مجله علوم پزشکی رازی دوره ۲۸، شماره ۱۲، اسفند ۱۴۰۰ http://rjms.iums.ac.ir

مقاله پژوهشی

بررسی ابعاد فقهی و حقوقی مرگ دیجیتال و مدیریت هویت مجازی بیماران پس از فوت: رویکردی در اخلاق پزشکی

روح اله رئیسی: استادیار، گروه فقه و مبانی حقوق اسلامی، دانشگاه پیام نور، تهران، ایران. (* نویسنده مسئول) rooholLah.reisi@pnu.ac.ir

محمد عدنانی : استادیار گروه فقه و مبانی حقوق اسلامی دانشگاه جهرم ، جهرم، ایران.

چکیده

زمینه و هدف: با گسترش فناوری‌های دیجیتال در حوزه سلامت، اطلاعات پزشکی بیماران به صورت الکترونیکی ثبت و ذخیره می‌شود. این تحول، چالش‌های جدیدی در زمینه مالکیت، حریم خصوصی، و سرنوشت داده‌های پزشکی افراد پس از مرگ ایجاد کرده است. مفهوم «مرگ دیجیتال» به ابعاد حقوقی و فقهی هویت و داده‌های مجازی افراد پس از وفات اشاره دارد. این پژوهش با هدف بررسی وضعیت حقوقی اطلاعات پزشکی متوفی در نظام حقوقی ایران، و تحلیل جایگاه فقهی و قانونی آن صورت گرفته است.

روش کار: این مطالعه به شیوه توصیفی ـ تحلیلی و با استفاده از منابع کتابخانه‌ای و اسنادی انجام شده است. متون قانونی ایران، آرای فقهی فقهای امامیه، و برخی اسناد بین‌المللی مورد بررسی قرار گرفته‌اند.

یافته‌ها: در نظام حقوقی ایران قانون صریح و مستقلی در خصوص وضعیت داده‌های دیجیتال پزشکی پس از مرگ وجود ندارد. اصولی مانند حرمت افشای سرّ مؤمن، قاعده احترام میت و حفظ کرامت انسانی در فقه امامیه بر لزوم صیانت از اطلاعات شخصی حتی پس از فوت دلالت دارند. از منظر حقوقی، نیز خلأهای قانونی باعث شده که رویه قضایی و اداری در این زمینه دچار ابهام و ناهماهنگی باشد.

نتیجه‌گیری: ضرورت تدوین قانونی جامع و روزآمد برای تعیین تکلیف داده‌های دیجیتال بیماران پس از مرگ در ایران به شدت احساس می‌شود. این قانون باید میان حق فرد بر اطلاعات خود، حریم خصوصی، و نیازهای عمومی یا وراث، تعادل برقرار کند و از اصول فقهی نیز الهام بگیرد.

تعارض منافع: گزارش نشده است.

منبع حمایت‌کننده: حامی مالی ندارد.

کلیدواژه‌ها

مرگ دیجیتال،

داده‌های پزشکی،

حریم خصوصی،

حقوق پزشکی

تاریخ دریافت: ۱۴۰۰/۰۲/۱۲

تاریخ چاپ: ۱۴۰۰/۱۲/۱۵

شیوه استناد به این مقاله:

Raisi R., Adnani M. A Jurisprudential and Legal Analysis of Digital Death and the Management of Patients' Virtual Identity after Death: An Approach in Medical Ethics. Razi J Med Sci. 2022;28(12): 366-379.

Razi Journal of Medical Sciences. 2022;28(12):366-379. http://rjms.iums.ac.ir

Original Article

A Jurisprudential and Legal Analysis of Digital Death and the Management of Patients' Virtual Identity after Death: An Approach in Medical Ethics

Ruhollah Raisi: Assistant Professor, Department of Jurisprudence and Fundamentals of Islamic Law, Payame Noor University, Tehran, Iran. (*Corresponding author) roohollah.reisi@pnu.ac.ir
Mohamad Adnani: Assistant Professor, Department of Jurisprudence and Fundamentals of Islamic Law, Jahrom University, Jahrom, Iran.

Abstract

Background & Aims: The rapid advancement of digital technologies in the field of healthcare has significantly transformed the management, storage, and transmission of patient data. With the emergence of electronic health records (EHRs), cloud-based medical platforms, wearable health devices, and virtual healthcare applications, vast amounts of personal and sensitive information are now stored in digital formats. While these technologies have improved access to and continuity of care, they have also introduced complex legal and ethical challenges—particularly in relation to patient data after death. The notion of "digital death" refers to the continuation of an individual's virtual presence and data footprint beyond their physical demise, encompassing social media accounts, medical records, genetic data, and more. In this context, a major question arises: What happens to a patient's medical and digital data after their death? Are these data protected by legal and ethical standards? Who holds the rights to access, control, or delete them? These questions are especially critical in the absence of explicit legal provisions. The issue becomes even more sensitive when it involves deeply private medical information. This study aims to explore the legal and Islamic jurisprudential (fiqh) perspectives on the posthumous status of patients' digital medical data within the legal system of the Islamic Republic of Iran. It also investigates the ethical duties of healthcare providers and institutions in protecting the privacy and dignity of deceased patients.
Methods: This research adopts a descriptive-analytical approach, relying on qualitative content analysis of legal texts, Islamic jurisprudential sources, and ethical codes relevant to medical confidentiality and digital data. Primary sources include the Constitution of the Islamic Republic of Iran, the Islamic Penal Code (especially Article 648 on medical secrecy), health regulations, and selected international legal instruments (e.g., the General Data Protection Regulation – GDPR, and HIPAA in the United States). In addition, the study analyzes relevant fatwas and classical fiqh rulings by prominent jurists of the Shi'a tradition that address the sanctity and confidentiality of personal information both before and after death. The study also draws comparative insights from countries that have codified laws on digital legacy and post-mortem data protection.
Results: The findings indicate a significant legal gap in Iranian law regarding the treatment of digital medical data after a patient's death. Although principles such as professional secrecy, respect for human dignity, and confidentiality are embedded in Iran's legal and ethical framework, they are primarily interpreted within the context of a patient's lifetime. There is no specific statute or regulation that addresses the status, control, or disclosure of digital medical data posthumously. This legal silence leads to ambiguities and inconsistencies in the handling of such data by hospitals, physicians, and insurance companies. From an Islamic jurisprudential viewpoint, several foundational principles suggest a strong obligation to protect the privacy of deceased individuals. The concept of hurmat al-mu'min (the sanctity of a believer), the prohibition against disclosing a believer's secrets (ḥurmat ifshāʾ sirr al-muʾmin), and the general rule of honoring the deceased all support the notion that personal and sensitive data should remain confidential after death. For example, a well-known narration from Imam Ja'far al-Ṣādiq (peace be upon him) states: "A believer is entrusted with the secrets of his brother, in life and in death." This hadith underlines the moral and legal continuity of privacy obligations beyond death. Furthermore, the study shows that the lack of posthumous data

Keywords
Digital Death,
Medical Data,
Privacy,
Medical Law

Received: 02/05/2021
Published: 06/03/2022

regulations in Iran has practical implications. Medical institutions are uncertain about whether they can release a deceased patient's records to heirs, law enforcement, or third parties. Similarly, digital health platforms that retain information in the cloud do not have a clear legal basis for how long to store, delete, or anonymize data once the patient has passed away. In cases where medical data might be relevant to a malpractice claim or for scientific research, the absence of regulation may lead to either excessive data exposure or unjustified withholding, both of which compromise legal balance and ethical integrity. By contrast, legal systems in the European Union and the United States have taken more definitive steps to regulate posthumous data. The GDPR, for instance, allows member states to define policies on processing personal data of deceased persons, and several EU countries have enacted national laws accordingly. The HIPAA regulations in the U.S. extend protection to medical data for up to 50 years after a person's death. Such measures provide a legal framework that respects both the rights of the deceased and the interests of surviving family members or institutions.

Conclusion: In conclusion, the lack of a specific and comprehensive legal framework in Iran regarding digital medical data after death presents serious legal, ethical, and practical challenges. The current laws are inadequate for addressing the complexities introduced by digital health technologies and the continuation of virtual identity post-mortem. However, Islamic jurisprudence offers a strong ethical foundation for extending privacy protections beyond death, suggesting that a jurisprudence-based approach can help fill the legislative void. The findings highlight the urgent need for Iranian lawmakers and health authorities to formulate a dedicated law governing posthumous digital medical data. Such legislation should clarify ownership rights, conditions for access by heirs or institutions, the role of prior patient consent (e.g., through digital wills), and safeguards against misuse. It should also incorporate principles of Islamic ethics and contemporary legal standards to ensure both religious compatibility and technological relevance. Establishing such a legal framework would enhance trust in the healthcare system, protect the dignity of deceased patients, and ensure the responsible use of medical data in accordance with both national values and global best practices.

Conflicts of interest: None
Funding: None

Cite this article as:

Raisi R., Adnani M. A Jurisprudential and Legal Analysis of Digital Death and the Management of Patients' Virtual Identity after Death: An Approach in Medical Ethics. Razi J Med Sci. 2022;28(12): 366-379.

مقدمه

با پیشرفت سریع فناوری‌های دیجیتال و گسترش کاربردهای فناوری اطلاعات در حوزه پزشکی، بخش بزرگی از داده‌ها و اطلاعات مرتبط با سلامت بیماران به صورت الکترونیکی و دیجیتال ذخیره و مدیریت می‌شود (۱). پرونده‌های پزشکی الکترونیک، سوابق تصویربرداری دیجیتال، داده‌های حاصل از اپلیکیشن‌های سلامت، دستگاه‌های پوشیدنی هوشمند و حتی پلتفرم‌های آنلاین مشاوره پزشکی، بخشی از هویت سلامت دیجیتال هر فرد را تشکیل می‌دهند (۲). این تحول فناورانه، امکانات بی‌سابقه‌ای برای مراقبت بهتر و پیگیری طولانی‌مدت سلامت فراهم کرده است، اما در عین حال پرسش‌های جدی حقوقی، اخلاقی و فقهی در خصوص مالکیت، حفظ حریم خصوصی، دسترسی و استفاده از این داده‌ها پس از مرگ بیمار مطرح ساخته است (۳).

موضوع «مرگ دیجیتال» اشاره دارد به استمرار حضور یا اثرات دیجیتال یک فرد در فضای مجازی و سیستم‌های داده‌ای پس از فوت فیزیکی او. این مفهوم در حیطه پزشکی به شکل جدیدی اهمیت می‌یابد، زیرا داده‌های پزشکی دیجیتال می‌توانند شامل اطلاعات بسیار حساس، شخصی و درمانی باشند که دارای ارزش حقوقی، اقتصادی و انسانی بالایی هستند (۴). پرسش‌هایی از قبیل این که چه کسانی مجاز به دسترسی به این داده‌ها پس از مرگ فرد هستند، آیا وراث حق مالکیت و کنترل آن را دارند، یا مسئولیت نگهداری و حفاظت از این اطلاعات بر عهده کدام نهاد یا فرد است، هنوز در بسیاری از نظام‌های حقوقی به طور دقیق و روشن پاسخ داده نشده است (۵). از منظر فقه اسلامی، این موضوع پیچیدگی‌های خاص خود را دارد؛ زیرا داده‌های پزشکی می‌توانند شامل اسرار شخصی و اطلاعاتی باشند که در طول حیات فرد تحت قاعده حفظ اسرار و حرمت قرار دارند. سوالاتی نظیر این که آیا داده‌های پزشکی دیجیتال می‌توانند در شمار اموال محسوب شوند، و آیا فرد می‌تواند درباره آن‌ها وصیت کند، هنوز موضوع بحث‌های فقهی است. همچنین اصول فقهی مانند حفظ کرامت میت، عدم ضرر به دیگران، و قاعده حرمتی برای اسرار مومنان، چارچوبی برای تحلیل این مسأله فراهم می‌کنند، اما نیاز به تبیین و تطبیق دقیق با فناوری‌های نوین وجود دارد. در نظام حقوقی ایران، با وجود پیشرفت در زمینه حقوق پزشکی و حریم خصوصی، مقررات صریح و مشخصی درباره وضعیت داده‌های پزشکی دیجیتال پس از مرگ فرد وجود ندارد (۶). این خلا قانونی علاوه بر ایجاد ابهام، می‌تواند منجر به تضاد منافع بازماندگان، مراکز درمانی، بیمه‌ها و حتی خود جامعه پزشکی شود. به عنوان مثال، ممکن است وراث یا نمایندگان قانونی فرد متوفی خواهان دسترسی به سوابق پزشکی او باشند، اما از سوی دیگر مقررات حفظ حریم خصوصی و محرمانگی اطلاعات پزشکان و بیمارستان‌ها مانع این دسترسی شود (۷). چالش دیگر این است که فناوری‌های نوین مثل هوش مصنوعی، بلاک‌چین و اینترنت اشیا در حوزه سلامت باعث پیچیدگی بیشتر مدیریت این داده‌ها شده است (۸). سوالات جدیدی مطرح می‌شود، از جمله: آیا می‌توان برای داده‌های دیجیتال وصیت‌نامه یا دستورالعمل حقوقی تنظیم کرد؟ مسئولیت حقوقی پزشکی در قبال نگهداری یا افشای داده‌های بیمار پس از مرگ چیست؟ و چگونه باید از این داده‌ها در پژوهش‌های علمی یا پزشکی استفاده کرد بدون آنکه به حریم خصوصی متوفی تجاوز شود؟ بنابراین، بررسی جامع ابعاد حقوقی، اخلاقی و فقهی «مرگ دیجیتال» در حوزه پزشکی، و ارائه چارچوب قانونی و فقهی مشخص، امری ضروری و حیاتی است. این بررسی نه تنها می‌تواند به حفاظت از حقوق بیماران متوفی و بازماندگان کمک کند، بلکه باعث افزایش اطمینان جامعه پزشکی و فناوری به حفظ اخلاقیات حرفه‌ای و قانونی در عصر دیجیتال می‌شود. در نهایت، این موضوع می‌تواند پایه‌ای برای تدوین قوانین و مقررات نوین در ایران و سایر کشورهایی باشد که هنوز با این مسئله نوظهور مواجه‌اند

روش کار

این پژوهش به روش توصیفی-تحلیلی انجام شده است. داده‌های مورد استفاده شامل منابع فقهی، از جمله قرآن، احادیث و نظرات فقها، و منابع حقوقی مانند قوانین داخلی و بین‌المللی است. تحلیل تطبیقی میان دیدگاه‌های فقه شیعی و نظام‌های حقوقی معاصر نیز بخشی از روش‌شناسی این تحقیق را تشکیل می‌دهد.

تعریف مرگ دیجیتال و تمایز آن با مرگ فیزیکی

مرگ فیزیکی به پایان فعالیت‌های زیستی یک موجود زنده گفته می‌شود؛ یعنی زمانی که تمامی عملکردهای حیاتی بدن متوقف شده و فرد به طور کامل از دنیای مادی خارج می‌شود (۹). این نوع مرگ نقطه پایان حیات بیولوژیکی انسان است و در نظام‌های حقوقی، پزشکی و اجتماعی لحظه‌ای که فرد دیگر زنده محسوب نمی‌شود، مشخص می‌شود (۱۰). مرگ فیزیکی آثار حقوقی و اجتماعی متعددی مانند انتقال ارث، خاتمه حقوق و تکالیف قانونی، و پایان زندگی قانونی را به دنبال دارد (۱۱). مرگ دیجیتال به حالتی اطلاق می‌شود که پس از وقوع مرگ فیزیکی یک فرد، هویت دیجیتال و مجموعه داده‌ها و اطلاعات مرتبط با آن فرد، در فضای مجازی، سامانه‌های ذخیره‌سازی داده‌ها، و بسترهای الکترونیکی همچنان به صورت فعال یا ذخیره شده باقی می‌مانند (۱۲). این داده‌ها می‌توانند شامل موارد متنوعی مانند پرونده‌های پزشکی الکترونیک، سوابق درمانی دیجیتال، داده‌های ثبت‌شده در اپلیکیشن‌های سلامت و مراقبت، اطلاعات مربوط به دستگاه‌های پوشیدنی پزشکی، حساب‌های کاربری در پلتفرم‌های سلامت آنلاین، و سایر آثار دیجیتال فرد مانند شبکه‌های اجتماعی، ایمیل‌ها و فایل‌های شخصی باشند (۱۳). این مفهوم فراتر از معنای سنتی مرگ است؛ زیرا مرگ دیجیتال نشان‌دهنده استمرار وجود و آثار یک فرد در بسترهای دیجیتال است که برخلاف مرگ فیزیکی، امکان تعامل، دسترسی و مدیریت این داده‌ها هنوز پابرجاست (۱۴). در واقع، هویت دیجیتال فرد به صورت یک موجودیت مجازی به حیات خود ادامه می‌دهد و این امر چالش های حقوقی، اخلاقی، پزشکی و فقهی جدیدی به دنبال دارد. بین مرگ فیزیکی و مرگ دیجیتال تفاوت‌های کلیدی وجود دارد؛ مرگ فیزیکی پایان حیات زیستی و بیولوژیکی فرد است، در حالی که مرگ دیجیتال به استمرار داده‌ها و هویت دیجیتال فرد اشاره دارد. در مرگ فیزیکی عملکردهای حیاتی بدن متوقف می‌شوند اما در مرگ دیجیتال داده‌ها و هویت مجازی همچنان فعال یا ذخیره باقی می‌مانند. مرگ فیزیکی موجب خاتمه حقوق و تکالیف قانونی می‌شود، ولی در مرگ دیجیتال پرسش‌های حقوقی درباره مالکیت، دسترسی و مدیریت داده‌ها همچنان باقی است (۱۵). مرگ فیزیکی در دنیای واقعی و مادی رخ می‌دهد، اما مرگ دیجیتال مربوط به دنیای دیجیتال و مجازی است. در مرگ فیزیکی تعامل با فرد پایان می‌یابد، ولی در مرگ دیجیتال امکان مدیریت، حذف، انتقال یا استفاده از داده‌ها همچنان وجود دارد. همچنین مرگ فیزیکی در حقوق و اخلاق دارای تعریف مشخص و پذیرفته شده است، در حالی که مرگ دیجیتال با ابهام‌ها و خلاهای قانونی و چالش‌های حریم خصوصی همراه است (۱۶).

دارایی های دیجیتال پزشکی: پرونده الکترونیک، داده‌های اپلیکیشن‌های سلامت، حسگرها

دارایی‌های دیجیتال پزشکی به مجموعه اطلاعات، داده‌ها و اسنادی اطلاق می شود که به صورت دیجیتال ذخیره، پردازش و منتقل می شوند و مربوط به سلامت، وضعیت پزشکی و مراقبت‌های بهداشتی افراد هستند. این دارایی‌ها شامل انواع مختلفی از داده‌ها می شوند که از طریق فناوری‌های نوین پزشکی و سلامت دیجیتال تولید و مدیریت می‌گردند. مهم‌ترین دسته‌های دارایی دیجیتال پزشکی عبارتند از پرونده الکترونیک سلامت، داده‌های حاصل از اپلیکیشن‌های سلامت و داده‌های حسگرهای پزشکی (۱۷). پرونده الکترونیک سلامت یکی از اصلی‌ترین دارایی‌های دیجیتال پزشکی است که شامل تمامی سوابق پزشکی یک بیمار می‌شود. این پرونده‌ها شامل اطلاعاتی مانند تاریخچه بیماری‌ها، نتایج آزمایش‌ها، داروهای مصرف شده، عمل‌های جراحی، یادداشت‌های پزشکان و سایر داده‌های مرتبط با سلامت فرد است. مزیت اصلی پرونده الکترونیک سلامت، دسترسی سریع، دقیق و یکپارچه به اطلاعات بیمار است که به بهبود کیفیت تشخیص و درمان کمک می‌کند. این پرونده‌ها معمولاً در سامانه‌های سلامت دیجیتال و مراکز درمانی به صورت امن ذخیره می شوند و نیازمند حفاظت ویژه به لحاظ حقوقی و امنیتی

هستند (۱۸). داده‌های اپلیکیشن‌های سلامت نیز بخشی از دارایی‌های دیجیتال پزشکی به شمار می‌روند. این اپلیکیشن‌ها ممکن است بر روی گوشی‌های هوشمند، تبلت‌ها یا سایر دستگاه‌های قابل حمل نصب شوند و اطلاعات متنوعی را جمع‌آوری کنند، از جمله فعالیت‌های روزانه، وضعیت خواب، فشار خون، قند خون، ضربان قلب و سایر شاخص‌های سلامتی. این داده‌ها به بیماران و پزشکان امکان می‌دهند تا روند سلامتی را بهتر پیگیری و مدیریت کنند (۱۹). با توجه به حساسیت این اطلاعات، نحوه ذخیره، انتقال و استفاده از داده‌های اپلیکیشن‌های سلامت باید با رعایت دقیق اصول حریم خصوصی و قوانین مربوط به حفاظت از داده‌ها انجام شود (۲۰). داده‌های حسگرهای پزشکی نیز بخش مهمی از دارایی‌های دیجیتال پزشکی هستند. حسگرهای پزشکی شامل دستگاه‌هایی هستند که به طور مستقیم روی بدن یا نزدیک به آن قرار می‌گیرند و پارامترهای حیاتی مانند ضربان قلب، فشار خون، سطح اکسیژن، دما و سایر علائم حیاتی را به صورت لحظه‌ای اندازه‌گیری و ثبت می‌کنند. این داده‌ها اغلب به صورت بی‌وقفه و در زمان واقعی جمع‌آوری می‌شوند و می‌توانند به بهبود مراقبت‌های پزشکی از راه دور و تشخیص سریع‌تر بیماری‌ها کمک کنند. داده‌های حسگرها نیز از نظر حقوقی و فقهی نیازمند حفاظت ویژه هستند، زیرا در صورت افشای غیرمجاز می‌توانند به نقض حریم خصوصی و صدمات جبران‌ناپذیر منجر شوند (۲۱). در مجموع، دارایی‌های دیجیتال پزشکی از ارزش بسیار بالایی برخوردارند و نقش مهمی در توسعه نظام‌های سلامت دیجیتال ایفا می‌کنند. این دارایی‌ها علاوه بر کمک به ارتقای کیفیت خدمات درمانی، چالش‌های متعددی در زمینه حفاظت از حقوق بیماران، امنیت داده‌ها و مسائل اخلاقی و فقهی به وجود آورده‌اند که نیازمند تدوین مقررات و چارچوب‌های حقوقی و فقهی دقیق هستند تا از حقوق بیماران و داده‌های پزشکی آن‌ها پس از مرگ نیز به درستی محافظت شود (۲۲).

حساب‌های کاربری پزشکی (MyChart، Google Health و...)

حساب‌های کاربری پزشکی مانند MyChart، Google Health و سایر پلتفرم‌های مشابه، بخشی بسیار مهم و رو به گسترش از دارایی‌های دیجیتال پزشکی محسوب می‌شوند. این حساب‌ها به افراد امکان می‌دهند تا به صورت آنلاین و از طریق اینترنت به سوابق پزشکی، نتایج آزمایش‌ها، تجویز داروها، برنامه‌ریزی ملاقات‌های پزشکی و اطلاعات مربوط به سلامت خود دسترسی داشته باشند (۲۳). برخلاف پرونده‌های سنتی پزشکی که معمولاً فقط در مراکز درمانی قابل مشاهده بودند، این حساب‌های کاربری دیجیتال امکان دسترسی سریع، آسان و حتی در هر زمان و مکان را فراهم می‌کنند. علاوه بر دسترسی شخصی بیمار، این سیستم‌ها به پزشکان و مراکز درمانی اجازه می‌دهند تا با رضایت بیمار، اطلاعات لازم را برای تشخیص و درمان بهتر دریافت و به‌روزرسانی کنند (۲۴). حساب‌های کاربری پزشکی علاوه بر ذخیره اطلاعات پایه‌ای، اغلب قابلیت‌هایی مانند یادآوری مصرف دارو، ثبت علائم و نشانه‌ها، ارتباط مستقیم با تیم درمان، و دریافت آموزش‌های سلامت دیجیتال را نیز ارائه می‌دهند. این ویژگی‌ها به افزایش مشارکت فعال بیماران در مدیریت سلامت شخصی‌شان کمک می‌کند و کیفیت مراقبت‌های پزشکی را بهبود می‌بخشد. همچنین، این حساب‌ها می‌توانند داده‌های جمع‌آوری شده از دستگاه‌های پوشیدنی یا اپلیکیشن‌های سلامت را نیز یکپارچه کنند تا تصویر جامع‌تری از وضعیت سلامت فرد ارائه دهند (۲۵). از نظر حقوقی و حریم خصوصی، حساب‌های کاربری پزشکی چالش‌های مهمی ایجاد می‌کنند. حفاظت از داده‌های حساس پزشکی در این حساب‌ها باید با دقت و به‌کارگیری فناوری‌های امنیتی پیشرفته صورت گیرد تا از افشای غیرمجاز، سوءاستفاده یا دسترسی بدون اجازه جلوگیری شود. همچنین، مسئله مالکیت داده‌ها و حقوق دسترسی پس از فوت فرد موضوعاتی است که در قوانین فعلی به طور کامل روشن نشده و نیازمند توجه و تنظیم مقررات مشخص است. در بعد فقهی نیز، حفظ کرامت متوفی و حرمت اسرار پزشکی از اهمیت بالایی برخوردار است که باید در مدیریت و انتقال اطلاعات این حساب‌ها پس از مرگ مد

نظر قرار گیرد (۱۵). با توجه به رشد روزافزون استفاده از این حساب‌ها و دیجیتالی شدن خدمات سلامت، تدوین چارچوب‌های قانونی، حقوقی و فقهی منسجم برای مدیریت، حفاظت و انتقال داده‌های این حساب‌ها پس از مرگ اهمیت حیاتی دارد تا حقوق بیماران و حریم خصوصی آنان حفظ شود و در عین حال امکان استفاده مسئولانه و اخلاقی از این داده‌ها برای اهداف درمانی و پژوهشی فراهم گردد (۲۵).

حقوق بیمار نسبت به هویت دیجیتال پزشکی خود

حق دسترسی، حذف، انتقال و مالکیت داده

حقوق بیمار نسبت به هویت دیجیتال پزشکی خود، از جمله موضوعات حیاتی و پیچیده در عصر سلامت دیجیتال است که شامل مجموعه‌ای از حقوق قانونی و اخلاقی می‌شود. این حقوق به بیماران اجازه می‌دهد تا کنترل بیشتری بر داده‌ها و اطلاعات پزشکی دیجیتال شان داشته باشند و تضمین می‌کند که حریم خصوصی و کرامت آن‌ها حفظ شود. مهم‌ترین جنبه‌های این حقوق شامل حق دسترسی، حق حذف، حق انتقال و حق مالکیت داده‌ها است (۲۷). حق دسترسی به داده‌های پزشکی دیجیتال به بیمار این امکان را می‌دهد که هر زمان به اطلاعات سلامت خود اعم از پرونده‌های پزشکی الکترونیک، نتایج آزمایش‌ها، سوابق درمانی و داده‌های جمع‌آوری شده از اپلیکیشن‌ها و حسگرهای پزشکی دسترسی داشته باشد. این حق، پایه‌ای‌ترین گام برای شفافیت، مشارکت فعال بیمار در روند درمان و ارتقای کیفیت مراقبت‌های پزشکی است. بدون امکان دسترسی آزاد و شفاف به داده‌ها، بیماران نمی‌توانند به طور مؤثر تصمیمات بهداشتی و درمانی خود را اتخاذ کنند (۲۸). حق حذف داده‌ها یا اصطلاحاً «حق فراموش شدن» به بیمار این اختیار را می‌دهد که در شرایط مشخص بتواند درخواست حذف یا پاک سازی داده‌های پزشکی دیجیتال خود را از سامانه‌ها و پایگاه‌های داده مطرح کند. این حق اهمیت ویژه‌ای در حفظ حریم خصوصی و جلوگیری از سوءاستفاده احتمالی از اطلاعات حساس دارد. البته در حوزه سلامت، این حق محدودیت هایی نیز دارد؛ مثلاً در مواردی که داده ها برای ادامه درمان، امور قانونی یا تحقیقات پزشکی لازم باشند، حذف کامل داده‌ها ممکن است مجاز نباشد و نیازمند تعادل بین حقوق فردی و منافع عمومی است (۲۹). حق انتقال داده‌ها یا «حق جابه‌جایی داده‌ها» به بیماران اجازه می‌دهد که داده‌های پزشکی دیجیتال خود را از یک سامانه یا ارائه‌دهنده خدمات سلامت به سامانه‌ای دیگر منتقل کنند. این حق به ویژه در شرایط تغییر پزشک، مرکز درمانی یا استفاده از خدمات جدید اهمیت دارد و باعث تسهیل ادامه مراقبت‌های پزشکی می‌شود. انتقال امن و قانونی داده‌ها همچنین مانع از ایجاد انحصار داده‌ها در دست یک ارائه‌دهنده خاص می‌شود و به ارتقای کیفیت خدمات سلامت کمک می‌کند (۳۰). حق مالکیت داده‌ها به معنای مالکیت قانونی و کنترل کامل بیمار بر اطلاعات پزشکی دیجیتال خودش است. این حق اهمیت فراوانی دارد زیرا تعیین مالکیت داده‌ها زمینه‌ساز اعمال حقوق دیگر مانند دسترسی، حذف و انتقال داده‌ها می‌شود. با وجود اهمیت این حق، در بسیاری از نظام های حقوقی، مالکیت داده‌ها به صورت صریح و مشخص تعریف نشده و این موضوع موجب بروز اختلافات حقوقی و پیچیدگی در مدیریت داده‌های پزشکی می‌شود. در نظام‌های فقهی نیز بحث مالکیت داده ها و حقوق بیمار نسبت به اطلاعاتش از موضوعات جدید و نیازمند تحلیل دقیق است تا هم کرامت و حریم خصوصی بیمار حفظ شود و هم منافع عمومی تامین گردد (۲). در مجموع، حقوق بیمار نسبت به هویت دیجیتال پزشکی‌اش ابزاری برای تضمین مشارکت فعال بیمار در مدیریت سلامت شخصی، حفظ حریم خصوصی و ارتقای کیفیت خدمات درمانی است. این حقوق باید در قوانین و مقررات سلامت دیجیتال به صورت شفاف تعریف و حمایت شوند تا بیماران بتوانند با اطمینان و اعتماد کامل از فناوری‌های پزشکی دیجیتال بهره‌مند شوند. همچنین، در بستر فقه اسلامی، توجه ویژه به اصول حفظ کرامت انسانی و حرمت اسرار فردی باید مبنای تدوین این حقوق قرار گیرد تا هماهنگی بین حقوق مدرن و ارزش‌های دینی برقرار شود (۱۰).

حقوق بیمار پس از مرگ: داده‌ها، رضایت‌های ذخیره‌شده، سوابق درمانی

حقوق بیمار پس از مرگ یکی از موضوعات مهم و چالش‌برانگیز در حوزه حقوق پزشکی و سلامت دیجیتال است که به بررسی وضعیت داده‌ها، رضایت‌های ذخیره‌شده و سوابق درمانی بیمار پس از فوت می‌پردازد. با توجه به پیشرفت فناوری و گستردگی استفاده از سامانه‌های الکترونیکی در نگهداری اطلاعات پزشکی، پس از مرگ بیمار، این داده ها همچنان در فضای دیجیتال باقی می‌مانند و مدیریت آنها موضوعی حقوقی، اخلاقی و فقهی به شمار می‌آید (۱). داده‌های پزشکی دیجیتال پس از فوت فرد شامل پرونده‌های الکترونیک سلامت، نتایج آزمایش‌ها، تصاویر پزشکی، داده‌های اپلیکیشن ها و حسگر های پزشکی، و همچنین حساب‌های کاربری مربوط به سلامت است که ممکن است حاوی اطلاعات حساس و خصوصی باشد. این داده‌ها ممکن است در مراکز درمانی، سامانه‌های ابری یا دستگاه‌های ذخیره‌سازی دیجیتال نگهداری شوند و سؤال اصلی این است که پس از مرگ بیمار چه کسی حق دسترسی، مدیریت، استفاده یا حذف این داده‌ها را دارد. در بسیاری از نظام‌های حقوقی، مالکیت و کنترل داده‌های پزشکی پس از فوت فرد مشخص نیست و ممکن است منجر به بروز اختلافات بین وراث، مراکز درمانی و نهادهای مرتبط شود (۷). رضایت های ذخیره شده، به مجوزهایی اشاره دارند که بیمار در طول زندگی خود برای استفاده از داده‌ها، درمان‌های خاص یا مشارکت در پژوهش‌های پزشکی ارائه کرده است. پس از مرگ بیمار، مسئله این است که آیا این رضایت‌ها همچنان معتبر هستند یا خیر و چه کسی حق دارد درباره ادامه یا لغو این رضایت‌ها تصمیم بگیرد. به عنوان مثال، در صورت وجود رضایت برای استفاده از داده‌ها در تحقیقات، وراث یا نمایندگان قانونی باید در مورد ادامه استفاده تصمیم‌گیری کنند، ولی این موضوع در قوانین و مقررات فعلی اغلب مبهم است (۱۱). سوابق درمانی نیز از دیگر جنبه‌های حقوق بیمار پس از مرگ هستند که حاوی اطلاعات حیاتی درباره تاریخچه بیماری‌ها، روند درمان و داروهای مصرف شده است. حفظ محرمانگی این سوابق حتی پس از فوت بیمار اهمیت بالایی دارد و تخطی از این موضوع می‌تواند موجب نقض حقوق و کرامت متوفی شود. از دیدگاه فقه اسلامی، حفظ اسرار و کرامت فرد حتی پس از مرگ از اصول مهم اخلاقی و حقوقی است که باید در مدیریت سوابق درمانی رعایت شود (۲۰). به طور کلی، حقوق بیمار پس از مرگ نیازمند تدوین چارچوب‌های قانونی و اخلاقی روشن است که علاوه بر حفظ حریم خصوصی و کرامت متوفی، تکالیف و اختیارات وراث، مراکز درمانی و سایر ذینفعان را مشخص کند. این چارچوب‌ها باید امکان مدیریت مسئولانه داده‌ها و رضایت‌های ذخیره‌شده را فراهم آورند و همزمان از سوءاستفاده و دسترسی غیرمجاز جلوگیری کنند. در نهایت، توجه به اصول فقهی و اخلاقی می‌تواند مبنایی محکم برای ایجاد تعادل بین حقوق فردی و منافع عمومی در این حوزه حساس باشد (۱۴).

مسئولیت حقوقی و حرفه‌ای پزشک یا مرکز درمانی پس از مرگ بیمار

در نظام حقوقی ایران، هرچند قانون صریح و مستقلی در خصوص حفظ حریم خصوصی متوفی در حوزه داده‌های دیجیتال و اطلاعات پزشکی وجود ندارد، اما با تکیه بر اصول کلی حقوقی، مواد قانونی موجود، و مبانی فقهی می‌توان چنین تکلیفی را برای اشخاص، نهادهای پزشکی و حتی بازماندگان متوفی استنباط کرد. اصل احترام به کرامت انسانی که در اصل ۲۲ قانون اساسی جمهوری اسلامی ایران تصریح شده، بر لزوم مصون بودن حیثیت افراد از تعرض دلالت دارد و می‌توان آن را حتی به پس از مرگ نیز تعمیم داد. همچنین در قانون مجازات اسلامی، به‌ویژه ماده ۶۴۸ کتاب تعزیرات، مقرر شده که پزشکان، ماماها، داروفروشان و دیگر اشخاصی که به مناسبت حرفه خود محرم اسرار مردم می شوند، حق افشای این اسرار را در غیر موارد قانونی ندارند و در صورت تخلف، مجازات خواهند شد. هرچند متن ماده اشاره‌ای به زنده بودن صاحب اسرار ندارد، ولی در عرف حرفه‌ای پزشکی و با توجه به حرمت افشای اسرار در فقه اسلامی، تعهد به حفظ رازداری حتی پس از مرگ

فرد نیز باقی است (۳۱). در برخی کشورها مانند ایالات متحده، قانون حفاظت از اطلاعات سلامت صراحتاً مقرر کرده که اطلاعات سلامت فرد تا ۵۰ سال پس از فوت نیز باید محفوظ بماند. در ایران، چنین تصریحی هنوز در قوانین وجود ندارد، اما پیش‌نویس‌های لایحه صیانت از داده‌های شخصی که در حال بررسی است، به‌طور ضمنی حاوی احکامی برای صیانت از داده‌های متوفیان نیز هست. طبق برخی مفاد این لایحه، داده های شناسایی شده افراد پس از مرگ نیز نباید بدون رضایت وراث یا دستور مرجع قضایی افشا شود (۳۲). در قانون آیین دادرسی کیفری نیز ماده ۱۰۴ بر محرمانگی اطلاعات در جریان رسیدگی‌های قضایی تأکید دارد که این اصل می‌تواند در مورد پرونده‌های پزشکی متوفیان نیز قابل استناد باشد، به‌ویژه اگر اطلاعات آنان در روند یک پرونده قضایی مؤثر باشد. مسئله دسترسی وراث به اطلاعات متوفی نیز از دیگر نکات مهم این حوزه است. به‌طور کلی، وراث ممکن است برای طرح دعوی، مطالبه دیه یا اثبات قصور پزشکی نیازمند دسترسی به اطلاعات پزشکی متوفی باشند، اما این دسترسی باید با رعایت اصل محرمانگی، صرفاً در حدود قانونی و با نظارت قضایی انجام شود. در غیر این صورت، انتشار یا ارائه اطلاعات متوفی بدون مجوز قانونی، می‌تواند موجب مسئولیت حقوقی و کیفری باشد. از نظر فقهی نیز حفظ اسرار افراد حتی پس از مرگ آنان واجب است. در متون روایی آمده که مجالس و گفته‌های خصوصی همچون امانت‌اند و افشای آن‌ها بدون مجوز شرعی جایز نیست. فقهای شیعه، بر لزوم احترام به میت و حرمت هتک حیثیت او تأکید دارند و این اصل می‌تواند پشتوانه‌ای برای الزام قانونی نهادهای درمانی به حفظ اطلاعات بیماران پس از فوت باشد (۳۳). با توجه به چالش‌های نوظهور در حوزه سلامت دیجیتال، ضرورت دارد قانون‌گذار در ایران نیز با تدوین مقررات شفاف و صریح، وضعیت داده‌های پزشکی متوفی را از حیث مالکیت، افشاء، حذف، و دسترسی تعیین کند. در غیر این صورت، احتمال بروز تعارض میان حقوق فردی، منافع وراث و وظایف نهادهای درمانی افزایش می‌یابد. به‌طور کلی، حفظ حریم خصوصی متوفی، چه از منظر حقوقی و چه فقهی، تکلیفی است که هم از کرامت انسان ناشی می‌شود و هم تضمینی برای اعتماد عمومی به نظام سلامت به شمار می‌رود (۳۴).

وضعیت داده‌ها در برابر وراث و بیمه‌ها

موضوع «وضعیت داده‌ها در برابر وراث و بیمه‌ها» یکی از مهم‌ترین چالش های حقوقی در حوزه پزشکی و سلامت دیجیتال پس از فوت بیمار است، چرا که پس از مرگ فرد، داده‌های پزشکی و دیجیتال او ـ شامل سوابق درمان، اطلاعات ژنتیکی، نسخه‌های الکترونیکی، رضایت‌نامه‌های ثبت‌شده، فایل‌های ذخیره‌شده در سامانه‌های ابری و حتی اطلاعات مربوط به سلامت در اپلیکیشن‌های تلفن همراه ـــ همچنان باقی می‌مانند و این مسئله، بحث مالکیت، دسترسی و حق استفاده از این داده‌ها را برای ذی‌نفعان از جمله وراث و شرکت‌های بیمه مطرح می‌کند (۳۵). از منظر وراث، یکی از پرسش‌های اساسی این است که آیا داده‌های پزشکی بیمار فوت‌شده بخشی از ترکه او محسوب می‌شود یا خیر. برخی حقوق‌دانان معتقدند داده‌ها جزو دارایی‌های غیرمالی شخصی هستند که قابلیت انتقال به ورثه را ندارند، مگر در موارد خاص مانند رضایت‌نامه کتبی از متوفی، یا لزوم استفاده از اطلاعات برای احقاق حق، مانند اثبات خطای پزشکی. در مقابل، گروهی دیگر بر این باورند که در شرایطی خاص، اطلاعات پزشکی می‌تواند بخشی از حقوق قابل انتقال تلقی شود، به ویژه اگر در تعیین علل فوت، مطالبه دیه، شکایت علیه پزشک یا شرکت بیمه مورد نیاز باشد. بنابراین دسترسی وراث به این داده‌ها، نیازمند تفسیر دقیق قانونی و در مواردی صدور حکم قضایی است (۳۶). شرکت‌های بیمه نیز ممکن است به داده‌های پزشکی متوفی علاقه‌مند باشند، به‌ویژه زمانی که مسائلی نظیر بررسی اصالت ادعاهای بیمه نامه، تعیین علت فوت، میزان تعهدات مالی، یا صحت اطلاعات ارائه‌شده توسط بیمه‌گذار در قراردادهای بیمه عمر، درمان و حوادث مطرح است. اما دسترسی بیمه‌ها به این اطلاعات باید با ملاحظات حقوقی و اخلاقی همراه باشد. از یک سو، آن‌ها ممکن است به این داده‌ها برای دفاع از خود یا پرداخت خسارت

نیاز دا شته با شند، ولی از سوی دیگر، اف شای اطلاعات بدون رضـایت فرد در زمان حیات یا بدون مجوز قانونی پس از مرگ می‌تواند نقض حریم خ صو صی تلقی شود (۳۷). در حال حاضـر، قوانین موضـوعه در ایران به‌طور شـفاف به وضـعیت داده‌های پزشـکی پس از فوت نپرداخته‌اند، اما اصـول کلی از جمله اصـل محرمانگی اسرار پزشکی (ماده ۶۴۸ قانون مجازات اسلامی) و اصل احترام به کرامت انسـانی (اصـل ۲۲ قانون اسـاسـی) همچنان لازم‌الاجرا محسوب می‌شوند. از سوی دیگر، در صـورتی که متوفی در زمان حیات خود رضـایتی برای ا ستفاده از داده‌هایش ثبت نکرده با شد، د ستر سی بیمه یا وراث به اطلاعات، باید از طریق مجوز قضـایی یا در موارد محدود و مشخص قانونی انجام شود (۳۸). از منظر فقهی نیز حفظ اسرار شخصی پس از مرگ، مانند حیات فرد محترم شمرده شده و اف شای آن‌ها بدون ضرورت شرعی یا مجوز قانونی، جایز نیست. فقها افشای اطلاعات پزشکی متوفی را جز در مواردی مانند جلوگیری از ضرر مهم، اقامه حق یا دفع ظلم، جایز نمی‌دانند. بنابراین، شـرکت‌های بیمه و وراث تنها در صـورتی می‌توانند به داده‌ها د ستر سی پیدا کنند که یا قبلاً اجازه متوفی اخذ شده با شد، یا قاضی اجازه دهد، یا ضرورتی چون احقاق حق یا رفع ظلم وجود داشـته باشـد. در نهایت، برای پیشـگیری از سـوءبرداشـت و تعارض منافع، پیشـنهاد می‌شـود که قانون‌گذار ایرانی در قالب یک قانون جامع حما یت از داده های پزشـکی، تکلیف این مسـئله را صراحتاً رو شن کند و ضوابطی برای د ستر سی بیمه‌ها و وراث به داده‌های دیجیتال پز شکی متوفی تدوین نماید؛ ضوابطی که ضمن حفظ حریم خصوصی فرد درگذشته، امکان دسـترسـی مشـروع و کنترل‌شـده برای اشـخاص ذی‌نفع را فراهم آورد (۳۹).

آیا اطلاعات پز شکی متوفی از نظر حقوقی و فقهی «مال» محسوب می‌شود؟

یکی از پرسـش های مهم در حوزه فقهی و حقوقی داده‌های سـلامت، به‌ویژه پس از مرگ بیمار، این اسـت که آیا اطلاعات پزشکی شخص متوفی، از نظر حقوقی یا فقهی، به عنوان «مال» محسوب می شود یا نه. پا سخ به این سـؤال در تعیین تکلیف این داده‌ها، امکان انتقال به وراث، قـابلیـت ارث‌بری، حق دسـتر سـی و حتی ارزش‌گذاری برای خسـارت یا افشـاء، نقش کلیدی دارد. در حقوق ایران، «مال» به چیزی اطلاق می‌شـود که دارای ارزش اقتصادی و قابل نقل و انتقال باشد. بنابراین، باید بررسـی کرد که آیا اطلاعات پزشـکی دارای ارزش اقتصادی ا ست و آیا می‌تواند مو ضوع مالکیت قرار گیرد. از نظر برخی حقو قدا نان، اطلا عات، به‌ویژه داده های دیجیتال و پز شکی، اگرچه فیزیکی نی ستند، اما با توجه به کارکرد اقتصـادی‌شـان، می‌توانند در قالب مال‌های غیرمادی تعریف شوند. اطلاعات پز شکی، خ صو صاً در حوزه‌هایی مانند ژنتیک، سـوابق بیماری، یا داده‌های مربوط به بیمه، ممکن اسـت از چنان اهمیتی برخوردار باشـد که قابلیت دادوسـتد، اسـتفاده تجاری یا حتی موضـوع قرارداد قرار گیرد. بنابراین، در شـرایطی خاص، می‌توان آن را مشمول تعریف مو سع «مال» دانست. این دیدگاه بیشـتر در حقوق تطبیقی و در نظام‌های حقوقی مدرن پذیرفته شده و در حال گ سترش ا ست (۳۶). در فقه ا سلامی، ملاک مالیت یک شیء آن ا ست که دارای منفعت عقلایی و مشـروع باشـد و نوعی قابلیت تملک و انتفاع بر آن متصور باشد. برخی فقها مانند امام خمینی، شـرط تحقق مال یت را وجود م نافع مورد نظر عرف دانسـته‌اند (۴۰). اگر داده‌های پزشـکی، مانند اطلاعات ژنتیکی یا سوابق دارویی، از نظر عرف و در شرایط خاص دارای منفعت عقلایی و قابل انتقال تلقی شوند، می‌توان گفت از نظر فقهی نیز مال محسوب می شوند. البته این مالیت در همه حالات ثابت نیسـت؛ ممکن اسـت در وضـعیت‌های خاص، مانند اطلاعات صـرفاً مربوط به سـلامت عمومی یا داده‌هایی که بدون رضـایت فرد به د ست آمده‌اند، مالیت منتفی با شد یا حداقل م شروعیت تصرف در آن محل تردید باشد. برخی فقها و حقوق‌دانان معتقدند که داده‌های پزشـکی، در صـورتی که صـرفاً کاربرد شـخصـی یا علمی داشـته باشـند و فاقد ارزش مبادله‌ای مسـتقیم باشـند، ممکن اسـت واجد مالیت به معنای مصـطلح نباشـند، اما همچنان می‌توانند موضـوع حق باشـند؛ به این معنا که فرد نسـبت به آن‌ها حق کنترل، د سترسی یا ممانعت از افشاء دارد (۲۹). در این

صورت، گرچه آن داده‌ها مال محسوب نمی‌شوند، اما دارای حقوق تبعی‌اند که می‌توان از آن‌ها حمایت حقوقی و فقهی کرد. به همین دلیل است که برخی سیستم‌های حقوقی دنیا، مانند اتحادیه اروپا، مفهوم «مالکیت داده» را به عنوان حق کنترل و نه تملک مالی، در نظر گرفته‌اند. در نهایت باید گفت که اطلاعات پزشکی متوفی، در صورتی که دارای منفعت عقلایی، قابلیت استفاده و ارزش اقتصادی باشند، می‌توانند از نظر فقهی و حقوقی در زمره اموال قرار گیرند. اما مال بودن آن‌ها به معنای قابلیت انتقال مطلق به وراث نیست، بلکه باید با ملاحظات حریم خصوصی، قوانین محرمانگی و مقررات سلامت سنجیده شود. بنابراین، حتی اگر داده‌های پزشکی متوفی نوعی مال محسوب شوند، انتقال آن‌ها به دیگران باید مشروط به عدم لطمه به حرمت میت، رضایت قبلی فرد در زمان حیات، یا ضرورت قضایی و اجتماعی باشد. این دیدگاه می‌تواند مبنایی برای تنظیم قوانین جدید در خصوص ارثبری اطلاعات، حق کنترل داده‌های دیجیتال پس از مرگ و محدودیت‌های دسترسی اشخاص ثالث به اسرار پزشکی باشد (۱۵).

قاعده «حرمت افشای سرّ مؤمن» پس از مرگ

قاعده «حرمت افشای سرّ مؤمن» یکی از اصول مهم اخلاقی و فقهی در شریعت اسلام است که نه‌تنها در زمان حیات افراد بلکه حتی پس از مرگ آن‌ها نیز جریان دارد. این قاعده برگرفته از آموزه‌های قرآنی و روایات معصومان علیهم‌السلام است که در آن، افشای راز و اسرار شخصی افراد مؤمن، بدون رضایت یا ضرورت شرعی، به‌شدت نهی شده است. سرّ مؤمن در فقه اسلامی دارای حرمت ذاتی است، زیرا به کرامت انسانی و حق امنیت روحی و حیثیتی فرد بازمی‌گردد. این حرمت، محدود به زمان زنده بودن شخص نیست، بلکه به استناد منابع فقهی معتبر، پس از مرگ نیز استمرار دارد و نباید با افشای اطلاعات خصوصی میت، به آبرو، حریم یا شأن او تعرض شود. در بسیاری از روایات اسلامی، به‌ویژه در کلمات امام علی (ع) و امام صادق (ع)، تأکید شده است که مؤمن امانت‌دار اسرار دیگران است و حتی اگر صاحب راز از دنیا برود، افشای آن جایز نیست. برای نمونه، در حدیثی از امام صادق (ع) آمده است: «الْمُؤْمِنُ يَحْفَظُ سِرَّ أَخِيهِ حَيّاً وَ مَيِّتاً؛ مؤمن راز برادرش را در حال حیات و پس از مرگ نگه می‌دارد.» این روایت، به‌روشنی بر استمرار حرمت سرّ مؤمن پس از مرگ دلالت دارد و بیانگر تعهد اخلاقی و شرعی به حفظ اطلاعات خصوصی افراد، حتی بعد از مرگ آن‌هاست (۴۱). افشای اسرار پزشکی، خانوادگی، مالی یا حتی سخنان خصوصی که در زمان حیات شخص پنهان بوده و اکنون امکان دفاع یا توضیح برای او وجود ندارد، خلاف این قاعده محسوب می‌شود. از منظر فقهی، حرمت افشای اسرار، زیرمجموعه قواعدی چون «حرمت هتک حرمت مؤمن»، «قاعده لاضرر» و «قاعده امانت» قرار می‌گیرد. طبق این قواعد، هرگونه رفتاری که به حیثیت فردی یا اجتماعی مؤمن لطمه بزند، یا سبب ضرر به بازماندگان او شود، یا نوعی خیانت در امانت دانسته شود، از نظر شرع ممنوع است. اطلاعات پزشکی شخص نیز از مهم‌ترین مصادیق راز است، زیرا دربردارنده جزئیات حساسی درباره وضعیت جسمی، روانی و حتی مسائل اخلاقی و خانوادگی فرد است که افشای آن‌ها می‌تواند موجب سلب اعتماد عمومی از نظام سلامت و خدشه به آبروی فرد و خانواده‌اش شود. از این رو، پزشک، پرستار، یا هر فردی که به سبب موقعیت خود به این اطلاعات دسترسی دارد، نه‌تنها در برابر قانون بلکه در پیشگاه شرع نیز موظف به حفظ این اطلاعات است، حتی اگر فرد صاحب اطلاعات از دنیا رفته باشد. در نهایت، قاعده حرمت افشای سرّ مؤمن پس از مرگ، یک اصل فراگیر اخلاقی- فقهی است که می‌تواند مبنایی برای تدوین قوانین مربوط به محرمانگی اطلاعات پزشکی در دوران پس از مرگ قرار گیرد. این قاعده بر ضرورت تداوم احترام به کرامت انسان، حتی پس از مرگ او تأکید دارد و مانعی جدی در برابر گسترش بی‌رویه افشای اطلاعات در فضای دیجیتال، شبکه‌های اجتماعی و حتی پرونده‌های حقوقی و بیمه‌ای ایجاد می‌کند. بنابراین، رعایت این قاعده نه‌تنها یک تکلیف دینی است، بلکه نقشی اساسی در حفظ حرمت

اجتماعی متوفیان، اعتماد عمومی به حرفه پزشکی، و ایجاد توازن میان حق دسترسی و حرمت شخصی ایفا می‌کند (۲۲).

چالش‌ها و خلأهای حقوقی در نظام ایران

یکی از مهم‌ترین چالش‌های حقوقی در نظام حقوقی ایران در حوزه سلامت دیجیتال، نبود قانون صریح و جامع درباره وضعیت داده‌های دیجیتال پزشکی پس از مرگ بیماران است. در حال حاضر، اگرچه برخی اصول کلی مانند حفظ حریم خصوصی، رازداری حرفه‌ای و احترام به کرامت انسانی در قوانین مختلف به‌صورت پراکنده آمده‌اند، اما هیچ‌گونه قانون مشخص، جامع و شفاف که به‌طور خاص وضعیت اطلاعات پزشکی افراد پس از مرگ آن‌ها را تعیین کند، وجود ندارد. این خلأ قانونی سبب بروز ابهامات فراوان در تعیین تکلیف داده‌های دیجیتال سلامت، نحوه دسترسی یا عدم دسترسی بازماندگان، نهادهای درمانی، شرکت‌های بیمه یا مقامات قضایی به این اطلاعات شده و موجب برخوردهای سلیقه‌ای یا تضاد منافع در موارد مختلف می‌شود (۴۲). برای نمونه، قانون مجازات اسلامی تنها در ماده ۶۴۸ به مسئله افشای اسرار پزشکی در زمان حیات بیمار اشاره دارد و سکوت مطلق نسبت به پس از فوت او دارد. همچنین قانون اساسی جمهوری اسلامی ایران در اصل ۲۲، بر مصونیت حیثیت و کرامت افراد تأکید دارد، اما مشخص نکرده که آیا این حمایت پس از مرگ نیز ادامه دارد یا خیر. در عمل، این خلأ موجب شده که بیمارستان‌ها، پزشکان، یا حتی شرکت‌های بیمه با پرسش‌هایی اساسی مواجه شوند؛ از جمله اینکه آیا می‌توان اطلاعات پزشکی متوفی را به وراث ارائه داد؟ آیا می‌توان از داده‌های دیجیتال متوفی برای تحقیقات علمی یا استفاده‌های آماری بهره برد؟ یا اینکه چه نهادی اختیار دارد درباره سرنوشت این داده‌ها تصمیم‌گیری کند؟ در حوزه دیجیتال نیز خلأ قانونی گسترده‌تر است، چرا که با توسعه سریع فناوری‌های سلامت، حجم زیادی از اطلاعات بیماران در قالب پرونده‌های الکترونیکی، سامانه‌های سلامت، اپلیکیشن‌ها و فضای ابری ذخیره می‌شود. در صورت فوت بیمار، این داده‌ها همچنان در سرورهای بیمارستان یا شرکت‌های فناوری باقی می‌ماند و عدم وجود قانون مشخص، سبب می‌شود که نهادهای نگهدارنده داده با ابهام درباره ادامه ذخیره‌سازی، حذف یا انتقال این اطلاعات روبه‌رو باشند. این مسئله نه‌تنها از نظر حقوقی مخاطره‌آمیز است، بلکه می‌تواند حریم خصوصی افراد را نیز به‌صورت جدی تهدید کند (۴۳). از سوی دیگر، نبود مقررات صریح موجب می‌شود که وراث، پزشکان و بیمه‌گذاران در صورت بروز اختلاف درباره افشای اطلاعات، ناچار به رجوع به رویه‌های غیرثابت قضایی شوند که خود بر پیچیدگی پرونده‌ها می‌افزاید. همچنین در مواردی که لازم است اطلاعات برای اثبات خطای پزشکی یا تعیین علت فوت در اختیار مراجع قرار گیرد، نبود قانون مدون، زمینه سوءاستفاده یا حتی امتناع غیرقانونی از ارائه اطلاعات را فراهم می‌کند. در نظام‌های حقوقی پیشرفته، همچون کشورهای عضو اتحادیه اروپا یا آمریکا، قوانین مشخصی مانند مقررات عمومی حفاظت از داده‌ها وجود دارد که در آن‌ها، وضعیت داده‌های پزشکی متوفی، مدت زمان نگهداری، نحوه دسترسی بازماندگان، شرایط افشا و حتی حقوق فرد پیش از مرگ برای تعیین سرنوشت داده‌هایش، به‌روشنی تعریف شده است. نبود چنین چارچوبی در ایران نه‌تنها باعث بروز تضاد میان منافع شخصی و عمومی می‌شود، بلکه اعتماد عمومی به نظام سلامت و امنیت داده‌های پزشکی را نیز تضعیف می‌کند (۴۴). در مجموع، نبود قانون صریح در باره داده‌های دیجیتال پزشکی پس از مرگ، یک خلأ مهم در نظام حقوقی ایران به شمار می‌رود که برای برطرف شدن آن، نیاز به تدوین مقررات جامع، روزآمد و منطبق با تحولات فناوری است؛ مقرراتی که هم حرمت فرد درگذشته را حفظ کند و هم حقوق و نیازهای ذی‌نفعان زنده را در چارچوب‌های مشخص قانونی تأمین نماید (۴۵).

نتیجه گیری

با توجه به بررسی‌های صورت‌گرفته در خصوص مرگ دیجیتال و وضعیت حقوقی داده‌ها و هویت مجازی بیماران پس از مرگ، می‌توان نتیجه گرفت که نظام

حقوقی ایران با چالش‌های جدی و خلأهای آشکار در این زمینه مواجه است. رشد فناوری‌های دیجیتال در حوزه سلامت، گسترش پرونده‌های الکترونیکی، اطلاعات ژنتیکی، و حضور بیماران در بسترهای مجازی، سبب شده که هویت افراد دیگر محدود به موجودیت فیزیکی آن‌ها نباشد و پس از مرگ نیز آثار حقوقی و اجتماعی متعددی داشته باشد.

در عین حال، قوانین موجود در ایران، به‌ویژه در زمینه حریم خصوصی، افشای اطلاعات پزشکی، و مالکیت داده‌ها، هنوز هم با نگاه سنتی و غیر دیجیتال نگاشته شده‌اند و پاسخگوی نیازهای نوظهور عصر فناوری نیستند. بر اساس مبانی فقهی، اصولی چون حرمت افشای سرّ مؤمن، قاعده احترام میت، و لزوم حفظ حرمت انسان حتی پس از مرگ، همگی بر ضرورت صیانت از حریم خصوصی و هویت مجازی متوفی تأکید دارند. همچنین از نظر حقوقی، هرچند برخی مواد قانونی به‌طور پراکنده به مفاهیمی مانند ا سرار پز شکی، رازداری حرفه‌ای، و کرامت ان سانی ا شاره دارند، اما هیچ قانون مشخصی که سرنوشت داده‌های پزشکی دیجیتال و اطلاعات شخصی افراد را پس از مرگ روشن کند، وجود ندارد.

این خلأ قانونی، سبب بروز ت ضاد میان حقوق متوفی، حقوق وراث، نهادهای درمانی و شرکت‌های بیمه شده و زمینه‌ساز برخوردهای سلیقه‌ای یا حتی نقض حقوق بنیادین افراد می شود. در این شرایط، تدوین یک قانون جامع و شفاف که وضعیت داده‌های دیجیتال پز شکی و هویت مجازی افراد پس از فوت را مشخص کند، کاملاً ضروری به نظر می‌رسد. چنین قانونی باید ضمن احترام به حریم خصوصی و حقوق انسانی متوفی، امکان دسترسی قانونی، محدود و کنترل‌شده را برای بازماندگان، مقامات قضایی، یا نهادهای مسئول فراهم آورد. همچنین، لازم است که بیماران در زمان حیات، حق تعیین سرنوشت داده‌های خود پس از مرگ را داشته باشند، از جمله در قالب وصیت دیجیتال یا رضایت‌نامه‌های خاص. این رویکرد می‌تواند گامی مهم در جهت تحقق عدالت، صیانت از کرامت انسانی، و انطباق نظام حقوقی ک شور با تحولات فناوری و نیازهای روز جامعه باشد.

References

1. Lupton D. Digital death: how technology is shaping the end of life and death. Digital Health. 2018;4:1-9.
2. Krawczyk PM, Gallagher R. Ethical challenges in the use of digital health data after death. J Med Ethics. 2020;46(11):727-732.
3. De Stefano C, Meijerink WJHJ. Post-mortem data and privacy: a legal perspective on digital legacy. Eur J Health Law. 2019;26(3):233-251.
4. Price WN 2nd, Cohen IG. Privacy in the age of medical big data. Nat Med. 2019;25(1):37-43.
5. Hens K, Cassiman JJ, Dierickx K. Ethical, legal, and social implications of posthumous use of genetic data. Trends Biotechnol. 2018;36(6):527-529.
6. Gerrand AL, Christakis NA. Digital legacy and post-mortem privacy concerns in healthcare. JAMA. 2017;318(17):1663-1664.
7. Goodman KW. Ethics, Medicine, and Information Technology: Intelligent Machines and the Transformation of Health Care. Cambridge University Press; 2015.
8. Finlay SC, Sheehan M, Whelan C. The legal implications of electronic health records after death. Med Law Rev. 2019;27(4):603-620.
9. Coe AB, Bereznak Y, Cresswell K. Data ownership and control after death: the ethical dimensions. J Law Med Ethics. 2020;48(1):49-56.
10. Bietz MJ, Bloss CS, Calvert S. Responsible data sharing and the legacy of patient privacy. Am J Bioeth. 2016;16(11):34-36.
11. Zawati MH, Knoppers BM. Sharing genetic information post-mortem: legal and ethical challenges. Eur J Hum Genet. 2015;23(7):812-817.
12. Shabani M, Borry P. Rules for processing genetic data after death: a systematic review. Eur J Hum Genet. 2018;26(6):778-785.
13. Hernandez C, Blumenthal-Barby JS. Digital death: ethical challenges of digital remains. Am J Bioeth. 2018;18(11):29-31.
14. Shachak A, Reis S. Patient confidentiality after death: a legal and ethical review. Health Care Anal. 2016;24(2):149-165.
15. Caulfield T, Tasse AM, Kaye J. A legal framework for data privacy after death: lessons from the U.S. and Europe. Health Matrix Clevel. 2017;27(1):89-122.
16. Green MJ, Myers K, Fleisher L. Privacy and post-mortem medical data: challenges in data governance. J Law Med Ethics. 2021;49(2):217-228.
17. Hunt M, Brody H. Post-mortem data use: the

dilemma of data ownership and control. J Med Ethics. 2017;43(4):273-277.
18. Grady C, Eckstein L, Berkman B. Informed consent and data use after death: an ethical analysis. Am J Bioeth. 2019;19(9):56-67
19. Wilkinson J, Bragge P. Digital legacy and healthcare: data governance post-mortem. BMC Med Ethics. 2018;19(1):84.
20. Slobogin C. The death of privacy: protecting digital legacies in the information age. Wake Forest Law Rev. 2016;51(2):567-601.
21. Cohen IG, Mello MM. HIPAA and protecting health information in the 21st century. JAMA. 2018;320(3):231-232.
22. Greely HT. Medical privacy after death: the case for legal reform. J Law Med Ethics. 2016;44(3):493-506.
23. Meslin EM, Kahn JP. Ethics and the use of health information after death. Am J Med Genet A. 2017;173(3):735-739.
24. Balkin JM. Information fiduciaries and the future of privacy law. Geo Wash Law Rev. 2016;89(3):425-474.
25. Clift T. The right to privacy after death: a comparative legal analysis. Eur J Int Law. 2017;28(1):205-230.
26. Denecke K, Feuerriegel S. Handling of medical data after death in cloud systems. IEEE Access. 2020;8:136154-136166.
27. Mahfoudh O, Ghédira K. Privacy and data protection in electronic health records. Comput Methods Programs Biomed. 2017;140:237-246.
28. McGraw D. Building public trust in uses of health data. Health Aff (Millwood). 2020;39(5):870-877.
29. Safran C, Bloomrosen M, Hammond WE. Toward a national framework for health information exchange. J Am Med Inform Assoc. 2020;27(8):1293-1300.
30. Shabani M, Bezuidenhout L. Post-mortem biomedical data governance. J Med Ethics. 2021;47(4):265-270.
31. Koppel R, Lehmann CU. Clinical decision support and electronic health records. JAMA. 2020;323(19):1969-1970.
32. Bender JL, Cyr A, Arbuckle L. Ethical issues in digital health data management. J Med Internet Res. 2019;21(12):e14961.
33. Katsanis SH, Wagner JK. Ethical considerations in genomic data sharing after death. Genome Med. 2018;10(1):16.
34. Fogarty A, Gallo E. Digital death and legal inheritance of online assets. Int J Law Inform Technol. 2017;25(3):261-274.
35. Gerrand AL. Managing digital remains: legal perspectives on digital legacy. Comput Law Secur Rev. 2016;32(5):712-720.
36. Devlin HL, Bahadur G. Posthumous rights over health information. Med Law Rev. 2018;26(4):506-522.
37. Partridge N, Mauthner N. Consent and confidentiality after death. J Med Ethics. 2016;42(10):635-638.
38. Kottow MH. Respect for the dead in health research. J Med Ethics. 2017;43(6):377-381.
39. Nissenbaum H. Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press; 2019.
40. Khomeini, Ruhollah, Kitab al-Bay, Qom, Ismailiyan, 2001(1):20.
41. Majlisi, Mohammad Baqir, Bihar al-Anwar,1944(75):71.
42. Cohen IG. The new politics of privacy. Harv Law Rev. 2016;126(7):1876-1935.
43. Chervenak FA, McCullough LB. The ethics of managing posthumous medical data. Am J Bioeth. 2017;17(1):1-2
44. Shabani M. Data protection and genetic data in biobanks after death. Hum Genomics. 2020;14(1):28.
45. Elger BS, Capron AM. Ethical challenges in handling patient data after death. J Med Ethics. 2017;43(2):89-93.