-- Journal of Private Law Research------
Winter 2026, 14 (53), 206-246
Jplr.atu.ac.ir
DOI: 10.22054/jplr.2025.88038.2955

ATU PRESS

Original Research
Received: 07/Sep/2025
Accepted: 28/Oct/2025
ISSN: 2345-3583
eISSN: 2476-6232

The Attitude of Iranian Law and European Union Law towards Metadata and the Place of Privacy in It

Hossein Khanlari Bahnamiri* | Department of Law, Faculty of Humanities, University of Damghan, Damghan, Iran

Mohammad Hossein Taghipour Darzinaghibi | Department of Private Law, Faculty of Law and Political Science, University of Mazandaran, Babolsar, Iran

Hamed Agha Amini Fashami | PhD student, Department of Private Law, Faculty of Law and Political Science, University of Mazandaran, Babolsar, Iran

Extended Abstract

One of the current concerns of humanity is the protection of privacy related to metadata. Data is not secure even when processed by the most advanced and powerful companies with financial resources, which makes it more necessary to pay attention to data and metadata in the new era. Metadata is data about data that is created by individuals to achieve a specific goal or function. In fact, metadata is a systematic way that makes information resources accessible and understandable to users. Metadata, such as smartphone metadata, is one of the most important privacy concerns. The concern for citizens

* Corresponding Author: H.khanlaribahnamiri@du.ac.ir
How to Cite: Khanlari Bahnamiri, H. , TAGHIPOUR,, M. H. and Aghaaminifashmi,. H. (2026). The Attitude of Iranian Law and European Union Law towards Metadata and the Place of Privacy in It. *Private Law Research*, 14 (53), 207 -246. Doi: 10.22054/jplr.2025.88038.2955

of society alike is that metadata, much like data, can reveal sensitive and personal information of a user. In line with the advancement of technology and information technology, the European Union has taken very useful and effective measures to protect the privacy of data and metadata and has pursued the issue of metadata and privacy seriously and in a disciplined manner since 2018, while in Iran this discussion has not been examined in detail and comprehensively; of course, perhaps the risks of violating this privacy have not yet been taken seriously. Therefore, the main question of the research is whether privacy in the field of metadata, as protected in the legal system of the European Union, has been examined in the legal system of Iran? The research method in this article is analytical-comparative, and library resources and online articles and books have been used. The findings show that by examining all Iranian laws regarding the protection of privacy and data, it can be claimed that the discussion of metadata has not been included in these laws at all, and some of the related laws have only addressed data in cyberspace and the importance of privacy. In this regard, although the E-Commerce Law is the best law in providing protection on data privacy issues in Iran, it falls short in respecting important principles of data privacy protection. In fact, the E-Commerce Law, which contains some provisions on data messages, is insufficient in protecting electronic consumers. Iran needs a specific law on the protection of personal data and, of course, metadata. The provisions in the E-Commerce Law do not generally meet some prominent principles of data privacy. For example, it does not fully protect individuals' personal information and only identifies sensitive personal data such as medical and health data. E-business websites collect information online, but most of them do not have any policy/privacy statement, or at least this policy is not available online, such as the online store Digi Kala. The E-Commerce Law constitutes the primary law in Iran that contains some provisions (Articles 59-61) on the protection of personal data. However, for such a law, the protection of personal data is limited to a specific context, namely, in the context of electronic consumers who deal with online

commerce, and there is no mention or attempt to frame the rules on metadata and privacy in this law, which is the most relevant law in Iran in the field of data and privacy. However, regarding privacy and metadata in the European Union, it can be said that the e-Privacy and Communications Regulation is located alongside the European Union Data Protection Law, which are two relatively separate and, of course, complementary laws in the field of metadata and privacy. In fact, the e-Privacy and Communications Regulation implements a European directive, also known as the "e-Privacy Directive". This institution recognizes that widespread public access to mobile digital networks and the Internet creates new opportunities for businesses and users, but also new risks to their privacy. The European Union is replacing the current Privacy Act with a new Privacy Regulation to align with the EU version of the Data Protection Act. Among the features of this directive are: ensuring the security of electronic communications services, ensuring the confidentiality of communications regarding traffic data, requiring the anonymity of traffic data, requiring full billing by Internet service providers, requiring consent for the processing of users' static data, and other such matters. As a result, in EU law, electronic communications and metadata privacy laws have a very advanced, comprehensive and enforceable framework, and are being developed with three approaches: (1) service-oriented, (2) data-oriented, and (3) value-oriented, and with respect to the principles governing these approaches such as the principles of transparency, trust, non-discrimination, ownership and control, security, minimum access, informed consent, which create the right of access, the right to rectification, the right to be forgotten (deleted), the right to restriction of processing, the right to data portability, and the right to object for individuals. Although each approach has its strengths and weaknesses, the focus of all three approaches has been on protecting citizens' privacy from metadata. This issue has been clearly addressed in European Union law, but the Iranian legal system, apart from the issuance of an executive directive to improve the protection of user privacy and the method of collecting, processing, and maintaining

user information in open space systems and platforms, which was developed with a service-oriented approach, has not addressed much about the importance of metadata and privacy in the new era, and the existing laws are still in their early stages and lack executive details and a supervisory Institution. Therefore, it is recommended to develop a comprehensive law similar to the GDPR, establish an independent supervisory body, or require companies to be transparent in their privacy policies, or enact a specific and comprehensive law using the approaches mentioned in European Union laws, especially the General Data Protection Regulation, which guarantees the rights of data subjects.

Keywords: Metadata, European Union, privacy, Iranian law, supervisory institution

مقاله پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۶/۱۶ تاریخ پذیرش: ۱۴۰۴/۰۸/۰۶ ISSN: ۲۳۴۵-۳۵۸۳ eISSN: ۲۴۷۶-۶۳۳۲

-- فصلنامه علمی پژوهش حقوق خصوصی ---------

دوره ۱٤، شماره ۵۳، زمستان ۱٤۰٤، ۲۰۷-۲٤٦

Jplr.atu.ac.ir

DOI: 10.22054/jplr.2025.88038.2955

نگرش حقوق ایران و اتحادیهٔ اروپا نسبت به ابرداده و جایگاه حریم خصوصی در آن

حسین خانلری بهنمیری* استادیار گروه حقوق، دانشکده علوم انسانی، دانشگاه دامغان، دامغان، ایران

محمد حسین تقی پور درزی نقیبی استادیار گروه حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه مازندران، بابلسر، ایران

حامد آقا امینی فشمی دانشجوی دکتری حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه مازندران، بابلسر، ایران

چکیده

حفظ حریم خصوصی مربوط به ابرداده‌ها، یکی از نگرانی‌های مهم اشخاص موضوع داده محسوب می‌شود، که نیازمند حمایت‌های قانونی است. در جوامع امروزی که حریم خصوصی افراد با مسئلهٔ فناوری اطلاعات، به‌ویژه داده‌ها ارتباط تنگاتنگی دارد، حفظ حریم خصوصی افراد اهمیت دوچندانی می‌یابد. روش تحقیق در این مقاله به شکل تحلیلی-تطبیقی است. یافته‌ها نشان می‌دهد، اتحادیهٔ اروپا به‌طور خاص با تصویب مقررات عمومی حفاظت از داده‌ها (GDPR)، از سه رویکرد خدمات‌محور، داده‌محور و ارزش‌محور بهره گرفته و باتوجه به اصول حاکم بر این رویکردها مانند اصل شفاف‌سازی، اصل حداقل دسترسی، حاکمیت ابرداده‌ها، در پی قانونمند ساختن حوزهٔ ابرداده و میزان‌سازی جایگاه حریم خصوصی بوده است، درحالی‌که حقوق داخلی در زمینهٔ ابرداده و حریم خصوصی، به‌جز یک دستورالعمل که با رویکرد خدمات‌محور وضع شده است، فاقد قانون خاص و جامع در این حوزه است. ازاین‌رو، پیشنهاد می‌شود قانونی خاص و جامع با بهره‌گیری از رویکردهای مذکور در قوانین اتحادیهٔ اروپا خصوصاً مقررات عمومی حفاظت از داده‌ها و اصول حاکم بر آن‌ها، که متضمن حقوق اشخاص موضوع داده هستند، تدوین و تصویب شود.

کلیدواژه‌ها: ابرداده، اتحادیهٔ اروپا، حریم خصوصی، حقوق ایران، نهاد نظارتی.

* نویسنده مسئول: H.khanlaribahnamiri@du.ac.ir

مقدمه

حقّ حفظ حریم خصوصی در تمام اسناد اصلی بین‌المللی و منطقه‌ای حقوق بشر (مانند اعلامیهٔ جهانی حقوق بشر، میثاق بین‌المللی حقوق مدنی و سیاسی، کنوانسیون کارگران مهاجر سازمان ملل، کنوانسیون حقوق کودک سازمان ملل، مادهٔ ۸ کنوانسیون ۱۹۵۰ اروپا برای حمایت از حقوق بشر و آزادی‌های اساسی و معاهدات مختلف منطقه‌ای و بین‌المللی دیگر) بیان شده است. همان‌گونه که مادهٔ ۱۲ اعلامیهٔ جهانی حقوق بشر مقرر داشته است: «احدی در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات خود نباید مورد مداخله‌های خودسرانه واقع شود و شرافت و اسم و رسمش نباید مورد حمله قرار گیرد. هرکس حق دارد که درمقابل این‌گونه مداخلات و حملات، مورد حمایت قانون قرار گیرد»؛ یعنی این اعلامیه، نقض حریم خصوصی را ممنوع اعلام کرده است[1] بر طبق قوانین مدنی و شهروندی، حریم خصوصی یک حقّ انسانی است که نتیجهٔ رعایت و حفظ آن احساس امنیت و آرامش افراد یک جامعه است، حریم شخصی یا خصوصی به افراد این امکان را می‌دهد تا برای محافظت از خود دربرابر مداخلات غیرمجاز در زندگی‌شان مرزهایی ایجاد کنند، و یکی از دغدغه‌های امروزی بشر حفظ حریم خصوصی مربوط به ابرداده‌هاست. داده‌ها حتی زمانی که توسط پیشرفته‌ترین و قدرتمندترین شرکت‌های دارای منابع مالی پردازش می‌شوند، ایمن نیستند، این موضوع توجه به داده‌ها و ابرداده‌ها را در عصر جدید بیش از پیش ضروری می‌کند(Steiner, 2017: 56). ابرداده؛ داده‌هایی دربارهٔ داده‌ها است که ازسوی افراد برای نیل به یک هدف یا یک عملکرد خاص ایجاد شده است. درواقع، ابرداده روشی نظام‌مند است که منابع اطلاعاتی را برای کاربران دسترس‌پذیر و قابل فهم می‌سازد. ابرداده‌هایی مثل ابرداده‌های تلفن هوشمند یکی از مهم‌ترین نگرانی‌های مربوط به حریم خصوصی هستند، نگرانی شهروندان جامعه به‌طور یکسان این است که ابرداده‌ها، بسیار شبیه به داده‌ها، می‌توانند اطلاعات حساس و شخصی یک کاربر را فاش کنند. در راستای پیشرفت تکنولوژی و فناوری اطلاعات، اتحادیهٔ اروپا

---

۱ بنافی، فرشته، «حفاظت از حق حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی»، *پژوهش حقوق خصوصی*، دورهٔ ۱۲، شمارهٔ ۴۵ (۱۴۰۲)، ص ۱۶۰.

اقدامات بسیار مفید و مؤثری برای حفظ حریم خصوصی داده‌ها و ابرداده‌ها برداشته و مسئلهٔ ابرداده و حریم خصوصی را از سال ۲۰۱۸ به‌طور جدی و با رویکردی ضابطه‌مند دنبال کرده است، این در حالی است که در ایران این بحث به‌طور دقیق و همه‌جانبه مورد بررسی قرار نگرفته است؛ شاید به این دلیل که خطرات نقض این حریم خصوصی هنوز جدی نگرفته نشده است. ازاین‌رو، سؤال اصلی پژوهش این است که آیا حریم خصوصی درزمینهٔ ابرداده‌ها آن‌گونه که در نظام حقوقی اتحادیهٔ اروپا مورد حمایت قرار گرفته، در نظام حقوقی ایران مورد مداقه قرار گرفته است؟ در این مقاله سعی شده است باتوجه به سطح تحلیلی متفاوت و با ارائهٔ سه سطح خدمات‌محور، داده‌محور و ارزش‌محور در حقوق اتحادیهٔ اروپا، تحلیلی جامع دربارهٔ ابرداده و حریم خصوصی با نگاهی به قوانین داخلی انجام شود، تا درنهایت راهکاری برای نظام حقوقی ایران پیشنهاد گردد.

۱- حریم خصوصی:

در لغت‌نامهٔ *دهخدا* حریم به معنای بازداشتن از...و بی‌بهره گردانیدن از... می‌باشد[۱].حریم خصوصی قلمروی از زندگی هر فرد است که انتظار معقول دارد دیگران بدون رضایت او وارد آن نشوند یا به اطلاعات آن قلمرو دسترسی نداشته باشند[۲].

به زبان ساده‌تر حریم خصوصی همان اطلاعات و زندگی شخصی افراد است[۳].همچنین، حریم خصوصی افراد، یعنی حریمی خصوصی که انتظار می‌رود قانون و نظم رعایت شود و از نفوذ افراد دیگر محافظت شود[۴].(معنای حریم خصوصی در طول تاریخ خود در پاسخ به موجی پس از موج قابلیت‌های فناوری جدید و پیکربندی‌های اجتماعی مورد مناقشه

---

۱ دهخدا، علی‌اکبر، *لغت‌نامه دهخدا*، جلد ششم، چاپ دوم، (تهران: دانشگاه تهران، ۱۳۷۷)، ص۳۴۵.

۲ صفایی، سید حسین؛ جعفری، علی، «رابطه آزادی اطلاعات با حریم خصوصی»، *حقوق اسلامی*، شمارهٔ ۳۳، (۱۳۹۱)، ص ۱۳۷.

۳ شجاعی کاریزکی، مرضیه، «جایگاه حریم خصوصی افراد در حقوق مدنی و قوانین موضوعه ایران»، *دستاوردهای نوین در مطالعات علوم اسلامی*، شمارهٔ ۳۳، (۱۳۹۹)، ص۱۰۳.

۴ شجاع سنگچولی، مهرویه، «حق حریم خصوصی کودکان در حقوق موضوعه ایران و کنوانسیون حقوق کودک»، *حقوق و مطالعات نوین*، شمارهٔ ۱، (۱۳۹۹)، ص۴.

بوده است. دور کنونی مناقشات بر سر حفظ حریم خصوصی، که با علم داده تقویت می‌شود، بسیاری از مفسران را ناامید کرده و برای برخی دیگر به‌منزلهٔ به صدا درآمدن ناقوس مرگ برای حفظ حریم خصوصی بوده است. به‌نظر می‌رسد که اختلافات مربوط به حریم خصوصی نه ویژگی تصادفی این مفهوم است و نه شرط تأسف‌انگیز کاربرد آن. حریم خصوصی اساساً مورد مناقشه است[۱].باوجوداین، چنین می‌نماید که حریم خصوصی یک مفهوم معنادار و ارزشمند است. بحث‌های فلسفی درمورد تعاریف حریم خصوصی در نیمهٔ دوم قرن بیستم برجسته شد و عمیقاً تحت تأثیر توسعهٔ حفاظت از حریم خصوصی در قانون قرار گرفت. برخی از حریم خصوصی به‌عنوان تمرکز بر کنترل اطلاعات درمورد خود دفاع می‌کنند، درحالی‌که برخی دیگر آن را یک مفهوم گسترده‌تر و ضروری برای کرامت انسانی تلقی می‌کنند. در جهان داده‌ها می‌توان گفت که حریم خصوصی حالتی است که شخص در داشتن فضای شخصی یا داده‌هایی که نمی‌خواهد با دیگران به اشتراک بگذارد قرار گرفته است. در این راستا، حریم خصوصی با مقولهٔ حفاظت از داده‌ها قرابت می‌یابد. براین مبنا حفاظت از داده‌ها نه‌تنها به محرمانه نگه‌داشتن اطلاعات شخصی مربوط می‌شود، بلکه شامل ایجاد یک چارچوب قابل اعتماد برای جمع‌آوری، تبادل و استفاده از داده‌های شخصی در معاملات آنلاین نیز هست[۲].همچنین حریم خصوصی یک حقّ اساسی و واجد شرایط انسانی است. حقّ حفظ حریم خصوصی در تمام اسناد اصلی بین‌المللی و منطقه‌ای حقوق بشر (مانند مادهٔ ۱۲ اعلامیهٔ جهانی حقوق بشر، میثاق بین‌المللی حقوق مدنی و سیاسی[۳]،کنوانسیون کارگران مهاجر سازمان ملل، کنوانسیون حقوق کودک سازمان ملل، مادهٔ ۸ کنوانسیون ۱۹۵۰ اروپا برای حمایت از حقوق بشر و آزادی‌های اساسی و معاهدات مختلف منطقه‌ای و بین‌المللی دیگر) آمده است.ضمن اینکه دیوان اروپایی

1 Mulligan, D. K., Koopman, C., & Doty, N. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, 374(2083).(2016), p.374.

2 Munir, Bakar A, Yasin, Mohd SH , Information and Communication Technology Law: State, Internet and Information, Legal and Regulatory Challenges. Sweet and Maxwell Asia, Kuala Lumpur.(2010),p.5.

ICCPR۳

حقوق بشر در آرای متعددی اصطلاح حریم خصوصی را مفهومی گسترده دانسته است که تمامیت جسمی و روانی اشخاص را نیز دربر می‌گیرد[۱].

حقوق مندرج در اسناد حقوق بشر به‌طور کلی به دو بخش مطلق و مقید تقسیم می‌شود، محدود شدن برخی از حقوق مانند حقّ حیات، حقّ برخورداری از محاکمهٔ عادلانه و حقّ مصونیت دربرابر مجازات‌های خشن و غیرانسانی، امری تحمل‌ناپذیر است که نمونه‌های فوق در دستهٔ حقوق مطلق جای می‌گیرند، و اعمال آن‌ها صرف‌نظر از اقلیم جغرافیایی فرهنگی و سوابق تاریخی محلّ اجرای آن صورت می‌گیرد. ولی حقوق دیگری وجود دارد که اجرای مطلق آن به علت برخورد با حقوق فردی و منافع اجتماعی امکان‌پذیر نیست و باید مقید گردند، مانند حریم خصوصی که قیدپذیر است و در هر نظام حقوقی، محدودهٔ اعمال مشخصی دارد[۲].فقه اسلامی نیز با مبحث حریم خصوصی ناآشنا نبوده است، از پژوهش در منابع شرع اسلام برمی‌آید که حمایت از حریم خصوصی اعتقادات، محلّ زندگی، اموال، مراسلات و ارتباط افراد از همان ابتدای ظهور اسلام وجود داشته و تحت تعابیری ازجمله حقّ مالکیت، حقّ در پناه اصل برائت، حقّ مصونیت از تجسس و تفتیش، ممنوعیت آشکارسازی اسرار، حقّ انتخاب دین و اعتقادات، حرمت غیبت، ممنوعیت استراق سمع، ممنوعیت اشاعهٔ فحشا و ... مورد حمایت قرار گرفته است[۳].

ابرداده برای حفظ حریم خصوصی مهم است زیرا می‌تواند اطلاعاتی را درمورد محتوا و زمینهٔ یک فایل فاش کند، حتی اگر خود فایل حاوی اطلاعات قابل شناسایی نباشد. از این جهت، توجه به نقش ابرداده در حمایت از حریم خصوصی کاربران در حقوق و قوانین مدنی ضروری است. چه اینکه ابرداده می‌تواند کلّ اطلاعات شخص را بدون خواندن محتوای پیام به شخص ثالث بازگو کند و با فایل‌های در دسترس، می‌تواند اطلاعات اضافی و بالقوهٔ حساس شخصی را فراتر از آنچه در متن یک فایل وجود دارد، آشکار کند. براین

---

۱ مجاهد، افشین، «رویکردی تطبیقی بر حریم خصوصی»، *پژوهش‌های حقوق تطبیقی عدل و انصاف*، شمارهٔ ۱۳ (۱۴۰۰)، ص ۸.

۲ کاتوزیان، ناصر؛ رحیمی، حبیب‌الله، *آزادی اندیشه و بیان*، چاپ اول، (تهران: دانشگاه تهران، ۱۳۸۲)، ص ۱۸۰ .

۳ حسینی، مهدی؛ برزویی، محمدرضا، «مبانی و مؤلفه‌های فقهی حمایت از حریم خصوصی افراد در فضای مجازی»، *مطالعات حقوق بشر اسلامی*، شمارهٔ ۱۳(۱۳۹۶)، ص ۱۱۳ .

اساس، مداقه در خود ابرداده، و حریم خصوصی، بر بحث‌های انتظامی و کیفری تقدم دارد؛ به این دلیل که ابتدا باید موضوع بحث -یعنی ابرداده و ارتباط آن با حریم خصوصی- روشن شود و سپس برای مداقهٔ بیشتر، ابعاد دیگر آن مورد تحلیل قرار گیرد. بااین‌حال، همچنان خلاء قانونی خاص درخصوص حمایت از حریم خصوصی در کشور وجود دارد، شایان ذکر است در سال ۱۳۸۴ و در اواخر دولت هشتم «لایحهٔ مربوط به حفظ حریم خصوصی» به مجلس شورای اسلامی تقدیم شد؛ اقدامی که حرکتی مثبت تلقی می‌گردید و با استقبال مجلس و مرکز پژوهش‌های آن نیز روبه‌رو شد، متأسفانه قبل از رسیدگی و تصویب آن در فروردین ۱۳۸۵ توسط دولت جدید پس گرفته شد[۱].

۲- ابرداده:

دراین بخش، داده، با ابرداده، متفاوت انگاشته شده است؛ زیرا درحالی‌که داده‌ها می‌توانند صرفاً بخشی از اطلاعات، فهرستی از اندازه‌گیری‌ها، یا مشاهدات، داستان یا توصیف یک موجودیت خاص باشند، ابرداده اطلاعاتی را درمورد داده اصلی ارائه می‌کند؛ اطلاعاتی که به شناسایی ماهیت و ویژگی‌های آن داده کمک می‌کند. از این حیث، ابرداده[۲]«داده‌ای است که اطلاعاتی درباره سایر داده‌ها ارائه می‌کند»، اما شامل محتوای خود داده‌ها -مانند متن یک پیام یا تصویر- به‌طور خاص نمی‌شود. درواقع ابرداده به معنای «داده‌های مربوط به داده‌ها» است. اگرچه پیشوند «متا یا ابر» به معنای «بعد» یا «فراتر» است، اما در معرفت‌شناسی به معنای «درباره» استفاده می‌شود. ابرداده به‌عنوان داده‌ای تعریف می‌شود که اطلاعاتی دربارهٔ یک یا چند جنبه از داده‌ها ارائه می‌دهد. از ابرداده برای خلاصه کردن اطلاعات اولیه درمورد داده‌ها استفاده می‌شود که می‌تواند ردیابی و کار با داده‌های خاص را آسان‌تر کند[۳].برخی از نمونه‌های ابرداده عبارتند از:

---

۱ زارعیان، داود؛ واحد، فائزه، «بررسی حقوق رگولاتوری‌های حمایت از داده»، *رسانه*، شمارهٔ ۷۲، (۱۳۹۹)، ص ۶۶ .

2 Metadata

3 Steiner, Tobias . "Metadaten und OER: Geschichte einer Beziehung (Metadata and OER: [hi]story of a relationship)". Synergie. Fachmagazin für Digitalisierung in der Lehre (in German). 04:.(2017), p 54.

ابزار ایجاد داده‌ها، هدف داده‌ها، زمان و تاریخ ایجاد، خالق یا نویسندهٔ داده‌ها، مکان در یک شبکهٔ کامپیوتری که در آن داده‌ها ایجاد شده است، استانداردهای مورد استفاده، حجم فایل، کیفیت داده، منبع داده‌ها، فرایندی که برای ایجاد داده‌ها استفاده می‌شود.

به‌طور کلی، ابرداده روشی سیستماتیک است که منابع اطلاعاتی را در دسترس و برای کاربران قابل درک می‌کند. اساس استفاده از ابرداده تسهیل جست‌وجو، مکان‌یابی، انتخاب، ارزیابی و مستندسازی منابع شبکه است که باعث افزایش دقت بازیابی و تسهیل جست‌وجوی منابع شبکه می‌شود. به‌بیانی دیگر، ابرداده، داده‌ای است که داده‌های دیگر را توصیف می‌کند. درواقع، برنامه‌ها یا فایل‌ها دارای ابرداده‌هایی هستند که می‌توانند اطلاعاتی مانند نوع فایل و تاریخ ایجاد آن را در اختیار کاربران قرار دهند. همچنین می‌توان از ابرداده برای فهرست‌نویسی و مرتب‌سازی اطلاعات استفاده کرد. ابرداده، می‌تواند در پایگاه داده‌ها و سیستم‌هایی که نیاز به فیلتر کردن داده‌ها برای معیارهایی مانند نویسنده، تاریخ مبدأ یا نوع فایل دارند، ضروری باشد. یک مثال دیجیتالی از ابرداده زمانی است که یک پخش‌کننده MP3 نام، هنرمند و طول یک آهنگ را نمایش می‌دهد. همچنین می‌توان این مثال را مطرح کرد که یک تصویر دیجیتالی ممکن است شامل متادیتا باشد که اندازهٔ تصویر، عمق رنگ، وضوح، زمان ایجاد، سرعت شاتر و سایر داده‌ها را توصیف می‌کند. می‌توان گفت که فراداده می‌تواند یک سند متنی باشد که حاوی اطلاعاتی درمورد مدت زمان سند، هویت نویسنده، زمان نگارش سند و خلاصهٔ کوتاهی از سند باشد. ابرداده در صفحات وب همچنین می‌تواند حاوی توضیحات محتوای صفحه و نیز کلمات کلیدی مرتبط با محتوا باشد. این پیوندها اغلب «متاتگ»[1] نامیده می‌شوند که تا اواخر دههٔ ۱۹۹۰ به‌عنوان عامل اصلی در تعیین ترتیب جست‌وجوی وب استفاده می‌شد. اتکا به متاتگ‌ها در جست‌وجوهای وب در اواخر دههٔ ۱۹۹۰ به دلیل «پر کردن کلمات کلیدی»[2] کاهش یافت[3].(متاتگ‌ها عمدتاً برای فریب موتورهای جست‌وجو به این دلیل که برخی

1 Metatags
2 keyword stuffing
3 Beyene, Wondwossen Mulualem . "Metadata and universal access in digital library environments". Library Hi Tech. 35 (2):,(2017), p. 210-212.

وب‌سایت‌ها ارتباط بیشتری نسبت به آنچه واقعاً داشتند در جست‌وجو دارند، مورد سوء استفاده قرار می‌گرفتند[۱]. مجلهٔ *اسلیت*[۲] در سال ۲۰۱۳ گزارش داد که تفسیر دولت ایالات متحده از «فراداده» می‌تواند گسترده باشد و ممکن است حاوی محتوای پیام مانند خطوط موضوع ایمیل‌ها باشد[۳]. بنابراین ابرداده می‌تواند در گسترهٔ محتوای پیام‌های ایمیل نیز قرار گیرد که ارتباط مستقیمی با حریم خصوصی دارد.

باتوجه به نقش و اهمیت ابرداده که به‌طور مستقیم با حریم خصوصی افراد ارتباط پیدا می‌کند و اهمیت حفاظت از داده‌ها و جلوگیری از افشای حریم خصوصی افراد، باوجود تصویب قوانینی ازجمله قانون جرایم سایبری (۱۳۸۸)، قانون آزادی دسترسی به اطلاعات (۱۳۸۸)، منشور حقوق شهروندی (۱۳۹۵) درکشور، در عمل به‌نظر می‌رسد که تنها سند جامعی که در این خصوص تا حدودی نسبتاً مرتبط بدان پرداخته است، «لایحهٔ صیانت و حفاظت از داده‌های شخصی» است که به گزارش مرکز روابط‌عمومی و اطلاع‌رسانی وزارت ارتباطات و فناوری اطلاعات، در مرداد ۱۳۹۷، رونمایی شد. این سند در حال حاضر جامع‌ترین سند موجود است؛ اما هنوز به تصویب قوه مقننه نرسیده است و طبعاً قدرت اجرایی ندارد. پیشتر، دو لایحه با عناوین «حمایت از حریم خصوصی» و «لایحهٔ آزادی اطلاعات» در دههٔ هشتاد نیز به مجلس تقدیم شده بود، اما درنهایت اقدامی که منجر به تصویب آن‌ها بشود، صورت نپذیرفت. به هر صورت، درزمینهٔ ابرداده و حریم خصوصی نمی‌توان قانونی جامع و مانع را در ایران یافت.

۳- حریم خصوصی و ابرداده در قوانین ایران:

اصطلاح حریم به مکانی اطلاق می‌شود که باید از آن محافظت و دفاع کرد و هیچ‌کس حقّ تعرض به آن را ندارد. علاوه‌بر این، ازآنجاکه حریم خصوصی بخشی از زندگی یک فرد است که به‌وسیلهٔ قانون یا عرف تعیین شده و مورد احترام قرار می‌گیرد، اگر حریم

---

1 Rouse, Margaret . "Metadata". WhatIs. TechTarget.(2014), p. 1-3.

۲ Slate اسلیت یک مجلهٔ آنلاین مترقی است که به امور جاری، سیاست و فرهنگ در ایالات متحده می‌پردازد.

3 Wolff, Josephine . "Newly Released Documents Show How Government Inflated the Definition of Metadata". Slate Magazine. (2013), p 4-6.

خصوصیِ شخصی امنیت یا آسایش دیگری را مختل کند، همین قانون می‌تواند و مجاز است آن را محدود کند[۱].البته در قوانین موضوعه علی‌الخصوص قانون مدنی، هرجا موضوع حریم مطرح می گردد بیشتر حریم املاک و انهار متبادر به ذهن می گردد جایی که دکتر لنگرودی در کتاب *ترمینولوژی حقوق* حریم را مقداری از اراضی اطراف ملک و قنات و نهر که برای کمال انتفاع از آن ضرورت دارد تعریف کرده‌اند[۲].(

در طول قرن بیستم تعرضات جدید ناشی از پیشرفت تکنولوژی، شامل ضبط مکالمات تلفنی خصوصی، قابلیت جمع آوری، ذخیره و به‌دست آوردن داده‌ها و اطلاعات باعث شد تا حریم خصوصی به‌عنوان یک حقّ مهم و اساسی شناخته شود. به‌طوری که در سطح بین‌المللی با جدیت فراوانی دنبال شد و اعلامیهٔ حقوق بشر در سال ۱۹۴۸ در مادهٔ ۱۲ و میثاق بین‌المللی حقوق مدنی و سیاسی در مادهٔ ۱۷ این حق را به رسمیت شناختند[۳].

در ادامه به قوانین داخلی که در ارتباط با حریم خصوصی و ابر داده است، اشاره خواهد شد:

۳-۱. لوایح و طرح‌های پیشنهادی

درزمینهٔ تبیین دقیق حقوق اشخاص موضوع داده، نظام حقوقی ایران موادّ قانونی مصرح ندارد و صرفاً در این باره به ارائهٔ طرح و لایحه پرداخته است، برای نمونه پیش‌نویس لایحهٔ «صیانت و حفاظت از داده‌های شخصی» که در تیرماه ۱۳۹۷ در سایت وزارت ارتباطات و فناوری اطلاعات ایران منتشر شده است و یا طرح «حمایت و حفاظت از داده و اطلاعات شخصی» که در شهریور ۱۴۰۰ در صحن علنی مجلس اعلام وصول شده است، هر دو در جهت حمایت از داده‌های شخصی و اشخاص موضوع داده تدوین شده‌اند و در آن‌ها به

---

۱ الماسی، علی؛ محمدیان شیرمرد، مرضیه، «ملاک‌های حریم خصوصی در فقه امامیه و حقوق اساسی ایران: تطبیق با خودروی شخصی». *مطالعات فقهی‌حقوقی زن و خانواده*، دورهٔ ۲، شمارهٔ ۳، (۱۳۹۸)، ص ۳۱.

۲ جعفری لنگرودی، محمدجعفر، *ترمینولوژی حقوق*، *چاپ سیزدهم*، (تهران: گنج دانش، ۱۳۸۲)، ص ۲۱۴.

۳ موسی‌زاده، ابراهیم؛ مصطفی‌زاده، فهیم، «نگاهی به مفهوم و مبانی حق بر حریم خصوصی در نظام حقوقی عرفی»، *دانش حقوق عمومی*، شمارهٔ ۲، (۱۳۹۱)، ص ۵۰.

برخی حقوق اشخاص موضوع داده اشاره شده است، اما باتوجه به وضعیت این اسناد که اعتبار قانونی ندارند و نیز از آن جهت که حمایت کافی از حقوق اشخاص موضوع آن‌ها صورت نگرفته است، خالی از اشکال نیستند. همچنین در این خصوص می‌توان به پیش‌نویس طرح قانون «حمایت از حقوق کاربران و خدمات پایهٔ کاربردی فضای مجازی» مورخ ۱۴۰۰/۴/۲۶ اشاره کرد، فارغ از اختلافات بسیار درمورد این طرح، باوجود سند مذکوردر راستای حمایت از کاربران وضع شده است، اما در آن به حقوق اشخاص موضوع داده پرداخته نشده و درواقع این طرح به رسالت خود که حمایت مؤثر از حقوق کاربران است، عمل نکرده است، چنین کاستی‌هایی در مصوبات شورای‌عالی فضای مجازی نیز قابل مشاهده است و از مصوبات یادشده نیز نمی‌توان به‌طور دقیق حقوق اشخاص موضوع داده را به‌دست آورد و از اشخاص موضوع داده حمایت مؤثر کرد[1]. (ازجمله مصوبهٔ «سیاست‌های کلی حفاظت از داده‌های شخصی» مصوب ۱۳۹۹، با کاستی‌های اجرایی (فاقد ضمانت اجرای قوی) و مفهومی مانند کاستی در تعریف دادهٔ شخصی، که ممکن است ابرداده‌ها را به‌صورت شفاف و صریح پوشش ندهد، روبه‌روست. و یاوجود استثنائات گسترده و مبهم در این مصوبه، استثنائاتی مانند «امنیت ملی» و «اقتضائات نظام» بدون تعریف دقیق و چارچوب مشخص، می‌تواند به‌راحتی ازسوی نهادهای دولتی و امنیتی مورد استناد قرار گیرد و کلّ چارچوب حفاظت از داده را خنثی کند.

در متن لایحهٔ صیانت و حفاظت از داده‌های شخصی، جای خالی تعریف و مسئولیت‌انگاری صریح نهاد متقاضی پردازش به‌وضوح احساس می‌شود، ضمن اینکه لایحه از نظر ادبیات قانون‌نویسی و نیز در تعیین تفضیلی تکالیف و مسئولیت‌ها با ضعف‌های آشکاری مواجه است[2].

---

۱ لطیف‌زاده، مهدیه؛ قبولی درافشان، سید محمد مهدی؛ محسنی، سعید؛ عابدی، محمد، «حمایت از دادهٔ شخصی در حقوق اتحادیهٔ اروپا و امکان‌سنجی آن در نظام حقوقی ایران»، *مطالعات حقوق عمومی دانشگاه تهران*، دورهٔ ۵۳، شمارهٔ ۲، (۱۴۰۲)، ص ۹۹۷.

۲ بادینی، حسن؛ کرمی، حمزه، «بررسی تطبیقی مسئولیت‌های نهاد متقاضی پردازش، کنترل‌گر و پردازش‌گر تحت مقررات اروپایی حمایت از داده‌های شخصی و لایحه صیانت و حفاظت از داده‌های شخصی»، *تحقیقات حقوقی*، شمارهٔ ۹۵، (۱۴۰۰)، ص ۱۵۵.

۳-۲. قانون اساسی

قانون اساسی جمهوری اسلامی ایران به‌طور کلی به حریم خصوصی اشاره دارد اما به‌طور خاص به موضوع حفاظت از داده‌ها و اطلاعات شخصی نمی‌پردازد. اصل بیست‌ودوم قانون اساسی مقرر می‌دارد: « حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص از تعرض مصون است مگر در مواردی که قانون تجویز کند.» قانون اساسی به‌صراحت از حریم خصوصی محافظت نمی‌کند، اگرچه به‌عنوان قانون عالی کشور، اصول مربوط به چنین هدفی را در بر می‌گیرد[۱].(

۳-۳. قوانین کیفری

در قانون آیین دادرسی کیفری مصوب سال ۱۳۹۲ درمورد حفظ حریم خصوصی تصریح نشده است و تنها به برخی از جنبه‌های مرتبط مانند حریم خصوصی منازل، اماکن و اشیاء و ارتباطات اشاره شده است، درمورد داده‌ها، ماده‌ای که بتوان به‌طور خاص به آن اشاره کرد مادهٔ ۶۵۸ از قانون یادشده است که بر طبق آن حفظ حریم خصوصی افراد و امنیت داده‌های شخصی آنان مورد تأکید قرار گرفته است.

قانون جرایم رایانه‌ای ایران مصوب سال ۱۳۸۸ به حقوق افراد ازجمله مصرف‌کنندگان برای داشتن حریم خصوصی اشاره می‌کند و برای افرادی که از طریق سیستم‌های الکترونیکی به حریم خصوصی افراد تجاوز می‌کنند مجازات کیفری تعیین کرده است. بر این اساس، هرگونه نقض حریم خصوصی افراد جرم تلقی می‌شود. مواردی از قبیل افشای شفاهی یا چاپی اطلاعات شخصی، جعل حقایق برای تحقیر حیثیت عمومی افراد، یا لطمه زدن به شهرت از طریق توهین و افترا، نقض حقوق آن‌ها محسوب می‌گردد. درنهایت، باتوجه به اطلاق مادهٔ یک قانون جرایم رایانه‌ای، صرف دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیلهٔ تدابیر امنیتی حفاظت شده باشند، مشمول

---

۱ بخشایشی بایقوت، محرم؛ حیدری منور، حسین، «حریم خصوصی در حقوق ایران و اسناد بین‌المللی»، *مطالعات بین‌المللی پلیس*، دورهٔ ۸، شمارهٔ ۲۹، (۱۳۹۶)، ص ۲۰۸.

مقررات مادهٔ مذکور خواهد بود و شیوهٔ دسترسی، اعم‌از غیرمستقیم یا با واسطه،تأثیری در اصل موضوع ماده ندارد[۱].

۳-٤. قوانین مدنی

در قانون مدنی مادهٔ خاصی به موضوع حریم خصوصی اختصاص داده نشده است. البته، قراردادهای خصوصی برای عدم افشای اطلاعات، عموماً براساس اصل آزادی قراردادها طبق مادهٔ ۱۰ قانون مدنی ایران مورد تأیید قرار گرفته است. صرف‌نظر از اعتبار قراردادهای خصوصی (در صورت مخالف نبودن با قوانین امری)، مادهٔ ۱ قانون مسئولیت مدنی مقرر می‌دارد: «هرکس بدون مجوز قانونی عمداً یا درنتیجه بی‌احتیاطی به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت تجارتی 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». البته بیان این امر که نقض حریم خصوصی اطلاعاتی، عموماً منجر به خسارت معنوی می‌شود، این واقعیت را نفی نمی‌کند که در برخی موارد خاص، تعدی به اطلاعات خصوصی و فراتر از آن تعدی به طیف قابل توجهی از داده‌های شخصی افراد که قابلیت تجاری و ارزش اقتصادی دارد، می‌تواند سبب ورود خسارت مادی شود. در این صورت مطالبهٔ خسارت براساس قواعد مسئولیت مدنی امکان‌پذیر است، به‌ویژه اگر نقض حریم خصوصی اطلاعاتی فی‌نفسه تقصیر محسوب شود[۲].

۳-۵. قوانین خاص داده‌ها

قوانین خاص شامل مقررات مربوط به حفاظت از داده‌ها در ایران عبارتند از: قانون تجارت الکترونیک، مصوب ۱۳۸۳؛ قانون جرایم رایانه‌ای، مصوب ۱۳۸۸؛ و قانون انتشار و

---

۱ قناد، فاطمه؛ شریف،الهام، «مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌ها ی اتحادیهٔ اروپا»، *حقوق فناوری‌های نوین*، شمارهٔ ۴(ب)، (۱۴۰۰)، ص ۱۴ .

۲ عبدی‌پور، ابراهیم، «رویکرد نظام‌های حقوقی نسبت به نقض حریم خصوصی اطلاعاتی در شبکه‌های اجتماعی مجازی»، *نشریهٔ پژوهشی تطبیقی حقوق اسلام و غرب*، شمارهٔ ۳،(۱۳۹۴)، ص ۱۲۴.

دسترسی به داده‌ها، که از سال ۱۳۸۸ لازم‌الاجرا شد. سایر قوانین و مقررات نیز حفاظت از داده‌ها را در یک زمینهٔ خاص الزامی می‌کنند[۱].براساس مادهٔ ۵۸ قانون تجارت الکترونیک، «ذخیره، پردازش و یا توزیع «داده‌پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاههای عقیدتی، مذهبی، خصوصیات اخلاقی و «داده‌پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیرقانونی است.» قانون تجارت الکترونیک مهم‌ترین قانونی است که بر مبادلهٔ داده‌های الکترونیکی حاکم است. این قانون از یک‌سو دادهٔ پیام شخصی را تعریف کرده و ازسوی دیگر، اصول پردازش داده‌های شخصی و حقوق اشخاص موضوع داده را تعریف کرده و ارزش اثباتی داده‌ها را پیش‌بینی کرده است، باوجوداین، این قانون صرفاً بر معاملات افراد در فضای مجازی حاکم است و روابط گسترده‌ای را که خارج از معاملات ازجمله در ارتباط با سکوهای مجازی وجود دارد، دربر نمی‌گیرد[۲].(

بررسی موادّ ۷۳-۷۱ قانون تجارت الکترونیک و تحلیل شرایط تحقق مسئولیت مدنی،نشان می‌دهد،دو نوع مسئولیت مدنی و کیفری برای حمایت از دادهٔ پیام‌های الکترونیک وجود دارد[۳].

مطابق مادهٔ ۶ قانون انتشار و دسترسی به داده‌ها، اطلاعات خصوصی فقط توسط شخصی که داده‌ها به او تعلق دارد یا از طرف نمایندهٔ مجاز، قابل دسترسی است، اما مطابق مادهٔ ۲ همین قانون هر شخص ایرانی می‌تواند به اطلاعات عمومی دسترسی آزاد داشته باشد (به استثنای مواردی که توسط قوانین مربوطه ممنوع شده است). همچنین قانون انتشار و دسترسی به داده‌ها (براساس مادهٔ ۲۱) حقّ مطالبهٔ خسارت (براساس قانون مسئولیت مدنی) را در صورت وارد شدن ضرر و زیان درنتیجهٔ انتشار داده‌های غیرواقعی یا داده‌های واقعی

---

۱ قناد فاطمه؛ علیقلی امیره، «مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی»، *حقوق قراردادها و فناوری‌های نوین*، دورهٔ ۱ ، شمارهٔ ۱ ، (۱۳۹۹)، صص ۲۹۷-۳۲۲ .

۲ انصاری، باقر؛ عطار، شیما، «حمایت از داده‌ها در چین، مطالعه تطبیقی با رویکرد حمایت از داده‌ها در آمریکا و اتحادیه اروپا»، *مطالعات حقوق تطبیقی*، دورهٔ ۱۳، شمارهٔ ۱، (۱۴۰۱)، ص ۱۰۹ .

۳ علی‌احمدی،حسین؛ شوق‌نیان،آرش، «رعایت حریم خصوصی در فضای مجازی مورد مطالعه :ایران»، *مدیریت فردا*، شمارهٔ ۵۷، (۱۳۹۷)، ص ۱۴۲.

برخلاف مفاد این قانون به رسمیت می‌شناسد. نقض قانون انتشار و دسترسی به داده‌ها یک جرم تلقی می‌شود که منجر به جریمهٔ مالی بین ۳۰۰,۰۰۰ تا ۱۰۰,۰۰۰,۰۰۰ ریال می‌شود. در مواردی که قوانین دیگر مجازات‌های بالاتری را برای همان جرایم تعیین می‌کنند، مجازات بالاتری اعمال می‌شود. این قانون حقّ دسترسی شهروندان ایرانی به اطلاعات موجود در مؤسسات عمومی و آن دسته از مؤسسات خصوصی را که خدمات عمومی ارائه می‌دهند، شناسایی کرده و در موادّ ۱۴ و ۱۵ خود، اطلاعات مربوط به حریم خصوصی یا اطلاعات شخصی را از شمول حقّ دسترسی عمومی خارج دانسته است. تنها اشخاص موضوع داده، اجازهٔ دسترسی به این اطلاعات را دارند، دسترسی سایر اشخاص به اطلاعات خصوصی منوط به رضایت صریح و مکتوب شخص موضوع داده شده است[۱].

علاوه‌بر این، قانون مجازات اسلامی افشای اطلاعاتی را که پزشکان، داروسازان، جراحان و سایر افراد مورد اعتماد در حین انجام کار خود به‌دست آورده‌اند، قابل مجازات دانسته است. جمع‌آوری اطلاعات طبقه‌بندی‌شده برای توزیع نیز در شرایط خاص جرم محسوب می‌شود. اما هک و نقض حریم خصوصی داده‌های کاربران اینترنتی و اجتماعی در ایران تهدیدی جدی برای فعالان سایبری است. سهولت جمع‌آوری و انتشار داده‌ها در وب و ویژگی‌های محیط الکترونیکی منجر به نگرانی‌های فزایندهٔ بسیاری از مشتریان بالقوه درمورد افشای اطلاعات شخصی به ارائه‌دهندگان کالا/خدمات الکترونیکی در ایران شده است.

البته به سند حمایتی و تنظیم مقررات حریم خصوصی کاربران در فضای مجازی (مصوب ۱۳۹۶) نیز می‌توان اشاره کرد، این سند که توسط شورای‌عالی فضای مجازی تصویب شد، یک سند بالادستی و سیاستی است که اصول کلی و اهداف حفاظت از داده‌ها را تعیین می‌کند. براساس این سند، دستگاه‌های مختلف موظف به تهیهٔ قوانین و مقررات جزئی‌تر شده‌اند. این سند بر اصولی مانند **رضایت آگاهانه، شفافیت، حداقل بودن داده‌ها و امنیت** تأکید دارد.

---

۱ منبع پیشین

با بررسی تمام قوانین ایران درزمینهٔ حفاظت از حریم خصوصی و داده‌ها، می‌توان مدعی شد که بحث ابرداده، اساساً در این قوانین وارد نشده است و برخی از قوانین مرتبط تنها به داده‌ها در فضای مجازی و اهمیت حریم خصوصی پرداخته‌اند. در این‌باره اگرچه قانون تجارت الکترونیکی بهترین قانون در ارائهٔ حفاظت درمورد مسائل مربوط به حریم خصوصی داده‌ها در ایران است، اما در رعایت اصول مهم حفاظت از حریم خصوصی داده‌ها کوتاهی می‌کند. درواقع، قانون تجارت الکترونیکی که حاوی برخی مقررات درمورد پیام‌های داده است، در حمایت از مصرف‌کنندگان الکترونیکی ناکافی است. ایران به قانون خاصی درزمینهٔ حفاظت از داده‌های شخصی و البته ابرداده‌ها نیاز دارد. مقررات موجود در قانون تجارت الکترونیکی برخی از اصول برجستهٔ حریم خصوصی داده‌ها را معمولاً برآورده نمی‌سازد. به‌عنوان مثال، این قانون از اطلاعات شخصی افراد به‌طور کامل محافظت نمی‌کند و تنها داده‌های شخصی حساس مانند داده‌های پزشکی و بهداشتی را شناسایی می‌کند. وب‌سایت‌های کسب‌وکار الکترونیکی نیز اطلاعات کاربران را به‌صورت آنلاین جمع‌آوری می‌کنند، اما بسیاری از آن‌ها فاقد بیانیهٔ خط‌مشی/حریم خصوصی هستند یا دست‌کم این خط‌مشی به‌صورت آنلاین در دسترس نیست مانند فروشگاه آنلاین دیجی‌کالا. افزون‌بر این، برخی از بیانیه‌های حفظ حریم خصوصی/خط‌مشی نامشخص یا گمراه‌کننده هستند و گاهی اوقات معنایی ندارند. در برخی موارد، بیانیه‌های خط‌مشی مختصر هستند و در مفاد قانون تجارت الکترونیکی یا هر قانون دیگری گنجانده شده‌اند. به‌طور کلی، باوجود دقت و توجهٔ اتحادیهٔ اروپا به ابرداده‌ها و حریم خصوصی، در حقوق و قوانین ایران نمی‌توان به قانونی در این زمینه و یا موادّی مرتبط دست پیدا کرد؛ همان‌گونه که پیش‌تر اشاره شد، قانون تجارت الکترونیک قانون اولیه در ایران را تشکیل می‌دهد که حاوی برخی مقررات (موادّ ۶۱-۵۹) درمورد حفاظت از داده‌های شخصی است. بااین‌حال، در چنین قانونی، حفاظت از داده‌های شخصی به یک زمینهٔ خاص محدود می‌شود؛ یعنی به حوزهٔ مصرف‌کنندگان الکترونیکی که با تجارت اینترنتی سروکار دارند. در این قانون -که مرتبط‌ترین قانون ایران درزمینهٔ داده‌ها و حریم خصوصی به‌شمار می‌آید- هیچ اشاره یا تلاشی برای چارچوب‌گذاری قوانین دربارهٔ ابرداده‌ها و حریم خصوصی صورت نگرفته

است. در ادامه، سعی شده است تا نگرش اتحادیهٔ اروپا به ابرداده و حریم خصوصی برای فهم ادعای بالا مورد تحلیل قرار گیرد.

٤-نگرش اتحادیهٔ اروپا به ابرداده و حریم خصوصی:

سه رویکرد را می‌توان در رابطه با ابرداده و مدیریت آن در حوزهٔ حریم خصوصی در قوانین اتحادیهٔ اروپا شناسایی کرد که در ذیل بدان اشاره می‌شود:

۱-٤- رویکرد خدمات‌محور:[1]

تصویب مقررات پیشنهادی حریم خصوصی الکترونیکی، برای محافظت از حقوق اساسی حریم خصوصی و حفاظت از داده‌های شخصی، در عصر دیجیتال بسیار مهم است. حریم خصوصی و حفاظت از داده‌ها ارزش‌های اصلی اتحادیهٔ اروپا هستند که در کنوانسیون اروپایی حقوق بشر[2] و منشور حقوق اساسی اتحادیهٔ اروپا به‌رسمیت شناخته شده‌اند، که باید در تمامی سیاست‌های اتحادیهٔ اروپا طبق این معاهده رعایت شود.

براین اساس، درخصوص حریم خصوصی و ابرداده‌ها در اتحادیهٔ اروپا می‌توان گفت که مقررات حریم خصوصی و ارتباطات الکترونیکی[3] در کنار قانون حفاظت از داده‌ها اتحادیهٔ اروپا[4] قرار دارد که دو قانون نسبتاً مجزا و البته کامل‌کنندهٔ یکدیگر درزمینهٔ ابرداده‌ها و بحث حریم خصوصی هستند. درواقع، مقررات حریم خصوصی و ارتباطات الکترونیکی دستورالعمل اروپایی EC/۵۸/۲۰۰۲ را اجرا می‌کند که به‌عنوان «دستورالعمل حفظ حریم خصوصی الکترونیک» نیز شناخته می‌شود. این نهاد تشخیص می‌دهد که دسترسی گستردهٔ عمومی به شبکه‌های دیجیتال موبایل و اینترنت، فرصت‌های جدیدی را برای کسب‌وکارها و کاربران ایجاد می‌کند، اما در عین حال خطرات جدیدی را برای حریم خصوصی آنان به همراه دارد. اتحادیهٔ اروپا در حال جایگزینی قانون فعلی حریم

1 A service-centric approach
2 European Convention on Human Rights
3 The Privacy and Electronic Communications Regulations (PECR)
4 The General Data Protection Regulation(GDPR)

خصوصی الکترونیکی با مقررات جدید حریم خصوصی الکترونیکی[۱] است تا این مقررات در کنار نسخهٔ اروپاییِ قانون حفاظت از داده‌ها قرار گیرد.ازجمله ویژگی‌های این دستورالعمل عبارت است از؛ تضمین امنیت خدمات ارتباطات الکترونیکی، تضمین محرمانگی ارتباطات در خصوص داده‌های عبوری، لزوم بی‌نام بودن داده‌های عبوری، لزوم ارائهٔ صورت‌حساب کامل ازسوی ارائه‌دهندگان خدمات اینترنتی، لزوم کسب رضایت برای پردازش داده‌های ثابت کاربران و مواردی دیگر از این دست هستند[۲].

هدف از وضع دستورالعمل مذکورکه درجهت تکمیل سایر دستورالعمل‌ها در این زمینه تنظیم شده است، احترام به حقوق اساسی اشخاص به‌ویژه حقوق مندرج در موادّ ۷ و ۸ منشور حقوق اساسی اتحادیهٔ اروپا ونیز کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی اشخاص است[۳].

در یک رویکرد خدمات محور برای توسعهٔ دامنهٔ قوانین حریم خصوصی ارتباطات الکترونیکی، در رابطه با مدیریت شایستهٔ حریم خصوصی در قبال ابرداده‌ها، محدودهٔ قوانین براساس خدمات مختلف مشخص می‌شود. به‌طور خلاصه، چنین قوانینی فقط برای انواع خاصی از شرکت‌هایی که در بازارهای ارتباطات الکترونیکی مربوطه فعالیت می‌کنند اعمال می‌شود. درواقع، دستورالعمل حفظ حریم خصوصی الکترونیکی عمدتاً از یک رویکرد خدمات‌محور استفاده می‌کند. دلیل اصلی این محدودهٔ خاص، پیشینهٔ دستورالعمل به‌عنوان بخشی از چارچوب نظارتی برای بازارهای ارتباطات الکترونیکی است[۴]. (یکی از ویژگی‌های اصلی این چارچوب نظارتی، شناخت ویژگی‌های خاص بازار شبکه‌ها و خدمات ارتباطات الکترونیکی و ارزش آن‌ها برای کاربران و جامعه است. این چارچوب،

---

1 ePR

۲ زرکلام، ستار، «حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا)»، *پژوهش‌های حقوق اسلامی*، شمارهٔ ۲۵، (۱۳۸۶)، ص ۱۸۴ .

۳ قناد، فاطمه، «حمایت از داده پیام‌های شخصی در بستر تجارت الکترونیکی»، *تحقیقات حقوقی*، شمارهٔ ۵۶، (۱۳۹۰)، ص ۸۱۶.

4 Schnabel, C., ‘Privacy and Data Protection in Electronic Communications Law’, in C. Koenig, et al. (eds), EC Competition and Telecommunications Law, Kluwer Law International.(2009), p 509-568.

پویایی‌های خاص ورود به بازار و اثرات شبکه را در صنعت مخابرات شناسایی می‌کند. هدف این چارچوب تقویت رقابت بین خدمات مربوطه و در عین حال فراهم کردن اتصال و قابلیت همکاری شبکه‌ها و خدمات است[1] .(

در مجموع، نقطهٔ قوت اصلی رویکرد خدمات‌محور در محدودهٔ قوانین حریم خصوصی ارتباطات الکترونیکی، امکان تعیین محدوده‌ای روشن و واضح است. بحث دیگری که به نفع رویکرد خدمات‌محور مطرح می‌شود، این است که داشتن قوانین ویژه برای زیرساخت‌های ارتباطی منطقی به‌نظر می‌رسد؛ زیرا آن‌ها در موقعیتی هستند که می‌توانند در سطحی متفاوت از خدماتی که صرفاً از زیرساخت استفاده می‌کنند، با حریم خصوصی ارتباطات افراد تداخل داشته باشند. ضعف اصلی یک رویکرد خدمات‌محور این است که چنین رویکردی می‌تواند از دیدگاه کاربر منجر به تفاوت‌های دلخواه بین حفاظت از حریم خصوصی قابل اعمال برای سرویس‌های عملکردی مشابه شود. در این رویکرد، تمرکز اصلی بر ارائهٔ یک **خدمت ارزشمند و بی‌دردسر** به کاربر است. حفاظت از حریم خصوصی و ابرداده‌ها، بخشی از کیفیت آن خدمت محسوب می‌شود.

رژیم خاص دستورالعمل حریم خصوصی الکترونیکی برای ابرداده‌ها در مادهٔ ۵، ۶ و ۹ تقریباً به شرح زیر است:

برای پردازش ابرداده‌ها توسط سرویس‌های تنظیم‌شده، رضایت کاربر یا مشترک لازم است، مگر اینکه استثنای مشخصی اعمال شود. ابرداده‌ها در این قانون، «هر داده‌ای است که به‌منظور انتقال یک ارتباط در یک شبکه ارتباطات الکترونیکی یا برای صدور صورت‌حساب پردازش می‌شود».[2] نمونه‌هایی از ابرداده‌ها، زمان برقراری ارتباط، و اطلاعات آدرس‌دهی افراد درگیر در یک ارتباط، مانند آدرس ایمیل یا آدرس IP مورد استفاده برای دسترسی به اینترنت است. با فناوری ارتباطات مدرن، مرز بین داده‌های ترافیکی و محتوای ارتباطات به‌طور فزاینده ای مبهم شده است. برای مثال، موضوع یک

1 Alexiadis ,e.g. & P. & M. Cave, 'Regulation and Competition Law in Telecommunications and Other Network Industries', in: R. Baldwin, M. Cave & M. Lodge (eds.), The Oxford handbook of Regulation, Oxford University Press,(2010), p. 3-4.

2 Article 2(b) of the e-Privacy Directive.

پیام ایمیل می‌تواند هم به‌عنوان ابرداده‌ها و هم محتوای ارتباطی دیده شود. نظارت بر ابرداده‌های ارتباطات در طول زمان می‌تواند تصویری دقیق از زندگی افراد ارائه دهد[1].

قانون عمومی حفاظت از داده‌ها در ۲۵ مه ۲۰۱۸ اجرایی شد و مجموعه‌ای از قوانین حفظ حریم خصوصی داده‌ها را در بر می‌گیرد که شامل ذخیره‌سازی، انتقال و به اشتراک‌گذاری داده‌ها، هم در داخل و هم در خارج از اتحادیهٔ اروپا و گسترش به منطقهٔ اقتصادی اروپا می‌شود. مقررات عمومی حفاظت از داده‌هامسئولیت بیشتری را بر عهدهٔ مؤسسات برای محافظت از حریم خصوصی داده‌های شخصی می‌گذارد، مانند اطمینان از وجود یک کنترل‌کنندهٔ داده برای نظارت بر امنیت داده‌ها. علاوه‌بر این، «حریم خصوصی با طراحی» مقررات عمومی حفاظت از داده‌ها ایجاب می‌کند که حفاظت از داده‌ها باید در مرحلهٔ طراحی مطالعه مورد بحث و اجرا قرار گیرد. یکی از قوی‌ترین پیام‌های ذاتی مقررات عمومی حفاظت از داده‌ها اتحادیهٔ اروپا این است که افراد، کنترل بسیار بیشتری بر داده‌های خود دارند. این به بهترین وجه در قانون مقررات عمومی حفاظت از داده‌ها برجسته شده است که مستلزم برخورداری افراد از «حقّ فراموش شدن» است. «حق فراموش شدن»[2] اساساً به این معنی است که یک فرد می‌تواند درخواست کند که تاریخچهٔ تحقیقاتی کامل کاغذی و الکترونیکی آن‌ها برای یک سازمان خاص «پاک شود»[3] براساس این قانون، هنگامی که یک شرکت‌کننده که در اتحادیهٔ اروپا زندگی می‌کند «حقّ فراموش شدن» خود را استناد می‌کند، هرگونه اطلاعات شخصی و شناسایی‌نشده پاک می‌شود یا از بین می‌رود. می‌توان استدلال کرد که اگر فردی حق دارد داده‌های خود را حذف کند یا از بین ببرد، «کنترل‌کنندگان داده» هستند. بااین‌حال، «حقّ فراموش شدن» قانون عمومی حفاظت از داده‌ها درمورد داده‌های کاملاً ناشناس منتشرشده اعمال نمی‌شود. داده‌های کاملاً ناشناس حاوی پیوند کدگذاری‌شده نیستند، که این امکان را می‌دهد تا داده‌ها به

1 Breyer P., ‘Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR’, European Law Journal, Vol. 11, No. 3.(2014), p. 365-375.

2 Right to be Forgotten

۳ توحیدی، احمدرضا؛ شریفی‌کیا، محمدعلی، «محدوده اعمال حق بر فراموشی در فضای سایبر با تمرکز بر رویه دیوان دادگستری اتحادیه اروپا». *پژوهش حقوق خصوصی*، دورهٔ ۱۲، شمارهٔ ۴۷، (۱۴۰۳)، ص ۲۳۴ .

یک فرد خاص ردیابی شوند. قانون عمومی حفاظت از داده‌ها به‌وضوح برای هر پردازش داده‌های مربوط به افراد در اتحادیهٔ اروپا، یا هر نظارت بر افراد در اتحادیهٔ اروپا، صرف‌نظر از اینکه کنترل‌کننده در کجا مستقر است، به‌طور کامل اعمال می‌شود. انبوهی از خصوصی‌ترین اطلاعات به‌وسیلهٔ خدمات ارتباطی جمع‌آوری می‌شود که به‌صورت جداگانه یا به‌عنوان بخشی از رسانه‌های اجتماعی یا سایر بسترهای اینترنتی ارائه می‌شود. اینها فواره‌های دیجیتالی هستند که اطلاعات بسیار دقیقی دربارهٔ زندگی ما از آن‌ها به‌دست می‌آید. داده‌های موقعیت مکانی هر حرکتی را نشان می‌دهد، نشان می‌دهد که ما کجا زندگی می‌کنیم، کار می‌کنیم و خرید می‌کنیم، در کدام کافه‌ها و رستوران‌ها شرکت می‌کنیم، در کدام رویدادهای سیاسی شرکت می‌کنیم، به کدام خدمات پزشکی نیاز داریم. چنین ابرداده‌هایی درمورد زمان، تعداد دفعات و با چه کسی پیام‌ها و تماس‌ها را ردّ و بدل می‌کنیم، موقعیت اجتماعی ما را آشکار می‌کند: چه کسانی دوستان خوبی هستند، چقدر با اعضای خانواده‌مان صمیمی هستیم، چقدر در محل کار یا با تماس‌های خصوصی وقت می‌گذرانیم. تمامی این اطلاعات و بسیاری موارد دیگر را می‌توان بدون نگاه کردن به محتوای اطلاعات جمع‌آوری کرد. این اطلاعاتی است که مردم حق دارند انتظار داشته باشند بیشترین میزان کنترل را بر آن داشته باشند. در اتحادیهٔ اروپا، مقررات عمومی حفاظت از داده‌ها[1] قوانین جامعی را برای پردازش داده‌های شخصی ارائه می‌کند. علاوه‌بر این، قانونگذار اتحادیهٔ اروپا در نظر دارد قوانین خاصی را برای حفاظت از محرمانگی ارتباطات، مقرراتی جداگانه برای حفظ حریم خصوصی الکترونیکی وضع کند. در یک جمع‌بندی می‌توان بیان داشت در یک نظام خدمات‌محور، **سازمان‌ها و کسب‌وکارها به‌عنوان ارائه‌دهندگان خدمت تلقی شوند** که موظفند با شفافیت، پاسخ‌گویی و ایجاد امکان کنترل برای کاربران، از داده‌های آنان محافظت کنند، **قوانین، چارچوبی را فراهم می‌کنند** تا این خدمات به بهترین شکل ارائه شوند، نه اینکه صرفاً لیستی از ممنوعیت‌ها باشند. **طراحی برای حریم خصوصی، ابزارهای عملی مانند پرتابل بودن ابر داده‌ها،** به‌عنوان بخشی از خدمت به کاربر در نظر گرفته می‌شوند. یکی از

1 the General Data Protection Regulation (GDPR)

اصول حاکم بر این رویکرد شفاف‌سازی است یعنی خدمت‌دهنده موظف است به زبان ساده و قابل درک به کاربر اطلاع دهد که چه ابرداده‌هایی جمع‌آوری می‌شود، هدف از این کار چیست و چگونه از آن محافظت می‌شود. و از دیگر اصول حاکم بر این رویکرد می توان به رضایت آگاهانه(بدون اجبار)، حداقل دسترسی و ارزش متقابل اشاره کرد. در نظام حقوقی ایران نیز، کمیسیون عالی تنظیم مقررات فضای مجازی کشور در تاریخ ۱۴۰۲/۱۰/۱۱ باتوجه به رویکرد نظام خدمات‌محور، نسبت به وضع دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوهٔ جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجاز اقدام کرده است، که رعایت اصولی مانند شفاف‌سازی، رضایت آگاهانه، حداقل دسترسی، حقّ فراموش شدن در آن مشهود است، که این دستورالعمل گامی مثبت در راستای حفظ حریم خصوصی اشخاص موضوع داده در حقوق ایران تلقی می‌گردد.

۲-٤- رویکرد داده‌محور[1]

رویکرد دوم برای توسعهٔ دامنهٔ قوانین حفظ حریم خصوصی ارتباطات الکترونیکی، داده‌محوری است. یک رویکرد داده‌محور با تنظیم قوانینی برای جمع‌آوری و استفاده از انواع داده‌های شخصی از منافع حریم خصوصی محافظت می‌کند[2]. یک رویکرد داده‌محور به مقررات حریم خصوصی در قلب حداقل صد قانون حفظ حریم خصوصی داده در سراسر جهان قرار دارد[3]. (برای مثال، دستورالعمل کلی حفاظت از داده‌ها در صورتی اعمال می‌شود که «داده‌های شخصی» پردازش شوند.[4]

نمونهٔ دیگری از رویکرد داده‌محور به قوانین محدوده، رژیم سختگیرانه برای «دسته‌های خاص» داده‌های شخصی (که داده‌های حساس نیز نامیده می‌شود) در

1 A data-centric approach
2 R. Clarke ‘Beyond the OECD guidelines: Privacy protection for the 21st Century’, , www.rogerclarke.com/DV/PP21C.html .(2015), p. 1.
3 Greenleaf ‘Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories’, Journal of Law, Information & Science, Vol. 23, No. 1.(2013), p. 3.
4 See article 3(1) of the Data Protection Directive

دستورالعمل حفاظت از داده‌ها است. دسته‌بندی‌های ویژهٔ داده‌ها به‌عنوان «داده‌های شخصی که منشأ نژادی یا قومیتی، عقاید سیاسی، اعتقادات مذهبی یا فلسفی، عضویت در اتحادیهٔ‌های کارگری، و (...) اطلاعات مربوط به سلامت یا زندگی جنسی را آشکار می‌کند، تعریف می‌شوند. [۱]پردازش این دسته از داده‌ها اصولاً ممنوع است، مگر اینکه استثنایی قانونی مانند ضرورت پزشکی اعمال شود. [۲]یک کشور عضو می‌تواند با دادن «رضایت صریح» به افراد موضوع داده اجازهٔ لغو این ممنوعیت را بدهد[3] .

رویکرد داده‌محور نقاط ضعفی دارد. قانون با تمرکز صرفاً بر تنظیم پردازش داده‌های شخصی، ممکن است هدف نهایی یعنی محافظت از مردم و رفاه اجتماعی را نادیده بگیرد. براین اساس، زمانی که اطلاعات خاص «شخصی» می‌شوند، تعیین اطلاعات به‌طور فزاینده‌ای دشوار است. افزون‌بر این، قوانین مربوط به پردازش منصفانهٔ داده‌های شخصی می‌تواند نسبت به ابزارهای استخراج یا ضبط داده‌ها حساس نباشد. علاوه‌بر این، حتی درصورتی‌که هیچ اطلاعات شخصی درمورد یک شخص خاص ضبط نشده باشد، ممکن است همچنان عدم تعادل قدرت وجود داشته باشد که نیاز به مداخلهٔ نظارتی دارد[۴].(

در عین حال، گسترش جمع‌آوری داده‌ها، حقوق مهم حریم خصوصی را به خطر می‌اندازد. در آوریل ۲۰۱۴، در پروندهٔ «حقوق دیجیتال ایرلند» دادگاه دادگستری اروپا[۵] دستورالعمل حفظ داده‌ها را لغو کرد، یک قانون اتحادیهٔ اروپا که به ارائه‌دهندگان خدمات مخابراتی اجازه می‌داد تا ابرداده‌ها را از ایمیل‌ها، پیام‌های متنی و تماس‌های تلفنی شهروندان اتحادیهٔ اروپا حفظ کنند. به مدت دو سال، متوجه شد که نتوانسته است الزامات تناسب طبق قوانین اتحادیهٔ اروپا را برآورده کند. به‌طور مشابه، در اکتبر ۲۰۱۵، در پروندهٔ «Maximillian Schrems v» دولت بدون «حفاظت کافی» حقوقی را که توسط دستورالعمل حفاظت از داده‌های اتحادیهٔ اروپا محافظت می‌شود، نقض کرد. این تصمیم‌ها

1 See article 8(1) of the Data Protection Directive.
2 See article 8(c) of the Data Protection Directive.
3 See article 8(2)(a) of the Data Protection Directive.
4 Bennett, C.J, 'In Defence of Privacy: the concept and the regime', Surveillance & Society , Vol. 8, No. 4, ,(2011), pp. 485-496.
5 ECJ

نتیجهٔ دادگاه‌های اروپایی بود که حقوق حریم خصوصی داخلی را درمقابل نگرانی‌های امنیتی جهانی و منافع بازار متعادل می‌کردند. در دستورالعمل حفاظت از داده‌های اتحادیهٔ اروپا[1]، حقّ حفظ حریم خصوصی به‌عنوان یک «حق و آزادی اساسی»[2] توصیف شده است. این احساس در سایر اسناد برجستهٔ اتحادیهٔ اروپا مانند کنوانسیون حمایت از حقوق بشر و آزادی‌های اساسی[3] نیز منعکس شده است. باوجود برخورد بسیار متفاوت با حقّ حفظ حریم خصوصی در ایالات متحده و اتحادیهٔ اروپا، افراد در عصر انتقال اطلاعات سریع و یک اقتصاد جهانی به‌هم‌پیوسته زندگی می‌کنند که در آن اشتراک گذاری داده‌های خصوصی در سراسر مرزها ضروری است. بنابراین، استانداردهای حفاظت از اطلاعات شخصی راه‌حل‌های قانونی را برای نقض حقوق موضوع داده‌ها ایجاد می‌کند و با تأکید بر عدالت رویه‌ای، ضمن رسیدگی به جمع‌آوری، پردازش، و تبادل اطلاعات و توسعهٔ حقوقی عملی، به توسعهٔ قانون حفاظت از اطلاعات شخصی اصولی مانند محدودیت شیء[4] کمک می‌کند[5]. (از ویژگی‌های بارز رویکرد داده‌محور می‌توان به **تمرکز بر چرخهٔ حیات کامل داده، طبقه‌بندی داده‌ها براساس حساسیت، تعریف روشن نقش‌ها و مسئولیت‌ها مانند کنترل کنندهٔ داده و یا پردازشگر داده اشاره کرد.** در این رویکرد، تمرکز اصلی بر **خود داده و ارزش اقتصادی و تحلیلی** آن است. ابرداده‌ها به‌عنوان یک **دارایی ارزشمند** تلقی می‌شوند که باید مدیریت، تحلیل و درنهایت به‌منظور ایجاد ارزش اقتصادی از آن‌ها بهره‌برداری شود. از اصول حاکم بر این رویکرد می‌توان به مالکیت وکنترل، امنیت، حاکمیت ابرداده‌ها، بهینه‌سازی برای تحلیل اشاره کرد. البته ممکن است در این رویکرد اصل حداقل دسترسی نادیده گرفته شود و به‌نوعی حریم خصوصی شخص را خدشه‌دار کند. در نظام حقوقی ایران به‌طور کلی بین «داده‌های شخصی» و «داده‌های حساس» تمایز نظام‌مند قائل نمی‌شوند. برای مثال، داده‌های

1 Directive
2 fundamental right and freedom
3 the Convention for the Protection of Human Rights and Fundamental Freedoms
4 object limitation
5 PARK, SEONUK, A Comparative Analysis of US and EU Data Privacy Laws, Publisher : The Institute for Legal Studies Dong-A University, (83,(2019),), pp.269-310.

مربوط به سلامت، گرایش‌های سیاسی یا عقاید مذهبی در زمرهٔ داده‌های دارای حمایت ویژه قرار نمی‌گیرند؛ و همچنین تعریف و تفکیک مسئولیتی میان کنترل‌کنندهٔ داده با پردازشگر داده وجود ندارد. حمایت از داده‌ها در ایران عمدتاً «حوزه‌ای» است؛ یعنی، برای بخش‌های خاص مانند **بانکداری** (قانون مقررات حفاظت از اسرار بانکی)، پزشکی (قانون اخلاق پزشکی)، مقررات ویژه‌ای وجود دارد؛ امری که موجب می‌شود جنبهٔ حمایتی قانون فراگیر نباشد. درحالی‌که اتخاذ رویکرد داده‌محور، سبب اعتماد، کاهش تبعیض و افزایش امنیت حقوق کاربران در تمامی حوزه‌ها خواهد بود.

۳-٤ رویکرد ارزش‌محور[1]

تلفن‌های همراه به یکی از محبوب‌ترین دستگاه‌ها برای حفظ ارتباطات اجتماعی و همچنین ثبت اطلاعات دیجیتال درمورد زندگی شخصی تبدیل شده‌اند. حریم خصوصی ابرداده‌هایی که در این فرایند تولید می‌شوند، موضوع بحث‌های شدید در چند سال گذشته بوده است، اما بیشتر بحث بر روی سنگ‌اندازی چنین داده‌هایی متمرکز شده است. در عین حال، چنین ابرداده‌ای پیش‌تر برای استنباط خودکار ترجیحات کاربر برای محصولات تجاری، رسانه‌ها یا آژانس‌های سیاسی مورداستفاده قرار گرفته است. بنابراین رویکرد سوم برای توسعهٔ محدودهٔ چارچوب حریم خصوصی ارتباطات الکترونیکی، ارزش‌محور است و بر ارزش‌های اجتماعی اساسی که نیاز به حفاظت دارند، تمرکز دارد. این ارزش‌ها شامل حقّ زندگی خصوصی و محرمانگی ارتباطات و همچنین پردازش منصفانهٔ داده‌های شخصی مرتبط با ارتباطات است که از طریق منشور حقوق اساسی اتحادیهٔ اروپا و کنوانسیون اروپایی حقوق بشر محافظت می‌شود. همان‌گونه که در مقدمهٔ آن آمده است، دستورالعمل فعلی حریم خصوصی الکترونیکی بر این ارزش‌های اساسی درزمینهٔ ارتباطات الکترونیکی تمرکز دارد. هدف این دستورالعمل، محافظت از داده‌ها و حقوق حریم خصوصی در چارچوب منشور حقوق اساسی اتحادیهٔ اروپا است[2].(

1 A value-centric approach

2 . McCullagh, ‘The social, cultural, epistemological and technical basis of the concept of’ ‘private’ data’, PhD thesis University of Manchester.(2015), p. 189.

علاوه‌بر محافظت از محرمانگی ارتباطات خصوصی، دستورالعمل حفظ حریم خصوصی الکترونیک محدودیت‌های خاصی را برای پردازش ابرداده‌های مرتبط با ارتباطات، ارائه می‌کند. این حمایت‌های خاص باید در پرتو حقّ اساسی برای حفاظت از داده‌های شخصی، در منشور حقوق اساسی اتحادیهٔ اروپا دیده شود[1]. علاوه‌بر این، ابرداده‌های ارتباطات الکترونیکی در محدودهٔ حقّ ارتباطات خصوصی در کنوانسیون اروپایی حقوق بشر و منشور حقوق اساسی اتحادیهٔ اروپا قرار می‌گیرند.[2] ارزش‌هایی که در حال حاضر در دستورالعمل حفظ حریم خصوصی الکترونیکی مورد تأکید قرار نگرفته‌اند، آزادی بیان و آزادی برقراری ارتباط به‌طور کلی است. این مقادیر به‌طور خاص در دستورالعمل فعلی حفظ حریم خصوصی الکترونیکی ذکر نشده است. بااین‌حال، اعمال مؤثر حقّ آزادی بیان به‌طور فزاینده‌ای به دسترسی به شبکه‌های ارتباطات الکترونیکی و شرایطی که تحت آن دسترسی می‌تواند رخ دهد، ازجمله حفاظت از حریم خصوصی و داده‌های شخصی، وابسته است. از طرف دیگر قانون عمومی حفاظت از داده‌ها برای هر سازمانی که داده‌های شخصی از اتحادیهٔ اروپا را پردازش می‌کند -صرف‌نظر از اینکه پردازش آن در کجا انجام می‌شود- اعمال می‌گردد. این بدان معناست که قانون عمومی حفاظت از داده‌ها می‌تواند برای هر سازمانی در هر نقطه از جهان اعمال شود و همهٔ سازمان‌ها باید تجزیه و تحلیل انجام دهند تا مشخص شود که آیا داده‌های شخصی اتحادیهٔ اروپا را پردازش می‌کنند یا خیر. در آخر در پاسخ به این پرسش که، آیا داده‌های شخصی ابرداده مشمول قانون عمومی حفاظت از داده‌ها هستند؟ می‌توان گفت که در این راستا متادیتا مشخص کرده است که مشمول رعایت قانون عمومی حفاظت از داده‌ها است.

از ویژگی‌های برجستهٔ رویکرد ارزش‌محور این است که حقوقی مثل حقّ دسترسی، حقّ اصلاح، حقّ فراموشی و حقّ انتقال‌پذیری داده‌ها را به افراد می‌دهد که کنترل آنان را بر داده‌هایشان تضمین می‌کند. **درواقع** این رویکرد، فراتر از خدمت رفته و براساس

1 Article 8 of the Charter of Fundamental Rights of the European Union.
2 Article 7 of the EU Charter of Fundamental Rights; article 8 of the European Convention on Human Rights. See also: Court of Justice of the EU 8 April 2014, C-293/12 (Digital Rights Ireland).

اصول اخلاقی، فرهنگی و هنجارهای اجتماعی بنا شده است. حریم خصوصی در اینجا خود یک **ارزش ذاتی** است، نه صرفاً یک ویژگی فنی یا خدماتی. از اصول حاکم بر این رویکرد می توان به احترام به کرامت انسانی، اعتماد، عدم تبعیض، مصلحت عمومی اشاره کرد درخصوص نگرش نظام حقوقی ایران به رویکرد ارزش‌محور، شاید بتوان به سند حمایتی و تنظیم مقررات حریم خصوصی کاربران مصوب (۱۳۹۶) اشاره کرد. این سند، یک استثنا و گامی به جلو محسوب می‌شود. در مقدمه و اصول این سند، به‌صراحت به «حقوق کاربران» و اصولی مانند «رضایت آگاهانه»، «حداقل‌سازی داده» و «امنیت» اشاره شده است. این سند از نظر گفتمانی به رویکرد ارزش‌محور نزدیک است، اما **به دلیل فقدان ضمانت اجرای قوی و قانونی شدن کامل، هنوز نتوانسته است فرهنگ حقوقی حاکم را تغییر دهد.**

اتحادیهٔ اروپا در قالب سه رویکردی که در بالا مورد اشاره قرار گرفته است، سعی کرده است تا در ساختن قوانینی نو قدم بردارد؛ البته در سال‌های اخیر، تلاش‌های اتحادیهٔ اروپا درزمینهٔ ابرداده‌ها و حریم خصوصی، تداوم پیدا کرده است. مقررات حریم خصوصی و ارتباطات الکترونیکی[1] در کنار قانون حفاظت از داده‌ها اتحادیهٔ اروپا[2] درصدد ارائهٔ چارچوبی قانونی بوده‌اند تا شهروندان در سایهٔ آن برحقوق خود آگاه باشند. مقررات جدید حریم خصوصی الکترونیکی[3] نیز باتوجه به گسترش فناوری و کسب‌وکارهای جدید در دستور کار قرار گرفته است. از این جهت در رویکرد خدمات‌محور، ابرداده‌ها، که بیشتر در کسب‌وکارهای بزرگ، کاربردی هستند باتوجه به حریم خصوصی مردم، باید محدوده‌بندی شوند و قوانینی وجود دارد که این داده‌ها، نباید به نشر عمومی برسند. این قضیه درخصوص سرویس‌دهی به مشتری، در مادهٔ ۵، ۶ و ۹ رژیم خاص دستورالعمل حریم خصوصی الکترونیکی برای ابرداده‌ها مورد توجه قرار گرفته است و در قانون عمومی حفاظت از داده‌ها مصوب سال ۲۰۱۸ نیز دوباره مورد تأکید واقع شده است.

1 The Privacy and Electronic Communications Regulations (PECR)
2 The General Data Protection Regulation(GDPR)
3 ePR

در رویکرد داده‌محور، قوانین اتحادیهٔ اروپا، حریم خصوصی را به‌منزلهٔ یک حق و آزادی اساسی می‌شناسند و این حق را به آن‌ها می‌دهند که صاحب اطلاعاتی در مسائل شخص خود باشند؛ ازاین‌رو، ابرداده‌هایی که در مراکزی مانند بیمارستان‌ها، از اشخاص مختلف وجود دارند نباید بدون اجازهٔ آن‌ها منتشر شوند. رویکرد ارزش‌محور نیز داده‌های شخصی هر فرد را محترم و مختص به خود او در نظر می‌گیرد. در اتحادیهٔ اروپا در قالب قوانین تلاش‌هایی شده است و البته تداوم این تلاش‌ها درزمینهٔ حریم خصوصی و ابرداده‌ها، نشان از توجهٔ قانونگذار در این نهاد منطقه‌ای دارد. کمااینکه در سال ۲۰۲۳ نیز قانونی دیگر به نام قانون داده‌های اتحادیهٔ اروپا[1] توسط شورای اتحادیهٔ اروپا در جهت حفاظت از حریم خصوصی افراد جامعه در مقابل اطلاعات و داده‌ها، مورد تصویب قرار گرفت. اهمیت توجه به این قوانین نشان از فهم قانونگذار اتحادیهٔ اروپا از مسائل جدید در عصر ابرداده‌ها دارد؛ مسئله‌ای که در ایران کمتر مورد توجه قرار گرفته است.

نتیجه‌گیری

در حقوق داخلی، هیچ اشاره‌ای به ماهیت و جایگاه ابرداده‌ها در گسترهٔ حریم خصوصی نشده است و تنها در چند قانون به‌طور کلی به حریم خصوصی و داده‌ها پرداخته شده است که نیاز به تجدید نظر اساسی و بازیابی احساس می‌گردد. شرکت‌ها و حتی سیستم بانکی در ایران هنوز نه امنیت کافی دارند و نه به اقدامات کافی برای حمایت از حقوق مصرف کننده درزمینهٔ حفاظت از داده‌ها در معاملات آنلاین مجهز شده‌اند. سیاست‌های حفظ حریم خصوصی آن‌ها ناامن است و با تعهدات قانونی مطابقت ندارد و همچنین برای مصرف‌کنندگان مضر است. مفاد قانون تجارت الکترونیک برای محیط الکترونیکی مناسب و به‌روز نیست وحفاظت از داده‌های تجاری را نیز پوشش نمی‌دهد. قانون درمورد حفاظت از داده‌های افراد زیر سنّ قانونی و به‌ویژه کودکان سکوت کرده است. علاوه‌بر این، به اقدامات فنی و سازمانی کارآمد در تراکنش‌های آنلاین اشاره‌ای نمی‌کند و نیز شرایط استثنایی -مانند منافع عمومی- را که در آن داده‌ها ممکن است بدون رضایت

1 the EU Data Act

موضوع داده به‌دست آیند، روشن نمی‌کند. همچنین، درمورد داده‌های شخصی مربوط به افتراهای مجرمانهٔ افراد سکوت می‌کند. با این وصف، نظام حقوقی ایران فاقد یک **قانون جامع درمورد حفاظت از ابرداده‌ها** است که به‌طور شفاف، حقوقی مانند؛ حقّ فراموش شدن، حقّ جابه‌جایی داده‌ها، نحوهٔ انتقال داده به خارج از کشور و سازوکارهای دقیق شکایت و جبران خسارت را پیش‌بینی کرده باشد. درحالی‌که در حقوق اتحادیهٔ اروپا قوانین حریم خصوصی ارتباطات الکترونیکی و ابرداده، دارای یک چارچوب بسیار پیشرفته، جامع و اجرایی است، و با سه رویکرد (۱) خدمات‌محور، (۲) داده‌محور، و (۳) ارزش‌محور، و باتوجه به اصول حاکم بر این رویکردها مانند اصل شفاف سازی، اعتماد، عدم تبعیض، مالکیت وکنترل، امنیت، حداقل دسترسی، رضایت آگاهانه در حال توسعه است، که موجد حقّ دسترسی، حقّ اصلاح، حقّ فراموشی(حذف)، حقّ محدودیت پردازش، حقّ انتقال‌پذیری داده و حقّ اعتراض برای اشخاص است. اگرچه هریک از رویکردها دارای نقاط قوت و ضعف هستند، اما تمرکز هر سه رویکرد بر حفظ حریم خصوصی شهروندان در مقابل ابرداده‌ها بوده است. این مسئله به‌وضوح در قوانین اتحادیهٔ اروپا، مورد توجه قرار گرفته است ولی نظام حقوقی ایران، به‌غیر از وضع دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوهٔ جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجاز که با رویکرد خدمات‌محور تدوین شده‌اند، چندان درزمینهٔ اهمیت ابرداده و حریم خصوصی در عصر جدید ورود پیدا نکرده است، و قوانین موجود هنوز در مراحل اولیه و فاقد جزئیات اجرایی و نهاد ناظر مستقل است. ازاین‌رو، تدوین قانون جامع مشابه GDPR، ایجاد نهاد ناظر مستقل، یا الزام شرکت‌ها به شفافیت در سیاست‌های حریم خصوصی یا تصویب یک قانون خاص و جامع با بهره‌گیری از رویکردی‌های یادشده در قوانین اتحادیهٔ اروپا خصوصاً مقررات عمومی حفاظت از داده‌ها که متضمن حقوق اشخاص موضوع داده است، پیشنهاد می‌شود.

تعارض منافع

تعارض منافع وجود ندارد.

ORCID

Hossein Khanlari Bahnamiri https://orcid.org/0000-0002-9706-2296

Mohammad Hossein Taghipour Darzinaghibi https://orcid.org/0000-0003-4804-5681

Hamed Agha Amini Fashami https://orcid.org/0009-0004-5144-037X

منابع

الف- فارسی

کتاب‌ها:

- جعفری لنگرودی، محمدجعفر، *ترمینولوژی حقوق*، چاپ سیزدهم، (تهران: گنج دانش، ۱۳۸۲).
- دهخدا، علی‌اکبر، *لغت‌نامه دهخدا*، جلد ششم، چاپ دوم، (تهران: دانشگاه تهران، ۱۳۷۷).
- کاتوزیان، ناصر؛ رحیمی، حبیب‌الله، *آزادی اندیشه و بیان*، چاپ اول، (تهران: دانشگاه تهران، ۱۳۸۲).

مقالات:

- الماسی، علی؛ محمدیان شیرمرد، مرضیه، «ملاک‌های حریم خصوصی در فقه امامیه و حقوق اساسی ایران: تطبیق با خودروی شخصی». *مطالعات فقهی‌حقوقی زن و خانواده*، دورهٔ ۲، شمارهٔ ۳، صص ۲۹–۵۲، (۱۳۹۸).
- انصاری، باقر؛ عطار، شیما، «حمایت از داده‌ها در چین، مطالعه تطبیقی با رویکرد حمایت از داده‌ها در آمریکا و اتحادیه اروپا»، *مطالعات حقوق تطبیقی*، دورهٔ ۱۳، شمارهٔ ۱، صص. ۹۱–۱۱۳، (۱۴۰۱).
- بادینی، حسن؛ کرمی، حمزه. «بررسی تطبیقی مسئولیت‌های نهاد متقاضی پردازش، کنترل‌گر و پردازش‌گر تحت مقررات اروپایی حمایت از داده‌های شخصی و لایحه صیانت و حفاظت از داده‌های شخصی»، *تحقیقات حقوقی*، شمارهٔ ۹۵، صص. ۱۳۷–۱۵۸، (۱۴۰۰).

- بخشایشی بایقوت، محرم؛ حیدری منور، حسین، «حریم خصوصی در حقوق ایران و اسناد بین‌المللی»، *مطالعات بین‌المللی پلیس*، دورهٔ ۸، شمارهٔ ۲۹، صص. ۲۰۷–۲۳۲، (۱۳۹۶).
- بنافی، فرشته، «حفاظت از حق حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی»، *پژوهش حقوق خصوصی*، دورهٔ ۱۲، شمارهٔ ۴۵، صص. ۱۴۹–۱۷۶، (۱۴۰۲).
- توحیدی، احمدرضا؛ شریفی‌کیا، محمدعلی، «محدوده اعمال حق بر فراموشی در فضای سایبر با تمرکز بر رویه دیوان دادگستری اتحادیه اروپا». پژوهش حقوق خصوصی، دورهٔ ۱۲، شمارهٔ ۴۷، صص. ۲۳۱–۲۶۲، (۱۴۰۳).
- حسینی، مهدی؛ برزویی، محمدرضا، «مبانی و مؤلفه‌های فقهی حمایت از حریم خصوصی افراد در فضای مجازی»، مطالعات حقوق بشر اسلامی، شمارهٔ ۱۳، صص. نامشخص.
- زارعیان، داود؛ واحد، فائزه، «بررسی حقوق رگولاتوری‌های حمایت از داده». *رسانه*، شمارهٔ ۱۱۸، صص. ۴۷–۷۲، (۱۳۹۹).
- زرکلام، ستار، «حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا)». *پژوهش‌های حقوق اسلامی*، شمارهٔ ۲۵، صص. ۱۷۳–۱۹۶، (۱۳۸۶).
- شجاعی کاریزکی، مرضیه، «جایگاه حریم خصوصی افراد در حقوق مدنی و قوانین موضوعه ایران»، *دستاوردهای نوین در مطالعات علوم اسلامی*، شماره ۳۳، صص.نامشخص، (۱۳۹۹).
- صفایی، سید حسین؛ جعفری، علی، «رابطه آزادی اطلاعات با حریم خصوصی»، *حقوق اسلامی*، شماره ۳۳، صص.نامشخص، (۱۳۹۱).
- عبدی‌پور، ابراهیم، «رویکرد نظام‌های حقوقی نسبت به نقض حریم خصوصی اطلاعاتی در شبکه‌های اجتماعی مجازی»، *نشریهٔ پژوهشی تطبیقی حقوق اسلام و غرب*، شمارهٔ ۳، صص.نامشخص، (۱۳۹۴).
- علی‌احمدی،حسین؛ شوق‌نیان،آرش، «رعایت حریم خصوصی در فضای مجازی مورد مطالعه :ایران»، *مدیریت فردا*، شمارهٔ ۵۷، صص ۱۴۴-۱۳۵، (۱۳۹۷).
- قناد، فاطمه، «حمایت از داده پیام‌های شخصی در بستر تجارت الکترونیکی»، *تحقیقات حقوقی*، شمارهٔ ۵۶، صص ۸۴۰-۸۰۹، (۱۳۹۰).
- قناد فاطمه؛ علیقلی امیره، «مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی»، *حقوق قراردادها و فناوری‌های نوین*، دورهٔ ۱ ، شمارهٔ ۱ ، صص ۲۹۷–۳۲۲، (۱۳۹۹).

- قناد، فاطمه؛ شریف،الهام، «مطالعه اجمالی حمایت از داده‌های شخصی در نظام حقوقی ایران و سند مقررات عمومی حفاظت از داده‌ها ی اتحادیهٔ اروپا»، *حقوق فناوری‌های نوین*، شمارهٔ ۴(ب)،صص ۱-۱۲، (۱۴۰۰).
- لطیف‌زاده، مهدیه؛ قبولی درافشان، سید محمد مهدی؛ محسنی، سعید؛ عابدی، محمد، «حمایت از دادهٔ شخصی در حقوق اتحادیهٔ اروپا و امکان‌سنجی آن در نظام حقوقی ایران»، *مطالعات حقوق عمومی دانشگاه تهران*، دورهٔ ۵۳، شمارهٔ ۲، صص ۹۸۱-۱۰۰۵، (۱۴۰۲) :doi 10.22059/jplsq.2021.324694.2786
- مجاهد، افشین، «رویکردی تطبیقی بر حریم خصوصی»، *پژوهش‌های حقوق تطبیقی عدل و انصاف*، شمارهٔ ۱۳، صص. نامشخص، (۱۴۰۰).
- موسوی‌طاها، سیدجواد، «مسئولیت مدنی ناشی از نقض حریم خصوصی در نظام حقوقی ایران و بررسی تطبیقی آن با قوانین موضوعه»، *مطالعات علوم اجتماعی*، شمارهٔ ۱، صص. نامشخص، (۱۴۰۰).
- موسی‌زاده، ابراهیم؛ مصطفی‌زاده، فهیم، «نگاهی به مفهوم و مبانی حق بر حریم خصوصی در نظام حقوقی عرفی»، *دانش حقوق عمومی*، شمارهٔ ۲، صص. نامشخص، (۱۳۹۱).

ب- منابع خارجی

23-Alexiadis ,e.g. & P. & M. Cave, ‘Regulation and Competition Law in Telecommunications and Other Network Industries’, in: R. Baldwin, M. Cave & M. Lodge (eds.), The Oxford handbook of Regulation, Oxford University Press,(2010).

24-Beyene, Wondwossen Mulualem . "Metadata and universal access in digital library environments". Library Hi Tech. 35 (2): 210–221,(2017).

25- Bennett, C.J, ‘In Defence of Privacy: the concept and the regime’, Surveillance & Society , Vol. 8, No. 4, pp. 485-496,(2011).

26- Breyer P., ‘Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR’, European Law Journal, Vol. 11, No. 3.(2014).

27-G. Greenleaf ‘Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories’, Journal of Law, Information & Science, Vol. 23, No. 1.(2013)

28-Steiner, Tobias . "Metadaten und OER: Geschichte einer Beziehung (Metadata and OER: [hi]story of a relationship)". Synergie. Fachmagazin für Digitalisierung in der Lehre (in German). 04: 54.(2017).

29-Schnabel, C., ‘Privacy and Data Protection in Electronic Communications Law’, in C. Koenig, et al. (eds), EC Competition and Telecommunications Law, Kluwer Law International.(2009)

30-R. Clarke ‘Beyond the OECD guidelines: Privacy protection for the 21st Century’, , www.rogerclarke.com/DV/PP21C.html .(2015).

31-Rouse, Margaret . "Metadata". WhatIs. TechTarget.(2014)

32-PARK, SEONUK, A Comparative Analysis of US and EU Data Privacy Laws, Publisher : The Institute for Legal Studies Dong-A University, (83), pp.269-310,(2019).

33-K. McCullagh, ‘The social, cultural, epistemological and technical basis of the concept of’ ‘private’ data’, PhD thesis University of Manchester.(2015).

34-Mulligan, D. K., Koopman, C., & Doty, N. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy.

Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, 374(2083).(2016).

35-Munir, Bakar A, Yasin, Mohd SH , Information and Communication Technology Law: State, Internet and Information, Legal and Regulatory Challenges. Sweet and Maxwell Asia, Kuala Lumpur.(2010).

36-Wolff, Josephine . "Newly Released Documents Show How Government Inflated the Definition of Metadata". Slate Magazine. (2013).

Translated Persian references

1.Abdipour, Ebrahim, The approach of legal systems towards the violation of information privacy in virtual social networks, Issue 3, Comparative Research Journal of Islamic and Western Law.(2015).

2. Ali Ahmadi, Hossein, Shoqnian, Arash, Respect for privacy in cyberspace, case study: Iran, Journal of Tomorrow's Management, 57, 144-135. (2018).

3-AlMassi, Ali, Mohammadian Shirmard, Marzieh. Privacy Criteria in Imami Jurisprudence and Iranian Fundamental Law: Application to Private Vehicles. Jurisprudential Studies on Women and Family Law, 2(3), 29-52.(2019).

4-Ansari, Baqer, Attar, Shima, Data Protection in China, A Comparative Study with the Approach of Data Protection in the United States and the European Union, Journal of Comparative Law Studies, 13(1), 113-91.(2019).

5-Badini, Hassan, Karami, Hamzeh, A Comparative Study of the Responsibilities of the Data Controller, Controller and Processor under

the European Data Protection Regulations and the Bill on the Protection of Personal Data, Journal of Legal Research, 95, 137-158.(2020).

6-Bakhshaishi Bayqout, Mohamad, Heidari Munawar, Hossein. Privacy in Iranian Law and International Documents. Quarterly Journal of International Police Studies, 8(29), 207-232.(2017).

7. Banafi, Fereshteh, Protection of the Right to Information Privacy Against Threats from Military Artificial Intelligence, Private Law Research, 12 (45), 149-176.(2003).

8.Dehkhoda, Ali Akbar. Dehkhoda Dictionary. Volume 6. Second Edition. Tehran University Press.(2018).

9-Ghannad, Fatemeh, Protection of Personal Data and Privacy in the Context of Electronic Commerce, Journal of Legal Research, 56, 840-809.(2011).

10-Ghannad, Fatemeh, Aligholi Amireh, The Concept and Importance of Personal Data and Privacy and Types of Its Protection in Cyberspace, Contract Law and New Technologies, Volume 1, Issue 1; From Page 297 to Page 322.(2010).

11-Ghannad, Fatemeh and Sharif, Elham, Overview of the Protection of Personal Data in the Iranian Legal System and the General Data Protection Regulation of the European Union, Journal of Law of New Technologies, Issue 4(b), Pages 1-12 ,(2011).

12.Hosseini, Mehdi, and Borzoei, Mohammad Reza, Fundamentals and Jurisprudential Components of Protecting Individuals' Privacy in Cyberspace, Issue 13, Journal of Islamic Human Rights Studies.(2017).

13.Jafari Langroodi, Mohammad Jafar, Legal Terminology, 13th Edition, Ganj Danesh Publications.(2003).

14.Katouzian, Naser and Rahimi, Habibollah, Freedom of Thought and Expression, First Edition, University of Tehran Press. (2003).

15-Latifzadeh, Mahdieh, Qabulif Darafshan, Seyyed Mohammad Mahdi, Mohseni, Saeed, & Abedi, Mohammad. Protection of personal data in European Union law and its feasibility in the Iranian legal system. Quarterly Journal of Public Law Studies, University of Tehran, 53(2), 981-1005. doi: 10.22059/jplsq.2021.324694.2786 , (2012).

16.Mojahed, Afshin, A Comparative Approach to Privacy, Issue 13, Journal of Comparative Law Research, Justice and Fairness. (2001).

17-Mousavi Taha, Seyed Javad, Civil Liability Arising from Violation of Privacy in the Iranian Legal System and Its Comparative Study with Statutory Laws, Issue 1, Journal of Social Science Studies.(2001).

18- Musazadeh, Ebrahim and Mostafazadeh, Fahim, A look at the concept and foundations of the right to privacy in the customary legal system, No. 2, Danesh Haraq Public Journal.(2012).

19.Safaei, Seyed Hossein and Jafari, Ali, The relationship between freedom of information and privacy, Issue 33, Islamic Law Journal.(2012).

20.Shoja Sangchouli, Mehrovieh, Children's right to privacy in Iranian statutory law and the Convention on the Rights of the Child, Law and Modern Studies Winter - Issue 1 (2019).

21-Shojai Karizaki, Marzieh, The position of individuals' privacy in civil law and statutory laws of Iran, Issue 33, Journal of New Achievements in Islamic Sciences Studies.(2019).

22. Tohidi, Ahmad Reza, Sharifi Kia, Mohammad Ali. The Limits of the Right to Be Forgotten in Cyberspace, Focusing on the Case Law of the Court of Justice of the European Union, Private Law Research, 12 (47); 231-262.(2003).

23-Zareyan, Davud, Vaheed, Faezeh, A Study of Data Protection Regulatory Law, Media Journal, 118, 47-72. (2019).

24-Zarkalam, Sattar, Privacy of Internet Communications (Study in Iranian and European Union Law), Journal of Islamic Law Research, 25, 196-173. (2007).

اســـتناد به این مقاله: خانلری بهنمیری، حســـین، تقی پور درزی نقیبی، محمد حســـین و آقا امینی فشـــمی، حامد . (۱۴۰۴). نگرش حقوق ایران و اتحادیهٔ اروپا نســـبت به ابرداده و جایگاه حریم خصـــوصـــی در آن. *پژوهش حقوق خصوصی*، ۱۴ (۵۳)، ۲۰۷-۲۴۶.

doi: 10.22054/jplr.2025.88038.2955