Journal Homepage: https://journals.sbmu.ac.ir/be DOI: https://doi.org/10.22037/bioeth.v15i40.48354

Original Article Open Access

Akhlāq-i zīstī

i.e., Bioethics Journal

2025; 15: e26

Challenges of Protecting Patient Health Data in Smart Healthcare

Tahmine Esfandiary[1], Hamid Rostaei Sadrabadi[2*], Nasrolah Jafari khosroabadi[3], Seyed Ahmad Mirkhalili[4]

1. Department of Law, Faculty of Theology and Islamic Studies, Meybod University, Meybod, Iran.
2. Department of Jurisprudence and Islamic Law, Faculty of Theology and Islamic Studies, Meybod University, Meybod, Iran.
3. Department of Law, Faculty of Theology and Islamic Studies, Meybod University, Meybod, Iran.
4. Department of Jurisprudence and Islamic Law, Faculty of Theology and Islamic Studies, Meybod University, Meybod, Iran.

ABSTRACT

Background and Aim: The processing of individuals' data by artificial intelligence in the health sector is closely linked to the necessity of preserving their privacy. Accordingly, the aim of the present article is to examine, on one hand, ethical challenges such as informed consent, inequality and discrimination, and lack of transparency and explain ability, and on the other hand, legal challenges such as the legal personality of therapeutic robots, unauthorized access and breach of patient data confidentiality, and secondary use of data, in the realm of protecting patients' personal health data.

Methods: This article, using a descriptive-analytical method and library resources, examines the ethical and legal challenges of protecting patient health data in smart healthcare.

Ethical Considerations: In all stages of writing this research, the originality of texts, honesty, and trustworthiness have been observed.

Results: Protecting patient health data is an essential matter in the field of smart healthcare. Based on this, the European Union has made the first efforts to enact protective laws in the form of data protection regulations in 2016. However, in Iranian law, the issue of data protection has not been specifically addressed, and it seems that enacting data protection regulations, especially health-centric data regulations, as soon as possible, is a necessity.

Conclusion: Since artificial intelligence is an emerging phenomenon in various domains such as legal and medical sciences, different countries are striving to enact relevant regulations. The complexity, technicality, and specialized nature of artificial intelligence have created numerous ethical and legal challenges, such as the issue of the possibility of recognizing an independent legal personality for therapeutic robots, the potential breach of patient health data by medical centers, and the use of discriminatory data in patient treatment, matters that had not been raised in legal science before.

Keywords: Privacy, Therapeutic Robot, Data Protection, Medical Law.

Corresponding Author: Hamid Rostaei Sadrabadi; **Email:** rostaei@meybod.ac.ir

Received: April 16, 2025; **Accepted:** July 26, 2025; **Published Online:** December 28, 2025

Please cite this article as:

Esfandiary T, Rostaei Sadrabadi H, Jafari khosroabadi N, Mirkhalili SA. Challenges of Protecting Patient Health Data in Smart Healthcare. Akhlaq-i zisti, i.e., Bioethics Journal. 2025; 15: e26.

DOI: https://doi.org/10.22037/bioeth.v15i40.48354 Journal Homepage: https://journals.sbmu.ac.ir/be

دسترسی آزاد مقاله پژوهشی

مجله اخلاق زیستی

دوره پانزدهم، ۱۴۰۴

چالش‌های حفاظت از داده‌های سلامت بیماران در درمان‌های هوشمند

تهمینه اسفندیاری[۱]، حمید روستایی صدرآبادی[۲*]، نصراله جعفری خسروآبادی[۳]، سیداحمد میرخلیلی[۴]

۱. گروه حقوق، دانشکده الهیات و معارف اسلامی، دانشگاه میبد، میبد، ایران.

۲. گروه فقه و حقوق اسلامی، دانشکده الهیات و معارف اسلامی، دانشگاه میبد، میبد، ایران.

۳. گروه حقوق، دانشکده الهیات و معارف اسلامی، دانشگاه میبد، میبد، ایران.

۴. گروه فقه و حقوق اسلامی، دانشکده الهیات و معارف اسلامی، دانشگاه میبد، میبد، ایران.

چکیده

زمینه و هدف: پردازش داده‌های اشخاص توسط هوش مصنوعی در حوزه سلامت ارتباط تنگاتنگی با لزوم حفظ حریم خصوصی آنان دارد. بر همین اساس، هدف مقاله حاضر، بررسی چالش‌های اخلاقی مانند رضایت آگاهانه، نابرابری و تبعیض و عدم شفافیت و توضیح‌پذیری از یک سو و چالش‌های حقوقی مانند شخصیت حقوقیِ ربات‌های درمانگر، دسترسی غیرمجاز و نقض محرمانگی داده‌های بیماران و استفاده ثانویه از داده‌ها، از سوی دیگر، در حوزه حفاظت از داده‌های سلامت شخصی بیماران است.

روش: این مقاله به روش توصیفی ـ تحلیلی و با استفاده از منابع کتابخانه‌ای به بررسی چالش‌های اخلاقی و حقوقیِ حفاظت از داده‌های سلامت بیماران در درمان‌های هوشمند پرداخته است.

ملاحظات اخلاقی: در تمام مراحل نگارش پژوهش حاضر، اصالت متون، صداقت و امانتداری رعایت شده است.

یافته‌ها: حفاظت از داده‌های سلامت بیماران امری ضروری در حوزه درمان هوشمند است. بر این اساس، اتحادیه اروپا نخستین تلاش‌ها را در تصویب قوانین حمایتی در قالب مقررات حفاظت از داده‌ها در سال ۲۰۱۶ م. به عمل آورده است. اما در حقوق ایران، به مسأله حفاظت از داده‌ها به صورت ویژه پرداخته نشده است و به نظر می‌رسد، تصویب هرچه زودتر مقررات حفاظت از داده‌ها به‌خصوص داده‌های سلامت‌محور، امری ضروری است.

نتیجه‌گیری: از آنجا که هوش مصنوعی در قلمروهای مختلف مانند دانش حقوق و پزشکی، پدیده‌ای نوظهور است، لذا کشورهای مختلف در تلاش تصویب مقررات مرتبط هستند. پیچیدگی، فنی و تخصصی بودنِ هوش مصنوعی چالش‌های متعدد اخلاقی و حقوقی مانند مسأاله امکان شناسایی شخصیت حقوقی مستقل برای ربات‌های درمانگر، نقض احتمالیِ داده‌های سلامت بیماران توسط مراکز درمانی و استفاده از داده‌های تبعیض‌آمیز درمان بیماران را ایجاد کرده است که تا قبل از آن چنین موضوعاتی در دانش حقوق مطرح نشده بود.

واژگان کلیدی: حریم خصوصی، ربات درمانگر، حفاظت از داده‌ها، حقوق پزشکی

نویسنده مسئول: حمید روستایی صدرآبادی؛ **پست الکترونیک:** rostaei@meybod.ac.ir

تاریخ دریافت: ۱۴۰۴/۰۱/۲۷؛ **تاریخ پذیرش:** ۱۴۰۴/۰۵/۰۴؛ **تاریخ انتشار:** ۱۴۰۴/۱۰/۰۷

خواهشمند است این مقاله به روش زیر مورد استناد قرار گیرد:

Esfandiary T, Rostaei Sadrabadi H, Jafari khosroabadi N, Mirkhalili SA. Challenges of Protecting Patient Health Data in Smart Healthcare. Akhlaq-i zisti, i.e., Bioethics Journal. 2025; 15: e26.

مقدمه

پیشرفت‌های دانش بشری در قلمروی علوم پزشکی و فناوری هوش مصنوعی، کشورهای مختلف را بر آن داشته است تا با توجه به نیازهای بشر در حوزه سلامت، به دنبال هوشمندسازی آن باشند و ازاین‌رو، سرمایه‌گذاری‌های زیادی جهت توسعه این فناوری در حوزه پزشکی صورت گرفته است. این رویکرد، در تشخیص و درمان بیماری‌های مختلف تأثیر به سزایی گذاشته است. نظام درمان هوشمند به مراقبت‌های پزشکی اشاره دارد که از هوش مصنوعی برای بررسی داده‌های سلامت محور و کمک به فرآیند درمان استفاده می‌کند. بر همین اساس است که تعریف هوش مصنوعی نیز داده محور است؛ به نحوی که در بند ۱۲ قانون هوش مصنوعی اتحادیه اروپا (۲۰۲۴) از هوش مصنوعی به سیستم‌هایی تعبیر شده است که از داده‌ها یاد می‌گیرند که چگونه با برخورداری از درجه‌ای از استقلال به اهداف معین دست یابند و نسبت به تصمیم‌گیری و عمل اقدام کنند. بنابراین، می‌توان گفت که هوش مصنوعی با این پیش‌فرض ایجاد شده است که هوش انسانی را می‌توان توسط یک ماشین شبیه‌سازی نمود.

سازوکار درمان هوشمند، جلوه‌های متعددی دارد مانند: تشخیص بیماری، برنامه‌ریزی درمان، پرونده سلامت هوشمند چت ربات‌ها و دستیاران پزشکی مجازی. هوش مصنوعی در مراقبت‌های پزشکی به کمک در مراقبت‌های بالینی یا تصمیم‌گیری محدود نمی‌شود و با شناسایی خودکار شباهت‌ها در سوابق پزشکی بیماران، می‌تواند در شناسایی سریع بیماری‌ها و درمان آن‌ها به پزشکان کمک نماید. برای نمونه فناوری پزشکی واتسون که با عنوان «سلامت واتسون» شناخته می‌شود حجم زیادی از اطلاعات سلامت بیماران را برای ارائه توصیه‌های پزشکی جهت درمان سرطان، ابتدا استخراج و تجزیه و تحلیل نموده و سپس برنامه درمانی منحصر به فردی برای بیمار ارائه می‌دهد (۱). سیاست‌گذاران کشور ایران نیز اهمیت موضوع پزشکی هوشمند را دریافته‌اند و بر همین اساس در ماده ۶۹ قانون برنامه پنج ساله هفتم پیشرفت جمهوری اسلامی ایران (۱۴۰۳-۱۴۰۷)، برای وزارت بهداشت، درمان و آموزش پزشکی تکالیفی را در راستای ایجاد نظام هوشمند سلامت و مدیریت اطلاعات آن پیش‌بینی کرده است.

اگرچه به‌کارگیری هوش مصنوعی در حوزه‌های مختلف ازجمله حقوق سلامت منجر به تحولات گسترده‌ای شده است، اما کاربرد آن با چالش‌های گوناگونی همراه است که استفاده از آن را نیازمند سیاست‌گذاری دقیق و تصویب قوانین و آیین‌نامه‌های فنی به ویژه در زمینه حفاظت از داده‌های شخصی می‌نماید. داده‌های شخصی عبارتست از هرگونه اطلاعات مستقیم یا غیرمستقیم دربارهٔ یک شخص حقیقی با هویت مشخص یا قابل شناسایی که از طریق ارجاع به یک شمارهٔ شناسایی یا یک یا چند عنصر که ویژهٔ آن شخص است (مانند هویت جسمی، ژنتیکی، اقتصادی) صورت می‌گیرد (۲). این موضوع در لایحهٔ حفاظت از داده‌های شخصی ۱۴۰۳ نیز اشاره شده است. همچنین اطلاعات سلامت شخص موضوع داده در دسته داده‌های شخصی حساس قرارداده شده است. یکی از مهم‌ترین چالش‌های به‌کارگیری هوش مصنوعی در حوزه سلامت، موضوعِ حفاظت از داده‌های سلامت شخصی بیماران در درمان‌های هوشمند است. لازم به ذکر است که داده‌های سلامتِ شخصی بیماران شامل طیف گسترده‌ای از اطلاعات مربوط به سلامت جسمی یا روانی یک فرد مانند داده‌های ژنتیکی، آزمایشگاهی، درمان‌های روانپزشکی و ... می‌شود (۳).

ازجمله مهمترین قوانین بین‌المللی در زمینه حمایت از داده‌ها و حریم خصوصی اشخاص، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا General Data Protection Regulation (GDPR) است که در سال ۲۰۱۶ تصویب و از سال ۲۰۱۸ میلادی لازم‌الاجرا شده است. قانون پیش‌گفته، داده‌های راجع به سلامت اشخاص را در دستهٔ حساس قرار داده است و جهت پیشگیری از افشا، جمع‌آوری و پردازشِ غیر مجاز، آن‌ها را تحت پروتکل‌های امنیتی قرار داده و رعایت اصولی مانند شفافیت، امنیت و رضایت کاربران را ضروری اعلام کرده است.

در قانون هوش مصنوعی اتحادیه اروپا مصوب ۲۰۲۴ م. نیز بر حفظ و تضمین حریم خصوصی و حفاظت از داده‌های شخصی در کل چرخه حیات سیستم هوش مصنوعی تأکید شده است (مواد ۲۷ و ۶۴).

باید در نظر داشت که اگرچه استفاده از هوش مصنوعی در پزشکی مزایای بسیاری مانندِ تسهیل و تسریع روند درمان، ذخیره‌سازی سوابق بیماران، برنامه‌ریزی درمان و پزشکیِ شخصی‌سازی شده دارد، اما هنگامی که فناوری هوش مصنوعی در ارائه خدمات پزشکی، مورد استفاده قرار می‌گیرد، برای تجزیه و تحلیل حجم وسیعی از داده‌های مربوط به سلامت بیمار و کمک به تشخیص و درمان وی، اقدام به جمع‌آوری و ذخیره‌سازی داده‌های شخصی، ازجمله سوابق پزشکی، اطلاعات ژنتیکی و ... می‌نماید (۴). استفاده گسترده از چنین داده‌هایی برای تجزیه و تحلیل توسط هوش مصنوعی، خطرات ذاتی را برای حریم خصوصی بیماران و داده‌های شخصی آنان در زمینه‌های جمع‌آوری اطلاعات، پردازش و انتشار آن ایجاد می‌نماید. ازاین‌رو، ضروری است که چالش‌های پیش روی ارائه‌دهندگان مراقبت‌های پزشکی با نگاهی گذرا به چارچوب قانونی حاکم بر استفاده از داده‌های سلامت شخصی هوشمند بررسی شود. بدین‌سان، در این جستار، چالش‌های حفاظت از داده‌های سلامت شخصیِ بیماران در درمان‌های هوشمند در دو بخش اخلاقی و حقوقی واکاوی می‌شود.

روش

این مقاله به روش توصیفی ـ تحلیلی و با استفاده از منابع کتابخانه‌ای به بررسی چالش‌های اخلاقی و حقوقیِ حفاظت از داده‌های سلامت بیماران در درمان‌های هوشمند پرداخته است.

یافته‌ها

حفاظت از داده‌های سلامت بیماران امری ضروری در حوزه درمان هوشمند است. بر این اساس، اتحادیه اروپا نخستین تلاش‌ها را در تصویب قوانین حمایتی در قالب مقررات حفاظت از داده‌ها در سال ۲۰۱۶ م. به عمل آورده است. اما در حقوق ایران، به مسأله حفاظت از داده‌ها به صورت ویژه پرداخته نشده است و به نظر می‌رسد، تصویب هرچه زودتر مقررات حفاظت از داده‌ها به‌خصوص داده‌های سلامت‌محور، امری ضروری است.

این تحقیق نشان داد که پرداختن به چالش‌های اخلاقی و حقوقی حفاظت از داده‌های سلامت در عصر درمان هوشمند، فراتر از یک الزام قانونی، یک ضرورت انسان‌محور برای حفظ کرامت و خودمختاری بیماران است. از منظر اخلاقی، هوش مصنوعی با ایجاد عدم تقارن اطلاعاتی بی‌سابقه، هسته اصلی اصل رضایت آگاهانه را به چالش می‌کشد. چگونه می‌توان از بیماری رضایت واقعاً آگاهانه گرفت، وقتی که نحوه پردازش داده‌هایش توسط یک الگوریتم «جعبه سیاه» حتی برای طراحان آن نیز به طور کامل قابل توضیح نیست؟ این کمبود شفافیت و توضیح‌پذیری نه تنها حق انتخاب بیمار را مخدوش می‌کند، بلکه مسئولیت اخلاقی پیامدهای تصمیمات اتوماتیک را در موارد خطا، به موضوعی غامض تبدیل می‌نماید.

از نگاه حقوقی، چالش‌ها ملموس‌تر و فوری‌تر هستند. نخست، مسئله شخصیت حقوقی عامل هوشمند مطرح است. در صورت وقوع خطای تشخیصی یا درمانی توسط یک ربات درمانگر یا سیستم توصیه‌گر بالینی، تکلیف مسئولیت مدنی و کیفری چیست؟ آیا می‌توان یک نرم‌افزار یا ربات را مقصر دانست، یا مسئولیت نهایتاً متوجه پزشک، بیمارستان، تولیدکننده یا طراح الگوریتم است؟ این خلأ حقوقی می‌تواند به بی‌مسئولیتی و عدم دسترسی بیمار به جبران خسارت مناسب منجر شود. دوم، تهدید نقض محرمانگی به شکل گسترده‌ای وجود دارد. تمرکز حجم عظیمی از داده‌های حساس سلامت در سامانه‌های دیجیتال، آنها را به هدفی جذاب برای حملات سایبری و نیز دسترسی غیرمجاز کارکنان داخلی تبدیل می‌کند. سوم، استفاده ثانویه از داده‌های جمع‌آوری‌شده برای اهداف تحقیقاتی یا تجاری، بدون رضایت صریح و ویژه

بیماران، نقض حریم خصوصی محسوب می‌شود و می‌تواند به تبعیض در قیمت‌گذاری بیمه یا استخدام بینجامد.

بحث

۱. چالش‌های اخلاقی

چالش‌های اخلاقی پیرامون حفاظت از داده‌های سلامت شخصیِ بیماران در درمان‌های هوشمند شامل رضایت آگاهانه، نابرابری و تبعیض، عدم شفافیت و توضیح‌پذیری می‌باشد که در ادامه بررسی خواهند شد.

۱-۱. رضایت آگاهانه: حمایت از استقلال و رضایت بیمار یک اصل اساسی در اخلاق پزشکی است که شامل حق پذیرش یا رد برخی از درمان‌ها و همچنین حق بیمار برای لغو تصمیم پیشین او می‌باشد. با توجه به این موضوع، لازم است که تمام اقدامات حرفه‌ای در زمینه پزشکی/ سلامت با رضایت آگاهانه قبلی بیمار باشد. به‌طور سنتی، رابطه پزشک و بیمار رو در رو است، اما هوش مصنوعی توسعه مراقبت‌های پزشکی را از طریق ربات‌ها یا چت بات‌ها (Chatbots) و همچنین از طریق سیستم‌های پزشکی از راه دور (telemedicine systems) امکان‌پذیر کرده است که توسعه آن با همه‌گیری کووید-۱۹ تسریع شده است.

بر این اساس، در سیستم درمان هوشمند از یک سو، جهت تجزیه و تحلیل و تصمیم‌گیری نیاز به دسترسی به داده‌های سلامت بیمار است، اما از سوی دیگر، احترام به حریم خصوصی بیمار مستلزم کسب رضایت آگاهانهٔ وی برای جمع‌آوری، ذخیره و استفاده از داده‌های سلامت وی است. رضایت آگاهانه مبتنی بر این اصل است که بیمار باید پیش از درمان، اطلاعات کافی دریافت کرده و در مورد اصول اولیه نحوه عملکرد هوش مصنوعی و هدف از پردازش اطلاعات، مطلع شود تا بتواند آگاهانه به ادامه درمان رضایت دهد (۵). در این راستا، اطلاعات لازم در مورد دامنه و چگونگی جمع‌آوری و استفاده از داده‌های بیمار و خطرات و مزایای بالقوه جمع‌آوری تحلیل داده‌های راجع به وی توسط هوش مصنوعی باید به‌طور صریح، روشن و دقیق در اختیار بیمار یا نماینده وی قرار گیرد تا موافقت یا مخالفت خویش را در این خصوص اعلام نمایند (۶).

برخی بر این باورند که در بیشتر موارد، عدم اطلاع بیمار درخصوص استفاده از داده‌های سلامت توسط هوش مصنوعی، نقضِ حقِ بر رضایت آگاهانه محسوب نمی‌شود و ممکن است توضیح در مورد جزییات فنی، بر تصمیم‌گیری بیمار اثر منفی بگذارد (۷). البته، این استدلال صحیح به نظر نمی‌رسد و باید قایل به تفکیک شد؛ بدین‌صورت که در مواردی که اطلاعات راجع به بیماری یا شرایط خاصی در بیمار است ـ مانند علایم بیماری ایدز ـ وی باید به‌طور واضح و شفاف در جریان امر قرار گرفته تا با اطلاعات کافی نسبت به آن رضایت داشته باشد، اما اگر داده‌های سلامت بیمار تنها یک عامل جزئی مانند میزان درجه بدن در حین عمل جراحی باشد، ارائه اطلاعات به‌طور جزیی در مورد آن ضروری به نظر نمی‌رسد.

مقررات عمومی حفاظت از داده‌های خصوصی اتحادیه اروپا که بر موضوع حمایت از داده‌های شخصی افراد تأکید دارد، در مواد ۶ و ۱۲ به ضرورت آگاهی بخشی ـ کمّی و کیفی ـ به دارنده اطلاعات و رضایت وی نسبت به این موضوع اشاره نموده است. همچنین، بر حق اجتناب شخصِ موضوع داده (بیمار) از قرار گرفتن در معرض تصمیم‌گیری‌های هوشمند تأکید شده است، مگر آنکه رضایت صریح داشته باشد و یا این پردازش در راستای منافع قانونی و مشروع باشد. قانون مذکور پردازشِ داده‌های شخصی راجع به سلامت و ژنتیک را ممنوع کرده است، مگر شخصِ موضوعِ داده، صریحاً با پردازش آن برای یک یا چند هدف مشخص موافقت کرده باشد (بند ۲ ماده ۹)، که بیانگر ضرورت وجود رضایت آگاهانه بیمار نسبت به پردازش داده‌های شخصی و سلامت وی توسط هوش مصنوعی است. درواقع، اطلاعات راجع به پردازش داده‌های شخصی، توسط هوش مصنوعی باید به‌طور شفاف و قابل فهم در اختیار بیمار قرار بگیرد. یکی از موضوعات مورد تأکید در قانون فوق، درخصوص پردازش اطلاعات مربوط به افراد زیر ۱۶ سال است که باید با رضایت ولی قانونی آن‌ها باشد و پردازشگرِ اطلاعات باید به شیوه قانونی از رضایت ولی قانونی فرد اطمینان یابد (بند ۱ ماده ۸)، که این امر درخصوص

پردازش داده‌های شخصی بیماران در فرایند درمان هوشمند نیز قابل اجرا است. قانون تجارت الکترونیک ایران نیز درخصوص حمایت از داده‌های شخصی افراد، ذخیره، پردازش و توزیع آن‌ها را مشروط به رضایت صریح شخص و رعایت اصولی نموده است (ماده ۵۸) و ذخیره و پردازش و توزیع داده پیام‌های شخصی در بستر مبادلات الکترونیکی را با لحاظ شرایطی ازجمله هدف مشخص، ضرورت و تناسب با اهداف تعیین شده، صحیح و مجاز می‌داند (ماده ۵۹).

۱-۲. نابرابری و تبعیض: برابری در مراقبت‌های پزشکی یک مفهوم چند وجهی است که شامل توزیع عادلانه منابع، فرصت‌ها و نتایج در میان بیماران مختلف است. سیستم‌های مراقبت پزشکی باید دسترسی به منابع سلامت شهروندان را بدون تبعیض فراهم کنند. هوش مصنوعی یک فناوری داده محور است. داده‌های تعریف شده برای هوش مصنوعی ـ مانند سن، جنس یا نژاد ـ در نظام سلامت یک کشور، می‌توانند منجر به برخی سوگیری‌ها در فرآیند درمان، جهت‌گیری در فرآیند پردازش اطلاعات بیمار و در نهایت منجر به توصیه‌های درمانی جانبدارانه شود (۸). هنگامی که این داده‌ها به یک مدل هوش مصنوعی داده می‌شود، مدل، این سوگیری‌ها را یاد می‌گیرد و بازتولید می‌کند.

تصمیمات تشخیصی و درمانیِ هوش مصنوعی براساس داده‌های اولیه‌ای که دریافت می‌کند، شکل می‌گیرد. این داده‌ها می‌تواند از منابع مختلفی مانند پرونده پزشکی و سوابق عمومی و بالینی افراد به دست بیایند. بدین‌سان، استفاده از اطلاعات شخصی بیماران به‌عنوان داده‌های ورودی ربات درمانی هوشمند ممکن است در ابتدا بی‌ضرر به نظر برسند، اما می‌توانند اطلاعات زیادی را در مورد زندگی بیمار ازجمله نژاد، جنسیت، بیماری و ... نشان دهند و اگر یک سیستم هوش مصنوعی مغرضانه یا تبعیض‌آمیز عمل کند، می‌تواند از این داده‌ها سوء استفاده نماید و در نهایت منجر به نتایج ناعادلانه یا حتی زیانبار برای بیماران شود. برای نمونه، وقتی الگوریتمی که برای تشخیص سرطان استفاده می‌شود، روی بیمارانی با نژاد یا رنگ پوست خاص پردازش شود، ممکن است نتواند به درستی سرطان را در بیماران دیگر ـ مثلاً اقلیت نژادی در آن کشور ـ تشخیص دهد (۹).

بنابراین، ضروری است که اطمینان حاصل شود که داده‌های سیستم‌های هوش مصنوعی به صورت متنوع بوده و بدون تبعیض شامل تمام بیماران (از هر نژاد، جنسیت و قومیتی با ویژگی‌های زیستی متفاوت) شود تا مانع از سوءگیری در درمان هوشمند شود. بدین‌سان، یکی از کاربردهای هوش مصنوعی در امور پزشکی، تشخیص صحیح‌تر و دقیق‌تر بیماری است. نشانه‌های بیمار به سیستم وارد می‌شود و سپس ربات درمانگر، داده واقعی را بررسی می‌کند و به کادر پزشکی تشخیص خود را پیشنهاد می‌دهد. ربات تجربه‌اش را از طریق آموزش به دست می‌آورد و یاد می‌گیرد که چگونه بین انواع نشانه‌ها تفکیک قائل شود و علائم غیر مهم را نیز نادیده بگیرد. دقیقاً در همین مرحله است که داده‌های تبعیض‌آمیز و دارای تعصباتِ جنسیتی، نژادی و ... می‌تواند ربات را نیز دچار اشتباه نماید، به نحوی که در بیماری مشابه، ممکن است تشخیص‌های مختلفی را ارائه نماید که گاه منجر به ضرر بیماران شود.

در نهایت، از آنجا که ضرورت عدم تبعیض بین بیماران باید همواره به‌عنوان یک حق مورد شناسایی قرار گیرد (حق بر عدم تبعیض)، برای تشخیص این امر که تصمیمات درمانی و تشخیصی ربات درمانگر در مواجه با بیماران مختلف، تبعیض‌آمیز است یا خیر از معیار مشروعیت هدف و ضرورت داشتن می‌توان بهره جست. منظور از مشروعیت هدف هوش مصنوعی در حوزه پزشکی این است که تصمیم‌گیری نهایی آن منتج به هدفی با قابلیت ارائه به بیمار باشد. بنابراین، برای مثال اگر هوش مصنوعی در زمینه شناسایی درمان‌های جدید سرطان خون به کار گرفته شود، یک هدف مشروع در حوزه پزشکی تلقی می‌گردد. معیار ضرورت تشخیص نیز به چگونگی تصمیم‌گیریِ لحظه‌ای هوش مصنوعی در مواجه با بیمارانِ دارای علایم و شرایط یکسان اشاره دارد که اگر ربات درمانگر، رفتار مشابهی نشان ندهد نشانگر تبعیض‌آمیز بودن عملکرد آن است. برای نمونه، ممکن است هنگام جراحی با ربات هوشمند،

خونریزی در بدن بیمار اتفاق بیفتد، حال اگر عملکرد و تصمیم‌گیری ربات با توجه به سفید یا سیاه‌پوست بودن بیمار، متفاوت باشد، نشان‌دهنده وجود تبعیض در روند درمان توسط ربات است (۱۰).

۳-۱. عدم شفافیت و توضیح‌پذیری: در حوزه‌های خاصی مانند مراقبت‌های پزشکی و درمانی، شفافیت اهمیت دوچندانی دارد، زیرا به‌طور مستقیم با سلامت شهروندان در ارتباط است. بر این اساس، اگرچه ورود هوش مصنوعی به حوزه پزشکی، چشم‌اندازهای جدیدی را در پیشگیری، درمان و بهینه‌سازی منابع پزشکی باز نموده است، اما تفسیر برخی از الگوریتم‌های هوش مصنوعی به دلیل پیچیدگی و چندوجهی بودنِ آن‌ها، دشوار است (۱۱). لازم به ذکر است که در سیستم‌های مبتنی بر هوش مصنوعی دو روش متمایز برای دسته‌بندی الگوریتم‌ها و مدل‌ها مطرح است: قابل تفسیر (جعبه سفید) و غیرقابل تفسیر (جعبه سیاه). این تمایز براساس وضوح رابطه بین داده‌های ورودی و خروجی و نتایج تولید شده توسط مدل است. مدل‌های سفید دارای ویژگی‌های قابل تشخیص و قابل فهمی هستند که به‌طور شفاف و قابل درک به توضیح تأثیر متغیرها در پیش‌بینی نتایج کمک می‌کنند.

در هر حال، فقدان شفافیت، نگرانی‌های مربوط به حریم خصوصی را افزایش می‌دهد، زیرا ممکن است بیمار توانایی درک اینکه چه عواملی بر عملکرد هوش مصنوعی تأثیر می‌گذارد و یا از داده‌های شخصی و یا راجع به سلامتی آنان چگونه استفاده می‌شود، نداشته باشد. فقدان توضیح‌پذیری می‌تواند اعتماد را از بین ببرد و مانع از تصمیم‌گیری آگاهانه در مورد مراقبت‌های پزشکی هوشمند شود.

بنابراین، آگاهی شخص موضوع اطلاعات (بیمار) از کیفیت و کمیّت داده‌های شخصی و سلامت‌مدار، دسترسی هوش مصنوعی به آن‌ها، هدف پردازش اطلاعات و نحوه استفاده از آن‌ها جهت شفافیت ضروری است؛ زیرا صرفاً یک شخص آگاه می‌تواند نسبت به چگونگیِ پردازش داده‌های شخصی خود، کنترل داشته باشد و به‌طور مؤثر حقوق خود را در این خصوص اِعمال کند. به این موضوع در مواد ۱۲ تا ۱۵ قانون حفاظت از داده‌های عمومی اتحادیه اروپا نیز توجه شده و نسبت به ارائه اطلاعات به شخص موضوع داده به صورت شفاف با استفاده از زبان قابل فهم، تأکید شده است (۱۲). به‌طورکلی، شفافیت در نظام سلامت هوشمند باید به‌عنوان یک فرآیند پیوسته و به‌عنوان یک اصل قانونی در نظر گرفته شود و شامل معیارهای مختلفی مانند توضیح‌پذیری و تفسیرپذیری، نگهداری سوابق و مستندسازی باشد.

بنابراین، باید به بیمار اطلاعاتی که جهت اطمینان وی از پردازش منصفانه و شفاف داده‌ها ضروری است، ارائه گردد. یک سازوکار پزشکی مبتنی بر هوش مصنوعی در صورتی به اندازه کافی شفاف تلقی می‌شود که امکان توضیح‌پذیری متعارف در مورد چگونگی پردازش و استفاده از داده‌های بیماران را برای آنان فراهم نماید (۱۳). از آنجا که فناوری هوش مصنوعی پیچیدگی‌های خاصی دارد، ضروری است که شفاف‌سازی درخصوص چگونگی استفاده از داده‌ها متناسب با سطح درک بیماران و به‌طور قابل فهم ـ در قالب فیلم‌ها و یا تصاویر همراه با متن به زبان ساده ـ انجام شود. همچنین، لازم است تا با پیش‌بینی نهادهای قانونی، زمینه‌های عدم شفافیت و به تبع آن، نقض حریم خصوصی بیماران شناسایی شود تا ضمن پیشگیری از وقوع آن، دستورالعمل‌های فنی مناسب به لحاظ تضمین حفاظت از داده‌ها شخصی، در روند درمان هوشمند تهیه شود.

یکی از مناسب‌ترین اقدامات در راستای مبارزه با عدم شفافیت، ایجاد حق دسترسی به اطلاعات پردازش شده برای بیمار است که در ماده ۱۵ قانون حفاظت از داده‌های عمومی اتحادیه اروپا پیش‌بینی شده است و به فرد، حق دریافت یک نسخه از داده‌های شخصی و سایر اطلاعات تکمیلی را می‌دهد. حق دسترسی در ماده ۵۹ قانون تجارات الکترونیک نیز مورد توجه قرار گرفته است. این امر به اشخاص موضوع داده (بیماران) این امکان را می‌دهد که درخصوص چگونگی پردازش داده‌های سلامت آنان و قانونی بودن این روند اطلاعات لازم را کسب نمایند.

۲.چالش‌های حقوقی

درخصوص چالش‌های حقوقی حفاظت از داده‌های سلامت شخصیِ بیماران در درمان‌های هوشمند بررسی موضوعاتی مانند امکان شناسایی شخصیت حقوقی ربات جهت مسئولیتِ نقض داده‌ها، دسترسی غیر مجاز و نقض محرمانگی داده‌های بیماران و استفاده ثانویه از داده‌ها ضروری می‌باشد.

۲-۱. امکان شناسایی شخصیت حقوقی ربات جهت مسئولیتِ نقض داده‌ها: فناوری هوش مصنوعی چالش‌های حقوقی متعددی را در حوزه شناسایی مسئولیت برای جبران خساراتِ مالی و معنوی ناشی از نقض حریم خصوصی بیماران در حوزه سلامت هوشمند ایجاد نموده است. اینکه آیا هوش مصنوعی می‌تواند به تنهایی حریم خصوصی بیماران را نقض نماید از یک‌سو و از سوی دیگر، چالش اساسیِ امکان شناسایی شخصیت حقوقی برای هوش مصنوعی برای احراز مسئولیت آن، از سوی دیگر به چالش حقوقیِ مهمی در این حوزه تبدیل شده است. البته باید در نظر داشت که جهت شناسایی اشخاص مسئول در روند درمان هوشمند، چالش‌های جدی وجود دارد؛ زیرا در این فرآیند تحلیل الگوریتم‌ها و فرآیندهای دخیل در عملکرد هوش مصنوعی دشوار است و فرآیندی که برای رسیدن به نتیجه طی می‌کند به راحتی قابل تشخیص نیست و گاه این امر می‌تواند رابطه سببیت بین ضرر و عملکرد پزشک، تولیدکننده و یا سایر متصدیان را از بین ببرد. برای نمونه، در فرضی که سازنده و پزشک کلیه اقدامات لازم برای حفظ امنیت داده‌های بیمار را پیش‌بینی نموده‌اند، اما ربات درمانگر با اقدامی غیرقابل پیش‌بینی موجبات نقض حریم خصوصی بیمار و افشای داده‌های راجع به وی را فراهم آورد، بیمار باید برای جبران خسارات خویش به چه کسی مراجعه نماید؟ با توجه به پیشرفت‌های روزافزون هوش مصنوعی به سوی خودمختاری و استقلال کامل، آیا می‌توان همچنان، بر این نظر بود که در فرض عدم انتساب مسئولیتِ نقض حریم خصوصی بیمار به سازنده و طراح و پزشک (کاربر)؛ امکان مراجعه به خود هوش مصنوعی نیز وجود ندارد و خسارات بیمار باید بدون جبران باقی بماند! فرضیه‌های مختلفی درخصوص مسئول نهایی جبران خسارات ناشی از اقدامات ربات هوشمند پزشکی متصور است.

در این راستا، برخی معتقدند که باید شخصیت هوش مصنوعی را در قالب شخصیت انسان تحلیل نمود (۱۴)، اما باید در نظر داشت که اگرچه سعی بر آن شده تا عملکرد هوش مصنوعی مبتنی بر الگوریتم‌های مشابه تفکر و منطق انسان طراحی شود، اما ماهیت آن با تغییر در الگوها و الگوریتم‌های سازنده‌اش قابل تغییر است. حال آنکه ماهیت ذات انسان حتی با تغییر در الگوهای ژنتیکی باز هم قابل تغییر و دگرگونی نیست. به همین دلیل برخی سعی نموده‌اند هوش مصنوعی را نماینده‌ای تلقی نمایند که تحت دستور کاربر یا سازنده‌اش عمل می‌نماید. ازاین‌رو، به‌طور دقیق نمی‌توان ربات را مسئول دانست، زیرا در بیشتر نظام‌های حقوقی برای اجرای نمایندگی، وجود اهلیت قانونی و شروطی مانند قصد و رضا نیاز است که تصور آن برای ربات هوشمند کمی دور از منطق است (۱۵).

برخی نیز بر این باورند که باید ماهیت آن را در قالب‌های ابزاری تحت کنترل انسان و به‌عنوان شیء تلقی نمود، زیرا هوش مصنوعی عنصری از یک سیستم فناوری اطلاعات است که توسط انسان برای انجام وظایف خاص ایجاد می‌شود و در نهایت توسط انسان، برنامه‌نویسی شده است (۱۶). بنابراین، در صورت نقض حریم خصوصی بیمار، انتساب مطلق مسئولیت به هوش مصنوعی و معاف نمودن سایر اشخاص اعم از شرکت سازنده ربات، پزشک و بیمارستان از مسئولیت احتمالی منطقی نیست و موجب می‌شود تا آن‌ها از هوش مصنوعی به‌عنوان سپری برای محافظت از خویش در برابر قانون، بهره ببرند. ازاین‌رو، در نظر گرفتن مسئولیت برای سازنده و کاربر ربات هوشمند پزشکی سبب بازدارندگی است و خطر آسیب‌های ناشی از عملکرد این نوع ابزار هوشمند را کاهش می‌دهد.

در نهایت، به نظر می‌رسد که با وجود تلاش‌های گسترده برای تولید ربات‌های خود مختار و اعطای شخصیت حقوقی به آن ـ برای نمونه کشور عربستان در سال ۲۰۱۷ به ربات انسان‌نمای سوفیا تابعیت اعطا نمود ـ باید راه میانه را برگزید و اندکی از این فرضیه که هوش مصنوعی صرفاً یک ابزار در دست انسان

است، فاصله گرفت. زیرا این دیدگاه نتیجه عدم امکان پیش‌بینی نحوه عملکرد هوش مصنوعی در آینده است و سرعت گسترش فناوری هوش مصنوعی پزشکی، نیازمند تحلیل دقیق امکان اعطای ظرفیت قانونی شخصیت حقوقی به آن در آینده است.

بنابراین، باید تدبیری اندیشید تا با همان منطق که به شرکت‌ها شخصیت حقوقی داده شده و دارای اموال و حقوق و تعهدات هستند، برای هوش مصنوعی نیز شخصیت حقوقی مستقل لحاظ شود تا در زمانی که اقدامات خودسرانه و پیش‌بینی‌ناپذیر آن منجر به نقض حریم خصوصی بیمار شود با اجباری نمودن ثبت هوش مصنوعی درمانگر، پیش‌بینی دارایی و سرمایه و بیمه نمودن آن، خسارات وارده به بیمار جبران شود. البته باید در نظر داشت که در نظر گرفتن شخصیت حقوقی و مسئولیت برای ربات پزشکی نیازمند قانونگذاری و ایجاد نظام حقوقی با زیر ساخت‌های امنیتیِ مناسب است.

در سال‌های اخیر، تلاش‌هایی در راستای تحقق نظریه اعطای شخصیت حقوقی به هوش مصنوعی شده است و طرفداران این نظریه بر این باورند که با توجه به اینکه ربات‌های درمانگر مستقل تصمیم می‌گیرند، لذا به سطحی از خود مختاری رسیده‌اند که بتوانند با درک محیط اطراف و تحلیل داده‌ها، تصمیم لازم و مناسب را جهت درمان اتخاذ نمایند و درواقع، ربات درمانگر را باید به مثابه یک شخصیت حقوقی مانند شرکت‌ها، با حقوق و وظایف خاص خود و به‌طور مستقل از سازنده و پزشک (کاربر) تلقی نمود (۱۷). در جهت تقویت این نظر می‌توان به بند م ماده ۲ و بند ب ماده ۱۸ قانون تجارت الکترونیکی ایران اشاره نمود که سیستم رایانه‌ای را دارای شخصیت حقوقی دانسته است. لازم به ذکر است که پارلمان اروپا نیز شخصیت حقوقی برای هوش مصنوعی را ـ در مواردی که مستقلاً عمل می‌نمایند و یا به‌بطور مستقل با محیط اطراف تعامل دارند ـ در قالب شخص الکترونیک (Electronic person) به رسمیت شناخته است و برای جبران خسارات ناشی از اقدامات زیان بارِ ربات‌های هوشمند، طرح بیمه اجباری و صندوق جبران خسارت را پیش‌بینی نموده است (۱۸).

۲-۲. دسترسی غیر مجاز و نقض محرمانگی داده‌های بیماران: یکی از جنبه‌های حیاتی هوش مصنوعی حفاظت از حریم خصوصی (اطلاعات بیمار) است. ضرورت حفاظت به این دلیل است که هوش مصنوعی اساساً به داده‌های بزرگ برای گسترش و استقرار آن وابسته است. بنابراین، استفاده از سازوکارهایی که نقض اطلاعات و همچنین محرمانه بودن آن‌ها را تضمین می‌کند، بسیار مهم است، زیرا هوش مصنوعی داده‌های ارائه شده توسط بیماران و افراد را یاد می‌گیرد و از آن‌ها استفاده می‌کند. این فرآیند، در نهایت ناشناس‌سازی اطلاعات مربوط به بیماران را قبل از تجزیه و تحلیل داده‌ها توسط هوش مصنوعی حیاتی می‌نماید. اگرچه در حال حاضر چند قانون برای محافظت از حریم خصوصی افراد وجود دارد، مانند قانون انتقال پاسخگویی بیمه درمانی (HIPAA) ۱۹۹۶ در ایالات متحده آمریکا و مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR)، که البته به صورت خاص به حمایت از داده‌های بیماران در حوزه سلامت هوشمند اشاره‌ای ندارند. چالش مورد اشاره مربوط به اجرای سازوکارهایی خواهد بود که عدم شناسایی فرد را برای جمع‌آوری داده‌های پزشکی تضمین کند. درنتیجه وجود یک سامانه بین‌المللیِ نظارتی بر داده‌های بیماران ـ فارغ از هرگونه تبعیض ـ امری ضروری می‌باشد.

بر همین اساس، مجمع جهانی اقتصاد در سوئیس در سال ۲۰۲۳ م.، بخش خدمات پزشکی را با ۱۰.۹۳ میلیون دلار به‌عنوان پرهزینه‌ترین حوزه ناشی از نقض داده‌ها گزارش کرد (۱۹). هرچند تلاش‌هایی برای مقابله با آن در ایالات متحده (با تصویب قانون امنیت سایبری و زیرساخت ۲۰۱۸ م) و اتحادیه اروپا (دستورالعمل اتحادیه اروپا ۸۸/۲۰۱۹) برای ارتقای ایمنی داده‌ها انجام شده است. امروزه تردیدی در شناسایی اطلاعاتِ پزشکی (اگر دارای ارزش اقتصادی باشد) به‌عنوان مال وجود ندارد. بنابراین، پایگاه اطلاعاتی مربوط بیماران برای صاحبان آن جزو اسرار تجاری محسوب می‌شود و دستیابی به آن‌ها توسط افراد غیرصالح ممکن است منجر به نقض حریم خصوصی بیماران شود. برای نمونه، تولیدکنندگان محصولات و ارائه‌دهندگان خدمات پزشکی با کمک این

اطلاعات، جامعه هدف خود را به راحتی شناسایی نموده و مستقیم با آنان در ارتباط قرار می‌گیرند (۲۰).

مقصود از نقض محرمانگی داده‌های بیماران دستیابی افراد غیرمجاز به داده‌ها، در اختیار قرار دادن این اطلاعات برای دیگران و نهایتاً افشای آن‌ها می‌باشد. به‌طورکلی، جمع‌آوری و ذخیره‌سازی گسترده داده‌های سلامت شخصی بیماران، خطر دسترسی غیرمجاز و نقض داده‌ها را افزایش می‌دهد. این سیستم‌ها بیشتر بر تجمیع داده‌ها تکیه می‌کنند و اطلاعات را از منابع مختلف جمع‌آوری می‌نمایند (۲۱). برای نمونه، در مواردی که یک بیمار تحت درمان هوشمند قرار می‌گیرد، ربات درمانگر بیمارستان الف با ربات‌های سایر مراکز درمانی داده و اطلاعات را تبادل می‌نماید تا بهترین شیوه درمان را برای بیمار برگزیند و همین موضوع، فرآیند خطر نقض داده‌ها را افزایش می‌دهد، زیرا نقاط ورود بیشتری برای مهاجمان بالقوه ایجاد می‌شود.

همچنین، با توجه به ذخیره اطلاعات شخصی و سلامت بیماران در سیستم هوشمند درمان، مرتکبان سایبری ممکن است آن‌ها را برای دسترسی به اطلاعات بیمار هدف قرار دهند که منجر به سرقت هویت، کلاهبرداری یا سایر اشکال سوء استفاده شود. در حوزه نقض داده‌های پزشکی هوشمند، اقداماتی مانندِ فیشینگ ـ در این روش مجرمان سایبری با ایجاد لینک‌های جعلی به روش‌های مختلف بزه‌دیده را به وب‌سایت مورد نظر هدایت نموده و سپس اقدام به ربودن اطلاعات حساس آنان می‌نمایند ـ و دسترسی غیرمجاز رایج هستند و می‌توانند نه‌تنها حریم خصوصی بیمار، بلکه یکپارچگی سیستم‌های مراقبت‌های پزشکی را نیز به خطر بیندازند (۲۲). همچنین، از آنجا که حفظ محرمانگی اطلاعات سلامت شهروندان هر جامعه اهمیت به‌سزایی دارد؛ دسترسی اشخاص غیرمجاز و نقض محرمانگی داده‌های بیماران حتی ممکن است تهدیدی برای امنیت روانی یک کشور تلقی شود. در همین راستا، تبصره ۱ ماده ۳ قانون جرایم رایانه‌ای داده‌های سری را داده‌هایی می‌داند که افشای آن به امنیت کشور یا منافع ملی لطمه وارد کند. ازاین‌رو، داده‌های پزشکی هوشمندِ بیماران جزو این گروه است که ناقضان آن تحت شمول مواد ۳ و ۴ این قانون قرار می‌دهد.

مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا نیز الزامات سختگیرانه‌ای را در مورد نحوه نگهداری، ذخیره و محافظت از داده‌های شخصی (از جمله داده‌های مرتبط با سلامت) اِعمال می‌کند که شامل اقداماتی مانند مستعارسازی ـ طبق ماده ۴ مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا حالتی است که داده‌های شخصی بدون استفاده از سایر اطلاعات قابلیت نسبت داده شدن به فرد خاص و مشخصی را نداشته باشد. این اطلاعات به صورت جداگانه نگهداری و ذخیره می‌شود و تحت ارزیابی قرار می‌گیرند تا اطمینان حاصل شود که داده‌های شخصی به شخص حقیقی قابل شناسایی نسبت داده نشده باشد ـ و رمزنگاری داده‌های شخصی و ارزیابی منظم معیارهای فنی و سازمانی برای تضمین امنیت پردازش است (ماده ۳۲). برای نمونه در سال ۲۰۲۱ م. نقض گسترده اطلاعات در مورد حدود پانصد هزار بیمار توسط شرکت دِدالوس بیولوژی (Dedalus Biologie) در کشور فرانسه صورت گرفت. بر این اساس، مشخصات شخصی، شماره تأمین اجتماعی، نام پزشک تجویزکننده، تاریخ معاینه و همه اطلاعات پزشکی (اچ‌آی‌وی، سرطان‌ها، بیماری‌های ژنتیکی، بارداری، درمان دارویی یا داده‌های ژنتیکی) بیماران در فضای مجازی منتشر شد. براساس یافته‌های کلیدی سازمان‌های نظارتی در این حوزه مشخص شد که این شرکت، داده‌های سلامتِ بیماران را به برخی آزمایشگاه‌های تجزیه و تحلیل امور پزشکی می‌فروشد و بر این اساس، چند تخلف شناسایی شد. عدم رمزگذاری داده‌های شخصی ذخیره شده در سرور، عدم حذف خودکار داده‌ها پس از انتقال به نرم‌افزار دیگر، عدم احراز هویت کاربری که به داده‌ها دسترسی داشته است، استفاده از حساب‌های کاربری مشترک توسط چندین کارمند در قسمت خصوصی سرور، عدم نظارت و توجه به گزارش هشدارهای امنیتی بر روی سرور اطلاعات بیماران؛ این موارد در مجموع منجر به نقض داده‌های پزشکی بیماران بسیار زیادی شد و در نهایت، شرکت فوق نیز با استناد به مواد ۲۸، ۲۹ و ۳۲

براساس مقررات عمومی حفاظت از داده‌های اتحادیه اروپا مصوب ۲۰۱۶ م. به جزای نقدی به مبلغ ۱.۵ میلیون یورو محکوم شد (۲۳).

همچنین این رویه در کشور آمریکا نیز درخصوص دو نرم‌افزار هوشمند درمانگر به نام‌های Betterhelp و Cerebral قابل مشاهده است که از سوی کمیسیون تجارت فدرال آمریکا به اتهام اشتراک‌گذاری و افشای اطلاعات داده‌های شخصی بیمارانی که از این نرم‌افزارهای درمانگر استفاده می‌نمودند در فیس‌بوک، گوگل و سایر سکوهای برخط محکوم شدند (۲۴). البته به نظر می‌رسد، باید در این خصوص تدابیری اتخاذ شود تا بین نوع اطلاعات بیماری و شیوه‌های امنیتی حفاظت از آن تناسب لازم بر قرار شود. بنابراین، روش‌های امنیتی در مورد داده‌های فرد مبتلا به آبله مرغان، درخصوص اطلاعات افراد مبتلا به ایدز که برای بیماران از حساسیت بیشتری برخوردار است باید متفاوت باشد و با روش‌هایی مانند کدگذاری و ... از اطلاعات این دسته از بیماران حفاظت شود.

لازم به ذکر است که بیمار حق دارد در صورت هک یا افشای اطلاعاتش فوری از این موضوع مطلع شود. یکی از حمایت‌های قانونی درخصوص حمایت از موضوع داده، حق پاک‌سازی اطلاعات است (ماده ۱۷) که به کاربر اجازه می‌دهد تا به صورت شفاهی یا کتبی و حتی بدون هیچ دلیل خاصی خواستار حذف داده‌هایش از پایگاه داده‌ها شود که نقش مؤثری در حمایت از بیماران در برابر نقض داده‌های پزشکی آنان دارد.

۲-۳. استفاده ثانویه از داده‌ها: یکی از شیوه‌های نقض حریم خصوص بیماران، تغییر کاربری و استفاده ثانویه از داده‌های شخصی آنان است. بدین‌معنی که داده‌های بیمار که در ابتدا برای هدف خاصی (معمولاً درمان) با رضایت وی جمع‌آوری شده است، برای هدف دیگری استفاده شود. برای نمونه می‌توان یک مرکز درمانی را تصور کرد که از داده‌های سلامت شخصی بیمار که جهت ذخیره و تجزیه و تحلیل توسط ربات هوشمند پزشکی برای یک عمل جراحی جمع‌آوری شده است؛ به‌عنوان بخشی از یک مطالعه تحقیقاتی دیگر نیز استفاده کند. با توجه به تفاوت‌های اساسی بین کاربردهای اولیه و بعدی داده‌ها، مورد دوم، استفاده ثانویه است. بر این اساس، وقوع این امر درخصوص داده‌های سلامت بیماران که به صورت هوشمند و در قالب پرونده الکترونیک سلامت در سیستم مراکز درمانی ذخیره می‌شود، محتمل است (۲۵). مسأله‌ای که همواره باید در نظر داشت این است که استفاده ثانویه از اطلاعات سلامت بیماران برای پیشرفت و بروزرسانی در سیستم درمان و سلامت امری اجتناب‌ناپذیر است و حتی گاه مراکز درمانی به ناچار اطلاعات خاصی را بدون توجه به رضایت بیمار افشا می‌کنند. در مقررات عمومی حفاظت از داده‌ها اتحادیه اروپا (ماده ۹) نیز به استفاده ثانویه از داده‌های کاربران در راستای منافع عمومی یا منافع قانونی اشاره نموده است.

در همین راستا، مقررات فضای داده‌های سلامت اروپا (EHDS) ۲۰۲۲ م. یک چارچوب جامع برای استفاده ثانویه از داده‌های سلامت پیش‌بینی نموده است. این پیشنهاد بیشتر اهداف مجاز و ممنوع را در مواد ۳۴ و ۳۵ مشخص می‌کند و هدف آن ایجاد تعادل بین استفاده از داده‌ها برای اهداف مفید و حفظ حقوق فردی است. اهداف مجاز شامل فعالیت‌های توسعه‌ای و نوآورانه است؛ در حالی که اهداف ممنوعه شامل استفاده مضر علیه افراد، تبلیغات، دسترسی داده‌ها به اشخاص ثالث و غیرمجاز و گسترش محصولات مضر است.

برخی بر این باورند که اطلاعات بیماران در پزشکی هوشمند باید در نظام سلامت باقی بماند و در خارج از بخش بهداشت و درمان یا برای استفاده تجاری یا منافع مالی نباید مجدد استفاده (استفاده ثانویه) شود. بنابراین، استفاده ثانویهٔ مجاز از اطلاعات بیماران صرفاً در راستای امور تحقیقاتی و سازمان‌های غیر دولتی است و اگر قرار است اطلاعات خارج از سیستم بهداشتی بهره‌برداری گردد، ابتدا باید رضایت آگاهانه بیمار دریافت شود (۲۶). در این خصوص به نظر می‌رسد در چشم‌انداز به سرعت در حال تحول توسعه هوش مصنوعی پزشکی، استفاده ثانویه از داده‌های سلامت به‌عنوان سنگ‌بنای حیاتی اهمیت چارچوب‌های حاکمیت داده‌های قوی و شفاف، به‌ویژه زمانی است که نهادهای تجاری به داده‌های بهداشتی در مقیاس بزرگ تکیه می‌کنند. نهادهای تجاری نقش

برجسته‌ای را در پیشرفت هوش مصنوعی پزشکی ایفا می‌کنند و دسترسی آن‌ها به مخازن وسیع داده‌های سلامت، پتانسیل زیادی برای اکتشافات پیشگامانه دارد. با این حال، این دسترسی باید توسط یک چارچوب قابل اعتماد و شفاف حاکمیت داده پشتیبانی شود. چنین چارچوبی نه‌تنها به استقلال افراد در مورد داده‌های سلامتی آن‌ها احترام می‌گذارد، بلکه تضمین می‌کند که افراد نحوه دسترسی و استفاده از داده‌های آن‌ها توسط این نهادها را درک می‌کنند (۲۷).

جهت جلوگیری از نقض داده‌های شخصی بیماران در استفاده ثانویه از اطلاعات آنان الزاماتی حقوقی و فنی مانند محدودیت پردازش، محدودیت استفاده از اطلاعات و امکان اصلاح اطلاعات را می‌توان در نظر گرفت. هرچند به‌طور معمول در فرم‌های اخذ رضایت از بیمار موارد متعدد با گستره وسیع را ذکر می‌نمایند تا از ادعای احتمالی نقض حریم خصوصی در پردازش اطلاعات جهت اهداف مختلف ثانویه جلوگیری شود اما جهت حفظ حقوق بیمار در این زمینه با توجه به مواد ۱۶-۱۸ مقررات حفاظت از داده‌های خصوصی اتحادیه اروپا، می‌توان محدودیت‌هایی برای استفاده از اطلاعات بیمار ایجاد نمود به نحوی که اطلاعات جمع‌آوری شده یا پردازش‌شده، برای استفاده در غیر موارد موضوع رضایت مأخوذه، به استفادهٔ دیگری نرسد. همچنین ضروری است تا امکان اصلاح و پاک کردن اطلاعات برای شخص موضوع اطلاعات (بیمار) فراهم باشد (۲۸).

نتیجه‌گیری

بخش مراقبت‌های پزشکی یکی از امیدوارکننده‌ترین زمینه‌ها برای به‌کارگیری هوش مصنوعی است تا با قابلیت‌هایی که دارد بتواند تغییرات انقلابی در حوزه پزشکی ایجاد کند. هم‌گرایی هوش مصنوعی با بخش مراقبت‌های بهداشتی امکانات بی‌سابقه‌ای را برای سلامت شهروندان ارائه می‌دهد، اما به‌طور هم‌زمان مسائل مهمی را در مورد حفاظت از داده‌های شخصی ایجاد می‌کند. به عبارت دیگر، هوش مصنوعی در زمینه پزشکی به‌طور مداوم در تمام تخصص‌ها گسترش می‌یابد و اجرای آن انتظارات زیادی را نه‌تنها برای بهبود مراقبت از بیماران، بلکه برای تسهیل دسترسی به مراقبت‌های درمانی و بهداشتی در مکان‌هایی که بیماران در دسترسی به متخصصان یا مراقبت‌های پزشکی مشکل دارند، افزایش داده است.

بر همین اساس، سازمان بهداشت جهانی نیز اعلام کرده است که «هوش مصنوعی تعهد گسترده‌ای برای امور پزشکی دارد، با این حال، فرصت‌ها و چالش‌های هوش مصنوعی بسیار نزدیک به یکدیگرند» (۲۹). بر این اساس، یکی از مهم‌ترین مسائل در حوزه حقوق سلامت هوشمند، علاوه بر مسئولیت خسارات وارده ناشی از ورود هوش مصنوعی به حوزه درمان، اعمال جراحی و ...، حمایت از حریم خصوصی و اطلاعات بیماران می‌باشد. زیرا این اطلاعات امروزه دیگر امکان دسترسی بالا و به موازات آن، نقض گسترده دارد. از همین رو است که هوشمندسازیِ خدمات پزشکی و استفاده روزافزون از فناوری‌ها برای جمع‌آوری و پردازش اطلاعات، نیاز به قوانین حفاظتی سختگیرانه را ضروری ساخته است. اتحادیه اروپا به‌عنوان نهاد بین‌المللیِ پیشگام در این زمینه، با تصویب قانون هوش مصنوعی در سال ۲۰۲۴ م. گام‌های نخست را برداشته است.

در نظام حقوقی ایران نیز با توجه به نو بودن به‌کارگیری فناوری هوش مصنوعی در حوزه سلامت، طبیعتاً نیاز به قانونگذاری افتراقی و مختصِ حمایت از داده‌های پزشکی احساس می‌شود. با نگرشی در قوانین موجود، با اغماض می‌توان گفت جز قانون تجارت الکترونیکی مصوب ۱۳۸۲ ـ که البته بیشتر با اهداف تجارتی نگارش یافته است ـ و قانون جرایم رایانه‌ای مصوب ۱۳۸۸ ـ که صرفاً به جرم‌انگاری پرداخته است ـ قانونِ ویژه‌ای در این خصوص وجود ندارد. البته لایحه «حمایت و حفاظت از داده و اطلاعات شخصی» که در مجلس شورای اسلامی در انتظار تصویب است، با پیش‌بینیِ مسئولیت‌های مدنی (جبران خسارات مادی و معنوی) و کیفریِ ویژهٔ نقض داده‌ها، تا حد زیادی می‌تواند حریم خصوصی افراد در حوزه‌های مختلف مانند امور پزشکی را تأمین نماید.

در هر حال، برای حفاظت از داده‌های سلامت شخصی افراد اقدامات پیشگیرانه‌ای نیز باید انجام شود:

۱) اطمینان از استفاده انحصاری از داده‌های بهداشتی برای مقاصد پزشکی و علمی و جلوگیری از سوء استفاده از آن‌ها برای مقاصد تجاری و ... . ۲) به حداقل رساندن خطر دسترسی شخص ثالث به داده‌های حساس، از طریق اجرای اقدامات امنیتی فنی و سازمانی و پیش‌بینی حق دسترسیِ خود بیمار به اطلاعات شخصی. ۳) الزام به اطلاع بیماران از پردازش داده‌ها و حقوق آن‌ها، تضمین شفافیت و اعتمادسازی. ۴) توسعه زیرساخت‌های امن برای ذخیره‌سازی و انتقال داده‌ها. ۵) محافظت از داده‌ها در برابر حملات سایبری و نقض آن‌ها. ۶) ایجاد تعادل بین نیاز به دسترسی به داده‌های سلامت مدار برای اهداف تحقیقاتی و حفاظت از حریم خصوصی افراد. ۷) آموزش کنشگران حوزه سلامت اعم از پزشکان، پرستاران و ... در رابطه با تعهداتشان برای حفاظت از داده‌های پزشکی و رویه‌هایی که باید رعایت شود. داده‌های سلامت یک آماج جذاب برای حملات سایبری هستند و اجرای اقدامات امنیتی پیشرفته مانند رمزگذاری و ناشناس‌سازی برای جلوگیری از نقض احتمالی آن‌ها ضروری است. همچنین، پدیده تبعیض الگوریتمی که ضد اصول اخلاق پزشکی می‌باشد، نیز به شدت نگران‌کننده است. زیرا الگوریتم‌هایی هوش مصنوعی که از داده‌های سلامت سایر بیماران جمع‌آوری می‌شود، ممکن است ازیک‌سو منجر به تصمیم‌های پزشکی ناعادلانه یا اشتباه شود و از سوی دیگر، منجر به ایجاد مسئولیت مدنی و نقض اصل برابری در دسترسی به مراقبت‌های پزشکی شود.

مشارکت نویسندگان

تهمینه اسفندیاری: جمع‌آوری داده‌ها، تدوین و نگارش مقاله.

حمید روستایی صدرآبادی: طراحی ایده، نظارت و همکاری در فرآیند تدوین مقاله.

نصراله جعفری خسروآبادی: نظارت و همکاری در فرآیند تدوین مقاله.

سیداحمد میرخلیلی: مشاوره و همکاری در فرآیند تدوین مقاله.

تضاد منافع

نویسندگان هیچ‌گونه تضاد منافع احتمالی را در رابطه با تحقیق، تألیف و انتشار این مقاله اعلام نکرده‌اند.

تشکر و قدردانی

ابراز نشده است.

تأمین مالی

نویسندگان اظهار می‌نمایند که هیچ‌گونه حمایت مالی برای تحقیق، تألیف و انتشار این مقاله دریافت نکرده‌اند.

ملاحظات اخلاقی

در پژوهش حاضر جنبه‌های اخلاقی مطالعه کتابخانه‌ای شامل اصالت متون، صداقت و امانتداری رعایت شده است.

بیانیه هوش مصنوعی

نویسندگان اعلام می‌دارند که در فرایند تحقیق، نگارش و ویرایش این مقاله، از هیچ‌گونه ابزار هوش مصنوعی استفاده نشده است.

References

1. Sharafoddini A, Dubin JA, Lee J. Patient similarity in prediction models based on health data: a scoping review. JMIR medical informatics. 2017; 5(1): e6730.

2. Ansari B. Mass Communication Law.1th Ed.Tehran: Samt Publications; 2022. [Persian]

3. Lupton M, Australia GC. Can Patient Information Held by an AI Robot Be Protected by the Duty of Confidentiality?. International Journal of Medical Science and Health Research. 2020; 4(4): 41-55.

4. Manheim K, Kaplan L. Artificial Intelligence: Risks to Privacy and Democracy. Yale Journal of Law and Technology. 2019; 37(21): 151-160.

5. Waldoch K. Informed Consent for the Use of AI in the Process of Providing Medical Services: Review of European and Comparative Law. 2024; 57(2): 121-134

6. Iserson KV. Informed consent for artificial intelligence in emergency medicine: A practical guide. The American Journal of Emergency Medicine. 2024; 76: 225-230.

7. Cohen IG. Informed Consent and Medical Artificial Intelligence: What to Tell the Patient?. The Georgetown Law Journal. 2020; 108(20): 1425–1469

8. Caliskan A, Bryson JJ, Narayanan A. Semantics derived automatically from language corpora contain human-like biases. Science. 2017; 356(6334): 183-186.

9. Wojcik MA. Algorithmic discrimination in health care: an EU law perspective. Health and Human Rights. 2022; 24(1): 93-103.

10. Schönberger D. Artificial intelligence in healthcare: a critical analysis of the legal and ethical implications. International Journal of Law and Information Technology. 2019; 27(2): 171-203.

11. Loyola-Gonzalez O. Black-box vs. white-box: Understanding their advantages and weaknesses from a practical point of view. IEEE access. 2019; 7: 154096-113.

12. Voigt P, Von dem Bussche A. The eu general data protection regulation (gdpr). A practical guide, 1st ed., Cham: Springer International Publishing; 2017.

13. Kiseleva A, Kotzinos D, De Hert P. Transparency of AI in healthcare as a multilayered system of accountabilities: between legal requirements and technical limitations. Frontiers in artificial intelligence. 2022; 5: 879603.

14. Florina M. Liability Issues Concerning Self-Driving Vehicles: EJRR Special Issue on the Man and the Machine. 2016; 7(2): 335-341.

15. Shahbazinia M, Zolghadr MJ. Recognizing Artificial Intelligence (AI) As A Legal Person: Providing A Policy Proposal to The Iranian Legislator. Journal of Science and Technology Policy. 2024; 17(3): 41-53.[Persian]

16. Hekmatnia M, Mohammadi M, Vaseghi M. civil Liability for damages caused by robots based on autonomous artificial intelligence. Islamic Law. 2019; 16(60): 231-258. [Persian]

17. Staszkiewicz P, Horobiowski J, Szelągowska A, Strzelecka AM. Artificial intelligence legal personality and accountability: auditors' accounts of capabilities and challenges for instrument boundary. Meditari Accountancy Research. 2024; 32(7): 120-146.

18. Parliament EU. Civil Law Rules on Robotics: European Parliament Resolution of 16 February 2017 with Recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL)). Official Journal of the European Union https://www. europarl. europa.eu/doceo/document/TA-8-2017-0051_EN. html (accessed 9/10/2024). 2017.

19. World Economic Forum, 'Healthcare pays the highest price of any sector for cyberattacks – that's why cyber resilience is key', 1 February 2024 https://www.weforum.org/agenda. accessed 19 April 2024.

20. Karimi A, Rahimipour I, Hassani M. Telemedicine crimes resulted from electronic health. Medical Law Journal. 2010; 4(14): 47-69. [Persian]

21. Finlayson SG, Bowers JD, Ito J, Zittrain JL, Beam AL, Kohane IS. Adversarial attacks on medical machine learning. Science. 2019; 363(6433): 1287-1289.

22. McLeod A, Dolezel D. Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems. 2018; 108: 57-68.

23. Health data breach: Dedalus Biologie fined 1.5 million euros.Web site. https://www.edpb.europa.eu/ news/national-news.Updated 15 April 2022. Accessed 4 May 2022.

24. Nguyen T. The Ethical Governance of Artificial Intelligence and Machine Learning in Healthcare. 1th Ed, New York: Ethics International Press Limited; 2023.

25. Shah SM, Khan RA. Secondary use of electronic health record: Opportunities and challenges. IEEE access. 2020; 8: 136947-65.

26. Kerasidou A, Kerasidou C. Data-driven research and healthcare: public trust, data governance and the NHS. BMC medical ethics. 2023; 24(1): 51.

27. Ho CH. Secondary use of health data for medical AI: A cross-regional examination of Taiwan and the EU. Asian Bioethics Review. 2024; 16(3): 407-422.

28. Dehghanpour S, Navid R. Investigating the Threats to Privacy and the Legal Requirements for Protecting It in the Use of Self-Driving Vehicles: Quarterly Journal of Private Law Studies. 2022; 51(4): 695-715. [Persian]

29. WHO guidance on Artificial Intelligence to improve healthcare, mitigate risks worldwide. UN News, Web site: https://news.un.org/en/story/2021/06/1094902. 28 June 2021, accessed 19 April 2024