Review article (Narrative Review)

Medical Big Data and its Ethical Challenges in Violation of Patient Privacy

A. Ghasempour Ph.D.
Ph.D. Graduated in Private Law, Faculty of Law and Political Science, University of Tehran.

Abstract

Background: Big data refers to a large volume of information that is increasing day by day, and by analyzing it, various cause and effect relationships that have not been discovered so far can be established. This capability has many applications in various fields, including the field of health and wellness, so that it is predicted that very valuable results will be obtained in the field of diagnosis, prevention and treatment of diseases. On the other hand, in addition to the numerous benefits of big data, attention should also be paid to the ethical challenges that medical big data creates. This means that the use of medical big data requires the aggregation of information related to patients and those who participate in medical research, and this "potentially" entails the risk of violating the privacy and "autonomy" of patients. The author of the article, using an analytical and descriptive method and by studying the works of other authors, has examined the challenges of the medical field in relation to big data.

Conclusion: Although obtaining "informed consent" from patients or other stakeholders and "anonymizing" data are still necessary, they are not sufficient in the current situation to meet the challenges arising from big data. The author has also suggested solutions in continuation and in complement to the above solutions; some of the most important of these solutions include the use of differential privacy, conditional consent (case-based), and data transfer. Also, reviewing laws and regulations in terms of providing more severe criminal responses and determining heavier civil liability for privacy violations is another solution.

Keywords: *Medical Privacy, Big Data, Ethics, Anonymization, Challenge*

***Corresponding Author**: A. Ghasempour, Ph.D. Graduated in Private Law, Faculty of Law and Political Science, University of Tehran. Email: Amin.Ghasempour@ut.ac.ir

How to cite: Ghasempour A. Medical big data and its ethical challenges in violation of patient privacy. Ethics in Science and Technology. 2025,20(2): 9-18.

Vol. 20, No. 2, 2025

مقاله مروری (مروری توصیفی)

کلان‌داده‌های پزشکی و چالش‌های اخلاقی آن از حیث نقض حریم خصوصی بیماران

دکتر امین قاسم پور

دانش آموختهٔ دکتری حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران.

(تاریخ دریافت: ۱۴۰۲/۱۱/۲۰، تاریخ پذیرش: ۱۴۰۳/۰۲/۱۲)

چکیده

زمینه: کلان‌داده‌ها به حجم زیادی از اطلاعات گفته می‌شود که به طور روزافزون بر حجم آن‌ها افزوده می‌گردد و از تجزیه و تحلیل آن‌ها می‌توان روابط علّت و معلولی مختلفی را که تاکنون کشف نشده بود، احراز نمود. این قابلیت، کاربرد زیادی در حوزه‌های مختلف از جمله در حوزه‌ی بهداشت و سلامت دارد، به طوری که پیش‌بینی می‌شود از این رهگذر، نتایج بسیار ارزشمندی در زمینه‌ی تشخیص، پیشگیری و درمان بیماری‌ها حاصل گردد. از سوی دیگر، در کنار مزایای پرشمار کلان‌داده‌ها باید به چالش‌های اخلاقی‌ای که کلان‌داده‌های پزشکی ایجاد می‌کنند نیز توجه نمود. بدین معنا که استفاده از کلان‌داده‌های پزشکی مستلزم تجمیع اطلاعات مربوط به بیماران و کسانی است که در تحقیقات پزشکی شرکت می‌کنند و این امر «به طور بالقوه»، خطر نقض حریم خصوصی و «خودمختاری» بیماران را در پی دارد. نویسندهٔ مقاله، با روش تحلیلی و توصیفی و با مطالعهٔ آثار سایر نویسندگان چالش‌های حوزه پزشکی در ارتباط با کلان‌داده‌ها را بررسی نموده است.

نتیجه‌گیری: اخذ «رضایت آگاهانه» از بیماران یا سایر ذی‌نفعان و «گمنام‌سازیِ» داده‌ها اگرچه همچنان ضروری هستند، لکن در وضعیت فعلی در برابر چالش‌های ناشی از کلان‌داده‌ها تکافوی لازم را ندارند. نویسنده همچنین در ادامه و در تکمیل راهکارهای فوق، راهکارهایی را پیشنهاد نموده است؛ برخی از مهم‌ترین این راهکارها عبارتند از بکارگیری حریم خصوصی افتراقی، رضایت مقیّد (موردی)، داده‌سپاری. همچنین بازنگری در قوانین و مقرّرات از حیث ارائهٔ پاسخ‌های کیفریِ شدیدتر و نیز تعیین مسئولیت مدنی سنگین‌تر در خصوص نقض حریم خصوصی، راهکار دیگری محسوب می‌گردد.

کلید واژگان: حریم خصوصی پزشکی، کلان‌داده، اخلاق، گمنام‌سازی، چالش

سرآغاز

کلان‌داده‌ها[۱] به حجم زیادی از اطلاعات گفته می‌شود که به طور پیوسته بر حجم آنها اضافه می‌گردد و از آنجا که از تجزیه و تحلیل آنها می‌توان به وجود رابطهٔ علّیت بین بسیاری از پدیده‌ها پی برد، نویدبخش تحولّی شگرف در علم پزشکی در زمینه تشخیص[۲]، درمان[۳] و پیشگیری[۴] بیماری‌ها هستند.

داده‌های جمع‌آوری‌شده از منابع خارج از محیط پزشکی سنتی (مانند عادات غذایی، رفتاری و...)، می‌تواند برای اهداف پزشکی بسیار ارزشمند باشد. به عنوان مثال، «در دانشگاه جان هاپکینز محققان توانستند مکان و زمان شیوع آنفولانزا را بر اساس توئیت‌های کاربران پیش‌بینی کنند. در بیمارستان کودکان بوستون، محققان توانستند پارامتر «چاقیِ» اهالی منطقه را با استفاده از میزان «پسندیدن» یا به اصطلاح، لایک‌کردنِ کاربران در شبکه‌های اجتماعی برآورد، ردیابی و نقشه‌برداری کنند.» (۱)

همچنین کلان‌داده‌ها نسبت به «آزمایش‌های تصادفی کنترل‌شده[۵]» که برای کشف درمان برخی بیماری‌ها به طور تصادفی انجام می‌شود نیز از جهات بسیاری برتری دارند: توضیح آنکه در حالی که «آزمایش‌های تصادفی کنترل‌شده» نقشی حیاتی در توسعه درمان‌های جدید ایفا می‌کنند، (۲) با چالش‌هایی نظیر هزینه‌های بالا، مشکلات نمونه‌گیری آماری، عدم تعمیم‌پذیری[۶] نتایج مداخلات و ملاحظات اخلاقی[۷] در انتخاب تصادفی بیماران روبرو هستند. در مقابل، کلان‌داده‌ها با اتکا به داده‌های ارزان‌قیمت و انبوه حاصل از مراقبت از بیماران و زندگی روزمره، ضمن ارائهٔ همان فواید، از چالش‌های مذکور مصون هستند. بر این اساس حتی ادعا شده است که کلان‌داده‌ها قادرند «پزشکی شخصی[۸]» را تا حدّ زیادی پیشرفت دهند. (۳، ۴، ۵ و ۶)؛

نویسندهٔ مسئول: نشانی الکترونیکی : **Amin.Ghasempour@ut.ac.ir**

با این وجود باید دانست که بسیاری از کارکردهای مفید کلان‌داده‌ها به شرح فوق، سال‌ها است که در حدّ یک وعده مانده و هنوز به طور سراسری عملی نشده است. حتی برخی نویسندگان معتقدند ممکن است کلان‌داده‌ها هرگز نتوانند انتظارات آنچنانیِ پیش‌گفته را برآورده کنند. از سوی دیگر، تمام مزایای کلان‌داده‌ها، با فرض تحقّق عملی، در گروِ داشتن اطلاعات بیشتر در مورد بیماران به وجود خواهد آمد. به موازات تجمیع داده‌های بیشتر، خطرات مربوط به حفظ حریم خصوصی[9] نیز بیشتر می‌شود. با تجمیع داده‌ها، خطر سوءاستفاده از آنها نیز بیشتر می‌شود.

محیط‌های پزشکی از جمله بسترهایی هستند که چالش‌های حریم خصوصی در مورد آنها همواره موضوع پژوهش‌های محقّقین بوده است. مراجعه به مطب پزشک یا بیمارستان، بیماران و خانواده‌های آنها را تا حدّ زیادی در معرض آسیب (نسبت به حریم خصوصی) قرار می‌دهد. (۷). به همین ترتیب، افراد برای مشارکت در تحقیقات بهداشتی، باید تا حدّی از حریم خصوصی اطلاعات و حریم خصوصی فضای احساسی خود صرف‌نظر کنند.

بر این اساس و با این مقدّمه، بحث را در بیان تفصیلی چالش‌های کلان‌داده‌ها و سپس راهکارهای کنترل این چالش‌ها پیگیری می‌نماییم تا در عین بهره‌مندی از مزایای کلان‌داده‌ها، خطرات آن نیز به حدّاقل برسد. پیش از پرداختن به بحث اصلی، تعریف برخی اصطلاحات (کلان‌داده و حریم خصوصی پزشکی) که لازمهٔ ورود به مباحث بعدی است به صورت مختصر مورد بررسی قرار خواهند گرفت.

بحث

مفهوم‌شناسی

۱. کلان‌داده

«کلان‌داده» اصطلاحی است که حجم زیادی از داده‌ها را که به صورت مستمر به مقدار آنها اضافه می‌شود توصیف می‌کند. معتبرترین تعریف از کلان‌داده‌ها، آنها را از سه بُعد تقسیم‌بندی می‌کند: «حجم» (یا مقیاس)، «سرعت» و تنوع. (۸) برخی نویسندگان نیز «اعتبار»، «نوسان»، «صحت» و «ارزش» را به عناصر کلان‌داده اضافه کرده‌اند (۳۹) ولی در تعریف متداول، این عوامل، داخل در تعریف کلان‌داده محسوب نمی‌گردد.

مقدار کلان‌داده به ظرفیت آن بستگی دارد که می‌تواند مقادیر زیادی از اطلاعات را سریع‌تر از هر زمان دیگر و از منابع مختلف، در یک مجموعه‌دادهٔ واحد قرار دهد به طوری که امکان شناسایی عناصر و موضوعات «مرتبط» را فراهم می‌کند؛ سازوکاری که جز از طریق آن، امکان شناختن آن موضوعات و ارتباط آنها با یکدیگر میّسر نباشد. کلان‌داده‌ها را می‌توان برای تصمیم‌گیری بهتر و حرکت‌های راهبردی در عرصه‌های مختلف (پزشکی، تجاری، سیاسی و...) تجزیه و تحلیل کرد و هم‌اینک بسیاری از اندیشمندان و محقّقان در حوزه‌های مختلف بر همین مبنا پیشنهادها و نمونه‌هایی را ارائه کرده‌اند. (۹، ۱۰ و ۱۱). به طور کلّی کلان‌داده‌ها به دلیل امکان استفادهٔ تجاری یا اقتصادی، از نظر مالی ارزشمند تلقّی می‌گردند.

کلان‌داده‌های پزشکی نیز نوعی از کلان‌داده در معنای عام هستند؛ داده‌های پزشکی را می‌توان در تاریخچه نرم‌افزارهای مرورگر، برنامه‌های مورد استفاده در تلفن‌های هوشمند، داده‌های ثبت‌شده در فناوری‌های پزشکی پوشیدنی (تن‌کردنی)، لیست خرید و موارد دیگر یافت.

۲. حریم خصوصی پزشکی

تعاریف مختلفی از «حریم خصوصی» در نوشتارهای حقوقی ارائه شده است که از معنای عرفی آن دور نیست. عمدهٔ تعاریف، این مفهوم را در ارتباط با نحوهٔ دسترسی دیگران به اطلاعات یا فضای روانی فرد تعریف کرده‌اند. برخی گفته‌اند «حریم خصوصی عبارت است از دور نگه داشتن اطلاعات شخصی و فضای احساسیِ شخصی فرد از دسترس دیگران» (۱۲ و ۱۳). اطلاعات شخصی نوعی اطلاعات است که شخصی در یک جامعه خاص نمی‌خواهد با کسی در میان بگذارد، یا اطلاعاتی که فرد نسبت به آن حساسیت ویژه دارد.

یکی از مفاهیمی که ذیل بحث حریم خصوصی بررسی می‌گردد و در واقع شاخه‌ای آن است، «حریم خصوصی پزشکی» است. حریم خصوصی پزشکی به دور نگه داشتن اطلاعات شخصی مربوط به وضعیت سلامتی فرد از دسترس دیگران و همچنین دور نگه داشتن حریم خصوصی فرد از دسترس دیگران در محیط‌های پزشکی، اطلاق می‌شود. برخی نویسندگان پس از بیان چنین تعریفی، بر دوگانگی بین «حریم خصوصی جسمانی» و «حریم خصوصی اطلاعات و اسرار» (به عنوان دو عنصر مشخّص در تعریف «حریم خصوصی پزشکی») تصریح می‌کنند. (۱۴)

گفتنی است برخی از محققان در حوزهٔ حقوق پزشکی، ذیل عنوان «حریم خصوصی» مواردی را همچون «حریم خصوصی چندنفره[10]» (مانند «در میان گذاشتن صمیمانه یا محرمانهٔ» مرگ، بیماری و بهبودی) و «حریم خصوصی مالکانه[11]» (مانند مالکیت شخصی و نظارت بر شناساگران شخصی، داده‌های ژنتیکی و گونه‌های زیستی)؛ و «حریم خصوصی تصمیم‌گیری[12]» منقسم و بررسی می‌کنند (۱۵) و برخی دیگر از نویسندگان بر این تقسیم‌بندی و زیرمجموعه‌ها تاخته‌اند؛ به عقیده منتقدین، آنچه را که در این دیدگاه در بستر «حریم خصوصی» و مصداقی از آن تعریف شده است، می‌توان با سایر مفاهیم حقوقیِ شناخته‌شده بررسی و حمایت کرد و نیازی به ابداع مفاهیم جدید نیست؛ به عنوان مثال، اگر بکارگیری اصطلاح «حریم خصوصی مالکانه» در بحث اطلاعات مندرج در داده‌های ژنتیکی، بابت تضمین و حمایت حقوق مالی بیماران است (یعنی اینکه چه کسی و با چه شرایطی می‌تواند از داده‌های ژنتیکی آنان سود ببرد)، این بحث در واقع مربوط به «حق مالکیت» است، نه حریم خصوصی. همچنین آنچه در دیدگاه مورد نقد، «حریم خصوصیِ تصمیم‌گیری» نامیده شده است، بیشتر مربوط به کاری است که منافع شخص در انجام انفرادیِ آن کار بدون دخالت

دیگران است و این مفهوم نیز مربوط به «خودمختاری» است، نه حریم خصوصی. (۱)

بنابراین به جای آنکه در مفهوم حریم خصوصی دچار تکلّف شویم، به همان تعاریف مرسوم که در ابتدای بند ذکر شد اکتفا می‌نماییم. (۱۶).

چالش‌های کلان‌داده‌ها در رابطه با حریم خصوصی پزشکی

چنانکه در مقدّمهٔ این پژوهش ذکر شد، تمام مزایای پزشکی احتمالی کلان‌داده‌ها، با فرض عملی شدن آنها، در گروِ داشتن اطلاعات بیشتر در مورد بیماران به وجود خواهد آمد. هر زمان داده جمع‌آوری شود، خطر سوءاستفاده از اطلاعات و سایر چالش‌ها وجود دارد که در ادامه برخی از آنها مورد بررسی قرار می‌گیرند.

۱. امکان افشای اطلاعات پزشکی اشخاص (هک شدن و...) و نقض حقوق معنوی آنها

هنگامی که در گذشته سوابق پزشکی یا داده‌های حاصل از مطالعات در بیمارستان‌ها و مطب پزشکان در کاغذ درج و جمع‌آوری می‌شد، معمولاً در مکانی محرز و صندوقی دربسته نگه داشته می‌شدند و احتمال دسترسی عموم افراد به آنها بسیار بعید بود. با الکترونیکی شدن سوابق پزشکی و ذخیرهٔ آنها در رایانه‌های متّصل به اینترنت، خطر نقض داده‌ها، درز اطلاعات و سوءاستفاده‌ها افزایش یافت؛ توسعه و در اصطلاح «بلوغ» دولت الکترونیک نیز بر این خطر افزوده است (۱۷ و ۱۸). «در وضعیت کنونی، توزیع و نگهداری سوابق پزشکی در سامانه‌های پزشکی رقومی (دیجیتال)، یک فرآیند اساسی است. به عنوان مثال طی انتقال تصاویر پزشکی برای ثبت داده‌های بیماران کوید-۱۹ در یک عمل جراحی، ممکن است نیاز به ارسال جزئیات بیماری و تصاویر پزشکی به یک آسیب‌شناس و یا رادیولوژیست باشد... بنابراین یکی از مهم‌ترین چالش‌ها و مشکلات موجود در سامانهٔ «پروندهٔ الکترونیکی سلامت[۱۳]»، جابجایی اطلاعات محرمانهٔ پزشکی بدون تحریف است.» (۱۹). از سوی دیگر، هر داده‌ای که در دستگاه متصل به اینترنت نگهداری می‌شود به‌طور بالقوه قابل نفوذ است و داده‌هایی که در معرض نفوذ قرار گرفته، ممکن است در نهایت در معرض دید قرار گرفته و حتّی در «پایگاه تاریک» فروخته شود. (۲۰)

داده‌های پزشکی نه‌تنها از منابع سنتی مانند پرونده‌های الکترونیک سلامت و داده‌های مربوط به «توالی‌یابی ژنتیکیِ» «ریزاندام‌گان هم‌زیست»، بلکه از برنامه‌های تلفن‌های هوشمند، شبکه‌های اجتماعی، جستجوهای اینترنتی، داده‌های محیطی (به عنوان مثال داده‌های مربوط به کیفیت هوا)، حس‌گرهای محیط، فناوری‌های پوشیدنی و غیره به دست می‌آیند. در واقع، داده‌های مربوط به وضعیت پزشکی و سلامت افراد، بیش از مطب پزشکان و محیط بیمارستان‌ها، در زندگی روزمرهٔ آنها یافت می‌شود.

همهٔ این اطلاعات را می‌توان به‌طور نامحدود ذخیره کرد. این امر به مرور زمان اجازه می‌دهد تا داده‌ها برای مقاصدی غیر از آنچه برای آنها جمع‌آوری شده‌اند به‌کارگیری شوند. برخی از این کاربردها می‌توانند منافع صاحبان آن داده‌ها را به مخاطره اندازد و از زمانی که شرکت‌های خصوصی در برخی کشورها امکان عهده‌دار شدن مراقبت‌های پزشکی را یافتند، استفاده شرکت‌های خصوصی از داده‌های پزشکی به یک نگرانی جدی تبدیل شده است. به عنوان مثال، «شرکت «دیپ‌مایند» متعلّق به گوگل با شرکت «اِن.اچ.اس.» در انگلستان تصمیم گرفتند تا مشترکاً یک برنامه کاربردی بالینی در حوزهٔ آسیب‌های کلیوی ایجاد کنند؛ میلیون‌ها پروندهٔ پزشکی بدون اطلاع بیماران یا بدون کسب رضایت از آنها با این شرکت به اشتراک گذاشته شد. ماه‌ها بعد، دفتر کمیساریای اطلاعات انگلستان این کار را غیرقانونی اعلام کرد. در این مورد حتی اگر شرکت دیپ‌مایند به عموم مردم این اطمینان را داده بود که داده‌های پزشکی آنها، به حساب‌ها، محصولات یا خدمات شرکت گوگل پیوند نخواهند خورد، باز هم چنین تعهدی فاقد ضمانت اجرای حقوقی می‌بود و در واقع یک تعهّد اخلاقی محسوب می‌گردید.» (۱)

داده‌های پزشکی افراد می‌تواند به مقاصد مختلفی مورد استفاده قرار گیرد: فروختن به اشخاص ثالث، بازاریابی هدفمند، قیمت‌گذاری شخصی (به عنوان مثال فروش برخی محصولات خاص با قیمت بالاتر به افرادی که بیشتر آنها را می‌خواهند یا به آنها نیاز دارند) یا برای توسعه ابزارهای هوش مصنوعی که می‌توانند در آینده به روش‌های ناشناخته‌ای بکارگیری شوند. گفته شده است که هدف شرکت *DeepMind* از کمک به توسعهٔ این برنامه از همان ابتدا به دست آوردن داده‌ها برای پروژه‌های تحقیقاتی- تجاری در زمینهٔ «یادگیری ماشین» بود (۲۱ و ۲۲). در مواردی ممکن است داده‌هایی حسّاس با این اعتقاد که آن داده‌ها می‌تواند به نحوی به بیماران کمک کند، در اختیار یک شرکت قرار داده شود.

۲. ایجاد قدرت‌های انحصاری از حیث دسترسی به اطلاعات

یکی از چالش‌های بزرگ که مستقیماً مربوط به حریم خصوصی نیست، بلکه مربوط به قدرتی است که در پیِ دسترسی به داده‌های خصوصی حاصل می‌شود، این است که شرکت‌هایی که توانایی مالی و فناوری بزرگ و کلانی دارند، دسترسی به مراقبت‌های پزشکی را در انحصار خود درآورند. نفوذ در جمع‌آوری داده‌ها منجر به انحصار می‌شود و نفوذ در جمع‌آوری داده‌های حساس می‌تواند منجر به ایجاد انواع خاصی از انحصارهای مسأله‌ساز و بحران‌زا گردد. (۲۳) به عنوان مثال شرکت گوگل می‌تواند از نظر تجزیه و تحلیل داده‌ها در حوزهٔ سلامت و بهداشت، موقعیت انحصاری پیدا کند؛ زیرا شرکتی است که اطلاعات بیشتری در مورد افراد در سراسر جهان در اختیار دارد. این شرکت ممکن است با استفاده از این داده‌ها، پیشرفته‌ترین الگوریتم‌ها را برای تشخیص پزشکی ایجاد کند و سایر رقبای احتمالی که فاقد این حجم از داده هستند، در مقابل این غول اینترنتی، شانسی برای پیروزی نخواهند داشت. لذا اگر به شرکت‌های بزرگ اجازه دهیم به داده‌ها و همچنین به حوزهٔ مراقبت‌های پزشکی، دسترسی و آنها را در اختیار داشته باشند، ممکن است قیمت خدمات درمانی و پزشکی در درازمدّت، سر به فلک بکشد و ارائهٔ خدمات پزشکی به افراد منوط به ارائهٔ غیرمنصفانهٔ

اطلاعات از سوی ایشان گردد (به عنوان مثال علاوه بر پرداخت هزینهٔ درمان، بیماران را مجبور کنند که در روند مراقبت‌های پزشکی، کلیهٔ اطلاعات شخصی خود را ارائه دهند).

۳. امکان اِعمال تبعیض‌های ناروا

چالش دیگر، شامل مواردی است که افراد به دلیل برخی ویژگی‌ها و یا سوابق پزشکی (مثلاً به دلیل ابتلا به بیماری خاص یا باردار بودن) در محل کار خود مورد تبعیض[۱۴] قرار می‌گیرند. همچنین شرکت‌های بیمه می‌توانند با استفاده از اطلاعات پزشکی افراد، حقّ بیمهٔ برخی از افراد را بیشتر از دیگران مقرّر کنند؛ به عنوان مثال اِعمال جریمه نسبت به کسانی که به اندازه کافی ورزش نمی‌کنند، یا بدتر از آن، کسانی که دارای ژن‌هایی خطرناک هستند (۲۴ و ۲۵). ممکن است شرکت‌های دارویی با شناسایی افرادی که وابستگی و احتیاج شدیدی به دارویی خاص دارند، در حالی که فقط از آن شرکت‌ها می‌توانند آن دارو را تهیه نمایند، تبعیض قیمتی روا داشته و بابت آن هزینه بیشتری دریافت کنند. اما ایرادی که ممکن است در بحث تبعیض مطرح گردد آنکه خدمت‌رسانی متفاوت به افراد، با توجه به میزان اهتمام هر یک از آنها به سلامتی خود، چندان هم ناعادلانه و ناروا نیست؛ در واقع، کلان‌داده‌ها حتی اگر بکارگیری آنها منجر به نقض حریم خصوصی پزشکی افراد شود، باز هم باید مورد استقبال قرار گیرند، زیرا از این رهگذر می‌توان پی برد که هر فرد، تا چه حد در حفظ سلامتی خود کوشا و مسئولیت‌پذیر بوده است؛ بدین معنا که بیمارانی که قصور کمتری نسبت به بیماری خود دارند و با وجود رعایت توصیه‌های بهداشتی و پزشکی، ناخواسته بیمار شده‌اند، مزایا و خدمات بیشتری دریافت کنند، و بیمارانی با قصور در امر سلامتی، سهم بیشتری در بیماری خود دارند، خدماتی کمتر؛ نظام توزیع مسئولیت به شرح فوق، عادلانه‌تر از آن است که همهٔ بیماران، ولو آنان که به تقصیر و اِهمال خود دچار بیماری شده‌اند، به طور مساوی از خدمات درمانی بهره‌مند گردند. بدین‌سان تبعیض فوق مصداق تبعیض موجّه است.

در پاسخ به ایراد فوق باید گفت انتساب مسئولیتِ بیماری به شخص بیمار با تکیه بر تحلیل‌های برآمده از کلان‌داده‌ها، هم از حیث اثباتی و هم از حیث ثبوتی با محظورهایی مواجه است و در نهایت منتج به توزیع ناعادلانه و غیرواقع‌گرایانهٔ مسئولیت می‌گردد:

ایراد اثباتی عبارت است از اینکه الگوریتمی که کلان‌داده‌ها بر اساس آن عمل می‌کنند ممکن است دچار خطا شود و تحلیل‌های نادرستی از ویژگی‌های افراد و وضع زندگی آنها ارائه دهد، کما اینکه تاکنون نیز خطاهایی از این دست در آنها دیده شده است. کمااینکه «صحت» و اعتبار، امری ذاتی در تعریف کلان‌داده‌ها نیست؛ داده‌های نادرست هنوز هم می‌توانند بخشی از کلان‌داده‌ها باشند و وجود خطا در کلان‌داده‌ها منافاتی با تعریف آنها ندارد.

از حیث ثبوتی نیز باید توجه داشت، اینکه یک بیمار را بابت سهل‌انگاری در امر سلامتیِ خود، کمتر از بیمارانی که در امر سلامتی کوشیده ولی به هر حال بیمار شده‌اند، مستحق خدمات درمانی بدانیم، صرفاً یک تصمیم‌گیری و ارزیابی علمی نیست بلکه عملاً نوعی ارزش‌گذاری فلسفی و ورود به مبانی فلسفی «مسئولیت» محسوب شده و در واقع بستگی به آن دارد که ما چه تعریفی از «مسئولیت[۱۵]» ارائه دهیم؛ این در حالی است که ما در اینجا در مقامی نیستیم که بتوانیم در خوانش‌های شناخته‌شده پیرامون اصل «مسئولیت» و مبانی آن، آزادانه بدعت‌آفرینی کنیم (۲۶ و ۲۷) و به عنوان مثال، ضمانت اجرای تعهّد به حفظ سلامتی را محرومیت از خدمات پزشکی قرار دهیم.

وانگهی، «سلامتی»، نه صددرصد ولی تا حد زیادی امری غیرقابل پیش‌بینی و بسته به اموری خارج از ارادهٔ افراد است: ترکیبی از داشتن ژن‌های مناسب، زندگی در یک محیط سالم، داشتن موقعیت مناسب زندگی و غیره در این رابطه دخیل‌اند. به عنوان مثال سرطان شایع‌ترین علت مرگ در جهان است، و مطالعات اخیر نشان می‌دهد که بیشتر سرطان‌ها نتیجه جهش‌های تصادفی ژن‌ها است و در این رابطه قصور بیمار نقشی ندارد. پس با توجه به سهم زیاد شانس در وضعیت سلامت، یک عامل مهم برای اطمینان از داشتن برابری در برخورداری از فرصت مناسب برای همه شهروندان، فراهم کردن دسترسی همگانی به خدمات بهداشتی است. حفظ سلامت به امکان دسترسی به طیف وسیعی از فرصت‌های موجود در یک جامعه معین کمک می‌کند. آنچه به ایجاد برابری فرصت‌ها کمک می‌کند، ارائه دسترسی همگانی و عمومی به مراقبت‌های بهداشتی، است.

با عنایت به چالش‌های ذکرشده در مورد داده‌های کلان، اکنون باید بررسی نماییم که آیا امکان کاهش و یا کنترل این چالش‌ها و خطرات وجود دارد یا خیر؟ در صورت مثبت بودن پاسخ، چه راهکارهایی وجود دارد. ناگفته پیدا است هدف از این بررسی، بهره‌مندیِ ایمن و بی‌خطر از مزایای کلان‌داده‌ها است. در ادامه به این موضوع می‌پردازیم.

راهکارهای کاهش خطرات و کنترل چالش‌های کلان‌داده

در پزشکی سنّتی و تا پیش از آنکه افکار نویسندگان و پزشکان با پدیده‌ای به نام کلان‌داده و چالش‌های آن درگیر شود، برای حفظ و حراست از حریم خصوصی بیماران، تدابیر، منشورهای اخلاقی و نیز قوانین و مقرّراتی وجود داشته و دارد. به عنوان مثال، «رازداری» یکی از اصول اخلاقی (معمولاً ذیل اصل «خودمختاری») است که پزشکان و به طور کلی کادر درمان می‌بایست به آن ملتزم باشند؛ این اصل در تطوّرات تاریخی و با ایجاد نظام‌های قانونگذاری، به جهان حقوق نیز پا نهاده و اکنون در کسوت قوانین و مقرّرات، به قید مجازات، الزام حقوقی یافته است. (۲۸ و ۲۹).

به طور خلاصه می‌توان گفت ابزارها و تمهیدات سنّتی فوق در جهت محرمانه ماندن اطلاعات بیماران اندیشیده شده‌اند. بدیهی است محرمانه ماندن نیز خود مستلزم آن است که افراد تحقیق‌شونده قابل شناسایی نباشند. برای تحقق این هدف (ناشناس ماندن)، محقّقان و کارشناسان از طریق تجمیع و استفاده از «شناسه» (بجای نام واقعی) داده‌ها را از بین می‌برند و آنها را اصطلاحاً «گمنام‌سازی» می‌نمایند. (۳۰) گمنام‌سازی نیز خود به روش‌های مختلفی (معمولاً «تصادفی‌سازی» و «کلّیت‌بخشی») قابل اِعمال است. (۳۱)

شایان ذکر است ماده ۳ شیوه‌نامه تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی، مصوّب ۱۳۹۷ (مرجع تصویب: کمیسیون انتشار و دسترسی آزاد به اطلاعات)، اطلاعاتی را که هویت مالک در آنها هویدا نیست، در عداد اطلاعات شخصی و خصوصی نمی‌داند. به زودی خواهیم گفت که این ترتیب در مواجهه با کلان‌داده‌ها قابل انتقاد به نظر می‌رسد.

علاوه بر گمنام‌سازی، راهکار دیگری که به از دیرباز برای حفاظت بیشتر نسبت به حریم خصوصی انجام می‌گرفته است، اخذ «رضایت آگاهانه» از شرکت‌کنندگان (آزمودنی‌ها) و یا بیماران می‌باشد. برای اخذ چنین رضایت‌نامه‌ای، شرکت‌کنندگان باید بدانند که چه داده‌هایی درباره آنها جمع‌آوری و چگونه مدیریت می‌شود. همچنین این افراد باید از حق خود برای کناره‌گیری از تحقیق در هر زمان آگاه شوند و به آنها باید گفت که از آغاز تا پایان روند تحقیق، چه اتفاقی برای اطلاعات آنها خواهد افتاد (۳۲ و ۳۳). در بحث رضایت آگاهانه، داده‌ها اصولاً باید پس از استفاده در تحقیقات حذف شوند.

البته «گمنام‌سازی» (ناشناس ماندن) و «رضایت آگاهانه» نیز حتّی در گذشته که بحث کلان‌داده‌ها به شکل فعلی مطرح نبود، ابزاری کامل و جامع برای محافظت از حریم خصوصی تلقّی نمی‌شدند (۳۰) لکن تا حدّ بسیار زیادی برای نیل به مقصود، مقبولیت داشتند. به عنوان مثال داده‌های ژنتیکی در برابر گمنام‌سازی مقاومت می‌کنند و در واقع گمنام‌سازی در مورد آنها سالبه به انتفای موضوع است، زیرا داده‌های ژنتیکی منحصر به فرد هستند و در واقع، گمنام شدن آنها مستلزم آن است که مفاد آن داده، به هیچ شخصی قابل انتساب نباشد! همچنین در برخی موارد، اخذ رضایت آگاهانهٔ معتبر، غیرممکن است (به عنوان مثال اگر فرد موضوع آزمایش، فاقد اهلیت یا در کما باشد). اما چنانکه ذکر شد، با وجود نواقص مزبور و تا پیش از ظهور کلان‌داده‌ها و چالش‌های آن، «گمنام‌سازی» و «رضایت آگاهانه» اغلب ابزار خوبی برای محافظت از حریم خصوصی محسوب می‌گردیدند، به ویژه اینکه با اقدامات جبرانی دیگر، کاستی‌های آنها قابل جبران بود. با این وجود، کلان‌داده‌ها به دلیل نوع کارکرد ویژهٔ خود، سازوکار «گمنام‌سازی» و «رضایت آگاهانه» را عملاً خنثی می‌کنند، به طوری که استفاده از این دو تمهید با دشواری روبه‌رو می‌گردد.

توضیح آنکه در بحث گمنام‌سازی، هرچه نقاط دادهٔ بیشتری درباره افراد داشته باشیم، شناسایی آنها آسان‌تر است و کلان‌داده‌ها نقطه‌داده‌های زیادی را در مورد افراد به دست می‌دهند. به طور مثال، در محل کار یا زندگی شما فقط یک فرد هم‌قد شما وجود دارد که در آنجا کار و یا زندگی می‌کند (و آن خودِ شما هستید). برای شناسایی هر فرد، تنها دو یا سه نقطه‌داده کافی است. با توجه به افزایش روزافزون اطلاعات عمومی که در مورد مردم بدست می‌آید، شناسایی افراد به مراتب آسان‌تر نیز خواهد شد. علاوه بر این، برای اطمینان از تشخیص صحیح و درمان مناسب، آن داده‌ها حتماً باید به درستی به صاحب واقعی‌شان مرتبط گردند و با کس دیگر اشتباه گرفته نشود. بنابراین، هرکس باید با شناسهٔ پزشکیِ منحصربه‌فرد، علامت‌گذاری (تگ‌زنی) شود، تا شناسایی به راحتی ممکن گردد. اینها مواردی است که اثر گمنام‌سازی را تا حدّ بسیار زیادی خنثی می‌کند (مثلاً با وجود گمنام‌سازی و شناسه‌گذاری در مورد یک فرد، با استفاده از نقطه‌داده‌هایی که از کلان‌داده‌ها بدست آمده است معلوم می‌گردد که این شناسه مربوط به آن فرد است). از این رو پیشتر ذکر شد که ماده ۳ شیوه‌نامهٔ تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی در وضعیت فعلی قابل نقد به نظر می‌رسد.

حتی اگر گمنام‌سازیِ داده‌ها به روشی ایمن امکان‌پذیر نیز باشد و مرتبط‌سازی هر داده به صاحب واقعی آن را به کلّی ناممکن کند (ایمنی در سطح فردی)، تجزیه و تحلیل داده‌های جمع شده می‌تواند منجر به آسیب‌هایی در سطح گروهی مانند انگ‌زنی و تبعیض نسبت به گروهی خاص از مردم شود. چنین آسیب‌هایی می‌تواند بر همه افراد یک گروه معین (و نه فقط افرادی که با رضایت خود وارد روند تحقیقات شده‌اند) تأثیر منفی و تبعیض‌آمیز بگذارد.

آنچه گفتیم محدودیت‌های مربوط به گمنام‌سازی در مواجهه با کلان‌داده‌ها بود. اما کلان‌داده‌ها در موضوع «رضایت آگاهانه» نیز اثری مشابه و خنثی‌گر دارند؛ کلان‌داده‌ها برای کشف همبستگی‌های پیش‌بینی‌نشده طراحی شده‌اند، که نشان می‌دهد با توجه به حصول یافته‌های جدید در آینده (ناشی از کشف همبستگی‌های بین داده‌ها)، اطمینان چندانی برای گمنام‌ماندن افراد وجود ندارد. بنابراین، حتی اگر افراد موضوع تحقیق، «رضایت» دهند که داده‌های خود را در میان بگذارند، نمی‌توان رضایت ایشان را به طور کامل «آگاهانه» دانست، زیرا نمی‌توان با افراد در مورد کاربردهای آتی و عواقب احتمالی استفاده از داده‌های آنها در آینده با قاطعیت صحبت کرد، چنانکه حتی محققان نیز نمی‌توانند انواع همبستگی‌های بین داده‌ها را کشف کرده و در مورد چگونگی استفاده از این داده‌ها در آینده تضمین دهند. به عبارت دیگر ممکن است در آینده، همبستگی‌های جدیدی بین داده‌های فعلی کشف گردد؛ امری که اگر صاحبان آن داده‌ها می‌دانستند، شاید حاضر به ارائهٔ اطلاعات خود در آن مورد نمی‌شدند.

بنابراین، «گمنام‌سازی» و اخذ «رضایت آگاهانه» به شکل فعلی نمی‌تواند از حریم پزشکی افراد در عصر دیجیتال محافظت کند و این دو مورد، نگرانی‌ها در مورد قدرت ناشی از جمع آوری اطلاعات حساس را بخوبی مرتفع نمی‌کنند.

همچنین دیدیم که برخی از راهکارهایی که در گذشته موجب می‌شدند «گمنام‌سازی» و «رضایت دادن»، ابزارهای مناسبی برای حفاظت داده باشند، جنبهٔ تکمیلی داشتند؛ مانند نگه داشتن پرونده‌های کاغذی در یک صندوق قفل‌شده که فقط محققان ذی‌صلاح به آن دسترسی داشتند. اکنون به فراخور شرایط جدید در عصر کلان‌داده‌ها برخی اقدامات مکمّل دیگر را می‌توان برشمرد که خطرات مرتبط با داده‌ها را به حدّاقل برساند. این اقدامات را می‌توان در سه دسته کلّی بررسی کرد: بازنگری در قوانین و مقرّرات، بازنگری در تعریف و چگونگی «رضایت» آگاهانه و بالأخره اِعمال سازوکار حریم خصوصی افتراقی یا تفاضلی؛ این موارد را در ادامه بررسی می‌کنیم.

۱. بازنگری در مقررات و ضمانت‌های اجرایی (تنظیم‌گری مجدّد)

اقدامات مرتبط با کسب و نگهداری داده‌ها باید به گونهٔ شایسته‌تری مقرره‌گذاری شود تا از منافع صاحبان داده‌ها محافظت شود. استفاده نامناسب از داده‌ها، شامل بازشناسی افراد در پایگاه‌های اطلاعاتی که قبلاً گمنام‌سازی شده‌اند و نیز تبعیض، باید جرم‌انگاری گردد. به همین ترتیب، اگر صاحبان داده، رضایت صریح خود را اعلام نکرده باشند، مرتبط‌سازی اطلاعات پزشکیِ مندرج در پایگاه‌های تحقیقاتی به سایر منابع داده را باید غیرقانونی بدانیم. اگر بنا باشد خطر افشای داده‌ها به صاحبان آنها تحمیل شود (به عنوان مثال با استنباط اطلاعات حساس از اطلاعات غیر حساس، یا با ذخیره‌سازی داده‌ها به گونه‌ای که امکان شناسایی و سوءاستفاده را فراهم کند)، داده‌های پزشکی نباید از افرادی به دست آید که نخواسته‌اند در روند تحقیقات شرکت کنند؛ مانند زمانی که داده‌ها از رسانه‌های اجتماعی یا انجمن‌های باز پایگاه‌های داده تجزیه و تحلیل می‌شوند، یا هنگامی که پزشکان، بیمارستان‌ها یا داروخانه‌ها داده‌های پزشکی را بدون اطلاع بیماران با شرکت‌های تجزیه و تحلیل داده به اشتراک می‌گذارند. با این حال، اِعمال چنین رویکردی ممکن است در نگاه نخست، دشوار و چالش‌برانگیز به نظر برسد و البته با وجود مقررات سخت‌گیرانه، خطرات ناشی از نقض حریم خصوصی باز هم از بین نمی‌روند. به همین دلیل، محدودیت‌های مقرّر در خصوص نحوهٔ استفاده از داده‌ها کافی نیست و باید محدودیت‌ها و جرم‌انگاری‌های بیشتری در این خصوص اعمال شود.

آیین‌نامه جامع حفاظت از داده‌ها مصوّب ۲۰۱۶ از سوی پارلمان اتّحادیه اروپا، به تنظیم مقررات، توضیح شرایط و فرآیندهای مربوط به داده‌های شخصی اشخاص حقیقی و حقوقی و پردازش آنها، تضمین حفاظت از داده‌های شخصی و جریان آزاد اطلاعات، حقوق مبنا و آزادی اشخاص حقیقی درون اتحادیهٔ اروپا می‌پردازد. این آیین‌نامه از ۴ خرداد ۱۳۹۷ لازم‌الاجرا شده است و هر شخص حقیقی یا حقوقی که به پردازش داده‌های اشخاص به منظور فروش کالا یا خدمات به شهروندان اتحادیه ی اروپا می‌پردازد باید مفاد این آیین‌نامه را اجرا کرده و مطابق آن عمل کند. این آیین‌نامه چنانکه در ماده سوم خود مقرّر کرده است، نه‌تنها دربارهٔ سازمان‌های درون اتحادیهٔ اروپا، بلکه نسبت به سازمان‌هایی که به پردازش داده‌های شخصی مرتبط با افراد درون اتحادیهٔ اروپا، برای پیشنهاد کالا یا خدمات، صرف‌نظر از این که پرداخت به چه شکل باشد می‌پردازند یا رفتار اشخاص موضوع داده را درون اتحادیه مانیتور می‌کنند نیز لازم‌الاجرا است؛ حتی اگر در خارج از اتحادیهٔ اروپا باشند یا تابعیت اروپایی نداشته باشند. از این رو برای شرکت‌ها و مؤسسات ایرانی که مشمول این دو مورد می‌شوند یا از نتایج این پردازش‌ها بهره‌برداری می‌کنند حائز توجه و اهمیت است. (۳۴)

بازنگری در قوانین و مقرّرات، صرفاً به جرم‌انگاری و نظارت پسینی به شرح فوق، محدود نمی‌شود، بلکه نحوهٔ دسترسی به اطلاعات اشخاص در بدو تولیدِ آن اطلاعات نیز می‌تواند تحت بازرسی و نظارت (پیشینی) قرار گیرد. به عنوان مثال «قانون قابلیت انتقال و مسئولیت بیمه سلامت» موسوم به «هیپا» مصوّب ۱۹۹۶ در آمریکا باعث اصلاحات و تحولات بزرگی در امر بیمه و ساماندهی نحوهٔ دسترسی به اطلاعات بیمه‌شدگان گردید و برخی محقّقین ایرانی در انطباقِ این قانون با وضعیت نظام بیمه ایران ابراز داشته‌اند: «برخی از مشکلات نظام بیمهٔ درمانی ایران در مقایسه با مشکلات نظام بیمهٔ سلامت آمریکا، که منجر به تصویب هیپا گردید، هم‌سان می‌باشند» (۳۵). ایشان سپس با استناد به این هم‌سانی، برخی از سازوکارهای آن قانون را در ایران قابل اجرا دانسته، گفته‌اند «به عنوان مثال صاحب‌نظران با انجام فرایند تبادل الکترونیک داده‌ها، ایجاد شناسهٔ ملّی در صنعت مراقبت بهداشتی کشور و اجرای نظام هماهنگ اطلاعات جامع بیمه‌شدگان، که از ابعاد مهم هیپا می‌باشند، موافقند.» (۳۵) شایان ذکر است برخی نویسندگان، عبارت «قانون انتقال و پاسخ‌گویی الکترونیک بیمهٔ سلامت» را به عنوان معادل فارسی قانون مزبور انتخاب کرده‌اند. (۳۵)

۲. بازنگری در تعریف و چگونگی «رضایت» آگاهانه

لزوم اخذ رضایت، همواره به مثابه نگهبانی گرانقدر در زمینهٔ دسترسی به داده‌ها بوده، اما لازم است عملکرد آن به فراخور ساختار کلان‌داده‌ها به روز شود. در این راستا، راهکارهای مختلفی به ذهن می‌رسد.

الف) اخذ رضایت از صاحبان داده برای هر بار استفاده از داده‌ها و قرار دادن بار مسئولیت بر دوش آنها

در خصوص به روزرسانی سازوکار اخذ رضایت، یک راهکار این است که بار مسئولیت به دوش بیماران قرار داده شود تا کنترل اطلاعاتشان را خود به‌دست گرفته و در این خصوص پاسخ‌گو شوند. حتی با توجه به اینکه دانستیم این نوع رضایت‌نامه‌ها در شکل فعلی، به دلیل عدم اطمینان در مورد آیندهٔ کلان‌داده‌ها، محدود تلقّی شده و کاملاً آگاهانه محسوب نمی‌شوند، می‌توان مقرّر کرد که برای هر بار استفاده از داده‌های بیماران، رضایتی جداگانه از ایشان درخواست گردد.

ایراد این راهکار آن است که هم برای نهادها و هم برای افراد، بسیار پرزحمت است. به‌علاوه، سپردن مسئولیتِ داده‌های پزشکی به صاحبان آنها، به احتمال زیاد منجر به مواجههٔ ایشان با حجم فزاینده‌ای از درخواست‌های پی‌درپی جهت کسب رضایت خواهد شد و متعاقباً این امر می‌تواند منجر به اشتراک‌گذاریِ چندبارهٔ اطلاعات گردد؛ امری که ممکن است پشیمانیِ دیرهنگامِ صاحبان داده‌ها را از ابراز رضایت در پی داشته باشد؛ در حالی که می‌دانند «آبِ رفته به جوی باز نخواهد گشت».

ب) رضایت مقیّد (موضوعی)

پیشنهاد دیگر که کمی کاراتر به نظر می‌رسد، آن است که افراد بتوانند در چگونگی استفاده از داده‌های خود، به صورت موضوعی دست به انتخاب بزنند (به عنوان مثال شخص بتواند تصمیم بگیرد که از داده‌های وی فقط برای تحقیقات حوزهٔ «دیابت» استفاده شود) و از آن به «رضایت مقیّد» یا رضایت موضوعی یاد می‌کنیم. در همین راستا، کارشناسان فنّی در بسیاری از کشورها، رابطی را در محیط نرم‌افزاری را ایجاد کرده‌اند که به بیماران اجازه می‌دهد نسبت به استفاده از داده‌های خود، امکان ابراز «رضایت پویا» داشته باشند؛ بدین معنا که به آنها این

امکان را می‌دهد تا در عین حال که در آزمایش‌ها و تحقیقات شرکت می‌کنند، قلمروی رضایت خود را در هر زمان به نحو دلخواه تغییر دهند.

ج) داده‌سپاری؛ اعطال وکالت به کارشناسان معتمد (رضایت با واسطه)

گزینهٔ دیگر آن است که اشخاصی مورد اعتماد و در عین حال متخصّص، در قالب سازمان‌های مردم‌نهاد، هیأت‌امنا و غیره، به نمایندگی از صاحبان داده، در خصوص نحوهٔ جمع‌آوری و به‌اشتراک‌گذاری داده‌ها با شرکت‌ها و محقّقان، مذاکره و احیاناً توافق کنند. این تمهید از این جهت اندیشیده شده است که در بسیاری از موارد، صاحبان داده، افراد مجرّب و خبره‌ای نیستند تا بتوانند در تشخیص حوزهٔ مناسب جهت ارائهٔ داده‌های خود و نیز تشخیص شرکت‌های قابل اعتماد، به درستی اقدام کنند. این سازوکار، که نگارندهٔ مقاله، عنوانِ «داده‌سپاری» را برای آن انتخاب کرده است، هنوز در ایران نهادینه نشده است. البته، انتخاب نماینده جهت انجام امور تخصّصی یا جهت یافتن نماینده‌ای دیگر، امر جدیدی نیست؛ الاّ اینکه این‌بار در حوزهٔ داده‌ها و حریم خصوصی پیشنهاد شده است. در حقوق خارجی گفته شده است که در طراحی مدل «داده‌سپاری»، می‌توان از اتّحادیه‌های کارگری الهام گرفت (۱).

به علاوه، از حیث مسئولیت‌پذیری نیز ضروری است از حیث فناوریِ حفاظت از داده‌ها نیز سرمایه‌گذاری‌های لازم از سوی شرکت‌ها و موسسات ذی‌ربط (مانند وزارت ارتباطات و فناوری اطلاعات، شرکت‌های خصوصی حوزه فناوری اطلاعات و...) صورت گیرد تا داده‌های پزشکی به ایمن‌ترین شکل ممکن مدیریت و حفاظت گردند. در ماده ۲۰ قانون برنامه ششم توسعه مصوّب ۱۳۹۵/۱۲/۱۴ و همچنین بندهای ۲۰ و ۲۴ سیاست‌های برنامه هفتم توسعه، ابلاغی از سوی مقام رهبری اشاراتی به لزوم سرمایه‌گذاری در این حوزه شده است.

۳. اِعمال سازوکار حریم خصوصی افتراقی یا تفاضلی

«این روش معمولاً برای جلوگیری از حمله‌هایی به کار می‌رود که هکر بخواهد با استفاده از پرس‌وجوها و تفاضل آنها به اطلاعات یکی از افراد دسترسی داشته باشد.» (۳۱). توضیح کامل و تفصیلیِ این روش به دلیل تخصّصی بودن و آمیختگیِ زیاد با حوزهٔ فناوری از بحث این نوشتار خارج است و مطالعهٔ تفصیلی و فنّی آن در پژوهشی جداگانه شایسته است (۳۶، ۳۷ و ۳۸)؛ اجمالاً می‌توان گفت در این راهکار، «اعدادی تصادفی به نحوی به مجموعه داده‌ها اضافه می‌شود که تأثیر وجود یا عدم وجود هر یک از داده‌ها در کل داده به حداقل برسد.» (همان) در واقع، در این روش، جهت نهان‌سازی سوابق داده‌های فردی، موجی از پارازیت‌ها یا نویزهای دقیق و هدفمند به یک پایگاه‌داده وارد می‌شود تا شناسایی یا مرتبط‌سازی داده‌ها به صاحب آنها را تا حدّ بسیار زیادی دشوار کند. این روش اکنون در سایر حوزه‌ها بیش‌وکم در حال اجرا است و نتایج بسیار رضایت‌بخشی داشته است. رضایت‌بخش بودن نتایج به‌ویژه از آن جهت است که می‌دانیم در حالت کلّی اصولاً افزایش ضریب محرمانگی و ایمنی داده‌ها رابطهٔ معکوسی با «کیفیت تصمیم‌گیری» در مطالعه‌ای دارد که قرار است در آن بر مبنای کلان‌داده‌ها سیاست‌گذاری انجام شود و از سوی دیگر، در روش حریم خصوصی افتراقی، تا حدّ زیادی توانسته‌اند ضمن رعایت ضریب محرمانگی داده‌ها، همچنان بهره‌وری و سودمندی داده‌ها را در بالاترین سطح حفظ نمایند. به نظر می‌رسد در میان راهکارهای رفع چالش‌های کلان‌داده‌ها راهکار مورد بحث، مناسب‌ترین باشد. (۳۶ و ۴۰)

نتیجه‌گیری

کلان‌داده‌ها در حوزه پزشکی نیز همانند سایر حوزه‌ها قابلیت‌های گوناگون و پرفایده‌ای در مراحل پیشگیری، تشخیص و درمان دارند. این مزیت در کنار ارزان‌قیمت بودن آنها اهمیت کلان‌داده‌ها را دوچندان کرده است. اما چالش‌های اخلاقی مربوط به نقض حریم خصوصی ناشی از کلان‌داده‌ها را نباید نادیده گرفت. این چالش در هر حوزه‌ای که کلان‌داده‌ها بکارگیری می‌شوند وجود دارد و حوزهٔ پزشکی نیز از این جرگه بیرون نیست.

باید اذعان نمود در مواردی در هر حال نقض حریم خصوصی اجتناب‌ناپذیر است. به‌عنوان مثال داده‌های ژنتیکی در برابر گمنام‌سازی مقاومت می‌کنند و در واقع گمنام‌سازی در مورد آنها سالبه به انتفای موضوع است، زیرا داده‌های ژنتیکی منحصربه‌فرد هستند و در واقع، گمنام شدن آنها مستلزم آن است که مفاد آن داده، به هیچ شخصی قابل انتساب نباشد. همچنین انجام برخی مداخلات پزشکی لاجرم ملازمه با صرف‌نظر کردن بیمار از بخشی از حریم خصوصی خود می‌باشد. اما صرف‌نظر از موارد اجتناب‌ناپذیر، می‌توان با راهکارهای تکمیلی و جبرانی تا حدّ زیادی ضمن بهره‌مندی از مزایای کلان‌داده‌های پزشکی، محرمانگی آنها را نیز رعایت نمود و از این طریق چالش مربوط به نقض حریم خصوصی بیماران و شرکت‌کنندگان در تحقیقات پزشکی را رفع کرد. برخی از این راه‌کارها عبارتند از بازنگری در مقررات و ضمانت‌های اجرایی (تنظیم‌گری مجدّد)، الزامی شدن اخذ رضایت از صاحبان داده برای هر بار استفاده از داده‌ها، تعریف مفهوم رضایت مقیّد (موضوعی) و الزامی شدن اخذ آن از بیماران، داده‌سپاری (اعطای وکالت به کارشناسان معتمد جهت استفاده از داده‌ها در مواضع لازم و مطمئن)، پیش‌بینی سازوکار حذف داده‌ها پس از استفاده در تحقیقات پزشکی و بالأخص: اِعمال سازوکار حریم خصوصی افتراقی یا تفاضلی. راهکار اخیر، یکی از بهترین راهکارهای رفع چالش‌های مزبور است و اجرایی شدن این راهکار مستلزم فراهم بودن پاره‌ای بسترها و امکانات فنّی است. بر این اساس لازم است ضمن پشتیبانی نهادهای تصمیم‌گیر و در نظر گرفتن بودجه برای آن، سازوکار اِعمال آن در عرصهٔ پزشکی در ایران فراهم گردد.

در نظام قوانین و مقرّرات ایران اگرچه به نقض حریم خصوصی اشاره شده است لکن ضروری است در این خصوص قوانین و مقرّرات مزبور بازنگری شده و در این خصوص تفصیلات بیشتری همراه با ضمانت اجرا در نظر گرفته شود. ایجاد سازمان‌های مختص نظارت بر حریم

خصوصی بیماران و سایر ذی‌نفعان یکی دیگر از راهکارها و پیشـنهادها می‌باشد که در وضعیت فعلی خلأ آن در ایران احساس می‌گردد.

ملاحظه‌های اخلاقی

در پژوهش حاضر حق معنوی مولفین آثار مـورد احتـرام قـرار گرفتـه و قوانین تعارض منافع کاملا مورد توجه قرار گرفته است.

واژه نامه

1. Big data	کلان داده‌ها
2. Diagnosis	تشخیص
3. Treatment	درمان
4. Prevention	پیشگیری
5. Randomized controlled trial	آزمایش تصادفی کنترل شده
6. Generalization	تعمیم پذیری
7. Ethical consideration	ملاحظات اخلاقی
8. Personalized medicine	پزشکی شخصی
9. Privacy	حریم خصوصی
10. Multi-person privacy	حریم خصوصی چند نفره
11. Proprietary privacy	حریم خصوصی مالکانه
12. Decision-making privacy	حریم خصوصی تصمیم گیری
13. Electronic health record	پرونده الکترونیک سلامت
14. Discrimination	تبعیض
15. Liability	مسئولیت

References

1. Véliz C. Medical privacy and big data: a further reason in favour of public universal healthcare coverage. In T. C. de Campos, J. Herring & A. M. Phillips (eds.), Philosophical Foundations of Medical Law. Oxford, U.K.: Oxford University Press. 2019.
2. Treasure T, Takkenberg JJM. Randomized trials and big data analysis: we need the best of both worlds. Eur J Cardiothorac Surg, 2018; 53(5): 910–914. Doi: 10.1093/ejcts/ezy056
3. Hulsen T, Jamuar SS, Moody AR, Karnes JH, Varga O, Hedensted S, Spreafico R, Hafler DA and McKinney EF. From big data to precision medicine. Frontiers in Medicine, 2019; 6:34. Doi: https://doi.org/10.3389/fmed.2019.00034
4. Schaefer O, Shyong T, Sun S. (2019), Precision Medicine and Big Data, Asian Bioethics Review, 2019; 11: 275–288 277. Doi: https://doi.org/10.1007/s41649-019-00094-2.
5. Agharezaee N, Forouzesh F. Ethics in precision medicine. Iranian Journal of Biological Sciences, 2020; 15(2): 45-52. (In Persian)
6. Miri Moghaddam E. Personalized medicine, a new approach of the healthcare system. J Birjand Univ Med Sci. 2019; 26 (3):186-188 (In Persian).
7. Beni-Hessane AA, Khaloufi H. Big healthcare data: preserving security and privacy. Journal of Big Data, 5:1. 2018. https://doi.org/10.1186/s40537-017-0110-7.
8. Halili K, Valavi M. Big data technology, opportunities, challenges, and strategies. Interdisciplinary Studies on Strategic Knowledge, 2017; 28(28): 7-28. (In Persian).
9. Hatami B, Yaghoubi N, Mousavi Z. The Impact of Big Data on Customer Satisfaction and Revenue Management in the Aviation Industry", Management Sciences Research, 2022; 1(4): 110-120.
10. yazdani HR, Sohrabi B, Jalilian M. Identifying qualitative indicators for evaluating IoT business models based on big data analysis in the smart city. Modern Research in Decision Making, 2021; 6(2): 125-154.
11. Mahmoudi M, Filsaraei M. Big Data Analysis for Predicting Financial Behaviors Based on Machine Learning. New Research in Management and Accounting. 2020; 41: 243-256.
12. Shahbaz Qahfarrokhi S. People's physical privacy in the mirror of Imamiah Jurisprudence and Iran's Laws. Religious Researches, 2013; 9(1): 55-70. doi: 10.22059/jorr.2013.35771
13. Ansari B. Privacy. 1st ed. Iran/Tehran: Samt Publication. 2007. (In Persian).
14. Hashemi Bajgani SJ, Tolaei A, Beiki Shorkhi M. (2016), "Privacy in Medical Practices. Jurisprudence, Law and Criminal Science, 2016; 1(2): 66-79.
15. Allen A. Privacy and medicine' in EN Zalta (ed). The Stanford Encyclopedia of Philosophy; 1st ed. 2009. Accessed: December 2022.
16. Valipour Y. Philosophy of information jurisprudence and the concept of the term privacy. Researches on Islamic Jurisprudence and Fundamentals of Law. 2018; 1: 79-106.
17. Jamshidi MJ .Challenges of preserving citizens' information privacy in e-government. Citizens' Rights Studies, 2017; 4: 335-360.
18. Jafarzadeh Y, Amin Kaleybar N. Government interference in individuals' privacy in civil rights. Citizens' Rights Studies, 2020; 17: 211-224.
19. Zabihi J, Grailo H. Security, confidentiality, and privacy of information in the field of health with data EPR embedding in medical MRI images based on HVS model. Iran J Forensic Med 2021; 27 (3) :191-201.
20. Ghorbani I. Analysis of the role of dark web dimensions in the spread of drug and psychotropic crimes in cyberspace. Intelligence and Criminal Research. 2019;14(1):29-54.
21. Asghari Oskoei M, Khanizadeh F, Bahador A. Application of Data Mining through Machine Learning Algorithms to Study Effect of Car Features in Predicting Financial Claim of Motor Third Party Liability Insurance. Iranian Journal of Insurance Research, 2020; 35(1): 33-66. Doi: 10.22056/jir.2020.228093.2724
22. Bozorgy SS, Lazar F. Investigation of the machine learning approach and its applications in digital marketing. Management and Accounting Studies, 2020; 6(2): 179-186.
23. Fadishei H, Niroomand R, Mohammadzadeh E. Obligations & strategies of professional ethic in higher education system. Ethics in Science and Technology

2017; 11 (4) :18-24. Dor: 20.1001.1.22517634.1395.11.4.4.8
24. Bani Mustafa F. Big Data and Insurance: Implications for Innovation, Competition, and Privacy. Insurance, 2019; 52: 1-10.
25. Price WN, Cohen IG. Privacy in the age of medical big data, Nature Medicine, 2019; 25: 37–43. Doi: https://doi.org/10.1038/s41591-018-0272-7
26. Akhlaghi M. The philosophy of responsibility in islam and the role of education in realizing it. Journal of Islamic Education Research, 2016; 7(3): 47-64. doi: 10.22103/jir.2016.1402
27. Auhagen A E, Bierhoff HW. Responsibility: The many faces of a social phenomenon: Philosophical foundations of responsibility (by: Dieter Birnba Cher), London: Routledge. 2002.
28. Saghatoleslami A. The nature of ethical problems of research in cyberspace. Ethics in Science and Technology 2011; 6 (3) :48-61. Dor: 20.1001.1.22517634.1390.6.3.6.3
29. Farhud DD. Implications of ethical issues in medical genetics. Ethics in Science and Technology 2014; 9 (1). Dor: 20.1001.1.22517634.1393.9.1.12.6
30. Amiri, F. Privacy in Database Publishing in the Presence of Adversaryâs Background Knowledge. Iranian Journal of Information Processing and Management, 2020; 36(1): 211-242. doi: 10.35050/JIPM010.2020.019
31. Hassaninasab M, Sar-Golzaie-Javan M, Ariyanian E. A Review of Anonymization Techniques and Challenges in Big Data. Tehran: International Conference on Web Research. 2022.
32. Abbasi M, Safaei S, Ghafourian M. Analyzing the role of patient autonomy in informed consent. Bioethics Journal, 2019; 8(29): 43-51. Doi: https://doi.org/10.22037/bioeth.v8i29.24186
33. Yousefirad N. Jurisprudential and legal foundations of the sufficiency of informed consent for acquittal in physician liability. Medical Figh, 2016; 8: 67-107. Doi: https://doi.org/10.22037/mfj.v8i27-26.14606
34. Rezaei A, Ahmadi R. Regulations on the protection of natural persons with respect to the processing of personal data and data transfer. Tehran: Institute of Communications and Information Technology: Institute for ICT Policy Research and Strategic Management. 2018. Available at: https://ieaf.ir/Public_Resource/NRM/GDPR-V1.pdf
35. Asadi F, Hosseini A, Moghaddasi H, Esmaeili M. A study of HIPAA and the possibility of its implementation in Iran. Health Information Management, 2012; 8(6): 900-980.
36. Deldar F, Abadi M. Dissemination of Trajectory Databases with Differential Privacy Guarantees. Electronic and Cyber Defense, 2021; 9(1): 29-42.
37. Liyue F, Hongxia J. A practical framework for privacy-preserving data analytics" international world wide web conference committee (IW3C2); 2015; Doi: dx.doi.org/10.1145/2736277.2741122
38. Muneeb H, Mubashir HR, Jinjun C. Differential privacy in blockchain technology: A futuristic approach. Journal of Parallel and Distributed Computing, 2020; 145. Doi: https://doi.org/10.1016/j.jpdc.2020.06.003.
39. Khan MA, Uddin MF, Gupta N, Seven V's of big data: understanding big data to extract value' (Proceedings of Zone 1 Conference of the American Society for Engineering Education, 2014). Doi: 10.1109/ASEEZone1.2014.6820689.
40. Sharifi A, Safaei H, Almasi N, Savraei P. The civil and ethical liabilities regarding the violation of individuals´ personality rights in cyberspace. Ethics in Science and Technology 2023; 18 (3) :84-91. Dor: 20.1001.1.22517634.1402.18.3.12.3