

Civil Liability for Violations of Individuals' Privacy and Personal Data in Cyberspace

Mehdi Golshanfar^{1*}

1*- M.A. Student in Law, Allameh Tabataba'i University, Tehran, Iran

ABSTRACT

Privacy and the protection of personal data in the digital age have become one of the most significant legal and social issues, as their violation can lead to extensive consequences for individuals and organizations. The main research question of this study is how civil liability is defined in relation to the violation of privacy and unauthorized disclosure of personal data in cyberspace, and to what extent existing legal frameworks are capable of addressing such violations. The importance of this topic lies in the fact that, with the expansion of online services and the increasing volume of personal data, the threats posed by misuse and privacy breaches have become more complex and widespread, making the determination of precise legal responsibility essential to prevent material and moral damages. The aim of this article is to analyze and examine civil liability of individuals and entities regarding personal data breaches and to propose measures to strengthen the enforcement of users' rights in cyberspace. The research method in this study is descriptive-analytical and based on documentary analysis, reviewing legal sources, judicial precedents, and theoretical studies in digital law. The findings indicate that despite the existence of protective laws, legal gaps and weak oversight in many areas hinder full realization of users' rights, especially in cases of violations by non-official entities or at the international level, where judicial accountability is limited. The innovation of this study lies in providing an integrated analytical framework that categorizes and evaluates civil liability in various domains of personal data violations, facilitating the identification of legal weaknesses and suggesting reforms. The results of this research can serve as a basis for legal policymaking and raising awareness among institutions and users about safeguarding privacy in cyberspace.

Keywords:

Privacy, Personal Data, Civil Liability, Cyberspace, Violation of User Rights

How to Cite: golshanfar, M. (2025). Civil Liability for Violations of Individuals' Privacy and Personal Data in Cyberspace. *Cyber Law*, 1(3), 84-103.

DOI: 10.22054/jocl.2325.75063.4814

Journal of Cyber Law in Development and Evolution is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.

© Authors



* Corresponding Author: mehdi.golshanfar@atu.ac.ir

مسئولیت مدنی در قبال نقض حریم خصوصی افراد و داده های شخصی افراد در فضای سایبری

مهدی گلشن فر*

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه علامه طباطبائی، تهران، ایران

چکیده

حریم خصوصی و حفاظت از داده های شخصی در عصر دیجیتال به یکی از مهم ترین مسائل حقوقی و اجتماعی تبدیل شده است، به گونه ای که نقض این حقوق می تواند پیامدهای گسترده ای برای افراد و سازمان ها به همراه داشته باشد. پرسش اصلی این پژوهش این است که مسئولیت مدنی در قبال نقض حریم خصوصی و افشای غیرمجاز داده های شخصی در فضای سایبری چگونه تعریف می شود و چارچوب های حقوقی موجود تا چه میزان توانایی مقابله با چنین تخلفاتی را دارند. اهمیت این موضوع از آن جهت است که با گسترش خدمات آنلاین و افزایش حجم داده های شخصی، تهدیدهای ناشی از سوءاستفاده و نقض حریم خصوصی بیش از پیش پیچیده و گسترده شده و نیاز به تعیین مسئولیت قانونی دقیق برای جلوگیری از خسارت های مادی و معنوی، ضروری می نماید. هدف این مقاله تحلیل و بررسی مسئولیت مدنی افراد و نهادها در قبال نقض داده های شخصی و ارائه راهکارهایی برای تقویت ضمانات اجرای حقوق کاربران در فضای سایبری است. روش پژوهش در این مقاله توصیفی-تحلیلی و مبتنی بر مطالعه اسنادی است و منابع قانونی، رویه های قضایی و مطالعات نظری در زمینه حقوق دیجیتال مورد بررسی قرار گرفته اند. یافته های تحقیق نشان می دهد که علی رغم وجود قوانین حمایتی، خلأهای قانونی و ضعف نظارت در بسیاری از حوزه ها مانع تحقق کامل حقوق کاربران شده است و به ویژه در موارد تخلف توسط نهادهای غیررسمی یا در سطح بین المللی، پاسخگویی قضایی محدود است. نوآوری این پژوهش در ارائه چارچوب تحلیلی یکپارچه ای است که مسئولیت مدنی را در حوزه های مختلف نقض داده های شخصی دسته بندی و ارزیابی می کند و امکان شناسایی نقاط ضعف قانونی و پیشنهاد اصلاحات را فراهم می آورد. نتایج حاصل از این تحقیق می تواند مبنایی برای سیاست گذاری های حقوقی و افزایش آگاهی نهادها و کاربران درباره حفظ حریم خصوصی در فضای سایبری باشد.

کلیدواژه ها:

حریم خصوصی، داده های شخصی، مسئولیت مدنی، فضای سایبری، نقض حقوق کاربران

نحوه استناد:

گلشن فر، مهدی. (۱۴۰۴). مسئولیت مدنی در قبال نقض حریم خصوصی افراد و داده های شخصی افراد در فضای سایبری. حقوق سایبری، ۱(۳)، ۸۴-۱۰۳

نشریه حقوق سایبری در توسعه و تکامل تحت مجوز کرییتیو کامنز انتساب - غیرتجاری ۴.۰ بین المللی منتشر شده است.

©نویسندگان



* ایمیل نویسنده مسئول: mehdi.golshanfar@atu.ac.ir

موضوع مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی در فضای سایبری، از جمله مسائل پیچیده و نوظهور در نظام‌های حقوقی معاصر است که با پیشرفت فناوری اطلاعات و ارتباطات، ابعاد گسترده‌تری یافته است. در نظام حقوقی ایران، این مسئله به‌ویژه در فضای سایبری و با توجه به توسعه روزافزون استفاده از اینترنت و فضای مجازی، اهمیت ویژه‌ای پیدا کرده است. با وجود اینکه در قانون اساسی جمهوری اسلامی ایران به برخی از مصادیق حریم خصوصی مانند مسکن، مکاتبات و مکالمات اشاره شده است (اصل ۲۲)، اما خلأ قانونی در زمینه حفاظت از داده‌های شخصی و مسئولیت مدنی ناشی از نقض آن‌ها مشهود است. قوانین پراکنده‌ای مانند قانون تجارت الکترونیکی (۱۳۸۲)، قانون جرایم رایانه‌ای (۱۳۸۸) و منشور حقوق شهروندی (۱۳۹۲) به موضوعاتی مرتبط با حریم خصوصی پرداخته‌اند، اما هیچ‌کدام به‌صورت جامع و یکپارچه به مسئولیت مدنی در قبال نقض داده‌های شخصی نپرداخته‌اند (جعفری و رهبرپور، ۱۳۹۶؛ قاسم‌زاده لیاپی و رئیس، ۱۳۹۹).

اهمیت این موضوع زمانی بیشتر نمایان می‌شود که با چالش‌های حقوقی و اجتماعی روز مواجه می‌شویم. نقض حریم خصوصی و افشای داده‌های شخصی می‌تواند منجر به خسارات مادی و معنوی فراوانی برای افراد شود. برای مثال، در فضای سایبری، هک اطلاعات شخصی، افشای غیرمجاز داده‌ها یا سوءاستفاده از آن‌ها می‌تواند آسیب‌های جبران‌ناپذیری به حقوق فردی وارد کند. این مسائل نه تنها حقوق فردی افراد را تهدید می‌کند، بلکه اعتماد عمومی به فضای مجازی و سیستم‌های الکترونیکی را نیز کاهش می‌دهد (کرمی، ۱۴۰۱). مطالعه پژوهش‌های موجود در این زمینه نشان می‌دهد که این موضوع تاکنون مورد توجه محققان و پژوهشگران قرار گرفته است. برای نمونه، جعفری و رهبرپور (۱۳۹۶) در مقاله‌ای به بررسی مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه پرداخته‌اند و به پیچیدگی‌های این مسئولیت در مقایسه با سایر انواع حریم خصوصی اشاره کرده‌اند. همچنین، قاسم‌زاده لیاپی و رئیس (۱۳۹۹) در مقاله‌ای به چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبری پرداخته‌اند و به خلأهای قانونی در این زمینه اشاره کرده‌اند. علاوه بر این، کرمی (۱۴۰۱) در کتابی به بررسی مسئولیت مدنی ناشی از نقض حریم خصوصی در فضای سایبر پرداخته است و به ارکان مسئولیت مدنی در این حوزه اشاره کرده است. با وجود این پژوهش‌ها، خلأهای پژوهشی همچنان در این حوزه وجود دارد. به‌ویژه، نیاز به بررسی تطبیقی مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی در فضای سایبری در نظام‌های حقوقی مختلف و ارائه راهکارهای عملی برای تقویت ضمانت‌های اجرایی در این زمینه احساس می‌شود. پرسش‌های اصلی این تحقیق عبارتند از:

۱. مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی در فضای سایبری در نظام حقوقی ایران چگونه تعریف می‌شود؟
۲. چه خلأهای قانونی و اجرایی در این زمینه وجود دارد؟
۳. راهکارهای تقویت ضمانت‌های اجرایی در این حوزه چیست؟

هدف این مقاله تحلیل و بررسی مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی در فضای سایبری در نظام حقوقی ایران است. این تحقیق به دنبال شناسایی خلأهای قانونی و اجرایی در این حوزه و ارائه پیشنهادهایی برای تقویت ضمانت‌های اجرایی در زمینه حفاظت از داده‌های شخصی و حریم خصوصی افراد است. روش پژوهش در این

مقاله تحلیلی-توصیفی و مبتنی بر مطالعه اسنادی است. در این راستا، قوانین و مقررات مرتبط با حریم خصوصی و داده‌های شخصی در نظام حقوقی ایران مورد بررسی قرار گرفته است. همچنین، آرای قضائی مرتبط با نقض حریم خصوصی و داده‌های شخصی تحلیل شده است تا خلأهای قانونی و اجرایی در این زمینه شناسایی شود.

حریم خصوصی

حریم خصوصی به معنای حق فرد در کنترل اطلاعات شخصی خود و جلوگیری از دخالت‌های غیرمجاز دیگران در زندگی خصوصی اوست (Westin, ۱۹۶۷, p. ۷). این حق در حقوق بین‌الملل و حقوق داخلی کشورها به‌عنوان یکی از حقوق بنیادین انسان‌ها شناخته شده است (Universal Declaration of Human Rights, ۱۹۴۸, Art. ۱۲; International Covenant on Civil and Political Rights, ۱۹۶۶, Art. ۱۷, p. ۴۵). در حقوق بین‌الملل، ماده ۱۲ اعلامیه جهانی حقوق بشر تصریح می‌کند که «هیچ کس نباید مورد مداخله خودسرانه یا تعرض غیرقانونی در زندگی خصوصی، خانواده، مسکن یا مکاتبات خود قرار گیرد» (UDHR, ۱۹۴۸, p. ۱۲). همچنین، ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی به‌صراحت حفاظت قانونی از حریم خصوصی افراد را تضمین کرده و مداخلات قانونی را تنها در موارد ضرورت و با رعایت ضوابط قانونی مجاز می‌داند (ICCPR, ۱۹۶۶, p. ۴۶).

در نظام حقوقی ایران، اصل ۲۲ قانون اساسی حفاظت از حیثیت، جان، مال، حقوق، مسکن و شغل افراد را تضمین کرده و تعرض به آن‌ها را تنها در موارد قانونی مجاز می‌داند (Constitution of Iran, ۱۹۷۹, Art. ۲۲, p. ۸). علاوه بر آن، اصل ۲۵ قانون اساسی بر حفظ حریم مکاتبات و ارتباطات تأکید دارد (Constitution of Iran, ۱۹۷۹, Art. ۲۵, p. ۹). در قوانین عادی، ماده ۶۶۵ قانون مجازات اسلامی ورود غیرمجاز به منزل دیگران را جرم‌انگاری کرده و مسئولیت کیفری متخلفان را مشخص می‌کند (Islamic Penal Code, ۲۰۱۳, Art. ۶۶۵, p. ۱۱۲). همچنین، ماده ۱۷ قانون جرایم رایانه‌ای دسترسی غیرمجاز به داده‌های شخصی را جرم‌انگاری کرده و مجازات‌هایی تعیین کرده است (Computer Crimes Act, ۲۰۰۹, Art. ۱۷, p. ۳۵). با وجود این تضمین‌ها، چالش‌هایی همچنان وجود دارد. یکی از مهم‌ترین این چالش‌ها، فقدان یک قانون جامع و مدون برای حفاظت از حریم خصوصی در ایران است، که موجب پراکندگی مقررات و عدم شفافیت در تعریف مفاهیم کلیدی مانند «داده‌های شخصی» و «حریم خصوصی دیجیتال» شده است (Karami, ۲۰۲۱, p. ۷۸). علاوه بر این، تحولات سریع فناوری‌های اطلاعات و ارتباطات، چالش‌های جدیدی برای حفاظت از حریم خصوصی ایجاد کرده که قوانین فعلی به‌طور کامل پاسخگوی آن‌ها نیستند (Solove, ۲۰۲۱, p. ۱۰۳). برای تقویت حمایت از حریم خصوصی، پیشنهاد می‌شود: تصویب قانون جامع حفاظت از حریم خصوصی و داده‌های شخصی، به‌روزرسانی قوانین موجود برای تطبیق با فناوری‌های نوین، ایجاد نهادهای مستقل نظارتی و فرهنگ‌سازی حقوقی در میان مردم و مقامات قضائی (GDPR, ۲۰۱۶, Art. ۵-۷, Karami, ۲۰۲۱, p. ۸۰). حریم خصوصی به‌عنوان یکی از حقوق بنیادین انسان‌ها، نیازمند حمایت قانونی و اجرایی مؤثر است، به‌ویژه در عصر دیجیتال که حفاظت از داده‌های شخصی اهمیت بیشتری یافته است (Solove, ۲۰۲۱, p. ۱۲۰). قوانین و مقررات باید به‌صورت جامع و شفاف طراحی شوند تا حقوق فردی شهروندان در مقابل دخالت‌های غیرمجاز حفظ شود.

داده‌های شخصی:

داده‌های شخصی به اطلاعاتی اطلاق می‌شود که می‌تواند به‌طور مستقیم یا غیرمستقیم هویت یک فرد را شناسایی کند (Solove, ۲۰۲۱, p. ۴۵). این داده‌ها شامل نام، شماره شناسنامه، شماره ملی، آدرس محل سکونت، شماره تلفن،

آدرس ایمیل، اطلاعات مالی، سوابق پزشکی و سایر اطلاعات مشابه هستند که قابلیت شناسایی فرد را دارند (GDPR, Art. ۲۰۱۶, p. ۱(۴), (۱۲)). داده‌های شخصی در عصر دیجیتال اهمیت ویژه‌ای یافته‌اند، زیرا جمع‌آوری، پردازش و استفاده غیرمجاز از آن‌ها می‌تواند پیامدهای جدی برای حقوق و آزادی‌های فرد ایجاد کند (Karami, ۲۰۲۱, p. ۵۸). در حقوق بین‌الملل، حفاظت از داده‌های شخصی به‌عنوان بخشی از حق حریم خصوصی شناخته می‌شود. ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (ICCPR, ۱۹۶۶, p. ۴۶) و اصول (GDPR, Art. ۲۰۱۶, ۵-۷) تأکید دارند که افراد حق دارند کنترل کاملی بر داده‌های شخصی خود داشته باشند و هرگونه جمع‌آوری یا پردازش داده‌ها باید با رضایت فرد و مطابق با قوانین مشخص انجام شود. در حقوق داخلی ایران، مفاهیم مرتبط با داده‌های شخصی عمدتاً در قانون جرایم رایانه‌ای و قوانین حفاظت از حریم خصوصی مورد توجه قرار گرفته است. ماده ۱۲ این قانون دسترسی غیرمجاز به داده‌های شخصی را جرم‌انگاری کرده و مجازات‌های کیفری برای آن پیش‌بینی نموده است (Computer Crimes Act, Art. ۲۰۰۹, p. ۱۲, (۳۵)). همچنین، پیش‌نویس قانون حفاظت از داده‌های شخصی که هنوز تصویب نشده است، تعاریف دقیق‌تری از «داده‌های شخصی» ارائه می‌دهد و مسئولیت پردازش‌کنندگان داده‌ها را مشخص می‌کند (Karami, ۲۰۲۱, p. ۶۰). داده‌های شخصی ممکن است به صورت مستقیم، مانند نام و شماره شناسنامه، یا غیرمستقیم، مانند ترکیب اطلاعاتی که هویت فرد را مشخص می‌کند، شناسایی شوند (Solove, ۲۰۲۱, p. ۴۷). این امر باعث می‌شود که حفاظت قانونی از داده‌های شخصی به‌طور جامع و دقیق ضروری باشد، زیرا حتی انتشار یا پردازش داده‌های غیرمستقیم می‌تواند منجر به نقض حریم خصوصی شود.

از دیدگاه فقهی و حقوق اسلامی، داده‌های شخصی به‌عنوان اطلاعات حساس تلقی می‌شوند و افشای غیرمجاز آن‌ها مشمول اصولی مانند حرمت تجسس و حرمت افشای اسرار است (جعفری و رهبرپور، ۱۳۹۶، ص. ۴۲). به همین دلیل، مسئولیت مدنی ناشی از افشای داده‌های شخصی در فقه نیز قابل پذیرش است و جبران خسارت به فرد متضرر الزامی است. می‌توان نتیجه گرفت که داده‌های شخصی یکی از عناصر اصلی حریم خصوصی هستند و حفاظت از آن‌ها مستلزم ایجاد قوانین دقیق، شفاف و هماهنگ با استانداردهای بین‌المللی است. فقدان چارچوب قانونی جامع در ایران و نبود آگاهی کافی از حقوق داده‌های شخصی، خطرات بالقوه‌ای برای شهروندان ایجاد می‌کند و ضرورت تصویب قوانین مدون و آموزش حقوقی در این حوزه را برجسته می‌سازد (Karami, ۲۰۲۱, p. ۶۲-۶۳).

فضای سایبری:

فضای سایبری به محیط دیجیتال و شبکه‌های ارتباطی اطلاق می‌شود که امکان تبادل اطلاعات و داده‌ها را فراهم می‌آورد (Castells, ۲۰۱۰, p. ۴۵). این فضا شامل اینترنت، شبکه‌های اجتماعی، پایگاه‌های داده، سیستم‌های پردازش ابری، پیام‌رسان‌ها، و سایر سیستم‌های الکترونیکی است که افراد و سازمان‌ها را قادر می‌سازد اطلاعات را به‌صورت فوری تولید، ذخیره، انتقال و پردازش کنند (Solove, ۲۰۲۱, p. ۵۲). فضای سایبری نه تنها محلی برای تبادل اطلاعات است، بلکه به بستری برای تعاملات اقتصادی، اجتماعی، فرهنگی و سیاسی تبدیل شده است (Kshetri, ۲۰۱۶, p. ۳۲). در این محیط، داده‌های شخصی و اطلاعات حساس افراد به‌سرعت منتقل می‌شوند و همین ویژگی باعث می‌شود که حفاظت از حریم خصوصی و امنیت داده‌ها در آن اهمیت حیاتی پیدا کند (Karami, ۲۰۲۱, p. ۷۰). بعبارت دیگر فضای سایبری محیطی گسترده و پیچیده است که با رشد فناوری و تعاملات دیجیتال، حفاظت از داده‌های شخصی و

حقوق شهروندان را به چالشی مهم تبدیل کرده است. تعریف دقیق فضای سایبری و مسئولیت‌های مرتبط با آن در قوانین داخلی و بین‌المللی، پیش‌نیاز ایجاد امنیت و اعتماد در تعاملات دیجیتال است (Karami, ۲۰۲۱, p. ۷۵). در حقوق بین‌الملل، فضای سایبری به‌عنوان محیطی برای اجرای حقوق دیجیتال و حفاظت از داده‌ها مورد توجه قرار گرفته است. به‌عنوان نمونه، مقررات عمومی حفاظت از داده‌ها (GDPR) اتحادیه اروپا، فضای سایبری را بستری برای پردازش داده‌های شخصی در سطح دیجیتال می‌شناسد و برای محافظت از حقوق افراد، اصولی مانند محدودیت پردازش، شفافیت و اطلاع‌رسانی را وضع کرده است (GDPR, Art. ۲۰۱۶, p. ۷-۵, ۱۲). در حقوق داخلی ایران نیز فضای سایبری توسط قوانین مختلفی مانند قانون جرایم رایانه‌ای (ماده ۱۲ و ۱۷)، قانون تجارت الکترونیکی (ماده ۷۸) و پیش‌نویس قانون حفاظت از داده‌های شخصی مورد توجه قرار گرفته است (Computer Crimes Act, ۲۰۰۹, Art. ۱۲, p. ۳۵, E-Commerce Act, ۲۰۰۲, Art. ۷۸, p. ۷۸, Karami, ۲۰۲۱, p. ۷۱). این قوانین به‌صورت مستقیم یا غیرمستقیم مسئولیت افراد و مؤسسات در قبال داده‌های شخصی و حریم خصوصی در فضای سایبری را تعیین می‌کنند.

چالش‌های اصلی در فضای سایبری شامل نقض حریم خصوصی، دسترسی غیرمجاز به داده‌ها، افشای اطلاعات شخصی، حملات سایبری و سوءاستفاده اقتصادی از داده‌ها است (Solove, ۲۰۲۱, p. ۵۵). این چالش‌ها موجب شده‌اند که تدوین قوانین جامع و هماهنگ با استانداردهای بین‌المللی، آموزش کاربران و ارتقای امنیت فناوری‌های اطلاعات و ارتباطات، بیش از پیش ضروری شود (Karami, ۲۰۲۱, p. ۷۲). از منظر فقهی و حقوق اسلامی، ورود غیرمجاز به فضای سایبری و افشای اطلاعات خصوصی افراد، مشابه ورود غیرمجاز به زندگی خصوصی و مکاتبات افراد قلمداد می‌شود و می‌تواند مسئولیت مدنی و کیفری ایجاد کند (جعفری و رهبرپور، ۱۳۹۶، ص. ۵۰). بنابراین، فضای سایبری به‌عنوان بستری که اطلاعات شخصی و فعالیت‌های روزمره افراد را پوشش می‌دهد، نیازمند چارچوب‌های قانونی و نظارتی دقیق است.

مسئولیت مدنی:

مسئولیت مدنی به تعهد قانونی فرد یا نهادی اطلاق می‌شود که در صورت نقض حقوق دیگران، موظف به جبران خسارت وارده باشد. این مسئولیت می‌تواند ناشی از تقصیر، فعل زیان‌بار یا ترک فعل باشد و هدف آن جبران خسارت مادی یا معنوی قربانی و بازگرداندن او به وضعیت سابق است (Shavell, ۲۰۰۴, p. ۱۲). مسئولیت مدنی به دو دسته کلی تقسیم می‌شود: مسئولیت قراردادی، که ناشی از نقض تعهدات قراردادی است، و مسئولیت خارج از قرارداد، که در اثر فعل یا ترک فعل زیان‌بار برای دیگران ایجاد می‌شود (Karami, ۲۰۲۱, p. ۹۰). در حقوق داخلی ایران، مسئولیت مدنی اساساً در قانون مدنی تعریف شده است. بر اساس ماده ۱ قانون مسئولیت مدنی: «هر کس بدون مجوز قانونی عمداً یا در نتیجه بی‌احتیاطی به جان، مال، آزادی، حیثیت یا حقوق دیگران لطمه وارد کند، مسئول جبران خسارت است» (Civil Liability Act, ۱۹۳۹, Art. ۱, p. ۳). این ماده پایه و اساس مسئولیت مدنی ناشی از افعال زیان‌بار را تشکیل می‌دهد و شامل نقض حریم خصوصی و داده‌های شخصی نیز می‌شود. علاوه بر آن، ماده ۲ قانون مدنی تقصیر و خطای فرد را به‌عنوان شرط مسئولیت تعیین کرده و بیان می‌کند که فرد مقصر باید خسارت وارده را جبران کند (Civil Code, ۱۹۳۹, Art. ۲, p. ۵).

در زمینه نقض حریم خصوصی و داده‌های شخصی در فضای سایبری، قوانین خاصی نیز وجود دارد. ماده ۱۲ قانون جرایم رایانه‌ای، دسترسی غیرمجاز به داده‌های شخصی را جرم‌انگاری کرده و مسئولیت کیفری و مدنی را مشخص می‌کند (Computer Crimes Act, ۲۰۰۹, Art. ۱۲, p. ۳۵). همچنین، ماده ۷۸ قانون تجارت الکترونیکی مؤسسات ارائه‌دهنده خدمات دیجیتال را در برابر خسارات ناشی از نقض سیستم مسئول می‌داند، مگر آنکه خسارت ناشی از فعل شخص ثالث باشد (E-Commerce Act, ۲۰۰۲, Art. ۷۸, p. ۴۴). از منظر حقوق بین‌الملل و مقایسه‌ای، مسئولیت مدنی برای نقض حقوق حریم خصوصی در فضای دیجیتال نیز مطرح است. به‌عنوان مثال، GDPR اتحادیه اروپا نه تنها پردازش غیرمجاز داده‌ها را ممنوع کرده، بلکه جبران خسارت ناشی از افشای داده‌های شخصی را نیز پیش‌بینی کرده است (GDPR, ۲۰۱۶, Art. ۸۲, p. ۲۰). همچنین، تفسیر عمومی ۱۶ میثاق بین‌المللی حقوق مدنی و سیاسی (ICCPR) تأکید دارد که نقض حریم خصوصی افراد توسط دولت یا اشخاص، مستلزم جبران و اقدامات اصلاحی است (ICCPR, ۱۹۶۶, p. ۴۶).

دیدگاه‌های دکتربین حقوقی نیز بر اهمیت مسئولیت مدنی در حفاظت از حریم خصوصی تأکید دارند (Solove, ۲۰۲۱, p. ۷۵). معتقد است که مسئولیت مدنی ابزار اصلی جلوگیری از سوءاستفاده از داده‌های شخصی و تضمین حقوق دیجیتال شهروندان است. از منظر فقهی نیز، افشای غیرمجاز اسرار شخصی مشمول مسئولیت مدنی و الزام به جبران خسارت است (جعفری و رهبرپور، ۱۳۹۶، ص. ۵۲). با توجه به موارد فوق، مسئولیت مدنی نقش کلیدی در تضمین حفاظت از حریم خصوصی و داده‌های شخصی دارد. فقدان چارچوب قانونی جامع در ایران موجب شده است که تحقق این مسئولیت با چالش مواجه شود و ضرورت تصویب قوانین مدون و به‌روزرسانی مقررات موجود بیش از پیش احساس شود (Karami, ۲۰۲۱, p. ۹۵).

مبانی فلسفی

در فلسفه حقوق، حریم خصوصی به‌عنوان یکی از ارکان اصلی آزادی فردی و کرامت انسانی شناخته می‌شود. جان استوارت میل در کتاب خود «در باب آزادی» تأکید می‌کند که افراد باید دارای حوزه‌ای از زندگی شخصی باشند که دولت و دیگران نتوانند بدون مجوز و ضرورت موجه در آن مداخله کنند (Mill, ۱۸۵۹, p. ۱۴). او استدلال می‌کند که محدود کردن حریم خصوصی تنها زمانی مجاز است که رفتار فرد امنیت عمومی یا حقوق دیگران را تهدید کند. این دیدگاه مبنایی برای تبیین تعادل بین آزادی فردی و منافع اجتماعی فراهم می‌آورد و نقش حریم خصوصی را در ایجاد شرایط مناسب برای توسعه شخصیت و اختیار فردی روشن می‌کند. مفهوم حریم خصوصی از دیدگاه فلسفی با کرامت انسانی نیز پیوند خورده است. کرامت انسانی مستلزم احترام به حریم شخصی افراد و حفاظت از اطلاعات شخصی آنهاست، زیرا نقض حریم خصوصی به‌طور مستقیم می‌تواند کرامت فرد را مخدوش کند (Raz, ۱۹۸۶, p. ۷۰). در این چارچوب، مسئولیت مدنی ناشی از نقض حریم خصوصی نیز از نظر فلسفی توجیه می‌شود، زیرا جبران خسارت برای بازگرداندن حقوق فرد و اصلاح تعادل اجتماعی ضروری است.

دیدگاه دیگر در فلسفه حقوق، نظریه حقوق طبیعی است. نظریه پردازان حقوق طبیعی مانند لوک (Locke, ۱۶۸۹, p. ۱۲۰) معتقدند که هر فرد دارای حقوق ذاتی و غیرقابل سلب است، از جمله حق کنترل بر اطلاعات شخصی خود. به این ترتیب، هرگونه مداخله غیرمجاز در داده‌ها یا حریم خصوصی، نقض حقوق ذاتی فرد محسوب شده و مسئولیت مدنی یا کیفری را به دنبال دارد. این نگرش فلسفی مبنایی برای قوانین مدرن حریم خصوصی در حقوق بین‌الملل و داخلی فراهم

می‌کند و نشان می‌دهد که حقوق فردی در فضای خصوصی، هم از منظر اخلاقی و هم از منظر قانونی واجد اهمیت است.

از منظر فلسفه اخلاق، تئوری کنش عقلانی و احترام متقابل نیز به حریم خصوصی مرتبط است. کاتولیک‌ها و فیلسوفان معاصر بر این باورند که رعایت حریم خصوصی دیگران، نوعی احترام به شأن و شخصیت فردی است و نقض آن، تخلف از اصول اخلاقی و اجتماعی محسوب می‌شود (Waldron, ۲۰۰۰, p. ۹۰). این مبانی فلسفی به‌طور مستقیم با مقررات قانونی مانند اصل ۲۲ قانون اساسی ایران و مواد قانون جرایم رایانه‌ای همخوانی دارند و مشروعیت حقوقی مسئولیت مدنی در قبال نقض حریم خصوصی را تقویت می‌کنند. در مجموع، مبانی فلسفی حریم خصوصی نشان می‌دهند که حفاظت از حوزه شخصی افراد نه تنها یک ضرورت قانونی، بلکه یک ضرورت اخلاقی و اجتماعی است. این دیدگاه فلسفی پایه‌های نظری مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی در فضای سایبری را تقویت می‌کند و دلیل موجهی برای تدوین قوانین دقیق و اجرای عدالت در این حوزه فراهم می‌آورد (Mill, ۱۸۵۹, p. ۱۶; Raz, ۱۹۸۶; Waldron, ۲۰۰۰, p. ۹۳).

مبانی فقهی

در فقه اسلامی، حریم خصوصی و حفاظت از داده‌های شخصی با اصولی بنیادین مانند «حرمت افشای اسرار»، «حرمت تجسس» و «حرمت غیبت» پیوند خورده است (مطهری، ۱۳۸۴، ص. ۱۵۲). حرمت افشای اسرار بیان می‌کند که افشای اطلاعات خصوصی دیگران بدون اجازه آنان ممنوع است و ناقض حقوق فردی محسوب می‌شود. حرمت تجسس نیز منع می‌کند که افراد بدون مجوز یا ضرورت موجه وارد زندگی خصوصی دیگران شوند، حتی اگر این دسترسی از طریق فضای سایبری باشد (جعفری و رهبرپور، ۱۳۹۶، ص. ۵۰). حرمت غیبت، علاوه بر جنبه اخلاقی، نقض حریم خصوصی افراد را نیز منع می‌کند و هرگونه انتشار اطلاعات شخصی دیگران بدون رضایت آنان را ناپسند و مستلزم جبران می‌داند. فقها با پذیرش نظریه «مال‌انگاری حریم خصوصی» بیان می‌کنند که حریم خصوصی مانند مال شخصی دارای ارزش مادی است و هرگونه تجاوز به آن مستلزم جبران خسارت است (نوری، ۱۳۹۵، ص. ۸۲). بر اساس این دیدگاه، افشای داده‌های شخصی یا نقض حریم خصوصی افراد در فضای سایبری، اگرچه ممکن است به‌صورت غیرمستقیم انجام شود، مشمول مسئولیت مدنی است و فرد متضرر حق دارد خسارات وارده را مطالبه کند. این نظریه مبنایی برای تطبیق اصول فقهی با چارچوب حقوقی مدرن محسوب می‌شود و نشان می‌دهد که حفاظت از داده‌های شخصی در عصر دیجیتال نیز از دیدگاه فقهی اهمیت دارد.

علاوه بر این، برخی فقهاء تأکید کرده‌اند که حتی دسترسی غیرمجاز به اطلاعات دیجیتال دیگران، مانند ورود به حساب‌های شخصی یا سرقت داده‌های الکترونیکی، مصداق تجسس و افشای اسرار است و موجب مسئولیت مدنی و گاهی کیفری می‌شود (جعفری و رهبرپور، ۱۳۹۶، ص. ۵۲). این دیدگاه با اصول قانون مدنی ایران (ماده ۱ و ۲ قانون مسئولیت مدنی) هماهنگ است که هرگونه تجاوز به حقوق دیگران، اعم از حقوق مادی یا معنوی، مستلزم جبران خسارت است (Civil Liability Act, Art. ۱۹۳۹, p. ۱-۲, ۳-۵). پس مبانی فقهی نشان می‌دهند که حفاظت از حریم خصوصی و داده‌های شخصی نه تنها ضرورت اخلاقی دارد، بلکه از نظر قانونی و مدنی نیز قابل حمایت است. ترکیب اصول فقهی با مقررات مدرن، به ویژه در حوزه فضای سایبری، موجب می‌شود چارچوبی مستحکم برای مسئولیت مدنی در قبال نقض داده‌های شخصی و حریم خصوصی ایجاد شود (Karami, ۲۰۲۱, p. ۹۸).

مبانی حقوقی

در حقوق ایران، مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی در چندین قانون مورد توجه قرار گرفته است، هرچند این توجه پراکنده و ناقص است. ماده ۱ قانون مسئولیت مدنی تصریح می‌کند که «هر کس بدون مجوز قانونی عمداً یا در نتیجه بی‌احتیاطی به جان، مال، آزادی، حیثیت یا حقوق دیگران لطمه وارد کند، مسئول جبران خسارت است» (Art. ۱۹۳۹ Civil Liability Act, p. ۱, Art. ۳). این ماده پایه و اساس مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی را تشکیل می‌دهد و نشان می‌دهد که هرگونه تعرض به حقوق فردی، اعم از مادی یا معنوی، مستلزم جبران خسارت است. همچنین، ماده ۲ قانون مسئولیت مدنی تقصیر یا خطای فرد را شرط تحقق مسئولیت مدنی دانسته و بیان می‌کند که فرد مقصر موظف به جبران خسارت وارده است (Art. ۱۹۳۹ Civil Liability Act, p. ۲, Art. ۵). در حوزه فضای سایبری، قانون جرایم رایانه‌ای نقش اساسی دارد. ماده ۱۲ این قانون دسترسی غیرمجاز به داده‌های شخصی را جرم‌انگاری کرده و علاوه بر مسئولیت کیفری، موجب مسئولیت مدنی برای جبران خسارت فرد متضرر می‌شود (Art. ۲۰۰۹ Computer Crimes Act, p. ۱۲, Art. ۳۵). همچنین، قانون تجارت الکترونیکی با تأکید بر مسئولیت ارائه‌دهندگان خدمات دیجیتال، در ماده ۷۸ بیان می‌کند که این نهادها موظف به حفظ داده‌ها و جلوگیری از خسارات ناشی از نقص سیستم هستند، مگر آنکه خسارت ناشی از فعل شخص ثالث باشد (E-Commerce Act, p. ۷۸, Art. ۲۰۰۲). (۴۴).

با وجود این مقررات، خلأ قانونی در حمایت از حریم خصوصی و داده‌های شخصی در فضای سایبری همچنان محسوس است. قوانین موجود به صورت پراکنده موضوع را پوشش می‌دهند و چارچوبی جامع برای تعریف مسئولیت مدنی و نحوه جبران خسارت ناشی از نقض داده‌ها ارائه نمی‌دهند (Karami, ۲۰۲۱, p. ۱۰۰). این کمبود به‌ویژه در تعریف مفاهیم کلیدی مانند «داده‌های شخصی»، «پردازش غیرمجاز» و «مسئولیت ارائه‌دهندگان خدمات دیجیتال» مشاهده می‌شود و باعث ایجاد ابهام در رسیدگی قضایی می‌شود.

دیدگاه‌های دکتربین حقوقی بر لزوم ایجاد چارچوب قانونی منسجم تأکید دارند. حقوق‌دانان معتقدند که مسئولیت مدنی در فضای سایبری باید شامل خسارات مادی و معنوی ناشی از افشای داده‌ها باشد و شمول آن به داده‌های دیجیتال و فعالیت‌های آنلاین افراد گسترش یابد (Solove, ۲۰۲۱, p. ۸۷). علاوه بر آن، قوانین بین‌المللی مانند GDPR اتحادیه اروپا نمونه‌ای از چارچوب قانونی جامع هستند که الزامات مشخصی برای پردازش داده‌ها، شفافیت، رضایت فرد و مسئولیت ارائه‌دهندگان خدمات دیجیتال وضع کرده‌اند (GDPR, Art. ۲۰۱۶, p. ۸۲, ۷-۵, Art. ۱۲-۲۰). تطبیق این اصول با قوانین ایران می‌تواند خلأهای قانونی موجود را کاهش دهد و حفاظت مؤثرتری از حقوق شهروندان در فضای سایبری فراهم کند و در نهایت مبانی حقوقی نشان می‌دهند که اگرچه قوانین ایران پایه‌های اولیه مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی را فراهم کرده‌اند، اما نیازمند تدوین قوانین جامع و هماهنگ با استانداردهای بین‌المللی برای ایجاد حفاظت کامل از حقوق افراد در فضای دیجیتال است (Karami, ۲۰۲۱, p. ۱۰۲).

مبانی اقتصادی

از دیدگاه اقتصادی، داده‌های شخصی به‌عنوان کالایی باارزش در فضای سایبری محسوب می‌شوند که امکان تبادل، پردازش و بهره‌برداری تجاری از آن‌ها وجود دارد (Acquisti, Taylor, & Wagman, ۲۰۱۶, p. ۳). این داده‌ها شامل اطلاعات هویتی، مالی، رفتاری و ترجیحات کاربران است که شرکت‌ها و سازمان‌ها می‌توانند از آن‌ها برای

بازاریابی هدفمند، ارائه خدمات سفارشی و افزایش سود استفاده کنند. در واقع، داده‌های شخصی نوعی دارایی دیجیتال هستند که ارزش اقتصادی مستقیم و غیرمستقیم دارند و مدیریت آن‌ها نقش کلیدی در ایجاد ارزش برای کسب و کارها ایفا می‌کند (OECD, ۲۰۱۳, p. ۱۲). سوءاستفاده یا افشای غیرمجاز داده‌های شخصی می‌تواند منافع اقتصادی قابل توجهی را برای اشخاص ثالث به همراه داشته باشد، اما در عین حال خسارت مالی و غیرمالی به مالک داده وارد کند (Acquisti et al., ۲۰۱۶, p. ۵). به همین دلیل، حفاظت از داده‌های شخصی نه تنها از منظر حقوقی اهمیت دارد، بلکه ضرورت اقتصادی نیز دارد، زیرا تضمین امنیت داده‌ها موجب اعتماد کاربران، پایداری بازارهای دیجیتال و کاهش هزینه‌های ناشی از سوءاستفاده می‌شود.

مباحث اقتصادی همچنین به بازار اطلاعات و منافع متضاد طرف‌ها اشاره دارند. داده‌های شخصی به دلیل قابلیت پردازش و تجمع، به منبع درآمد قابل توجهی برای ارائه‌دهندگان خدمات دیجیتال تبدیل شده‌اند. در صورتی که مقررات حفاظتی ناکافی باشد، انگیزه برای سوءاستفاده افزایش یافته و هزینه‌های اجتماعی ناشی از نقض حریم خصوصی افزایش می‌یابد (Varian, ۲۰۱۰, p. ۲۲). به عبارت دیگر، اقتصاد داده‌ها با مسئله «بازار ناکارآمد اطلاعات» روبه‌روست که در آن عدم شفافیت و فقدان حفاظت قانونی، موجب ایجاد خسارت برای کاربران و بهره‌برداری غیرمجاز توسط شرکت‌ها می‌شود. از منظر سیاست‌گذاری اقتصادی، تدوین قوانین جامع و شفاف برای حفاظت از داده‌های شخصی، ایجاد سازوکارهای نظارتی و جبران خسارت، به کاهش هزینه‌های اجتماعی و افزایش بهره‌وری اقتصادی کمک می‌کند (OECD, ۲۰۱۳, p. ۱۵). این مبانی اقتصادی همچنین توجیه‌کننده وضع مقرراتی مانند GDPR اتحادیه اروپا و الزام ارائه‌دهندگان خدمات دیجیتال به حفاظت از داده‌های کاربران است، زیرا این مقررات علاوه بر تأمین حقوق شهروندان، به افزایش کارایی و اعتماد در بازار دیجیتال نیز کمک می‌کند (GDPR, Art. ۵-۷, p. ۱۲-۱۳). در نتیجه، حفاظت از داده‌های شخصی در فضای سایبری نه تنها ضرورت حقوقی و اخلاقی دارد، بلکه از منظر اقتصادی نیز یک الزام حیاتی است. نادیده گرفتن این موضوع می‌تواند منجر به خسارات مالی، کاهش اعتماد کاربران و ناکارآمدی بازار داده‌ها شود، در حالی که ایجاد چارچوب قانونی و نظارتی مناسب، موجب ارتقای بهره‌وری اقتصادی و حفاظت از منافع فردی و اجتماعی خواهد شد (Acquisti et al., ۲۰۱۶, p. ۹).

نظریه‌های حقوقی مرتبط

نظریه تقصیر

بر اساس نظریه تقصیر، مسئولیت مدنی زمانی محقق می‌شود که فرد یا نهادی با اقدام زیان‌بار یا ترک فعل ناشی از بی‌احتیاطی یا غفلت، خسارت به دیگری وارد کند (Shavell, ۲۰۰۴, p. ۱۵). در این چارچوب، عنصر تقصیر شرط اصلی تحقق مسئولیت مدنی است و بدون وجود تقصیر، الزام به جبران خسارت به‌طور معمول منتفی خواهد بود. نظریه تقصیر، در بسیاری از نظام‌های حقوقی مدرن پایه و اساس مسئولیت خارج از قرارداد را تشکیل می‌دهد و موجب می‌شود که فرد یا سازمانی که از استانداردهای مراقبتی لازم تخطی کرده است، مسئول جبران خسارت باشد. در حقوق ایران، این نظریه در ماده ۱ قانون مسئولیت مدنی مورد تأکید قرار گرفته است: «هر کس بدون مجوز قانونی عمداً یا در نتیجه بی‌احتیاطی به جان، مال، آزادی، حیثیت یا حقوق دیگران لطمه وارد کند، مسئول جبران خسارت است» (Civil Liability Act, Art. ۱, p. ۳). همچنین، ماده ۲ قانون مسئولیت مدنی، عنصر تقصیر یا خطا را شرط تحقق

مسئولیت مدنی دانسته و بیان می‌کند که فرد متضرر حق مطالبه جبران خسارت را دارد (Civil Liability Act,) (۵, p. ۲, Art. ۱۹۳۹).

در زمینه حریم خصوصی و داده‌های شخصی در فضای سایبری، نظریه تقصیر به‌طور مستقیم کاربرد دارد. برای مثال، اگر یک شرکت ارائه‌دهنده خدمات دیجیتال با بی‌توجهی به اصول امنیت داده‌ها، اطلاعات شخصی کاربران را افشا کند، مطابق نظریه تقصیر مسئولیت مدنی آن شرکت محقق می‌شود. همچنین، دسترسی غیرمجاز به داده‌های شخصی افراد یا انتشار غیرمجاز اطلاعات شخصی، مصداق فعل زیان‌بار ناشی از تقصیر تلقی می‌شود (Computer Crimes Act,) (۳۵, p. ۱۲, Art. ۲۰۰۹).

دیدگاه دکترین حقوقی نیز بر اهمیت عنصر تقصیر تأکید دارد. Solove (۲۰۲۱, p. ۷۸) معتقد است که برای ایجاد مسئولیت مدنی در زمینه نقض حریم خصوصی، باید تقصیر فرد یا سازمان مشخص شود و اثبات شود که خسارت ناشی از فعل یا ترک فعل او بوده است. همچنین کریمی (۲۰۲۱) در پژوهشی بیان می‌کند که نظریه تقصیر پایه‌ای منطقی برای توجیه جبران خسارت ناشی از افشای داده‌های شخصی فراهم می‌کند، زیرا بدون وجود تقصیر، الزام قانونی به جبران خسارت کاهش می‌یابد (Karami ۲۰۲۱, p. ۱۰۵).

به این ترتیب، نظریه تقصیر مبنای حقوقی مهمی برای مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی در فضای سایبری محسوب می‌شود و در تطبیق با قوانین ایران و استانداردهای بین‌المللی، چارچوب منطقی برای تعیین مسئولیت افراد و مؤسسات ارائه می‌دهد.

نظریه خطر

نظریه خطر بر این اصل استوار است که مسئولیت مدنی می‌تواند حتی در صورت فقدان تقصیر نیز محقق شود، هرگاه فعالیت یا اقدام فرد یا نهاد، خطر بالقوه‌ای برای دیگران ایجاد کند و این خطر منجر به خسارت شود (Dukeminier & Krier, ۲۰۱۰, p. ۴۵). در این چارچوب، مسئولیت مبتنی بر ایجاد خطر است و الزامی به اثبات تقصیر فرد وجود ندارد، زیرا صرف ایجاد شرایطی که ممکن است به دیگری آسیب برساند، مبنای مسئولیت تلقی می‌شود. این نظریه معمولاً در فعالیت‌های پرخطر، صنایع حساس، حمل‌ونقل، و محیط‌های کاری که احتمال وقوع حوادث بالا است، کاربرد دارد.

در حقوق ایران، نظریه خطر در برخی موارد پذیرفته شده است. به‌عنوان نمونه، ماده ۳۳۷ قانون مدنی و رویه قضایی مرتبط، مسئولیت کارفرما در قبال کارگران تحت شرایطی که فعالیت‌های خطرناک انجام می‌دهند، حتی بدون تقصیر کارفرما، را تأیید می‌کند (Civil Code, ۱۹۳۹, Art. ۳۳۷, p. ۱۲۰). همچنین، برخی دکترین حقوقی به این نتیجه رسیده‌اند که مالک یا بهره‌بردار اشیاء پرخطر یا تأسیسات عمومی در صورت ایجاد خسارت به دیگران، مسئول جبران آن است حتی اگر تقصیر مستقیمی مرتکب نشده باشد (Karami, ۲۰۲۱, p. ۱۰۸). در زمینه نقض حریم خصوصی و داده‌های شخصی در فضای سایبری، نظریه خطر اهمیت ویژه‌ای دارد. ارائه‌دهندگان خدمات دیجیتال، شبکه‌های اجتماعی و پلتفرم‌های آنلاین با نگهداری و پردازش حجم عظیمی از داده‌های شخصی، بالقوه خطر افشای این داده‌ها را ایجاد می‌کنند. بر اساس نظریه خطر، حتی اگر شرکت یا فردی تقصیر مشخصی نداشته باشد، مسئولیت مدنی برای جبران خسارت ناشی از سوءاستفاده یا افشای داده‌ها قابل اعمال است (Solove, ۲۰۲۱, p. ۸۱). این دیدگاه به‌ویژه در موارد حملات سایبری، نفوذ غیرمجاز به سیستم‌ها و نشت داده‌ها اهمیت دارد، زیرا فقدان تقصیر نمی‌تواند مانع از جبران خسارت افراد آسیب‌دیده شود.

دیدگاه دکترین حقوقی نیز بر لزوم اعمال نظریه خطر در فضای سایبری تأکید دارد. همچنین نظریه خطر پایه قانونی مناسبی برای الزام ارائه‌دهندگان خدمات دیجیتال به اتخاذ تدابیر امنیتی و جبران خسارات ناشی از نقض داده‌ها فراهم می‌کند، زیرا فعالیت آن‌ها به‌طور ذاتی با ریسک برای کاربران همراه است. از منظر تطبیقی، برخی مقررات بین‌المللی، از جمله GDPR اتحادیه اروپا، با الزامات امنیت داده‌ها و جبران خسارت ناشی از نقض آن، نشان می‌دهند که مسئولیت مستقل از تقصیر در حفاظت از داده‌ها قابل اعمال است (Art. ۲۰۱۶ GDPR, p. ۸۲, ۲۰۲۰). پس، نظریه خطر مبنای حقوقی مهمی برای مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی در فضای سایبری است و موجب تقویت چارچوب قانونی حفاظت از کاربران و ایجاد انگیزه برای رعایت استانداردهای امنیتی توسط شرکت‌ها و نهادهای دیجیتال می‌شود.

نظریه مال‌انگاری حریم خصوصی

نظریه مال‌انگاری حریم خصوصی بر این اصل استوار است که حریم خصوصی و داده‌های شخصی همانند یک دارایی یا مال قابل ارزش‌گذاری هستند و هرگونه نقض آن، خسارت مادی و قابل جبران ایجاد می‌کند (Solove, ۲۰۲۱, p. ۸۵). بر اساس این دیدگاه، اطلاعات شخصی مانند نام، شماره شناسنامه، آدرس، سوابق پزشکی و داده‌های رفتاری افراد، ارزش اقتصادی و حقوقی دارند و هرگونه افشای غیرمجاز یا استفاده ناصحیح از آن‌ها می‌تواند زیان مالی و معنوی برای مالک داده ایجاد کند. در حقوق ایران، نظریه مال‌انگاری حریم خصوصی در برخی آراء قضایی و مباحث دکترین حقوقی مورد توجه قرار گرفته است. به‌عنوان مثال، برخی دادگاه‌ها در پرونده‌های مرتبط با نشر اطلاعات شخصی یا دسترسی غیرمجاز به حساب‌های کاربران، خسارت وارده را به‌عنوان خسارت مالی شناسایی کرده و الزام به جبران آن را صادر کرده‌اند (جعفری و رهبری، ۱۳۹۶، ص. ۵۴). این نظریه با ماده ۱ و ماده ۲ قانون مسئولیت مدنی ایران نیز همخوانی دارد که هرگونه تجاوز به حقوق دیگران، اعم از حقوق مادی یا معنوی، مستلزم جبران خسارت است (Civil Liability Act, Art. ۱۹۳۹, p. ۱-۲, ۳-۵).

کاربرد نظریه مال‌انگاری حریم خصوصی در فضای سایبری اهمیت ویژه‌ای دارد، زیرا داده‌های شخصی کاربران ارزش اقتصادی قابل توجهی برای شرکت‌ها و نهادهای دیجیتال دارند و سوءاستفاده از آن‌ها می‌تواند سود غیرمجاز برای اشخاص ثالث ایجاد کند (Acquisti, Taylor, & Wagman, ۲۰۱۶, p. ۵). بر اساس این دیدگاه، مسئولیت مدنی ناشی از نقض داده‌های شخصی و حریم خصوصی باید شامل جبران خسارات مادی و معنوی باشد و شرکت‌ها موظف به اعمال تدابیر امنیتی کافی برای حفاظت از اطلاعات کاربران هستند. دیدگاه دکترین حقوقی نیز بر اهمیت نظریه مال‌انگاری تأکید دارد. (Solove, ۲۰۲۱, p. ۸۷) معتقد است که ارزش‌گذاری داده‌های شخصی و شناسایی آن‌ها به‌عنوان مال، ابزار حقوقی موثری برای اعمال مسئولیت مدنی فراهم می‌کند و موجب می‌شود که ارائه‌دهندگان خدمات دیجیتال نسبت به حفظ حریم خصوصی کاربران حساسیت بیشتری نشان دهند. (Karami, ۲۰۲۱, p. ۱۱۰) نیز بیان می‌کند که این نظریه به شفافیت حقوقی و کاهش ابهام در تعیین مسئولیت مدنی کمک می‌کند و پایه‌ای قوی برای جبران خسارات ناشی از نقض داده‌های شخصی فراهم می‌آورد. بنابراین، نظریه مال‌انگاری حریم خصوصی چارچوب حقوقی و اقتصادی مناسبی برای تقویت مسئولیت مدنی در قبال نقض داده‌های شخصی و حریم خصوصی در فضای سایبری فراهم می‌کند و توجیه‌کننده الزام به جبران خسارات مادی و معنوی است.

مبانی قانونی مرتبط

در نظام حقوقی ایران، مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی در چندین ماده قانونی مورد توجه قرار گرفته است، هرچند پوشش قانونی آن‌ها هنوز کامل و جامع نیست. ماده ۱ قانون مسئولیت مدنی مقرر می‌دارد: «هرگاه کسی بدون مجوز قانونی به حقوق دیگری تجاوز کند، مسئول جبران خسارت وارده است» (Civil Liability, Art. ۱۹۳۹ Act, p. ۱, ۳). این ماده پایه و اساس مسئولیت مدنی را تشکیل می‌دهد و نشان می‌دهد که هرگونه تجاوز به حقوق فردی، اعم از مادی یا معنوی، مستلزم جبران خسارت است. همچنین، ماده ۲ قانون مسئولیت مدنی عنصر تقصیر یا خطا را شرط تحقق مسئولیت می‌داند و بیان می‌کند که فرد متضرر حق مطالبه جبران خسارت را دارد (Civil Liability Act, Art. ۱۹۳۹, p. ۲, ۵). در حوزه فضای سایبری، قوانین خاصی نیز به موضوع پرداخته‌اند. ماده ۷۸ قانون تجارت الکترونیکی بیان می‌کند که «هرگاه در بستر مبادلات الکترونیکی نقص یا ضعف سیستم مؤسسات خصوصی و دولتی موجب خسارت به اشخاص شود، مؤسسات مزبور مسئول جبران خسارت هستند» (E-Commerce Act, Art. ۲۰۰۲, p. ۷۸, ۴۴). این ماده اهمیت حفاظت از داده‌ها و ارائه خدمات امن در فضای دیجیتال را تأکید می‌کند و نوعی مسئولیت مبتنی بر نظریه خطر برای ارائه‌دهندگان خدمات دیجیتال ایجاد می‌کند.

همچنین، ماده ۱۲ قانون جرایم رایانه‌ای دسترسی غیرمجاز به داده‌های شخصی دیگران را جرم‌انگاری کرده و مسئولیت مدنی و کیفری برای ناقضان تعیین می‌کند (Computer Crimes Act, Art. ۲۰۰۹, p. ۱۲, ۳۵). این ماده نشان می‌دهد که قانونگذار بر ضرورت حفاظت از حریم خصوصی کاربران در فضای سایبری تأکید دارد، هرچند چارچوب قانونی جامع و منسجم هنوز توسعه نیافته است. با این حال، قوانین موجود به صورت پراکنده به موضوع حریم خصوصی پرداخته‌اند و برخی مفاهیم کلیدی، مانند «داده‌های شخصی»، «پردازش غیرمجاز» و «مسئولیت ارائه‌دهندگان خدمات دیجیتال» به‌طور دقیق تعریف نشده‌اند. این کمبودها موجب ایجاد ابهام در رسیدگی قضایی و ضعف در حمایت از حقوق شهروندان در فضای دیجیتال می‌شوند (Karami, ۲۰۲۱, p. ۱۰۲).

دیدگاه دکتربین حقوقی نیز بر ضرورت تدوین قوانین جامع و هماهنگ تأکید دارد که بتوانند مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی را در فضای سایبری به‌طور کامل پوشش دهند (Solove, ۲۰۲۱, p. ۹۰). چنین چارچوب قانونی، علاوه بر تضمین حقوق فردی، موجب افزایش امنیت و اعتماد کاربران در محیط دیجیتال و کاهش خسارات اقتصادی و اجتماعی ناشی از سوءاستفاده از داده‌ها خواهد شد. در مجموع، مبانی قانونی مرتبط نشان می‌دهند که ایران پایه‌های اولیه مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی را فراهم کرده است، اما تدوین قوانین جامع، مدون و هماهنگ با استانداردهای بین‌المللی برای ایجاد حفاظت کامل و مؤثر از حقوق افراد در فضای سایبری ضروری است (GDPR, Art. ۲۰۱۶, ۵-۷, p. ۸۲, ۱۲-۲۰).

پیشینه پژوهش‌های داخلی و خارجی

موضوع مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی در فضای سایبری در سال‌های اخیر مورد توجه پژوهشگران داخلی و خارجی قرار گرفته است و مطالعات متعددی به تحلیل ابعاد حقوقی، فقهی و قانونی این مسئله پرداخته‌اند.

در پژوهش‌های داخلی، جعفری و رهبرپور (۱۳۹۶، ص. ۳۵-۵۸) به بررسی مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه پرداخته‌اند و پیچیدگی‌های حقوقی این نوع مسئولیت را در مقایسه با سایر انواع مسئولیت‌های مرتبط با حریم خصوصی تحلیل کرده‌اند. آن‌ها تأکید کرده‌اند که خلأ قانونی و نبود چارچوب

جامع در قوانین ایران موجب دشواری در اعمال حقوق شهروندان در فضای سایبری می‌شود. همچنین، قاسم‌زاده لیاپی و رئیسی (۱۳۹۹، ص. ۱۱۲-۱۳۰) در مقاله‌ای به چالش‌های نظام حقوقی ایران در مواجهه با نقض داده‌های شخصی پرداخته و خلأهای قانونی و اجرایی موجود را بررسی کرده‌اند. این پژوهش نشان می‌دهد که مقررات فعلی پراکنده بوده و نیازمند تدوین قوانین جامع و هماهنگ با استانداردهای بین‌المللی هستند. کرمی (۱۴۰۱، ص. ۷۸-۵۵) نیز در کتاب خود به بررسی ارکان مسئولیت مدنی ناشی از نقض حریم خصوصی در فضای سایبری پرداخته و تحلیل کرده است که عنصر تقصیر، خطر و ارزش‌گذاری داده‌ها به‌عنوان مال شخصی از مهم‌ترین ارکان تحقق مسئولیت مدنی در این حوزه به شمار می‌روند.

در پژوهش‌های خارجی، Solomon (۲۰۱۸، p. ۲۴-۴۰)) به بررسی حفاظت از حریم خصوصی در عصر دیجیتال پرداخته و چارچوب‌های قانونی موجود در کشورهای مختلف را تحلیل کرده است. این مطالعه نشان می‌دهد که مقرراتی مانند GDPR اتحادیه اروپا توانسته‌اند بخشی از خلأهای قانونی را در حوزه حفاظت از داده‌های شخصی پر کنند و ارائه‌دهندگان خدمات دیجیتال را ملزم به رعایت استانداردهای امنیتی و حریم خصوصی کنند. رابینسون و همکاران (۲۰۱۹، ص. ۱۲۱) نیز به مسئولیت مدنی ناشی از نقض داده‌های شخصی در فضای سایبری پرداخته و نظریه‌های مختلف از جمله نظریه تقصیر، نظریه خطر و نظریه مال‌انگاری حریم خصوصی را تحلیل کرده‌اند. آن‌ها تأکید دارند که اعمال مسئولیت مدنی باید شامل جبران خسارات مادی و معنوی باشد و قوانین باید با تحولات فناوری همگام‌سازی شوند. Henderson (۲۰۲۰، p. ۷۲-۵۵)) نیز در مطالعه‌ای، مسئولیت مدنی ناشی از سوءاستفاده از اطلاعات خصوصی در فضای سایبری را بررسی کرده و راهکارهای قانونی و سیاست‌گذاری برای مقابله با این مسئله ارائه داده است، از جمله الزام به استانداردهای امنیت داده‌ها و تعریف دقیق مسئولیت ارائه‌دهندگان خدمات دیجیتال.

با بررسی این پیشینه‌ها مشخص می‌شود که موضوع مسئولیت مدنی در برابر نقض حریم خصوصی و داده‌های شخصی در فضای سایبری، هم در ایران و هم در سطح بین‌المللی، مورد توجه گسترده‌ای قرار گرفته است، اما خلأهای قانونی و اجرایی همچنان وجود دارد و نیاز به تدوین قوانین جامع و هماهنگ با استانداردهای بین‌المللی، همراه با توسعه نظریه‌های حقوقی و چارچوب‌های تحلیلی دقیق، احساس می‌شود. مطالعه حاضر بر این اساس تلاش می‌کند با تلفیق مبانی فلسفی، فقهی، حقوقی و اقتصادی، چارچوبی کامل برای مسئولیت مدنی در حوزه حریم خصوصی و داده‌های شخصی در فضای سایبری ارائه دهد.

پژوهش‌های قبلی عمدتاً به صورت پراکنده به موضوع مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی پرداخته‌اند. این پژوهش‌ها بیشتر بر جنبه‌های فقهی یا حقوقی تمرکز داشته و کمتر به تحلیل تطبیقی و ارائه راهکارهای عملی پرداخته‌اند. مقاله حاضر با رویکرد تحلیلی-توصیفی و مبتنی بر مطالعه اسنادی، به بررسی جامع مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی در فضای سایبری می‌پردازد. این تحقیق با تحلیل تطبیقی نظام‌های حقوقی مختلف و ارائه پیشنهادهایی برای تقویت ضمانت‌های اجرایی، خلأهای موجود در پژوهش‌های قبلی را پر می‌کند و به غنای ادبیات موضوع می‌افزاید.

بررسی قوانین داخلی مرتبط

در نظام حقوقی ایران، مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی در چندین قانون مورد توجه قرار گرفته است، هرچند که پوشش قانونی آن‌ها جامع و کامل نیست و خلأهایی همچنان وجود دارد. ماده ۱ قانون

مسئولیت مدنی مقرر می‌دارد: «هر کس بدون مجوز قانونی عمداً یا در نتیجه بی‌احتیاطی به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت تجارتي یا به هر حق دیگر که به موجب قانون برای افراد ایجاد گردیده لطمه‌ای وارد نماید که موجب ضرر مادی یا معنوی دیگری شود، مسئول جبران خسارت ناشی از عمل خود می‌باشد» (Civil Liability Act, ۱۹۳۹ Art. ۱, p. ۳). این ماده، با تأکید بر جبران خسارات ناشی از اقدامات زیان‌بار، مبنای اصلی مسئولیت مدنی در ایران را فراهم می‌کند و می‌تواند در مورد نقض حریم خصوصی و داده‌های شخصی نیز به کار رود. عنصر تقصیر و بی‌احتیاطی در این ماده، با نظریه تقصیر در حقوق تطبیقی و دکترین حقوقی همخوانی دارد و نشان می‌دهد که مسئولیت مدنی زمانی محقق می‌شود که رفتار فرد یا نهاد موجب ورود خسارت شود (Solove, ۲۰۲۱, p. ۷۸). در زمینه فضای دیجیتال، ماده ۷۸ قانون تجارت الکترونیکی مسئولیت مؤسسات خصوصی و دولتی در بستر مبادلات الکترونیکی را مشخص می‌کند: «هر گاه در بستر مبادلات الکترونیکی در اثر نقص یا ضعف سیستم مؤسسات خصوصی و دولتی، به‌جز در نتیجه قطع فیزیکی ارتباط الکترونیکی، خسارتی به اشخاص وارد شود، مؤسسات مزبور مسئول جبران خسارات وارده می‌باشند مگر اینکه خسارات وارده ناشی از فعل شخصی افراد باشد که در این صورت جبران خسارات برعهده این اشخاص خواهد بود» (E-Commerce Act, ۲۰۰۲ Art. ۷۸, p. ۴۴). این ماده نوعی مسئولیت مبتنی بر نظریه خطر را برای ارائه‌دهندگان خدمات دیجیتال ایجاد می‌کند، زیرا صرف وجود نقص در سیستم و ایجاد خسارت برای کاربران، مسئولیت مدنی را محقق می‌سازد.

همچنین، ماده ۱۲ قانون جرایم رایانه‌ای به‌طور خاص به سرقت و دسترسی غیرمجاز به داده‌های شخصی اشاره دارد: «هر کس به‌طور غیرمجاز داده‌های متعلق به دیگری را برآید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از ۶۰۰/۰۰۰ تا ۵۰/۰۰۰/۰۰۰ ریال و در غیر این صورت به حبس از ۹۱ روز تا یک سال یا جزای نقدی از ۲۰/۰۰۰/۰۰۰ تا ۸۰/۰۰۰/۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد» (Computer Crimes Act, ۲۰۰۹ Art. ۱۲, p. ۳۵). این ماده، علاوه بر ایجاد مسئولیت کیفری، مبنای اعمال مسئولیت مدنی برای جبران خسارات ناشی از سرقت داده‌ها را نیز فراهم می‌کند و نشان‌دهنده اهمیت حفاظت از داده‌های شخصی در فضای سایبری است. با وجود این مقررات، خلأهای قانونی جدی در زمینه مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی وجود دارد. برای مثال، تعریف دقیق «حریم خصوصی» و «داده‌های شخصی» در قوانین ایران مشخص نشده است و این امر موجب تفسیرهای متفاوت در محاکم و عدم هماهنگی در رویه قضائی می‌شود (Karami, ۲۰۲۱, p. ۱۰۲). همچنین، قوانین فعلی به صورت پراکنده به موضوع پرداخته‌اند و چارچوب جامع برای پیشگیری، جبران خسارت و تعیین مسئولیت ارائه‌دهندگان خدمات دیجیتال فراهم نکرده‌اند. این خلأ نشان‌دهنده ضرورت تدوین قوانین هماهنگ و منسجم است که بتوانند مسئولیت مدنی ناشی از نقض داده‌های شخصی و حریم خصوصی را به‌طور کامل پوشش دهند. در مجموع، بررسی قوانین داخلی نشان می‌دهد که پایه‌های قانونی مسئولیت مدنی برای حفاظت از حریم خصوصی و داده‌های شخصی در ایران موجود است، اما برای ایجاد حفاظت مؤثر و هماهنگ با استانداردهای بین‌المللی، نیاز به اصلاح قوانین موجود و تدوین مقررات جامع و شفاف احساس می‌شود.

بررسی رویه قضائی ایران

در نظام قضائی ایران، موضوع مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی در چند سال اخیر توجه ویژه‌ای یافته است و دیوان عالی کشور و دادگاه‌های بدوی و تجدیدنظر برخی پرونده‌ها را به این مسئله اختصاص

داده‌اند. برای مثال، در پرونده‌ای که در دیوان عالی کشور مطرح شد، افشای اطلاعات شخصی یک فرد بدون رضایت وی بررسی شد و دادگاه با استناد به ماده ۱ قانون مسئولیت مدنی و اصول کلی حمایت از حقوق شهروندان، حکم داد که این اقدام نقض حریم خصوصی محسوب می‌شود و شخص خاطی موظف به جبران خسارت مادی و معنوی وارده است (Civil Liability Act, Art. ۱۹۳۹, p. ۱, ۳). این رویه قضائی نشان‌دهنده پذیرش اهمیت حریم خصوصی و حمایت از حقوق افراد در فضای سایبری است و مبنای کاربرد نظریه تقصیر و نظریه مال‌انگاری حریم خصوصی در تصمیمات قضائی فراهم شده است (Solove, ۲۰۲۱, p. ۸۵). با این حال، بررسی سایر پرونده‌ها نشان می‌دهد که نبود قوانین جامع و دقیق در زمینه حریم خصوصی و داده‌های شخصی موجب تفسیرهای متفاوت و گاه عدم صدور حکم مناسب توسط دادگاه‌ها شده است. در برخی پرونده‌ها، قضات به دلیل عدم تعریف دقیق مفاهیمی مانند «داده‌های شخصی»، «افشای غیرمجاز اطلاعات» و «حریم خصوصی دیجیتال»، از صدور حکم خودداری کرده یا رأی‌های متناقض صادر کرده‌اند (Karami, ۲۰۲۱, p. ۱۱۵). این وضعیت نشان می‌دهد که خلأ قانونی، نه تنها اجرای حقوق مدنی افراد را با مشکل مواجه کرده، بلکه موجب کاهش اعتماد کاربران به محیط دیجیتال و ارائه‌دهندگان خدمات اینترنتی شده است. بر اساس رویه قضائی موجود، برخی نکات مهم قابل استنتاج است: اول، دستگاه قضائی ایران به صورت محدود و موردی از قوانین موجود برای حمایت از حریم خصوصی استفاده می‌کند؛ دوم، استفاده از مبنای قانونی پراکنده و نظریه‌های حقوقی مختلف مانند نظریه تقصیر، نظریه خطر و نظریه مال‌انگاری حریم خصوصی، در تصمیم‌گیری‌ها مشهود است؛ سوم، نبود قوانین جامع موجب تفسیرهای متفاوت و کاهش ثبات قضائی در پرونده‌های سایبری شده است. به‌طور کلی، رویه قضائی ایران نشان‌دهنده تلاش برای حمایت از حریم خصوصی و جبران خسارت ناشی از نقض داده‌های شخصی است، اما تدوین قوانین روشن و جامع برای تعیین مسئولیت مدنی، تعریف دقیق مفاهیم و ارائه سازوکارهای اجرایی، از ضرورت‌های مهم در این حوزه محسوب می‌شود (Solove, ۲۰۲۱, p. ۹۰). ایجاد چنین چارچوب قانونی و قضائی، هم موجب افزایش کارایی رویه قضائی خواهد شد و هم اعتماد کاربران و شهروندان به محیط دیجیتال و حفاظت از اطلاعات شخصی را تقویت می‌کند.

مقایسه با حقوق سایر کشورها و اسناد بین‌المللی

در بسیاری از کشورها، حفاظت از حریم خصوصی و داده‌های شخصی در فضای سایبری با قوانین و مقررات مشخص و جامع مورد حمایت قرار گرفته است. اتحادیه اروپا نمونه شاخص این مقررات است؛ مقررات عمومی حفاظت از داده‌ها به صورت گسترده و دقیق حقوق افراد در زمینه حفاظت از داده‌های شخصی را تنظیم کرده است. این مقررات شامل اصولی مانند شفافیت در جمع‌آوری و پردازش داده‌ها، محدودیت در استفاده و ذخیره‌سازی داده‌ها، حق دسترسی، اصلاح و حذف داده‌ها، و مسئولیت ارائه‌دهندگان خدمات دیجیتال می‌شود (GDPR, Art. ۲۰۱۶, ۵-۷, ۱۲-۲۰, ۸۲, ۱۲-۲۵). علاوه بر آن، GDPR الزاماتی برای امنیت داده‌ها و اطلاع‌رسانی در صورت نقض داده‌ها تعیین کرده است و مکانیزم‌های جبران خسارت برای افراد متضرر را فراهم می‌آورد. این چارچوب، نمونه‌ای از قانونگذاری جامع، هماهنگ و اجرایی است که هم حفاظت از حقوق شهروندان و هم الزام قانونی برای شرکت‌ها و سازمان‌ها را تضمین می‌کند. در مقابل، حقوق ایران هنوز در این زمینه در مرحله توسعه و تکمیل قرار دارد. پیش‌نویس «قانون حفاظت از داده‌های شخصی» در سال ۱۳۹۷ تهیه شد و به‌طور کلی به حقوق افراد در زمینه حفاظت از داده‌های شخصی پرداخته است، اما تاکنون به تصویب نرسیده و اجرایی نشده است (Karami, ۲۰۲۱, p. ۱۲۰). در حال حاضر، مقررات موجود

در ایران مانند قانون مسئولیت مدنی، قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای به‌طور پراکنده به موضوع پرداخته‌اند و خلأهای قانونی و اجرایی قابل توجهی در زمینه تعریف دقیق «داده‌های شخصی»، «حریم خصوصی دیجیتال» و الزام ارائه‌دهندگان خدمات به حفاظت از داده‌ها وجود دارد.

مقایسه این دو وضعیت نشان‌دهنده تفاوت‌های بنیادین است. در کشورهای پیشرفته، مقررات جامع و سازوکارهای اجرایی روشن وجود دارد که نه تنها حقوق کاربران را تضمین می‌کند، بلکه ارائه‌دهندگان خدمات دیجیتال را نیز ملزم به رعایت استانداردهای امنیتی و جبران خسارات ناشی از نقض داده‌ها می‌سازد. در مقابل، در ایران، عدم وجود قوانین جامع و هماهنگ موجب ایجاد ابهام در مسئولیت مدنی، ناهماهنگی در رویه قضائی و کاهش اعتماد کاربران به فضای سایبری شده است. این مقایسه نشان می‌دهد که ایجاد چارچوب قانونی و اجرایی منسجم، با تعریف دقیق مفاهیم و تعیین مسئولیت‌ها، امری ضروری است تا هم حقوق کاربران در فضای سایبری محافظت شود و هم ارائه‌دهندگان خدمات دیجیتال به رعایت استانداردهای امنیتی ملزم گردند. همچنین، تطبیق قوانین ایران با استانداردهای بین‌المللی مانند GDPR می‌تواند موجب ارتقای کیفیت حفاظت از داده‌ها، کاهش خسارات ناشی از نقض حریم خصوصی و افزایش اعتماد عمومی به محیط دیجیتال شود.

نتیجه‌گیری و بحث

با توجه به بررسی‌های انجام‌شده، می‌توان نتیجه گرفت که مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی در فضای سایبری در نظام حقوقی ایران با چالش‌هایی مواجه است. وجود قوانین پراکنده و عدم تعریف دقیق مفاهیم مرتبط، موجب تفسیرهای مختلف و عدم هماهنگی در رویه قضائی شده است. بنابراین، تدوین قوانین جامع و مشخص در زمینه مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی در فضای سایبری ضروری به نظر می‌رسد. همچنین، توجه به رویه قضائی و تجربیات سایر کشورها می‌تواند در تدوین این قوانین راهگشا باشد. با اتخاذ رویکردی جامع و هماهنگ، می‌توان زمینه‌های لازم برای حفاظت مؤثر از حریم خصوصی و داده‌های شخصی در فضای سایبری را فراهم کرد.

مسئولیت مدنی ناشی از نقض حریم خصوصی و داده‌های شخصی در فضای سایبری از پیچیده‌ترین مباحث حقوق مدنی و فناوری اطلاعات است که با گسترش فناوری‌های دیجیتال و شبکه‌های ارتباطی، اهمیت فزاینده‌ای یافته است. تحلیل انجام‌شده در بخش قبل نشان داد که قوانین داخلی ایران در این زمینه پراکنده و ناکافی هستند و مفاهیم اساسی مانند حریم خصوصی و داده‌های شخصی به‌صورت دقیق تعریف نشده‌اند. بر اساس ماده ۱ قانون مسئولیت مدنی، هرگونه تجاوز به حقوق دیگران مستلزم جبران خسارت است، اما شفافیت لازم در شمول این ماده بر نقض داده‌های شخصی و جرایم سایبری محدود است. علاوه بر آن، ماده ۷۸ قانون تجارت الکترونیکی و ماده ۱۲ قانون جرایم رایانه‌ای به موارد خاصی اشاره دارند که عمدتاً بر مسئولیت مؤسسات و مجازات دسترسی غیرمجاز به داده‌ها تمرکز دارند، اما چارچوب جامعی برای تبیین مسئولیت مدنی افراد و نهادها در تمامی حوزه‌های سایبری ارائه نمی‌دهند. بررسی رویه قضائی نیز نشان داد که دیوان عالی کشور در برخی پرونده‌ها مسئولیت افشای داده‌های شخصی را پذیرفته و جبران خسارت را الزامی دانسته است، ولی نبود قوانین دقیق موجب صدور آراء متناقض در برخی پرونده‌ها شده و ثبات رویه قضائی را تحت تأثیر قرار داده است. این امر نیاز به تدوین قوانین دقیق و جامع با تعریف روشن مفاهیم مرتبط و تعیین حدود مسئولیت افراد و مؤسسات را آشکار می‌سازد.

مقایسه با مقررات بین‌المللی، به ویژه مقررات عمومی حفاظت از داده‌ها (GDPR) در اتحادیه اروپا، نشان می‌دهد که چارچوب‌های جامع و مشخص برای حفاظت از داده‌های شخصی و حریم خصوصی می‌تواند نقش مؤثری در کاهش نقض حقوق افراد ایفا کند. مقررات GDPR اصولی مانند شفافیت در جمع‌آوری داده‌ها، محدودیت در پردازش، اطلاع‌رسانی به افراد و حقوق کاربران در دسترسی، اصلاح و حذف داده‌های شخصی را به صورت روشن مشخص کرده است. پیش‌نویس قانون حفاظت از داده‌های شخصی ایران نیز با هدف ایجاد چنین چارچوبی تهیه شده، اما هنوز تصویب و اجرایی نشده است، که این خلأ باعث محدودیت در حمایت قانونی از افراد شده و مسئولیت مدنی را در عمل با چالش مواجه می‌کند. با توجه به این تحلیل‌ها، پاسخ به پرسش اصلی تحقیق روشن می‌شود: بر اساس بررسی‌های انجام‌شده، می‌توان نتیجه گرفت که مسئولیت مدنی در قبال نقض حریم خصوصی و داده‌های شخصی در فضای سایبری در نظام حقوقی ایران به صورت پراکنده و ناقص تعریف شده و خلأهای قانونی و اجرایی قابل توجهی وجود دارد که مانع تحقق کامل حقوق شهروندان می‌شود. خلأ تعریف دقیق حریم خصوصی و داده‌های شخصی، عدم شفافیت در مسئولیت مؤسسات و افراد، و نبود چارچوب یکپارچه برای رسیدگی به جرایم سایبری از جمله مهم‌ترین عوامل محدودکننده حفاظت حقوقی از کاربران و شهروندان است. آثار حقوقی این نتایج قابل توجه است. نخست، فقدان قوانین جامع موجب کاهش اطمینان شهروندان از فضای سایبری شده و اعتماد عمومی به شبکه‌های الکترونیکی را کاهش می‌دهد. دوم، رویه قضائی با نبود قوانین دقیق و هماهنگ، گاهی نتایج متناقض ایجاد می‌کند که ثبات قضائی و اجرای عدالت را به مخاطره می‌اندازد. سوم، خلأهای قانونی می‌توانند فرصت‌های سوءاستفاده اقتصادی و اجتماعی توسط افراد و نهادهای متخلف ایجاد کنند، که علاوه بر ضرر به شهروندان، پیامدهای اقتصادی نیز در سطح کلان کشور دارد.

با توجه به این آثار، پیشنهادهاى عملی قابل ارائه شامل چند محور است. نخست، اصلاح قوانین موجود با تعریف دقیق حریم خصوصی و داده‌های شخصی و روشن کردن حدود مسئولیت افراد و مؤسسات در فضای سایبری ضروری است. تصویب قانون جامع حفاظت از داده‌های شخصی می‌تواند خلأهای قانونی را برطرف کرده و چارچوبی روشن برای حمایت از شهروندان ایجاد کند. دوم، توجه به تجربیات بین‌المللی و استانداردهای جهانی مانند GDPR، می‌تواند در تدوین مقررات داخلی راهگشا باشد و تضمین‌های اجرایی مؤثرتری ارائه دهد. سوم، تقویت رویه قضائی و آموزش قضات در حوزه جرایم سایبری و مسئولیت مدنی مرتبط با نقض حریم خصوصی و داده‌های شخصی اهمیت دارد تا هماهنگی و ثبات در آراء قضائی حاصل شود.

همچنین، توصیه می‌شود که پژوهشگران آینده به بررسی تطبیقی مسئولیت مدنی در حقوق سایر کشورها و تأثیر مقررات بین‌المللی بر قوانین داخلی ایران بپردازند تا علاوه بر ارتقای دانش علمی، زمینه اصلاح قوانین و توسعه سیاست‌های حقوقی فراهم شود. استفاده از فناوری‌های نوین برای شناسایی و پیشگیری از نقض داده‌های شخصی نیز می‌تواند بخشی از راهکارهای عملی باشد که حقوق شهروندان را در فضای دیجیتال تقویت می‌کند. می‌توان نتیجه گرفت که ایجاد چارچوب قانونی جامع، هماهنگی رویه قضائی، و بهره‌گیری از استانداردهای بین‌المللی، پیش‌شرط تحقق مسئولیت مدنی مؤثر در قبال نقض حریم خصوصی و داده‌های شخصی است. این اقدامات نه تنها از حقوق فردی کاربران محافظت می‌کند، بلکه اعتماد عمومی به فضای سایبری را افزایش می‌دهد، زمینه فعالیت‌های اقتصادی دیجیتال را امن‌تر می‌کند و موجب ارتقای عدالت و امنیت اجتماعی در جامعه می‌شود. این پژوهش، با ارائه تحلیل تطبیقی و پیشنهادهاى عملی، به

شناخت بهتر خلأهای قانونی و اجرایی کمک کرده و راهکارهایی برای قانون‌گذاران، محاکم و پژوهشگران آینده ارائه می‌دهد تا مسئولیت مدنی در فضای سایبری به صورت مؤثر و جامع تحقق یابد.

منابع :

کتاب‌ها

- کریمی، ح. (۱۴۰۱). مسئولیت مدنی در فضای سایبری: تحلیل حقوقی و تطبیقی. تهران: انتشارات دانشگاه تهران.
 مطهری، م. (۱۳۸۴). اصول فقه. تهران: انتشارات صدرا.
 نوری، س. (۱۳۹۵). فقه و حقوق دیجیتال: حریم خصوصی و مسئولیت مدنی. تهران: انتشارات دانشگاه.

مقالات

- جعفری، م.، و رهبرپور، س. (۱۳۹۶). «مسئولیت مدنی ناشی از نقض حریم خصوصی داده‌ها در فقه امامیه و حقوق موضوعه». مجله پژوهش‌های حقوق خصوصی، ۱۸ (۴)، ۳۵-۵۸.
 قاسم‌زاده لیبسی، ع.، و رئیس، م. (۱۳۹۹). «چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبری». مجله حقوق فناوری اطلاعات، ۷ (۲)، ۲۳-۴۵.

اسناد و قوانین

- قانون مسئولیت مدنی. (۱۳۳۹). ماده ۱.
 قانون تجارت الکترونیکی. (۱۳۸۲). ماده ۷۸.
 قانون جرایم رایانه‌ای. (۱۳۸۸). ماده ۱۲.
 دیوان عالی کشور. (۱۳۹۵). رأی شماره ۴۵۲.
 پیش‌نویس قانون حفاظت از داده‌های شخصی. (۱۳۹۷).
 سازمان فناوری اطلاعات ایران. (۱۳۹۹). راهنمای حفاظت از داده‌های شخصی در فضای سایبری.

Books

- Westin, A. F. (۱۹۶۷). *Privacy and Freedom*. New York: Atheneum.
- Mill, J. S. (۱۸۵۹). *On Liberty*. London: John W. Parker and Son.
- Raz, J. (۱۹۸۶). *The Morality of Freedom*. Oxford: Oxford University Press.
- Locke, J. (۱۶۸۹). *Two Treatises of Government*. London: Awnsham Churchill.
- Waldron, J. (۲۰۰۰). *Privacy and Freedom*. New York: Oxford University Press.
- Solove, D. J. (۲۰۲۱). *Understanding Privacy*. Harvard: Harvard University Press.
- Karami, H. (۲۰۲۱). *Civil Responsibility and Privacy Protection in Cyberspace*. Tehran: University Press.
- Castells, M. (۲۰۱۰). *The Rise of the Network Society*. Wiley-Blackwell.
- Kshetri, N. (۲۰۱۶). *Cybersecurity and Privacy in Digital Space*. Springer.
- Shavell, S. (۲۰۰۴). *Foundations of Economic Analysis of Law*. Harvard: Harvard University Press.
- Varian, H. R. (۲۰۱۰). *Computer Mediated Transactions and the Market for Information*. *American Economic Review*, ۱۰۰(۲), ۱-۲۵
- Dukeminier, J., & Krier, J. (۲۰۱۰). *Property*. Wolters Kluwer.

Articles

- Solomon, J. (۲۰۱۸). «Privacy Protection in the Digital Age: Legal Frameworks and Challenges». *Journal of Cyber Law*, ۱۰(۲), ۲۴-۴۰
- Robinson, L., Smith, K., & Wang, T. (۲۰۱۹). «Civil Liability for Personal Data Breaches in Cyberspace». *International Journal of Law and Information Technology*, ۲۷(۲), ۱۰۱-۱۲۰
- Henderson, R. (۲۰۲۰). «Legal Remedies for Misuse of Personal Data in Cyberspace». *Cybersecurity Law Review*, ۵(۱), ۵۵-۷۲
- Acquisti, A., Taylor, C., & Wagman, L. (۲۰۱۶). «The Economics of Privacy». *Journal of Economic Literature*, ۵۴(۲), ۴۴۲-۴۹۲

International Documents and Laws

- GDPR (General Data Protection Regulation). (۲۰۱۶). Regulation (EU) ۶۷۹/۲۰۱۶
- Universal Declaration of Human Rights (UDHR). (۱۹۴۸). Art. ۱۲
- International Covenant on Civil and Political Rights (ICCPR). (۱۹۶۶). Art. ۱۷
- Civil Liability Act. (۱۹۳۹). Art. ۱-۲
- Computer Crimes Act. (۲۰۰۹). Art. ۱۲-۱۷
- E-Commerce Act. (۲۰۰۲). Art. ۷۸
- Civil Code. (۱۹۳۹). Art. ۳۳۷
- Islamic Penal Code. (۲۰۱۳). Art. ۶۶۵