Comparative Studies in Jurisprudence, Law, and Politics

A Comparative Study of the Jurisprudential and Legal Foundations of Personal Data Protection in Iranian Law and the Legal System of the European Union, with Emphasis on the Principle of Human Dignity

1. Ali Kari*: Department of Theology Education, Faculty of Humanities, Farhangian University, Urmia, Iran. Email: a_kari@cfu.ac.ir (Corresponding Author)

ABSTRACT

Digital transformation and the expansion of the processing of identity-related, biometric, financial, medical, and behavioral data have made the protection of personal data one of the fundamental issues of contemporary law. Violations involving such data, in addition to infringing upon privacy, may undermine individuals' autonomy, freedom of choice, dignity, and right to informational self-determination. Accordingly, the principle of human dignity constitutes a fundamental basis for regulating the limits of the collection, storage, use, and transfer of personal information. The present study aims to comparatively examine the jurisprudential and legal foundations of personal data protection in Iranian law and the legal system of the European Union, with particular emphasis on the principle of human dignity. The study employs a descriptive-analytical and comparative methodology, and the required data were collected through an examination of sources of Imamī jurisprudence, Iranian legislation, the Charter of Fundamental Rights of the European Union, and the General Data Protection Regulation (GDPR). The findings indicate that, within Imamī jurisprudence, principles such as the inherent dignity of the human person, the prohibition of unlawful inquiry and spying, the prohibition of causing harm, respect for individuals' dignity and reputation, and the requirement of consent provide substantial normative capacity for justifying the protection of personal data. In Iranian law, the Constitution, the Electronic Commerce Law, and the Computer Crimes Law also provide certain forms of protection; however, the fragmentation of regulations, limitations in their scope of application, the absence of an independent supervisory authority, and the lack of a comprehensive accountability mechanism have reduced the effectiveness of these protections. In contrast, the European Union, by recognizing data protection as a fundamental right, has established a coherent legal framework based on transparency, purpose limitation, data minimization, valid consent, accountability, and independent supervision. The findings of the study indicate that the development of a comprehensive personal data protection regime in Iran should be grounded in the capacities of Islamic jurisprudence and the principle of human dignity and, while taking into account the requirements of the domestic legal system, should draw upon the effective mechanisms developed within the European Union.

Keywords: *Personal Data, Human Dignity, Imamī Jurisprudence, Iranian Law, European Union*

How to cite: Kari, A. (2027). A Comparative Study of the Jurisprudential and Legal Foundations of Personal Data Protection in Iranian Law and the Legal System of the European Union, with Emphasis on the Principle of Human Dignity. *Comparative Studies in Jurisprudence, Law, and Politics*, *9*(5), 1-19.

Submit Date: 10 May 2026
Revise Date: 14 August 2026
Accept Date: 21 August 2026
Initial Publish Date: 21 August 2026
Final Publish Date: 22 December 2027

پژوهش‌های تطبیقی فقه، حقوق و سیاست

مطالعه تطبیقی مبانی فقهی و حقوقی حمایت از داده‌های شخصی در حقوق ایران و نظام حقوقی اتحادیه اروپا با تأکید بر اصل کرامت انسانی

۱. علی کاری*: دانشجوی کارشناسی ارشد فقه و مبانی حقوق اسلامی، گروه آموزش الهیات، دانشکده علوم انسانی، دانشگاه فرهنگیان، ارومیه، ایران. پست الکترونیک: a_kari@cfu.ac.ir (نویسنده مسئول)

چکیده

تحول دیجیتال و گسترش پردازش داده‌های هویتی، زیستی، مالی، پزشکی و رفتاری، حمایت از داده‌های شخصی را به یکی از مسائل اساسی حقوق معاصر تبدیل کرده است. نقض این داده‌ها افزون بر تعرض به حریم خصوصی، می‌تواند استقلال، آزادی انتخاب، حیثیت و حق تعیین سرنوشت اطلاعاتی اشخاص را مخدوش سازد؛ ازاین‌رو، اصل کرامت انسانی مبنایی بنیادین برای تنظیم حدود گردآوری، نگهداری، استفاده و انتقال اطلاعات شخصی محسوب می‌شود. پژوهش حاضر با هدف مطالعه تطبیقی مبانی فقهی و حقوقی حمایت از داده‌های شخصی در حقوق ایران و نظام حقوقی اتحادیه اروپا، با تأکید بر اصل کرامت انسانی، انجام شده است. روش پژوهش توصیفی ـ تحلیلی و تطبیقی است و داده‌های مورد نیاز از طریق مطالعه منابع فقه امامیه، قوانین ایران، منشور حقوق بنیادین اتحادیه اروپا و مقررات عمومی حفاظت از داده‌ها گردآوری شده‌اند. یافته‌ها نشان می‌دهد که در فقه امامیه، اصولی همچون کرامت ذاتی انسان، حرمت تجسس، منع اضرار، احترام به حیثیت و آبروی اشخاص و لزوم اذن، ظرفیت مناسبی برای توجیه حمایت از داده‌های شخصی دارند. در حقوق ایران نیز قانون اساسی، قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای حمایت‌هایی را پیش‌بینی کرده‌اند، اما پراکندگی مقررات، محدودیت قلمرو اجرا، نبود مرجع نظارتی مستقل و فقدان سازوکار جامع پاسخ‌گویی، اثربخشی این حمایت‌ها را کاهش داده است. در مقابل، اتحادیه اروپا با شناسایی حفاظت از داده به‌عنوان حقی بنیادین، نظامی منسجم مبتنی بر شفافیت، محدودیت هدف، کمینه‌سازی داده، رضایت معتبر، پاسخ‌گویی و نظارت مستقل ایجاد کرده است. نتیجه پژوهش بیانگر آن است که تدوین نظام جامع حمایت از داده‌های شخصی در ایران باید بر ظرفیت‌های فقهی و اصل کرامت انسانی استوار شود و ضمن توجه به اقتضائات حقوق داخلی، از سازوکارهای کارآمد اتحادیه اروپا بهره گیرد.

واژگان کلیدی: *داده‌های شخصی، کرامت انسانی، فقه امامیه، حقوق ایران، اتحادیه اروپا*

نحوه استناددهی: کاری، علی. (۱۴۰۶). مطالعه تطبیقی مبانی فقهی و حقوقی حمایت از داده‌های شخصی در حقوق ایران و نظام حقوقی اتحادیه اروپا با تأکید بر اصل کرامت انسانی. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۹(۵)، ۱۹-۱.

تاریخ ارسال: ۲۰ اردیبهشت ۱۴۰۵
تاریخ بازنگری: ۲۳ مرداد ۱۴۰۵
تاریخ پذیرش: ۳۰ مرداد ۱۴۰۵
تاریخ چاپ اولیه: ۳۰ مرداد ۱۴۰۵
تاریخ چاپ نهایی: ۱ دی ۱۴۰۶

مقدمه

گسترش دولت الکترونیکی، شبکه‌های اجتماعی، خدمات بانکی برخط، سکوهای تجاری و سامانه‌های مبتنی بر هوش مصنوعی، داده‌های شخصی را به یکی از مهم‌ترین منابع قدرت اقتصادی و اجتماعی تبدیل کرده است. اطلاعات هویتی، مالی، زیستی، پزشکی، مکانی و رفتاری افراد در مقیاسی گسترده جمع‌آوری و پردازش می‌شود و امکان ترکیب این داده‌ها، پیش‌بینی رفتار، دسته‌بندی اشخاص و تصمیم‌گیری خودکار درباره آنان را فراهم می‌سازد. در چنین وضعیتی، نقض داده‌های شخصی صرفاً تعرض به یک دارایی اطلاعاتی نیست، بلکه می‌تواند استقلال فرد، آزادی انتخاب، آبرو، امنیت روانی و امکان تعیین سرنوشت او را مخدوش کند. ازاین‌رو، حمایت از داده‌های شخصی با اصل کرامت انسانی پیوندی بنیادین دارد؛ زیرا تبدیل انسان به موضوع شناسایی، نظارت یا بهره‌برداری اطلاعاتی بدون آگاهی و اختیار مؤثر او، با شناسایی انسان به‌عنوان موجودی صاحب اراده و غایت مستقل ناسازگار است (Ansari, 2004).

در مبانی اسلامی، اگرچه اصطلاح «داده شخصی» با معنای فنی امروز سابقه نداشته است، مجموعه‌ای از اصول و قواعد می‌تواند مبنای حمایت از آن قرار گیرد. تکریم بنی‌آدم در آیه ۷۰ سوره اسراء، منع تجسس در آیه ۱۲ سوره حجرات و منع ورود بدون اذن به حریم اشخاص در آیه ۲۷ سوره نور، جایگاه احترام به شخصیت، اسرار و قلمرو اختصاصی انسان را نشان می‌دهد. قواعد لاضرر، حرمت ایذاء، احترام مال و عرض مؤمن، منع افشای سر و اصل سلطه انسان بر شئون متعلق به خویش نیز ظرفیت آن را دارند که در مواجهه با گردآوری، افشا، انتقال و بهره‌برداری زیان‌بار از اطلاعات شخصی به کار گرفته شوند. بااین‌حال، استخراج یک نظام منسجم حمایت از داده از این مبانی، نیازمند تبیین رابطه میان کرامت ذاتی انسان، رضایت، حق کنترل اطلاعات، مصالح عمومی و حدود مداخله حکومت است. حمایت فقهی از حریم خصوصی غالباً از طریق مفاهیمی مانند منع تجسس، حرمت غیبت، مالکیت، منع اضرار و احترام به حیثیت صورت گرفته و هنوز درباره تبدیل این مبانی پراکنده به حقوق مشخص صاحب داده، تکالیف پردازشگر و ضمانت‌اجرای نهادی اتفاق‌نظر روشنی وجود ندارد (Ansari, 2004).

در نظام حقوقی ایران نیز برخی ظرفیت‌های حمایتی قابل شناسایی است. اصول ۲۲ و ۲۵ قانون اساسی، حیثیت، حقوق، مسکن، مکاتبات و ارتباطات اشخاص را از تعرض مصون می‌دانند و اصل ۲۳ از تفتیش عقاید جلوگیری می‌کند (Ansari, 2004). مواد ۵۸ و ۵۹ قانون تجارت الکترونیکی، پردازش برخی داده‌های حساس بدون رضایت صریح را ممنوع کرده و اصولی مانند تعیین هدف، تناسب، صحت داده، دسترسی، اصلاح و محو اطلاعات را پذیرفته‌اند (Heydari & Jafari, 2020). قانون جرایم رایانه‌ای نیز دسترسی غیرمجاز و انتشار زیان‌بار یا هتک‌کننده اسرار خصوصی را جرم‌انگاری کرده است. با وجود این، حمایت‌های موجود پراکنده، بخشی و غالباً واکنشی‌اند. محدود بودن قلمرو قانون تجارت الکترونیکی به «داده‌پیام» در بستر مبادلات الکترونیکی، ابهام در دامنه داده‌های مشمول حمایت، فقدان چارچوب جامع برای پردازش بخش عمومی و خصوصی و ضعف سازوکار نظارت مستقل از مهم‌ترین کاستی‌ها به شمار می‌آیند (Heydari & Jafari, 2020). استمرار فرایند تقنینی طرح‌ها و لوایح مرتبط نیز نشان می‌دهد که ایران هنوز با مسئله طراحی یک نظام جامع و لازم‌الاجرای حفاظت از داده روبه‌رو است.

در مقابل، اتحادیه اروپا حمایت از داده‌های شخصی را به‌عنوان حقی مستقل و بنیادین صورت‌بندی کرده است. ماده ۱ منشور حقوق بنیادین اتحادیه، کرامت انسانی را تعرض‌ناپذیر می‌داند؛ ماده ۷ از زندگی خصوصی و ارتباطات حمایت می‌کند و ماده ۸ به‌صراحت حق هر شخص بر حفاظت از داده‌های مربوط به خود، پردازش منصفانه برای اهداف معین، دسترسی، اصلاح و نظارت مرجع مستقل را به رسمیت می‌شناسد (Latifzadeh et al., 2022). مقررات عمومی حفاظت از داده‌ها نیز با پذیرش اصول قانونمندی، شفافیت، محدودیت هدف، کمینه‌سازی

داده، صحت، محدودیت نگهداری، امنیت و پاسخ‌گویی، مجموعه‌ای از حقوق اجرایی برای صاحب داده و تکالیف مشخص برای کنترل‌گران و پردازشگران ایجاد کرده است. حق دسترسی، اصلاح، حذف، محدودسازی پردازش، قابلیت انتقال داده، اعتراض، حفاظت از داده از مرحله طراحی، ارزیابی اثرات پردازش‌های پرخطر و نظارت مراجع مستقل، این نظام را از حمایت صرفاً کیفری فراتر برده است (Latifzadeh et al., 2022).

با وجود انسجام نسبی الگوی اروپایی، حق حفاظت از داده در آن نیز مطلق نیست و باید با آزادی بیان، امنیت عمومی، فعالیت اقتصادی و سایر حقوق بنیادین بر پایه ضرورت و تناسب متوازن شود. همین امر نشان می‌دهد که مطالعه تطبیقی نباید به مقایسه ظاهری مواد قانونی یا انتقال مستقیم مقررات اروپایی به حقوق ایران محدود شود. مسئله اصلی آن است که آیا مبانی فقه امامیه و اصول حقوقی ایران ظرفیت تأسیس یک نظام حق‌محور و کرامت‌مدار را دارند و این ظرفیت چگونه می‌تواند به قواعد روشن درباره رضایت معتبر، محدودیت هدف، حداقل‌گرایی داده، حقوق صاحب داده، مسئولیت پردازشگر، نظارت مستقل و جبران خسارت تبدیل شود.

پژوهش‌های موجود عمدتاً یا حریم خصوصی را از منظر فقه و حقوق ایران بررسی کرده‌اند یا مقررات اروپایی را به‌صورت توصیفی معرفی کرده‌اند. پیوند منظم میان مبانی فقهی، اصل کرامت انسانی و سازوکارهای اجرایی حفاظت از داده کمتر موضوع تحلیل تطبیقی قرار گرفته است. بنابراین، مسئله محوری پژوهش حاضر، شناسایی وجوه اشتراک و افتراق مبانی فقهی و حقوقی حمایت از داده‌های شخصی در ایران و اتحادیه اروپا و ارزیابی میزان انطباق قواعد موجود با الزامات کرامت انسانی است. بر این اساس، پژوهش در پی پاسخ به این پرسش است که اصل کرامت انسانی چگونه می‌تواند مبنای توجیه، تفسیر و تحدید پردازش داده‌های شخصی قرار گیرد و با بهره‌گیری سنجیده از تجربه اتحادیه اروپا، چه الگوی حقوقی متناسبی برای رفع خلأهای تقنینی و تضمین مؤثر حقوق اشخاص در ایران قابل ارائه است.

پیشینه پژوهش

ادبیات حقوقی مرتبط با حمایت از داده‌های شخصی را می‌توان در سه حوزه کلی بررسی کرد: مطالعات ناظر بر حریم خصوصی و مبانی فقهی آن، پژوهش‌های مربوط به حمایت قانونی از داده‌های شخصی در حقوق ایران و مطالعات تبیین‌کننده نظام حفاظت از داده‌ها در اتحادیه اروپا. بررسی این آثار نشان می‌دهد که با وجود توجه روزافزون به ابعاد حقوقی پردازش اطلاعات، پیوند نظام‌مند میان اصل کرامت انسانی، قواعد فقه امامیه و سازوکارهای اجرایی حفاظت از داده‌ها همچنان نیازمند مطالعه‌ای مستقل است.

در میان مطالعات فارسی، انصاری (Ansari, 2004) از نخستین پژوهشگرانی است که حریم خصوصی را در حقوق اسلام، حقوق تطبیقی و نظام حقوقی ایران به‌صورت منظم بررسی کرده است. وی با تحلیل مبانی ارزشی حریم خصوصی، آن را با استقلال فردی، کرامت انسانی، مصونیت شخصیت و جلوگیری از تبدیل انسان به موضوع نظارت و بهره‌برداری دیگران مرتبط می‌داند. اهمیت این پژوهش در آشکار ساختن ظرفیت منابع اسلامی و قواعد حقوقی موجود برای حمایت از قلمرو خصوصی اشخاص است. بااین‌حال، مطالعه مزبور پیش از توسعه شبکه‌های اجتماعی، پردازش کلان‌داده‌ها، تصمیم‌گیری الگوریتمی و تصویب مقررات عمومی حفاظت از داده‌های اتحادیه اروپا انجام شده است؛ ازاین‌رو، مفاهیمی مانند پاسخ‌گویی کنترل‌گر، حفاظت از داده در طراحی و به‌طور پیش‌فرض، ارزیابی اثر پردازش و حق اعتراض به تصمیم‌گیری خودکار را پوشش نمی‌دهد.

حسینی و برزویی (Hosseini & Barzoui, 2017) در پژوهش «مبانی و مؤلفه‌های فقهی حمایت از حریم خصوصی افراد در فضای مجازی»، ظرفیت قواعد و اصول فقهی برای حمایت از حریم خصوصی در محیط دیجیتال را بررسی کرده‌اند. این نویسندگان با استناد به

قواعدی مانند حرمت مؤمن، احترام به حریم اشخاص، منع تجسس، منع استراق سمع، حرمت افشای اسرار و منع اشاعه فحشا، مداخله غیرمجاز در اطلاعات خصوصی را از منظر فقه امامیه قابل منع دانسته‌اند. مزیت این مطالعه، انتقال مفاهیم فقهی حریم خصوصی به فضای مجازی است؛ بااین‌حال، موضوع اصلی آن حمایت از حریم خصوصی است و به استقلال مفهومی حق حفاظت از داده‌های شخصی، مسئولیت کنترل‌گر و پردازشگر، حقوق مستمر صاحب داده و ضرورت ایجاد مرجع نظارتی مستقل نمی‌پردازد.

حیدری و جعفری (Heydari & Jafari, 2020) حمایت کیفری از داده‌پیام‌های شخصی را در قانون تجارت الکترونیکی بررسی کرده‌اند. یافته‌های آنان نشان می‌دهد که محدود بودن قلمرو حمایت ماده ۵۸ این قانون، تمرکز آن بر برخی داده‌های حساس و فقدان پوشش کامل رفتارهایی مانند گردآوری، تحلیل، ترکیب، انتقال و بهره‌برداری ثانویه از داده‌ها، موجب شده است حمایت کیفری موجود با تحولات فناوری تناسب کافی نداشته باشد. این مطالعه در شناسایی خلأهای جرم‌انگاری اهمیت دارد، اما بیشتر بر واکنش کیفری پس از وقوع نقض متمرکز است و تکالیف پیشگیرانه، حقوق صاحبان داده و سازوکارهای نظارت اداری را بررسی نمی‌کند.

اکبری و فلاحیان (Hosseini & Barzoui, 2017) نیز با مطالعه حریم خصوصی در نظام حقوقی ایران و اسلام، ارتباط آن را با کرامت ذاتی انسان و ضرورت حمایت از استقلال و حیثیت اشخاص تبیین کرده‌اند. نتیجه این پژوهش بر وجود پشتوانه‌های فقهی و قانون اساسی برای حمایت از حریم خصوصی و ضرورت تدوین قانون جامع تأکید دارد. با وجود ارزش نظری این مطالعه، حفاظت از داده‌های شخصی در آن عمدتاً یکی از مصادیق حریم خصوصی تلقی شده است؛ درحالی‌که حق حفاظت از داده، پردازش اطلاعات غیرمحرمانه و حتی داده‌هایی را که در فضای عمومی در دسترس قرار گرفته‌اند نیز، در صورت انتساب به شخص معین یا قابل شناسایی، در بر می‌گیرد.

لطیف‌زاده، قبولی‌درافشان، محسنی و عابدی (Latifzadeh et al., 2022) در پژوهشی تطبیقی، اسباب مشروعیت پردازش داده‌های شخصی در ماده ۶ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا را با ظرفیت‌های حقوق ایران مقایسه کرده‌اند. آنان نشان داده‌اند که مبانی‌ای مانند رضایت، ضرورت اجرای قرارداد، انجام تکلیف قانونی، حمایت از منافع حیاتی و تأمین منافع مشروع را می‌توان در منابع حقوق ایران بازشناسی کرد؛ اما فقدان چارچوب تقنینی منسجم، حدود و شرایط استناد به این مبانی را مبهم ساخته است. این پژوهش در انتقال یکی از مهم‌ترین عناصر مقررات اروپایی به حقوق ایران موفق است، ولی تمام چرخه حیات داده، از مرحله گردآوری تا حذف، انتقال، نظارت و جبران خسارت را پوشش نمی‌دهد.

در مطالعات جدیدتر، حاجعلی و حسین‌پور (Latifzadeh et al., 2022) خلأهای تقنینی حمایت از داده‌های شخصی کودکان در ایران را با توجه به مقررات اتحادیه اروپا و بریتانیا بررسی کرده‌اند. این پژوهش بر ضرورت رضایت معتبر، طراحی متناسب با سن، شفافیت قابل فهم برای کودک، کمینه‌سازی داده و ارزیابی آثار پردازش تأکید دارد. اهمیت آن در توجه به گروه‌های آسیب‌پذیر و پردازش‌های پرخطر است؛ بااین‌حال، قلمرو آن به داده‌های کودکان محدود است و یک نظریه عمومی درباره مبانی فقهی و حقوقی حمایت از داده‌های همه اشخاص ارائه نمی‌کند.

در ادبیات لاتین، لینسکی با تفکیک حفاظت از داده از مفهوم سنتی حریم خصوصی، آن را حقی بنیادین و ابزاری برای توزیع قدرت میان اشخاص، دولت‌ها و بنگاه‌های پردازشگر معرفی کرده است (Latifzadeh et al., 2022). هیجمانس نیز با بررسی جایگاه ماده ۸ منشور حقوق بنیادین اتحادیه اروپا، نقش نظارت مستقل، کنترل قضایی و اجرای هماهنگ را در اثربخشی حق حفاظت از داده برجسته می‌سازد (Latifzadeh et al., 2022). برکان با تمرکز بر رویه دیوان دادگستری اتحادیه اروپا، «هسته اساسی» حقوق حریم خصوصی و حفاظت از

داده‌ها را معیاری برای ارزیابی مداخلات شدید و نامتناسب می‌داند (Latifzadeh et al., 2022). همچنین هوفنگل، واندر اسلوت و بورگسیوس نشان داده‌اند که مقررات عمومی حفاظت از داده‌ها صرفاً مجموعه‌ای از قواعد مربوط به رضایت نیست، بلکه نظامی چندلایه متشکل از اصول پردازش، حقوق صاحب داده، تکالیف پیشگیرانه، پاسخ‌گویی، نظارت مستقل و ضمانت اجراست (Latifzadeh et al., 2022).

جمع‌بندی پیشینه نشان می‌دهد که سه خلأ اساسی همچنان باقی است. نخست، بخش عمده مطالعات فقهی و حقوقی ایران، حفاظت از داده‌های شخصی را در چارچوب مفهوم حریم خصوصی تحلیل کرده‌اند؛ درنتیجه، استقلال نسبی حق حفاظت از داده و شمول آن بر تمام مراحل پردازش، حتی در مواردی که داده الزاماً محرمانه نیست، کمتر تبیین شده است. دوم، در بسیاری از پژوهش‌های تطبیقی، مقررات ایران و اتحادیه اروپا در کنار یکدیگر توصیف شده‌اند، اما نحوه تبدیل مبانی فقهی و ارزش‌های بنیادین به حقوق قابل مطالبه، تکالیف فنی و سازوکارهای نهادی روشن نشده است. سوم، اصل کرامت انسانی غالباً در سطح یک ارزش کلی و انتزاعی باقی مانده و کارکرد تفسیری آن در موضوعاتی مانند اعتبار رضایت، منع بهره‌برداری تحقیرآمیز، محدودیت هدف، کمینه‌سازی داده، نمایه‌سازی، تصمیم‌گیری خودکار، پردازش داده‌های حساس و تناسب نظارت عمومی کمتر بررسی شده است.

نوآوری پژوهش حاضر در ارائه چارچوبی سه‌سطحی برای پیوند دادن مبانی ارزشی، قواعد فقهی و سازوکارهای اجرایی حمایت از داده‌های شخصی است. در سطح هنجاری، کرامت انسانی به‌عنوان منشأ حق شخص بر کنترل نسبی اطلاعات مربوط به خود و حد نهایی مداخله دولت و اشخاص خصوصی در شخصیت اطلاعاتی انسان تحلیل می‌شود. در سطح فقهی ـ حقوقی، قواعدی مانند حرمت تجسس، لزوم اذن، امانت‌داری، منع اضرار، احترام به عرض و آبروی اشخاص و حرمت افشای اسرار، به اصول عملیاتی قانونمندی، شفافیت، محدودیت هدف، کمینه‌سازی داده، محرمانگی، امنیت پردازش و جبران خسارت ارتباط داده می‌شوند. در سطح نهادی نیز سازوکارهای اتحادیه اروپا، از جمله حقوق قابل اعمال صاحب داده، ارزیابی اثر، حفاظت در طراحی، اعلام نقض، پاسخ‌گویی کنترل‌گر و نظارت مستقل، از حیث امکان استفاده در نظام حقوقی ایران ارزیابی می‌شوند.

بر این اساس، پژوهش حاضر به دنبال انتقال صوری یا تقلید کامل از الگوی اتحادیه اروپا نیست؛ بلکه می‌کوشد با اتکا به مبانی فقه امامیه، اصول قانون اساسی و تجربه تنظیمی اتحادیه اروپا، الگویی بومی، حق‌محور، فناوری‌خنثی و قابل اجرا برای حمایت از داده‌های شخصی در ایران ارائه کند. وجه متمایز پژوهش در این است که کرامت انسانی را از یک مبنای اعلامی به معیاری عملی برای قانون‌گذاری، تفسیر حقوق داده، طراحی تکالیف پردازشگران و سنجش مشروعیت مداخلات اطلاعاتی تبدیل می‌کند.

روش پژوهش

پژوهش حاضر از نظر هدف، بنیادی ـ کاربردی و از حیث ماهیت، کیفی است و به روش کتابخانه‌ای، اسنادی، توصیفی ـ تحلیلی و تطبیقی انجام می‌شود. داده‌های پژوهش از طریق مطالعه منابع معتبر فقه امامیه، شامل آیات قرآن کریم، روایات منقول در منابعی مانند الکافی، وسائل‌الشیعه و تهذیب‌الاحکام، آثار فقهی و قواعدی و پژوهش‌های تخصصی گردآوری شده‌اند. در بخش حقوق ایران، قانون اساسی، قانون مسئولیت مدنی، قانون تجارت الکترونیکی، قانون جرایم رایانه‌ای، قانون انتشار و دسترسی آزاد به اطلاعات، قانون مدیریت داده‌ها و اطلاعات ملی و دیدگاه‌های حقوقدانان ایرانی بررسی می‌شوند. در بخش اتحادیه اروپا نیز منشور حقوق بنیادین، مقررات عمومی حفاظت از داده‌ها، رهنمودهای هیئت اروپایی حفاظت از داده و آرای شاخص دیوان دادگستری اتحادیه اروپا مبنای تحلیل قرار می‌گیرند. مقایسه دو نظام با

رویکرد مسئله‌محور و بر اساس کارکرد حقوقی قواعد، شامل مبانی ارزشی حمایت، قلمرو داده و پردازش، مشروعیت پردازش، حقوق صاحبان داده، تکالیف پردازشگران و ساختار نظارت و جبران خسارت صورت می‌گیرد. در این فرایند، ابتدا مفاد و قلمرو قواعد هر نظام استخراج و تحلیل می‌شود و سپس امکان بهره‌گیری از تجربه اتحادیه اروپا با توجه به مبانی فقه امامیه، قانون اساسی و ساختار حقوقی ایران ارزیابی می‌گردد.

مفهوم داده‌های شخصی و تمایز آن از حریم خصوصی

داده شخصی در معنای حقوقی، هرگونه اطلاعات مرتبط با شخص طبیعی معین یا قابل شناسایی است. مطابق بند نخست ماده ۴ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا، شناسایی شخص ممکن است به‌طور مستقیم، مانند نام، شماره ملی یا تصویر چهره، یا به‌صورت غیرمستقیم، از طریق داده‌های مکانی، شناسه‌های برخط، اطلاعات زیستی، ژنتیکی، اقتصادی، اجتماعی یا ترکیب چند داده صورت گیرد. بنابراین، شخصی بودن داده به محرمانه بودن، حساس بودن یا قالب خاص آن وابسته نیست؛ بلکه معیار اصلی، وجود ارتباط میان اطلاعات و شخص معین یا قابل شناسایی است.

داده‌ای که به‌گونه‌ای برگشت‌ناپذیر ناشناس شده و با ابزارهایی که استفاده از آن‌ها به‌طور متعارف محتمل است نتوان آن را به شخص معینی منتسب کرد، از قلمرو حمایت ویژه داده‌های شخصی خارج می‌شود. در مقابل، «مستعارسازی» به معنای جایگزینی شناسه‌های مستقیم با کد یا علامت، لزوماً موجب خروج داده از قلمرو حمایت نمی‌شود. بند پنجم ماده ۴ و ملاحظه ۲۶ مقررات عمومی حفاظت از داده‌ها تصریح می‌کنند که اگر اطلاعات مستعارشده با استفاده از داده‌های تکمیلی قابلیت انتساب مجدد به شخص را داشته باشند، همچنان داده شخصی محسوب می‌شوند (Latifzadeh et al., 2022).

پردازش نیز مفهومی گسترده دارد و مجموعه اعمالی مانند گردآوری، ثبت، دسته‌بندی، ذخیره‌سازی، اصلاح، بازیابی، مشاهده، استفاده، تطبیق، ترکیب، انتقال، انتشار، محدودسازی، حذف و نابودی داده را در بر می‌گیرد. درنتیجه، حمایت حقوقی نباید صرفاً در زمان افشا یا انتشار اطلاعات فعال شود. گردآوری بیش از اندازه، نگهداری نامحدود، استفاده برای هدفی متفاوت، ایجاد نمایه رفتاری و انتقال به اشخاص ثالث نیز ممکن است حقوق و آزادی‌های فرد را در معرض خطر قرار دهد.

در حقوق ایران، تعریف جامع و فرابخشی از داده شخصی که بر تمام فعالیت‌های دولتی و خصوصی حاکم باشد، وجود ندارد. ماده ۵۸ قانون تجارت الکترونیکی، ذخیره، پردازش و توزیع برخی داده‌پیام‌های شخصی را که بیانگر ریشه قومی یا نژادی، دیدگاه‌های عقیدتی و مذهبی، خصوصیات اخلاقی و وضعیت جسمانی، روانی یا جنسی اشخاص هستند، بدون رضایت صریح آنان غیرقانونی می‌داند. این ماده گامی مهم در شناسایی داده‌های حساس است، اما حمایت آن به بستر مبادلات الکترونیکی و گروه خاصی از اطلاعات محدود شده است. مواد ۵۹ و ۶۰ همین قانون نیز شرایطی مانند تعیین هدف، تناسب داده با هدف، صحت اطلاعات و فراهم کردن امکان دسترسی و اصلاح را پیش‌بینی کرده‌اند. با وجود این، این مقررات یک نظام جامع برای تمام مراحل و انواع پردازش داده ایجاد نمی‌کنند (Heydari & Jafari, 2020).

قانون جرایم رایانه‌ای نیز رفتارهایی مانند دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و انتشار غیرمجاز صوت، تصویر یا اسرار خصوصی را جرم‌انگاری کرده است. این قانون عمدتاً بر مقابله کیفری با رفتارهای معین تمرکز دارد و تعریف جامع داده شخصی، حقوق صاحب داده و تکالیف پیشگیرانه دارنده یا پردازشگر داده را ارائه نمی‌کند. قانون انتشار و دسترسی آزاد به اطلاعات نیز افشای اطلاعات

شخصی را محدود ساخته است، اما موضوع اصلی آن تعیین حدود دسترسی به اطلاعات عمومی است، نه تنظیم جامع چرخه پردازش داده‌های شخصی.

حریم خصوصی و حفاظت از داده‌های شخصی دارای قلمروهای مرتبط، اما متمایزند. حریم خصوصی در مفهوم سنتی، حق مصونیت شخص در برابر مداخله ناموجه در زندگی خصوصی، مسکن، مکاتبات، ارتباطات، بدن، روابط خانوادگی و امور محرمانه اوست. اصول ۲۲ و ۲۵ قانون اساسی از مهم‌ترین مبانی این حمایت در حقوق ایران هستند. اصل ۲۲، حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص را از تعرض مصون می‌داند و اصل ۲۵ بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات و تجسس را جز به حکم قانون ممنوع اعلام می‌کند.

در مقابل، حفاظت از داده‌های شخصی مجموعه‌ای از قواعد مستمر درباره تمام چرخه عمر داده است؛ حتی زمانی که اطلاعات مورد پردازش محرمانه یا متعلق به خلوت شخص نباشد. برای مثال، نام و شماره تماس مشتری ممکن است به‌تنهایی راز خصوصی محسوب نشود، اما دریافت‌کننده این اطلاعات همچنان باید آن‌ها را در حدود هدف اعلام‌شده استفاده کند، از جمع‌آوری اطلاعات زائد بپرهیزد، امنیت داده را تأمین کند و امکان دسترسی و اصلاح اطلاعات را فراهم سازد. از همین جهت، انصاری حریم خصوصی را با کرامت، استقلال و جلوگیری از ابزار شدن انسان مرتبط می‌داند، اما حمایت از داده را می‌توان صورت تخصصی‌تر و نهادی‌شده همین حمایت در محیط اطلاعاتی دانست (Ansari, 2004).

تفاوت دیگر به ساختار ضمانت اجرا مربوط است. در الگوی سنتی حریم خصوصی، حمایت غالباً پس از مداخله یا ورود ضرر فعال می‌شود و شخص زیان‌دیده باید وقوع تعرض و رابطه آن با خسارت را اثبات کند. در نظام جامع حفاظت از داده، نقض تکالیفی مانند فقدان مبنای قانونی، اطلاع‌رسانی نکردن، جمع‌آوری بیش از حد یا فقدان تدابیر امنیتی، ممکن است مستقل از اثبات خسارت محسوس، موجب مداخله مرجع ناظر شود. بنابراین، حفاظت از داده را می‌توان نظامی برای تنظیم قدرت اطلاعاتی دولت‌ها و بنگاه‌ها و تضمین کنترل نسبی شخص بر جریان اطلاعات مربوط به خود دانست. این کنترل مطلق نیست و ممکن است بر اساس قانون و با رعایت ضرورت، تناسب، حقوق دیگران و منافع عمومی محدود شود.

مفهوم و جایگاه اصل کرامت انسانی

کرامت انسانی بیانگر ارزش ذاتی انسان است؛ ارزشی که به موقعیت اقتصادی، تابعیت، جنسیت، عقیده، سلامت، توانایی جسمانی یا میزان سودمندی او برای دولت و بازار وابسته نیست. نتیجه حقوقی پذیرش کرامت آن است که انسان نباید صرفاً وسیله‌ای برای تحقق منافع دیگران یا موضوعی منفعل برای گردآوری، تحلیل و بهره‌برداری اطلاعاتی تلقی شود. برخورداری از شخصیت مستقل، احترام به حیثیت، امکان تصمیم‌گیری آگاهانه و مصونیت از رفتارهای تحقیرآمیز، از مهم‌ترین آثار این اصل‌اند (Ansari, 2004; Javadi Amoli, 2005).

مبنای قرآنی کرامت در آیه «وَلَقَدْ كَرَّمْنَا بَنِي آدَمَ» آشکار است (اسراء: ۷۰). اطلاق «بنی‌آدم» نشان می‌دهد که اصل تکریم به نوع انسان تعلق دارد. این کرامت در اندیشه اسلامی با مسئولیت اخلاقی و اجتماعی همراه است، اما مسئولیت‌پذیری انسان، مجوز تعرض بی‌ضابطه به آبرو، اسرار، ارتباطات و تمامیت معنوی او نیست. در منابع روایی نیز حرمت و حیثیت مؤمن مورد تأکید قرار گرفته و تعرض به عرض و آبروی او رفتاری ناروا شناخته شده است (Al-Hurr al-Amili, 1988; Al-Kulayni, 1986).

در حقوق اساسی ایران، بند ششم اصل دوم، «کرامت و ارزش والای انسان و آزادی توأم با مسئولیت او در برابر خدا» را از پایه‌های نظام جمهوری اسلامی معرفی می‌کند. اصل ۲۲، حیثیت و حقوق اشخاص را مصون از تعرض می‌داند و اصل ۲۵ از محرمانگی ارتباطات و ممنوعیت تجسس حمایت می‌کند. اصل ۴۰ نیز مقرر می‌دارد هیچ‌کس نمی‌تواند اعمال حق خویش را وسیله اضرار به دیگری یا تجاوز به منافع عمومی قرار دهد. از مجموع این اصول می‌توان نتیجه گرفت که جمع‌آوری، تحلیل یا انتشار اطلاعات اشخاص باید دارای مبنای قانونی باشد و به حیثیت، آزادی و حقوق آنان آسیب نامتناسب وارد نکند.

کرامت در حقوق داده صرفاً مبنایی اخلاقی نیست و می‌تواند دست‌کم پنج کارکرد حقوقی داشته باشد. نخست، شخص را صاحب حق می‌شناسد و او را از جایگاه موضوع منفعل پردازش خارج می‌کند. دوم، ضرورت اطلاع‌رسانی روشن و اخذ رضایت آگاهانه را توجیه می‌کند. سوم، بهره‌برداری تحقیرآمیز، تبعیض‌آفرین یا فریبنده از اطلاعات اشخاص را محدود می‌سازد. چهارم، لزوم ایجاد امکان دسترسی، اصلاح، اعتراض و جبران خسارت را توضیح می‌دهد. پنجم، معیاری برای ارزیابی مشروعیت و تناسب نظارت‌های دولتی و خصوصی فراهم می‌آورد. این اصل بر اعتبار رضایت نیز اثر می‌گذارد. رضایتی که در نتیجه اکراه، فریب، وابستگی شدید یا فقدان آگاهی شکل گرفته باشد، نمی‌تواند مجوزی نامحدود برای بهره‌برداری از داده‌های شخصی ایجاد کند. مطابق ماده ۱۹۰ قانون مدنی، قصد و رضای طرفین از شرایط اساسی صحت معامله است و ماده ۱۹۹ نیز رضای ناشی از اشتباه یا اکراه را مؤثر نمی‌داند. ماده ۹۵۹ قانون مدنی نیز سلب کلی حق تمتع یا اجرای تمام یا بخشی از حقوق مدنی را نمی‌پذیرد. بنابراین، شرطی که به موجب آن شخص تمام اختیارات کنونی و آینده خود نسبت به داده‌هایش را به‌صورت کلی، دائمی و نامحدود اسقاط کند، از منظر قواعد عمومی قراردادها، حقوق شخصیت و کرامت انسانی با ایراد جدی مواجه است.

در حقوق اتحادیه اروپا نیز ماده ۱ منشور حقوق بنیادین، کرامت انسان را تعرض‌ناپذیر می‌داند و مواد ۷ و ۸ به‌ترتیب حق احترام به زندگی خصوصی و حق حفاظت از داده‌های شخصی را به رسمیت می‌شناسند. ملاحظه ۴ مقررات عمومی حفاظت از داده‌ها اعلام می‌کند که پردازش داده‌ها باید در خدمت انسان باشد و حق حفاظت از داده، با رعایت اصل تناسب و سایر حقوق بنیادین اعمال شود. اهمیت الگوی اروپایی برای حقوق ایران در آن است که کرامت را از سطح ارزش اعلامی به اصول و ضمانت اجراهایی مانند شفافیت، پاسخ‌گویی، محدودیت هدف، کمینه‌سازی داده و نظارت مستقل تبدیل کرده است. متن رسمی منشور و متن رسمی مقررات عمومی حفاظت از داده‌ها

مبانی فقهی حمایت از داده‌های شخصی

کرامت و احترام به شخصیت انسان

اصل تکریم بنی‌آدم، پایه ارزشی حمایت از تمامیت مادی و معنوی انسان محسوب می‌شود. آیه ۷۰ سوره اسراء، انسان را برخوردار از کرامتی می‌داند که تعرض به حیثیت، آبرو و شخصیت او را محتاج دلیل معتبر می‌سازد. در روایات نیز حرمت مؤمن جایگاهی والا دارد و تعرض به عرض و آبروی او مورد نکوهش قرار گرفته است (Al-Hurr al-Amili, 1988; Al-Kulayni, 1986).

داده شخصی صرفاً مجموعه‌ای از اعداد و نشانه‌های فاقد پیوند با انسان نیست؛ زیرا ممکن است هویت، وضعیت جسمانی، عقاید، روابط، رفتارها و ویژگی‌های شخصیتی فرد را بازنمایی کند. تحریف، افشای ناموجه یا استفاده تحقیرآمیز از این اطلاعات می‌تواند به شخصیت و حیثیت فرد آسیب وارد کند. ازاین‌رو، داده‌های مربوط به انسان را نمی‌توان صرفاً شیئی اقتصادی یا منبعی اداری تلقی کرد. هرگونه بهره‌برداری از آن باید با کرامت، حقوق شخصیت و احترام به عرض و آبروی اشخاص سازگار باشد (Ansari, 2004; Hosseini & Barzoui, 2017).

پیوند داده با شخصیت انسان سبب می‌شود که الگوی مالکیت مطلق برای تحلیل تمام روابط اطلاعاتی کافی نباشد. شخص می‌تواند برای هدفی معین و مدتی مشخص، اجازه استفاده از اطلاعات خود را صادر کند، اما انتقال کلی و همیشگی تمام اختیارات نسبت به داده‌های فعلی و آینده، به‌ویژه در وضعیت نابرابری قدرت قراردادی، با حقوق شخصیت و ماده ۹۵۹ قانون مدنی قابل مناقشه است. از این منظر، «اذن یا مجوز بهره‌برداری مقید» با ماهیت داده‌های شخصی سازگارتر از انتقال مطلق مالکیت است.

حرمت تجسس و منع تحصیل پنهانی اطلاعات

مهم‌ترین مبنای قرآنی منع تجسس، فرمان «وَلَا تَجَسَّسُوا» در آیه ۱۲ سوره حجرات است. تجسس در معنای فقهی، جست‌وجو و کاوش برای دستیابی به امور پنهان و اطلاعاتی است که صاحب آن تمایلی به آشکار شدنشان ندارد. موضوع این حکم تنها ورود فیزیکی به حریم دیگری نیست و می‌تواند دسترسی پنهانی به مکاتبات، ارتباطات و اطلاعات شخصی را نیز در بر گیرد (Ansari, 2004; Kharrazi, 2009).

در محیط دیجیتال، نفوذ به حساب کاربری، نصب مخفیانه ابزار رهگیری، شنود ارتباطات، بازیابی پنهانی پیام‌ها، خرید و استفاده از داده‌های سرقت‌شده و ترکیب شناسه‌های پراکنده برای کشف اوصاف خصوصی شخص، ممکن است از حیث موضوع و کارکرد در قلمرو تجسس قرار گیرند. این تحلیل با اصل ۲۵ قانون اساسی و مقررات قانون جرایم رایانه‌ای درباره دسترسی و شنود غیرمجاز نیز هماهنگ است.

بااین‌حال، هرگونه گردآوری اطلاعات را نمی‌توان تجسس حرام محسوب کرد. تحقق تجسس به عواملی مانند پنهانی بودن اطلاعات، شیوه دستیابی، انتظار متعارف شخص از محرمانگی، هدف گردآوری و فقدان مجوز معتبر بستگی دارد. همچنین، تجسس مبتنی بر حکم قضایی یا ضرورت قانونی، تابع شرایط و محدودیت‌های خاص است. صرف ادعای امنیت یا منفعت عمومی برای رفع حرمت کافی نیست؛ مداخله باید بر پایه قانون روشن، ضرورت واقعی، محدودیت موضوعی و زمانی و رعایت تناسب صورت گیرد. خرازی نیز میان صدق عنوان تجسس و وجود دلیل ثانوی برای رفع حکم حرمت تفکیک می‌کند؛ بنابراین، انگیزه مفید ممکن است در حکم اثرگذار باشد، اما لزوماً عنوان تجسس را از بین نمی‌برد (Kharrazi, 2009).

اذن، رضایت و رعایت حدود اجازه

آیات ۲۷ و ۲۸ سوره نور ورود به خانه دیگران را پیش از استیناس، سلام و کسب اجازه ممنوع می‌کنند. موضوع مستقیم این آیات، حریم مکانی است؛ اما با توجه به ملاک احترام به قلمرو اختصاصی انسان، می‌توان از آن‌ها برای تقویت اصل لزوم اذن در دسترسی به اطلاعات شخصی استفاده کرد. این تسری باید در حد ملاک مشترک انجام شود و نباید ادعا کرد که آیات مزبور مستقیماً درباره پردازش داده‌های دیجیتال حکم کرده‌اند (Ansari, 2004; Hosseini & Barzoui, 2017).

اذن معتبر نیازمند آگاهی، اختیار و تعیین حدود استفاده است. مواد ۱۹۰ و ۱۹۱ قانون مدنی نیز قصد و رضای معتبر را از عناصر اساسی اعمال حقوقی می‌دانند. بر این اساس، سکوت، گزینه‌های از پیش انتخاب‌شده، پنهان کردن هدف واقعی پردازش، ارائه توضیحات پیچیده و نامفهوم یا وابسته کردن خدمت ضروری به پذیرش پردازش غیرضروری، نمی‌تواند در همه موارد رضایت معتبر ایجاد کند. ماده ۵۸ قانون تجارت الکترونیکی نیز پردازش داده‌پیام‌های حساس را به رضایت صریح شخص منوط کرده است.

اذن، مجوزی نامحدود نیست و حدود آن بر اساس هدف اعلام‌شده، شرایط توافق و فهم عرفی طرفین تعیین می‌شود. استفاده از داده برای هدفی ناسازگار، انتقال آن به اشخاص ثالث ناشناخته یا نگهداری اطلاعات پس از پایان ضرورت، می‌تواند خروج از حدود اذن محسوب شود.

مواد ۲۲۰ و ۲۲۵ قانون مدنی نیز آثار عرفی و متعارف قرارداد را در تعیین حدود تعهدات مؤثر می‌دانند. بنابراین، رضایت به دریافت یک خدمت را نمی‌توان به‌طور خودکار رضایت به تمام پردازش‌های فعلی و آینده تلقی کرد.

رجوع از اذن نیز باید با توجه به ماهیت رابطه حقوقی بررسی شود. در مواردی که پردازش صرفاً بر اذن شخص استوار است و حق مکتسب، تعهد قراردادی معتبر یا تکلیف قانونی مستقلی وجود ندارد، رجوع از اذن می‌تواند ادامه پردازش را فاقد مجوز کند. با وجود این، رجوع از رضایت نمی‌تواند تعهدات قانونی مانند نگهداری اسناد مالی یا اجرای حکم قضایی را از میان ببرد. این تفکیک برای جلوگیری از مطلق‌انگاری رضایت ضروری است.

امانت‌داری، رازداری و منع افشای اسرار

آیه ۵۸ سوره نساء به ادای امانت فرمان می‌دهد و آیه ۲۷ سوره انفال مؤمنان را از خیانت در امانت بازمی‌دارد. در منابع روایی امامیه نیز حفظ اسرار و خودداری از افشای آنچه در اختیار شخص قرار گرفته، مورد تأکید قرار دارد (Al-Hurr al-Amili, 1988; Al-Kulayni, 1986; Al-Tamimi al-Amidi, 1987). بر این اساس، هنگامی که اطلاعات برای ارائه خدمت، درمان، انجام معامله یا اجرای وظیفه اداری در اختیار شخص یا سازمانی قرار می‌گیرد، دریافت‌کننده نسبت به حفظ و استفاده هدفمند از آن مسئول است.

تصرف امانی در داده، دریافت‌کننده را مجاز نمی‌سازد که اطلاعات را خارج از هدف مورد توافق استفاده کند یا در اختیار اشخاص فاقد صلاحیت قرار دهد. از این مبنا می‌توان تکالیفی مانند محرمانگی، تعیین سطح دسترسی، ثبت دسترسی کارکنان، انتخاب پیمانکار قابل اعتماد و حذف یا بازگرداندن اطلاعات پس از پایان ضرورت را استنباط و با قواعد قانونی تکمیل کرد.

امانت‌داری دیجیتال به خودداری از افشای عمدی محدود نیست. واگذاری دسترسی بیش از حد نیاز، نگهداری داده در سامانه ناامن، بی‌توجهی به آسیب‌پذیری‌های شناخته‌شده و فقدان تدابیر متعارف برای پیشگیری از نشت اطلاعات نیز ممکن است با تکلیف حفظ امانت و قاعده منع اضرار ناسازگار باشد. تعیین مصادیق دقیق اقدامات امنیتی، موضوعی تخصصی و متغیر است و باید در قوانین و استانداردهای فنی تعیین شود؛ اما اصل لزوم مراقبت را می‌توان از امانت، لاضرر و قواعد مسئولیت مدنی استنباط کرد.

البته قاعده امانت تمام وضعیت‌های پردازش داده را پوشش نمی‌دهد. برخی اطلاعات مستقیماً از شخص دریافت نمی‌شوند، بلکه از رفتار او مشاهده یا از ترکیب داده‌ها استنباط می‌شوند. در این موارد، برای ایجاد تکلیف حمایت باید افزون بر امانت، به قواعدی مانند حرمت تجسس، لاضرر، احترام به شخصیت و منع هتک حیثیت استناد کرد.

قاعده لاضرر و جبران خسارت

قاعده لاضرر از مهم‌ترین مبانی فقهی حمایت در برابر آثار زیان‌بار پردازش داده است. مستند اصلی این قاعده، حدیث «لا ضرر و لا ضرار» است که در منابع روایی امامیه نقل شده و فقها درباره مفاد و قلمرو آن به تفصیل بحث کرده‌اند (Al-Hurr al-Amili, 1988; Makarem Shirazi, 1990; Mousavi Bojnourdi, 1998).

افشای اطلاعات پزشکی، مالی، خانوادگی، اعتقادی یا حیثیتی ممکن است موجب ضرر مادی، لطمه به اعتبار، تبعیض، محرومیت شغلی یا آسیب روانی شود. در چنین مواردی، قواعد لاضرر، اتلاف و تسبیب می‌توانند مبنای منع رفتار زیان‌بار و حسب مورد، مسئولیت عامل زیان را فراهم کنند. مواد ۱ و ۲ قانون مسئولیت مدنی نیز لطمه به حیثیت، شهرت، آزادی و سایر حقوق قانونی اشخاص را در صورت ورود خسارت، موجب مسئولیت می‌دانند. ماده ۱۰ این قانون نیز امکان جبران لطمه به حیثیت و اعتبار شخصی یا خانوادگی را پیش‌بینی کرده است.

مسئولیت ممکن است ناشی از افشای عمدی داده یا بی‌احتیاطی در حفاظت از آن باشد. اگر سازمانی بدون رعایت تدابیر متعارف امنیتی زمینه دسترسی غیرمجاز را فراهم کند، مسئولیت آن می‌تواند بر مبنای تقصیر، تسبیب و نقض تکلیف قانونی بررسی شود. میزان مسئولیت به قابلیت پیش‌بینی زیان، سطح خطر پردازش، نوع داده، امکانات فنی و رابطه سببیت بستگی دارد.

احترام به عرض و منع اشاعه امور زیان‌بار

آیه ۱۲ سوره حجرات در کنار منع تجسس، از غیبت و تعرض به آبروی دیگران نهی می‌کند و آیه ۱۹ سوره نور اشاعه فحشا درباره مؤمنان را محکوم می‌سازد. از مجموع این ادله می‌توان ممنوعیت انتشار اطلاعاتی را استنباط کرد که موجب هتک حیثیت، تحقیر یا گسترش ناموجه امور خصوصی اشخاص می‌شوند. این مبنا به‌ویژه در انتشار داده‌های پزشکی، خانوادگی، جنسی و تصاویر خصوصی اهمیت دارد (Ansari, 2004; Hosseini & Barzoui, 2017).

بااین‌حال، منع افشا مطلق نیست. افشای اطلاعات ممکن است بر اساس حکم قانون، دفاع از حق، رسیدگی قضایی یا ضرورت معتبر مجاز باشد. در چنین مواردی نیز باید اصل تناسب رعایت شود و تنها اطلاعات ضروری در اختیار مرجع صالح قرار گیرد. انتشار عمومی اطلاعات، هنگامی که ارائه محدود آن به مرجع قانونی کافی است، ممکن است از حدود ضرورت فراتر رود.

نسخه زیر کوتاه‌تر، منسجم‌تر و مبتنی بر منابع اصیل فقه امامیه، قوانین ایران و اسناد رسمی اتحادیه اروپا تنظیم شده است.

قاعده لاضرر و مسئولیت ناشی از پردازش داده

قاعده لاضرر، پردازشی را که موجب زیان نامشروع مادی یا معنوی به اشخاص شود، نفی می‌کند. افشای داده‌های پزشکی، مالی یا خانوادگی ممکن است به سرقت هویت، تبعیض، لطمه به اعتبار یا آسیب روانی منتهی شود. در چنین مواردی، قواعد لاضرر، اتلاف و تسبیب می‌توانند مبنای منع رفتار زیان‌بار و مسئولیت عامل آن قرار گیرند (Al-Hurr al-Amili, 1988; Mohaghegh Damad, 2016; Mousavi Bojnourdi, 1998). مواد ۱ و ۲ قانون مسئولیت مدنی نیز ورود خسارت به حیثیت، شهرت و سایر حقوق قانونی اشخاص را موجب مسئولیت می‌دانند. ازآنجاکه برخی خسارت‌های اطلاعاتی پس از انتشار داده به‌طور کامل جبران‌پذیر نیستند، تکلیف پیشگیری، تأمین امنیت و محدودسازی پردازش را می‌توان از مجموع قواعد لاضرر، امانت و احتیاط متعارف استنباط کرد.

حرمت غیبت، اشاعه فحشا و هتک عرض

آیه ۱۲ سوره حجرات غیبت و تعرض به آبروی اشخاص و آیه ۱۹ سوره نور اشاعه فحشا در جامعه مؤمنان را منع می‌کند. در منابع روایی امامیه نیز افشای اسرار و هتک حرمت مؤمن نکوهش شده است (Al-Hurr al-Amili, 1988; Al-Kulayni, 1986). بر این اساس، انتشار تصاویر خصوصی، سوابق پزشکی و اطلاعات تحقیرآمیز، حتی در صورت صحت، ممکن است نامشروع باشد؛ زیرا حقیقت داشتن اطلاعات همواره مجوز افشای آن نیست. دادخواهی، شهادت، اجرای قانون یا تأمین مصلحت عمومی می‌تواند افشا را در حدود ضرورت مجاز سازد، مشروط بر آنکه دامنه انتشار متناسب باشد و راه کم‌زیان‌تری وجود نداشته باشد (Ansari, 2004; Hosseini & Barzoui, 2017).

حمایت از داده‌های شخصی در حقوق ایران

ظرفیت‌های قانون اساسی

قانون اساسی حق مستقلی با عنوان «حفاظت از داده‌های شخصی» مقرر نکرده، اما مبانی آن را فراهم ساخته است. بند ششم اصل دوم بر کرامت انسان، اصل ۲۲ بر مصونیت حیثیت و حقوق اشخاص، اصل ۲۳ بر منع تفتیش عقاید و اصل ۲۵ بر محرمانگی مکاتبات و ممنوعیت تجسس تأکید دارند. از مجموع این اصول می‌توان مصونیت اطلاعاتی اشخاص را استنباط کرد. عبارت «مگر به حکم قانون» در اصل ۲۵ نیز باید محدود تفسیر شود؛ به‌گونه‌ای که قانون، هدف، دامنه، مدت، مرجع دسترسی و امکان نظارت و اعتراض را مشخص کند. مجوزهای کلی و نامحدود با کرامت انسانی و اصل منع اضرار سازگار نیستند (Ansari, 2004).

قانون تجارت الکترونیکی

مواد ۵۸ تا ۶۱ قانون تجارت الکترونیکی مهم‌ترین مقررات صریح ایران درباره داده‌های شخصی‌اند. ماده ۵۸ پردازش داده‌پیام‌های مرتبط با منشأ قومی، عقاید، ویژگی‌های اخلاقی و وضعیت جسمانی، روانی یا جنسی را بدون رضایت صریح غیرقانونی می‌داند. ماده ۵۹ نیز تعیین هدف، تناسب داده، صحت اطلاعات و امکان دسترسی، اصلاح و محو را مقرر کرده است. بااین‌حال، این حمایت به بستر مبادلات الکترونیکی محدود است و تعریف جامع داده شخصی، تکلیف اعلام نقض، ارزیابی خطر و مرجع ناظر مستقل را در بر نمی‌گیرد (Heydari & Jafari, 2020).

قانون جرایم رایانه‌ای و مسئولیت مدنی

قانون جرایم رایانه‌ای، دسترسی و شنود غیرمجاز و انتشار زیان‌بار صوت، تصویر یا اسرار خصوصی اشخاص را جرم‌انگاری کرده است. این قانون بیشتر ماهیت کیفری و واکنشی دارد و رفتارهایی مانند جمع‌آوری بیش از نیاز، نگهداری نامحدود یا استفاده ثانویه از داده را به‌صورت جامع تنظیم نمی‌کند. در حوزه جبران خسارت نیز مواد ۱، ۲ و ۱۰ قانون مسئولیت مدنی امکان مطالبه خسارت مادی و معنوی ناشی از نقض حیثیت و حقوق اشخاص را فراهم می‌کنند؛ هرچند اثبات تقصیر، رابطه سببیت و میزان خسارت در پردازش‌های پیچیده همچنان دشوار است.

دسترسی آزاد به اطلاعات و حکمرانی داده

مواد ۱۴ و ۱۵ قانون انتشار و دسترسی آزاد به اطلاعات، افشای اطلاعات شخصی و خصوصی را محدود می‌کنند. قانون مدیریت داده‌ها و اطلاعات ملی مصوب ۱۴۰۱ نیز تبادل داده میان دستگاه‌ها و پایگاه‌های اطلاعاتی را سامان می‌دهد، اما جهت‌گیری اصلی آن افزایش کارآمدی اداری است و حقوق تفصیلی اشخاص، مبانی پردازش و نظارت مستقل در مرکز آن قرار ندارد. بنابراین، حقوق ایران دارای حمایت‌های پراکنده است، اما هنوز قانون جامع و هماهنگی برای تنظیم تمام چرخه عمر داده‌های شخصی ندارد.

حمایت از داده‌های شخصی در اتحادیه اروپا

بنیان‌های حقوقی

مواد ۱، ۷ و ۸ منشور حقوق بنیادین اتحادیه اروپا به‌ترتیب کرامت انسانی، احترام به زندگی خصوصی و حفاظت از داده‌های شخصی را شناسایی کرده‌اند. ماده ۸ منشور، پردازش منصفانه، تعیین هدف، وجود رضایت یا مبنای قانونی، حق دسترسی و اصلاح و نظارت مرجع مستقل را ضروری می‌داند. ماده ۵۲ نیز محدودیت این حقوق را به وجود قانون، هدف مشروع، ضرورت و تناسب منوط کرده است. دیوان دادگستری

اتحادیه اروپا نیز در پرونده‌های Digital Rights Ireland و Schrems II بر ممنوعیت نظارت گسترده و ضرورت وجود راه جبران مؤثر تأکید کرده است.

اصول و مشروعیت پردازش

ماده ۵ مقررات عمومی حفاظت از داده‌ها، اصول قانونمندی، انصاف، شفافیت، محدودیت هدف، کمینه‌سازی، صحت، محدودیت نگهداری، امنیت و پاسخ‌گویی را مقرر می‌کند. ماده ۶ نیز رضایت، اجرای قرارداد، تکلیف قانونی، منافع حیاتی، وظیفه عمومی و منافع مشروع را از مبانی پردازش می‌داند. بنابراین، رضایت تنها مبنای پردازش نیست و باید آزادانه، آگاهانه، مشخص و قابل پس‌گرفتن باشد. ماده ۹ نیز برای داده‌های حساس، از جمله اطلاعات سلامت، ژنتیکی، زیستی، مذهبی و سیاسی، حمایت شدیدتری مقرر کرده است (Latifzadeh et al., 2022).

حقوق صاحب داده و نظارت

مقررات عمومی حفاظت از داده‌ها، حقوق اطلاع، دسترسی، اصلاح، حذف، محدودسازی، انتقال و اعتراض را شناسایی کرده است. ماده ۲۲ نیز در برابر برخی تصمیم‌های کاملاً خودکار دارای آثار حقوقی یا مهم، تضمین‌هایی مانند مداخله انسانی و امکان اعتراض پیش‌بینی می‌کند. مواد ۲۵، ۳۲ و ۳۵ به‌ترتیب حفاظت در طراحی، امنیت متناسب با خطر و ارزیابی اثر را الزامی می‌سازند. اجرای این مقررات بر عهده مراجع نظارتی مستقل است که اختیار تحقیق، صدور دستور، توقف پردازش و اعمال جریمه دارند.

تحلیل تطبیقی دو نظام حقوقی

تفاوت اصلی دو نظام در فقدان مبانی حمایتی در ایران نیست؛ بلکه در میزان تبدیل این مبانی به حقوق، تکالیف و ضمانت اجراست. فقه امامیه با قواعد کرامت، منع تجسس، اذن، امانت، لاضرر و حرمت هتک عرض، پشتوانه هنجاری مناسبی فراهم می‌کند. قانون اساسی و قوانین عادی ایران نیز بخشی از این حمایت را پذیرفته‌اند، اما مقررات همچنان پراکنده‌اند. اتحادیه اروپا همین ارزش‌ها را در قالب تعریف جامع داده، اصول پردازش، حقوق صاحب داده، تکالیف پیشگیرانه و نظارت مستقل عملیاتی کرده است.

جدول ۱. مقایسه تطبیقی

محور	فقه و حقوق ایران	اتحادیه اروپا
مبنای حمایت	کرامت، منع تجسس، امانت و لاضرر	کرامت، حریم خصوصی و حق مستقل حفاظت از داده
قلمرو	تعاریف پراکنده و بخشی	تعریف جامع و فناوری‌خنثی
حقوق شخص	محدود و پراکنده	اطلاع، دسترسی، اصلاح، حذف و اعتراض
پیشگیری	عمدتاً حمایت پس از نقض	حفاظت در طراحی و ارزیابی اثر
نظارت	فقدان مرجع مستقل جامع	مراجع تخصصی و مستقل

ازاین‌رو، استفاده از تجربه اتحادیه اروپا به معنای تقلید تقنینی نیست. عناصر قابل اقتباس باید با فقه امامیه، قانون اساسی و ساختار اداری ایران سازگار شوند. معیار مشترک برای مداخله در داده‌ها نیز می‌تواند وجود مبنای قانونی روشن، هدف مشروع، ضرورت و تناسب باشد.

کاستی‌های حقوق ایران و راهکارهای پیشنهادی

مهم‌ترین کاستی حقوق ایران، فقدان قانونی جامع و فناوری‌خنثی است. قانون آینده باید داده شخصی، داده حساس، پردازش، کنترل‌گر و پردازشگر را تعریف و مبانی مشروعیت پردازش را مشخص کند. همچنین، حقوق آگاهی، دسترسی، اصلاح، حذف، اعتراض و حمایت در برابر تصمیم‌های خودکار باید به‌صورت قابل مطالبه شناسایی شوند.

تأسیس مرجع نظارتی مستقل، الزام حفاظت از داده در طراحی، ارزیابی اثر پردازش‌های پرخطر و اعلام رخدادهای امنیتی نیز ضروری است. ضمانت اجرا باید ترکیبی از دستور اصلاح یا توقف، جریمه اداری، جبران خسارت مادی و معنوی و در موارد عمدی و شدید، پاسخ کیفری باشد. استثناهای امنیتی نیز باید قانونی، ضروری، متناسب، زمان‌مند و قابل نظارت باشند.

یافته‌های پژوهش نشان می‌دهد که حمایت فقهی از داده‌های شخصی بر یک دلیل منفرد استوار نیست. کرامت، ارزش موضوع حمایت؛ منع تجسس، شیوه تحصیل اطلاعات؛ اذن، حدود اختیار شخص؛ امانت، نحوه نگهداری؛ لاضرر، پیشگیری و جبران؛ و حرمت هتک عرض، آثار انتشار را تبیین می‌کند. بنابراین، تحلیل داده شخصی صرفاً بر مبنای مالکیت، با ماهیت شخصیتی آن سازگار نیست.

یافته دیگر، تفاوت میان «کفایت مبنا» و «کفایت نظام حقوقی» است. وجود قواعد فقهی و اصول قانون اساسی به‌تنهایی برای حمایت مؤثر کافی نیست؛ این مبانی باید به حقوق روشن، تکالیف مشخص، مرجع مستقل و ضمانت اجرای مؤثر تبدیل شوند. تجربه اتحادیه اروپا در تعریف جامع، پاسخ‌گویی، ارزیابی اثر و نظارت مستقل قابل استفاده است، مشروط بر آنکه با ساختار حقوقی ایران سازگار شود.

نتیجه‌گیری

فقه امامیه و قانون اساسی ایران ظرفیت مناسبی برای حمایت از داده‌های شخصی دارند. تکریم انسان، حرمت تجسس، لزوم اذن، امانت‌داری، منع اضرار و احترام به حیثیت می‌توانند مبنای محدودسازی گردآوری، استفاده و افشای ناموجه داده باشند. بااین‌حال، قوانین ایران بخشی و پراکنده‌اند و تعریف جامع، حقوق یکپارچه صاحب داده، تکالیف پیشگیرانه و مرجع ناظر مستقل در آن‌ها کامل نیست.

بر این اساس، تدوین قانون جامع حفاظت از داده‌های شخصی ضروری است. این قانون باید ضمن اتکا به فقه امامیه و اصول قانون اساسی، تعریف فناوری‌خنثی داده، اصل پاسخ‌گویی، حقوق دسترسی و اعتراض، حمایت از داده‌های حساس، ارزیابی اثر، اعلام رخداد و نظارت مستقل را پیش‌بینی کند. چنین الگویی می‌تواند اصل کرامت انسانی را از یک ارزش کلی به معیار عملی حکمرانی داده تبدیل سازد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

The rapid expansion of digital government, social networks, online banking, commercial platforms, data-driven services, and artificial intelligence systems has transformed personal data into a major source of economic, administrative, and social power. Identity-related, financial, biometric, medical, locational, and behavioral information is now collected, combined, analyzed, and transferred on an unprecedented scale, enabling organizations not only to identify individuals but also to profile them, predict their behavior, classify them into categories, and make automated or semi-automated decisions affecting their opportunities and rights. Under these conditions, the protection of personal data cannot be reduced to the protection of confidential information or to conventional notions of secrecy. Unlawful or disproportionate data processing may affect individual autonomy, freedom of choice, reputation, psychological security, equality, and the capacity of individuals to exercise meaningful control over information concerning themselves. This broader understanding

establishes a direct connection between personal data protection and the principle of human dignity, because treating individuals merely as objects of surveillance, prediction, or informational exploitation is inconsistent with recognizing them as autonomous bearers of rights and intrinsic worth (Ansari, 2004; Javadi Amoli, 2005). Within Imamī jurisprudence, although the technical concept of "personal data" did not historically exist in its contemporary form, a considerable normative foundation for its protection can be identified in the principles of human dignity, the prohibition of spying and intrusive inquiry, respect for reputation and honor, the requirement of permission, the obligation to preserve entrusted information, the prohibition of causing harm, and the protection of private affairs (Hosseini & Barzoui, 2017; Kharrazi, 2009). In Iranian law, these jurisprudential foundations are reflected, albeit incompletely, in constitutional guarantees of dignity, privacy, communications, and freedom from unlawful investigation, as well as in statutory provisions governing electronic commerce, computer-related offenses, and civil liability. By contrast, the European Union has developed a more coherent and rights-based framework in which personal data protection is explicitly recognized as a fundamental right and is operationalized through detailed principles, enforceable data-subject rights, accountability duties, preventive safeguards, and independent supervision (Latifzadeh et al., 2022). Against this background, the present study seeks to provide a comparative analysis of the jurisprudential and legal foundations of personal data protection in Iranian law and the legal system of the European Union, with particular emphasis on human dignity as a normative principle capable of connecting ethical foundations, legal rights, institutional duties, and mechanisms of accountability.

The principal objective of the study is to determine whether the normative resources of Imamī jurisprudence and Iranian law are capable of supporting a comprehensive, rights-oriented, and dignity-based system of personal data protection comparable in functional terms, though not necessarily identical in institutional design, to the European model. The study therefore focuses on several interrelated questions: how human dignity can justify limitations on the collection, storage, use, disclosure, combination, and transfer of personal information; how consent, permission, confidentiality, non-maleficence, and respect for personal honor can be translated from jurisprudential principles into contemporary data-protection rules; and which features of the European Union framework may be adapted to Iranian law without disregarding its constitutional and jurisprudential foundations. Particular attention is given to the distinction between privacy and personal data protection. Privacy traditionally protects individuals against unjustified intrusion into their private life, home, correspondence, body, family relations, and confidential affairs, whereas data protection regulates the entire life cycle of information even when the relevant information is not inherently secret. Thus, information such as a name, contact number, public identifier, or behavioral pattern may still require legal protection because the essential criterion is not secrecy but identifiability and the effects of processing on the individual. This distinction is consistent with the broader Iranian literature on privacy, which links protection of the private sphere to autonomy, dignity, and resistance to the instrumentalization of individuals (Ansari, 2004; Hosseini & Barzoui, 2017). The European approach reinforces this distinction by treating lawful processing as a continuous regulatory obligation rather than merely as a prohibition against disclosure. Its emphasis on purpose limitation, data minimization, transparency, accountability, valid consent, and continuing rights of access, rectification, objection, and erasure illustrates how a dignity-based conception of informational autonomy can be converted into operational legal standards (Latifzadeh et al., 2022). Accordingly, the comparative analysis is not confined to textual similarities between

laws but examines whether each system can transform foundational values into specific rights, organizational duties, preventive obligations, supervisory mechanisms, and remedies.

Methodologically, the research is fundamental-applied in purpose, qualitative in nature, and based on a library, documentary, descriptive-analytical, and comparative approach. The jurisprudential part of the study examines Qurʾanic principles, Imamī narrations, classical jurisprudential works, legal maxims, and contemporary scholarship relevant to human dignity, privacy, spying, permission, confidentiality, trust, harm, and reputation. Particular reliance is placed on foundational Imamī sources addressing the inviolability of believers, secrecy, trust, and the prohibition of harmful conduct (Al-Hurr al-Amili, 1988; Al-Kulayni, 1986; Al-Tamimi al-Amidi, 1987). The legal analysis of Iran covers constitutional principles, the Electronic Commerce Law, the Computer Crimes Law, civil-liability rules, and other statutory instruments that directly or indirectly regulate access to and processing of personal information. Existing Iranian scholarship is used to assess the scope and shortcomings of these fragmented protections, particularly in relation to electronic data messages, sensitive information, unlawful access, and disclosure (Heydari & Jafari, 2020). The comparative component examines the principal characteristics of the European Union data-protection model, especially the recognition of data protection as a fundamental right, the existence of lawful grounds for processing, the special treatment of sensitive data, the rights granted to data subjects, and the responsibilities imposed on controllers and processors (Latifzadeh et al., 2022). The comparison is problem-oriented rather than purely formal: the two legal systems are evaluated according to the functions performed by their rules, including the normative basis of protection, the definition and scope of personal data, legitimacy of processing, the legal status of consent, obligations of confidentiality and security, prevention of harmful processing, rights of access and objection, institutional supervision, and compensation for damage. This method enables the study to distinguish between the existence of normative foundations and the existence of a fully developed regulatory system, a distinction that is essential for assessing the present condition of Iranian data law.

The findings regarding Imamī jurisprudence demonstrate that protection of personal data can be supported by a network of mutually reinforcing principles rather than by a single jurisprudential rule. Human dignity provides the overarching normative justification by recognizing the individual as a subject of rights whose personality, honor, autonomy, and private sphere cannot be treated merely as instruments of governmental or commercial interests (Ansari, 2004; Javadi Amoli, 2005). The prohibition of spying and intrusive investigation establishes an important limit on secret acquisition of information and can extend, by functional analogy, to unauthorized access to digital communications, covert surveillance, hidden tracking, and efforts to infer concealed characteristics from fragmented data (Kharrazi, 2009). The requirement of permission supports the proposition that access to or use of personal information must ordinarily occur within a defined and intelligible scope, while the legal effect of such permission depends on genuine awareness, voluntariness, and limitation to the agreed purpose. This reasoning is compatible with the broader jurisprudential and legal understanding that permission cannot reasonably be interpreted as unlimited authorization for all present and future uses of information. The principles of trustworthiness and confidentiality further establish that information entrusted to physicians, banks, employers, online platforms, administrative bodies, and other recipients cannot legitimately be repurposed or disclosed beyond the purpose for which it was obtained (Al-Kulayni, 1986; Al-Tamimi al-Amidi, 1987). In addition, the rule of no harm provides a basis for preventing and remedying data practices that lead to material or non-material injury, including reputational harm, discrimination, identity theft, psychological

injury, or social exclusion (Makarem Shirazi, 1990; Mohaghegh Damad, 2016; Mousavi Bojnourdi, 1998). The prohibition of violating personal honor and exposing private matters similarly supports restrictions on the dissemination of medical, familial, sexual, religious, or otherwise dignity-sensitive information (Hosseini & Barzoui, 2017). Taken together, these principles show that Imamī jurisprudence possesses substantial capacity to justify contemporary data-protection norms, although this capacity must still be translated into precise statutory rights and institutional duties.

The comparative legal findings reveal a significant asymmetry between Iran and the European Union. Iranian law contains several important protective elements, but these remain dispersed across different legal instruments and are not organized into a comprehensive and technology-neutral data-protection regime. Constitutional guarantees protect dignity, reputation, communications, and freedom from unlawful investigation, while the Electronic Commerce Law introduces specific safeguards for certain categories of personal data and recognizes requirements such as explicit consent, purpose specification, proportionality, accuracy, access, correction, and deletion. Nevertheless, its practical scope is limited, particularly because much of its language is tied to electronic transactions and data messages rather than to all public- and private-sector processing activities (Heydari & Jafari, 2020). Criminal law also prohibits certain forms of unauthorized access, interception, and harmful disclosure, but this model is primarily reactive and does not comprehensively regulate excessive collection, indefinite retention, secondary use, profiling, or organizational accountability. The European Union framework, by contrast, structures data protection as an integrated system based on legality, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, security, and accountability. It recognizes multiple lawful bases for processing rather than treating consent as the sole justification, while at the same time requiring consent, where relied upon, to be freely given, specific, informed, and withdrawable (Latifzadeh et al., 2022). It also provides data subjects with continuing procedural and substantive rights and imposes preventive duties concerning security, high-risk processing, organizational accountability, and responsible design. The central difference, therefore, is not that Iranian jurisprudence and law lack normative support for protecting personal data; rather, the European system has more effectively converted foundational values into clear definitions, enforceable rights, ex ante duties, institutional supervision, and structured remedies. This distinction between normative adequacy and regulatory adequacy constitutes one of the study's most important findings and indicates that the principal challenge facing Iranian law is the institutional and legislative operationalization of already recognizable ethical, jurisprudential, and constitutional foundations.

In conclusion, the study demonstrates that the protection of personal data in Iran can be grounded in a coherent combination of Imamī jurisprudential principles, constitutional values, and contemporary legal requirements without requiring the uncritical transplantation of a foreign regulatory model. Human dignity can serve as the central normative principle connecting the prohibition of intrusive information gathering, the requirement of meaningful authorization, duties of confidentiality and security, restrictions on harmful disclosure, and the right to seek effective redress. The analysis further shows that the principal weakness of the current Iranian framework lies not in the absence of protective values but in the fragmentation of legal rules, the limited scope of existing statutes, the lack of unified terminology, the absence of comprehensive and enforceable data-subject rights, insufficient preventive duties for controllers and processors, and the lack of an independent supervisory structure capable of overseeing both public and private processing. A future comprehensive data-protection law should therefore define personal and sensitive data in technology-neutral terms, regulate the full life cycle of processing, establish clear lawful grounds,

require transparency and purpose limitation, recognize rights of access, correction, deletion, and objection, impose security and accountability obligations, regulate automated decision-making and high-risk processing, and provide effective administrative, civil, and, where necessary, criminal remedies. Independent supervision should form an essential part of this framework, while public-security exceptions should be narrowly framed, legally authorized, necessary, proportionate, time-limited, and subject to review. Such an approach would make it possible to transform human dignity from an abstract constitutional and jurisprudential value into an operational standard for data governance and would provide a more coherent basis for balancing technological development, administrative efficiency, commercial innovation, public interests, and the fundamental rights of individuals in Iran.

References

Al-Hurr al-Amili, M. i. a.-H. (1988). *Wasa'il al-Shi'a ila Tahsil Masa'il al-Shari'a*. Mu'assasat Al al-Bayt.

Al-Kulayni, M. i. Y. q. (1986). *Al-Kafi*. Dar al-Kutub al-Islamiyya.

Al-Tamimi al-Amidi, A. a.-W. (1987). *Ghurar al-Hikam wa Durar al-Kalim*. Islamic Culture Publishing Office.

Ansari, B. (2004). Privacy and Its Protection in Islamic Law, Comparative Law, and Iranian Law. *Journal of the Faculty of Law and Political Science, University of Tehran*(66), 1-54.

Heydari, A. M., & Jafari, A. (2020). Crimes against Personal Data Messages in Electronic Commerce. *Criminal Law Research Quarterly*, *11*(1), 51-74.

Hosseini, M., & Barzoui, M. (2017). Jurisprudential Foundations and Components of Protecting Individuals' Privacy in Cyberspace. *Islamic human rights studies*(13), 115-137.

Javadi Amoli, A. (2005). *Right and Duty in Islam*. Esra Publishing Center.

Kharrazi, S. M. (2009). An Inquiry into the Jurisprudential Ruling on Espionage and Investigation. *Ahl al-Bayt Jurisprudence Quarterly*(26).

Latifzadeh, M., Ghabouli Darafshan, S. M. M., Mohseni, S., & Abedi, M. (2022). Explaining the Grounds of Legitimacy for Personal Data Processing from the Perspective of European Union and Iranian Law. *Legal Studies*, *14*(3), 325-364. https://doi.org/10.22099/jls.2022.40620.4390

Makarem Shirazi, N. (1990). *Al-Qawa'id al-Fiqhiyya*. Imam Ali ibn Abi Talib School.

Mohaghegh Damad, S. M. (2016). *Principles of Islamic Jurisprudence: Civil Section; Ownership and Liability*. Center for the Publication of Islamic Sciences.

Mousavi Bojnourdi, S. M. (1998). *Al-Qawa'id al-Fiqhiyya*. Al-Hadi Publishing.