داده‌های شخصی در بطن کلان‌داده‌ها و پایگاه‌های داده: چالش‌های فنی و حقوقی اجرا و تفکیک‌پذیری حقوق کاربران

*
امیرمحمد
قربان نیا

**
زهرا
شاکری

| فصلنامه پژوهشنامه بازرگانی | شماره ۱۱۸ | دوره ۳۰ | بهار ۱۴۰۵ | ۱۶۳-۱۳۷ |

https://doi.org/10.22034/ijts.2026.2069496.4182

| دریافت: ۱۴۰۴/۰۵/۲۹ | بازنگری: ۱۴۰۵/۰۲/۱۶ | پذیرش: ۱۴۰۵/۰۲/۲۱ |

کلیدواژه‌ها

پایگاه داده/ حقوق اشخاص موضوع داده/ داده‌های شخصی/ کلان‌داده/ مالکیت فکری

چکیده[1]

با گسترش فناوری‌های داده‌محور، داده‌های شخصی به‌طور فزاینده در قالب کلان‌داده‌ها و پایگاه‌های داده گردآوری، ذخیره و تحلیل می‌شوند. این ساختارها که برای بهره‌برداری گسترده و هوشمند از اطلاعات طراحی شده‌اند، ضمن ارائه مزایای فراوان برای کسب‌وکارها، چالش‌های بنیادینی در زمینه حقوق اشخاص موضوع داده ایجاد می‌کنند. در محیط‌های کلان‌داده‌ای، داده‌ها به‌شکل انبوه، متنوع و به‌هم‌پیوسته جمع‌آوری می‌شوند و اعمال حقوق فردی نظیر دسترسی، اصلاح، حذف یا انتقال، با موانع فنی و ساختاری جدی روبه‌رو است؛ زیرا تفکیک داده‌های یک شخص از مجموعه داده‌ها اغلب پیچیده یا ناممکن می‌شود. همچنین در پایگاه‌های داده تحت مالکیت شرکت‌ها، داده‌های شخصی بخشی از دارایی اطلاعاتی قلمداد می‌شوند و این امر تعارضی میان حقوق مالکیت فکری شرکت‌ها بر پایگاه داده و حقوق حریم خصوصی اشخاص پدید می‌آورد. پرسش اصلی مقاله آن است که در تقاطع کلان‌داده و پایگاه داده،

*. دانش آموخته کارشناسی ارشد، حقوق خصوصی، دانشگاه تهران، تهران، ایران. amir.ghorbannia@ut.ac.ir

**. دانشیار دانشکده حقوق و علوم سیاسی دانشگاه تهران، تهران، ایران. zshakeri@ut.ac.ir

▪ زهرا شاکری، نویسنده مسئول

چه چالش‌های حقوقی و فنی در تضمین حقوق اشخاص بروز می‌کند و واکنش نظام‌های حقوقی چگونه بوده است؟ مطالعه حاضر با روش توصیفی‌تحلیلی و مبتنی بر منابع کتابخانه‌ای نشان می‌دهد که در حوزه کلان‌داده، هنوز خلا مقررات‌گذاری وجود دارد و اجرای حقوق اشخاص نیازمند قواعد ویژه‌ای است. در پایگاه‌های داده نیز حمایت مالکیت فکری صرفاً به طراحی و سازمان‌دهی پایگاه تعلق دارد و داده‌های شخصی خام همچنان تابع قواعد حریم خصوصی و حفاظت از داده باقی می‌مانند.

طبقه‌بندی JEL: K24, K33, K42, O33, L86

Personal Data within Big Data and Databases: Technical and Legal Challenges in the Enforcement and Separability of Data Subject Rights

Amir mohammad Ghorban nia, Master's Graduate in Private Law, University of Tehran, Tehran, Iran.

Zahra Shakeri, Associate Professor, Faculty of Law and Political Science, University of Tehran, Tehran, Iran. (Corresponding Author)

Vol 30, No. 118, Spring 2026 Journal of Trade Studies (JTS)

https://doi.org/10.22034/ijts.2026.2069496.4182

| Received: 20 Aug. 2025 | Revised: 6 May. 2026 | Accepted: 11 May. 2026 |

Abstract

With the expansion of data-driven technologies, personal data is increasingly collected, stored, and analyzed within big data systems and databases. These structures, designed to enable large-scale and intelligent information processing, provide substantial benefits for businesses but simultaneously generate fundamental challenges regarding data subject rights. In big data environments, data is gathered in massive, diverse, and interconnected forms, making the exercise of individual rights such as access, rectification, erasure, or portability highly difficult due to technical and structural barriers; isolating a single person's data within such datasets often proves complex or even impossible. In company-owned databases, personal data is frequently treated as part of the informational assets, creating tensions between corporate intellectual property rights over the database and individuals' privacy rights. The central question addressed in this article is what legal and technical challenges emerge at the intersection of big data and databases in safeguarding data subject rights, and how legal systems have responded. Using a descriptive-analytical method and based on library research, the study finds that big data remains subject to a significant regulatory gap, as most legal frameworks have yet to extend data protection obligations specifically to this context. Accordingly, enforcing data subject rights requires new regulations tailored to the distinctive features of big data. Regarding databases, intellectual property protection applies only to the design, structure, and organization of the database, while raw personal data remains subject to privacy and data protection regulations.

zshakeri@ut.ac.ir JEL Classification: K24, K33, K42, O33, L86

Keywords: Big Data, Databases, Data Subject Rights, Intellectual Property, Personal Data.

Data Availability: The data used or generated in this research are presented in the text of the article.

Conflicts of Interest: The authors of this paper declared no conflict of interest regarding the authorship or publication of this article.

۱. مقدمه

یکی از پرسش‌های بنیادین در نظام حقوقی حمایت از داده‌های شخصی آن است که ساختارهای فنی گردآوری و سازمان‌دهی داده‌ها تا چه اندازه بر امکان اعمال حقوق اشخاص موضوع داده اثر می‌گذارند. داده‌ها در مسیر پردازش، از حالت منفرد و غیرساختاریافته به قالب‌های پیچیده‌تری چون پایگاه‌ها و کلان‌داده منتقل می‌شوند. هرچه این قالب‌ها منسجم‌تر می‌شوند، شناسایی منبع، انتساب داده به فرد و تفکیک داده‌های شخصی دشوارتر شده و قابلیت اعمال حقوقی چون دسترسی، حذف و انتقال محدودتر می‌گردد.

در محیط‌های داده‌محور، داده‌های شخصی عمدتاً در دو قالب اصلی ذخیره و تحلیل می‌شوند: کلان‌داده‌ها و پایگاه‌های داده. کلان‌داده‌ها به‌دلیل حجم انبوه، تنوع و پیوندهای درونی، شفافیت کمی دارند و اجرای حقوق اشخاص را با موانع فنی و مفهومی مواجه می‌کنند؛ گاه تعیین تعلق داده به شخص خاص ناممکن است. در پایگاه‌های داده نیز، با وجود ساختار سازمان‌یافته، چالش دیگری بروز می‌کند: مالکیت پایگاه‌ها در دست شرکت‌هاست و داده‌های شخصی بخشی از دارایی اطلاعاتی تلقی می‌شوند. این امر تعارضی میان حقوق مالکیت فکری شرکت‌ها بر ساختار پایگاه و حقوق اشخاص بر داده‌های خود ایجاد می‌کند؛ به‌ویژه آنکه برخی شرکت‌ها داده‌های شخصی را نیز به‌عنوان دارایی معرفی می‌کنند.

ضرورت بررسی موضوع از آن‌جا ناشی می‌شود که بسیاری از نظام‌های حقوقی، مقررات خود را بدون تفکیک میان قالب‌های داده‌ای تدوین کرده‌اند و الزامات ناظر بر کلان‌داده یا وضعیت داده‌ها در مالکیت فکری پایگاه‌ها همچنان فاقد شفافیت است. در نتیجه، حقوق اشخاص در معرض تهدید و شرکت‌ها نیز با نااطمینانی حقوقی مواجه‌اند. بر این اساس، پرسش‌های اصلی عبارتند از: ۱. تأثیر قالب‌های فنی بر اجرای حقوق اشخاص؛ ۲. چالش‌های فنی و حقوقی در اعمال حقوقی چون دسترسی، حذف و انتقال؛ ۳. نحوه تحلیل تعارض میان مالکیت فکری شرکت‌ها و حقوق فردی بر داده‌ها؛ ۴. میزان پاسخ‌گویی نظام‌های حقوقی موجود به این وضعیت. یافته‌های مقدماتی نشان می‌دهد در کلان‌داده‌ها مقررات صریحی وجود ندارد و اعمال بسیاری از حقوق در عمل غیرممکن است. در حوزه پایگاه‌ها نیز باید میان مالکیت شرکت‌ها بر طراحی و سازمان‌دهی، و داده‌های شخصی ذخیره‌شده که تابع قواعد حریم خصوصی‌اند، تمایز گذاشت.

مقاله حاضر در دو بخش تنظیم شده است: نخست، تعریف و چارچوب‌بندی مفاهیم کلیدی چون داده‌های شخصی، کلان‌داده و پایگاه داده؛ سپس، بررسی چالش‌های فنی و حقوقی اعمال حقوق داده‌ها و تحلیل نسبت میان مالکیت فکری پایگاه‌ها و حقوق فردی بر داده‌ها. در فقدان قانون خاص در ایران، تحلیل عمدتاً بر حقوق اتحادیه اروپا، به‌عنوان نظام پیشگام و الگوی جهانی و حقوق ایالات متحده مبتنی است. از آنجاکه موضوع در ایران نو و فاقد مقررات صریح است، منابع فارسی عمدتاً به‌طور کلی به حریم

خصوصی، مالکیت فکری یا جنبه‌های فنی پرداخته‌اند و به تعارض میان حقوق فردی و حقوق ناشی از ساختارهای داده‌ای اشاره مستقیمی نکرده‌اند.[1] ازاین‌رو، پیشینه پژوهش حاضر بر مطالعات تطبیقی انگلیسی‌زبان تکیه دارد.

۲. تعریف مفاهیم اصلی

در بخش اول این پژوهش با عنایت به اهمیت آشنایی با مفاهیم فنی در راستای شناسایی ابعاد حقوقی آن‌ها، مفهوم داده‌های شخصی، کلان داده‌ها و پایگاه داده مورد تعریف و بررسی قرار می‌گیرند.

۲-۱. داده‌های شخصی

حق بر حریم خصوصی از حقوق بنیادین انسان‌هاست که در دنیای مدرن، به‌ویژه در بازارهای دیجیتال، بعدی نوین به نام حریم خصوصی اطلاعاتی یافته و در مرکز آن، مفهوم داده‌های شخصی قرار دارد.[2] یکی از جامع‌ترین تعاریف داده شخصی در بند ۱ ماده ۴ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا[3] آمده است که هر نوع اطلاعات مربوط به فردی حقیقی شناسایی‌شده یا قابل‌شناسایی را شامل می‌شود؛ فرد قابل شناسایی کسی است که از طریق داده‌هایی چون نام، شماره شناسایی، داده‌های مکانی، شناسه‌های آنلاین یا ویژگی‌های فردی و اجتماعی قابل شناسایی باشد.

کشورهای مختلف تعاریف مشابهی پذیرفته‌اند. در بریتانیا، قانون حفاظت از داده‌ها ۲۰۱۸[4]، علی‌رغم خروج از اتحادیه اروپا، همان تعریف را حفظ کرده است. قوانین ملی آلمان[5]، چین[6] و هند[7] نیز همین رویکرد را دارند. در ایالات متحده تعریف واحد فدرال وجود ندارد، اما قوانین بخشی، داده‌های شخصی را تعریف کرده‌اند؛ مثلاً قانون قابلیت انتقال و مسئولیت‌پذیری بیمه‌های درمانی ۱۹۹۶[8] اطلاعات سلامت قابل‌شناسایی را داده شخصی می‌داند. در سطح ایالتی، قانون حفظ حریم خصوصی مصرف‌کنندگان

---

۱. تنها منبع فارسی موجود در این زمینه، پایان‌نامه‌ای (قربان نیا، امیرمحمد، (۱۴۰۳)، وضعیت حقوقی داده‌های اشخاص در فرض تملک و ادغام شرکت‌ها، پایان‌نامه کارشناسی ارشد، حقوق خصوصی، دانشگاه تهران.) است که به تعارض مذکور می‌پردازد.

۲. قربان نیا، (۱۴۰۳)؛ ص ۵۳.

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation GDPR), art 4(1).

4. UK Data Protection Act 2018.

5. Bundesdatenschutzgesetz BDSG 2018.

6. Personal Information Protection Law PIPL, 2021.

7. Digital Personal Data Protection Act, 2023.

8. Health insurance portability and accountability act of 1996 (HIPAA), CFR §160.103 45: Protected Health Information (PHI).

کالیفرنیا[1] هر داده مرتبط با فرد یا خانوار از جمله نام، آدرس، شناسه دستگاه، تاریخچه مرورگر و داده‌های زیستی را داده شخصی می‌شمارد. قانون حمایت از داده‌های مصرف‌کنندگان ویرجینیا ۲۰۲۱[2] نیز تعریفی مشابه مقررات اروپایی ارائه کرده است.

در ایران نیز تعاریف متعددی ارائه شده است. قانون انتشار و دسترسی آزاد به اطلاعات، داده‌های فردی را شامل نام، نشانی، سوابق بیماری و اطلاعات مالی می‌داند. در قانون تجارت الکترونیکی، داده‌پیام‌های شخصی پیام‌هایی مرتبط با فرد حقیقی تعریف شده‌اند. کمیسیون انتشار و دسترسی آزاد نیز در شیوه‌نامه خود داده‌های شخصی را در دسته‌های هویتی، مکانی، اقتصادی و سلامت تقسیم کرده است. در پیش‌نویس لایحه حمایت از داده‌ها و حریم خصوصی، داده شخصی هر داده‌ای است که به‌تنهایی یا همراه سایر داده‌ها به شناسایی فرد بینجامد. طرح الزام به انتشار داده ۱۴۰۳ و طرح حفاظت از داده‌های شخصی ۱۴۰۳ نیز همین تعریف کلی را پذیرفته‌اند.

۲-۲. کلان داده‌ها

در سال‌های اخیر، شتاب تحولات فناورانه و گسترش توان پردازش داده موجب پیدایش مفهومی نو در زیست‌بوم دیجیتال شده است: کلان‌داده[3]. برخلاف داده‌های منفرد، کلان‌داده‌ها به‌دلیل حجم عظیم، سرعت بالای تولید و تنوع ساختاری، در قالب مجموعه‌هایی پیچیده شکل می‌گیرند که مدیریت آن‌ها با روش‌های سنتی ممکن نیست.[4] این سه ویژگی «حجم»، «سرعت» و «تنوع» در ادبیات فنی با مدل «V۳»[5] شناخته می‌شوند؛ برخی پژوهشگران معیارهایی چون اعتبار[6]، ارزش[7] و تغییرپذیری[8] را نیز افزوده و الگوی «V6» را پیشنهاد کرده‌اند.[9]

حجم به گستردگی داده‌هایی اشاره دارد که معمولاً در مقیاس ترابایت یا پتابایت و بیشتر سنجیده می‌شوند. شبکه‌های اجتماعی، اینترنت اشیاء، حسگرها و سامانه‌های مالی از منابع کلیدی‌اند و به زیرساخت‌های توزیع‌شده نیاز دارند.[10] سرعت بیانگر نرخ تولید و پردازش لحظه‌ای داده‌ها است، مانند

---

1. California consumer privacy act 2019, 1798.140 Section.
2. Virginia consumer data protection act 2021, 575-59.1 Section.
3. Big Data
4. ASPE, (2018); pp 3-4.

۵. حجم (Volume)، سرعت (Velocity) و تنوع (Variety).

6. Veracity
7. Value
8. Validation

۹. متولی و دیگران، (۱۳۹۶)؛ ص ۱۱.

10. Big data LDN, (2018).

اطلاعات بازار سرمایه یا رفتار کاربران که تحلیل‌گران باید فوراً به آن پاسخ دهند.[1] تنوع نیز به گوناگونی داده‌ها از نظر قالب و منبع اشاره دارد. دسته‌بندی داده‌ها از منظر حقوقی اهمیت خاصی دارد و شامل: ۱) شخصی؛ ۲) مستعار؛ ۳) ناشناس؛ و ۴) غیرشخصی است .مرزبندی این دسته‌ها در محیط کلان‌داده چالش‌برانگیز است.[2]

ویژگی‌های دیگر نیز مؤثرند: اعتبار به صحت و سازگاری داده‌ها مربوط است و داده‌های نادرست می‌توانند تحلیل‌ها را گمراه کنند؛ ارزش به امکان استخراج بینش کاربردی اشاره دارد، زیرا داده فاقد ارزش فقط هزینه‌زا خواهد بود؛ و تغییرپذیری به بی‌ثباتی معنایی یا زمینه‌ای داده‌ها مرتبط است، مانند الگوهای رفتاری متغیر در شبکه‌های اجتماعی که تحلیل‌گران باید آن‌ها را در پیش‌بینی‌ها لحاظ کنند.[3]

۲-۳. پایگاه داده

هنگامی که داده‌ها بر پایه طراحی هدفمند و ساختاریافته گردآوری شوند و در محیطی سامان‌مند و کنترل‌پذیر ذخیره گردند که امکان جست‌وجو، بازیابی، به‌روزرسانی و مدیریت کارآمد اطلاعات را فراهم کند، می‌توان آن‌ها را جزئی از یک پایگاه داده[4] به‌شمار آورد. دستیابی به این سطح از سازمان‌دهی عمدتاً از طریق بهره‌گیری از سامانه‌های مدیریت پایگاه داده[5] ممکن می‌گردد؛ سامانه‌هایی که افزون بر تسهیل پردازش داده‌های حجیم، به حفظ انسجام داده‌ها، اعمال کنترل‌های چندلایه بر سطوح دسترسی، و ممانعت از دسترسی‌های غیرمجاز نیز کمک می‌کنند.[6]

در اسناد حقوقی بین‌المللی، از جمله بند ۲ ماده ۱۰ موافقت‌نامه جنبه‌های تجاری حقوق مالکیت فکری[7] پایگاه داده به‌عنوان مجموعه‌ای ترکیبی از داده‌ها یا دیگر عناصر تعریف شده است که، فارغ از قالب آن‌ها (چه به‌صورت ماشینی خوانا و چه در اشکال دیگر)، در صورتی‌که انتخاب یا چیدمان محتوای آن متضمن خلاقیت فکری باشد، می‌تواند تحت حمایت مالکیت ادبی و هنری قرار گیرد. در ماده ۱ دستورالعمل پایگاه داده اتحادیه اروپا[8] نیز، پایگاه داده به‌عنوان مجموعه‌ای از آثار، داده‌ها یا دیگر مواد مستقل که به‌صورت نظام‌مند یا روش‌مند سامان‌دهی شده و هر یک از اجزای آن به‌صورت جداگانه از طریق وسایل الکترونیکی یا سایر روش‌ها قابل دستیابی باشد، تعریف شده است.

---

1. Velivela et al, (2016); pp 171-173.
2. Radon, (2015); pp 5-8.
3. Chancey, (2024).
4. Database
5. Database management system
6. Elmasri & Navathe, (2015); pp 4-29.
7. World Trade Organization. (1994). Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). art 10(2).
8. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases.

در حقوق ایران، بند ۲۳ ماده ۱ از پیش‌نویس لایحه قانون جامع حمایت از حقوق مالکیت ادبی و هنری پایگاه داده را به‌عنوان مجموعه‌ای از اطلاعات سازمان‌یافته معرفی می‌کند که امکان ارزیابی و جست‌وجو در آن فراهم باشد. علاوه‌بر این، ماده ۶۲ قانون تجارت الکترونیکی به‌صراحت اعلام می‌دارد که پایگاه‌های داده، در قالب داده‌پیام‌ها، مشمول حمایت حقوق مالکیت فکری قرار می‌گیرند.

۳. چالش‌های حمایت از داده‌های شخصی در بستر کلان داده‌ها و پایگاه‌های داده

کلان داده‌ها و پایگاه‌های داده به دلیل ویژگی‌هایی که برای هریک بیان شد، به‌صورت ذاتی، اعمال برخی مراقبت‌ها و محدودیت‌های مقررات حمایت از داده‌های شخصی را در مورد داده‌های مرتبط یا مختلط با خود، با چالش‌هایی مواجه می‌سازند. در این بخش، چالش‌های مذکور و راه‌کارهای موجود برای هرکدام، بررسی خواهند شد.

۳-۱. کلان داده‌ها و اعمال حقوق اشخاص موضوع داده

ریسک‌های کلان‌داده در تمام مراحل چرخه عمر آن[۱]، از گردآوری تا تحلیل نهایی، قابل مشاهده است.[۲]

۱. **گردآوری:** دسترسی غیرمجاز به داده‌ها به‌دلیل ضعف امنیتی یا سو استفاده داخلی از جدی‌ترین تهدیدها است. جمع‌آوری داده‌های شخصی بدون رضایت صریح، نقض حریم خصوصی محسوب می‌شود. همچنین، ترکیب داده‌های به‌ظاهر ناشناس با دیگر مجموعه‌ها می‌تواند به شناسایی هویت افراد بینجامد.

۲. **ذخیره‌سازی:** کلان داده‌ها با خطر افشای اطلاعات حساس مواجه‌اند. فقدان رمزگذاری مناسب، دسترسی هکرها را آسان می‌کند و سرقت داخلی نیز پیامدهای سنگینی برای اشخاص و سازمان‌ها دارد.

۳. **پردازش:** سوگیری الگوریتمی می‌تواند به تبعیض و آسیب ناعادلانه به گروه‌ها منجر شود. استفاده از داده‌ها برای تبلیغات هدفمند بدون رضایت آگاهانه نیز حقوق کاربران را نقض و اعتماد عمومی را کاهش می‌دهد.

۴. **اشتراک‌گذاری:** انتشار غیرمجاز، قاچاق یا فروش داده‌های شخصی، تهدیدی جدی برای حریم خصوصی است. اشتراک داده‌های اشخاص ثالث بدون رضایت، علاوه‌بر آسیب به حقوق فردی، می‌تواند موجب جریمه‌های سنگین شود.

---

۱. چرخه عمر داده‌ها: ۱. مجموعه‌سازی و جمع‌آوری، ۲. ذخیره‌سازی، ۳. پردازش، ۴. اشتراک‌گذاری، ۵. تحلیل.

2. Chancey, (2024).

۵. **تحلیل:** نظارت مستمر بر رفتار آنلاین یا آفلاین می‌تواند آزادی‌های فردی را نقض و احساس رصد دائمی ایجاد کند. همچنین، تحریف یا دستکاری داده‌ها برای جهت‌دهی افکار عمومی یا تصمیمات کلان، چالشی مهم در استفاده قانونی و اخلاقی از کلان‌داده‌ها است.

این مجموعه ریسک‌ها نشان می‌دهد که مدیریت کلان‌داده نیازمند رویکردی جامع است که در هر مرحله از چرخه، حقوق افراد را حمایت کند.

پردازش داده‌ها در مقیاس وسیع گاهی ممکن است با الزامات منشور حقوق بنیادین اتحادیه اروپا و مقررات عمومی حفاظت از داده‌ها نیز در تعارض قرار گیرد. بر اساس این اسناد، پردازش داده‌های شخصی باید فقط برای اهداف مشخص، مشروع و منصفانه انجام شده و نگهداری آن‌ها فراتر از زمان مورد نیاز نباشد. بهره‌برداری گسترده از داده‌ها مزایای قابل‌توجهی دارد، اما اصول بنیادی حفاظت از داده‌ها را نمی‌توان نادیده گرفت. بنابراین، شرکت‌ها و نهادها موظف‌اند از مرحله طراحی، تمهیدات امنیتی و فنی مبتنی بر حریم خصوصی را در ساختارها، فرایندها و خدمات خود اعمال کنند تا حقوق و آزادی‌های اشخاص موضوع داده حفظ شود. این رویکرد در اتحادیه اروپا با اصطلاحات «حریم خصوصی از طریق طراحی»[۱] و «پیش‌فرض‌های حریم‌محور»[۲] شناخته شده و به‌عنوان ابزاری پیشگیرانه برای مدیریت مسئولانه داده‌ها به‌کار می‌رود. با این حال، بسیاری سازمان‌ها تنها به رعایت اصول کلی مشروعیت و انصاف بسنده می‌کنند و از تعهدات تکمیلی مانند حذف داده‌های اضافی، تعیین دوره‌های نگهداری مشخص و اجتناب از انباشت داده‌های غیرضروری غافل می‌شوند.[۳]

بر اساس بند ۱ ماده ۵ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا[۴]، اصل محدودیت زمانی در نگهداری داده‌ها[۵] حاکم است؛ یعنی اطلاعات فقط به‌مدت لازم برای تحقق هدف پردازش حفظ شوند. سازمان‌ها باید برای هر دسته داده دوره نگهداری مشخص داشته و پس از پایان آن، سامانه‌های فنی برای

---

۱. «حریم خصوصی از طریق طراحی» (Privacy by Design) رویکردی پیشگیرانه در حفاظت از داده‌های شخصی است که به جای درمان نقض حریم خصوصی، بر پیشگیری از آن تأکید دارد. این اصل بر آن است که تدابیر فنی و سازمانی مربوط به حفظ حریم خصوصی باید از همان مراحل ابتدایی طراحی سامانه‌ها، خدمات و محصولات اطلاعاتی، در بطن ساختار آن‌ها گنجانده شود. در این رویکرد، حفاظت از داده‌ها نه یک ویژگی افزودنی، بلکه بخشی جدایی‌ناپذیر از فرآیند طراحی تلقی می‌شود. حریم خصوصی از طریق طراحی، با اصولی چون پیش‌فرض حفاظت از حریم خصوصی، تمام‌گرایی در چرخه حیات داده، شفافیت و اولویت‌بخشی به منافع کاربران پیوند دارد. این رویکرد نخستین‌بار توسط دکتر آن کاوکیان مطرح شد و بعدها در مقرراتی چون GDPR به رسمیت شناخته شد.

۲. «پیش‌فرض‌های حریم‌محور» (Privacy by Default) اصلی مکمل برای «حریم خصوصی از طریق طراحی» است که بر لزوم تنظیم محصولات، خدمات و سامانه‌های پردازش داده به‌گونه‌ای تأکید دارد که در حالت پیش‌فرض، بیشترین سطح ممکن از حفاظت حریم خصوصی افراد رعایت شود. بر اساس این اصل، بدون نیاز به اقدام خاصی از سوی کاربر، تنها داده‌های ضروری گردآوری و پردازش می‌شوند و دسترسی به اطلاعات شخصی، به حداقل مورد نیاز محدود می‌گردد. به بیان دیگر، جمع‌آوری داده، مدت نگهداری، دسترسی‌ها و اهداف استفاده از ابتدا به‌گونه‌ای تنظیم می‌شوند که با اصول کمینه‌سازی، هدف‌مندی و محدودیت سازگار باشند. این اصل در ماده ۲۵ مقررات عمومی حفاظت داده اتحادیه اروپا GDPR تصریح شده است.

3. Moryl & Synowiec, (2024).

4. GDPR, art 5(1).

5. Storage limitation

حذف خودکار و ایمن داده‌ها را پیاده‌سازی کنند. بی‌توجهی به این الزامات می‌تواند حقوق اشخاص را نقض و مخاطرات امنیتی و مسئولیت‌های قانونی گسترده ایجاد کند.[1]

همچنین یکی از مهم‌ترین و بحث‌برانگیزترین کاربردهای کلان‌داده‌ها، استفاده از آن‌ها در الگوریتم‌های یادگیری ماشینی[2] و سامانه‌های هوش مصنوعی[3] است. این فناوری‌ها به سازمان‌ها امکان می‌دهند با تحلیل انبوه داده‌های رفتاری، جمعیت‌شناختی یا بیومتریک، تصمیم‌های خودکار درباره افراد اتخاذ کرده یا آن‌ها را وارد فرایند پروفایل‌سازی نمایند. الگوریتم‌ها با الگوهای به‌دست‌آمده، رفتار، علایق، قابلیت‌ها یا ویژگی‌های فردی را پیش‌بینی می‌کنند؛ روندی که در بازاریابی هدفمند، ارائه تسهیلات مالی، بیمه‌های سلامت و نظام عدالت کیفری کاربرد دارد.[4] اگرچه این فناوری‌ها منافع عمومی مانند شناسایی زودهنگام بیماری‌ها، کاهش آلودگی محیطی و ارتقای کارایی حمل‌ونقل شهری دارند، اما تهدیدهای جدی برای حقوق و آزادی‌های افراد، به‌ویژه حق بر حریم خصوصی، ایجاد می‌کنند. تحلیل‌های پیش‌نگرانه ممکن است نتایجی همچون احتمال ابتلا به بیماری یا ورشکستگی مالی ارائه دهند که بدون اطلاع یا رضایت شخص، موجب رد درخواست وام، افزایش نرخ بیمه یا از بین رفتن فرصت‌های شغلی شود. حقوق داده‌ها در اتحادیه اروپا با وضع سازوکارهای حمایتی، آثار منفی تصمیم‌گیری‌های خودکار و پروفایل‌سازی را کنترل می‌کند. ماده ۲۲ مقررات عمومی حفاظت از داده‌ها[5] به‌صراحت تصریح می‌کند افراد نباید بر اساس پردازش صرفاً خودکار، از جمله پروفایل‌سازی، تصمیم‌هایی دریافت کنند که آثار حقوقی یا مشابه قابل توجه داشته باشد. استثناها شامل مواردی است که تصمیم برای انعقاد یا اجرای قرارداد ضروری باشد[6]، مستند به مجوز قانونی کشور عضو باشد یا با رضایت آگاهانه فرد انجام شود. در این موارد نیز شخص باید امکان درخواست دخالت انسانی، اظهار نظر و اعتراض به تصمیم اتخاذشده را داشته باشد. ماده ۱۳ مقرره[7] نیز تصریح می‌کند که هنگام گردآوری داده‌ها، باید اطلاعاتی درباره منطق تصمیم‌گیری خودکار و اهمیت پیامدهای آن به فرد ارائه شود. این الزام بر شفافیت فرآیندهای خودکار تأکید دارد و از پنهان‌ماندن عملیات پروفایل‌سازی

---

1. Čtvrtník, (2023); pp 197-220.

۲. یادگیری ماشینی (Machine Learning) شاخه‌ای از هوش مصنوعی است که به سیستم‌ها امکان می‌دهد بدون برنامه‌نویسی صریح، از طریق داده‌ها و تجربه، الگوها را شناسایی کرده و تصمیم‌گیری یا پیش‌بینی کنند. این فناوری بر پایه الگوریتم‌هایی طراحی شده است که می‌توانند از داده‌های ورودی، قواعد یا روابط پنهان را استخراج و برای تحلیل داده‌های جدید به‌کار گیرند. یادگیری ماشینی به‌ویژه در تحلیل کلان‌داده، تشخیص الگوهای رفتاری کاربران، طبقه‌بندی اطلاعات، و بهینه‌سازی فرآیندها در حوزه‌هایی چون سلامت، بازاریابی، امنیت سایبری و شبکه‌های اجتماعی نقش کلیدی دارد. در این چارچوب، هرچه داده‌های بیشتری پردازش شود، عملکرد مدل نیز به‌مرور دقیق‌تر و کارآمدتر می‌گردد.

3. Artificial Intelligence

4. Zhou et al, (2017); pp 351-354.

5. GDPR, art 22.

۶. مثال بارز این مورد، استفاده از الگوریتم‌های اعتبارسنجی در فرآیند اعطای تسهیلات بانکی آنلاین است؛ جایی که تصمیم‌گیری خودکار برای ارزیابی سریع و دقیق توان بازپرداخت مشتری، شرط لازم برای انعقاد قرارداد وام محسوب می‌شود. در این فرایند، ارزیابی بدون مداخله انسانی صورت می‌گیرد اما با هدف اجرای مستقیم رابطه قراردادی بین بانک و مشتری انجام می‌شود.

7. GDPR, art 13.

جلوگیری می‌کند. برخی نظام‌های حقوقی ملی، مانند قانون حفاظت از داده‌های فرانسه، الزام کرده‌اند کنترل‌کننده باید درباره عملکرد الگوریتم توضیح دهد تا شفافیت، پاسخ‌گویی و جلوگیری از سوگیری الگوریتمی[1] تقویت شود.[2] همچنین بر اساس قانون هوش مصنوعی اتحادیه اروپا مصوب ۲۰۲۴[3]، سامانه‌های هوش مصنوعی بر اساس سطح ریسک طبقه‌بندی می‌شوند:

۱. ریسک غیرقابل قبول: استفاده از هوش مصنوعی برای امتیازدهی اجتماعی یا تشخیص چهره در زمان واقعی در اماکن عمومی، ممنوع است؛ ۲. ریسک بالا: سامانه‌های حساس مانند استخدام، آموزش، سلامت یا اجرای قانون که نیازمند شفافیت، نظارت انسانی و مدیریت داده‌ها هستند؛ ۳. ریسک محدود و ۴. ریسک کم، با الزاماتی سبک‌تر.

بنابراین، سامانه‌های یادگیری ماشینی که از کلان‌داده‌ها برای تحلیل رفتار یا تصمیم‌گیری خودکار استفاده می‌کنند، ممکن است در دسته سامانه‌های با ریسک بالا قرار گیرند و تابع ارزیابی ریسک، تضمین نظارت انسانی و شفاف‌سازی فرآیند باشند.[4]

چالش دیگر، ماهیت غیرتوضیح‌پذیر برخی سامانه‌های ملقب به جعبه‌سیاه[5] است که حتی طراحان نیز نمی‌توانند دلایل تصمیم‌ها را توضیح دهند. این ویژگی می‌تواند حقوق افراد را نقض کند. بنابراین، مقررات اتحادیه اروپا و قانون هوش مصنوعی، استفاده از این سامانه‌ها در قالب کلان داده‌ها را تنها در صورت پیش‌بینی سازوکار توضیح‌پذیری، ثبت تصمیمات و نظارت انسانی مؤثر مجاز می‌دانند.[6] توسعه سامانه‌های هوش مصنوعی برای تحلیل کلان داده‌ها باید طوری باشد که امکان تفسیر تصمیمات و پاسخ‌گویی حقوقی فراهم گردد.

با وجود نکات پیشین، باید اذعان کرد که مقررات موجود در حوزه حفاظت از داده‌ها، چه مقررات عمومی اتحادیه اروپا و چه قوانین ایالتی آمریکا، به‌طور مستقیم به کلان‌داده‌ها نپرداخته‌اند. با این‌حال، برداشت غالب در چارچوب حقوقی اتحادیه اروپا این است که اصول کلی پردازش داده‌های شخصی را می‌توان بر کلان‌داده‌ها نیز اعمال کرد؛ چالش اصلی، اجرای عملی آن‌ها در بستر کلان‌داده‌هاست. برای مثال، اصولی مانند محدودیت هدف، کفایت و تناسب در گردآوری اطلاعات و لزوم استفاده حداقلی از داده‌ها، در مواجهه

1. Algorithmic bias
2. Agh, (2020).
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).
4. Trail, (2024).
5. Black Box
6. Pavlidis, (2024); pp 294-300.

با حجم عظیم، جریان دائمی و اهداف نامشخص کلان‌داده‌ها، با موانع جدی روبه‌رو می‌شوند. افزون بر این، ماهیت پویای کلان‌داده که اغلب برای مصارف ثانویه، ترکیب با منابع دیگر یا تصمیم‌سازی پیش‌بینی‌محور استفاده می‌شود، اعمال حقوق فردی مانند حق آگاهی، دسترسی، اصلاح یا حذف داده‌ها را دشوار می‌سازد.[1]

این وضعیت نه‌تنها ساختار حقوقی حفاظت از داده‌ها را با چالش مواجه می‌کند، بلکه زمینه ورود دغدغه‌هایی مرتبط با حقوق رقابت، منع تبعیض و حمایت از مصرف‌کننده را نیز فراهم می‌آورد، زیرا پردازش گسترده و مداوم کلان‌داده‌ها تهدیدهایی مانند تصمیم‌گیری‌های خودکار، رفتارهای تبعیض‌آمیز و اقدامات انحصارطلبانه اقتصادی ایجاد می‌کند.

۳-۲. راه‌کارهای حفظ حریم داده‌های شخصی در بطن کلان‌داده‌ها

برای صیانت از حریم خصوصی و امنیت در اکوسیستم کلان‌داده، مجموعه‌ای از فناوری‌ها و روش‌های پیشرفته توسعه یافته‌اند که هدف اصلی آن‌ها پیشگیری از افشای ناخواسته اطلاعات حساس در طول چرخه عمر داده است. در ادامه، مهم‌ترین این رویکردها معرفی می‌شوند:

۱. فناوری کنترل دسترسی[2]

در بستر کلان‌داده، به‌دلیل تنوع بالای کاربران و پیچیدگی مجوزهای دسترسی، استفاده از سامانه‌های پیشرفته کنترل دسترسی اهمیت ویژه‌ای می‌یابد. یکی از رایج‌ترین الگوهای مورد استفاده، مدل کنترل دسترسی مبتنی بر نقش[3] است. در این مدل، دسترسی کاربران نه به‌صورت فردی، بلکه بر اساس نقش سازمانی آن‌ها در سیستم تعیین می‌شود. به‌عبارت دیگر، تنها کاربرانی که نقش‌شان مجوز لازم را دارد، به اطلاعات مشخصی دسترسی خواهند داشت. برای نمونه، در سامانه‌های درمانی، صرفاً پزشکان مجاز به مشاهده سوابق بیماران هستند، نه سایر پرسنل. اعمال کنترل‌های دقیق سطح‌بندی‌شده در نقاط ورودی داده‌ها، تضمین می‌کند که داده‌های حساس صرفاً در اختیار کاربران مجاز قرار گیرد و از دسترسی‌های غیرمجاز جلوگیری شود.

۲. رمزگذاری هومومورفیک[4]

رمزگذاری هومومورفیک روشی پیشرفته در رمزنگاری است که امکان انجام عملیات منطقی و ریاضی روی

---

۱. عطار، (۱۴۰۰)؛ صص ۳۹-۴۱.

2. Access Control Technologies
3. Role-Based Access Control - RBAC
4. Homomorphic Encryption - HE

داده‌های رمزگذاری‌شده را بدون نیاز به رمزگشایی آن‌ها فراهم می‌سازد. این ویژگی مزیت قابل‌توجهی برای محیط‌هایی دارد که داده‌ها باید در حالت رمزشده باقی بمانند، اما در عین حال تحلیل نیز روی آن‌ها انجام شود. برای مثال، در مورد داده‌های پزشکی رمزنگاری‌شده یک بیمار، می‌توان الگوریتم تحلیلی را مستقیماً روی نسخه رمزشده اعمال کرد و نتیجه تحلیل نیز به‌صورت رمزنگاری‌شده باقی بماند. از آن‌جا که داده‌ها در طول فرآیند پردازش افشا نمی‌شوند، احتمال نشت اطلاعات به‌شدت کاهش می‌یابد. این فناوری همچنان در مرحله توسعه و بهبود قرار دارد، اما پتانسیل بالایی برای تقویت حریم خصوصی در کلان‌داده دارد.

۳. محاسبات چندجانبه امن[1]

محاسبات چندجانبه امن مجموعه‌ای از الگوریتم‌ها و پروتکل‌هایی است که به چندین نهاد اجازه می‌دهد بدون افشای داده‌های خصوصی خود، به‌طور مشترک محاسباتی را انجام دهند. در این روش، هر مشارکت‌کننده تنها داده‌های خود را در اختیار دارد و به داده‌های دیگر طرف‌ها دسترسی ندارد، ولی نتیجه نهایی تحلیل میان تمام طرف‌ها به اشتراک گذاشته می‌شود. این رویکرد در مواردی مانند همکاری چند مرکز درمانی برای تحلیل آماری بدون افشای اطلاعات بیماران کاربرد دارد. هدف اصلی این تکنیک، حفاظت از حریم خصوصی، صحت محاسبات و پیشگیری از افشای اطلاعات جانبی است.

۴. فناوری ناشناس‌سازی داده‌ها[2]

ناشناس‌سازی داده‌ها یکی از رایج‌ترین روش‌ها برای حفاظت از حریم خصوصی در پایگاه‌های داده متمرکز و توزیع‌شده است. در این فرآیند، اطلاعاتی که به شناسایی افراد منجر می‌شود، از مجموعه داده حذف یا تغییر می‌یابد به‌گونه‌ای که بازشناسایی افراد خاص ممکن نباشد. فیلدهایی مانند نام، شماره ملی، ایمیل یا هر داده قابل‌ارجاع به هویت فردی، یا حذف می‌شوند یا با مقادیر تصادفی جایگزین می‌گردند. اهداف اصلی این روش شامل دو محور است: نخست، جلوگیری از افشای هویت[3] به‌طوری که هیچ رکوردی نباید حاوی اطلاعاتی باشد که امکان شناسایی مستقیم یا غیرمستقیم فرد را فراهم کند؛ دوم، پیشگیری از افشای ویژگی‌ها[4]، به این معنا که حتی در صورت ناشناس بودن رکوردها، نباید بتوان از طریق ویژگی‌های آشکار مانند سن یا منطقه جغرافیایی به ویژگی‌های حساس‌تری چون وضعیت سلامت یا ترجیحات فردی پی برد.[5]

1. Secure Multi-party Computation - SMC
2. Data Anonymization
3. Prevention of Identity Disclosure
4. Prevention of Attribute Disclosure
5. Jha et al, (2017); p 88.

در نهایت، باید اذعان کرد که مسئله حریم خصوصی در حوزه کلان‌داده‌ها ارتباطی مستقیم با میزان اعتماد کاربران دارد. هرچه اطلاعات گردآوری‌شده درباره افراد گسترده‌تر باشد، امکان تحلیل داده‌ها، اتصال نقاط پراکنده اطلاعاتی و شناسایی الگوهای رفتاری افزایش می‌یابد؛ به‌نحوی که پیش‌بینی رفتار آینده کاربران و ترسیم دقیق‌تری از هویت دیجیتال، علایق و سبک زندگی آن‌ها ممکن می‌شود. چنین ظرفیتی اگرچه زمینه‌ساز تحلیل‌های عمیق‌تر و توسعه بازاریابی هدفمند است، اما همزمان تهدیدهای جدی برای صیانت از حریم خصوصی نیز به‌همراه دارد.

از این‌رو، شفافیت درخصوص نحوه گردآوری، نگهداری، پردازش و بهره‌برداری از داده‌ها به ضرورتی اخلاقی و حقوقی تبدیل شده است. در چنین فضایی، لازم است نهادها و شرکت‌ها راهبردهایی مشخص و اثربخش برای اطلاع‌رسانی به کاربران در مورد چرایی و چگونگی استفاده از اطلاعات‌شان تدوین کنند. به‌ویژه ضروری است که به افراد توضیح داده شود چه تمهیدات فنی و مدیریتی جهت تطبیق با مقررات قانونی، کنترل دسترسی، کاهش احتمال بازشناسایی و حفظ محرمانگی داده‌ها پیش‌بینی شده است.

در راستای تحقق این اهداف، استفاده از ابزارهای تخصصی در حوزه حریم خصوصی که با زیرساخت‌های بومی کلان‌داده سازگار باشند، ضروری به‌نظر می‌رسد. این ابزارها[1] از طریق قابلیت‌هایی همچون طبقه‌بندی خودکار اطلاعات، شناسایی داده‌های حساس، اعمال سیاست‌های مبتنی بر نقش[2]، و ثبت دقیق سابقه دسترسی‌ها[3]، امکان نظارت مستمر و کنترل دقیق بر استفاده از داده‌ها را فراهم می‌کنند. چنین ابزارهایی

---

۱. آشنایی با ابزارهایی مانند Amazon Macie ، Cloudera Sentry و Hortonworks Ranger:

برنامه Cloudera Sentry ابزاری برای مدیریت سیاست‌های کنترل دسترسی مبتنی بر نقش (Role-Based Access Control یا RBAC) در محیط‌های توزیع‌شده داده، به‌ویژه پلتفرم Cloudera Hadoop است. این ابزار با فراهم ساختن امکان تعریف دقیق نقش‌ها و مجوزها، تضمین می‌کند که تنها کاربران مجاز قادر به مشاهده یا تغییر داده‌ها باشند. Sentry به‌گونه‌ای طراحی شده که بتواند سطح امنیت و حاکمیت داده را در سیستم‌های توزیع‌شده حفظ کند، و با ابزارهایی نظیر Impala ،Hive و Solr یکپارچگی کامل دارد. مزیت اصلی آن، نظارت دقیق بر مجوزهای دسترسی تا سطح جدول، ستون یا پایگاه‌داده است. برنامه Amazon Macie یک سرویس مدیریت‌شده امنیتی از شرکت آمازون است که با بهره‌گیری از یادگیری ماشینی، داده‌های حساس ذخیره‌شده در AWS (نظیر Amazon S۳) را شناسایی، طبقه‌بندی و پایش می‌کند. این ابزار به‌طور خاص برای کمک به حفاظت از داده‌های شخصی، مالی و دارای ارزش تجاری طراحی شده است. Macie می‌تواند فایل‌هایی را که حاوی اطلاعات شناسایی شخصی (PII) یا اطلاعات حساس دیگر هستند، شناسایی کرده و گزارش دهد. همچنین هشدارهایی نسبت به دسترسی‌های مشکوک یا تنظیمات نادرست ذخیره‌سازی ارائه می‌دهد، و در نتیجه نقش مهمی در رعایت الزامات قانونی و استانداردهای انطباق ایفا می‌کند. برنامه Apache Ranger، که توسط شرکت Hortonworks توسعه یافته است، یک چارچوب جامع برای مدیریت امنیت و حاکمیت داده در اکوسیستم Apache Hadoop است. این ابزار، امکان تعریف، اجرا و حسابرسی سیاست‌های دسترسی به داده‌ها را در سطوح مختلف فراهم می‌آورد. Ranger از مکانیسم‌های کنترل دسترسی مبتنی بر نقش، کاربر و منابع پشتیبانی می‌کند و می‌تواند بر اجزای مختلف Hadoop همچون HDFS، Hive، HBase، Knox، و Kafka اعمال شود. همچنین با رابط گرافیکی و APIهای قدرتمند، توانایی یکپارچگی با سیستم‌های هویت‌سنجی نظیر LDAP و Kerberos را دارد و ابزارهای تحلیلی برای بررسی رفتار کاربران و مدیریت ریسک فراهم می‌آورد.

۲. سیاست‌های دسترسی مبتنی بر نقش (Role-Based Access Control یا RBAC) یکی از متداول‌ترین الگوهای کنترل دسترسی در سامانه‌های اطلاعاتی است که به‌جای تخصیص مستقیم مجوز به هر کاربر، مجوزها را به «نقش‌ها» اختصاص می‌دهد و سپس کاربران به این نقش‌ها منتسب می‌شوند. هر نقش، مجموعه‌ای از مجوزهای لازم برای انجام وظایف خاص را دربرمی‌گیرد و کاربران بر اساس نقش شغلی یا عملیاتی خود، مجاز به دسترسی به منابع معین می‌شوند. این مدل موجب ساده‌سازی مدیریت مجوزها، افزایش مقیاس‌پذیری سامانه، و کاهش خطاهای انسانی در تخصیص دسترسی می‌شود. RBAC در بسیاری از سیستم‌های سازمانی و سامانه‌های داده‌محور، از جمله محیط‌های ابری، کلان‌داده و دولت الکترونیک، به‌کار گرفته می‌شود. همچنین، این مدل قابلیت انطباق با الزامات قانونی و استانداردهای امنیتی را تسهیل می‌کند.

۳. ثبت سوابق دقیق دسترسی‌ها (Audit Trails) به مجموعه‌ای از داده‌ها گفته می‌شود که جزئیات کامل مربوط به دسترسی کاربران به منابع اطلاعاتی را به‌صورت مستمر و منظم ثبت و نگهداری می‌کند. این سوابق معمولاً شامل اطلاعاتی مانند هویت کاربر، زمان دسترسی، نوع عملیات انجام‌شده، منابع مورداستفاده، و نتیجه اقدام (موفق یا ناموفق) هستند. هدف از ایجاد چنین ردپای دیجیتال، فراهم‌کردن امکان نظارت، کشف ناهنجاری‌ها، شناسایی رخنه‌های امنیتی و پاسخ‌گویی حقوقی یا سازمانی در برابر وقایع است. سامانه‌های ثبت سوابق بخشی ضروری از چارچوب‌های امنیت داده و انطباق قانونی‌اند و در محیط‌هایی با داده‌های حساس یا زیرساخت‌های حیاتی، نقش حیاتی دارند. این مکانیزم همچنین امکان ممیزی و بازبینی منظم فعالیت‌های کاربران و سامانه‌ها را فراهم می‌کند.

به‌ویژه در بسترهای توزیع‌شده و مقیاس‌پذیر پردازش کلان‌داده، نقش کلیدی در تسهیل تطبیق با الزامات حقوقی و ارتقای سطح پاسخگویی سازمان‌ها ایفا می‌کنند.[1]

۳-۳. نظام حمایت از پایگاه‌های داده

در اغلب نظام‌های حقوقی، حمایت از پایگاه‌های داده عمدتاً ناظر به ساختار و سازمان آن‌ها و ذیل مالکیت فکری، به‌ویژه کپی‌رایت[2]، ارزیابی می‌شود. حقوق مالکیت فکری یعنی مجموعه حق‌های منشأ یافته از خلاقیت‌های فکری در عرصه‌های صنعتی، ادبی، علمی و هنری[3]؛ لذا در بسیاری از کشورها، اگر گزینش و سامان‌دهی داده‌ها نوآورانه باشد، حق بهره‌برداری انحصاری به صاحب پایگاه تعلق می‌گیرد. با این‌حال، پایگاه‌های گسترده که تمامی اطلاعات ممکن را دربر می‌گیرند، از شرط گزینش برخوردار نبوده و امکان حمایت مؤلفانه کاهش می‌یابد؛ این حمایت صرفاً ناظر به ساختار است، نه محتوا.[4]

در اتحادیه اروپا، پایگاه‌های داده علاوه‌بر کپی‌رایت، از نظام حقوقی مستقل نیز برخوردارند. در امر تولید و گسترش دارایی‌های فکری، موضوع سرمایه‌گذاری دارای اهمیت بسیار است.[5] دستورالعمل ۱۹۹۶[6] اتحادیه اروپا پیش‌بینی می‌کند که حتی در نبود خلاقیت، اگر سرمایه‌گذاری قابل توجهی در گردآوری، اعتبارسنجی یا ارائه داده‌ها صورت گیرد، پایگاه مشمول «نظام خاص حمایتی»[7] می‌شود و کشورهای عضو موظف به اجرای آن‌اند.[8] مطابق ماده ۳، پایگاه دارای اصالت مشمول حمایت حق مؤلف است، اما بیشتر پایگاه‌ها به دلیل طراحی فنی صرف، واجد آن نیستند؛ بنابراین، سرمایه‌گذاری منجر به حمایت مؤلفانه نمی‌شود، اما این دو حمایت قابل جمع‌اند.[9]

نظام خاص حمایتی زمانی اعمال می‌شود که تولیدکننده منابع قابل‌توجه مالی، انسانی، فنی یا زمانی را صرف گردآوری، اعتبارسنجی و ارائه داده‌ها کرده باشد. ساختار پایگاه باید امکان بازیابی مستقل داده‌ها

---

1. Informatica, (n.d).
2. Copyright

۳. بزرگی، (۱۳۹۷)، ص ۱۱۶.

4. Europe, (n.d).

۵. بخت جو و کریمی، (۱۳۹۸)؛ ص ۱۴۴.

6. European Parliament and Council of the European Union. (1996). Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. Official Journal of the European Union, L77, 20-28.
7. Sui generis
8. Gervais, (2007); pp 1120-1126.

۹. برای مطالعه بیشتر مراجعه شود به:

- Davison, M. (2020). Databases and copyright protection, in T. Aplin (ed.), Research Handbook on Intellectual Property and Digital Technologies (Cheltenham: Edward Elgar).
- Minero, G. (2012). Did the Database Directive actually Harmonise the Database Copyright? Football Dataco Ltd. v. Britens Pools Ltd. and the ECJ's Rules against Subsistence of Database Copyright in Fixtures Lists. European Intellectual Property Review. pp 729-732.

را فراهم کند و این حمایت شامل پایگاه‌های غیرالکترونیکی و پویا نیز می‌شود.[1] این نظام دو کارکرد دارد: جلوگیری از استخراج تمام یا بخش عمده پایگاه توسط اشخاص ثالث و منع بازاستفاده از محتوای پایگاه. تفاوت این دو در آن است که استخراج جنبه انتخاب‌محور و ذهنی دارد، درحالی‌که بازاستفاده ناظر بر انتشار عمومی است.[2]

در اتحادیه اروپا، مفهوم سرمایه‌گذاری قابل توجه با معیار اصالت در کپی‌رایت تفاوت دارد. در نظام حق مؤلف، خلق اثر اصیل کفایت می‌کند، اما در رژیم حق ویژه، تأکید بر حجم و کیفیت سرمایه‌گذاری‌ها در گردآوری و ساختاردهی داده‌هاست[3]. این تمایز، به‌ویژه در تعامل با مقررات حفاظت از داده‌های شخصی، ممکن است پیچیدگی‌های حقوقی ایجاد کند.

در مقابل، در ایالات متحده تنها پایگاه‌های دارای خلاقیت ساختاری[4] مشمول کپی‌رایت‌اند. رأی دیوان عالی در یک پرونده شاخص[5]، گردآوری صرف داده‌های واقعی را از شمول حمایت خارج ساخت. در حقوق آمریکا نهادی مشابه نظام خاص اتحادیه اروپا وجود ندارد.[6] در ایران نیز ماده ۶۲ قانون تجارت الکترونیکی، پایگاه‌های داده را تحت حمایت مالکیت فکری قرار می‌دهد، اما در فقدان اصالت، به‌ویژه برای داده‌های صرفاً شخصی یا آماری، حمایت مؤلفانه با تردید مواجه است.[7]

۳-۴. تقابل حقوق ناشی از مالکیت فکری بر پایگاه داده و حق بر داده‌های شخصی

از چالش‌های اساسی در حقوق داده، تعیین حدود میان حقوق تولیدکنندگان پایگاه‌های داده و حقوق اشخاص موضوع داده‌هاست، به‌ویژه وقتی داده‌های شخصی در دل مجموعه‌های داده پردازش می‌شوند. با توجه به پیشرفت مداوم فناوری‌های داده‌محور، به‌ویژه کلان‌داده و هوش مصنوعی، اجرای حقوق انحصاری در این حوزه نیازمند تفسیرهای نو و مقررات دقیق‌تری است. در این میان، حمایت از منافع تولیدکنندگان و سرمایه‌گذاران نباید مانعی برای بهره‌برداری مشروع سایر بازیگران زنجیره ارزش داده، مانند

---

1. Graux, (2024).
2. European IP Helpdesk, (n.d).
۳. عالم زاده و دیگران، (۱۳۹۹)؛ صص ۱۰۵-۱۰۶.
4. Original works of authorship
5. Feist Publications, Inc. v. Rural Telephone Service Co., Inc., 499 U.S. 340.
۶. نظام خاص حمایتی پایگاه‌های داده در حال حاضر منحصر به حوزه حقوقی اروپا است و هیچ‌گونه حمایت معادل یا مشابهی در سایر نظام‌های حقوقی ملی یا در چارچوب معاهدات بین‌المللی وجود ندارد. همانند سایر انواع حقوق مالکیت فکری، حق انحصاری نسبت به پایگاه‌های داده نیز قابلیت انتقال، واگذاری یا اعطای مجوز از طریق قرارداد را دارد. از سوی دیگر، مشابه با نظام حق مؤلف، بهره‌مندی از حمایت قانونی برای این حق مستلزم ثبت رسمی نیست، اما در عمل، ثبت آن به‌منظور ایجاد امنیت حقوقی و تقویت جایگاه اقتصادی دارنده آن، توصیه می‌شود. نام انتخاب‌شده برای این حق مالکیت فکری جدید، در اصطلاحات رایج مالکیت فکری، نامأنوس به‌نظر می‌رسد: این حق، حق مؤلف نیست، بلکه یک حق مرتبط یا مجاور است و دارنده آن نیز مؤلف یا عنوانی مشابه نامیده نمی‌شود، بلکه پدیدآورنده پایگاه داده خوانده می‌شود. با این‌حال، حقوق مرتبط یا مجاوردیگری نیز وجود دارند که صرفاً از سرمایه‌گذاری انجام‌شده حمایت می‌کنند، مانند حق تهیه‌کنندگان آثار دیداری-شنیداری و موسیقایی یا حق شرکت‌های پخش رادیویی و تلویزیونی.
۷. صادقی و طهماسبی، (۱۳۸۶)؛ ص ۱۴۴.

توسعه‌دهندگان الگوریتم‌ها یا کاربران نهایی، ایجاد کند. ایجاد توازن میان این منافع گاه متعارض، محور اصلی در تفسیر نظام‌های حمایتی داده‌هاست.[1]

برای بررسی تعارض میان حق افراد بر داده‌های شخصی و حقوق شرکت‌ها در بهره‌برداری از پایگاه‌های داده، ابتدا باید حقوق متقابل طرفین شناسایی شود. در رأس این حقوق، حق بنیادین اشخاص نسبت به حریم خصوصی قرار دارد که مستلزم اطلاع‌رسانی شفاف و اخذ رضایت آگاهانه پیش از هرگونه پردازش است. همچنین، حقوقی مانند دسترسی، حذف و انتقال‌پذیری داده‌ها نیز برای افراد شناخته شده‌اند. این حقوق ممکن است با منافع تجاری شرکت‌ها در بهره‌برداری انحصاری از پایگاه‌های داده تعارض پیدا کنند، چراکه افشای یا حذف داده‌ها می‌تواند ارزش رقابتی آن‌ها را کاهش دهد.

مقررات عمومی حفاظت از داده‌ها در موادی مانند ۱۵ و ۲۰ و نیز در یادآوری شماره ۶۳[2]، به این تعارض‌ها اشاره دارد. مطابق ماده ۱۵، شخص موضوع داده حق دارد از وجود یا عدم وجود پردازش، محتوای داده‌های پردازش‌شده، و اطلاعاتی درباره اهداف و منطق پردازش آگاه شود و نسخه‌ای از داده‌های خود را دریافت کند. البته ماده ۱۵ تصریح می‌کند که اعمال حق دسترسی نباید ناقض حقوق و آزادی‌های دیگران باشد؛ عبارتی که می‌تواند شامل شرکت‌هایی باشد که پایگاه‌های داده را نگهداری می‌کنند. همین محدودیت در ماده ۲۰ درباره حق انتقال داده نیز آمده است. این حق به افراد اجازه می‌دهد داده‌های شخصی خود را در قالبی ساختارمند و قابل‌خواندن توسط ماشین دریافت و به کنترل‌کننده‌ای دیگر منتقل کنند؛ برای مثال، در مهاجرت از یک دستیار مجازی به دیگری. با وجود امکان بروز تعارض با حقوق مالکیت فکری، مقررات تصریح دارند که چنین انتقالی نباید به‌طور مطلق ممنوع شود و باید از طریق ملاحظات فنی و حقوقی مدیریت گردد. تفسیر غالب، به‌ویژه از سوی کارگروه ماده ۲۹، این شرط را ناظر بر حفظ داده‌های اشخاص ثالث می‌داند، نه جلوگیری کلی از انتقال داده‌ها به‌دلیل مالکیت شرکت‌ها.[3] اما درباره حق حذف یا حق انصراف از رضایت، چنین محدودیت‌هایی به‌صراحت ذکر نشده و در نتیجه، زمینه تفسیر و ابهام باقی مانده است. در این خصوص می‌توان گفت که حذف داده‌ها تابع قواعد عام مندرج در ماده ۱۷ می‌باشد[4]، حتی اگر در پایگاه‌های داده جای گرفته باشند.[5] با وجود این، بر اساس یادآوری شماره ۶۳ مقررات عمومی حفاظت از داده‌ها، افراد باید امکان دسترسی آسان

---

1. Gemma, (2021); p 738.

2. GDPR, art 15,20 & recital 63.

3. Article 29 Working Party, (2017a).

۴. متن ماده ۱۷: شخص موضوع داده‌ها حق دارد از کنترل‌کننده، حذف داده‌های شخصی مربوط به خود را بدون تأخیر غیرموجه، درخواست کند و کنترل‌کننده موظف است در صورت وجود یکی از دلایل زیر، داده‌های شخصی را بلافاصله حذف کند:

۱. داده‌های شخصی دیگر در رابطه با اهدافی که برای آن‌ها جمع‌آوری یا پردازش شده‌اند، ضروری نیستند، ۲. شخص موضوع داده رضایت خود را پس بگیرد و هیچ مبنای قانونی دیگری برای پردازش وجود نداشته باشد، ۳. شخص موضوع داده به پردازش اعتراض دارد و هیچ دلیل قانونی قاطعی برای پردازش وجود ندارد، ۴. داده‌های شخصی به‌طور غیرقانونی پردازش شده‌اند، ۵. داده‌های شخصی باید به دلیل رعایت یک الزام قانونی در قانون اتحادیه یا کشورهای عضو که کنترل‌کننده تابع آن است، پاک شوند.

5. Di Martino, (2019); pp 1-5.

و منظم به داده‌های شخصی خود، از جمله اطلاعات حساس مانند سوابق پزشکی، داشته باشند تا بتوانند مشروعیت پردازش را ارزیابی و در صورت لزوم آن را راستی‌آزمایی کنند. این دسترسی باید شامل اطلاعاتی درباره هدف پردازش، مدت نگهداری، گیرندگان، منطق پردازش خودکار (به‌ویژه در پروفایل‌سازی) و پیامدهای آن باشد. کنترل‌کننده‌ها نیز مکلف‌اند در صورت امکان، دسترسی امن و آنلاین به داده‌ها را برای افراد فراهم کنند. با این‌حال، اعمال این حق نباید ناقض حقوق و آزادی‌های دیگران، به‌ویژه مالکیت فکری بر نرم‌افزارها یا پایگاه‌های داده، باشد. با وجود این محدودیت، یادآوری مذکور تأکید دارد که وجود حق بر پایگاه‌داده نباید مانعی مطلق برای حق دسترسی افراد باشد. در نتیجه، هرچند مقررات اتحادیه اروپا در ظاهر میان حقوق مالکیت فکری و حق بر داده‌ها تعادلی محافظه‌کارانه برقرار کرده، اما تفسیرها نشان می‌دهند که حق دسترسی اشخاص موضوع داده، جز در موارد استثنایی و با توجیه مستدل، از اولویت برخوردار است.[1]

بنابر مطالب فوق، بر پایه مقررات عمومی حفاظت از داده‌ها، تنها دو حق، یعنی حق دسترسی و حق انتقال، در صورت تعارض با منافع دیگران، ممکن است با محدودیت‌هایی مواجه شوند. با این‌حال، حقوق انحصاری بر پایگاه‌های داده نمی‌تواند توجیهی برای تضعیف سایر حقوق بنیادین اشخاص موضوع داده، نظیر حق اطلاع‌رسانی، اصلاح، حذف، محدودسازی پردازش، اعتراض یا مصونیت از تصمیم‌گیری خودکار باشد. در این میان، حق اطلاع‌رسانی و حق اعتراض به تصمیم‌گیری‌های صرفاً خودکار، نقش محوری در حمایت از مصرف‌کنندگانی دارند که در معرض بهره‌برداری پنهان از داده‌هایشان توسط شرکت‌ها قرار می‌گیرند. حق اطلاع‌رسانی، تجلی اصل شفافیت در پردازش داده‌هاست؛ اصلی که در صدر اصول مندرج در ماده ۵ مقرره اروپا قرار دارد و متضمن الزام به آگاهی‌بخشی روشن، دقیق و صادقانه درباره نحوه، هدف و مسئول پردازش است. این تعهد، در شرایط استثنایی، به‌ویژه زمانی که داده‌ها از منابع ثالث به‌دست آمده باشند، ممکن است محدود شود. در چنین مواردی، شرط عدم اطلاع‌رسانی آن است که کاربر قبلاً مطلع شده باشد، اطلاع‌رسانی غیرممکن یا پرهزینه باشد، دستیابی به هدف پردازش را مختل کند، یا تعهدات قانونی و محرمانگی حرفه‌ای مانع افشای اطلاعات باشند.[2]

ماده ۴۸ دستورالعمل پایگاه داده اتحادیه اروپا ۱۹۹۶ تصریح می‌کند که حمایت از پایگاه‌های داده نباید ناقض مقررات حفاظت از داده‌های شخصی باشد. این ماده ضمن پذیرش هم‌زیستی حقوق مالکیت فکری و حقوق حریم خصوصی، تأکید دارد که حمایت از ساختار پایگاه داده نباید به محتوا، یعنی داده‌های شخصی، تسری یابد. برخی مراجع قضایی کشورهای عضو نیز پایگاه‌هایی حاوی اطلاعات مشتریان را مشروط به رعایت شرایط قانونی، مشمول حمایت دانسته‌اند؛ نشانه‌ای از تفکیک کارکرد و ماهیت این دو دسته حق.[3]

---

1. La Diega Noto & Sappa, (2020); p 442.
2. Article 29 Working Party, (2017b).
۳. عطار و پروین، (۱۴۰۰)؛ صص ۲۹۳-۲۹۵.

در حقوق ایران نیز ماده ۶ پیش‌نویس لایحه حمایت از داده‌ها تصریح می‌کند که مالکیت فکری بر داده‌ها نباید ناقض حقوق اشخاص موضوع داده باشد و در صورت تعارض، اولویت با حقوق اشخاص است. ماده ۵۱ قانون اجرای سیاست‌های کلی اصل ۴۴ نیز بیان می‌دارد که حقوق انحصاری ناشی از مالکیت فکری نباید موجب رویه‌های ضد رقابتی یا نقض سایر قوانین شود؛ شورای رقابت نیز مجاز به محدودسازی این حقوق در صورت بروز چنین تضادهایی خواهد بود.

یکی دیگر از چالش‌های اساسی در این زمینه، وضعیت حقوقی انتقال یا فروش پایگاه‌های داده، به‌ویژه زمانی است که شامل داده‌های شخصی می‌شوند. انتقال مالکیت بر پایگاه داده، به معنای آزادی مطلق در جابه‌جایی داده‌های اشخاص نیست و باید با رعایت الزامات قانونی مربوط به حفاظت از داده‌ها همراه باشد. شرکت انتقال‌دهنده موظف است تضمین کند که حقوق افراد، از جمله حق اطلاع، اعتراض، دسترسی، اصلاح یا حذف داده‌ها، نقض نشود. از منظر قراردادی نیز، انتقال‌دهنده باید مالک قانونی پایگاه بوده و اطمینان دهد که هیچ تعارضی با تعهدات پیشین یا قوانین جاری وجود ندارد.[۱] به‌ویژه در صورت وجود داده‌های حساس، این انتقال مشروط به اخذ رضایت صریح و آگاهانه از اشخاص موضوع داده خواهد بود. افزون بر این، حتی حق افشاء یا انتشار عمومی، که بخشی از حقوق مالک فکری محسوب می‌شود، در جایی که با داده‌های شخصی اشخاص ثالث تداخل دارد، باید تحت نظارت مقررات رازداری و حفاظت از داده‌ها اعمال شود. به‌این‌ترتیب، حاکمیت شرکت‌ها بر پایگاه‌های داده، مطلق نبوده و در صورت تعارض با حقوق بنیادین اشخاص، قابل تحدید خواهد بود.

در مجموع، گرچه مالکیت پایگاه‌های داده اصولاً قابل انتقال است[۲]، اما این انتقال نباید ناقض حقوق اشخاص موضوع داده‌ها باشد. در فرآیندهای انتقال، تیم‌های حقوقی و فنی باید ضمن شناسایی دارایی‌های فکری، به‌ویژه پایگاه‌های داده، ارتباط آن‌ها با حقوق افراد را به‌دقت بررسی و مدیریت کنند. این امر مستلزم تحلیل ریسک‌ها، تعهدات قراردادی و الزامات فنی مرتبط با انتقال داده‌ها است.[۳]

در بررسی‌های حقوقی، معمولاً تمرکز بر جنبه‌های رویه‌ای مانند وضعیت پرونده‌های مالکیت فکری است و به ارزیابی محتوایی و ماهیت داده‌ها کمتر توجه می‌شود. در حالی‌که توافق‌نامه‌های محرمانگی و شرایط استفاده می‌توانند نقش مهمی در حفاظت از داده‌های شخصی مرتبط با پایگاه داده ایفا کنند.[۴]

یکی از راه‌کارهای مکمل، اجرای فرآیندهای مستعارسازی یا ناشناس‌سازی پیش از انتقال پایگاه داده است. با این حال، این اقدامات نیز نوعی پردازش محسوب می‌شوند و باید مطابق مقررات پردازش ثانویه

---

۱. بیات و آزمندیان، (۱۴۰۲)؛ ص ۶۵.

۲. نعمتی و حسینی مقدم، (۱۳۹۹)؛ ص ۱۸۹.

3. Farhadi & Tovstiga, (2010); p 45.

4. Robins, (2008); p 324.

داده‌ها صورت گیرند تا هم از حقوق افراد محافظت شود و هم ریسک‌های حقوقی آتی کاهش یابد.

از منظر نظری، داده‌های شخصی به دلیل فقدان ویژگی‌هایی چون اصالت یا نوآوری، اصولاً مشمول حمایت مستقیم مالکیت فکری نیستند. این داده‌ها مواد اولیه محسوب می‌شوند، در حالی‌که حمایت فکری معطوف به محصول نهایی یا اثر خلاقانه است. تفکیک این دو سطح از داده، از بروز تعارض میان نظام‌های حمایتی جلوگیری می‌کند و از سوی دیگر، بهره‌برداری انحصاری از پایگاه‌های داده حاوی اطلاعات شخصی، چنانچه بدون رعایت مقررات داده انجام شود، می‌تواند نه‌تنها منافع مصرف‌کنندگان را تهدید کند، بلکه به منافع شرکت نیز لطمه بزند.

در نتیجه، تلفیق حقوق مالکیت فکری با حمایت از داده‌های شخصی مستلزم رویکردی منسجم و سنجیده است که ضمن پاسداشت حقوق فکری شرکت‌ها، به حقوق و آزادی‌های اشخاص موضوع داده نیز احترام گذارد. هرگونه پردازش و انتقال داده‌های شخصی باید منوط به رعایت کامل مقررات حفاظت از داده و اتخاذ تدابیر فنی و حقوقی مناسب باشد. البته از آنجایی‌که بسیاری از شرکت‌ها در حوزه طراحی و مدیریت پایگاه‌های داده فعالیت می‌کنند و منافع مشروع تجاری ایشان به شکل غیرمستقیم از طریق عنصر خلاقانه موجود در این پایگاه‌ها تامین می‌شود، ممکن است حقوق شرکت نیز با سو استفاده از مفاهیمی مثل حق بر داده‌های شخصی مورد تضییع، به‌ویژه توسط رقبا، قرار گیرد.[1] بنابراین برقراری این توازن، برای پیشگیری از سو استفاده و نقض حقوق فکری شرکت‌ها از یک سو و همچنین تقویت اعتماد کاربران و تضمین شفافیت و مشروعیت فرآیندهای پردازش و انتقال داده، امری حیاتی است.

۴. تحلیل ظرفیت‌های موجود نظام حقوقی ایران

در نظام حقوقی ایران، علیرغم نبود قانون جامع و خاص حفاظت از داده‌های شخصی، پایه‌های قانونی و فقهی متعددی وجود دارد که می‌تواند هم‌اکنون ظرفیت‌هایی بنیادین برای حمایت از حقوق اشخاص در حوزه داده‌ها فراهم کند. این ظرفیت‌ها، هرچند نیازمند تفسیر و به‌روزآوری حقوقی است، اما در وضعیت فعلی قابل استخراج و بهره‌برداری‌اند.

در سطح بنیادین، اصول قانون اساسی که بر مصونیت حیثیت و حقوق اشخاص تأکید دارند (اصل ۲۲)، اجازه نمی‌دهند پردازش بی‌ضابطه داده‌ها به تعرض به حریم خصوصی یا لطمه به شأن فردی بینجامد. داده شخصی را می‌توان ذیل حقوق اشخاص و در مواردی ذیل حیثیت تحلیل کرد؛ بنابراین گردآوری، تجمیع و تحلیل گسترده داده‌ها در قالب کلان‌داده، اگر بدون مبنای قانونی یا خارج از حدود ضرورت باشد، با این چارچوب ناسازگار است. همچنین ممنوعیت تجسس و افشای مکاتبات و ارتباطات (اصل ۲۵)، ستون حمایتی

---

۱. شاکری و حاجی حسینی، (۱۳۹۹)؛ ص ۷۵.

مهمی در برابر شنود، استخراج و پردازش غیرمجاز داده‌های ارتباطی و دیجیتال است. افزون بر این، منع تفتیش عقاید (اصل ۲۳) اهمیت ویژه‌ای در برخورد با داده‌های حساس، پروفایل‌سازی و تصمیم‌گیری‌های خودکار دارد؛ به‌ویژه زمانی که تحلیل داده‌ها به امتیازدهی، طبقه‌بندی یا محروم‌سازی افراد منجر می‌شود، این فرایند باید با تضمین‌های مربوط به برابر در قانون اساسی و عدم تبعیض سازگار باشد.

در حوزه حقوق مدنی، مواد ۳۰ و ۳۱ قانون مدنی حق انتفاع و تصرف مالک را به رسمیت می‌شناسند، اما آن را مقید به عدم اضرار به غیر می‌دانند. این قید، کلید حل تعارض است: مالکیت بر ساختار و سازمان‌دهی پایگاه داده به معنای مالکیت مطلق بر داده شخصی خام نیست. بهره‌برداری از پایگاه، اگر به زیان نامتعارف اشخاص منجر شود، از حمایت کامل مالکانه برخوردار نخواهد بود. افزون بر این، قواعد اتلاف و تسبیب در قانون مدنی (مواد ۳۲۸ و ۳۳۱) مقرر می‌کنند هر کس موجب تلف یا ورود خسارت به مال دیگری شود، ضامن است. در بستر داده، افشای غیرمجاز، حذف، دستکاری یا نشت اطلاعات می‌تواند منشأ مسئولیت باشد. قانون مسئولیت مدنی نیز این پیوند را تقویت می‌کند. هرگونه لطمه به حیثیت، آزادی یا هر حق دیگر افراد، اعم از عمدی یا ناشی از بی‌احتیاطی، موجب مسئولیت و جبران خسارت است (ماده ۱) و حتی خسارت معنوی نیز قابل مطالبه است (ماده ۱۰). بدین‌ترتیب، افشای داده شخصی، پردازش غیرمجاز، پروفایل‌سازی زیان‌بار یا قصور در تأمین امنیت سامانه‌ها می‌تواند ذیل لطمه به حیثیت یا حقوق اشخاص قرار گیرد. این ظرفیت، در وضعیت فعلی، مهم‌ترین پل برای ارائه راه‌کار عملی در برابر سو استفاده از داده‌ها است.

در سطح کیفری، قانون جرایم رایانه‌ای با جرم‌انگاری دسترسی و شنود غیرمجاز، تخریب، جعل، افشا و نقض امنیت سامانه‌ها، نشان می‌دهد که برخی اشکال تعرض به داده شخصی صرفاً تخلف مدنی نیست، بلکه می‌تواند وصف کیفری نیز داشته باشد. در نتیجه، استخراج یا افشای بدون مجوز داده‌های شخصی در کلان‌داده‌ها، بسته به مورد، می‌تواند مسئولیت دوگانه مدنی و کیفری ایجاد کند.

قانون تجارت الکترونیکی نیز با تأکید بر حمایت از داده‌پیام، محرمانگی و شفافیت اطلاعاتی در تعاملات الکترونیکی (ماده ۵۸ به بعد)، مبنایی برای لزوم اطلاع‌رسانی و رعایت رضایت در پردازش داده‌های کاربران فراهم می‌آورد. از سوی دیگر، قانون انتشار و دسترسی آزاد به اطلاعات، ضمن حمایت از شفافیت، استثنائات مربوط به حریم خصوصی را به رسمیت می‌شناسد؛ این تفکیک نشان می‌دهد که حتی در نظام حقوقی ایران، دسترسی و بهره‌برداری از اطلاعات حتی با انگیزه شفافیت و تامین منافع عمومی، همواره مقید به حفظ حقوق شخصی است.

در نهایت، مبانی فقهی این چارچوب را تکمیل می‌کند. قاعده لاضرر مانع آن است که مالک پایگاه از حق خود به‌گونه‌ای استفاده کند که موجب ضرر نامتعارف به اشخاص شود. قاعده تسلیط، به‌طور

معقول، نوعی حق کنترل فرد بر اطلاعات مرتبط با خود را توجیه می‌کند، هرچند این حق مطلق نبوده و در چارچوب نظم عمومی محدود می‌شود. حرمت تجسس، مبنای نقد گردآوری و ردیابی پنهانی داده‌هاست و قواعد اتلاف و تسبیب، ضمان ناشی از نشت یا پردازش ناامن داده را توجیه می‌کنند. همچنین احترام به مال و حق در فقه، امکان حمایت از داده شخصی را، حتی اگر مال در تعریف سنتی تلقی نشود، به‌عنوان حقی محترم فراهم می‌آورد.

برآیند این قواعد نشان می‌دهد که به‌عنوان یک راه‌کار موقت، بر مبنای منابع موجود در حقوق ایران، می‌توان میان حقوق شرکت‌ها نسبت به تحلیل کلان داده‌ها و مالکیت بر پایگاه داده به‌عنوان یک ساختار اطلاعاتی و حقوق اشخاص نسبت به داده‌های شخصی مربوط به خود تمایز قائل شد.

۵. نتیجه‌گیری و توصیه‌های سیاستی

تعارض میان حق بر داده‌های شخصی و حق بهره‌برداری از پایگاه‌ها و کلان‌داده‌ها در واقع نزاعی درباره تعیین حدود مشروع استفاده از اطلاعاتی است که مستقیماً با هویت و زندگی افراد پیوند دارند. از یک سو، ایجاد و بهره‌برداری از پایگاه‌های داده حاصل سرمایه‌گذاری فنی و اقتصادی و مشمول حمایت مالکیت فکری است؛ از سوی دیگر، داده‌های شخصی درون آن، تجلی حق بر حریم خصوصی و آزادی فردی بوده و نمی‌توان آن‌ها را دارایی صرف بهره‌بردار دانست. بنابراین هدف، طراحی سازوکاری است که اعمال حق بر کلان داده‌ها و مالکیت بر ساختار پایگاه داده را با حق کنترل اشخاص بر داده‌های خود در تعادل نگه دارد.

در نظام‌های پیشرفته مانند اتحادیه اروپا، این توازن به کمک مقرراتی چون مواد ۱۵ و ۲۰ مقررات عمومی حمایت از داده‌ها برقرار شده است که زیربنای آن شفافیت، پاسخ‌گویی و رعایت منافع مشروع هر دو طرف است. بهره‌گیری از فناوری‌های نوین مانند رمزگذاری هومومورفیک، مستعارسازی و کنترل دسترسی سلسله‌مراتبی نیز ابزار مکمل برای تحقق امنیت داده و تقلیل ریسک افشا محسوب می‌شود. افزون بر این، حقوق انحصاری پایگاه‌های داده نباید به داده‌های خام و شخصی تسری یابد، زیرا این داده‌ها فاقد اصالت لازم برای حمایت فکری‌اند. در تعارض میان حق بر داده‌های شخصی و حق انحصاری ناشی از پایگاه داده، باید به اصول بنیادین حقوق بشر، و اصل تقدم منافع اشخاص بر منافع اقتصادی صرف، توجه ویژه داشت.

در وضعیت فعلی حقوق ایران، هرچند قانون جامع حفاظت از داده‌های شخصی وجود ندارد، اما ترکیب مقررات پراکنده می‌تواند مبنای اقدام عملی باشد. تفسیر موسع از قانون مسئولیت مدنی امکان می‌دهد نقض یا افشای بدون مجوز داده‌های شخصی، لطمه به حیثیت و امنیت روانی تلقی شود و علاوه‌بر خسارت مادی، خسارت معنوی نیز قابل مطالبه باشد. این امر داده‌های شخصی را در قلمرو حمایت مدنی می‌نشاند.

در کنار آن، تنظیم قراردادی و رضایت آگاهانه می‌تواند بنیان پردازش مشروع باشد، مشروط بر آن‌که رضایت به شکل صریح، محدود به هدف مشخص، قابل اثبات و قابل رجوع، ارائه گردد. اصل شفافیت و حداقل‌گرایی داده نیز اقتضا دارد داده‌ها فقط در حد ضرورت جمع‌آوری شوند و کاربران از هدف و دامنه پردازش کاملاً مطلع باشند. این اصول را می‌توان با استناد به قواعدی چون حسن نیت و منع اضرار، حتی در نبود قانون خاص، جاری ساخت.

برای کارآمدی این چارچوب، باید ضمانت‌اجراهای تدریجی پیش‌بینی شود: از جبران خسارت مادی و معنوی تا دستور توقف پردازش یا انتشار داده، حذف یا اصلاح اطلاعات نادرست و در موارد لازم منع ادامه بهره‌برداری از داده‌های موضوع اختلاف و همچنین در موارد شدید، اعمال مجازات کیفری طبق قانون جرایم رایانه‌ای. نهادهای عمومی نیز در صورت نقض تعهدات داده‌ای، باید پاسخ‌گوی مسئولیت‌های اداری و انتظامی باشند.

برآیند این رویکرد نشان می‌دهد که حتی پیش از تصویب قانون جامع حفاظت از داده‌ها، می‌توان چارچوبی عملی برای کنترل سو استفاده از داده‌های شخصی در قالب کلان داده یا پایگاه‌های داده ایجاد کرد. با این‌حال، برای رفع ابهام‌های موجود و ایجاد تعادل پایدار میان نوآوری‌های داده‌محور و حقوق بنیادین اشخاص، ضروری است تدوین یک قانون جامع حمایت از داده‌های شخصی در دستور کار قرار گیرد؛ قانونی که نه‌تنها بر پایه اصول بنیادین حمایت از داده‌های شخصی، همچون شفافیت، رضایت آگاهانه، محدودیت هدف، و امنیت داده، استوار باشد، بلکه به‌گونه‌ای طراحی شود که توان پاسخ‌گویی به چالش‌های ناشی از ادغام داده‌ها در فرآیندهای نوین فناورانه نظیر یادگیری ماشینی، تحلیل پیش‌بینانه و هوش مصنوعی را نیز داشته باشد. در این چارچوب، در صورت تصویب چنین مقرره‌ای، درج مواد زیر پیشنهاد می‌شود:

ماده ۱، اصول عمومی در پردازش داده‌های شخصی و بهره‌برداری از کلان‌داده‌ها

۱. پردازش، گردآوری، تجمیع یا تحلیل داده‌های شخصی باید بر اساس اصل رضایت آگاهانه، ضرورت هدف، و شفافیت انجام گیرد.

۲. دارندگان پایگاه‌های داده و بهره‌برداران کلان‌داده موظف‌اند پیش از هرگونه پردازش، تأثیر احتمالی عملیات خود بر حریم خصوصی اشخاص را ارزیابی و گزارش آن را در دسترس نهاد ناظر قرار دهند.

۳. داده‌های شخصی باید به‌صورت ناشناس یا مستعار ذخیره و فقط تا زمان تحقق هدف مشخص‌شده نگهداری شوند.

۴. استفاده ثانویه از داده‌ها، انتقال فرامرزی یا تجاری‌سازی آن‌ها بدون رضایت جدید و صریح اشخاص ممنوع است.

۵. اشخاص موضوع داده حق دارند به داده‌های خود دسترسی داشته، آن را اصلاح یا حذف کنند، و در صورت امکان، انتقال‌پذیری داده‌ها را درخواست نمایند.

تبصره ۱: داده شخصی هرگونه داده مرتبط با شخص حقیقی قابل‌شناسایی است.

تبصره ۲: پردازش داده‌های ناشناس‌شده در صورتی مجاز است که بازشناسایی اشخاص با هزینه یا تلاش متعارف ممکن نباشد.

تبصره ۳: حق مالکیت فکری بر ساختار پایگاه داده نافی حقوق اشخاص نسبت به داده‌های شخصی مندرج در آن نیست. در تعارض میان منافع اقتصادی دارنده پایگاه و حق حریم اشخاص، حفظ حریم شخصی و کرامت انسانی مقدم است.

ماده ۲، ضمانت اجراها و نهاد ناظر

۱. نقض مفاد ماده ۱، حسب مورد، موجب مسئولیت مدنی، اداری و کیفری است. دادگاه می‌تواند حکم به جبران خسارت مادی و معنوی، توقف پردازش یا حذف داده صادر کند.

۲. هر شخصی که از پردازش یا افشای غیرمجاز داده متضرر شود، حق طرح دعوی نزد دادگاه صالح یا نهاد ناظر دارد.

۳. نهاد ناظر ملی حفاظت از داده‌های شخصی با صلاحیت فنی و حقوقی تشکیل می‌شود و وظیفه نظارت بر اجرای این مقررات، صدور مجوز انتقال داده، اعمال جریمه‌ها و ارزیابی پروژه‌های کلان‌داده‌ای را بر عهده دارد.

۴. انتقال یا فروش پایگاه داده‌ای که شامل داده‌های شناسایی‌شده است، فقط با تأیید نهاد ناظر و رعایت مقررات امنیتی مجاز است.

۵. در صورت استفاده از داده‌های شخصی در سامانه‌های هوش مصنوعی یا الگوریتم‌های پیش‌بینانه، رعایت اصل قابلیت توضیح تصمیمات خودکار و جلوگیری از تبعیض الگوریتمی الزامی است.

تبصره ۱: میزان جریمه‌ها و نحوه رسیدگی به تخلفات طبق آیین‌نامه‌ای است که ظرف شش ماه از تصویب این قانون به پیشنهاد نهاد ناظر و تأیید هیأت وزیران تدوین می‌شود.

تبصره ۲: داده‌های جمع‌آوری‌شده توسط نهادهای عمومی مشمول همان الزامات امنیت، شفافیت و رضایت آگاهانه‌اند و استفاده آن‌ها برای مقاصد غیرمرتبط ممنوع است.

تبصره ۳: این قانون با الهام از اصول بین‌المللی حمایت از داده‌ها از جمله مقررات اتحادیه اروپا تفسیر می‌شود، مگر آنکه با اصول بنیادین حقوق داخلی ناسازگار باشد.

دسترسی به داده

- داده‌های استفاده شده یا تولید شده در این پژوهش در متن مقاله ارائه شده است

تعارض منافع نویسندگان

- نویسندگان این مقاله اعلام می‌کنند که هیچ‌گونه تضاد منافعی در رابطه با نویسندگی و یا انتشار این مقاله ندارند.

منابع

- بخت جو، روح الله و کریمی، عباس، (۱۳۹۸)، تحولات نوین حمایت حقوقی از اسرار تجاری در بخشنامه جدید ۲۰۱۶ اتحادیه اروپا با مطالعه تطبیقی در حقوق ایران، پژوهشنامه بازرگانی، ۲۳(۹۰)، ۱۴۱-۱۶۸.
- بزرگی، وحید، (۱۳۹۷)، نظام حقوق مالکیت فکری مناسب برای کشورهای درحال توسعه: با اشاراتی در مورد ایران، پژوهشنامه بازرگانی، ۲۲(۸۸)، ۱۱۵-۱۵۴.
- بیات، فرهاد و آزمندیان، محمد صادق، (۱۴۰۲)، قراردادهای استارتاپی با تاکید بر قراردادهای مالکیت فکری، چاپ اول، دادبانان دانا، تهران.
- شاکری، زهرا و حاجی حسینی، علی، (۱۳۹۹)، نظام حقوقی حمایت از روش‌های کسب و کار؛ آموزه‌هایی برای استارتاپ‌ها، پژوهشنامه بازرگانی، ۲۴(۹۴)، ۷۵-۱۰۵.
- صادقی، محمود و طهماسبی، علی، (۱۳۸۶)، درآمدی بر حمایت از حقوق پدیدآورنده پایگاه داده، مجله فقه و حقوق، ۴(۱۳)، ۱۳۱-۱۵۲.
- عالم زاده، محمد و فرهادی، دانیال و طالقان غفاری، مهدی، (۱۳۹۹)، واکاوی تطبیقی ارتباط حق مالکیت فکری ناشی از اختراعات دارویی با حق بر سلامت از منظر قوانین موضوعه ایران و موافقت‌نامه تریپس، پژوهشنامه حقوق تطبیقی، 4(2)، 103-117، Doi: 10.22080/lps.2021.20423.1212.
- عطار، شیما، (۱۴۰۰)، جایگاه داده و کلان داده در نظام حقوق اموال و مالکیت در ایران و فرانسه، رساله دکتری، دانشکده حقوق، دانشگاه علامه طباطبایی، تهران.
- عطار، شیما و پروین، فرهاد، (۱۴۰۰)، حقوق اتحادیه اروپا و چالش شناسایی حق مالکیت بر داده‌ها در عصر اقتصاد دیجیتال، مجله حقوقی بین‌المللی، ۳۸(۶۵)، ۲۸۱-۳۰۴، Doi: 10.22066/cilamag.2021.245186.
- قربان نیا، امیرمحمد، (۱۴۰۳)، وضعیت حقوقی داده‌های اشخاص در فرض تملک و ادغام شرکت‌ها، پایان‌نامه کارشناسی ارشد، حقوق خصوصی، دانشگاه تهران.
- متولی، محمد مهدی و ظهوری آرام، رضا و الماسی، مهرداد، (۱۳۹۶)، مدیریت کلان داده با اکوسیستم هادوپ، چاپ اول، راستینو، تهران.
- نعمتی، احسان و حسینی مقدم، سیدحسن، (۱۳۹۹)، مطالعه تطبیقی سرقت علمی در حقوق ایران و اتحادیه اروپا، پژوهشنامه حقوق تطبیقی، ۴(۲)، ۱۸۰-۱۹۹، Doi: 10.22080/lps.2020.18367.1169.

- Agh, Jeren. (2020). The impact of the GDPR on Big Data. Available at: (https://techgdpr.com/blog/impact-of-gdpr-on-big-data/). Visited 2025/07/12.
- Alamzadeh, Mohammad & Farhadi, Danial & Taleghan Ghaffari, Mehdi. (2020). Comparative analysis of the relationship between intellectual property rights arising from pharmaceutical inventions and the right to health from the perspective of Iranian statutory laws and the TRIPS Agreement. Comparative Law Journal, 4(2), 103-117. Doi: 10.22080/lps.2021.20423.1212. [in Persian]
- Article 29 Working Party. (2017a). Guidelines on the right to data portability 16/EN WP 242 rev.01. Available at: (https://ec.europa.eu/newsroom/article29/items/611233/en). Visited 2025/07/15.
- Article 29 Working Party. (2017b). Guidelines on transparency under Regulation 2016/679, 2018/WP260 rev.01. Available at: (https://ec.europa.eu/newsroom/article29/items/622227/en). Visited 2025/07/15.
- ASPE. (2018). To Big Data or Not: Determining the Use of Big Data. Available at: (https://aspe.hhs.gov/sites/default/files/migrated_legacy_files//192001/ToBigData.pdf). Visited 2025/07/14.
- Attar, Shima. (2021). The Position of Data and Big Data in the Property and Ownership Law of Iran and France. PhD Dissertation. Faculty of Law, Allameh Tabataba'i University. Tehran. [in Persian]
- Attar, Shima & Parvin, Farhad. (2021). European Union Law and the Challenge of Recognizing Ownership Rights over Data in the Age of Digital Economy. International Law Journal. 38(65), 281-304. Doi: 10.22066/cilamag.2021.245186. [in Persian]

- Bakhtjoo, Ruhollah & Karimi, Abbas, (2019), New developments in the legal protection of trade secrets in the new 2016 European Union directive with a comparative study in Iranian law, Journal of Trade Studies, 23(90), 141-168. [in Persian]
- Bayat, Farhad & Azmandian, Mohammad Sadegh. (2023). Startup Contracts with Emphasis on Intellectual Property Contracts. 1st ed. Dadbanan Dana. Tehran. [in Persian]
- Big Data LDN. (n.d). The 3 Vs explained. Available at: (https://www.bigdataldn.com/en-gb/blog/data-engineering-platforms-architecture/big-data-the-3-vs-explained.html). Visited 2025/07/20.
- Bozorgi, Vahid, (2018), An appropriate intellectual property rights system for developing countries: with some references to Iran, Journal of Trade Studies, 22(88), 115-154, [in Persian].
- Čtvrtník, M. (2023). Data Minimisation—Storage Limitation—Archiving. In: Archives and Records. Palgrave Macmillan, Cham. Doi: 10.1007/978-3-031-18667-7_8.
- Chancey, Tyler. (2024). Big Data Privacy Issues: Protect Your Data with Advanced Analytics and Security. Available at: (https://www.scarlettgroup.com/big-data-privacy-concerns). Visited 2025/07/13.
- Di Martino, M. (2019). Personal information leakage by abusing the GDPR "Right of access". In Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security (SOUPS'19), USENIX Association. USA.
- Elmasri, R., & Navathe, S. B. (2015). Fundamentals of Database Systems. 7th ed. Pearson. London.
- Europe. (n.d). Database protection. Available at: (https://europa.eu/youreurope/business/running-business/intellectual-property/database-protection/index_en.htm). Visited 2025/07/10.
- European IP Helpdesk. (n.d). FAQs on Database Protection. Available at: (https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/european-ip-helpdesk/europe-frequently-asked-questions_en#Database_Protection_Domain_Protection). Visited 2025/07/12.
- Farhadi, Mehdi & Tovstiga, George. (2010). Intellectual property management in M&A transactions. Journal of Strategy and Management. 3(1), 32-49. Doi: 10.2139/ssrn.1357332.
- Gemma, Minero Alejandre. (2021). Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. European Review of Private Law. 5, 733-756. Doi: 10.54648/erpl2021039.
- Gervais, Daniel J. (2007). The Protection of Databases. 82 Chicago-Kent Law Review, 1109-1168.
- Ghorban nia, Amir Mohammad. (2024). Legal Status of Personal Data in the Event of Ownership and Company Mergers. Master's Thesis. University of Tehran. [in Persian]
- Graux, Hans. (2024). What is data ownership, and does it still matter under EU data law? Available at: (https://data.europa.eu/sites/default/files/report/What%20is%20data%20ownership%2C%20and%20does%20it%20still%20matter%20under%20EU%20data%20law.pdf). Visited 2025/07/12).
- Informatica. (n.d). Big Data and Privacy: What It Is and What You Need to Know. Available at: (https://www.informatica.com/resources/articles/what-is-big-data-privacy.html). Visited 2025/07/10.
- Jha, Anupama, Dave, Meenu & Supriya, Madan. (2017). Big Data Security and Privacy: A Review on Issues, Challenges and Privacy Preserving Methods. International Journal of Computer Applications. 177(4), 87-93. Doi: 10.47392/IRJASH.2025.011.
- La Diega Noto, Guido & Sappa, Cristiana. (2020). The Internet of Things at the Intersection of Data Protection and Trade Secrets: Non-Conventional Paths to Counter Data Appropriation and Empower Consumers. European Journal of Consumer Law. 3, 419-458.
- Motavalli, Mohammad Mehdi, Zahoori Aram, Reza & Almasi, Mehrdad. (2017). Big Data Management with Hadoop Ecosystem. 1st ed. Rastino. Tehran. [in Persian]

- Moryl, Beata & Synowiec, Sebastian. (2024). What is Privacy by Design and Privacy by Default under the GDPR. Available at: (https://piwikpro.de/blog/privacy-by-design-und-privacy-by-default/). Visited 2025/07/12. [in German]
- Nemati, Ehsan & Hosseini Moghadam, Seyed Hassan. (2020). A Comparative Study of Plagiarism in Iranian and European Union Law. Comparative Law Research Journal, 4(2), 180-199. Doi: 10.22080/lps.2020.18367.1169. [in Persian]
- Pavlidis, G. (2024). Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI. Law, Innovation and Technology. 16(1), 293-308. Doi: 10.1080/17579961.2024.2313795.
- Radoń, Barbara Anna. (2015). Trade Secrets Protection for 'Big Data': Personal Data as Trade Secrets in the European Union. Master Thesis. MIPLC. Munich.
- Robins, Martin B. (2008). Intellectual Property and Information Technology Due Diligence in Mergers and Acquisitions: A More Substantive Approach Needed. U. Ill. J. L. Tech. & Pol'y, 320-356.
- Sadeghi, Mahmoud & Tahmasebi, Ali. (2007). An Introduction to Legal Protection of Database Creators. Fiqh and Law Journal. 4(13), 131-152. [in Persian]
- Shakeri, Zahra and Haji Hosseini, Ali. (2019). Legal System Supporting Business Methods; Lessons for Startups, Journal of Business Research, 24(94), 75-105. [in Persian]
- Trail. (2024). EU AI Act: How risk is classified. Available at: (https://www.trail-ml.com/blog/eu-ai-act-how-risk-is-classified). Visited 2025/07/25).
- Velivela, Gopinath, Rao, Krishna, Challa, Yallamanda & Prakash, Purna. (2016). The Journey of Big Data: 3 V's to 32 V's. ISSN ONLINE. 5(3), 169-175.
- Zhou, Lina, Pan, Shimei, Wang, Jianwu & Vasilakos, Athanasios V. (2017). Machine learning on big data: Opportunities and challenges. Neurocomputing. 237, 350-361. Doi: 10.1016/j.neucom.2017.01.026.