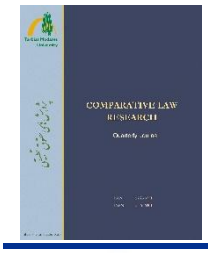

Comparative Law Research Quarterly, Vol. 30, No.2, Summer 2026, Pp. 37-66

The Legal Framework for the Protection of Privacy in the Digital Environment: A Comparative Study of the Legal Systems of the United States, the European Union, and Iran

ARTICLE INFO
DOI: 10.48311/clr.2025.101678.0

Article Type
Research Article

Authors:
[1] Abdolsaeed Shojaei*
ORCID: https://0009-0000-5575-035X
2 Shahram Rahmani
ORCID: https://0009-0002-0571-9260

Affiliation:
[1] Assistant Professor in Public Law, Payame Noor University, Tehran, Iran
[2] Assistant Professor in Private Law, Payame Noor University, Tehran, Iran

Correspondence:
Email: Dr.saeedshojaei62@pnu.ac.ir

Article History:
Received:2025/07/09
Received in Revised form: 2025/10/17
Accepted: 2025/12/01

Abstract

The development of digital technologies, alongside their undeniable advantages, has generated serious challenges for the protection of privacy. The emergence of social networks, artificial intelligence, and the Internet of Things has enabled the large-scale collection of personal data by both public and private actors, thereby significantly diminishing individuals' control over their own information. Adopting a descriptive-analytical approach, this research examines the challenges of privacy protection across three legal systems: the United States, the European Union, and Iran. In the United States, the legal framework for privacy protection is based on statutes such as the Privacy Act of 1974 and the Children's Online Privacy Protection Act (COPPA), which emphasize self-regulation and the role of the private sector. However, due to a lack of regulatory coherence and heavy reliance on voluntary compliance mechanisms, this system faces significant enforcement challenges. By contrast, the European Union, through the General Data Protection Regulation (GDPR), has established a comprehensive and stringent regime grounded in principles such as transparency, consent, and the right to be forgotten. In Iran, although constitutional principles—particularly Articles 22 and 25 of the Constitution—along with sectoral laws such as the Computer Crimes Act and the Electronic Commerce Act provide fragmented forms of privacy protection, the absence of a comprehensive data protection statute, regulatory fragmentation, and weak oversight mechanisms constitute major challenges. The findings of this research emphasize the importance of employing protective technologies such as encryption and digital identity management, as well as the critical role of user education and cooperation between governmental and civil institutions in enhancing data protection.

Keywords: Privacy, Cyberspace, General Data Protection Regulation (GDPR), Computer Crimes Act, Personal Data Protection in Iran

Copyright © 2026, TMU Press. This open-access article is published under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (https://creativecommons.org/licenses/by-nc/4.0) which permits Share (copy and redistribute the material in any medium or format) and Adapt (remix, transform, and build upon the material) under the Attribution-NonCommercial terms.

فصلنامه پژوهش‌های حقوق تطبیقی
دوره ۳۰، شماره ۲، تابستان ۱۴۰۵
صص ۳۷-۶۶
مقاله پژوهشی

Comparative Law Research Quarterly
Vol.30, No.2, Summer 2026
Pp 1-66
Original Article

چهارچوب حقوقی حفاظت از حریم خصوصی در بستر دیجیتال: مطالعه تطبیقی در نظام‌های حقوقی ایالات‌متحده، اتحادیه اروپا و ایران

عبدالسعید شجاعی[1*] ، شهرام رحمانی[2]

۱. عضو هیأت علمی دانشگاه پیام‌نور، تهران، ایران
۲. عضو هیأت علمی دانشگاه پیام‌نور، تهران، ایران

تاریخ ارسال : ۱۴۰۴/۰۴/۱۸ تاریخ بازنگری: ۱۴۰۴/۰۷/۲۵ تاریخ پذیرش: ۱۴۰۴/۰۹/۱۰

چکیده

تحولات فناوری‌های دیجیتال در کنار مزایا، چالش‌های جدی برای حریم خصوصی ایجاد کرده‌اند. ظهور شبکه‌های اجتماعی، هوش مصنوعی و اینترنت اشیا امکان جمع‌آوری گسترده داده‌های شخصی را برای نهادهای دولتی و خصوصی فراهم کرده و کنترل افراد بر اطلاعات خود را کاهش داده است. این پژوهش با رویکرد تحلیلی – توصیفی، چالش‌های حفاظت از حریم خصوصی را در ایالات‌متحده، اتحادیه اروپا و ایران بررسی می‌کند. در ایالات‌متحده، چهارچوب حقوقی حریم خصوصی مبتنی بر قوانینی مانند قانون حریم خصوصی ۱۹۷٤ و COPPA است که بر خودتنظیمی و نقش بخش خصوصی تأکید دارد، اما به‌دلیل نبود هماهنگی میان قوانین و اتکای زیاد به مقررات داوطلبانه، با مشکلات اجرایی مواجه است. در مقابل، اتحادیه اروپا با مقررات عمومی حفاظت از داده‌ها، نظامی جامع و سخت‌گیرانه مبتنی بر اصولی

* نویسندهٔ مسئول مقاله: Email: Dr.saeedshojaei62@pnu.ac.ir

کپی‌رایت © ۲۰۲٦، انتشارات دانشگاه تربیت مدرس (TMU Press). این مقاله به‌صورت دسترسی آزاد منتشر شده و تحت مجوز بین‌المللی Creative Commons Attribution-NonCommercial 4.0 قرار دارد. بر اساس این مجوز، شما می‌توانید این مطلب را در هر قالب و رسانه‌ای کپی، بازنشر و بازآفرینی کنید و یا آن را ویرایش و بازسازی نمایید، به شرط آنکه نام نویسنده را ذکر کرده و از آن برای مقاصد غیرتجاری استفاده کنید.

چون شفافیت، رضایت و حق فراموشی ارائه کرده است. در ایران، اگرچه اصول ۲۲ و ۲۵ قانون اساسی و قوانینی نظیر قانون جرایم رایانه‌ای و تجارت الکترونیکی به‌صورت پراکنده از حریم خصوصی حمایت می‌کنند، اما فقدان قانون جامع، پراکندگی مقررات و ضعف نظارت از چالش‌های مهم به شمار می‌رود. یافته‌ها بر اهمیت استفاده از فناوری‌های حفاظتی مانند رمزنگاری، مدیریت هویت دیجیتال و نقش آموزش کاربران و همکاری نهادهای دولتی و مدنی در ارتقای حفاظت از داده‌ها تأکید دارند.

واژگان کلیدی: حریم خصوصی، فضای مجازی، مقررات عمومی حفاظت از داده‌ها، قانون جرایم رایانه‌ای، حفاظت از داده‌های شخصی در ایران

۱. مقدمه

حریم خصوصی به‌عنوان یکی از حقوق بنیادین انسان مفهومی پیچیده و چندبعدی است که در عصر دیجیتال بُعد جدیدی به خود گرفته است. در دنیای امروز با گسترش فناوری‌های نوین و افزایش استفاده از اینترنت، ابعاد حریم خصوصی در فضای مجازی به چالشی جدی تبدیل شده است. این مفهوم نه‌تنها به حق فردی برای حفظ اطلاعات شخصی و کنترل بر داده‌های خود اشاره دارد، بلکه به تأثیرات عمیق آن بر حقوق عمومی، آزادی‌های فردی و امنیت اجتماعی نیز مرتبط است. حریم خصوصی به‌عنوان یک سپر حقوقی می‌تواند در برابر نقض آزادی‌ها و حقوق شهروندان عمل کند و در عین حال حفظ امنیت اجتماعی و اعتماد عمومی را تسهیل نماید.

در این مقاله به بررسی ابعاد مختلف حریم خصوصی در فضای مجازی پرداخته خواهد شد. تحلیل تأثیرات حریم خصوصی بر حقوق عمومی و شناسایی چالش‌های موجود در این زمینه هدف اصلی این پژوهش است؛ به‌ویژه در دنیای دیجیتال، جایی که اطلاعات به‌سرعت به اشتراک گذاشته می‌شوند و ردپاهای دیجیتال به‌راحتی قابل ردیابی هستند، پیگیری حریم خصوصی به یکی از اولویت‌های اصلی تبدیل شده است. چالش‌های مرتبط با این حوزه شامل نقض حریم خصوصی توسط نهادهای دولتی و خصوصی، دسترسی غیرمجاز به اطلاعات شخصی و عدم شفافیت در سیاست‌های حفظ حریم خصوصی است. علاوه‌براین، مقاله به بررسی راهکارهای

پیشنهادی برای تقویت و حمایت از حریم خصوصی در عصر دیجیتال خواهد پرداخت. این راهکارها می‌تواند شامل تدوین قوانین جدید، ایجاد آگاهی عمومی و ارتقای فرهنگ حفظ حریم خصوصی باشد. پرسش‌های کلیدی این مقاله شامل چالش‌های اصلی حریم خصوصی، تأثیرات آن بر جامعه و حقوق فردی و استراتژی‌های مؤثر برای حفاظت از این حق بنیادین خواهد بود.

پلان پژوهش حاضر مبتنی بر رویکردی تحلیلی - تطبیقی طراحی شده است تا از رهگذر تبیین مبانی نظری و مقایسه تطبیقی نظام‌های حقوقی ایالات‌متحده، اتحادیه اروپا و ایران تصویری جامع از چالش‌ها و راهکارهای حمایت از حریم خصوصی در بستر دیجیتال ارائه دهد. این ساختار از منطق درونی و پیوستگی مفهومی برخوردار است: ابتدا با بررسی مبانی نظری و حقوقی حریم خصوصی در حقوق عمومی، بنیآن‌های مفهومی و اصول بنیادین تبیین می‌شود؛ سپس در بخش دوم با تحلیل چالش‌های قانونی در فضای مجازی، قلمرو تهدیدات و نارسایی‌های ساختاری نظام‌های حقوقی آشکار می‌گردد؛ بخش سوم به مطالعه چهارچوب‌های قانونی و سیاست‌گذاری در سطح ملی و بین‌المللی اختصاص یافته تا ظرفیت‌ها و کاستی‌های نظام تقنینی ایران در پرتو تجارب تطبیقی بررسی شود، و نهایتاً بخش چهارم، با طرح راهکارهای فناورانه، آموزشی و نهادی پیوند میان تحلیل نظری و کاربرد عملی را برقرار می‌سازد. بنابراین، ترتیب منطقی فصول از مبانی مفهومی به سوی تحلیل چالش‌ها و ارائه راه‌حل‌ها حرکت کرده و انسجام علمی مقاله را در قالبی تطبیقی و مسئله‌محور تضمین می‌کند.

۲. مبانی نظری حریم خصوصی در حقوق عمومی

حریم خصوصی به‌عنوان یکی از حقوق بنیادین بشر، در چهارچوب‌های مختلف حقوقی تعریف و تبیین شده است. این مفهوم در طول زمان و با توجه به تحولات اجتماعی، فرهنگی و فناوری ابعاد گوناگونی پیدا کرده است. حریم خصوصی به‌طورکلی به حق فرد برای کنترل بر اطلاعات شخصی و زندگی خصوصی خود اشاره دارد (Posner, 1977: 393). این حق شامل آزادی از مداخله، نظارت و دخالت‌های غیرمجاز در زندگی فردی است و در بسیاری از نظام‌های حقوقی به‌عنوان یک حق اساسی و غیرقابل سلب شناخته می‌شود که باید در برابر هرگونه نقض حفاظت

شود.

ابعاد حقوقی حریم خصوصی شامل چند جنبه مهم است؛ یکی از این ابعاد حریم خصوصی اطلاعات است که به کنترل فرد بر اطلاعات شخصی و داده‌های خود اشاره دارد. در دنیای دیجیتال حفاظت از داده‌ها و اطلاعات شخصی در برابر دسترسی‌های غیرمجاز و سوءاستفاده‌های احتمالی از اهمیت ویژه‌ای برخوردار است. قوانین مختلف مانند مقررات عمومی حفاظت از داده‌ها[1] در اتحادیه اروپا به حمایت از این بعد اختصاص دارد (Hoofnagle, 2019: 89). بعد دیگر حریم خصوصی، حریم خصوصی ارتباطات است که به امنیت و محرمانگی ارتباطات فردی اشاره دارد. افراد باید حق داشته باشند که بدون ترس از نظارت یا شنود، با دیگران ارتباط برقرار کنند. این بعد شامل حفاظت از تماس‌ها، پیام‌ها و داده‌های دیجیتال است (Westin, 2003: 434).

حریم خصوصی یکی از حقوق بنیادین بشر است که در اسناد بین‌المللی حقوق بشر و قوانین اساسی کشورها مورد شناسایی و حمایت قرار گرفته است. به لحاظ حقوقی، این حق دارای دو بعد اساسی است: اول، حریم خصوصی فردی که به حق افراد در حفظ و کنترل اطلاعات شخصی و محرمانه خود مربوط می‌شود (Berween, 2002: 61-79) و دوم، حریم خصوصی خانوادگی و اجتماعی که ناظر بر حق افراد در برخورداری از یک زندگی خصوصی و خانوادگی بدون مداخله‌های غیرموجه است (Hamilton, 2006: 42-43).

در عصر دیجیتال مفهوم حریم خصوصی با چالش‌های نوینی مواجه شده است. پیشرفت‌های تکنولوژیک و گسترش شبکه‌های اجتماعی مرزهای سنتی حریم خصوصی را دستخوش تغییرات اساسی کرده است. در این راستا، دکترین حقوقی «حق بر داده‌های شخصی» به وجود آمده است که بر اساس آن افراد حق دارند بر نحوه جمع‌آوری، پردازش و استفاده از داده‌های شخصی خود کنترل داشته باشند. این حق به‌ویژه در چهارچوب مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا به رسمیت شناخته شده است که به افراد اجازه می‌دهد بر داده‌های خود مالکیت و کنترل داشته باشند و شامل حقوقی مانند حق رضایت صریح، حق فراموشی و حق

1. GDPR

انتقال داده‌ها می‌شود. این دکترین به افراد این امکان را می‌دهد که در برابر سوءاستفاده‌های احتمالی، از داده‌های شخصی خود محافظت کنند و به‌طورکلی به تقویت حقوق فردی و کاهش نابرابری‌های اطلاعاتی بین افراد و نهادهای پردازش‌کننده داده‌ها کمک می‌کند (Sembiring, 2024: 712). با توجه به مخاطرات نقض حریم خصوصی و امنیت داده‌ها در بستر دیجیتال مبتنی بر داده‌های شخصی، این پژوهش تمرکز خود را بر سامانه‌هایی معطوف می‌کند که از انواع دیگر داده‌ها استفاده می‌کنند. این سامانه دیجیتالی نمونه‌ای از دیجیتال‌سازی پیشرفته قوانین پیچیده است که بدون وابستگی افراطی به فناوری یا تمرکز انحصاری بر داده‌های شخصی عمل می‌کند (درامن، ١٤٠٤: ١٩١).

نکته حائز اهمیت این است که حمایت از حریم خصوصی در فضای سایبری مستلزم اتخاذ رویکردی جامع و چندوجهی است که هم جنبه‌های حقوقی و هم ابعاد فنی را در بر می‌گیرد. قانون‌گذاران باید ضمن به‌روزرسانی چهارچوب‌های قانونی موجود، مکانیسم‌های اجرایی مؤثری برای مقابله با نقض حریم خصوصی در نظر بگیرند. این امر به‌ویژه در مورد شرکت‌های فناوری و پلتفرم‌های آنلاین که حجم عظیمی از داده‌های کاربران را در اختیار دارند اهمیت ویژه‌ای می‌یابد. به‌عنوان یک بنیان در حقوق، هرگونه محدودیت یا مداخله در حریم خصوصی افراد باید مبتنی بر قانون ضروری و متناسب باشد. این امر مستلزم ایجاد توازن میان حقوق فردی و منافع عمومی است.

۲-۱) حریم خصوصی در نظام‌های حقوقی

۲-۱-۱) مبانی قانونی حریم خصوصی در ایالات‌متحده

حق بر حریم خصوصی در نظام حقوقی ایالات‌متحده آمریکا علی‌رغم عدم تصریح مستقیم در قانون اساسی، از طریق تفاسیر قضایی و دکترین حقوقی به‌عنوان یکی از حقوق بنیادین مورد شناسایی قرار گرفته است. این حق که ماهیتاً از مصادیق حقوق نسل اول بشر محسوب می‌شود عمدتاً از طریق تفسیر موسع اصلاحیه‌های چهارم، پنجم، نهم و چهاردهم قانون اساسی استنباط می‌گردد. در رویه قضایی دیوان‌عالی فدرال، مفهوم حریم خصوصی از طریق دکترین «حقوق

ضمنی»[۲] و نظریه «حریم معقول انتظار»[۳] توسعه یافته است (Levin & Nicholson, 2005: 357). این حقوق شامل حق زندگی خصوصی است که به‌طور ضمنی از بندهای مختلف قانون اساسی به‌ویژه متمم‌های اول، سوم، چهارم و نهم استنباط می‌شود. متمم چهارم به‌طور خاص بر حفاظت از افراد در برابر بازرسی‌های غیرمجاز تأکید دارد و به نوعی به حق حریم خصوصی اشاره می‌کند. همچنین آزادی بیان که در متمم اول قانون اساسی به آن تأکید شده است، به حق افراد برای بیان نظرات خود مربوط می‌شود. این دو حق، یعنی حق حریم خصوصی و آزادی بیان، به‌طور متقابل بر یکدیگر تأثیر می‌گذارند و در بسیاری از پرونده‌های قضایی به‌طور همزمان مورد بررسی قرار گرفته‌اند (Taslitz, 2002: 153-156).

دیوان‌عالی کشور در چندین پرونده مهم حق حریم خصوصی را به‌عنوان یک حق اساسی شناسایی کرده است. در پرونده «Griswold v. Connecticut» در سال ۱۹٦۵، دیوان‌عالی به‌طور ضمنی حق حریم خصوصی را در زمینه کنترل بر باروری شناسایی کرد و بر قوانین ایالتی که استفاده از وسایل پیشگیری از بارداری را ممنوع کرده بودند، تأکید داشت. دیوان اعلام کرد که چنین قوانینی به حریم خصوصی افراد تجاوز می‌کنند (Helscher, 1994: 38-41). در پرونده «Roe v. Wade» در سال ۱۹۷۳، حق زنان در تصمیم‌گیری درباره بارداری مطرح شد و دیوان‌عالی حق حریم خصوصی را در زمینه انتخاب‌های پزشکی و زندگی شخصی به رسمیت شناخت. دیوان در این تصمیم تأکید کرد که دولت نمی‌تواند به‌طور غیرمجاز در انتخاب‌های شخصی افراد دخالت کند (Annas, 1989: 1200).

در نظام حقوقی ایالات‌متحده قوانین متعددی در راستای حمایت از حریم خصوصی به تصویب رسیده‌اند که از مهم‌ترین آن‌ها می‌توان به دو قانون کلیدی اشاره کرد: قانون حفاظت از حریم خصوصی آنلاین کودکان[٤] مصوب ۱۹۹۸ به‌عنوان یک قانون خاص[٥] در حوزه حمایت از داده‌های شخصی افراد زیر ۱۳ سال تعهدات و الزامات قانونی متعددی را برای ارائه‌دهندگان

2. Penumbral Rights
3. Reasonable Expectation of Privacy
4. Children's Online Privacy Protection Act (COPPA)
5. Lex Specialis

خدمات آنلاین مقرر نموده است. این قانون با تأکید بر اصل «رضایت آگاهانه والدین»[6] مکانیسم‌های حمایتی ویژه‌ای را پیش‌بینی کرده است. همچنین اصل «شفافیت»[7] در جمع‌آوری و پردازش داده‌ها و «حق نظارت والدین»[8] از دیگر ارکان اساسی این قانون محسوب می‌شوند. به‌علاوه، قانون حریم خصوصی ۱۹۷٤[9] نیز به‌عنوان یکی از قوانین مادر در حوزه حفاظت از داده‌ها، چهارچوب حقوقی جامعی را برای مدیریت اطلاعات شخصی در بخش عمومی ارائه می‌دهد. این قانون با تکیه بر اصول «خودمختاری اطلاعاتی»[10] و «شفافیت اداری»[11] حقوق بنیادینی را برای شهروندان به رسمیت شناخته است که از آن جمله می‌توان به «حق دسترسی به اطلاعات»[12]، «حق تصحیح» [13] و «حق اعتراض»[14] اشاره کرد. این قوانین با پیش‌بینی ضمانت‌اجراهای مدنی و اداری و تعیین نهادهای ناظر مشخص، سازوکارهای اجرایی مؤثری را برای تضمین حقوق شهروندان در حوزه حفاظت از داده‌های شخصی فراهم آورده‌اند (Steeves & Mačėnaitė: 2022: 359-363).

علی‌رغم مبانی قانونی موجود، حریم خصوصی در ایالات‌متحده با چالش‌هایی مواجه است. نظارت دولتی به‌ویژه پس از تصویب قانون پاتریوت[15] که پس از حملات ۱۱ سپتامبر تصویب شد، به دولت اجازه می‌دهد که نظارت بیشتری بر فعالیت‌های شهروندان داشته باشد و این امر نگرانی‌هایی درباره نقض حریم خصوصی و آزادی‌های فردی ایجاد کرده است. همچنین در عصر دیجیتال، شرکت‌های فناوری اطلاعات به‌طور گسترده‌ای از داده‌های کاربران برای تحلیل و تبلیغات استفاده می‌کنند. با وجود قوانین موجود، هنوز مشکلاتی در زمینه شفافیت و حفاظت

6. Parental Informed Consent
7. Transparency
8. Parental Oversight Right
9. Privacy Act
10. Informational Self-determination
11. Administrative Transparency
12. Right of Access
13. Right of Rectification
14. Right to Object
15. Patriot Act

از داده‌ها وجود دارد (Sekhon, 2003: 119-125). مبانی قانونی حریم خصوصی در ایالات‌متحده شامل تفاسیر قضایی، قوانین فدرال و ایالتی است که به‌طور خاص به حفاظت از حقوق فردی و حریم خصوصی پرداخته‌اند، اما چالش‌های موجود در زمینه نظارت دولتی و سوءاستفاده از داده‌ها نشان‌دهنده نیاز به بهبود و تقویت این قوانین به‌منظور حفاظت مؤثرتر از حریم خصوصی شهروندان است.

۲-۱-۲) مبانی قانونی حریم خصوصی در اتحادیه اروپا

حریم خصوصی در اتحادیه اروپا به‌عنوان یک حق بنیادی و اساسی شناخته می‌شود که تحت تأثیر قوانین و مقررات متعدد قرار دارد. این حقوق به‌ویژه با توجه به تحولات فناوری و نیاز به حفاظت از داده‌های شخصی به‌طور مستمر موردتوجه قرار گرفته است. مقررات عمومی حفاظت از داده‌ها (GDPR) که در مه ۲۰۱۸ به‌طور رسمی اجرایی شد، یکی از مهم‌ترین و جامع‌ترین قوانین در زمینه حریم خصوصی و حفاظت از داده‌ها در اتحادیه اروپا است. این مقررات به‌طور خاص به حفاظت از حقوق فردی می‌پردازد و به افراد این حق را می‌دهد که بر اطلاعات شخصی خود کنترل داشته باشند. این شامل حق دسترسی به داده‌ها، حق اصلاح اطلاعات نادرست، حق حذف (حق فراموشی) و حق محدود کردن پردازش داده‌ها می‌شود. همچنین سازمان‌ها و شرکت‌ها ملزم به ارائه اطلاعات شفاف درباره نحوه جمع‌آوری و استفاده از داده‌های شخصی هستند. این امر شامل توضیحات درباره اهداف پردازش داده‌ها و مدت‌زمان نگهداری آن‌ها است. GDPR الزامات سخت‌گیرانه‌ای برای به‌دست آوردن رضایت افراد قبل از جمع‌آوری و پردازش داده‌های شخصی تعیین کرده است که این رضایت باید صریح، آگاهانه و قابل لغو باشد. کنوانسیون ۱۰۱ شورای اروپا که در سال ۱۹۸۱ به تصویب رسید اولین ابزار بین‌المللی در زمینه حفاظت از داده‌ها است. این کنوانسیون اصول اولیه را برای پردازش خودکار داده‌های شخصی تعیین می‌کند و به‌عنوان یک چهارچوب مرجع برای کشورهای عضو شورای اروپا عمل می‌نماید (Dove, 2018: 1014).

اتحادیه اروپا در موارد گوناگونی حفاظت از حریم خصوصی، زندگی خصوصی و حفاظت

از داده های شخصی را مورد شناسایی قرار داده است. در متون مختلف تأکید می‌شود که این حقوق باید در تمامی قوانین و مقررات اتحادیه اروپا موردتوجه قرار گیرد. علاوه‌براین، مقررات و قوانین کلی بسیاری از کشورهای عضو اتحادیه اروپا قوانین ملی خود را نیز برای حفاظت از حریم خصوصی و داده‌ها تصویب کرده‌اند (Bignami, 2007: 233-255). این قوانین ممکن است شامل مقررات خاص درباره حفظ حریم خصوصی در زمینه‌های مختلف مانند بهداشت، آموزش و رسانه‌ها باشد.

با وجود این، مبانی قانونی اتحادیه اروپا با چالش‌هایی در زمینه حفاظت از حریم خصوصی مواجه است. نگرانی‌هایی درباره نظارت دولتی و تبادل داده‌ها بین کشورهای مختلف وجود دارد که می‌تواند حریم خصوصی افراد را تهدید کند. همچنین پیشرفت‌های فناوری، به‌ویژه در زمینه هوش مصنوعی و داده‌های کلان نیاز به بازنگری و به‌روزرسانی قوانین را اجتناب‌ناپذیر می‌کند. مبانی قانونی حریم خصوصی در اتحادیه اروپا به‌طور جامع و سیستماتیک طراحی شده است تا حقوق فردی را در برابر تهدیدات و چالش‌های روزافزون حفاظت کند. با این حال، نیاز به به‌روزرسانی و تطبیق با تحولات فناوری و اجتماعی همچنان احساس می‌شود تا بتوان از حریم خصوصی افراد به‌طور مؤثر حمایت کرد.

۲-۲) مبانی قانونی حریم خصوصی در ایران

حریم خصوصی در ایران به‌عنوان یک حق انسانی شناخته می‌شود که در قوانین و مقررات مختلف به آن پرداخته شده است. هرچند تعریف و تبیین حریم خصوصی در نظام حقوقی ایران ممکن است به‌طور مستقیم و جامع مانند برخی دیگر از کشورها نباشد، اما مبانی قانونی و فقهی متعددی وجود دارد که به حفاظت از این حق توجه کرده‌اند. قانون اساسی جمهوری اسلامی ایران در چندین ماده به حریم خصوصی اشاره کرده است؛ به‌ویژه اصل ۲۵ این قانون به صراحت اعلام می‌کند که: «استراق‌سمع و هرگونه تجسس ممنوع است، مگر به موجب قانون». این اصل به‌عنوان یک اصل اساسی در حمایت از حریم خصوصی افراد در برابر مداخلات غیرمجاز دولت و نهادهای عمومی عمل می‌کند (واعظی و علی‌پور، ۱۳۸۹: ۱۳۸).

در قوانین جزایی ایران نیز به حفاظت از حریم خصوصی پرداخته شده است. به‌عنوان مثال، قانون مجازات اسلامی در برخی مواد به مسائل مرتبط با حریم خصوصی اشاره کرده و مجازات‌هایی برای نقض این حق در نظر گرفته است. افشای اطلاعات خصوصی و خانوادگی افراد بدون رضایت آن‌ها ممکن است تحت عناوین مختلف جرم محسوب شود (آخوندی، ۱۳۷۹: ۱۷۰؛ منصور، ۱۳۸۷: ۱٥٦؛ طالع خرسند، ۱۳۸٥: ۱۸٦؛ شکری و سیروس، ۱۳۸٥: ٦٤). همچنین قانون حمایت از حقوق مصرف‌کنندگان به حفاظت از اطلاعات شخصی مصرف‌کنندگان و جلوگیری از سوءاستفاده از این اطلاعات پرداخته است.

با گسترش فناوری‌های نوین و اینترنت، نیاز به تدوین قوانین جدید برای حفاظت از حریم خصوصی در فضای مجازی احساس شده است. به‌عنوان نمونه، قانون جرایم رایانه‌ای به‌منظور جلوگیری از تهدیدات سایبری و حفاظت از اطلاعات شخصی در بستر دیجیتال تصویب شده است و شامل مواردی مانند نفوذ به سیستم‌های اطلاعاتی و افشای اطلاعات محرمانه می‌شود (لاریجانی و هاشمی شاهرودی، ۱۳۸۸: ٥). همچنین قانون حفاظت از داده‌های شخصی در حال حاضر در مرحله تدوین و بررسی است و هدف آن ایجاد چهارچوبی برای حفاظت از داده‌های شخصی افراد در فضای مجازی و جلوگیری از سوءاستفاده از این داده‌ها است.[۱٦]

در نظام حقوقی ایران اصول فقهی نیز نقش مهمی در تعریف حریم خصوصی ایفا می‌کنند. احترام به زندگی خصوصی افراد و جلوگیری از افشای اسرار آن‌ها از جمله اصول اخلاقی و فقهی شناخته‌شده است که در متون دینی و فقهی تأکید شده و در بسیاری از موارد مبنای قوانین و مقررات قرار می‌گیرد (شهباز قهفرخی، ۱۳۹۲: ٦٤). با وجود مبانی قانونی موجود، حریم خصوصی در ایران با چالش‌هایی مواجه است؛ نظارت‌های دولتی به‌ویژه در زمینه‌های امنیتی ممکن است به نقض حریم خصوصی منجر شود. همچنین کمبود قوانین جامع و مشخص در زمینه حفاظت از حریم خصوصی و داده‌های شخصی احساس می‌شود. مبانی قانونی حریم خصوصی در ایران شامل قانون اساسی، قوانین مدنی و جزایی و اصول فقهی است که

---

۱٦. به نقل از سایت اندیشکده شفافیت برای ایران: https://tp4.ir

به‌طورکلی به حمایت از حقوق فردی و حفاظت از حریم خصوصی پرداخته‌اند. با این حال، چالش‌های موجود و نیاز به تدوین قوانین جامع‌تر، ضرورت توجه به این موضوع را در نظام حقوقی ایران نمایان می‌سازد.

۳. چالش‌های قانونی حفاظت از حریم خصوصی در فضای مجازی

چالش‌های قانونی حفاظت از حریم خصوصی در فضای مجازی شامل نقض حریم خصوصی، حملات سایبری، نظارت‌های دولتی و دسترسی غیرمجاز به داده‌های کاربران است که ممکن است به نقض حقوق فردی منجر شود. همچنین نبود قوانین جامع و شفاف در زمینه حفاظت از داده‌ها، به‌ویژه در برابر سوءاستفاده‌های تجاری و سایبری، یکی از مشکلات اصلی به شمار می‌آید. این مسائل در کنار پیشرفت سریع فناوری نیاز به بازنگری و تقویت چهارچوب‌های قانونی را اجتناب‌ناپذیر می‌کند.

۳-۱) نقض حریم خصوصی

داده‌کاوی و نظارت به‌عنوان دو ابزار کلیدی در عصر دیجیتال، به‌طور فزاینده‌ای در زندگی روزمره افراد و فعالیت‌های اقتصادی مدرن بشر مورد استفاده قرار می‌گیرند. این فرآیندها می‌توانند به جمع‌آوری و تحلیل حجم وسیعی از داده‌های شخصی منجر شوند که این امر چالش‌ها و خطرات متعددی را به همراه دارد. جمع‌آوری گسترده داده‌ها به‌ویژه بدون رضایت صریح افراد، می‌تواند به نقض حریم خصوصی منجر شود. شرکت‌ها و دولت‌ها معمولاً اطلاعاتی نظیر رفتار آنلاین، موقعیت جغرافیایی و حتی اطلاعات مالی افراد را جمع‌آوری می‌کنند. این عمل می‌تواند احساس عدم امنیت و خودسانسوری در کاربران ایجاد کند. داده‌های جمع‌آوری‌شده ممکن است به‌راحتی در معرض سوءاستفاده قرار گیرند. هکرها می‌توانند به اطلاعات حساس دسترسی پیدا کنند و از آن‌ها برای کلاهبرداری، هویت‌دزدی و سایر فعالیت‌های مجرمانه استفاده کنند. همچنین شرکت‌ها ممکن است از این داده‌ها برای اهداف تجاری غیرمجاز یا تحمیل تبلیغات هدفمند بهره‌برداری کنند (Rubinstein & Schwartz, 2008: 261).

داده‌کاوی الگوریتمی، به‌ویژه در قالب تحلیل‌های پیش‌بینانه مبتنی بر داده‌های تاریخی، واجد ظرفیت بازتولید سوگیری‌های ساختاری و تولید تبعیض سیستماتیک است. این فرآیند می‌تواند به شناسایی نادرست افراد و گروه‌ها هدف‌گیری ناعادلانه و تحدید حقوق بنیادین شهروندان منجر شود. هم‌زمان توسعه نظارت دیجیتال دولتی بر فعالیت‌های آنلاین به‌ویژه در نظام‌های سیاسی اقتدارگرا زمینه‌ساز گذار از امنیت‌محوری به کنترل اجتماعی داده‌محور و محدودسازی آزادی‌های فردی می‌گردد. فقدان شفافیت نهادی در گردآوری و بهره‌برداری از داده‌ها نیز این روند را تشدید کرده و نظام حکمرانی داده را با بحران مشروعیت، پاسخ‌گویی و حمایت حقوقی از حریم خصوصی مواجه می‌سازد (Rubinstein & Schwartz, 2008: 270-285). این فقدان شفافیت می‌تواند موجب بی‌اعتمادی عمومی و نگرانی‌های جدی درباره حریم خصوصی شود. به‌طورکلی داده‌کاوی و نظارت با وجود مزایای بالقوه‌ای که می‌توانند داشته باشند، به چالش‌های جدی در زمینه حفاظت از حریم خصوصی و حقوق فردی منجر می‌شوند. بنابراین ایجاد چهارچوب‌های قانونی و اخلاقی مناسب برای مدیریت این فرآیندها، به‌ویژه در عصر دیجیتال، از اهمیت ویژه‌ای برخوردار است.

۳-۲) حملات سایبری

در عصر دیجیتال تهدیدات امنیتی و حملات سایبری به یکی از بزرگ‌ترین چالش‌ها برای کاربران و سازمآن‌ها تبدیل شده است. این حملات نه‌تنها به اطلاعات حساسی که کاربران به اشتراک می‌گذارند آسیب می‌زنند، بلکه می‌توانند حریم خصوصی آن‌ها را به‌طور جدی تهدید کنند (Sapiński, 2023: 55). حملات فیشینگ که یکی از رایج‌ترین انواع حملات سایبری است، در آن مهاجمان تلاش می‌کنند کاربران را به ارائه اطلاعات شخصی خود مانند نام کاربری و رمز عبور ترغیب کنند. این حملات معمولاً از طریق ایمیل یا پیام‌های متنی انجام می‌شوند و می‌توانند به سرقت هویت و دسترسی غیرمجاز به حساب‌های کاربری منجر شوند (Alabdan, 2020: 1).

بدافزار در معنای تحلیلی، نرم‌افزاری است که از طریق ایجاد تفاوت ساختاری میان رفتار واقعی و رفتار مطلوب سیستم‌های نرم‌افزاری، موجب نادرستی عملکردی سیستم و نقض

الزامات درستی آن می‌شود. در این چهارچوب ماهیت مخرب بدافزار نه صرفاً در مصادیق فنی آن، بلکه در نقش آن به‌عنوان عامل تولید اختلال در صحت، امنیت و یکپارچگی اطلاعاتی سیستم‌ها و داده‌های کاربران قابل تبیین است (Kramer & Bradfield, 2010: 105). حملات انکار سرویس توزیع‌شده[17] با ایجاد ترافیک انبوه و اشباع منابع شبکه‌ای موجب اختلال در دسترسی‌پذیری خدمات آنلاین و از کار افتادن سامانه‌ها می‌شوند. هرچند این حملات مستقیماً متوجه حریم خصوصی کاربران نیستند، اما با مختل‌سازی دسترسی به اطلاعات و خدمات حیاتی، آثار اجتماعی و حقوقی قابل‌توجهی بر جای می‌گذارند. از این رو DDoS صرفاً یک تهدید فنی نیست، بلکه شکلی از اخلال ساختاری در نظم خدمات دیجیتال محسوب می‌شود (Kaur et al., 2017: 301).

حملات سایبری تأثیرات عمیقی بر حریم خصوصی کاربران دارند. با دسترسی غیرمجاز به اطلاعات شخصی مهاجمان می‌توانند هویت کاربران را سرقت کنند و از آن برای انجام فعالیت‌های مجرمانه استفاده کنند که این امر می‌تواند به آسیب‌های مالی و حقوقی برای قربانیان منجر شود. همچنین حملات سایبری می‌تواند به افشای اطلاعات خصوصی مانند پیام‌های شخصی، عکس‌ها و اطلاعات مالی منجر شود که نه‌تنها حریم خصوصی کاربران را نقض می‌کند، بلکه می‌تواند به تبعات اجتماعی و روانی جدی نیز منجر شود. این حملات همچنین می‌توانند به کاهش اعتماد کاربران به خدمات آنلاین و سازمان‌ها منجر شوند و به خسارات مالی و کاهش استفاده از خدمات منتهی شوند. پس از وقوع حملات سایبری، سازمان‌ها ممکن است تحت فشار قانونی قرار گیرند و ملزم به رعایت استانداردهای امنیتی بیشتری شوند. این امر می‌تواند هزینه‌های اضافی برای سازمان‌ها به همراه داشته باشد و بر نحوه مدیریت داده‌های کاربران تأثیر بگذارد. به‌طورکلی تهدیدات امنیتی و حملات سایبری به‌طور جدی حریم خصوصی کاربران را تهدید می‌کنند. با افزایش وابستگی به فناوری و فضای آنلاین نیاز به راهکارهای امنیتی مؤثر و آگاهی کاربران از خطرات موجود بیش از پیش احساس می‌شود. ایجاد سیاست‌ها و قوانین مناسب برای حفاظت از داده‌ها و حریم خصوصی کاربران می‌تواند از پیامدهای منفی حملات

17. DDoS

سایبری جلوگیری شود.

۳-۳) قوانین و محدودیت‌ها

در عصر دیجیتال حریم خصوصی کاربران به‌طور فزاینده‌ای در معرض تهدیدات و نقض‌های مختلف قرار دارد. علی‌رغم وجود قوانین و مقررات، ناکارآمدی‌های حقوقی و چالش‌های قانونی مانع از پیگیری مؤثر این نقض‌ها می‌شوند. یکی از بزرگ‌ترین ناکارآمدی‌ها در این حوزه عدم وجود چهارچوب‌های قانونی جامع و یکپارچه است. بسیاری از قوانین موجود به‌طور خاص به جنبه‌های مختلف حریم خصوصی در فضای مجازی نمی‌پردازند و این پراکندگی سبب می‌شود که افراد نتوانند به‌راحتی از حقوق خود دفاع کنند. همچنین بسیاری از قوانین قدیمی و ناکارآمد هستند و نمی‌توانند با چالش‌های جدیدی که فناوری‌های نوین به وجود می‌آورند سازگار شوند.

نظام حقوقی حفاظت از حریم خصوصی با نارسایی‌های ساختاری عمیقی مواجه است که مهم‌ترین آن ناتوانی در شناسایی و جبران مؤثر «آسیب‌های ناملموس داده‌محور» است. پیچیدگی و پراکندگی مقررات، ضعف چهارچوب‌های جبران خسارت معنوی، ناکارآمدی نظام دادرسی در تطبیق مفاهیم کلاسیک آسیب با واقعیت‌های دیجیتال و فقدان تخصص نهادی در رسیدگی به دعاوی داده‌محور موجب شده است بخش گسترده‌ای از نقض‌های حریم خصوصی خارج از چرخه‌ی حمایت قضایی مؤثر باقی بمانند. هم‌زمان ضعف ساختارهای نظارتی، عدم استقلال نهادی، عدم توازن قدرت در روابط کاربران و شرکت‌های بزرگ فناوری و ناکارآمدی نظام آگاهی‌بخشی حقوقی به شکل‌گیری یک نظام «حمایت صوری» از حریم خصوصی انجامیده است که فاقد کارآمدی اجرایی واقعی در تضمین حقوق بنیادین شهروندان است (Citron & Solove, 2022: 798).

برای برطرف‌سازی نارسایی‌های نظام حقوقی لازم است بازنگری بنیادین در روش‌های قانون‌گذاری و تقویت نهادها و سازوکارهای حمایتی صورت پذیرد. در طراحی و اجرای این مکانیسم‌ها باید اصول حاکمیت قانون و رویکرد عدالت ترمیمی به‌روشنی لحاظ شوند. اصلاحات باید جامع و چندبعدی باشد و هم‌زمان به جنبه‌های ماهوی حقوق (حقوق دسترسی، اصلاح و

عبدالسعید شجاعی و همکار ـــــــ

چندوجهی است. این رویکرد شامل تدوین و اجرای برنامه‌های جامع ارتقای سواد دیجیتال شهروندان، راه‌اندازی سامانه‌های هشدار نقض حریم خصوصی و ایجاد زیرساخت‌های حقوقی – نظارتی است. نهادهای تنظیم‌گر مستقل[۱۸] با بهره‌گیری از ابزارهای نظارتی همچون ممیزی‌های دوره‌ای[۱۹]، پایش مستمر[۲۰] و سازوکارهای پاسخگویی[۲۱] نقش محوری در تضمین رعایت اصول حفاظت از داده‌ها[۲۲] ایفا می‌کنند. این نهادها با استقرار سیستم‌های جامع مدیریت داده[۲۳]، پروتکل‌های امنیتی[۲٤] و چهارچوب‌های ارزیابی ریسک[۲۵] بر فرآیند پردازش داده‌های شخصی نظارت می‌کنند. همچنین صدور گواهینامه‌های انطباق[۲٦] و اعمال ضمانت‌های اجرایی[۲۷] در صورت نقض مقررات از دیگر کارویژه‌های این نهادها است. استقلال ساختاری و عملیاتی[۲۸] نهادها و مصونیت از فشارهای سیاسی – اقتصادی، پیش‌شرط اساسی برای اجرای مؤثر وظایف نظارتی و حمایتی آن‌ها است. این امر از طریق تعریف سازوکارهای شفاف پاسخگویی، تأمین منابع مالی مستقل و تضمین استقلال تصمیم‌گیری محقق می‌شود (Holt & Malčić, 2015: 155-178).

تحلیل جامع اثربخشی مکانیسم‌های حاکمیتی در حفاظت از حریم خصوصی مستلزم رویکردی یکپارچه و چندوجهی است. در این راستا، چهار محور اساسی شامل شفافیت و دسترس‌پذیری، پاسخگویی و کارآمدی نظارتی، جبران خسارت و حمایت‌های حقوقی و اعتمادسازی نهادی باید به‌صورت هماهنگ و منسجم موردتوجه قرار گیرند. شفافیت و

18. Regulatory Bodies
19. Periodic Audits
20. Continuous Monitoring
21. Accountability Mechanisms
22. Data Protection Principles
23. Data Governance Systems
24. Security Protocols
25. Risk Assessment Frameworks
26. Compliance Certificates
27. Enforcement Measures
28. Structural and Operational Independence

دسترس‌پذیری به‌عنوان پایه اصلی این ساختار از طریق سیستم‌های مدیریت اطلاعات عمومی و پروتکل‌های شفافیت فرآیندی، تحقق می‌یابد؛ این امر با تضمین دسترسی شهروندان به مکانیسم‌های حقوقی تکمیل می‌شود. همزمان، پاسخگویی و کارآمدی نظارتی از طریق سیستم‌های پایش انطباق و چهارچوب‌های ارزیابی ریسک عملیاتی می‌شود و با مکانیسم‌های اعمال قانون تقویت می‌گردد. در بعد حمایتی، جبران خسارت و حمایت‌های حقوقی با تدوین پروتکل‌های جبران خسارت و ایجاد سازوکارهای حمایت از قربانیان عملیاتی می‌شود؛ این فرآیند با سیستم‌های ردیابی و پیگیری نقض‌ها تکمیل می‌گردد. نهایتاً اعتمادسازی نهادی از طریق سیستم‌های شفافیت عملکرد مکانیسم‌های ارتباط با ذی‌نفعان و برنامه‌های ارتقای آگاهی عمومی محقق می‌شود (Aho & Duffield, 2020: 178-212). موفقیت این ساختار یکپارچه، مستلزم هماهنگی بین‌سازمانی قوی و اتخاذ رویکردهای مبتنی بر ریسک در تمامی سطوح است. این رویکرد جامع، چهارچوبی منسجم برای ارزیابی و بهبود مستمر عملکرد نهادهای نظارتی و حاکمیتی در حوزه حفاظت از حریم خصوصی فراهم می‌آورد. حفاظت از حریم خصوصی یک مسئولیت چندجانبه است که نیازمند همکاری دولت‌ها و نهادهای نظارتی است. این نهادها باید با تدوین قوانین جامع، نظارت مؤثر و آموزش عمومی به بهبود وضعیت حریم خصوصی کمک کنند. ارزیابی عملکرد آن‌ها نیز باید به‌طور مداوم انجام شود تا اطمینان حاصل شود که حقوق افراد به‌طور مؤثر حمایت می‌شود و نقض‌های حریم خصوصی به سرعت شناسایی و رسیدگی می‌شوند.

۴. چهارچوب‌های قانونی و سیاست‌گذاری

۴-۱) ظرفیت قوانین داخلی

حفاظت از حریم خصوصی یکی از مسائل مهم و حیاتی در حقوق بشر و حقوق شهروندی است. در ایران مجموعه‌ای از قوانین و مقررات وجود دارد که به‌نحوی به این موضوع مرتبط می‌شوند. قانون اساسی جمهوری اسلامی ایران کلیاتی را در خصوص محافظت از حریم خصوصی در اصل بیست‌وسوم گفته و حریم خصوصی افراد را مصون از تعرض دانسته و این وظیفه قوانین

عادی و خاص است که به جزئیات امر پرداخته و در محدود کردن عوامل ناقض حریم خصوصی اقدام نمایند. برای اینکه گرایش سیاسی و عقاید شهروندان از دسترس دستبرد احزاب سیاسی مصون بماند، باید قوانین کشورها به حمایت از حریم خصوصی و سیاسی شهروندان مبادرت ورزند. اغلب کشورها در قانون اساسی خود و دیگر قوانین مصونیت افکار سیاسی افراد را نسبت به هرگونه مداخله افراد یا نهادهای عمومی به رسمیت شناخته‌اند، اما قانون اساسی ایران به‌طور خاص و در قالب اصلی اختصاصی به این مفهوم نپرداخته و آزادی عقیده را به‌صورت کلی مورد حمایت و مصون از تعرض و مؤاخذه دانسته است.

علاوه‌براین، قانون اساسی ایران در اصل سی‌ونهم مصون ماندن حرمت و حیثیت اشخاصی که بازداشت و یا زندانی شده‌اند را مورد تأکید قرار داده و اشاره می‌کند هتک حرمت و حیثیت کسی که به حکم قانون دستگیر، بازداشت، زندانی یا تبعید شده به هر صورت که باشد ممنوع و موجب مجازات است. در واقع، حیثیت و حرمت افراد مصون از تجاوز است، هرچند که آن افراد به‌موجب قانون مجرم شناخته شده‌اند یا در زندان و یا در تبعید به سر می‌برند. مکاتبات و ارتباطات این افراد با وکیلشان و با خانواده و افراد دیگر از جمله حقوق قانونی و حریم خصوصی آن‌ها محسوب شده و مصون از دخالت است و تنها تحت شرایط خاصی کنترل می‌گردد. علی‌الاصول قواعد و قوانین باید در مسیری باشد که حیثیت و حرمت افراد جامعه را حتی در بحرانی‌ترین شرایط، از جمله بازداشت و دستگیری به سبب ارتکاب جرم، حفظ نماید (غرایاق زندی و دیگران، ۱۳۹٤: ۱۵۰-۱۵۱).

متأسفانه در حفاظت از اطلاعات شخصی مصرف‌کنندگان، در نظام حقوقی ایران قانون خاصی تاکنون به تصویب نرسیده است و لازم است با توجه به رشد روزافزون تکنولوژی‌های مدرن در زندگی بشر چنین قوانینی به تصویب مراجع قانونی برسد. با این حال، بر اساس ماده ۵۸ قانون تجارت الکترونیکی، کسب‌وکار مجازی قاعدتاً و به‌صورت پیش‌فرض نمی‌تواند داده‌های مربوط به مشتریان را ذخیره، پردازش یا توزیع کند، مگر اینکه از مصرف‌کننده یا کاربر صراحتاً اجازه بگیرد. لازم است شرکت‌ها و مؤسسات ملزم شوند که اطلاعات شخصی مشتریان را در حد ضرورت جمع‌آوری کرده و از افشای آن جلوگیری کنند. قانون جرایم رایانه‌ای به

تهدیدات سایبری و نقض حریم خصوصی در فضای مجازی پرداخته و مجازات‌هایی برای افشای اطلاعات شخصی بدون اجازه صاحب آن در نظر گرفته است.[۲۹] این قانون به‌ویژه در دنیای دیجیتال و با گسترش استفاده از اینترنت اهمیت ویژه‌ای پیدا کرده است.

علاوه‌براین، قانون ثبت احوال به حفاظت از اطلاعات هویتی افراد پرداخته و ثبت و نگهداری اطلاعات شخصی را تحت نظارت قرار می‌دهد. این قانون به‌طور خاص بر روی اطلاعات شخصی و هویتی تأکید دارد و هرگونه افشای غیرمجاز آن را ممنوع می‌کند. با این حال، چالش‌هایی نیز در زمینه حفاظت از حریم خصوصی وجود دارد. عدم وجود تعریف دقیق از حریم خصوصی در بسیاری از قوانین می‌تواند منجر به تفسیرهای مختلف شود. همچنین در بسیاری از موارد، نهادهای نظارتی برای اجرای قوانین، به‌ویژه در زمینه فضای مجازی، وجود ندارد یا کارآیی لازم را ندارند. همچنین، تناقضات قانونی بین قوانین مختلف ممکن است موجب سردرگمی در اجرای قوانین و حفاظت از حریم خصوصی شود. حفاظت از حریم خصوصی در ایران تحت‌تأثیر قوانین متعدد قرار دارد که هر یک به نوعی به این موضوع پرداخته‌اند. با وجود این، به‌منظور

---

۲۹. ماده ۱۶: هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به‌نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نودویک روز تا دوسال یا جزای نقدی از پنج میلیون ریال (۵.۰۰۰.۰۰۰) تا چهل میلیون ریال (۴۰.۰۰۰.۰۰۰) یا هر دو مجازات محکوم خواهد شد. (تبصره: چنانچه تغییر یا تحریف به‌صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.)

– ماده ۱۷: هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او، جز در موارد قانونی، منتشر کند یا در دسترس دیگران قرار دهد، به‌نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نودویک روز تا دوسال یا جزای نقدی از پنج میلیون ریال (۵.۰۰۰.۰۰۰) تا چهل میلیون ریال (۴۰.۰۰۰.۰۰۰) یا هر دو مجازات محکوم خواهد شد.

– ماده ۱۸: هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی، به‌وسیله سامانه رایانه‌ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را برخلاف حقیقت، رأساً یا به‌عنوان نقل‌قول، به شخص حقیقی یا حقوقی به‌طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یادشده به‌نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت (در صورت امکان)، به حبس از نودویک روز تا دوسال یا جزای نقدی از پنج میلیون ریال (۵.۰۰۰.۰۰۰) تا چهل میلیون ریال (۴۰.۰۰۰.۰۰۰) یا هر دو مجازات محکوم خواهد شد.

بهبود شرایط و افزایش اثربخشی قوانین، نیاز به بازنگری در قوانین، تعریف دقیق‌تر حریم خصوصی و تقویت نهادهای نظارتی احساس می‌شود. این اقدامات می‌تواند به تقویت حقوق شهروندی و حفاظت از حریم خصوصی در جامعه کمک کند.

۴-۲) معاهدات بین‌المللی

معاهدات بین‌المللی، به‌ویژه در زمینه حفاظت از داده‌ها و حریم خصوصی، تأثیر عمیقی بر قوانین داخلی و سیاست‌های ملی کشورهای مختلف از جمله ایران، دارند. یکی از برجسته‌ترین این معاهدات، مقررات عمومی حفاظت از داده‌ها (GDPR) اتحادیه اروپا است که به‌عنوان نمونه‌ای موفق در حفاظت از حریم خصوصی و داده‌های شخصی شناخته می‌شود. این معاهدات ممکن است کشورهای عضو را ملزم به بازنگری و اصلاح قوانین داخلی خود کنند؛ استانداردهای سخت‌گیرانه‌ای برای جمع‌آوری، پردازش و نگهداری داده‌های شخصی تعیین می‌کند و این استانداردها می‌توانند به کشورها فشار وارد کنند تا قوانین خود را با این الزامات همسو کنند. همچنین معاهدات بین‌المللی می‌توانند به ایجاد یک چهارچوب حقوقی واحد کمک کنند. کشورهایی که به GDPR پای‌بند هستند باید قوانین مشابهی را در زمینه حفاظت از داده‌های شخصی تدوین کنند تا از بروز تضادهای حقوقی در تجارت و تعاملات بین‌المللی جلوگیری شود (Wagner & Benecke, 2016: 353).

علاوه‌براین، معاهدات بین‌المللی می‌توانند آگاهی عمومی را در زمینه حفاظت از حریم خصوصی افزایش دهند. با پیروی از استانداردهای بین‌المللی دولت‌ها ممکن است بیشتر به نیازهای شهروندان در زمینه حفاظت از داده‌ها توجه کنند و به‌تدریج فرهنگ حقوق بشر و حفاظت از حریم خصوصی را در جامعه رواج دهند. همچنین کشورهای غیرعضو می‌توانند تحت فشار نهادهای بین‌المللی و جامعه مدنی قرار گیرند تا به اصول بین‌المللی احترام بگذارند که این فشارها می‌تواند موجب تغییرات مثبت در سیاست‌های داخلی و قوانین کشورها شود. با این حال، چالش‌هایی نیز در زمینه انطباق با این استانداردها وجود دارد. کشورهای مختلف ممکن است با دشواری‌هایی در انطباق با ارزش‌ها و اعتقادات فرهنگی مواجه شوند که می‌تواند بر نحوه

برداشت و اجرای قوانین مربوط به حریم خصوصی تأثیر بگذارد. همچنین حتی اگر قوانین داخلی بر اساس استانداردهای بین‌المللی اصلاح شوند، اجرای مؤثر آن‌ها نیازمند نهادهای نظارتی قوی و منابع کافی است. در بسیاری از کشورها نهادهای نظارتی ممکن است فاقد قدرت یا منابع لازم برای اجرای قوانین جدید باشند. در ایران با توجه به تحولات جهانی و تأثیرات آن جهت حفاظت از داده‌ها، برخی نهادها و سازمان‌ها به سمت پیاده‌سازی استانداردهای بین‌المللی در زمینه حفاظت از داده‌ها حرکت کرده‌اند. این تحولات می‌تواند به اصلاحات قانونی در آینده نزدیک منجر شود و به ایجاد بستری مناسب برای تجارت بین‌المللی و جذب سرمایه‌گذاری خارجی کمک کند.

به‌طورکلی، معاهدات منطقه‌ای و بین‌المللی تأثیر قابل‌توجهی بر قوانین داخلی و سیاست‌های ملی کشورهای مختلف دارند. این تأثیرات می‌توانند به اصلاحات قانونی، افزایش حساسیت به حریم خصوصی و فشارهای بین‌المللی منجر شوند. با این حال، چالش‌های فرهنگی، اجتماعی و اجرایی نیز وجود دارد که باید موردتوجه قرار گیرند. نتیجه اینکه انطباق با استانداردهای بین‌المللی می‌تواند به تقویت حقوق بشر و حفاظت از حریم خصوصی در سطح جهانی و ملی کمک کند.

۵. راهکارها و استراتژی‌ها برای حفاظت از حریم خصوصی

۵-۱) آموزش و آگاهی‌رسانی

حفاظت از حریم خصوصی در دنیای دیجیتال نه‌تنها به استفاده از فناوری‌های حفاظتی بستگی دارد، بلکه به آگاهی و آموزش کاربران نیز نیاز دارد. بسیاری از کاربران از حقوق خود و روش‌های حفاظت از حریم خصوصی به‌طور کامل مطلع نیستند و این موضوع آن‌ها را در معرض خطرات سایبری و نقض حریم خصوصی قرار می‌دهد. بنابراین برنامه‌های آموزشی و آگاهی‌رسانی در این زمینه از اهمیت بالایی برخوردار هستند. برنامه‌های آموزشی باید شامل افزایش آگاهی درباره حقوق حریم خصوصی کاربران باشد. آگاهی از این حقوق می‌تواند به کاربران کمک کند تا از حقوق خود در برابر نقض‌های احتمالی دفاع کنند. این برنامه‌ها باید اطلاعاتی درباره قوانین و مقررات مربوط به حریم خصوصی مانند GDPR و دیگر معاهدات

بین‌المللی و ملی ارائه دهند. با این آگاهی کاربران می‌توانند بفهمند چه داده‌هایی جمع‌آوری می‌شود و چگونه می‌توانند بر روی آن‌ها کنترل داشته باشند.

علاوه‌براین، آموزش روش‌های عملی برای حفاظت از حریم خصوصی نیز ضروری است. این شامل آموزش نحوه استفاده از ابزارهای حفاظتی، نرم‌افزارهای مدیریت گذرواژه و تکنیک‌های رمزگذاری می‌شود. کاربران همچنین باید با روش‌های جلوگیری از پیگیری آنلاین و به‌کارگیری تنظیمات حریم خصوصی در شبکه‌های اجتماعی آشنا شوند. برای اجرای برنامه‌های آموزشی، برگزاری کارگاه‌ها و سمینارها می‌تواند یک روش مؤثر باشد. این جلسات می‌توانند به‌صورت حضوری یا آنلاین برگزار شوند و شامل مباحثی از قبیل بهترین شیوه‌ها در حفظ حریم خصوصی، تکنیک‌های امنیتی و جدیدترین تهدیدات سایبری باشند. تولید محتوای آموزشی آنلاین، از جمله ویدئوها، مقالات و وبینارها نیز می‌تواند به‌عنوان یک منبع مفید در دسترس کاربران قرار گیرد و به‌راحتی به اشتراک گذاشته شود.

کمپین‌های اجتماعی نیز می‌توانند برای برگزاری آگاهی‌رسانی به کار روند و به جذب توجه و افزایش آگاهی در میان کاربران کمک کنند. این کمپین‌ها می‌توانند شامل اطلاعات کوتاه، نکات امنیتی و داستان‌های موفقیت افرادی باشند که با استفاده از تکنیک‌های حفاظت از حریم خصوصی از نقض‌های امنیتی جلوگیری کرده‌اند. آموزش و آگاهی‌رسانی در زمینه حفاظت از حریم خصوصی نقش مهمی در توانمندسازی کاربران دارد. با افزایش آگاهی درباره حقوق و روش‌های حفاظت از حریم خصوصی، کاربران می‌توانند به‌طور مؤثرتری از اطلاعات شخصی خود محافظت کنند و در برابر تهدیدات سایبری ایمن‌تر باشند. بنابراین، نیاز به برنامه‌های آموزشی مستمر و مؤثر در این حوزه احساس می‌شود که می‌تواند به تقویت فرهنگ احترام به حریم خصوصی در جامعه کمک کند.

۵-۲) نقش نهادهای مدنی

سازمان‌های مردم‌نهاد به‌عنوان اشخاص حقوقی مستقل مطابق با ماده ٥٨٤ قانون تجارت و اصل ٢٦ قانون اساسی، در چهارچوب حقوق عمومی به فعالیت می‌پردازند. این نهادها با استناد

به کنوانسیون‌های بین‌المللی حقوق بشر و اسناد حقوقی مرتبط با حریم خصوصی از جمله ماده ۱۲ اعلامیه جهانی حقوق بشر و ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی به صیانت از حقوق دیجیتال شهروندان مبادرت می‌ورزند. این سازمان‌ها با بهره‌گیری از ظرفیت‌های حقوقی موجود در قوانین موضوعه، به‌ویژه قانون حمایت از حقوق کاربران در فضای مجازی و قانون تجارت الکترونیک، اقدام به توانمندسازی حقوقی کاربران می‌نمایند. این مهم از طریق تبیین دکترین حقوقی حریم خصوصی و ارائه راهکارهای قانونی برای مقابله با نقض حریم خصوصی صورت می‌پذیرد (Mohamed, 2012: 97-106).

در زمینه آموزش تخصصی، نهادها با تمرکز بر مبانی حقوقی حفاظت از داده‌های شخصی و اصول حاکم بر پردازش داده‌ها مطابق با مقررات عمومی حفاظت از داده‌ها (GDPR)، اقدام به تشریح این اصول و آموزش مکانیزم‌های حقوقی مقابله با نقض حریم خصوصی می‌نمایند. این آموزش‌ها شامل دادخواهی در مراجع قضایی و شبه‌قضایی نیز می‌شود. به‌عنوان مثال، در یک مطالعه به بررسی چالش‌های سازمان‌ها در تطابق با GDPR پرداخته شده و راهکارهایی برای درک و عملیاتی کردن الزامات قانونی ارائه شده است. .

سازمان‌ها نقش مهمی در همگرایی نظام حقوقی داخلی با استانداردهای بین‌المللی حفاظت از داده‌ها ایفا می‌کنند. این سازمان‌ها با مشارکت در تدوین پروتکل‌های بین‌المللی و ارائه گزارش‌های تخصصی به نهادهای بین‌المللی، به ارتقای سطح حمایت‌های حقوقی از حریم خصوصی دیجیتال کمک می‌کنند. به‌عنوان مثال، برخی از سازمان‌ها به ایجاد و تقویت قوانین بین‌المللی در زمینه حفاظت از داده‌ها کمک می‌کنند و به این ترتیب به همگرایی نظام‌های حقوقی داخلی با این استانداردها می‌پردازند (Daugirdas, 2020: 201-233).

نهادها با تلفیق دانش حقوقی و فناوری راهکارهای عملی برای حفاظت از حریم خصوصی را در چهارچوب قوانین موضوعه ارائه می‌دهند. این راهکارها شامل استفاده از ابزارهای رمزنگاری قانونی، سرویس‌های VPN مجاز و سیستم‌های مدیریت هویت دیجیتال است که همگی در انطباق با الزامات قانونی طراحی و اجرا می‌شوند. به‌عنوان مثال، استفاده از VPN به‌عنوان ابزاری برای ایجاد اتصالات امن و حفاظت از داده‌ها در شبکه‌های عمومی به‌طور

گسترده‌ای در سازمان‌ها مورداستفاده قرار می‌گیرد. همچنین، ابزارهای رمزنگاری به‌عنوان یک روش مؤثر برای حفاظت از اطلاعات شخصی و جلوگیری از دسترسی غیرمجاز به داده‌ها شناخته شده‌اند. این رویکردها به نهادها این امکان را می‌دهد که با ارائه راهکارهای فنی و حقوقی، به حفاظت از حریم خصوصی کاربران در دنیای دیجیتال بپردازند (Yuejia, 2024: 12).

می‌توان اذعان داشت که نقش این نهادها در توسعه حقوق حریم خصوصی دیجیتال و ارتقای سواد حقوقی کاربران، امری انکارناپذیر است. این سازمان‌ها با ایجاد پیوند میان نظام حقوقی و نیازهای عملی کاربران به‌عنوان پل ارتباطی میان جامعه مدنی و نظام حقوقی عمل می‌کنند و نقش به‌سزایی در تکامل حقوق فضای مجازی ایفا می‌نمایند.

۶. نتیجه‌گیری

حفاظت از حریم خصوصی در فضای مجازی از منظر حقوق عمومی یک موضوع پیچیده و چندبعدی است که نیازمند توجه جدی به مبانی نظری، چالش‌های قانونی و چهارچوب‌های قانونی موجود است. مبانی نظری حریم خصوصی به‌عنوان یک حق بنیادین در حقوق عمومی نیاز به شفافیت و اعتبار قانونی دارد تا بتواند در برابر تهدیدات و نقض‌های ممکن، از جمله حملات سایبری و نقض‌های عمدی، محافظت کند. چالش‌های قانونی حفاظت از حریم خصوصی در فضای مجازی از جمله نقض حریم خصوصی، حملات سایبری و قوانین و محدودیت‌ها همگی نشان‌دهنده نیاز به تقویت نظارت و مدیریت در این حوزه است. نقش دولت و نهادهای نظارتی در ایجاد امنیت و حفاظت از حقوق شهروندان در برابر تهدیدات سایبری نقشی حیاتی دارد. این نهادها باید با به‌کارگیری ابزارهای نظارتی و حمایتی به تأمین حریم خصوصی کاربران در فضای مجازی بپردازند. چهارچوب‌های قانونی و سیاست‌گذاری در این زمینه نیز باید به‌طور مؤثر و هماهنگ با ظرفیت قوانین داخلی و معاهدات بین‌المللی تقویت شوند. این هماهنگی به ایجاد یک محیط قانونی مناسب برای حمایت از حریم خصوصی در فضای مجازی کمک خواهد کرد و به رشد و توسعه فناوری‌های نوین پاسخ‌گو خواهد بود. در نهایت، برای حفاظت از حریم خصوصی در فضای مجازی راهکارها و استراتژی‌های متعددی می‌توان به‌کار گرفت. نقش

عبدالسعید شجاعی و همکار ـــــــ

خصوصی در حقوق ایران»، *مجله مطالعات علوم اجتماعی*، دوره ۱، شماره ۱، صص ۱۴۸-۱۵۳.

۸. تقی‌پور درزی نقیبی، محمدحسین؛ موسوی خطیر، سیده طاهره و مهدی طالقان غفاری (۱۴۰۳). «محافظت از حریم خصوصی و اطلاعات شخصی: مطالعه تطبیقی بین حقوق ایران و حقوق کانادا»، *مجله پژوهش‌های حقوقی*، دوره ۲۳، شماره ۵۸، صص٦٥٥-٦٨٢.

۹. لاریجانی، علی و محمود هاشمی شاهرودی (۱۳۸۸). «قانون جرائم رایانه‌ای»، *فصلنامه قضاوت*، شماره ۵۷.

۱۰. واعظی، مجتبی و علی علی‌پور (۱۳۸۹). «بررسی موازین حقوقی حاکم بر حریم خصوصی و حمایت از آن در حقوق ایران»، *مجله حقوق خصوصی دانشگاه تهران*، شماره ۱۷، صص ۱۳۳-۱٦۳.

۷-۲) منابع انگلیسی

A) Books

11. Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C., & Nouwt, S. (Eds.) (2009). *Reinventing data protection?*, Springer Science & Business Media.

B) Articles

12. Abikoye, B. E., Adelusi, W., Umeorah, S. C., & Adelaja, A. O. (2024). "Integrating risk management in fintech and traditional financial institutions through AI and machine learning".
13. Aho, B., & Duffield, R. (2020). "Beyond surveillance capitalism", *Economy and Society*.
14. Alabdan, R. (2020). "Phishing attacks survey", *Future Internet*.
15. Annas, G. J. (1989). "The Supreme Court, privacy, and abortion", *New England Journal of Medicine.LK.*
16. Berween, M. (2002). "The fundamental human rights: an Islamic perspective", *The International Journal of Human Rights.*
17. Bignami, F. (2007). "Privacy and law enforcement in the European Union", *Chicago Journal of International Law.*

عبدالسعید شجاعی و همکار ـــــــ

Environment", *OIDA International Journal of Sustainable Development.*
33. Richard A. Posner (1977). "The right of privacy", *Georgia Law Review.*
34. Rubinstein, I. S., Lee, R. D., & Schwartz, P. M. (2008). "Data mining and Internet profiling", *University of Chicago Law Review.*
35. Sapiński, A. (2023). "The importance and challenges of information security in the digital age", *Scientific Journal of Bielsko-Biala School of Finance and Law.*
36. Sekhon, V. (2003). "The civil rights of others", *Texas Forum on Civil Liberties & Civil Rights.*
37. Sembiring, T. B., et al. (2024). "Digital Privacy Rights in the Age of Big Data", *Global International Journal of Innovative Research.*
38. Steeves, V., & Mačėnaitė, M. (2022). "Data protection and children's online privacy", In Research Handbook on Privacy and Data Protection Law (pp. 358–374). *Edward Elgar Publishing.*
39. Tan, C., Zhang, L., & Bao, L. (2020). "A Deep Exploration of BitLocker Encryption and Security Analysis", *In Proceedings of the 2020 IEEE 20th International Conference on Communication Technology (ICCT).*
40. Taslitz, A. E. (2002). "The Fourth Amendment in the twenty-first century", *Law and Contemporary Problems.*
41. Wagner, J., & Benecke, A. (2016). "National Legislation within the Framework of the GDPR", *European Data Protection Law Review.*
42. Westin, A. F. (2003). "Social and political dimensions of privacy", *Journal of Social Issues.*
43. Yuejia Qu (2024). "Privacy Protection in the Digital Age: Challenges and Strategies", *Transactions on Social Science, Education and Humanities Research.*

[In Persian]:

A) Books

44. Akhondi, Mahmoud (2000). *Ayin-e Dadresi-e Keyfari* [Criminal Procedure], Vol. 4. Qom: Entesharat-e Daneshgah-e Qom (Eshraq).
45. Mansour, Jahangir (2008). *Ghanoun-e Mojazat-e Eslami* [Islamic Penal Code], Tehran: Entesharat-e Kaj.
46. Shokri, Reza; Sirous, Ghader (2006). *Ghanoun-e Mojazat-e Eslami dar Nazm-e*

Hoghughi Konouni [Islamic Penal Code in the Current Legal Order], Tehran: Entesharat-e Mohajer.

47. Tale'e Kharasand, Hadi (2006). *Ghanoun-e Mojazat-e Eslami* [Islamic Penal Code], Tehran: Nashr-e Jamal al-Hagh.

B) Articles

48. Drummond, Ann & Moos, Ann (2025). "Hoosh-e Masnou'i va Ghanoun-gozari: Yek Morour-e Kolli [Artificial Intelligence and Lawmaking: An Overview]", Translated by: Ali Bahadori Jahromi, *Faslnameh Pazhouhesh-haye Hoghugh-e Tatbiqi (Quarterly of Comparative Law Studies),* 29(2), 187-213.
49. Gharayagh Zandi, Ahmad; Jamali Posht Masari, Soudabeh; Hafezi, Somayeh (2015). "Ahkam-e Harim-e Khosousi dar Hoghugh-e Iran [Rules of Privacy in Iranian Law]", *Majaleh Motale'at-e Oloum-e Ejtemaei (Journal of Social Sciences Studies)*, 1(1), 148-153.
50. Larijani, Ali & Hashemi Shahroudi, Mahmoud (2009). "Ghanoun-e Jara'em-e Rayane'i [Computer Crimes Act]", *Faslnameh Ghazavat (Judicial Quarterly)*, 57.
51. Shahbaz Ghahfarrokhi, Sajjad (2013). "Harim-e Khosousi-ye Fiziki-ye Afrad dar Ayineh-ye Feqh-e Emamiyeh va Hoghugh-e Iran [Physical Privacy of Individuals in the Light of Imami Jurisprudence and Iranian Law]", *Majaleh Pazhouhesh-haye Feqhi (Journal of Jurisprudential Studies)*, 9(1), 55-70.
52. Taghipour Darzi Naqibi, Mohammad Hossein; Mousavi Khatir, Seyedeh Tahereh; Taleqan Ghaffari, Mehdi (2024). "Mohafezat az Harim-e Khosousi va Etela'at-e Shakhsi: Motale'eh-ye Tatbiqi beyn-e Hoghugh-e Iran va Hoghugh-e Canada [Protection of Privacy and Personal Data: A Comparative Study between Iranian Law and Canadian Law]", *Majaleh Pazhouhesh-haye Hoghughi (Journal of Legal Research)*, 23(58), 655-682.
53. Va'ezi, Mojtaba & Alipour, Ali (2010). "Barrasi-ye Mavazin-e Hoghughi Hakem bar Harim-e Khosousi va Hemayat az An dar Hoghugh-e Iran [An Analysis of the Legal Standards Governing Privacy and Its Protection in Iranian Law]", *Majaleh Hoghugh-e Khosousi Daneshgah-e Tehran (Journal of Private Law, University of Tehran)*, 17, 133-163.