانی محسوب می‌شوند. تمرکز حجم عظیمی از داده‌های حساس در پلتفرم‌های متاورسی، خطر نقض امنیت و سوءاستفاده تجاری را افزایش می‌دهد و پرسش‌هایی اساسی درباره مسئولیت حقوقی ارائه‌دهندگان این خدمات مطرح می‌کند. از این منظر، کلینیک‌های مجازی بیش از آنکه صرفاً یک نوآوری فناورانه باشند، آزمونی جدی برای ظرفیت حقوقی نظام‌های سلامت در حفاظت از داده‌های بیماران به شمار می‌روند (Jones, 2025: 89).

۲-۲- انواع داده‌های سلامت تولیدشده در متاورس

داده‌های بیومتریک به اطلاعاتی اطلاق می‌شوند که ویژگی‌های فیزیکی و زیستی فرد را اندازه‌گیری و ثبت می‌کنند، مانند ضربان قلب، فشار خون، الگوهای تنفسی، حرکات چشم و اثر انگشت. در متاورس سلامت، حسگرها و تجهیزات واقعیت مجازی قادر به ضبط لحظه‌ای این داده‌ها هستند و امکان پایش مستمر وضعیت جسمی بیماران را فراهم می‌آورند. اهمیت این داده‌ها فراتر از کاربردهای تشخیصی است؛ زیرا تجزیه و تحلیل آن‌ها می‌تواند روندهای سلامت فردی را پیش‌بینی کرده و الگوریتم‌های درمانی مبتنی بر هوش مصنوعی را هدایت کند. با این حال، حجم و حساسیت داده‌های بیومتریک، ریسک‌های جدی برای حریم خصوصی ایجاد می‌کند، چرا که هرگونه افشا یا دستکاری این داده‌ها می‌تواند تبعات جبران‌ناپذیری برای سلامت و امنیت فرد به همراه داشته باشد (Kalpokas & Kalpokienė, 2023: 112).

داده‌های رفتاری و روانی، شامل اطلاعات مربوط به رفتارها، واکنش‌ها، عادات و الگوهای هیجانی بیماران هستند که در محیط متاورس از طریق تعاملات دیجیتال و حسگرهای محیطی جمع‌آوری می‌شوند. این داده‌ها امکان تحلیل دقیق الگوهای روان‌شناختی و شناسایی نیازهای درمانی را فراهم می‌کنند، اما هم‌زمان با ایجاد مخاطرات حقوقی و اخلاقی مواجه‌اند. در صورتی که این داده‌ها بدون نظارت و چارچوب قانونی مناسب پردازش شوند، می‌توانند به شکل‌گیری پروفایل‌های رفتاری، پیش‌بینی تصمیمات فرد و حتی دستکاری انتخاب‌های درمانی منجر شوند. تحلیل و حفاظت از داده‌های رفتاری و روانی نیازمند تلفیق استانداردهای امنیت اطلاعات و اصول اخلاقی مرتبط با حریم خصوصی است (Johnson, 2025: 145).

داده‌های ژنتیکی، شامل اطلاعات مربوط به ساختار DNA و الگوهای وراثتی افراد هستند که قابلیت پیش‌بینی خطرات بیماری، شناسایی استعدادهای پزشکی و حتی طراحی درمان‌های شخصی‌سازی شده را دارند. در متاورس، جمع‌آوری و پردازش این داده‌ها از طریق سامانه‌های تشخیصی دیجیتال و شبیه‌سازی‌های درمانی انجام می‌شود و توانایی تحلیل ژنتیکی به‌صورت گسترده و فوری فراهم می‌آید. ماهیت غیرقابل تغییر و حساس داده‌های ژنتیکی، خطرات جدی در زمینه تبعیض، سوءاستفاده تجاری و افشای غیرمجاز ایجاد می‌کند و اهمیت تدوین مقررات ویژه برای حفاظت از این داده‌ها را در محیط‌های مجازی برجسته می‌سازد (Tot & Slakoper, 2021: 77).

داده‌های تعاملات اجتماعی بیماران شامل اطلاعات مربوط به ارتباطات، شبکه‌های اجتماعی، فعالیت‌های گروهی و تعاملات تعاملی کاربران در متاورس است. این داده‌ها امکان شناسایی الگوهای ارتباطی، سطح تعامل اجتماعی، حمایت‌های روانی و حتی اثرات اجتماعی بیماری‌ها را فراهم می‌کنند. با این حال، این دسته از داده‌ها به دلیل ماهیت ترکیبی و گسترده خود، علاوه بر حریم خصوصی، مسائل مرتبط با مالکیت داده و مسئولیت حقوقی را نیز مطرح می‌کنند. در متاورس، ترکیب داده‌های سلامت با داده‌های اجتماعی می‌تواند تصویری جامع از زندگی شخصی فرد ایجاد کند و در صورت سوءاستفاده، پیامدهای جدی برای حقوق بنیادین کاربران داشته باشد (Lee & Lee, 2025: 63).

۳- وضعیت حقوقی حفاظت از داده‌های سلامت در نظام‌های حقوقی مختلف

بررسی وضعیت حقوقی حفاظت از داده‌های سلامت در نظام‌های حقوقی مختلف، امکان مقایسه چارچوب‌های قانونی، استانداردهای حفاظتی و رویکردهای نظارتی را فراهم می‌کند. با توجه به گستردگی و فرامرزی بودن متاورس، تحلیل تطبیقی نظام‌های حقوقی بین‌المللی، اتحادیه اروپا، ایالات متحده و ایران می‌تواند نقاط قوت، ضعف و خلأهای موجود را روشن سازد. این بررسی نه تنها توانایی قوانین فعلی را در مواجهه با داده‌های حساس سلامت نشان می‌دهد، بلکه ضرورت تدوین مقررات خاص و به‌روز برای حفاظت مؤثر از حریم خصوصی بیماران در محیط‌های مجازی را برجسته می‌کند.

۳-۱- حقوق بین‌الملل و اسناد جهانی

در سطح بین‌المللی، حفاظت از حریم خصوصی و داده‌های شخصی به‌عنوان بخشی از حقوق بنیادین انسان شناخته شده و در اسناد معتبر حقوق بشر و سلامت بازتاب یافته است. اعلامیه جهانی حقوق بشر به صراحت بر حق هر فرد برای مصونیت از مداخله غیرمجاز در زندگی خصوصی، خانواده، منزل و مکاتبات شخصی تأکید می‌کند و آن را یکی از اصول اساسی کرامت انسانی معرفی می‌کند (Lamprecht, 2025: 58). این حق، پایه‌ای برای حفاظت از داده‌های سلامت نیز محسوب می‌شود، زیرا اطلاعات پزشکی و زیستی افراد بخش جدایی‌ناپذیر حریم خصوصی آن‌ها را تشکیل می‌دهند و افشای غیرمجاز آن‌ها می‌تواند نقض جدی کرامت انسانی تلقی شود.

میثاق بین‌المللی حقوق مدنی و سیاسی نیز با تصریح به حق افراد در حفظ حریم خصوصی و محدودیت مداخلات دولتی و غیر دولتی، چارچوبی قانونی و الزام‌آور برای حمایت از داده‌های شخصی ایجاد کرده است (Milanez, 2024: 101). این میثاق، با تعمیم مفهوم حریم خصوصی به حوزه‌های دیجیتال و سلامت، معیارهایی برای رفتار مشروع ارائه‌دهندگان خدمات و نهادهای جمع‌آوری‌کننده داده فراهم می‌آورد. با این حال، متن کنونی میثاق و رویه‌های بین‌المللی عمدتاً بر محیط‌های سنتی دیجیتال و تراکنش‌های اینترنتی تمرکز دارند و هنوز به‌طور صریح با ویژگی‌های خاص محیط‌های تعاملی سه‌بعدی و فرامرزی مانند متاورس سازگار نشده‌اند.

سازمان جهانی بهداشت (WHO) نیز با انتشار دستورالعمل‌ها و چارچوب‌های اخلاقی برای پردازش داده‌های سلامت، اصول حریم خصوصی، امنیت اطلاعات و دسترسی مسئولانه به داده‌ها را مورد تأکید قرار داده است (Mooij, 2023: 77). اسناد WHO تأکید دارند که داده‌های سلامت باید با رعایت حداکثر استانداردهای حفاظت و با رضایت آگاهانه فرد مورد پردازش قرار گیرند و هرگونه استفاده فراتر از اهداف درمانی یا تحقیقاتی مجاز نباشد. با این حال، این اسناد هنوز فاقد مقررات مشخص برای محیط‌های متاورس هستند، جایی که داده‌ها به‌صورت لحظه‌ای، فرامرزی و در تعامل با سیستم‌های هوش مصنوعی جمع‌آوری و پردازش می‌شوند. بنابراین، در سطح بین‌المللی یک چارچوب اصولی و عرفی برای حفاظت از حریم خصوصی و داده‌های سلامت وجود دارد، اما فضای متاورس به دلیل ماهیت نوین، پیچیدگی فناوریانه و تعاملات فرامرزی، همچنان از خلأ هنجاری رنج می‌برد (Shackelford et al., 2025: 132). این خلأ نشان می‌دهد که نیاز فوری به توسعه مقررات و دستورالعمل‌های خاص متاورس سلامت وجود دارد تا حفاظت از حریم خصوصی بیماران به‌صورت مؤثر و جامع تضمین شود و استانداردهای بین‌المللی به محیط‌های دیجیتال تعاملی سه‌بعدی تعمیم یابند.

۳-۲- حقوق اتحادیه اروپا

در نظام حقوقی اتحادیه اروپا، مقررات عمومی حفاظت از داده‌ها به‌عنوان چارچوبی جامع برای حفاظت از داده‌های شخصی، به‌ویژه داده‌های سلامت، عمل می‌کند. این مقررات، داده‌های سلامت را جزو داده‌های حساس طبقه‌بندی کرده و پردازش آن‌ها را مشروط به رعایت الزامات ویژه‌ای از جمله کسب رضایت آگاهانه، ضرورت پردازش برای اهداف درمانی یا تحقیقاتی و تضمین امنیت داده‌ها می‌داند (Findlay, 2025: 102). چنین چارچوبی، با ارائه تعاریف روشن و الزامات مشخص، امکان پایش دقیق استفاده از داده‌های سلامت و جلوگیری از سوءاستفاده‌های احتمالی را فراهم می‌کند و در عین حال بر حق دسترسی و اصلاح داده‌ها توسط افراد تأکید دارد.

اصول پردازش داده‌ها در فضای دیجیتال بر مبنای شفافیت، محدودیت هدف، حداقل‌سازی داده‌ها، صحت و امنیت داده‌ها و مسؤلیت‌پذیری طراحی شده‌اند. این اصول ایجاب می‌کنند که هر گونه پردازش داده‌های سلامت، با هدف مشخص، محدود به حداقل داده‌های مورد نیاز و با تضمین صحت و امنیت کامل انجام شود (Fung et al., 2025: 87). رعایت این اصول نه تنها برای حفاظت از حریم خصوصی بیماران ضروری است، بلکه تضمینی برای اعتماد کاربران به سامانه‌های دیجیتال سلامت فراهم می‌آورد. همچنین، اصل پاسخگویی و ضرورت مستندسازی هر فعالیت پردازشی، امکان نظارت و بازخواست قانونی ارائه‌دهندگان خدمات را تقویت می‌کند و شفافیت در پردازش داده‌ها را ارتقا می‌دهد (Chen et al., 2024: 133).

با این حال، اعمال این مقررات در محیط‌های متاورسی با چالش‌های جدی مواجه است. ماهیت سه‌بعدی، تعاملی و فرامرزی متاورس، تشخیص حوزه صلاحیت قانونی و تعیین مسؤلیت پردازش داده‌ها را دشوار می‌کند. علاوه بر این، داده‌های سلامت در متاورس به شکل لحظه‌ای، مستمر و با حجم وسیعی از داده‌های رفتاری و زیستی جمع‌آوری می‌شوند که فرایند کسب رضایت آگاهانه و اعمال اصول حداقل‌سازی داده را پیچیده می‌سازد (Grinhaus, 2024: 74). چالش دیگر، وجود چندین بازیگر و ارائه‌دهنده خدمات است که داده‌های بیماران را با روش‌های متفاوت پردازش و تحلیل می‌کنند و امکان نظارت متمرکز را محدود می‌سازد. از این منظر، اجرای مقررات عمومی حفاظت از داده‌ها در متاورس نیازمند بازنگری و تطبیق با ویژگی‌های نوین محیط‌های دیجیتال فراگیر است تا حریم خصوصی بیماران به طور مؤثر تضمین شود.

۳-۳- وضعیت حقوقی ایران

در نظام حقوقی ایران، حق حریم خصوصی از اصول بنیادین حمایت‌شده در قانون اساسی است و به عنوان بخشی از کرامت انسانی و آزادی‌های فردی به رسمیت شناخته شده است. اصل ۲۲ قانون اساسی صراحت دارد که هرگونه تفتیش، بررسی و افشای اطلاعات شخصی افراد بدون اجازه قانونی ممنوع است و از این منظر، حفاظت از داده‌های سلامت نیز در چارچوب کلی حق حریم خصوصی قابل تبیین است. این اصل، مبنایی برای ارزیابی مشروعیت پردازش داده‌های حساس در فضای دیجیتال فراهم می‌آورد و نشان می‌دهد که نقض حریم خصوصی بیماران، حتی در بستر فناوری‌های نوین، با کرامت انسانی تضاد دارد.

قانون جرائم رایانه‌ای، به عنوان ابزار کیفری برای مقابله با نقض حریم خصوصی، مقرراتی مشخص را در خصوص دسترسی غیرمجاز به داده‌های شخصی و افشای اطلاعات محرمانه وضع کرده است. این قانون امکان تعقیب کیفری متخلفان را فراهم می‌کند و به صراحت هر گونه دسترسی، افشا یا سوءاستفاده از داده‌های شخصی بدون رضایت مالک داده را جرم‌انگاری کرده است. با این حال، محدوده قانونی این قانون عمدتاً بر فعالیت‌های سنتی دیجیتال و رایانه‌ای متمرکز است و کمتر به پیچیدگی‌های محیط‌های تعاملی سه‌بعدی و فرامرزی مانند متاورس پرداخته است که منجر به خلأهای کاربردی در حفاظت از داده‌های سلامت می‌شود.

علاوه بر قوانین کیفری، آیین‌نامه‌ها و سیاست‌های سلامت الکترونیک در ایران، چارچوب‌هایی برای ارائه خدمات درمانی از طریق بسترهای دیجیتال فراهم آورده‌اند. این اسناد به استانداردسازی فرآیندهای تبادل داده‌های سلامت، امنیت اطلاعات و حفظ محرمانگی بیماران توجه دارند و الزامات فنی و سازمانی لازم برای بهره‌گیری از سامانه‌های الکترونیک سلامت را تعیین می‌کنند. با این حال، این سیاست‌ها و آیین‌نامه‌ها عمدتاً بر بسترهای سنتی دیجیتال، سامانه‌های پرونده الکترونیک و خدمات تله‌مدیسین تمرکز دارند و به ویژگی‌ها و نیازهای ناشی از محیط‌های متاورسی، مانند پردازش داده‌های لحظه‌ای، تعاملات سه‌بعدی و فعالیت‌های فرامرزی، پاسخ نمی‌دهند.

نتیجه آنکه، علی‌رغم وجود اصول بنیادین قانونی و مقررات جزئی در حوزه حفاظت از داده‌ها و حریم خصوصی، فضای متاورس به عنوان محیطی نوظهور، همچنان با خلأهای تقنینی جدی مواجه است. قوانین و آیین‌نامه‌های موجود فاقد شفافیت و الزامات اختصاصی برای مدیریت داده‌های سلامت تولیدشده در متاورس هستند و نمی‌توانند پاسخگوی پیچیدگی‌های ناشی از تعاملات سه‌بعدی، پردازش لحظه‌ای داده‌ها و نقش بازیگران متعدد در این فضا باشند. این وضعیت نشان‌دهنده ضرورت بازنگری قانونی و تدوین مقررات اختصاصی است تا حفاظت از حریم خصوصی بیماران در محیط‌های دیجیتال نوین تضمین شود.

۴- چالش‌ها و تهدیدهای حقوقی متاورس برای حریم خصوصی بیماران

فضای متاورس، با ویژگی‌های منحصربه‌فرد خود از جمله تعامل سه‌بعدی، جمع‌آوری لحظه‌ای داده‌ها، فرامرزی بودن و نقش گسترده هوش مصنوعی، چالش‌های حقوقی جدید و پیچیده‌ای برای حفاظت از حریم خصوصی بیماران ایجاد کرده است. این محیط نوین، مرزهای سنتی قانون‌گذاری، مسئولیت و مالکیت داده‌ها را دچار ابهام می‌کند و خطر سوءاستفاده از داده‌های سلامت را افزایش می‌دهد. بررسی چالش‌ها و تهدیدهای حقوقی متاورس، امکان شناسایی نقاط ضعف چارچوب‌های قانونی موجود و ضرورت تدوین راهکارهای نوآورانه برای حفاظت مؤثر از حریم خصوصی بیماران را آشکار می‌سازد.

۴-۱- چالش‌های حقوقی

یکی از مهم‌ترین چالش‌های حقوقی متاورس، فقدان تعریف قانونی روشن از این فضا در اغلب نظام‌های حقوقی جهان است. عدم وجود تعریفی دقیق و واحد، تدوین قواعد حقوقی کاربردی و تعیین حوزه صلاحیت قانونی را دشوار می‌کند و باعث ایجاد ابهام در مسئولیت ارائه‌دهندگان خدمات و بازیگران مختلف در متاورس می‌شود (Council of Europe, 2024: 35). این خلأ تعریفی موجب شده است که قوانین موجود که عمدتاً برای فضای دیجیتال سنتی طراحی شده‌اند، نتوانند به‌طور مؤثر با پیچیدگی‌های محیط‌های سه‌بعدی و تعاملی متاورس سازگار شوند. در حقوق ایران نیز این چالش مشهود است و هیچ چارچوب قانونی اختصاصی برای شناسایی و تعریف متاورس وجود ندارد که محدودیت‌های قانونی برای پردازش داده‌های سلامت در آن را روشن سازد.

چالش دیگر، عدم شفافیت مالکیت داده‌ها در متاورس است. داده‌های سلامت تولیدشده در محیط‌های سه‌بعدی، هم‌زمان تحت کنترل چندین بازیگر شامل کاربران، ارائه‌دهندگان فناوری و شرکت‌های واسطه هستند که تعیین مالک اصلی داده و حق تصمیم‌گیری درباره پردازش آن را دشوار می‌کند (de Elizalde, 2024: 104). نبود وضوح در مالکیت داده‌ها می‌تواند منجر به اختلافات حقوقی، سوءاستفاده تجاری یا تبعیض علیه بیماران شود. در حقوق ایران نیز این مسأله مطرح است، زیرا قانون‌گذار هنوز مالکیت داده‌های دیجیتال، به‌ویژه داده‌های حساس سلامت در محیط‌های نوین مانند متاورس را به‌طور شفاف تعریف نکرده است.

مشکل تحقق رضایت آگاهانه واقعی نیز از دیگر چالش‌های کلیدی است. برای مشروعیت پردازش داده‌های سلامت، کسب رضایت آگاهانه بیمار ضروری است، اما معماری پیچیده پلتفرم‌های متاورسی، حجم بالای داده‌ها و پردازش‌های ثانویه، امکان فهم کامل پیامدهای پردازش را برای کاربر محدود می‌کند (Di Porto & Pollicino, 2025: 59). به عبارت دیگر، رضایت اغلب به شکل صوری و مبتنی بر پذیرش شرایط استفاده طولانی و غیر شفاف جمع‌آوری می‌شود و عملاً استقلال تصمیم‌گیری بیمار کاهش می‌یابد. این چالش در نظام حقوقی ایران نیز مشاهده می‌شود، زیرا هیچ مقررات اختصاصی برای تضمین رضایت آگاهانه در محیط‌های متاورسی وجود ندارد.

پردازش فرامرزی داده‌ها، به‌ویژه داده‌های سلامت، پیچیدگی دیگری ایجاد می‌کند. داده‌ها در متاورس ممکن است در سرورها و سیستم‌های واقع در کشورهای مختلف ذخیره و پردازش شوند که اختلاف قوانین ملی، استانداردهای امنیتی و شیوه‌های نظارتی را با هم در تضاد قرار می‌دهد (Jones et al., 2021: 142). این وضعیت تعیین مسئولیت قانونی، اعمال حقوق بیماران و تضمین رعایت حریم خصوصی را دشوار می‌کند. در ایران نیز چنین مسأله‌ای وجود دارد، زیرا قوانین ملی در مواجهه با داده‌های فرامرزی محدودیت‌ها و دستورالعمل‌های مشخصی برای متاورس ندارند و حفاظت از داده‌ها در این شرایط نیازمند بازنگری قانونی است. نتیجه آنکه چالش‌های حقوقی متاورس برای حفاظت از حریم خصوصی بیماران، از فقدان تعریف قانونی و شفافیت مالکیت داده‌ها تا دشواری کسب رضایت واقعی و پردازش فرامرزی داده‌ها گسترده است و تقریباً در تمامی نظام‌های حقوقی جهان و ایران به چشم می‌خورد. این وضعیت ضرورت تدوین چارچوب‌های قانونی نوآورانه و منسجم را برای محیط‌های دیجیتال تعاملی سه‌بعدی نشان می‌دهد.

۴-۲- تهدیدهای فناوریانه

نقض امنیت داده‌ها یکی از جدی‌ترین تهدیدهای فناوریانه متاورس برای حریم خصوصی بیماران به شمار می‌رود. محیط‌های متاورسی سلامت به دلیل جمع‌آوری لحظه‌ای و پیوسته حجم عظیمی از داده‌های حساس زیستی، روانی و رفتاری، هدف بالقوه حملات سایبری و نفوذهای غیرمجاز قرار دارند. ضعف در سامانه‌های امنیتی یا نقص در طراحی الگوریتم‌های پردازش داده می‌تواند منجر به افشای اطلاعات محرمانه بیماران و آسیب به سلامت جسمی و روانی آن‌ها شود (Abdusatarov, 2023: 198). در نظام حقوقی ایران نیز، تهدید نقض امنیت داده‌ها مطرح است و با وجود مقررات جزئی مرتبط با سلامت الکترونیک، چارچوبی اختصاصی برای محیط‌های متاورسی تدوین نشده است.

سوءاستفاده تجاری از داده‌های سلامت، تهدیدی دیگر است که به ماهیت اقتصادی داده‌های تولیدشده در متاورس مرتبط است. شرکت‌های فناوری و پلتفرم‌های متاورسی قادرند داده‌های بیماران را برای اهداف بازاریابی، تحلیل‌های تجاری یا توسعه الگوریتم‌های هوش مصنوعی به کار گیرند. چنین استفاده‌ای در بسیاری از نظام‌های حقوقی با چالش‌های اخلاقی و قانونی مواجه است و ضرورت شفافیت و محدودیت قانونی در پردازش داده‌ها را برجسته می‌کند (Aidonojie et al., 2024: 115). در حقوق ایران نیز این مسأله وجود دارد و با نبود مقررات اختصاصی برای استفاده تجاری از داده‌های سلامت در متاورس، بیماران در معرض خطر بهره‌برداری غیرمجاز قرار می‌گیرند.

پروفایل‌سازی بیماران یکی از پیامدهای فناوریانه پردازش داده‌ها در متاورس است. ترکیب داده‌های زیستی، روانی و رفتاری امکان ایجاد پروفایل‌های دقیق و پیش‌بینی‌کننده از وضعیت سلامت، ترجیحات درمانی و حتی رفتارهای آینده بیماران را فراهم می‌کند. این اقدام اگرچه می‌تواند کارایی درمان و شخصی‌سازی خدمات را افزایش دهد، اما در عین حال خطر تبعیض، برچسب‌زنی و محدود کردن آزادی تصمیم‌گیری بیمار را افزایش می‌دهد (Bisoyi, 2025: 142). در ایران نیز پروفایل‌سازی بیماران در محیط متاورسی بدون ضوابط مشخص حقوقی می‌تواند تهدیدی جدی برای حریم خصوصی باشد.

هوش مصنوعی و تحلیل داده‌های حساس، عامل دیگری است که پیچیدگی تهدیدهای فناوریانه را افزایش می‌دهد. الگوریتم‌های هوش مصنوعی قادر به تحلیل حجم عظیمی از داده‌های سلامت و استخراج الگوها، پیش‌بینی بیماری‌ها و ارائه توصیه‌های درمانی هستند. با این حال، پردازش داده‌ها توسط هوش مصنوعی بدون نظارت مناسب می‌تواند منجر به خطا، تبعیض الگوریتمی و استفاده غیرمجاز از اطلاعات حساس شود (Jones, 2025: 177). در نظام حقوقی ایران نیز این تهدید مطرح است، زیرا هیچ مقررات مشخصی برای محدود کردن تحلیل داده‌های حساس توسط سیستم‌های هوشمند در محیط‌های متاورسی وجود ندارد و بیماران در معرض آسیب‌های بالقوه قرار دارند. به این ترتیب، تهدیدهای فناوریانه متاورس برای حریم خصوصی بیماران، از نقض امنیت داده‌ها و سوءاستفاده تجاری گرفته تا پروفایل‌سازی و تحلیل هوشمند داده‌ها، در اغلب نظام‌های حقوقی جهان و ایران قابل مشاهده است و ضرورت توسعه چارچوب‌های حقوقی نوآورانه و اختصاصی برای مدیریت این ریسک‌ها را آشکار می‌سازد.

۵- متاورس؛ فرصت یا تهدید؟

متاورس در حوزه سلامت یک پدیده دوجوهی است که هم فرصت‌های نوین و هم تهدیدهای جدی برای بیماران و نظام‌های حقوقی ایجاد می‌کند. از یک سو، این فضا امکان دسترسی گسترده‌تر به خدمات درمانی، بهبود کیفیت مراقبت و شخصی‌سازی درمان‌ها را فراهم می‌آورد. از سوی دیگر، ویژگی‌های فناوریانه متاورس، مانند جمع‌آوری لحظه‌ای داده‌ها، تعاملات فرامرزی و تحلیل هوشمند اطلاعات حساس، چالش‌های حریم خصوصی و حفاظت قانونی را پیچیده‌تر می‌کند. بررسی انتقادی این فضا، امکان سنجش تعادل میان مزایا و ریسک‌ها و ارزیابی ظرفیت نظام‌های حقوقی موجود برای پاسخ به نیازهای نوین سلامت دیجیتال را فراهم می‌آورد.

۵-۱- فرصت‌های حقوقی و درمانی

استفاده از متاورس در حوزه سلامت امکان افزایش دسترسی به خدمات درمانی را به‌طور قابل‌توجهی فراهم می‌آورد. بیماران در مناطق دورافتاده یا با محدودیت‌های حرکتی می‌توانند از طریق محیط‌های مجازی با متخصصان و مراکز درمانی تعامل داشته باشند و مراقبت‌های پزشکی لازم را دریافت کنند. این دسترسی گسترده، علاوه بر کاهش نابرابری جغرافیایی، موجب تسهیل پیگیری درمان و ارتقاء سطح بهداشت عمومی می‌شود (Jones, 2025: 211).

متاورس همچنین ظرفیت ارتقاء کیفیت تشخیص و درمان را داراست. شبیه‌سازی‌های سه‌بعدی، پردازش داده‌های لحظه‌ای و تحلیل‌های پیشرفته، امکان مشاهده دقیق‌تر علائم، پیش‌بینی روند بیماری‌ها و طراحی درمان‌های شخصی‌سازی‌شده را فراهم می‌کند. این توانمندی‌ها می‌تواند دقت تشخیص را افزایش داده و خطاهای پزشکی را کاهش دهد، در نتیجه کیفیت خدمات درمانی بهبود می‌یابد و بیماران از درمان‌های مؤثرتر بهره‌مند می‌شوند (Milanez, 2024: 58).

یکی دیگر از فرصت‌های مهم متاورس، کاهش هزینه‌های درمان است. با امکان ارائه خدمات از راه دور و کاهش نیاز به حضور فیزیکی در مراکز درمانی، هزینه‌های حمل و نقل، بستری و زمان انتظار کاهش می‌یابد. همچنین، شبیه‌سازی‌ها و آموزش‌های مجازی می‌توانند هزینه‌های آموزشی و تمرینی کادر درمان را کاهش دهند و منابع مالی سیستم سلامت به‌صورت بهینه‌تری تخصیص یابد (Salami & Islam, 2025: 193). این کاهش هزینه‌ها نه تنها برای بیماران، بلکه برای نظام‌های سلامت و دولت‌ها نیز مزیت اقتصادی قابل‌توجهی ایجاد می‌کند.

متاورس می‌تواند بیماران را توانمند سازد و نقش فعال آن‌ها در مدیریت سلامت خود را افزایش دهد. دسترسی به داده‌های سلامت لحظه‌ای، امکان پیگیری روند درمان و تعامل با ابزارهای آموزشی و حمایتی، بیماران را قادر می‌سازد تصمیمات آگاهانه‌تری درباره سلامت خود اتخاذ کنند. توانمندسازی بیماران، علاوه بر ارتقاء کیفیت مراقبت، بر خودمختاری و استقلال آن‌ها تأکید دارد و زمینه را برای مشارکت فعال‌تر در فرآیندهای درمانی فراهم می‌کند (Jones, 2025: 218). به این ترتیب، متاورس با ایجاد دسترسی گسترده، بهبود کیفیت تشخیص و درمان، کاهش هزینه‌ها و توانمندسازی بیماران، فرصت‌های حقوقی و درمانی قابل‌توجهی برای نظام سلامت فراهم می‌آورد و ظرفیت‌های فناورانه آن می‌تواند به ارتقاء عدالت و کارآمدی در ارائه خدمات درمانی منجر شود.

۵-۲- تهدیدها و ریسک‌های حقوقی

متاورس، با جمع‌آوری گسترده و لحظه‌ای داده‌های سلامت، تهدیدی جدی برای حریم خصوصی بیماران ایجاد می‌کند. داده‌های زیستی، روانی و رفتاری که در این فضا تولید می‌شوند، بدون تضمین شفافیت در پردازش و مالکیت، در معرض افشا، سوءاستفاده و تحلیل‌های غیرمجاز قرار می‌گیرند. این وضعیت باعث تضعیف کنترل فرد بر اطلاعات شخصی خود شده و امکان تصمیم‌گیری آگاهانه درباره داده‌ها را محدود می‌کند (Council of Europe, 2024: 41). در نتیجه، بیماران از حق بنیادین خود برای حفاظت از حریم خصوصی محروم می‌شوند و اعتماد آن‌ها به خدمات درمانی دیجیتال کاهش می‌یابد.

نقض اصل کرامت انسانی نیز یکی دیگر از ریسک‌های حقوقی متاورس است. داده‌های سلامت نه تنها اطلاعات فنی درباره وضعیت جسمی یا روانی فرد هستند، بلکه بخشی از هویت و شخصیت او را شکل می‌دهند. پردازش و استفاده غیرمجاز از این داده‌ها می‌تواند به شکل‌گیری پروفایل‌های رفتاری، پیش‌بینی تصمیمات شخصی و حتی فشارهای درمانی یا اقتصادی منجر شود و در نتیجه کرامت فرد را تهدید کند (Brownsword, 2022: 75). فقدان مقررات مشخص برای محدود کردن چنین استفاده‌ای در محیط‌های مجازی، بیماران را در معرض آسیب‌های روانی و اجتماعی قرار می‌دهد و ضرورت بازتعریف حقوق بنیادین در فضای دیجیتال را برجسته می‌کند.

عدم توازن قدرت میان بیماران و شرکت‌های فناوری یکی دیگر از چالش‌های کلیدی حقوقی است. ارائه‌دهندگان پلتفرم‌های متاورسی به منابع عظیم داده‌ای، ابزارهای پردازشی پیشرفته و توان تحلیل هوشمند دسترسی دارند، درحالی‌که بیماران در موقعیت تصمیم‌گیری ضعیف قرار دارند و اغلب از پیچیدگی‌های فناورانه مطلع نیستند (Bisoyi, 2025: 128). این عدم توازن باعث

می‌شود قدرت واقعی کنترل داده‌ها و مدیریت فرآیند درمان از دست بیمار خارج شود و تسلط شرکت‌های فناوری بر جریان اطلاعات افزایش یابد. در حقوق ایران نیز این چالش قابل مشاهده است و نبود چارچوب‌های قانونی اختصاصی برای محیط‌های متاورسی، بیماران را در موقعیت ضعیف قرار داده و ریسک سوءاستفاده را افزایش می‌دهد. به‌طور کلی، تهدیدهای حقوقی متاورس شامل تضعیف حریم خصوصی، نقض کرامت انسانی و عدم توازن قدرت میان بیماران و شرکت‌های فناوری است. این تهدیدها نشان می‌دهند که بهره‌برداری از فرصت‌های درمانی متاورس بدون بازنگری قانونی و تدوین مقررات ویژه، می‌تواند به مخاطرات جدی برای حقوق بنیادین بیماران منجر شود و ضرورت توسعه چارچوب‌های حقوقی نوآورانه و جامع برای حفاظت از بیماران را برجسته می‌سازد.

نتیجه‌گیری

بررسی وضعیت حقوقی حفاظت از داده‌های سلامت در متاورس نشان می‌دهد که سؤال اصلی مقاله، یعنی «آیا چارچوب‌های حقوقی موجود قادر به حمایت از حریم خصوصی بیماران در متاورس هستند؟» پاسخ روشنی ندارد و تقریباً تمامی نظام‌های حقوقی جهان و ایران با خلأها و محدودیت‌های جدی مواجه‌اند. قوانین موجود، از جمله مقررات ملی و بین‌المللی حریم خصوصی، قوانین حفاظت از داده‌ها و آیین‌نامه‌های سلامت الکترونیک، تا حدی می‌توانند اصول کلی حفاظت از داده‌های حساس را تأمین کنند، اما توانایی آن‌ها در پاسخ به ویژگی‌های منحصربه‌فرد متاورس، مانند تعاملات سه‌بعدی، پردازش لحظه‌ای، تحلیل‌های هوش مصنوعی و فرامرزی بودن داده‌ها، ناکافی است. این وضعیت نشان می‌دهد که متاورس هم فرصت‌های نوینی برای ارتقاء سلامت و کارآمدی خدمات درمانی ایجاد کرده و هم تهدیدات قابل توجهی برای حریم خصوصی و کرامت بیماران به همراه دارد.

از منظر فرصت‌ها، متاورس امکان افزایش دسترسی بیماران به خدمات درمانی، بهبود کیفیت تشخیص و درمان، کاهش هزینه‌های مرتبط با مراقبت‌های حضوری و توانمندسازی بیماران برای مدیریت سلامت خود را فراهم می‌آورد. این قابلیت‌ها می‌توانند نظام‌های سلامت را کارآمدتر کرده و عدالت در ارائه خدمات درمانی را ارتقا دهند. در عین حال، تهدیدها شامل تضعیف حریم خصوصی، نقض کرامت انسانی، سوءاستفاده تجاری از داده‌های حساس، پروفایل‌سازی بیماران و عدم توازن قدرت میان بیماران و شرکت‌های فناوری است که بدون چارچوب قانونی مناسب، بیماران را در موقعیت آسیب‌پذیر قرار می‌دهد.

برای رفع این چالش‌ها، تدوین قانون خاص حفاظت از داده‌های سلامت دیجیتال ضروری است تا اصول، الزامات و محدودیت‌های مرتبط با پردازش داده‌های سلامت در محیط‌های نوین به‌صورت روشن تعیین شود. ایجاد چارچوب حقوقی اختصاصی برای متاورس سلامت نیز می‌تواند ابهامات مسئولیت، مالکیت داده و حوزه صلاحیت قانونی را کاهش دهد و تضمین‌کننده اجرای اصول حریم خصوصی و کرامت انسانی باشد. تقویت نظام رضایت آگاهانه دیجیتال، به گونه‌ای که بیماران بتوانند تصمیمات آگاهانه درباره پردازش داده‌های خود اتخاذ کنند، از دیگر ضرورت‌هاست. همچنین، الزام به رعایت اصل طراحی برای حریم خصوصی (حریم خصوصی از ابتدا در طراحی سیستم‌ها مدنظر قرار گیرد) و استفاده از ابزارهای فنی برای کاهش ریسک‌های احتمالی، می‌تواند امنیت داده‌ها را تضمین کند. نظارت نهادهای مستقل، به منظور ارزیابی و بازبینی عملکرد ارائه‌دهندگان خدمات در متاورس و تضمین رعایت الزامات قانونی، اهمیت بالایی دارد. در سطح بین‌المللی، همکاری و هماهنگی میان کشورها برای ایجاد استانداردهای جهانی و مدیریت پردازش فرامرزی داده‌های سلامت، می‌تواند امنیت و حریم خصوصی بیماران را در محیط‌های متاورسی افزایش دهد. در جمع‌بندی، متاورس در حوزه سلامت هم فرصت‌های بزرگ و هم تهدیدهای جدی ایجاد می‌کند و پاسخگویی به این چالش‌ها بدون بازنگری و توسعه چارچوب‌های حقوقی نوآورانه و جامع امکان‌پذیر نیست. تدوین قوانین اختصاصی، ایجاد چارچوب‌های حقوقی متاورس سلامت، تقویت رضایت آگاهانه دیجیتال، طراحی سیستم‌ها با محوریت حریم خصوصی، نظارت مستقل و همکاری بین‌المللی، عناصر کلیدی برای تضمین حفاظت از داده‌های سلامت و ارتقاء کرامت بیماران در فضای متاورس محسوب می‌شوند.



ملاحظات اخلاقی: ملاحظات اخلاقی مربوط به انجام پژوهش رعایت شده است.

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافع بوده است.

سهم نویسندگان: در این پژوهش، نویسنده مستقل عمل کرده است.

تشکر و قدردانی: از همه کسانی که در بازخوانی و ویرایش اثر همیاری و راهنمایی داشتند، قدردانی و تشکر می‌گردد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین مالی انجام گرفته است.

منابع و مأخذ

- Abdusatarov, J (2023). "Issues that Need to be Resolved when Developing the Legal Framework of International Private Law Relations in Metaverse". *World Bulletin of Management and Law*, 21: 193-204.
- Aidonojie, P. A; Eregbuonye, O; Ibeh, S; Antai, G. O & Kolawale, A. A (2024). "Prospects and Legal Challenges Regarding Intellectual Property Rights in Metaverse Operations in Nigeria". *Wacana Hukum*, 30(2): 109-129.
- Arora, D (2024). *Virtual Realms & Beyond: A Metaverse Research Odyssey: Exploration of Digital Realities in the Metaverse Environment*. Hague: Notion Press.
- Bhattathiri, P (2025). *Metaverse Development*. Hague: Educohack Press.
- Bisoyi, A (2025). *Blockchain and Legitimacy: The Rule of Law by Design*. London: Springer.
- Brownsword, R (2022). *Rethinking Law, Regulation, and Technology*. Hague: Edward Elgar Publishing.
- Bujosa Vadell, L. M; Mansour, N (2024). *Finance and Law in the Metaverse World: Regulation and Financial Innovation in the Virtual World*. London: Springer.
- Chen, H.-Y; Alam, N & Jenweeranon, P (2024). *Global Perspectives in the Metaverse: Law, Economics, and Finance*. London: Springer.
- Council of Europe (2024). *The Metaverse and Its Impact on Human Rights, the Rule of Law and Democracy*. Brussel: Council of Europe.
- de Elizalde, F (2024). Consumer Protection in the Metaverse. In *Research Handbook on the Metaverse and Law* (pp. 98-117). Edward Elgar Publishing.
- Dean Armstrong KC, Dean Armstrong, Dan Hyde, Sam Thomas (2023). *Blockchain and Cryptocurrency: International Legal and Regulatory Challenges*. Hague: Bloomsbury Academic.
- Di Porto, F & Pollicino, O (2025). *Law and Politics of Virtual Worlds: How NFTs and Metaverse are Reshaping Legal Systems*. London: Springer.
- Findlay, M (2025). *Governing the Metaverse: Law, Order and Freedom in Digital Space*. Hague: Edward Elgar.
- Fung, B. C. M; Fachkha, C & Tchakounté, F (2025). *Safe, Secure, Ethical, Responsible Technologies and Emerging Applications*. London: Springer.
- Grinhaus, A (2024). *A Practical Guide to Web3, Blockchain, and Smart Contract Law*. Toronto: LexisNexis Canada Incorporated.
- Jones, E; Ryan, F; Thanaraj, A & Wong, T (2021). *Digital Lawyering: Technology and Legal Practice in the 21st Century*. Hague: Routledge, Taylor & Francis Group.

-
- Jones, M. E (2025). *Digital Media Law: Rights, Rules, and Regulations in the Age of AI*. Hague: Bloomsbury Academic.
 - Johnson, M (2025). *Tech Law Architects*. New York: Publifye AS.
 - Kalpokas, I & Kalpokienė, J (2023). *Regulating the Metaverse: A Critical Assessment*. Hague: Taylor & Francis.
 - Lamprecht, A (2025). *Un 2.0 and the Metaverse: Are We Seeing What Is Possible?* Hague: Diplofoundation.
 - Lee, J & Lee, J.-A (2025). *Web3 Governance: Law and Policy*. Hague: Taylor & Francis.
 - Mallikarjunaiah, J. M (2024). *Ethico-Legal Dimensions of Advanced Technologies - A Pathway to Responsible Innovation*. Hague: Notion Press Media Pvt. Limited.
 - Marwood, V (2025). *Online Business Laws*. London: Publifye AS.
 - Meçik, O (2024). *Reskilling the Workforce for Technological Advancement*. London: IGI Global.
 - Milanez, M (2024). *The Legal Implications of the Metaverse*. London: Amazon Digital Services LLC.
 - Mooij, A (2023). *Regulating the Metaverse Economy*. London: Springer.
 - Ross, M (2025). *Law Tech Shift*. Hague: Publifye AS.
 - Salami, I & Islam, N (2025). *Metaverse Innovation: Technological, Financial, and Legal Perspectives*. London: Springer.
 - Shackelford, S; Mattioli, M; Prince, J & Marinotti, J (2025). *The Metaverse: What Everyone Needs to Know*. Oxford: Oxford University Press.
 - Tot, I & Slakoper, Z (2021). *Digital Technologies and the Law of Obligations*. Hague: Taylor & Francis.
 - Vemula, A (2025). *AI Laws: Governance, Ethics, and the Future of Artificial Intelligence*. London: Anand Vemula.