Original Article Open Access

The Iranian Association of Medical Law

Medical Law Journal

2026; 20: e18

Journal Homepage: http://ijmedicallaw.ir

Institute of Bioethics and Health Law

Artificial Intelligence in Health Systems: Juridical-Theological Protection of Patient Privacy and Ethical Obligations

Sayyed Mohammad Hadi Ghabooli Dorafshan[1*], Fatemeh Najibzadeh Vamegh Abadi[1]

1. Department of Islamic Jurisprudence and Principles of Islamic Law, Faculty of Theology and Islamic Studies, Ferdowsi University of Mashhad, Mashhad, Iran.

ABSTRACT

Background and Aim: The expanding use of artificial intelligence in diagnosis, monitoring and clinical decision support, while enhancing efficiency, has created an unprecedented dependence on deeply identity-related patient data. The central issue is how to safeguard patient dignity, privacy and autonomy throughout the entire data lifecycle without undermining therapeutic interests and clinical safety.

Method: This study adopts a descriptive-analytical approach based on library and documentary sources. It employs a comparative interpretation of Islamic jurisprudential foundations, the legal rules of Iran and the European Union and the ethical and technical standards governing the clinical use of artificial intelligence in healthcare systems.

Ethical Considerations: Scientific integrity, respect for individual rights, confidentiality and respect for intellectual property were observed throughout all stages of the research and writing process.

Results: The findings indicate that health data constitute an extension of the patient's personality and their effective protection requires data minimization, access control and output obfuscation. In Iranian law, the protection of dignity, the prohibition of intrusion and the criminalization of unauthorized disclosure and access, subject to explicit legal authorization, provide preventive and punitive safeguards. In the European Union, patient data governance, risk management, human oversight of high-risk systems and judicial and enforcement mechanisms establish a coherent accountability framework.

Conclusion: Effective protection of patient privacy in AI-based medicine requires the integration of a dignity-based normative foundation, legal and criminal safeguards and auditable technical standards. The European Union model offers a suitable reference point for developing clear digital health regulations in Iran.

Keywords: Artificial Intelligence; Patient Privacy; Algorithmic Justice; Informed Consent; Human Dignity

Corresponding Author: Sayyed Mohammad Hadi Ghabooli Dorafshan; **Email:** h.ghaboli@um.ac.ir

Received: August 04, 2025; **Accepted:** December 04, 2025; **Published Online:** May 10, 2026

Please cite this article as:

Ghabooli Dorafshan SMH, Najibzadeh Vamegh Abadi F. Artificial Intelligence in Health Systems: Juridical-Theological Protection of Patient Privacy and Ethical Obligations. Medical Law Journal. 2026; 20: e18.

دسترسی آزاد | مقاله پژوهشی

مجله حقوق پزشکی

دوره بیستم، ۱۴۰۵

Journal Homepage: http://ijmedicallaw.ir

هوش مصنوعی در نظام سلامت:

صیانت فقهی ـ حقوقی از حریم خصوصی بیمار و الزامات اخلاقی

سیدمحمدهادی قبولی درافشان[1*]، فاطمه نجیب‌زاده وامق‌آبادی[1]

۱. گروه فقه و مبانی حقوق اسلامی، دانشکده الهیات و معارف اسلامی، دانشگاه فردوسی مشهد، مشهد، ایران.

چکیده

زمینه و هدف: گسترش کاربرد هوش مصنوعی در تشخیص، پایش و تصمیم‌یار بالینی، در کنار افزایش کارایی، وابستگی فزاینده‌ای به داده‌های عمیقاً هویتی بیماران ایجاد کرده است. مسئله اصلی، تضمین کرامت، حریم خصوصی و خودمختاری بیمار در سراسر چرخه داده، بدون اخلال در منافع درمانی و ایمنی بالینی است.

روش: این پژوهش با روش توصیفی ـ تحلیلی و بر پایه منابع کتابخانه‌ای و اسنادی، از طریق تفسیر تطبیقی مبانی فقهی، قواعد حقوق ایران و اتحادیه اروپا، و نیز استانداردهای اخلاقی و فنی ناظر بر کاربرد بالینی هوش مصنوعی در نظام سلامت انجام شده است.

ملاحظات اخلاقی: پایبندی به صداقت علمی، رعایت حقوق اشخاص، رازداری و احترام به مالکیت فکری در تمامی مراحل نگارش رعایت شده است.

یافته‌ها: یافته‌ها نشان می‌دهد داده سلامت امتداد شخصیت بیمار است و صیانت از آن مستلزم حداقل‌گرایی در گردآوری، کنترل دسترسی و مبهم‌سازی خروجی‌هاست. در حقوق ایران، مصونیت حیثیت، منع تجسس و جرم‌انگاری افشا و دسترسی غیر مجاز، با شرط حکم صریح قانون، ظرفیت حمایت پیشینی و کیفری فراهم می‌کند. در اتحادیه اروپا نیز حاکمیت بیمار بر داده، مدیریت ریسک، نظارت انسانی بر سامانه‌های پرخطر و سازوکارهای اجرایی و قضایی، چهارچوبی منسجم برای پاسخگویی ایجاد کرده است.

نتیجه‌گیری: صیانت مؤثر از حریم بیمار در پزشکی مبتنی بر هوش مصنوعی مستلزم تلفیق مبنای هنجاری کرامت، ضمانت‌های حقوقی و کیفری و الزامات فنی قابل حسابرسی است. الگوی اتحادیه اروپا می‌تواند مبنای مناسبی برای تدوین مقررات شفاف سلامت دیجیتال در ایران باشد.

واژگان کلیدی: هوش مصنوعی؛ حریم خصوصی؛ عدالت الگوریتمی؛ رضایت آگاهانه؛ کرامت انسانی

نویسنده مسئول: سیدمحمدهادی قبولی درافشان؛ **پست الکترونیک:** h.ghaboli@um.ac.ir

تاریخ دریافت: ۱۴۰۴/۰۵/۱۳؛ **تاریخ پذیرش:** ۱۴۰۴/۰۹/۱۳؛ **تاریخ انتشار:** ۱۴۰۵/۰۲/۲۰

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

Ghabooli Dorafshan SMH, Najibzadeh Vamegh Abadi F. Artificial Intelligence in Health Systems: Juridical-Theological Protection of Patient Privacy and Ethical Obligations. Medical Law Journal. 2026; 20: e18.

مقدمه

گسترش کاربری هوش مصنوعی در مراقبت‌های بهداشتی و درمانی، ساختار سنتی رابطه بیمار ـ درمانگر را دگرگون کرده و پرسش‌های بنیادینی در باب حریم خصوصی، کرامت انسانی، مسئولیت‌پذیری حرفه‌ای و حدود مداخله مجاز در داده‌های سلامت انسان پدید آورده است. سامانه‌های تشخیصی و تصمیم‌یار، پایش از راه دور، پرونده الکترونیک سلامت و زیرساخت‌های تحلیل پیش‌بینانه، اکنون با دسترسی مستمر و عمیق به لایه‌های زیستی، روانی، جنسی و اجتماعی بیمار عمل می‌کنند؛ لایه‌هایی که نه فقط اطلاعات پزشکی، بلکه امتداد حیثیت و هویت شخصی فرد محسوب می‌شوند. در چنین بستری دیگر نمی‌توان حفاظت از داده سلامت را صرفاً به محرمانگی سنتی پزشک ـ بیمار یا «رضایت اولیه در بدو پذیرش» فرو کاست. پرسش اصلی این است که آیا می‌توان و باید این داده را به مثابه «امانت حیثیتی بیمار» تلقی کرد و کل زنجیره فناورانه سلامت را از بیمارستان تا پیمانکار پردازش داده و سکوی تحلیل الگوریتمی را در مقام امین پاسخگو نشاند. مقاله حاضر با اتخاذ رویکردی فقهی ـ حقوقی و با اتکا بر مفاهیمی چون کرامت ذاتی انسان و لزوم کتمان سر در اخلاق و فقه، در کنار بررسی ظرفیت‌ها و کاستی‌های حقوق موجود در ایران و الگوهای پیشرفته اتحادیه اروپا، به این پرسش می‌پردازد که صیانت از حریم بیمار در عصر سلامت مبتنی بر هوش مصنوعی چگونه باید بازتعریف و الزام‌آور شود، به گونه‌ای که حفاظت از داده نه یک توصیه اخلاقی، بلکه شرط مشروعیت خود سامانه سلامت تلقی گردد.

در پیشینه پژوهش، سه خط اصلی قابل مشاهده است: نخست، مقاله «تأثیرگذاری حق بر حریم خصوصی بیماران» (۱) با تفکیک آثار ایجابی و سلبی هوش مصنوعی نشان می‌دهد که از یک‌سو دسترسی به داده‌های بیمار تسریع و تقویت می‌شود و از سوی دیگر تمرکز ناایمن و پراکنده داده در سامانه‌های مختلف، در غیاب تنظیم‌گری منسجم، ریسک افشای گسترده و نقض حقوق اطلاعاتی را تشدید می‌کند. این تحلیل اهمیت مسأله را نشان می‌دهد، اما همچنان در سطح توصیف موقعیت و آسیب‌پذیری باقی می‌ماند و کمتر به این می‌پردازد که این وضعیت چگونه باید در سطح نهادی و هنجاری مهار و بازآرایی شود؛ دوم، مقاله «مسئولیت مدنی ناشی از نقض حق بر حریم خصوصی بیماران به واسطه به کارگیری سامانه‌های هوش مصنوعی در محیط‌های درمان» (۲) پرسش را در چهارچوب مسئولیت مدنی طرح می‌کند: آیا نقض حریم خصوصی در محیط درمان باید مسئولیت مبتنی بر تقصیر ایجاد کند یا مسئولیت محض؟ و این مسئولیت را باید به توسعه‌دهنده، کادر درمان، مدیریت مرکز درمانی یا به خود سامانه نسبت داد؟ این رویکرد اهمیت انتساب مسئولیت و جبران خسارت را برجسته می‌کند، اما تمرکز آن بر مرحله پس از وقوع خسارت است و کمتر به طراحی سازوکارهای پیشینی برای مهار دسترسی و چرخش داده و جلوگیری از شکل‌گیری آسیب می‌پردازد؛ سوم، مقاله «حفاظت از داده‌های پزشکی: تعامل حق بر حریم خصوصی و هوش مصنوعی» (۳) بر خطرات تمرکز داده‌های سلامت در دست بازیگران خصوصی و ضعف سازوکارهای نظارت عمومی در مشارکت‌های سلامت و فناوری تأکید می‌کند و هشدار می‌دهد که توانایی بازشناسایی مجدد داده‌های به ظاهر ناشناس، حتی با روش‌های متعارف امنیتی، به طورجدی رو به افزایش است. این مقاله به درستی بر ضرورت ارتقای سازوکارهای ناشناس‌سازی و نظارت سیستمی بر جریان داده تأکید دارد، اما وارد صورت‌بندی یک مدل بومی‌شده برای پیوند این ملاحظات با مبانی هنجاری فقهی و با ساختار حقوق عمومی ایران نمی‌شود. در مقایسه با این آثار، مقاله حاضر صرفاً به توصیف خطر یا به مطالبه جبران خسارت پس از وقوع نقض اکتفا نمی‌کند، بلکه در پی آن است که نشان دهد چگونه می‌توان با تکیه بر مبانی الزام‌آور کرامت و کتمان سر و با الهام از تجربه اتحادیه اروپا در بازتوزیع قدرت و مسئولیت در زنجیره سلامت دیجیتال، یک الگوی هنجاری و نهادی برای صیانت فعال از بیمار در ایران بنا کرد؛ الگویی که علاوه بر جرم‌انگاری و مسئولیت مدنی، بر «پیشگیری ساختاری» نیز استوار باشد.

نوآوری این پژوهش در سه محور تبیین می‌شود: نخست، داده سلامت بیمار نه «اطلاعات صرف»، بلکه «امانت حیثیتی» و

جزئی از کرامت شخصی تفسیر می‌شود؛ بر این مبنا، اصل «کتمان سر» از سکوت اخلاقی فرد درمانگر به تعهد ساختاری کل سامانه بالینی و داده‌محور ارتقا می‌یابد و تولید، ثبت، گردش و باز استفاده از داده باید به «حد ضرورت درمانی» محدود شود؛ هر استفاده ثانویه بدون رضایتِ قابلِ بازپس‌گیری و مستندسازی دقیق، مداخله در حریم حیثیتی است؛ دوم، ظرفیت‌های حقوق داخلی از مصونیت حیثیت و منع تجسس تا جرم‌انگاری شنود و افشای، بدون ابزارهای اجرایی مانند تعیین دقیق مجوز پردازش، ثبت رد پای دسترسی و الزام پاسخگویی فناورانه، از سطح اعلام ارزش فراتر نمی‌روند و نیازمند تنظیم‌گری ثانویه و نظارت هدفمند وزارت بهداشت‌اند؛ سوم، با الهام از اتحادیه اروپا می‌توان بیمار را به «صاحب حق قابل اعمال» و سکو یا پردازشگر را از «ناقل بی‌طرف» به «امینِ پاسخگو» تبدیل کرد و سامانه‌های تشخیصی و تصمیم‌یار را از آغاز چرخه عمر مقید به مدیریت ریسک، شفافیت، مستندسازی و مداخله انسانی نمود، سپس این منطق با مبانی فقهی و ظرفیت‌های تقنینی ایران بومی‌سازی می‌شود.

بر این اساس، پرسش‌های محوری عبارت است از: ۱ـ در حوزه سلامت مبتنی بر هوش مصنوعی، مرز مداخله مجاز در داده بیمار کجاست و کدام داده اساساً نباید تولید، ثبت یا وارد گردش ثانویه شود؟؛ ۲ـ چه آرایش نهادی و چه الزام‌های تقنینی تضمین می‌کند که از لحظه تولید تا باز استفاده، داده به مثابه «امانت حیثیتی» مدیریت شود؟؛ ۳ـ تجربه اتحادیه اروپا چگونه به نقشه تنظیم‌گری بومی و قابل اجرا در ایران ترجمه می‌گردد تا حقوق بیمار اعمال‌پذیر و مسئولیت سکوها و سامانه‌ها پیشینی و مستمر باشد؟

از حیث ساختار، پژوهش در چهار گام پیش می‌رود: در گام نخست، مفاهیم کلیدی؛ در گام دوم، مبانی فقهی و اخلاقی صیانت از بیمار در برابر مداخله فناورانه؛ در گام سوم، سازوکارهای حقوقی صیانت از حریم خصوصی و در گام چهارم، چالش‌های اخلاقی کاربست هوش مصنوعی در مراقبت‌های بهداشتی و درمانی و استانداردهای هنجاری مورد بررسی قرار می‌گیرد.

روش

روش پژوهش توصیفی ـ تحلیلی، مبتنی بر اسناد کتابخانه‌ای و رویکردی تطبیقی میان فقه و حقوق ملی و بین‌المللی است.

ملاحظات اخلاقی

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

یافته‌ها

یافته‌های این پژوهش نشان می‌دهد که داده‌های سلامت، به سبب پیوند وثیق با هویت جسمانی، روانی و حیثیتی بیمار، در هر سه سطح فقهی، حقوق داخلی و الگوی تنظیم‌گری اتحادیه اروپا، موضوع حمایتی مضاعف تلقی می‌شوند. در مبانی فقهی، کرامت ذاتی انسان و قاعده لزوم کتمان سرّ، اطلاعات پزشکی را در قلمرو امانتداری و وفاداری قرار می‌دهد و از این رهگذر، محرمانگی را از سطح تکلیف فردی پزشک فراتر برده و به سطح الزامات ساختاری در گردآوری، نگهداری و پردازش داده تسری می‌دهد. بر همین مبنا، محدودسازی جریان داده، جمع‌آوری در حد ضرورت درمانی، کنترل دسترسی و جلوگیری از انتساب مستقیم داده به اشخاص، با منطق فقهی صیانت از حیثیت و حریم بیمار سازگار است.

بررسی حقوق ایران نیز نشان می‌دهد که اصول قانون اساسی و برخی قواعد کیفری، از حیث حمایت از حیثیت، منع تجسس و ممنوعیت افشا و دسترسی غیر مجاز، ظرفیت قابل توجهی برای حمایت از داده‌های پزشکی فراهم کرده‌اند. با این حال، این ظرفیت‌ها در حوزه سلامت دیجیتال و سامانه‌های مبتنی بر هوش مصنوعی، هنوز در قالب چهارچوبی منسجم و صریح درباره حدود پردازش، استفاده ثانویه از داده، مدت نگهداری و مسئولیت بازیگران مختلف نهادینه نشده‌اند. یافته‌ها همچنین حاکی از آن است که با افزایش فاصله پردازش داده از ضرورت

مستقیم درمان، اهمیت رضایت آگاهانه، شفافیت هدف پردازش و امکان ردیابی جریان داده افزایش می‌یابد، به ویژه در مواردی مانند آموزش الگوریتم، استفاده پژوهشی و انتقال داده میان نهادها.

در مقابل، الگوی اتحادیه اروپا نشان می‌دهد که حمایت از داده سلامت تنها در قالب منع یا جرم‌انگاری خلاصه نمی‌شود، بلکه از طریق شناسایی داده سلامت به عنوان داده حساس، اعطای حقوق اجرایی به بیمار، توزیع مسئولیت میان کنشگران مختلف و پیش‌بینی الزامات فنی و سازمانی برای سامانه‌های پرخطر تحقق می‌یابد. در این چهارچوب، حق دسترسی، آگاهی، محدودسازی پردازش، انتقال‌پذیری داده و امکان مداخله انسانی، در کنار الزامات مربوط به مدیریت ریسک، کیفیت داده، مستندسازی و قابلیت حسابرسی، مجموعه‌ای از تضمین‌های به‌هم‌پیوسته را شکل می‌دهد. در مجموع، یافته‌ها بیانگر آن است که حمایت مؤثر از حریم بیمار در پزشکی مبتنی بر هوش مصنوعی، در گرو پیوند منسجم میان مبانی هنجاری، قواعد حقوقی و الزامات فنی در کل چرخه حیات داده و سامانه است.

بحث

۱ـ در منطق فقهی کرامت انسان و لزوم کتمان سر، داده سلامت امتداد شخصیت بیمار است و تعرض بی‌ضابطه به آن هم‌سنگ اخلال در حرمت و اعتماد است؛ ترجمه عملی این منطق، حداقلی‌سازی جمع‌آوری، قفل‌گذاری دسترسی از لحظه تولید و مبهم‌سازی خروجی‌های تحلیلی برای پیشگیری از بازشناسایی است.

۲ـ در حقوق ایران، اصول اساسیِ مصونیت حیثیت و منع تجسس همراه با جرم‌انگاری شنود و افشای اسرار درمانی، ظرفیت حمایت پیشینی و کیفری دارند، مشروط به تدوین «حکم قانون» صریح در سلامت دیجیتال، تفکیک ضرورت درمانی از بهره‌برداری ثانویه و الزام به ثبت ردپای دسترسی.

۳ـ در اتحادیه اروپا، یک معماری سه‌لایه برقرار است: حق‌مداری و حاکمیت بیمار بر داده، تکالیف پیشینی مبتنی بر مدیریت ریسک و نظارت انسانی برای سامانه‌های پرخطر، و سازوکارهای قضایی ـ اجرایی که سکوها و بهره‌برداران را به پاسخگویی فعال ملزم می‌کند.

۴ـ در بعد اخلاقی بالینی، کف پذیرش شامل شفافیت نقش سامانه، قابلیت حسابرسی، استمرار قضاوت انسانی در تصمیم‌های پرمخاطره، رضایت پویا و مرزبندی داده‌های واقعاً ضروری است.

۱. تبیین مفاهیم: با توجه به آنکه تحلیل کاربست هوش مصنوعی در مراقبت‌های بهداشتی و درمانی مبتنی بر مفاهیمی است که هر یک دارای بار نظری و پیامد عملی خاص هستند، ضروری است در آغاز پژوهش، این مفاهیم به صورت دقیق و عملیاتی تعریف شوند. در این قسمت، دو مفهوم کلیدی یعنی «حریم خصوصی» و «هوش مصنوعی» تبیین می‌گردد تا در ادامه مقاله، ابهام تفسیری در استدلال‌ها و نتایج به حداقل برسد.

۱-۱. حریم خصوصی: حریم خصوصی عرصه‌ای از زندگی هر فرد است که وی به طور معقول انتظار دارد بدون کسب رضایتش دیگران وارد آن نشوند؛ مطابق بند ۱ ماده ۲ طرح حمایت از حریم خصوصی، این قلمرو عبارت است از بخشی از زندگی هر شخص که عرفاً یا پس از اعلان قبلی و در چهارچوب قانون، نباید بدون رضایت وی به آن وارد شد، بر آن نظارت یا مشاهده داشت، به اطلاعات مربوط به آن دسترسی یافت یا در آن تعرض صورت داد (۴).

۱-۲. هوش مصنوعی: هوش مصنوعی به عنوان شاخه‌ای از علوم کامپیوتر، عبارت است از توانمندی سیستم‌ها در دریافت و پردازش داده‌های محیطی به منظور تفسیر صحیح ورودی‌ها، یادگیری پیوسته از این داده‌ها و تعدیل رفتار با انطباق انعطاف‌پذیر برای دستیابی به اهداف تعیین‌شده در شرایط متغیر (۵)، این ویژگی‌ها شامل به کارگیری الگوریتم‌های یادگیری ماشینی برای تشخیص الگو، پیش‌بینی رخدادها و بهینه‌سازی تصمیم‌ها با کمترین دخالت انسانی است (۶).

۲. مبانی فقهی صیانت از حریم خصوصی بیماران در به کارگیری هوش مصنوعی در مراقبت‌های بهداشتی و

درمانی: شتاب کاربست هوش مصنوعی در نظام سلامت، فراتر از مسائل فنی، پرسش‌های هنجاری درباره حدود گردآوری، تحلیل و باز استفاده از داده‌های بیمار، مسئولیت حرفه‌ای و پاسخگویی در خطاهای الگوریتمی و صیانت از حیثیت و حریم خصوصی را برمی‌انگیزد.

اصول فقهی مستقر، از جمله کرامت ذاتی انسان و قاعده لزوم کتمان سر، قابلیت ترجمه به زبان تعهدات حقوقی معاصر را دارند و مبنای تعریف مصونیت پیشینی داده سلامت فراهم می‌آورند. بر این بنیاد می‌توان قواعد الزام‌آور محرمانگی و حداقل‌گرایی داده، تحدید دسترسی و پردازش الگوریتمی و سازوکارهای پاسخگویی حرفه‌ای و نهادی را به صورت منسجم صورت‌بندی کرد. رویکرد تحلیلی ـ تطبیقی ارائه‌شده مسیر تبدیل این مبانی به پشتوانه‌های تقنینی، نظارتی و انتظامی لازم برای مواجهه با مخاطرات داده‌محور در مراقبت سلامت را تبیین می‌کند.

۲-۱. اصل کرامت ذاتی بشر: کرامت، به عنوان مبنایی بنیادین در سنت فقهی، از دیرباز محور بحث‌های هنجاری درباره شأن انسان بوده است. فراهیدی «کرامت» را «اسم منتسب به اکرام» می‌داند و آن را نه صرفاً یک صفت فردی، بلکه نشانه تکریم و حرمت‌گذاری به شخص تلقی می‌کند (۷). در فرهنگ دهخدا نیز کرامت دربرگیرنده مفاهیمی چون «ارزش، حرمت، حیثیت، بزرگواری، عزت، شرافت، شأن، جوانمردی و سخاوت» است (۸). این دامنه معنایی نشان می‌دهد که کرامت، فقط امری درونی و معنوی نیست، بلکه وضعیت اجتماعی و رابطه‌ای است که باید در رفتار دیگران نسبت به فرد نیز رعایت شود، از جمله در مواجهه با اطلاعات سلامت او.

محمدتقی جعفری تبریزی، میان دو بعد کرامت تمایز می‌گذارد: کرامت ذاتی (حیثیت طبیعی) که به جهت خلقت در وجود هر انسان مفروض است و سلب‌پذیر نیست و کرامت عرضی یا ارزشی که با کنش اخلاقی و رشد اختیاریِ فرد تقویت یا تضعیف می‌شود (۹). این دوگانه در آیه ۷۰ سوره اسراء: «وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ ... وَفَضَّلْنَاهُمْ عَلَى كَثِيرٍ مِمَّنْ خَلَقْنَا تَفْضِيلًا» منعکس است. آیه ۷۰ سوره اسراء کرامت را امتیازی عام برای نوع انسان می‌شناسد، نه امتیازی قراردادی یا مشروط. از این منظر، تعرض به حیثیت بیمار، از جمله افشای داده‌های سلامت جسمی، جنسی، روانی یا ژنتیکی او بدون ضرورت و رضایت، صرفاً نقض محرمانگی نیست، بلکه مداخله در کرامت نوع انسان تلقی می‌شود. نتیجه مستقیم این خوانش آن است که حمایت از داده سلامت در نظام مراقبت پزشکیِ دیجیتال باید در سطح «الزام هنجاری بنیادین» تعریف شود و نه فقط یک ملاحظه فنی یا اجرایی.

این تمایز میان کرامت ذاتی و کرامت ارزشی می‌تواند مبنای صورت‌بندی تعهدات نهادی در حوزه سلامت باشد. کرامت ذاتی مستلزم آن است که بیمار، حتی پیش از هر انتخاب یا رضایت خاص، در برابر تحقیر، برچسب‌گذاری و افشای اطلاعات هویتی و پزشکی‌اش مصون باشد. در سطح حقوقی و فناورانه، این به معنای ساخت نظامی است که از ابتدا مانع نشت و بازاستفاده غیر مجاز از داده‌های حساس سلامت شود. این ایده با مفهوم «حریم خصوصی از مرحله طراحی» («حریم خصوصی از مرحله طراحی» رویکردی است که الزامات صیانت از داده از بدو طراحی و معماری سامانه، به صورت پیش‌فرض و یکپارچه تعبیه می‌شود، نه به عنوان افزوده‌ای ثانویه در مراحل پایانی. در سطح اجرا، به جمع‌آوری حداقلی و هدفمند داده، تعیین روشن حدود استفاده و دوره نگهداری، کنترل دسترسی مبتنی بر نقش، رمزگذاری در ذخیره‌سازی و انتقال و رضایت قابل مشاهده، تفکیک‌پذیر و قابل بازپس‌گیری برای ذی‌نفع، متکی است (۱۰)) هم‌پوشانی دارد: حفاظت از داده نباید وظیفه‌ای پسینی و واکنشی باشد، بلکه باید در لایه معماری سامانه‌های مبتنی بر هوش مصنوعی ادغام شود. یکی از راهکارهای فنی کلیدی در این جهت، یادگیری توزیع‌شده است؛ مدلی که در آن الگوریتم تشخیصی هوش مصنوعی در همان محل نگهداری داده آموزش می‌بیند، بدون آنکه داده خام بیمار به یک مخزن مرکزی منتقل شود یا در اختیار بازیگران ثالث قرار گیرد (۱۱). ترجمه هنجاری این رویکرد چنین است: افشای داده سلامت بیمار (داده‌ای که در منطق

فقهی با حیثیت و آبروی او گره خورده)، حتی اگر در ظاهر «صرفاً داده تکنیکی» تلقی شود، باید مانند افشای «سرّ» او تلقی گردد، بنابراین نظام سلامت و ارائه‌دهندگان خدمات مبتنی بر هوش مصنوعی، مسئول پیشگیری فعال از هرگونه انتقال غیر ضروری داده خواهند بود.

در کنار این لایه مصون‌سازی پیش‌دستانه، کرامت عرضی به بعد مشارکت و عاملیت بیمار مربوط است. این بُعد اقتضا می‌کند که بیمار صرفاً «موضوع پردازش داده» نباشد، بلکه کنشگری آگاه در فرایند تصمیم‌سازی الگوریتمی باقی بماند. در حقوق سلامتِ دیجیتال، این ایده در قالب «رضایت پویا» («رضایت پویا» سازوکاری است که به جای اخذ یک‌باره و کلی رضایت، امکان اعلام، تفکیک، بازنگری و بازپس‌گیری رضایت را در طول زمان و به صورت مستمر برای هر دسته از داده و هر هدف پردازشی فراهم می‌کند. در سطح اجرا، از درگاه‌های کاربرمحور و داشبوردهای قابل فهم استفاده می‌شود تا بیمار برای هر کاربری (مراقبت مستقیم، پژوهش، آموزش الگوریتم و...) به طور جداگانه «اجازه یا عدم اجازه»، بازه زمانی، دامنه گیرندگان و شرایط اشتراک‌گذاری را تعیین و هر زمان بدون لطمه به کیفیت مراقبت، آن را اصلاح یا لغو کند (۱۲))، صورت‌بندی شده است: سازوکاری که به بیمار اجازه می‌دهد دامنه، مدت و سطح دسترسی به داده‌هایش را نه فقط در لحظه پذیرش خدمات درمانی، بلکه در طول زمان، به طور مستمر بازبینی، محدود، تمدید یا پس بگیرد (۱۳). چنین مدلی، رضایت را از یک امضای اداری در ابتدای پرونده پزشکی، به یک فرایند زنده و بازقابل مذاکره تبدیل می‌کند. از منظر هنجاری، این تحول به معنای آن است که حفظ آبرو و منع افشای اسرار (مفاهیمی که در فقه در زمره تکالیف قوی اخلاقی و اجتماعی قرار می‌گیرند)، باید در نظام سلامت امروز به صورت حق مستمر بیمار در کنترل پردازش الگوریتمی داده‌های خویش بازتاب یابد.

این تحلیل نشان می‌دهد پیوند مبانی فقهی کرامت با ابزارهای نوین حکمرانی داده، مانند حریم خصوصی مبتنی بر طراحی و رضایت آگاهانه پویا صرفاً جنبه نظری ندارد، بلکه قابلیت تبدیل‌شدن به تعهد حقوقی و استاندارد نظارتی را نیز دارد: نخست، کرامت ذاتی مبنای «مصونیت داده سلامت بیمار» است؛ داده سلامت باید به مثابه بخشی از شأن انسانی او فهم شود، بنابراین قابل معامله یا انتقال آزادانه نباشد؛ دوم، کرامت ارزشی مبنای «مشارکت مستمر بیمار در سرنوشت داده‌های خود» است، یعنی بیمار باید در جایگاه یک طرف فعال در تصمیم‌گیری الگوریتمی قرار گیرد، نه صرفاً منبع داده، بدین‌ترتیب، چهارچوب فقهی کرامت، در صورت ترجمه دقیق به زبان حقوق سلامت، می‌تواند پایه‌ای برای مسئولیت‌پذیری حرفه‌ای، پاسخگویی نهادی و تنظیم‌گری خاص سامانه‌های هوش مصنوعی در حوزه درمان و مراقبت بهداشتی فراهم کند. از منظر نگارندگان، با توجه به پیوند مستقیم میان کرامت انسان و محرمانگی داده با منابع فقهی و با در نظرگرفتن ظرفیت‌های فنی موجود مانند یادگیری توزیع‌شده و رضایت پویا، به نظر می‌رسد نظام سلامت ایران دیگر نمی‌تواند صرفاً به قواعد سنتی محرمانگی پزشکی اکتفا کند. مبنای کرامت ایجاب می‌کند که این بحث از سطح «توصیه اخلاقی» به سطح «الزام حقوقی» منتقل شود. به بیان مشخص‌تر: ۱ـ انتقال و تجمیع داده‌های سلامت بیمار بدون ضرورت و رضایت خاص باید به عنوان تعرض به کرامت ذاتی او ممنوع تلقی شود؛ ۲ـ بیمار باید صاحب یک حق مستمر و بازنگری‌پذیر در کنترل دسترسی الگوریتمی به داده‌های خود شناخته شود، نه صرفاً امضاکننده یک رضایت اولیه؛ ۳ـ ارائه‌دهندگان خدمات هوش مصنوعی در حوزه درمان باید نه فقط از حیث کارایی فنی، بلکه از حیث صیانت از «سرّ بیمار» و رعایت کرامت او، در برابر نهاد ناظر سلامت پاسخگو باشند. بر این اساس، کرامت بیمار باید به شاخص سنجش مشروعیت استفاده از هوش مصنوعی در سلامت تبدیل شود و نقض آن، نقض حداقل‌های قابل پذیرش در نظام سلامت محسوب گردد.

۲-۲. اصل لزوم کتمان سر: در فقه و اخلاق، «کتمان سر» صرفاً توصیه به نگفتن راز نیست، بلکه تثبیت یک حریم محرمانه پیرامون فرد است؛ حریمی که دسترسی به آن بدون اذن، هم از نظر اخلاقی مذموم و هم از نظر هنجاری قابل مؤاخذه دانسته شده است. فیض کاشانی افشای راز دیگری را

فعلی حرام و نوعی خیانت در امانت توصیف می‌کند، نه یک خطای سبک ارتباطی (۱۴). منابع روایی نیز دو تکلیف هم‌زمان را صورت‌بندی می‌کنند: نخست، شخص موظف است در افشای لایه‌های حساس زندگی خود بی‌مبالات نباشد و مراقب «پراکندگی کنترل‌نشده امور نهانی خویش» باشد («هَلَکَ مَن لَم یَحضُر أمرَهُ») (۱۵)؛ دوم، هر کس که رازی به او سپرده می‌شود مکلف به سکوت وفادارانه است و افشای آن «خیانت به امانت» تلقی می‌شود («مَن أفشی سرّاً استودعه فقد خانَهُ») (۱۵). بنابراین سکوت، یک لطف شخصی یا اقدام جوانمردانه صرف نیست، بلکه تعهدی است که نقض آن خیانت تلقی می‌گردد.

در بستر سلامت دیجیتال و سامانه‌های هوش مصنوعی، این منطق ابعاد تازه‌ای می‌یابد. بیمار در تعامل با سامانه‌های تشخیصی و پایشی نه فقط داده‌های زیستی و نتایج آزمایش، بلکه خصوصی‌ترین لایه‌های زندگی خود (وضعیت روانی، سابقه جنسی، تجربیات شخصی، مصرف مواد، بارداری و...) را در اختیار سیستم قرار می‌دهد. این اطلاعات از منظر این ادبیات، «سرّ» بیمار است نه صرفاً «داده پزشکی» (۱۶). تفاوت وضعیت کنونی با الگوی سنتی مراقبت آن است که این سر، دیگر نزد یک پزشک یا در یک پرونده ثابت باقی نمی‌ماند، بلکه در پایگاه‌های داده، مدل‌های یادگیرنده و خروجی‌های تحلیلی ثانویه تکثیر می‌شود. اگر این تکثیر و چرخش داده بدون مهار و بدون امکان سکوت رخ دهد، سرّ بیمار از حالت «امانت نزد امین» خارج و به «رازِ در گردش» بدل می‌شود؛ وضعیتی که مطابق منطق روایی، از سنخ خیانت است، حتی اگر افشا و بازتولید آن نه توسط یک فرد، بلکه از رهگذر سازوکار الگوریتمی رخ‌داده باشد (۱۷).

بر این مبنا، در عصر سلامت مبتنی بر هوش مصنوعی، کتمان سر باید به صورت اصل «کاهش جریان داده» فهم شود. تکلیف فقط منع افشای پسینی نیست، بلکه محدودکردن تولید، ثبت، تکثیر و دسترسی به راز بیمار از همان لحظه جمع‌آوری است. این را می‌توان «سکوت ساختاری» نامید: هرچه سامانه کمتر راز تولید و توزیع کند، نیاز به کنترل‌های جبرانی پس از نشت اطلاعات کاهش می‌یابد. این نگاه، تفاوت جدی با رویکردهای واکنشی کلاسیک محرمانگی دارد که مسأله را صرفاً در مرحله پس از افشا می‌بینند (۱۸).

فناوری‌های پیشرفته رمزنگاری و حریم داری ابزارهایی عملی برای نهادینه‌سازی «سکوت ساختاری» به شمار می‌آیند. در الگوی «رمزنگاری ویژگی‌مبنا» («رمزنگاری ویژگی مبنا» روشی است که قانونِ دسترسی را روی خودِ داده قفل می‌کند؛ فایل طوری رمز می‌شود که فقط کسانی که ویژگی‌های لازم (مثلاً نقش شغلی یا مجوز مشخص) را دارند بتوانند آن را باز کنند. مزیت این روش این است که اعمال دسترسی به سرور یا توافق‌های لحظه‌ای وابسته نیست و از همان ابتدا اصل «حدّ ضرورت» را اجرا می‌کند. در سلامت دیجیتال، این کار از پخش بی‌رویه اطلاعات جلوگیری می‌کند، البته مدیریت و ابطال کلیدهای دسترسی باید دقیق و به روز نگه داشته شود (۱۹))، داده سلامت از همان لحظه تولید به گونه‌ای رمز می‌شود که تنها دارندگان نقش‌ها یا ویژگی‌های از پیش تعریف‌شده با کلیدهای متناظر قادر به گشودن آن باشند (۲۰)، بدین‌ترتیب تصمیم درباره «چه کسی چه چیزی را ببیند» به زمان درخواست دسترسی موکول نمی‌شود، بلکه به صورت یک قاعده الزام‌آور در خود داده قفل می‌گردد و کنترل دسترسی را مستقل از سامانه‌های بیرونی تضمین می‌کند (۲۰). این سازوکار با منطق «کتمان سر» هم‌سو است: راز بیمار صرفاً نزد امانتدارانی که به صراحت مجاز شده‌اند «سپرده» می‌شود و برای سایر بازیگران اصولاً شنیدنی یا خواندنی نیست.

همچنین «محرمانگی تفاضلی» («محرمانگی تفاضلی» چهارچوبی ریاضی و هنجاری است که با افزودن «آشفتگی و اغتشاش کنترل‌شده» به خروجی‌های آماری، حضور یا عدم حضور یک فرد را از منظر استنباطی عملاً تمایزناپذیر می‌سازد. این «تصادفی‌سازی کالیبره شده» نسبت میان صیانت از حریم خصوصی و دقت تحلیلی را تنظیم می‌کند: هرچه شدت اغتشاش بالاتر رود، تضمین حریم قوی‌تر و کارایی آماری کمتر می‌شود (۱۹)) با افزودن نویز کنترل‌شده به خروجی‌های

تحلیلی سلامت، اجازه می‌دهد داده‌ها برای آموزش الگوریتم‌ها و تحلیل آماری استفاده شوند، بدون آنکه بتوان هویت بیمار یا جنبه‌های بسیار حساس زندگی او (مانند عادات جنسی، سابقه روان‌پزشکی یا وضعیت اعتیاد) را از نتایج بازسازی کرد (۲۱). این وضعیت در عمل برابر با «ابهام اجباری» است: سیستم حتی در هنگام پاسخ‌دادن ناگزیر است بخشی از راز را ناواضح کند. به تعبیر هنجاری، سامانه در مقام عمل، تعهد به کتمان را اجرا می‌کند، یعنی حتی وقتی سخن می‌گوید، به نحوی سخن می‌گوید که راز مستودَع قابل انتساب به صاحب راز نباشد (۲۱).

از منظر نگارندگان، با توجه به اینکه در منابع روایی افشای سر بیمار به مثابه خیانت تعریف شده است، می‌توان ادعا کرد که در نظام سلامت دیجیتال اصل لزوم کتمان سر باید به عنوان یک قاعده حاکم بر کل چرخه عمر داده فهم شود، نه صرفاً به عنوان محرمانگی حرفه‌ای پزشک. به طور خاص:

۱ـ ثبت و انباشت داده باید به حد ضرورت درمانی محدود شود و اطلاعاتی که صرفاً از حیث آبرویی و حیثیتی حساس‌اند، اما ارزش بالینی ندارند اصولاً نباید دیجیتالی و ذخیره‌ای شوند؛ این مرحله «پیشگیری از تولید راز قابل نشت» است.

۲ـ دسترسی باید از لحظه تولید داده مقید و قفل شود، با سازوکارهای سیاست‌محور مانند رمزنگاری مبتنی بر ویژگی که تعیین می‌کند چه نقشی در نظام مراقبت، چه سطحی از راز را می‌تواند ببیند.

۳ـ خروجی‌های پژوهشی و تحلیلی باید به طور سیستماتیک از طریق محرمانگی تفاضلی مبهم‌سازی شوند تا انتساب مستقیم راز به صاحب راز ناممکن باشد. بر این اساس، کتمان سر در عصر هوش مصنوعی به معنای «سکوت فردی پزشک» تقلیل‌پذیر نیست، بلکه اقتضا می‌کند کل سامانه بالینی و داده‌محور به گونه‌ای طراحی شود که اصولاً امکان نقض سکوت گسترده فراهم نشود. این جابه‌جایی از سکوت شخصی به سکوت سیستمی، ظرفیت آن را دارد که به زبان الزام نظارتی و مسئولیت حقوقی در حوزه سلامت دیجیتال ترجمه شود.

۳. سازوکار حقوقی صیانت از حریم خصوصی بیماران در به کارگیری هوش مصنوعی در مراقبت‌های بهداشتی و درمانی:

این بخش، سازوکارهای حقوقی صیانت از حریم خصوصی بیماران در کاربست هوش مصنوعی بالینی را با تمرکز بر تعیین حدود مشروع گردآوری، پردازش و باز استفاده از داده‌های سلامت و توزیع مسئولیت میان بازیگران درمانی و فناورانه تبیین می‌کند. در نظام تقنینی ایران، نسبت «اصول ۲۲ و ۲۵ قانون اساسی» با پردازش خودکار داده و نیز ظرفیت‌ها و کاستی‌های «قانون جرائم رایانه‌ای (به ویژه مواد ۲ و ۱۷)» از حیث جرم‌انگاری دسترسی و افشای غیر مجاز، الزامات «حکم قانون»، حد ضرورت درمانی و ثبت رد پای دسترسی بررسی می‌شود. در اتحادیه اروپا، منظومه حق‌مدار «مقررات عمومی حفاظت از داده‌ها» در کنار رژیم ایمنی‌محور «قانون هوش مصنوعی» و پشتوانه‌های قضایی دیوان عدالت اتحادیه اروپا واکاوی خواهد شد تا الگوی توأمان «حاکمیت بیمار بر داده» و «پاسخگویی پیشینیِ سامانه‌های پرخطر» به عنوان مرجع تطبیقی عرضه گردد.

۳-۱. نظام حقوقی ایران: نظام حقوقی ایران، هرچند هنوز فاقد یک رژیم اختصاصی و منسجم برای حکمرانی داده سلامت در بستر سامانه‌های هوش مصنوعی است، لکن دو ستون حقوقی نسبتاً صریح برای حمایت از بیمار در برابر مداخله فناورانه دارد: نخست، قانون اساسی جمهوری اسلامی ایران (به ویژه اصول ۲۲ و ۲۵)؛ دوم، قانون جرائم رایانه‌ای ۱۳۸۸ (به ویژه مواد ۲ و ۱۷). کنار هم قراردادن این دو ستون نشان می‌دهد که از منظر هنجاری، حیثیت و حریم بیمار در نظام سلامت دیجیتال باید موضوع حمایت پیشینی، اجرایی و کیفری باشد، اما شکاف‌های مهمی در اجرا و در نسبت با بازیگران خصوصی وجود دارد.

از منظر قانون اساسی، اصل ۲۲ اعلام می‌کند که «حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است، مگر در مواردی که قانون تجویز کند.» این اصل کرامت و حریم شخصی را در مرتبه حمایت اساسی قرار می‌دهد و هرگونه تعرض را جزء با مجوز صریح قانونی مردود می‌شمارد

(۲۲). در حوزه سلامت هوشمند، این امر بدان‌معناست که دسترسی، استخراج یا پردازش خودکار داده‌های پزشکی بیمار توسط سامانه‌های هوش مصنوعی فقط زمانی موجه است که مستند به مبنای قانونی مشخص و اعلام‌شده باشد، نه صرفاً به قرارداد داخلی مرکز درمان یا ضرورت ادعایی پیمانکار فناور (۲۳). بر مبنای همین قیاس، اصل ۲۵ که «بازرسی و نرساندن نامه‌ها، ضبط و فاش‌کردن مکالمات تلفنی، افشای مخابرات...، استراق سمع و هرگونه تجسس» را جزء به حکم قانون ممنوع می‌داند، در ویزیت از راه دور مستقیماً قابل اعمال است: ضبط، نگهداری و تحلیل خودکار مکالمه ویدیویی یا صوتی بیمار یا پزشک توسط یک سامانه پردازش گفتار یا پردازش زبان طبیعی که حاوی لایه‌های عمیق روانی، جنسی و خانوادگی بیمار است، بالقوه در معرض منع تجسس قرار دارد و تنها در صورت وجود مجوز قانونی صریح (و نه صرف ادعای «بهبود مستندسازی») می‌تواند موجه باشد (۲۴).

در کنار این حمایت اساسی، قانون جرائم رایانه‌ای برای آن پشتوانه کیفری فراهم می‌آورد. ماده ۲، شنود «محتوای در حال انتقال ارتباطات غیر عمومی» را جرم‌انگاری کرده و برای آن حبس و جزای نقدی مقرر می‌دارد. در محیط سلامت دیجیتال، «ارتباط غیر عمومی» فقط تماس تلفنی نیست، بلکه جریان زنده داده‌درمانی بیمار است: تصاویر پزشکی، ویدیوی زنده جراحی یا آندوسکوپی، علائم حیاتی لحظه‌ای، فایل‌های صوتی جلسات روان‌درمانی و گزارش‌های بالینی که بین تجهیزات، پرونده الکترونیک سلامت و ماژول‌های تحلیلی مبتنی بر یادگیری ماشین مبادله می‌شود (۲۵). هرگونه رهگیری، وارسی عمیق بسته‌های داده، ثبت رویدادهای سامانه یا استخراج این داده در حین انتقال، اگر خارج از ضرورت درمانی همان بیمار یا بدون رضایت معتبر او انجام شود، حتی اگر با عنوان «کنترل کیفیت» یا «آموزش الگوریتم» توجیه شود، می‌تواند مصداق «شنود غیر مجاز» تلقی گردد (۲۶). اهمیت این برداشت آن است که حمایت کیفری ماده ۲ پیشینی است: بیمار لازم نیست ابتدا دچار بی‌آبرویی علنی شود؛ همین مداخله غیر مجاز در جریان زنده داده سلامت بالقوه قابل تعقیب است (۲۳).

ماده ۱۷ قانون جرائم رایانه‌ای لایه دوم حمایت را تشکیل می‌دهد: «انتشار یا در دسترس‌پذیری» صوت، تصویر، فیلم خصوصی یا «اسرار دیگری» بدون رضایت، در صورتی که موجب ضرر یا «عرفاً موجب هتک حیثیت» شود، قابل مجازات است. در بستر درمان، ویدیوی جراحی، اسکن‌های تصویربرداری، تصویر از نواحی حساس بدن بیمار یا فایل صوتی جلسه روان‌درمانی، نمونه روشن اسرارند، زیرا در اوج آسیب‌پذیری و اعتماد تولید شده‌اند و اصلاً برای چرخش بیرون از تیم درمانی مقصود نشده‌اند (۲۷). رویه قضایی این برداشت را تثبیت کرده است: شعبه ۴۱ دادگاه تجدید نظر تهران در دادنامه شماره ۹۷۰۹۹۷۲۲۹۴۱۰۰۴۸۲ (۱۳۹۷ ش.) اعلام کرد ارسال تصویر فرد حتی در یک «گروه محدود» پیام‌رسان، «قراردادن در دسترس دیگران» است (۲۵)؛ دیوان عالی کشور نیز در رأی شماره ۹۴۰۹۹۸۲۹۲۵۴۰۱۴۰۷ (۱۳۹۵ ش.) تصریح نمود که برای احراز «هتک حیثیت عرفی» لازم نیست محتوا عریان یا جنسی آشکار باشد، بلکه معیار، قابلیت واردساختن لطمه اعتباری نوعی است (۲۸). نتیجه مستقیم برای سلامت دیجیتال این است که اشتراک‌گذاری فایل بالینی بیمار، حتی اگر در یک گروه محدود رزیدنت‌ها، تیم پژوهش یا شرکت فناور برای «آموزش مدل» بدون رضایت آگاهانه و مشخص بیمار، می‌تواند ذیل ماده ۱۷ وصف کیفری یابد، زیرا بیمار به طور پیش‌فرض راضی به دیده‌شدن بدن، روان یا سابقه درمانی‌اش بیرون از دایره درمان مستقیم نیست.

با این حال، هر دو ستون حمایتی دچار خلأهای هنجاری و اجرایی‌اند. در سطح اساسی، اصول ۲۲ و ۲۵ قانون اساسی استثنا را فقط «به حکم قانون» می‌پذیرند، اما نظام سلامت دیجیتال در ایران هنوز فاقد آیین‌نامه‌های شفاف، اختصاصی و عام‌الالزام برای پردازش خودکار داده درمانی است. در عمل، بیمارستان یا پیمانکار فناوری سلامت گاه استناد می‌کند به «آیین‌نامه داخلی» یا «رضایت کلی بدو پذیرش»، در حالی که این‌ها در مرتبه «حکم قانون» قرار نمی‌گیرند و به دشواری

می‌توان آن‌ها را ذیل استثنای اصول ۲۲ و ۲۵ قرارداد. پیامد آن، ناهمگونی و کاهش پیش‌بینی‌پذیری حقوقی بیمار است و ایجاد وضعیتی که در آن دسترسی فناورانه به حریم درمانی بیمار عملاً می‌تواند خارج از چهارچوب نظارت عمومی اتفاق بیفتد (۲۴). همین خلأ در قانون جرائم رایانه‌ای نیز بازتاب دارد: ماده ۲ «غیر مجاز» را دقیقاً خط‌کشی نکرده است، در حالی که همان کانال فنی که برای ایمنی درمان و پایش علائم حیاتی لازم است، می‌تواند برای استخراج ثانویه و انباشت بانک داده باارزش پژوهشی و تجاری نیز به کار رود و ماده ۱۷ که به «هتک حیثیت عرفی» متکی است، عمدتاً نتیجه‌محور باقی می‌ماند و سلب حاکمیت بیمار بر داده زیستی‌اش را پیش از وقوع بی‌آبرویی علنی به سختی پوشش می‌دهد. در کنار آن، ضعف ثبت منظم رویدادهای دسترسی و رهگیری مسیر خروج فایل‌های پزشکی در برخی مراکز درمانی و شرکت‌های فناور، بار اثبات را در عمل بر دوش خود بیمار می‌گذارد و توان بازدارندگی واقعی را محدود می‌کند. سقف دو سال حبس و جزای نقدی فعلی نیز، با توجه به ارزش اقتصادی و علمی مجموعه‌های تصویری پزشکی برای آموزش مدل‌های تشخیصی، لزوماً بازدارنده نیست و ممکن است صرفاً «هزینه قابل جذب» تلقی شود (۲۳).

از منظر نگارندگان برای آنکه این دو ستون حقوقی عملاً بتوانند حریم و حیثیت بیمار را در زیست‌بوم سلامت مبتنی بر هوش مصنوعی حمایت کنند، سه‌گام هنجاری ضروری است:

۱ـ تبیین «حکم قانون» در سلامت دیجیتال: وزارت بهداشت باید آیین‌نامه‌های شفاف و قابل استناد تدوین و اعلام کند که دقیقاً چه داده‌ای، برای چه هدفی، توسط کدام نهاد و تا چه مدت می‌تواند به طور خودکار استخراج، ذخیره و پردازش شود. رضایت کلی بدو پذیرش بیمارستانی یا مصالحه قراردادی با پیمانکار فناور جای این مرتبه را نمی‌گیرد و کف حمایتی قانون اساسی (اصل ۲۲ و اصل ۲۵) را تأمین نمی‌کند.

۲ـ بازتعریف شنود و انتشار در منطق سلامت دیجیتال: هرگونه رهگیری یا استخراج جریان زنده داده‌درمانی برای هدفی فراتر از مراقبت همان بیمار، از جمله آموزش الگوریتم، تحلیل ثانویه یا توسعه محصول بدون رضایت آگاهانه و مشخص باید به صراحت ذیل «شنود غیر مجاز» ماده ۲ قرار گیرد و بر مبنای رویه دادگاه تجدید نظر تهران و دیوان عالی کشور، به اشتراک‌گذاری فایل‌های درمانی بیمار، حتی در حلقه محدود آموزشی و پژوهشی باید «در دسترس‌پذیری» به معنای ماده ۱۷ تلقی شود، بی‌آنکه نیاز به انتشار عمومی یا محتوای عریان باشد؛ کافی است قابلیت لطمه حیثیتی نوعی احراز شود.

۳ـ الزام به رد پا و پاسخگویی: مراکز درمانی و پیمانکاران فناور باید مکلف شوند رویدادهای دقیق دسترسی و مسیر خروج هر فایل پزشکی را ثبت و نگهداری کنند، به نحوی که در دادرسی کیفری و انتظامی قابل استناد باشد. بدون این لایه اثباتی، مسئولیت‌پذیری واقعی شکل نمی‌گیرد و حمایت قانون اساسی و کیفری به سطح اعلام ارزشی تنزل می‌کند.

چنانچه این گام‌ها تثبیت نشوند، اصول ۲۲ و ۲۵ قانون اساسی که ظاهراً بیمار را در برابر تعرض به حیثیت، حریم گفتگو و حریم درمانی‌اش مصون می‌دانند و نیز مواد ۲ و ۱۷ قانون جرائم رایانه‌ای که ظاهراً شنود و در دسترس‌پذیری اسرار درمانی را جرم‌انگاری می‌کنند، در زیست‌جهان سلامت مبتنی بر هوش مصنوعی بیش از آنکه سازوکار حمایت فعال باشند، به بیانیه‌های ارزش‌گذارانه نزدیک خواهند شد. با این تثبیت اما همین دو پایه می‌توانند به یک رژیم پاسخگویی پیشینی و پسینی تبدیل شوند: پاسخگویی در لحظه دسترسی به داده، در لحظه انتقال و در لحظه بروز لطمه به حیثیت بیمار.

۳-۲. نظام حقوقی اتحادیه اروپا: مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا (GDPR: General Data Protection Regulation)، داده سلامت را «داده ویژه و حساس» می‌داند و اصل را بر منع پردازش آن می‌گذارد؛ پردازش فقط در موارد مضیق مجاز است، مانند رضایت صریح و مشخص بیمار برای یک هدف معین، ضرورت درمانی، ضرورت بهداشت عمومی یا پژوهش علمی با تضمین‌های فنی و سازمانی کافی (۲۹). مقررات عمومی حفاظت از داده‌ها علاوه بر محرمانگی، برای بیمار حقوق اجرایی قائل است، از جمله حق دسترسی و اطلاع از هدف پردازش، حق اصلاح، حق

محدودکردن پردازش، حق انتقال داده به ارائه‌دهنده دیگر و در مواردی حق حذف «حق فراموش‌شدن» (۳۰). بنابراین بهره‌بردار یک سامانه هوش مصنوعی تشخیصی یا تصمیم‌یار باید از پیش مبنای قانونی پردازش داده را مستند کرده و در صورت مطالبه، منبع داده، هدف، مدت نگهداری و حدود اشتراک‌گذاری آن را به طور قابل حسابرسی توضیح دهد؛ این وضعیت در ادبیات اتحادیه اروپا به عنوان «حاکمیت فرد بر داده سلامت خویش» صورت‌بندی شده است (۲۹).

رویه دیوان عدالت اتحادیه اروپا این حقوق را ضمانت‌دار کرده است. در آرای «گوگل اسپانیا (Google Spain) و «گوگل علیه آژانس اسپانیایی حفاظت از داده‌ها» و «ماریو کوستخا گونزالس جی‌سی (Mario Kostkha Gonzales J.C)» و دیگران علیه کمیسیون ملی انفورماتیک و آزادی‌ها فرانسه (GC and Others v Commission Nationale de L'informatique et des Libertés (CNIL), Case C-136/17 (24 September 2019)» و «گوگل علیه کمیسیون ملی انفورماتیک و آزادی‌ها»، دیوان تصریح کرد که حتی موتور جستجو یک «کنترل‌کننده داده» است و می‌توان آن را ملزم کرد پیوند میان نام فرد و اطلاعات حساس یا لطمه‌زننده به حیثیت او را حذف یا محدود کند و این تکلیف، دست کم در قلمرو اتحادیه، می‌تواند بر شرکت‌های فناوری تحمیل شود، حتی اگر زیرساخت آن‌ها خارج از اتحادیه باشد (۳۱). افزون بر این، دیوان اجازه داده است محاکم ملی سکوهای میزبانی محتوا را نه فقط به حذف محتوای ناقض حیثیت فرد، بلکه به حذف «محتوای معادل» نیز ملزم کنند و این الزام می‌تواند فرامرزی عمل کند (۳۱). پیامد عملی در حوزه سلامت این است که بیمار مواجه با افشای تصویر پزشکی تحقیرکننده یا اطلاعات درمانی انگ‌زننده فقط متکی به شکایت از منبع اولیه داخلی نیست، می‌تواند مستقیماً از خود سکو یا موتور جستجو مطالبه حذف و محدودسازی پیوند هویتی کند و سکو مکلف به اقدام فعال است.

موازی با این رژیم حق‌محور، اتحادیه اروپا «قانون هوش مصنوعی ((Artificial Intelligence Act (AI Act)» را تصویب کرده است که سامانه‌های هوش مصنوعی تشخیصی، تصمیم‌یار بالینی و پشتیبان درمانی را «پرخطر» می‌شمارد، چون خروجی آن‌ها می‌تواند مستقیماً بر سلامت و حقوق بنیادین بیمار اثر بگذارد (۳۲). این قانون برای این سامانه‌ها تکالیف پیشینی و مستمر تعریف می‌کند: مدیریت ریسک در کل چرخه عمر، تضمین کیفیت و نبود سوگیری ناموجه (به ویژه نسبت به گروه‌های آسیب‌پذیر)، مستندسازی فنی قابل حسابرسی، پیش‌بینی نظارت و مداخله مؤثر انسانی، تضمین استحکام و دقت و نیز پایش پس از استقرار و گزارش‌دهی رویدادهای مخاطره‌آمیز (۳۳).

تفاوت هنجاری روشن است، مقررات عمومی حفاظت از داده‌ها یک رژیم حق‌محور است که مشروعیت پردازش و کنترل بیمار بر داده سلامت خود را محور قرار می‌دهد (۳۲)، اما قانون هوش مصنوعی یک رژیم ایمنی و مسئولیت‌پذیری فناورانه است که توسعه‌دهنده و بهره‌بردار سامانه را از ابتدا در وضعیت پاسخگویی مهندسی و سازمانی قرار می‌دهد و اجازه نمی‌دهد مسئولیت به «الگوریتم» حواله شود (۳۳).

با وجود این نقاط قوت، سه خلأ اساسی باقی می‌ماند: نخست، هر دو سازوکار عمدتاً پسینی‌اند: بیمار باید ابتدا متوجه افشا یا لطمه حیثیتی بشود و سپس سازوکار اعتراض و حذف را فعال کند که در زمینه سلامت، جایی که فرد از نظر جسمی و روانی در وضعیت آسیب‌پذیر است، عملاً بار پیگیری را بر دوش همان فرد آسیب‌پذیر می‌گذارد (۳۴)؛ دوم، دیوان عدالت با واگذاری تکلیف حذف (و حتی حذف «محتوای معادل») به سکوهای خصوصی، عملاً تشخیص اینکه چه چیزی «هتک حیثیت بیمار» است و چه چیزی «افشای مشروع خطای نظام درمانی» را تا حدی به بازیگران اقتصادی واگذار کرده است، این «خصوصی‌سازی تشخیص کرامت» یک ریسک هنجاری است (۳۴)؛ سوم، در قانون هوش مصنوعی اتحادیه اروپا هنوز انتساب مسئولیت نهایی در صورت زیان بالینی ناشی از خطای الگوریتمی کاملاً شفاف نشده است: آیا پاسخگو توسعه‌دهنده است، عرضه‌کننده سامانه است یا ارائه‌دهنده خدمت درمانی که سامانه را به کار گرفته است؟ این «شکاف انتساب

مسئولیت» همچنان به قواعد صریح مسئولیت محصول و مسئولیت حرفه‌ای نیاز دارد (۳۴).

از منظر نگارندگان اتحادیه اروپا سه‌لایه مکمل را هم‌زمان به کار گرفته است: ۱ـ لایه حق‌مدار مقررات عمومی حفاظت از داده‌ها که بیمار را دارنده اختیار مداخله در گردآوری، نگهداری، پردازش و انتشار داده سلامت خود می‌شناسد. ۲ـ لایه قضایی و اجرایی دیوان عدالت که سکوهای دیجیتال را به ضامن فعال کرامت و آبروی بیمار تبدیل کرده و راه مطالبه مستقیم از آن‌ها را برای بیمار باز کرده است. ۳ـ لایه فناورانه و پیشینی قانون هوش مصنوعی که سامانه‌های پرخطر تشخیصی و درمانی را از ابتدا در وضعیت ریسک‌مدیری و نظارت انسانی مؤثر قرار می‌دهد. با این حال، تا زمانی که بار پیگیری اولیه همچنان بر دوش خود بیمار باقی بماند و مسئولیت نهایی در خطای الگوریتمی روشن نشود، خطر این وجود دارد که این رژیم پیشرفته در لحظه واقعی آسیب بالینی به جای حمایت فوری، صرفاً سازوکار اداری و منازعه بر سر صلاحیت تولید کند. در این خصوص پیشنهاد می‌شود: نخست، با جابه‌جایی بار اقدام از دوش بیمار به دوش عرضه‌کننده سکو و نهاد ناظر، سازوکارهای پیش‌دستانه الزام‌آور مانند «رصد خودکار مخاطرات»، «رابط واحد رسیدگی و حذف فوری» و «اعلام الزامی و بی‌درنگ نقض داده» برقرار شود؛ دوم، برای رفع ابهام در انتساب، نظام مسئولیت ترکیبی پیش‌بینی گردد: فرض تقصیر یا مسئولیت شبه‌محض برای تصمیم‌های بالینی پرخطر برآمده از سامانه، همراه با الزام به ثبت رد پای قابل حسابرسی، بیمه اجباری و تقسیم مسئولیت میان توسعه‌دهنده، بهره‌بردار و ارائه‌دهنده خدمت.

۴. چالش‌های اخلاقی کاربست هوش مصنوعی در مراقبت‌های بهداشتی و درمانی: در این بخش، چهارچوب اخلاقی کاربست هوش مصنوعی در سلامت با دو محور بررسی می‌شود: صیانت از حریم خصوصی و امنیت داده در معماری‌های چندبازیگری و بازطراحی رضایت از «امضای اولیه» به فرایندِ اعمال‌پذیر و بازبینی‌شونده که در ادامه بدان‌ها می‌پردازیم.

۴-۱. حفظ حریم خصوصی و امنیت داده‌های بیمار: سامانه‌های هوش مصنوعی در مراقبت سلامت به داده‌هایی عمیقاً هویتی و غیر قابل جبران مانند سوابق الکترونیک سلامت، داده‌های دارویی و تشخیصی، تصاویر پزشکی، داده‌های ژنومی، علائم حیاتی لحظه‌ای و حتی شاخص‌های رفتاری و سبک زندگی دسترسی پیدا می‌کنند (۳۶). برخلاف مدل سنتی که این داده نزد یک ارائه‌دهنده درمانی می‌مانْد، در معماری هوش مصنوعی این داده میان چند بازیگر اعم از مرکز درمانی، شرکت توسعه‌دهنده الگوریتم، زیرساخت پردازش ثالث و حتی نهاد پژوهشی یا صنعتی بازآموزنده مدل در گردش است و همین تکثر دسترسی ریسک نقض محرمانگی و بهره‌برداری ثانویه را بالا می‌برد (۳۶)، هرچند ابزارهایی چون رمزگذاری سرتاسری، کنترل سطح‌بندی‌شده دسترسی، ثبت و ممیزی کامل دسترسی‌ها، یادگیری فدرال و حریم‌داری تفاضلی به عنوان لایه‌های ضروری حفاظت مطرح شده‌اند (۳۸)، لکن ادبیات اخیر نشان می‌دهد که در داده‌های نایاب یا به شدت متمایز (مثلاً جهش ژنتیکی خاص یا بیماری نادر)، بازشناسایی فرد، حتی پس از ناشناس‌سازی نیز ممکن است و این می‌تواند به انگ‌زنی اجتماعی، تبعیض بیمه‌ای یا محدودیت شغلی بینجامد، یعنی پیامد تنها حیثیتی نیست، بلکه مادی و ساختاری است (۳۸). از منظر انتقادی، مشکل فقط خطر افشا نیست، بلکه شیوه نگاه به بیمار است، در بسیاری از پیاده‌سازی‌های تجاری و پژوهشی، داده بیمار عملاً به مثابه «سوخت مدل» تلقی می‌شود و نه امتداد شأن و هویت او، در نتیجه، رابطه درمانی مبتنی بر اعتماد می‌تواند به رابطه استخراج داده با منطق ریسک اطلاعاتی تنزل یابد، حتی اگر از نظر فنی «ایمن» مدیریت شده باشد (۳۹).

از منظر نگارندگان، نقطه کانونی صرفاً پیاده‌سازی ابزارهای امنیتی نیست، بلکه تعیین و التزام به «حد ضرورت» است؛ باید صریحاً تفکیک شود کدام داده برای مراقبت یا نظارت بالینی ضرورت دارد و کدام داده صرفاً به دلیل ارزش پژوهشی یا تجاری جمع‌آوری می‌شود؛ در غیر این صورت، مرز میان مراقبت مشروع و استخراج مستمر داده مخدوش می‌شود و

کرامت بیمار به عنوان صاحب داده، نه منبع داده، تضعیف خواهد شد. بر همین مبنا، نخست «قاعده حد ضرورت پیش‌فرض» باید به صورت الزام اجرایی نهادینه شود: انجام ارزیابی اثر پردازش پیش از هر پروژه، تنظیم صورت‌جلسه توجیهی ضرورت برای هر قلم داده، حذف و غیر فعال‌سازی خودکار اقلام غیر لازم و مشروط‌سازی هر دسترسی فراتر از ضرورت به مجوز مستقل همراه با ثبت رد پا؛ دوم، «مدیریت رضایت و شفافیت کاربری» به نحو اعمال پذیر برای خود بیمار برقرار گردد. برای مثال ایجاد داشبوردی که تفکیک استفاده درمانی، پژوهشی و تجاری و امکان بازپس‌گیری رضایت بدون تأثیر بر کیفیت درمان را به همراه حسابرسی‌های دوره‌ای توسط مرجع ثالث و ضمانت اجراهای معتبر علیه بهره‌برداری ثانویهِ بی‌رضایت (از تعلیق سامانه تا جریمه و محرومیت قراردادی) فراهم کند.

۴-۲. جمع‌آوری داده و رضایت آگاهانه: زیرساخت سلامت هوشمند فقط به پرونده پزشکی سنتی متکی نیست، بلکه داده‌های بسیار گسترده‌تری را از حسگرهای پوشیدنی، پایش خانگی علائم حیاتی، الگوی خواب و تغذیه، مصرف دارو و حتی شاخص‌های رفتاری و شناختی ثبت‌شده توسط تلفن همراه و فنوتیپ‌سازی دیجیتال گردآوری و بازاستفاده می‌کند (۴۰). در چنین محیطی، رضایت کلی و یک‌باره در ابتدای فرایند درمان دیگر کفایت اخلاقی ندارد.

استاندارد اخلاقی معاصر، رضایت را یک فرایند پویا و قابل بازبینی می‌داند: بیمار باید بداند چه نوع داده‌ای جمع می‌شود، برای چه اهدافی (مراقبت مستقیم یا نیز آموزش مدل، پژوهش و توسعه محصول تجاری آتی) استفاده می‌شود و بتواند برخی استفاده‌ها را مجاز و برخی دیگر را ممنوع کند و بعداً بدون تنزل کیفیت درمان آن رضایت را پس بگیرد (۴۱). به همین دلیل، رضایت آگاهانه در این فضا باید به «مدیریت رضایت» تبدیل شود، یعنی سامانه باید امکان مشاهده، اصلاح و لغو دامنه رضایت را در طول درمان برای خود بیمار فراهم کند، نه فقط در یک فرم اولیه (۴۲).

انتقادی که بدین امر وارد است این است که بسیاری از سامانه‌های هوش مصنوعی، به ویژه مبتنی بر یادگیری عمیق، حتی برای متخصصان هم کاملاً تبیین‌پذیر نیستند و این محدودیت شفافیت، دسترسی بیمار به «آگاهی واقعی» از پیامدهای بازاستفاده از داده‌اش را محدود می‌کند (۴۳).

از منظر نگارندگان، کانون بحث، «اختیار اعمال‌پذیر» است نه صرفاً اطلاع‌رسانی. رضایت در نظام سلامت مبتنی بر هوش مصنوعی فقط زمانی معتبر است که معماری نظام امکان اجرای واقعی آن را فراهم کند: استفاده‌های ثانویه (آموزش مدل، پژوهش، توسعه محصول) به صورت پیش‌فرض ممنوع بوده و صرفاً با «پیوستن آگاهانه و محدود به زمان» فعال شوند؛ دامنه رضایت به صورت لایه‌بندی‌شده بر حسب نوع داده و سطح ریسک تفکیک گردد و بیمار در یک «داشبورد رضایت» بتواند هر زمان اجازه‌هایش را ببیند، جزئی‌سازی کند یا بی‌هیچ پیامد درمانی باز پس گیرد. برای جبران تبیین‌ناپذیری مدل‌های پیچیده، لایه‌های تبیین کاربرمحور (از جمله برچسب ریسک تصمیم، خلاصه منطق سامانه در حد قابل فهم بالینی و پیامدهای محتمل برای کاربردهای ثانویه) همراه با «رسید رضایت» و «رد پای قابل حسابرسی دسترسی‌ها» در اختیار بیمار قرار گیرد و نیز مسیر اعتراض، توقف پردازش و ارجاع به بازبینی انسانی در تصمیم‌های پرمخاطره از پیش تعریف و قابل دسترس باشد. این مجموعه، رضایت را از یک امضای اداری به حقی زنده و اعمال‌پذیر تبدیل می‌کند و نسبت میان ضرورت درمانی و بهره‌برداری ثانویه را به صورت عملیاتی، شفاف و قابل پاسخگویی تنظیم می‌سازد.

۵. استانداردهای اخلاقی برای کاربست هوش مصنوعی در مراقبت‌های بهداشتی و درمانی

گسترش کاربری هوش مصنوعی در مراقبت سلامت، فهم سنتیِ محرمانگی، رضایت و امنیت داده بیمار را ناکافی کرده و ارزیابی هنجاری تازه‌ای می‌طلبد. در این چهارچوب، داده سلامت به مثابه «امانت حیثیتی» تلقی می‌شود و هر مداخله باید بر اصل ضرورت، شفافیت نقش سامانه و امکان اعمال اراده و کنترل مستمر

بیمار استوار باشد. آنچه در پی می‌آید، تصویری یکپارچه از مخاطرات و الزامات اخلاقی متناظر، همراه با نقد هنجاری و پیشنهادهای عملی برای بازآرایی مسئولیت‌ها در زنجیره سلامت دیجیتال ارائه می‌کند.

۵-۱. شفاف‌سازی نحوه استفاده از داده‌ها: در سطح استاندارد اخلاقی، شفاف‌سازی به معنای تبیین پیشینیِ نقش سامانه در مسیر مراقبت، ترسیم حدود مداخله آن در تصمیم‌گیری درمانی و تعیین مرجع مسئول پاسخگویی نسبت به پیامدهای خروجی‌های سامانه است، به گونه‌ای که برای بیمار و تیم بالینی روشن باشد آیا سامانه صرفاً ابزار تحلیلی اولویت‌بندی و علامت‌گذاری است یا توصیه درمانی تولید می‌کند، آیا نتیجه آن صرفاً نقش کمکی دارد یا مبنای اقدام بالینی قرار می‌گیرد و در صورت خطا کدام بازیگر حرفه‌ای اعم از توسعه‌دهنده، سازمان ارائه‌دهنده خدمت یا متخصص انسانی پاسخگو خواهد بود (۴۴). تحقق عملی این استاندارد مستلزم مستندسازی نهادی و قابلیت حسابرسی است: ثبت منظم ورودی‌های داده، مستندات فنی و منطق سامانه و مدل، نقاط اعمال قضاوت انسانی و «مسیر تصمیم» برای بازبینی حرفه‌ای پسینی (۴۵). از منظر انتقادی، مطالبه شفافیت زمانی واجد اثر هنجاری است که با الزامات طراحی قابل توضیح و مصنوعات فنی استاندارد مانند «مدل‌کارت» و «برگ‌اطلاعات داده‌ها» همراه شود، در غیر این صورت به اطلاع‌رسانی صوری تقلیل یافته و بنیانی برای پاسخگویی مؤثر فراهم نمی‌کند (۴۶).

از منظر نگارندگان، شفافیت نقش، زیربنای توزیع منصفانه مسئولیت و مانع شکل‌گیری «منطقه‌های خاکستری مسئولیت‌گریز» در تصمیم‌گیری بالینی است؛ پیشنهاد می‌شود بسته حداقلی مستندسازی (شامل ارزیابی اثر، مدل‌کارت و برگ‌اطلاعات داده‌ها) و رویه‌های بازبینی قابل حسابرسی، به صورت الزام نهادی پیش از استقرار سامانه تعریف و اجرا شود.

۵-۲. احترام به خودمختاری و حریم خصوصی بیمار: اصل خودمختاری اقتضا دارد بیمار بتواند به صورت آگاهانه و داوطلبانه درباره مسیر مراقبت و میزان اتکای فرآیند درمان به سامانه‌های هوش مصنوعی تصمیم بگیرد. این الزام اخلاقی در دو بعد به هم‌پیوسته تحقق می‌یابد: نخست، «قابلیت رجوع به انسان» و «قابلیت اعتراض و بازبینی»، بدین‌معنا که بیمار در تصمیم‌های پرمخاطره امکان درخواست ارزیابی انسانی مستقل، اخذ رأی دوم و بازبینی تصمیم پشتیبانی‌شده توسط سامانه را به طور عملی و از پیش‌طراحی‌شده در اختیار داشته باشد (۴۷)؛ دوم، «مرزبندی حریم خصوصی در مواجهه بالینی»، یعنی التزام به حداقل‌گرایی داده‌ای در تعامل با بیمار، تفکیک روشن میان داده‌های واقعاً لازم برای مراقبت و داده‌های اختیاری و پرهیز از تبدیل تشخیص بالینی به فرایند استخراج گسترده داده برای مقاصد فرعی خارج از نیاز مستقیم مراقبت (۴۸).

از منظر انتقادی، اتکای افراطی به خروجی‌های غیر توضیح‌پذیر، توان اعمال اراده آگاهانه بیمار را محدود و «رضایت» را به تشریفات اداری فروکاست می‌دهد، بنابراین ترجیح سامانه‌های تبیین‌پذیر یا دست‌کم فراهم‌کردن توضیح‌های کاربرمحور در تصمیم‌های پرمخاطره یک الزام هنجاری است (۴۸).

از منظر نگارندگان، صیانت از خودمختاری زمانی معنادار است که مسیر جایگزین انسانی برای تصمیم‌های پرخطر، امکان اعتراض و بازبینی مؤثر و مرزبندی شفاف داده‌های ضروری در مواجهه بالینی توأمان برقرار باشد؛ پیشنهاد می‌شود این سه شرط به صورت رویه‌های عملیاتی الزام‌آور، در موافقت‌نامه‌های خدمت و پروتکل‌های پذیرش سامانه‌های هوش‌محور درج و اجرا شود.

نتیجه‌گیری

منطق فقهی کرامت ذاتی و قاعده لزوم کتمان سرّ، داده‌های پزشکی بیمار را «امانت حیثیتی» می‌بینند و هر تعرض بی‌ضابطه را نقض وفاداری می‌داند. از این رو همه بازیگران عرصه سلامت از مرکز درمان تا پیمانکار و پردازشگر در مقام «امین» قرار می‌گیرند. پیام هنجاری قواعد فقهی روشن است: معماری داده باید بر «کاهش جریان داده» مبتنی بر جمع‌آوری و ثبت داده‌ها تا حد ضرورت درمانی، پرهیز از انباشت ابعاد غیر لازم زندگی بیمار، قفل‌گذاری دسترسی از

لحظه تولید و ابهام‌سازی کنترل‌شده در خروجی‌ها برای جلوگیری از انتساب مستقیم به افراد بنا شود، بدین‌سان، محرمانگی از «سکوت فردیِ پزشک» به «سکوت ساختاری سامانه» ارتقا می‌یابد و به الزام طراحی فنی و مسئولیت نهادی قابل مطالبه تبدیل می‌شود.

نظام حقوقی داخلی، از حیث اصول اساسی و قواعد کیفری، ظرفیت تبدیل این درک هنجاری به ضمانت اجرا را دارد، اما میان ظرفیت و اجرا هنوز شکاف معناداری باقی است. در سطح قانون اساسی، حیثیت و حریم بیمار مصون و هرگونه استراق و تجسس در ارتباطات حساس جزء به حکم صریح قانون ممنوع است؛ در سطح کیفری نیز شنود غیر مجاز و در دسترس‌پذیری اسرار قابل تعقیب تلقی می‌شود، به گونه‌ای که تعرض داده‌ای پیش از بی‌آبروشدن عمومی نیز پیامد حقوقی دارد. با این همه، فعلیت‌یابی حمایت‌ها منوط به سه پیش‌شرط است: نخست، تعیین عمومی و اعلام‌شده اینکه کدام داده، برای چه هدفی، توسط کدام نهاد و تا چه مدتی می‌تواند به طور خودکار استخراج، ذخیره و پردازش شود (نه به اتکای آیین‌نامه‌های داخلی یا توافق‌های خصوصی)؛ دوم، تلقی هر بهره‌برداری ثانویه از داده بیمار از آموزش و بازآموزی الگوریتم تا تحلیل‌های پژوهشی و تجاری خارج از مسیر مراقبت به عنوان مداخله در حریم، مگر با رضایت خاص، قابل بازپس‌گیری و مستند بیمار؛ سوم، الزام مراکز درمانی و شرکت‌های فناور به ثبت دقیق دسترسی‌ها و مسیرهای خروج هر فایل و سیگنال به نحوی که زنجیره جریان داده در رسیدگی انتظامی یا کیفری قابل بازسازی باشد. فقدان این شفافیت و پاسخگویی، حمایت‌های اساسی و کیفری را در عمل تهی می‌کند و بیمار را در برابر بازیگران فناورِ برخوردار از دسترسی عمیق به لایه‌های زیستی و روانی، بی‌پناه می‌گذارد.

رویکرد اتحادیه اروپا نشان می‌دهد که پرکردن شکاف‌های حمایتی تنها با تشدید ضمانت‌های کیفری حاصل نمی‌شود، بلکه نیازمند بازتعریف جایگاه بیمار در زنجیره داده و بازتوزیع مسئولیت میان همه بازیگران فناوری است. در این چهارچوب، داده سلامت ذاتاً «حساس» تلقی می‌شود و اصل بر منع پردازش است، مگر در موارد محدود و معین مانند ضرورت درمان، مصالح مشخص بهداشت عمومی یا رضایت صریح، هدفمند و قابل اعمال بیمار. پیامد این منطق، ارتقای بیمار از «منبع داده» به «دارنده حق بالفعل» است؛ حقی که صرفاً اخلاقی و انتزاعی نیست و به صورت حقوق اجرایی تجلی می‌یابد، همانند حق دسترسی به داده‌های خود، حق آگاهی از هدف و گیرندگان پردازش، حق تحدید یا تعلیق پردازش، حق انتقال‌پذیری داده به ارائه‌دهنده دیگر و در مواردی حق گسستن پیوند هویتی با محتوای لطمه‌زننده. نتیجه آنکه بیمار ناگزیر به اتکای صرف بر اعتماد نهادی نیست، بلکه می‌تواند حدود مداخله فناورانه را فعالانه تعیین و در صورت تعرض، از هر حلقه زنجیره به طور مستقیم مطالبه پاسخگویی کند.

افزون بر آن، اتحادیه اروپا مسئولیت صرف را بر عهده فرد پزشک یا حتی صرفاً بر عهده بیماران نمی‌گذارد. سکوهای دیجیتال و حتی موتورهای جستجو در جایگاه «کنشگران مسئول نسبت به کرامت فرد» قرار داده شده‌اند و مکلف‌اند پیوند میان هویت یک فرد و محتوای زیان‌بار برای حیثیت یا زندگی خصوصی او را محدود یا حذف کنند. این نکته در محیط سلامت اهمیت مضاعف دارد، زیرا افشای یک تصویر جراحی تحقیرکننده یا یک توصیف انگ‌زننده از وضعیت روانی یا جنسی، به سرعت و بدون نظارت می‌تواند در مقیاس جمعی بازتولید شود و آثار غیر قابل جبران بر زندگی حرفه‌ای و خانوادگی بیمار بر جای بگذارد. الزام سکو به مداخله فعال برای توقف این چرخه، عملاً یک تغییر پارادایم است؛ حفاظت از آبروی بیمار دیگر صرفاً یک تعهد درون حرفه‌ای پزشک و بیمار نیست، بلکه به تعهد زیرساختی پلتفرم‌های فناور نیز تبدیل می‌شود و این تعهد قابل پیگیری اداری و قضایی است.

لایه سوم این الگو، مسئولیت‌پذیری فنی و سازمانی است. سامانه‌های تشخیصی و تصمیم‌یارِ مبتنی بر هوش مصنوعی در حوزه سلامت، در این الگو در زمره سامانه‌های پرخطر قرار می‌گیرند و از همان ابتدای چرخه عمر خود ملزم‌اند مدیریت ریسک ساختاری داشته باشند، سوگیری و تبعیض ساختاری را پایش کنند، کیفیت و کفایت داده آموزشی را تضمین کنند،

مسیر و منطق تصمیم‌سازی را مستندسازی کنند و امکان مداخله و نظارت انسانی مؤثر را در تصمیم‌های بالینی حساس برقرار نگه دارند. پیامد این صورت‌بندی آن است که هیچ بازیگری نمی‌تواند خطا یا آسیب بالینی را به «خودکاربودن سامانه» یا «غیر قابل توضیح‌بودن مدل» حواله دهد. مسئولیت در اینجا پیشینی و توزیع‌شده است؛ توسعه‌دهنده، بهره‌بردار و ارائه‌دهنده خدمت درمانی همگی در معرض پرسش‌اند و همین پرسش‌پذیری تبدیل به سازوکار پیشگیرانه می‌شود.

چنین الگویی نشان می‌دهد که بلوغ تنظیم‌گری در سلامت دیجیتال، صرفاً در جرم‌انگاری افشا یا ممنوع‌کردن شنود خلاصه نمی‌شود، بلکه در پاسخ به سه پرسش بنیادین استقرار می‌یابد: ۱ـ چه کسی مجاز است چه نوع داده‌ای را بگیرد و برای چه هدف مشخصی؛ ۲ـ چه کسی از ابتدا و به طور مستمر پاسخگوی پیامدهای تصمیم الگوریتمی بر بدن و زیست اجتماعی بیمار است؛ ۳ـ بیمار در چه لحظه‌ای و با چه ابزار عملی می‌تواند مداخله کند، مانع شود، رضایت خود را تغییر دهد یا مسیر تصمیم‌گیری فناورانه را به بازبینی انسانی بکشاند.

از این منظر، مشروعیت کاربست هوش مصنوعی در مراقبت و درمان نه‌تنها به کارایی بالینی و شاخص‌های آماری دقت بستگی دارد، بلکه به رعایت یک بسته استاندارد هنجاری و نهادی بستگی دارد که باید صریحاً در سیاست‌گذاری سلامت داخلی نهادینه شود. عناصر این بسته را می‌توان در چهار محور عملیاتی خلاصه کرد:

۱ـ حریم خصوصی و امنیت داده: امنیت صرفاً یک لایه فنی (رمزگذاری، کنترل دسترسی، ممیزی دسترسی) نیست. اصل تنظیم‌گرانه باید «حد ضرورت» باشد، یعنی داده‌ای که برای مراقبت مستقیم ضرورت ندارد اصولاً نباید جمع‌آوری، انباشت یا به گردش ثانویه سپرده شود. این اصل، هم از کرامت ذاتی بیمار و هم از منطق کتمان سر پشتیبانی می‌کند.

۲ـ رضایت پویا و اعمال‌پذیر: رضایت معتبر باید قابل تفکیک به کاربری‌های مختلف، قابل بازبینی در طول زمان و قابل پس‌گرفتن بدون تهدید به افت کیفیت مراقبت باشد. بیمار باید بتواند استفاده درمانی بلاواسطه از داده خود را بپذیرد و هم‌زمان استفاده پژوهشی یا تجاری ثانویه را ممنوع کند و این منع باید در سطح سامانه و قراردادهای فناورانه محترم شمرده شود، نه صرفاً در کلام.

۳ـ شفافیت و قابلیت حسابرسی: نقش سامانه در تصمیم‌گیری بالینی، حدود مداخله آن در تجویز یا تشخیص و مرجع پاسخگو در صورت خطا باید پیشاپیش و به صورت مستند مشخص شود. مستندسازی ورودی‌های داده، مسیر پردازش، نقاط اعمال قضاوت انسانی و خروجی نهایی باید به گونه‌ای باشد که امکان بازبینی انتظامی و قضایی فراهم باشد و «منطقه خاکستری مسئولیت‌گریز» شکل نگیرد.

۴ـ خودمختاری و مداخله انسانی: بیمار باید بتواند در تصمیم‌های پرخطر تقاضای ارزیابی انسانی مستقل، رأی دوم یا بازبینی خروجی سامانه را مطرح کند و مسیر این اعتراض باید از پیش تعریف‌شده و اجرایی باشد. هم‌زمان، در مراجعه بالینی باید مرز میان «داده لازم برای مراقبت» و «داده‌ای که صرفاً برای تغذیه الگوریتم یا ارزش تجاری بعدی مطلوب است» برای بیمار روشن و قابل کنترل باشد؛ در غیر این صورت، رابطه درمانی به رابطه استخراج داده تنزل می‌یابد و حس کنترل بیمار بر سرنوشت بدنی و اطلاعاتی خود تضعیف می‌شود.

الگوی اتحادیه اروپا در عمل نشان می‌دهد که می‌توان این چهار محور را هم‌زمان به حقوق بیمار، تکلیف سکو و مسئولیت توسعه‌دهنده ـ بهره‌بردار سامانه ترجمه کرد و آن‌ها را در معرض پاسخگویی اجرایی و قضایی قرار داد. پیام مستقیم برای نظام سلامت مبتنی بر هوش مصنوعی در ایران این است که کرامت بیمار و راز درمانی او باید شاخص مشروعیت فنی و حقوقی سامانه تلقی شود. سامانه یا نهادی که نتواند حد ضرورت در جمع‌آوری داده، رضایت پویا و اعمال پذیر، شفافیت و قابلیت حسابرسی و حق بازبینی انسانی مؤثر را به صورت قابل اثبات تضمین کند، حتی اگر از نظر آماری دقیق و از نظر اقتصادی مقرون به صرفه باشد، نباید واجد وصف مشروعیت هنجاری در نظام سلامت شناخته شود. چنین صورت‌بندی، به جای آنکه بیمار را «منبع تغذیه الگوریتم» بداند، او را صاحب حق، صاحب صدا و صاحب‌اختیار

در برابر سامانه قرار می‌دهد و همین جابه‌جایی، شرط لازم برای اعتماد، پاسخگویی و پایداری اخلاقی در سلامت مبتنی بر هوش مصنوعی است.

مشارکت نویسندگان

سیدمحمدهادی قبولی درافشان: نظارت علمی بر فرایند پژوهش، راهبری و طبقه‌بندی مباحث، بازبینی انتقادی محتوا، تحلیل نهائی محتوا.

فاطمه نجیب‌زاده وامق‌آبادی: ایده‌پردازی اولیه پژوهش، گردآوری داده‌ها و منابع، نگارش پیش‌نویس مقاله.

نویسندگان نسخه نهایی را مطالعه و تأیید نموده و مسئولیت پاسخگویی در قبال پژوهش را پذیرفته‌اند.

تشکر و قدردانی

ابراز نشده است.

تضاد منافع

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

تأمین مالی

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

بیانیه هوش مصنوعی

نگارندگان بیان می‌دارند که در نگارش این پژوهش، از هوش مصنوعی بهره نبرده‌اند.

References

1. Bashipour Haghighi SA, Shojaeian KH, Alaee H. Feasibility Study of the Use of Artificial Intelligence in Medical and Therapeutic Proceedings with Emphasis on Governance Requirements in Respecting Individuals' Privacy. Medical Law Journal. 2024; 18: e60. [Persian]

2. Fallah Keti Latte N, Abbasi M, Ghorbani Gatab O. A Comparative Study of Civil Liability Resulting from the Use of Artificial Intelligence in Medical Surgeries from the Perspective of the Iranian and American Legal Systems. Medical Law Journal. 2024; 18: e28 [Persian]

3. Zamaneh Ghadim N, Abbaspour Jalali A. Medical data protection: The interaction of the right to privacy and artificial intelligence. HLJ. 2024; 2(2): 1-12. [Persian]

4. Safaei H, Jafari A. Relationship between information freedom and privacy. Journal of Islamic Law. 2012; 9(33): 136-159. [Persian]

5. Smith J. Siri, Siri, in my hand, who's the fairest in the land? On the interpretations, illustrations and implications of artificial intelligence. Business Horizons. 2019; 62(1): 15-25.

6. Gil de Zúñiga H, Goyanes M, Durotoye T. A scholarly definition of artificial intelligence (AI): Advancing AI as a conceptual framework in communication research. Political Communication. 2024; 41(2): 317-334.

7. Al-Farahidi ARK. Al-Ayn. Qom: Dâr al-Hijrah; 1989. p.45. [Arabic]

8. Dehkhoda AA. Loghat-nameh. Tehran: University of Tehran Press; 1998. p.52. [Persian]

9. Jafari Tabrizi MT. The Right to Human Dignity. Journal of Faculty of Law and Political Science. 1991; 27(1): 21-38. [Persian]

10. Danezis G, Domingo-Ferrer J, Hansen M, Hoepman JH, Le Métayer D, Tirtea R, et al. Privacy and data protection by design: From policy to engineering. Heraklion: ENISA Publications; 2015. p.1-79.

11. Rieke N, Hancox J, Li W, Milletari F, Roth HR, Albarqouni S, et al. The future of privacy-preserving AI in medical imaging: Federated learning. Nature Machine Intelligence. 2020; 2(11): 665-673.

12. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: A patient interface for twenty-first century research networks. European Journal of Human Genetics. 2015; 23(2): 141-146.

13. Fayz Kashani M. Kashf al-Asrar. Qom: Bostan-e Ketab; 1998. p.67. [Arabic]

14. Amidi AF. Ghorar al-Hekam wa Dorr al-Kalam. Beirut: Al-A'lami Publications; 1987. p.88. [Arabic]

15. World Health Organization. Ethics and governance of artificial intelligence for health. Geneva: World Health Organization; 2021. p.35.

16. Van Drumpt S, Vinti S, Gürses S. Secondary use under the European Health Data Space: Setting the scene and towards a research agenda on privacy-enhancing technologies. Frontiers in Digital Health. 2025; 7: 1602101-1602108.

17. Townend D. Privacy. Edited by Laurie G, Dove E, Ganguli-Mitra A, McMillan C, Postan E, Sethi N, et al. In: The Cambridge handbook of health research regulation. Cambridge: Cambridge University Press; 2021. p.73-80.

18. Hoepman JH. Privacy design strategies. Edited by Cuppens-Boulahia N, Cuppens F, Jajodia S, El Kalam AA, Sans T. In: ICT systems security and privacy protection. Berlin: Springer; 2014. p.446-459.

19. Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proceedings of the 2007 IEEE Symposium on Security and Privacy. Washington: IEEE; 2007. p.321-334.

20. Steinsbekk KS, Myskja BK, Solberg B. Broad consent versus dynamic consent in biobank research: Is passive participation an ethical problem? European Journal of Human Genetics. 2013; 21(9): 897-902.

21. Miri Rostami J. Commentary on the Constitution of the Islamic Republic of Iran. Tehran: Majd Publications; 2018. p.85. [Persian]

22. Gashani Sebehti H. Right to health in Iranian law. Tehran: Mojak Publications; 2024. p.98. [Persian]

23. Aslani S. The right to health: The impact of international norms on the right to health as a manifestation of human rights in Iran's public law. Tehran: Aydin Publications; 2018. p.112. [Persian]

24. Shafiei MS, Khamsipour F, Aboozari M. Cybercrimes and digital forensics. Tehran: Ketab Aval Publications; 2018. p.42. [Persian]

25. Cohen IG, Lynch HF, Vayena E, Gasser U. Big data, health law and bioethics. Cambridge: Cambridge University Press; 2018. p.45.

26. Tehran Province Court of Appeal, Branch 41. Judgment No.9709972294100482. Tehran: Judiciary of the Islamic Republic of Iran; 2018. [Persian]

27. Supreme Court of Iran. Ruling No. 9409982925401407. Tehran: Judiciary of the Islamic Republic of Iran; 2016. [Persian]

28. Kuner C. The global reach of EU data protection law. International Data Privacy Law. 2021; 11(1): 35-52.

29. Lynskey O. The foundations of EU data protection law. Oxford: Oxford University Press; 2022. p.145.

30. Globocnik J. The right to be forgotten is taking shape: CJEU judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17). GRUR International. 2020; 69(4): 380-388.

31. Schuett J. Regulating artificial intelligence in the European Union: Risk, compliance and enforcement. European Law Journal. 2024; 30(1): 1-23.

32. Minssen T, Gerke S, Aboy M, Price WN II, Cohen IG. Regulatory responses to medical machine learning. Journal of Law and the Biosciences. 2020; 7(1): lsaa002: 1-16.

33. Kirwan M, O'Rourke C, Whelan A. What GDPR and the Health Research Regulations (HRRs) mean for Ireland: "Explicit consent" a legal analysis. Irish Journal of Medical Science. 2020; 190(2): 515-521.

34. Pitel E, Leaşu F, Nicolau A, Rogozea L. Ethical aspects in the use of artificial intelligence in the process of drug development. Brasov Medical Journal. 2023; 1(2): 55-66.

35. Rony MK, Numan SM, Akter K, Tuj Johra F, Tushar H, Debnath M, et al. Nurses' perspectives on privacy and ethical concerns regarding artificial intelligence adoption in healthcare. Heliyon. 2024; 10(17): e36837: 1-12.

36. Ijaiya H. Balancing data privacy and technology advancements: Navigating ethical challenges and shaping policy solutions. International Journal of Research and Publications. 2024; 5(1): 1-14.

37. Bala I, Pindoo I, Mijwil MM, Abotaleb M, Yundong W. Ensuring security and privacy in healthcare systems: A review exploring challenges, solutions, future trends and the practical applications of artificial intelligence. Jordan Medical Journal. 2024; 58(3): 201-223.

38. Gabriel OT. Data privacy and ethical issues in collecting health care data using artificial intelligence among health workers. Ibadan: Center for Bioethics and Research; 2024. p.76.

39. Patel K. Ethical reflections on data-centric AI: Balancing benefits and risks. International Journal of Artificial Intelligence Research and Development. 2024; 2(1): 1-7.

40. Gambhir A, Jain N, Pandey M, Simran. Beyond the code: Bridging ethical and practical gaps in data privacy for AI-enhanced healthcare systems. In: Recent trends in artificial intelligence towards a smart world: Applications in industries and sectors. Singapore: Springer Nature; 2024. p.37-65.

41. Yanamala AK, Suryadevara S, Kalli VD. Balancing innovation and privacy: The intersection of data protection and artificial intelligence. International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence. 2024; 15(1): 1-43.

42. 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.

43. Amini M, Jesus M, Fanaei Sheikholeslami D, Alves P, Hassanzadeh Benam A, Hariri F. Artificial intelligence ethics and challenges in healthcare applications: A comprehensive review in the context of the European GDPR mandate. Machine Learning and Knowledge Extraction. 2023; 5(3): 1023-1035.

44. Das B, Khatua D. Ethical considerations for implementing AI-based solutions in digital health and medical analytics. In: Responsible AI for digital health and medical analytics. Hershey: IGI Global Scientific Publishing; 2025. p.241-266.

45. Aman Z, Qidwai MA. Society, healthcare and artificial intelligence: Navigating the intersections of innovation and ethical considerations. In: Intersection of human rights and AI in healthcare. Hershey: IGI Global Scientific Publishing; 2025. p.479-496.

46. Carapinha JL, Botes D, Carapinha R. Balancing innovation and ethics in AI governance for health technology assessment. Journal of Medical Economics. 2024; 27(1): 754-757.

47. Gupta S. Ethical, privacy and security issues in smart healthcare. In: Driving global health and sustainable development goals with smart technology. Hershey: IGI Global Scientific Publishing; 2025. p.83-98.

48. Zainab H, Khan R, Khan AH, Hussain HK. Reinforcement learning in cardiovascular therapy protocol: A new perspective. Lahore: Asian Medical Research Press; 2024. p.1-12.