Received: 09/05/2024
Review: 05/08/2024
Accepted: 12 /09/2024
DOI: 10.22054/jocl. 2035.85063.4533

Journal of Cyber Law
No(2),Vol(1) 84-103.
ISSN: 0972-6934
www.jocl.ir

Big Data Ownership from the Perspective of Intellectual Property Rights

Nazanin Yousefi [1], Sara Afshari [*2]

1- Ph.D. Student in Law, Islamic Azad University, Arak, Iran.

2*- Ph.D. Student in Law, Islamic Azad University, Arak, Iran.

ABSTRACT

With Big data, as a fundamental pillar of the digital era and knowledge-based economy, plays a central role in the production, processing, and analysis of complex information, and due to its large volume, variety, and high velocity, traditional methods are often insufficient. The main research question of this study is how ownership of data and related responsibilities can be identified and regulated within the framework of intellectual property rights. The importance of this topic lies in the fact that effective utilization of data enables innovation, economic security, and prevention of unauthorized use, while the absence of a comprehensive legal framework can pose a threat to technological development and the digital economy. This article aims to examine and analyze the role of intellectual property rights in protecting data ownership and determining direct and indirect responsibilities arising from the use of big data. The research method is descriptive-analytical and based on documentary and comparative study, analyzing laws, regulations, and relevant practices at national and international levels to identify legal challenges and opportunities for data utilization. The findings indicate that combining intellectual property tools, including copyright, patents, and trade secrets, along with contracts and security technologies, can establish a secure and sustainable legal framework for managing big data. Furthermore, identifying direct and indirect responsibilities of various entities and developing precise protective policies enhances economic security and promotes innovation. The innovation of this study lies in providing an integrated legal–technological solution for lawful and secure utilization of big data, contributing to the development of the digital economy and improvement of data-driven policymaking.

Keywords:
Big Data, Data Ownership, Intellectual Property Rights, Legal Responsibility

How to Cite: Afshari, S. and Yousefi, N. (2024). Big Data Ownership from the Perspective of Intellectual Property Rights. Cyber Law, 1(2), 84-103.
DOI: 10.22054/jocl.2035.85063.4533

* Corresponding Author: sara.afshari@iauarak.ac.ir

نشریه حقوق سایبری
شماره (۲) ۱۰۳-۸۴
دوره ۱۴۰۳

تاریخ دریافت: ۱۴۰۳/۰۲/۲۰
تاریخ اصلاح: ۱۴۰۳/۰۵/۱۵
تاریخ پذیرش: ۱۴۰۳/۰۶/۲۲

مالکیت داده‌های بزرگ از منظر حقوق مالکیت فکری

نازنین یوسفی [۱]، سارا افشاری [۲*]

۱- دانشجوی دکتری حقوق، دانشگاه آزاد اسلامی، اراک، ایران.

۲ - دانشجوی دکتری حقوق، دانشگاه آزاد اسلامی، اراک، ایران.

چکیده

داده‌های بزرگ به‌عنوان یکی از ارکان اساسی عصر دیجیتال و اقتصاد دانش‌بنیان، نقش محوری در تولید، پردازش و تحلیل اطلاعات پیچیده دارند و به دلیل حجم زیاد، تنوع و سرعت بالای تولید، امکان استفاده از روش‌های سنتی را محدود کرده‌اند. اهمیت این موضوع از آن جهت است که بهره‌برداری مؤثر از داده‌ها، تضمین نوآوری، امنیت اقتصادی و جلوگیری از سوءاستفاده‌های غیرمجاز را ممکن می‌سازد، و فقدان یک چارچوب قانونی جامع می‌تواند تهدیدی برای توسعه فناوری‌ها و اقتصاد دیجیتال محسوب شود. هدف این مقاله بررسی و تحلیل نقش حقوق مالکیت فکری در حمایت از مالکیت داده‌ها و تعیین مسئولیت‌های مستقیم و غیرمستقیم ناشی از استفاده از داده های بزرگ است. روش پژوهش در این مقاله توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی و تطبیقی است و با تحلیل قوانین، مقررات و رویه های مرتبط در سطح ملی و بین‌المللی، چالش‌ها و فرصت‌های قانونی بهره‌برداری از داده‌ها مورد بررسی قرار گرفته است. نتایج تحقیق نشان می‌دهد که استفاده از ترکیبی از ابزارهای حقوق مالکیت فکری، از جمله حق مؤلف، پتنت و اسرار تجاری، همراه با قراردادها و فناوری های امنیتی، می تواند چارچوبی قانونی، امن و پایدار برای مدیریت داده های بزرگ ایجاد کند. همچنین شناسایی مسئولیت های مستقیم و غیرمستقیم نهادهای مختلف و تدوین سیاست های حفاظتی دقیق، موجب ارتقای امنیت اقتصادی و تشویق نوآوری می‌شود. نوآوری این پژوهش در ارائه راهکار یکپارچه حقوقی–فناورانه برای بهره‌برداری قانونی و امن از داده‌های بزرگ است که می‌تواند به توسعه اقتصاد دیجیتال و بهبود سیاست‌گذاری داده‌محور کمک کند.

کلیدواژه‌ها:

داده‌های بزرگ، مالکیت داده، حقوق مالکیت فکری، مسئولیت قانونی

نحوه استناد:

افشاری, سارا و یوسفی, نازنین . (۱۴۰۳). مالکیت داده‌های بزرگ از منظر حقوق مالکیت فکری . حقوق سایبری, ۱(۲), ۱۰۳-۸۴.

* ایمیل نویسنده مسئول: sara.afshari@iauarak.ac.ir

مقدمه

در عصر دیجیتال، داده‌ها به یکی از با ارزش‌ترین دارایی‌های اقتصادی، اجتماعی و فناورانه تبدیل شده‌اند و مجموعه‌ای از فناوری‌ها و ابزارهای نوین امکان جمع‌آوری، پردازش و تحلیل آن‌ها را با سرعت و حجم بی‌سابقه فراهم کرده‌اند. داده‌های بزرگ یا Big Data به معنای مجموعه‌های عظیم اطلاعات هستند که ویژگی‌های حجم بالا، سرعت تولید زیاد و تنوع فرمت‌ها را دارا بوده و پردازش آن‌ها با روش‌های سنتی تقریبا غیرممکن است (Laney, 2001). امابا توجه به رشد روزافزون فناوری‌های ابری، اینترنت اشیا و هوش مصنوعی، داده‌ها نه تنها به صورت محلی بلکه در سطح جهانی تولید و منتقل می‌شوند و این مساله حفاظت حقوقی از آن‌ها را به یک ضرورت حیاتی تبدیل کرده است (Kitchin, 2014). داده‌های بزرگ شامل اطلاعات ساختاریافته، نیمه‌ساختاریافته و غیرساختاریافته هستند و منابع آن‌ها می‌تواند از شبکه‌های اجتماعی، دستگاه‌های هوشمند، سامانه‌های مالی و صنعتی و سنسورهای مختلف باشد. ارزش اقتصادی داده‌ها در صورتی محقق می‌شود که تحلیل و پردازش آن‌ها به صورت اصولی، قانونی و اخلاقی انجام گیرد، زیرا بهره‌برداری غیرمجاز یا سوءاستفاده از داده‌ها می‌تواند خسارت‌های جبران‌ناپذیری برای افراد و سازمان‌ها ایجاد کند (van der Sloot, 2019) و با توجه به اهمیت اقتصادی و اجتماعی داده‌ها، موضوع مالکیت آن‌ها و شناسایی حقوق مالکیت فکری مرتبط با آن‌ها مورد توجه پژوهشگران و قانونگذاران قرار گرفته است. مالکیت داده‌ها به معنای حق کنترل، استفاده، انتشار، انتقال و بهره‌برداری اقتصادی از داده‌ها است و حفاظت قانونی از این دارایی‌ها موجب حفظ امنیت حقوقی و ایجاد انگیزه برای نوآوری و توسعه فناوری می‌شود (Kuner, 2017). در محیط‌های دیجیتال و فناوری‌های داده‌محور، داده‌ها به سرعت قابل تکثیر هستند و تعیین مالک واقعی و حقوق استفاده‌کنندگان آن‌ها به یک چالش اساسی تبدیل شده است. مالکیت داده‌ها ممکن است به صورت مالکیت طبیعی، یعنی فرد یا سازمانی که داده را تولید یا جمع‌آوری می‌کند، مالک آن محسوب شود یا به صورت مالکیت قراردادی، که حقوق مالکیت بر اساس قراردادهای بین تولیدکنندگان داده، ارائه‌دهندگان خدمات و کاربران تعیین می‌شود، باشد. همچنین، مالکیت حقوقی یا فناورانه، که شامل استفاده از ابزارهای حقوق مالکیت فکری مانند حق مؤلف، پتنت و اسرار تجاری و فناوری‌های کنترل دسترسی است، یکی دیگر از ابعاد مالکیت داده‌ها محسوب می‌شود (Tene & Polonetsky, 2013).

ابزارهای حقوق مالکیت فکری، از جمله حق مؤلف، پتنت و اسرار تجاری، نقش کلیدی در حفاظت از داده‌های بزرگ دارند. حق مؤلف به مالک داده اجازه می‌دهد تا تکثیر، انتشار و نمایش داده‌ها را کنترل کند و به ویژه برای پایگاه‌های داده و نرم‌افزارهای پردازش داده‌ها قابل اعمال است. با این حال، حق مؤلف محدود به محتوای داده‌ها است و داده‌های خام و غیرساختاریافته معمولا از حمایت مستقیم برخوردار نیستند مگر آنکه در قالب یک پایگاه داده یا نرم‌افزار قابل محافظت باشند (Bainbridge, 2017). پتنت‌ها نیز به عنوان ابزار حمایت از اختراعات و فناوری‌های مرتبط با پردازش و تحلیل داده‌ها مورد استفاده قرار می‌گیرند و علاوه بر ایجاد حفاظت قانونی، موجب تشویق نوآوری و سرمایه‌گذاری در فناوری‌های داده‌ای می‌شوند (Hall & Harhoff, 2012). اسرار تجاری نیز امکان حفاظت از الگوریتم‌ها، روش‌های پردازش و داده‌های حساس را فراهم می‌کند و مزیت رقابتی شرکت‌ها را حفظ می‌کند، به شرطی که اقدامات لازم برای محرمانه نگه داشتن این اطلاعات اتخاذ شده باشد. چالش اصلی در اسرار تجاری، پیگیری نقض حقوق توسط اشخاص ثالث و اثبات مساعدت آن‌ها در نقض مالکیت است، که اهمیت شناسایی مسئولیت غیرمستقیم را نشان می‌دهد (نجفی،۱۳۹۸، ص ۴۶).

چالش‌های مالکیت داده‌های بزرگ تنها به ابزارهای حقوقی محدود نمی‌شود، بلکه مسائل پیچیده‌ای مانند مالکیت مشترک، انتقال داده‌ها به محیط ابری، استفاده غیرمجاز و حفظ امنیت و محرمانگی را نیز شامل می‌شود. (فیاضی،۱۴۰۱، ص ۴۶) در بسیاری از پروژه‌های داده‌محور، داده‌ها از منابع متعدد جمع‌آوری می‌شوند و تولیدکنندگان داده متعدد هستند که این وضعیت منجر به مالکیت مشترک می‌شود و سوالات مهمی درباره حقوق استفاده، بهره‌برداری اقتصادی و مسئولیت حقوقی در صورت نقض ایجاد می‌کند. مطالعات نشان می‌دهند که قراردادهای شفاف و حقوق دسترسی مشخص می‌تواند مالکیت مشترک داده‌ها را مدیریت کند و از بروز اختلافات حقوقی جلوگیری نماید (Tene & Polonetsky, 2013). علاوه بر این، محیط‌های ابری و سامانه‌های توزیع‌شده، با فراهم کردن امکان ذخیره و پردازش داده‌ها در مراکز داده مختلف و گاهی در کشورهای مختلف، شناسایی مالک واقعی داده‌ها و کنترل استفاده قانونی از آن‌ها را دشوار می‌سازد. قوانین بین‌المللی و رویه‌های قضایی مانند مقررات GDPR اتحادیه اروپا تلاش کرده‌اند تا با محدود کردن انتقال داده‌های شخصی و تعیین مجازات‌های سنگین برای سوءاستفاده، چارچوبی قانونی برای حفاظت از داده‌ها فراهم کنند (Kuner, 2017).

همچنین مسئولیت قانونی ناشی از استفاده غیرمجاز داده‌ها به دو دسته مستقیم و غیرمستقیم تقسیم می‌شود. مسئولیت مستقیم شامل اقداماتی است که توسط مالک یا کاربر اصلی داده‌ها صورت می‌گیرد، مانند تکثیر غیرمجاز، انتشار یا بهره‌برداری اقتصادی بدون مجوز. مسئولیت غیرمستقیم، به فعالیت‌هایی اشاره دارد که نقض حقوق مالکیت داده‌ها را تسهیل می‌کند، مانند ارائه پلتفرم‌های ابری بدون کنترل کافی یا ارائه فناوری‌هایی که امکان سوءاستفاده از داده‌ها را فراهم می‌کنند (Goldman, 2020). شناسایی و تعیین مسئولیت غیرمستقیم در نظام‌های حقوقی پیشرفته، ابزاری مهم برای حفاظت از داده‌های بزرگ محسوب می‌شود و موجب جلوگیری از سوءاستفاده و حمایت از مالکیت داده‌ها می‌گردد.اما با توجه به مستندات در ایران، قوانین مرتبط با داده‌های بزرگ و مالکیت آن‌ها هنوز به طور کامل تدوین نشده است، هرچند قوانین تجارت الکترونیک، حمایت از داده‌های شخصی و حق مؤلف بخشی از حمایت قانونی را فراهم می‌کنند. با این حال، مسئولیت غیرمستقیم و چارچوب جامع مالکیت داده‌ها به شکل صریح وجود ندارد و بهره‌گیری از تجربیات بین‌المللی و تطبیق آن با مبانی حقوقی موجود می‌تواند خلأهای قانونی را تا حد زیادی کاهش دهد (مولایی،۱۳۹۸، ص ۳۴). استفاده از قراردادهای دیجیتال، تعیین حقوق دسترسی و بهره‌برداری و اعمال استانداردهای امنیتی می‌تواند به ایجاد چارچوبی قانونی و عملیاتی برای حفاظت از داده‌های بزرگ کمک کند. می توان گفت اهمیت مالکیت داده‌های بزرگ فراتر از مباحث حقوقی است و تأثیر مستقیمی بر نوآوری، رقابت اقتصادی و توسعه فناوری دارد. حفاظت قانونی از داده‌ها، شفافیت در حقوق مالکیت و تعیین مسئولیت‌ها، علاوه بر ایجاد امنیت حقوقی، موجب افزایش اعتماد کاربران و سرمایه‌گذاران به محیط‌های داده‌محور می‌شود. بهره‌گیری از ابزارهای حقوق مالکیت فکری، ترکیب آن با مسئولیت مستقیم و غیرمستقیم و اعمال استانداردهای فناوری و مدیریتی، چارچوبی جامع برای حمایت از داده‌های بزرگ فراهم می‌کند و می‌تواند به رشد پایدار فناوری‌های داده‌محور و توسعه اقتصاد دیجیتال کمک نماید. بنابراین، تحلیل مالکیت داده‌های بزرگ از منظر حقوق مالکیت فکری، نه تنها یک ضرورت علمی و پژوهشی، بلکه یک الزام عملی برای ایجاد امنیت حقوقی، اقتصادی و فناورانه در عصر دیجیتال محسوب می‌شود (Kitchin, 2014; van der Sloot, 2019).

تعریف داده‌های بزرگ

داده‌های بزرگ به مجموعه‌های عظیم و متنوع داده گفته می‌شود که ویژگی‌های متمایز آن‌ها پردازش و تحلیل سنتی را غیرممکن می‌سازد و نیازمند فناوری‌ها و روش‌های نوین برای ذخیره‌سازی، مدیریت و تحلیل هستند. این داده‌ها اغلب شامل داده‌های ساختاریافته، نیمه‌ساختاریافته و غیرساختاریافته می‌شوند و از منابع مختلفی مانند شبکه‌های اجتماعی، دستگاه‌های هوشمند، سامانه‌های مالی و صنعتی، سنسورها و دستگاه‌های اینترنت اشیا جمع‌آوری می‌شوند (Laney, 2001). سه ویژگی اصلی داده‌های بزرگ که به اصطلاح «سه V» نامیده می‌شوند شامل حجم بالا (Volume)، سرعت تولید زیاد (Velocity) و تنوع داده‌ها (Variety) است. حجم داده‌ها به سرعت رشد می‌کند و هر روز میلیاردها گیگابایت داده تولید می‌شود، به گونه‌ای که ذخیره و پردازش آن‌ها با روش‌های سنتی تقریبا غیرممکن است. سرعت تولید داده‌ها نیز به دلیل تراکنش‌های آنلاین، تولید محتوای دیجیتال و فعالیت‌های دستگاه‌های متصل به شبکه، بسیار بالاست و نیازمند پردازش در زمان واقعی یا نزدیک به زمان واقعی می‌باشد. تنوع داده‌ها نیز از ویژگی‌های مهم Big Data است، زیرا داده‌ها می‌توانند به صورت متن، تصویر، ویدئو، صدا، داده‌های سنسوری یا داده‌های تراکنشی و ساختاریافته باشند و این تنوع تحلیل آن‌ها را پیچیده‌تر می‌کند (Kitchin, 2014).

ارزش داده‌های بزرگ تنها زمانی محقق می‌شود که تحلیل و پردازش آن‌ها به صورت اصولی و قانونی انجام شود و توانایی استخراج اطلاعات معنادار از این مجموعه‌های عظیم فراهم گردد. داده‌ها به خودی خود ارزشمند نیستند، بلکه ارزش آن‌ها در استخراج الگوها، روندها و اطلاعات قابل استفاده برای تصمیم‌گیری‌های اقتصادی، مدیریتی و فناورانه نهفته است. به همین دلیل، فناوری‌هایی مانند هوش مصنوعی، یادگیری ماشین، داده‌کاوی و پردازش موازی به کار گرفته می‌شوند تا بتوان از این حجم عظیم داده‌ها بهره‌برداری بهینه کرد و نتایج عملی و کاربردی استخراج نمود (Laney, 2001; Kitchin, 2014).یکی دیگر از ویژگی‌های داده‌های بزرگ، قابلیت اتصال و ادغام داده‌ها از منابع مختلف است. این داده‌ها می‌توانند از چندین سیستم و سازمان گردآوری شوند و با یکدیگر ترکیب شوند تا تحلیل‌های جامع‌تر و دقیق‌تری ارائه دهند. به عنوان مثال، داده‌های مربوط به سلامت بیماران می‌تواند از بیمارستان‌ها، آزمایشگاه‌ها، دستگاه‌های پوشیدنی و سامانه‌های بهداشتی جمع‌آوری شود و تحلیل آن‌ها می‌تواند به بهبود درمان و پیش‌بینی بیماری‌ها کمک کند. این ویژگی، همزمان با ایجاد فرصت‌های اقتصادی و اجتماعی، چالش‌های جدی در زمینه مالکیت داده‌ها، امنیت، محرمانگی و حفاظت قانونی آن‌ها ایجاد می‌کند (van der Sloot, 2019).

علاوه بر این، داده‌های بزرگ در بسیاری از صنایع نقش کلیدی دارند و می‌توانند موجب تصمیم‌گیری هوشمند و بهبود عملکرد سازمان‌ها شوند. صنایع مالی، سلامت، تولید، حمل و نقل و بازاریابی از جمله حوزه‌هایی هستند که داده‌های بزرگ در آن‌ها کاربرد گسترده دارد. در صنعت مالی، تحلیل تراکنش‌های مالی و رفتار مشتریان می‌تواند ریسک‌های اعتباری را کاهش دهد و فرصت‌های سرمایه‌گذاری را شناسایی کند. در حوزه سلامت، تحلیل داده‌های بیماران و اطلاعات پزشکی می‌تواند به پیشگیری از بیماری‌ها، بهبود درمان و کاهش هزینه‌ها کمک کند. همچنین، در صنعت تولید و لجستیک، تحلیل داده‌های حسگرها و فرآیندهای تولید می‌تواند بهره‌وری را افزایش داده و کیفیت محصولات را بهبود بخشد (Kitchin, 2014). اما با وجود مزایای گسترده داده‌های بزرگ، چالش‌های متعددی نیز در این حوزه وجود دارد. یکی از مهم‌ترین چالش‌ها، شناسایی مالکیت داده‌ها و حقوق قانونی مرتبط با آن‌ها است. داده‌ها به راحتی قابل تکثیر و اشتراک‌گذاری هستند و ممکن است چندین نهاد در تولید یا پردازش آن‌ها مشارکت داشته باشند. این

مساله تعیین مالک اصلی، حقوق استفاده‌کنندگان و مسئولیت‌های قانونی ناشی از سوءاستفاده را پیچیده می‌کند (Kuner, 2017). علاوه بر این، حفظ امنیت و محرمانگی داده‌ها از اهمیت بالایی برخوردار است، زیرا داده‌های بزرگ اغلب شامل اطلاعات حساس و شخصی هستند و هرگونه نقض امنیت می‌تواند پیامدهای جدی حقوقی، اقتصادی و اجتماعی داشته باشد.

یکی دیگر از ویژگی‌های داده‌های بزرگ، توانایی پردازش در زمان واقعی یا نزدیک به زمان واقعی است که امکان واکنش سریع به رویدادها و پیش‌بینی روندها را فراهم می‌کند. این ویژگی به خصوص در حوزه‌هایی مانند معاملات مالی، مدیریت ترافیک، امنیت سایبری و خدمات آنلاین اهمیت دارد. پردازش داده‌ها در حجم و سرعت بالا نیازمند فناوری‌های پیشرفته ذخیره‌سازی، محاسبات توزیع‌شده، الگوریتم‌های بهینه‌سازی و مدیریت کارآمد منابع است تا بتوان از حجم عظیم داده‌ها به صورت مؤثر بهره‌برداری کرد (van der Sloot, 2019). همچنین داده‌های بزرگ به دلیل حجم زیاد، سرعت تولید بالا و تنوع فرمت‌ها، پردازش آن‌ها با روش‌های سنتی غیرممکن است و تحلیل و پردازش اصولی و قانونی آن‌ها نیازمند استفاده از فناوری‌های نوین و چارچوب‌های حقوقی و مدیریتی است. داده‌های بزرگ نه تنها فرصت‌های اقتصادی و اجتماعی قابل توجهی فراهم می‌کنند، بلکه چالش‌های حقوقی و امنیتی مهمی نیز ایجاد می‌کنند. ارزش واقعی این داده‌ها زمانی آشکار می‌شود که تحلیل‌های دقیق، بهره‌برداری قانونی و حفاظت حقوقی از آن‌ها انجام شود و این مساله اهمیت ویژه‌ای برای قانونگذاران، سازمان‌ها و پژوهشگران دارد (Laney, 2001; Kitchin, 2014; van der Sloot, 2019; Kuner, 2017).

اهمیت مالکیت داده‌ها

مالکیت داده‌ها در عصر دیجیتال اهمیت بسزایی یافته است، زیرا داده‌ها به عنوان دارایی‌های استراتژیک نه تنها ارزش اقتصادی دارند، بلکه نقش کلیدی در تصمیم‌گیری‌های مدیریتی، نوآوری فناوری و توسعه اجتماعی ایفا می‌کنند (تراب نژاد،۱۳۹۹ ص ۴۵). داده‌ها در سطح فردی، سازمانی و ملی تولید می‌شوند و بهره‌برداری مؤثر از آن‌ها مستلزم شناسایی مالک، تعیین حقوق استفاده و اعمال محدودیت‌های قانونی است. مالکیت داده‌ها به مالک اجازه می‌دهد تا کنترل بر نحوه جمع‌آوری، ذخیره، پردازش و انتشار داده‌ها را حفظ کند و همچنین از بهره‌برداری اقتصادی و تجاری غیرمجاز جلوگیری نماید (Kuner, 2017). عدم تعیین مالکیت داده‌ها یا فقدان حفاظت قانونی می‌تواند منجر به تضاد منافع، سوءاستفاده از اطلاعات و کاهش انگیزه برای تولید و اشتراک‌گذاری داده‌ها شود. از این رو، مالکیت داده‌ها یک ابزار مهم برای تضمین امنیت حقوقی، کاهش ریسک‌های اقتصادی و حمایت از نوآوری محسوب می‌شود (van der Sloot, 2019).

در سطح سازمانی، مالکیت داده‌ها به مدیران و شرکت‌ها امکان می‌دهد تا از داده‌ها برای بهبود عملکرد، توسعه محصولات و خدمات و شناسایی فرصت‌های بازار استفاده کنند. سازمان‌هایی که مالکیت داده‌های خود را به صورت قانونی تثبیت کرده‌اند، قادر به ایجاد مزیت رقابتی پایدار و بهره‌برداری از دارایی‌های اطلاعاتی خود هستند. این مالکیت شامل حق تصمیم‌گیری در مورد دسترسی دیگران به داده‌ها، انتقال آن‌ها به محیط‌های ابری و تعیین نحوه استفاده تجاری است. در بسیاری از صنایع، داده‌ها به عنوان سرمایه‌های استراتژیک شناخته می‌شوند و حفاظت از مالکیت آن‌ها موجب افزایش ارزش اقتصادی و کاهش خطرات ناشی از دسترسی غیرمجاز می‌شود (Tene & Polonetsky, 2013).

از منظر حقوق مالکیت فکری، مالکیت داده‌ها می‌تواند با ابزارهایی مانند حق مؤلف، پتنت و اسرار تجاری حمایت شود. حق مؤلف امکان کنترل بر پایگاه‌های داده و نرم‌افزارهای مرتبط با پردازش داده‌ها را فراهم می‌کند و پتنت‌ها می‌توانند نوآوری‌های فناورانه و الگوریتم‌های پردازش داده را محافظت کنند. اسرار تجاری نیز از اطلاعات محرمانه و حساس حفاظت می‌کند و مزیت رقابتی را برای مالک داده ایجاد می‌نماید. این ابزارها، ضمن ایجاد حفاظت قانونی، انگیزه‌های اقتصادی برای سرمایه‌گذاری در فناوری‌های داده‌محور را نیز افزایش می‌دهند و به رشد و توسعه اقتصاد دیجیتال کمک می‌کنند (Bainbridge, 2017; Hall & Harhoff, 2012).مالکیت داده‌ها علاوه بر بعد اقتصادی، اهمیت اجتماعی و امنیتی نیز دارد. داده‌های شخصی و اطلاعات حساس افراد، مانند اطلاعات پزشکی، مالی یا رفتارهای آنلاین، در صورت عدم حفاظت قانونی می‌تواند مورد سوءاستفاده قرار گیرد و پیامدهای حقوقی و اجتماعی قابل توجهی داشته باشد. تعیین مالکیت و کنترل قانونی بر داده‌ها به افراد و سازمان‌ها اطمینان می‌دهد که اطلاعاتشان به صورت امن و اخلاقی مورد استفاده قرار می‌گیرد و امکان پیگیری قانونی در صورت نقض حقوق فراهم می‌شود. در این زمینه، نظام‌های حقوقی پیشرفته مسئولیت مستقیم و غیرمستقیم ناشی از استفاده غیرمجاز داده‌ها را شناسایی کرده‌اند و این اقدام به عنوان یک ابزار مهم برای حفاظت از مالکیت داده‌ها عمل می‌کند (طالب زاده،۱۳۹۷، ص ۱۴).

چالش‌های مالکیت داده‌ها شامل مالکیت مشترک، محیط‌های پردازش ابری و امکان تکثیر سریع داده‌ها است. در پروژه‌هایی که چندین سازمان یا فرد در تولید و پردازش داده‌ها مشارکت دارند، تعیین مالک اصلی و حقوق استفاده‌کنندگان از اهمیت ویژه‌ای برخوردار است. همچنین، با انتقال داده‌ها به محیط‌های ابری و استفاده از سرویس‌های توزیع‌شده، کنترل مستقیم بر داده‌ها کاهش می‌یابد و نیاز به چارچوب‌های قانونی و قراردادی مشخص احساس می‌شود. قراردادهای دیجیتال، تعیین حقوق دسترسی و بهره‌برداری و اعمال محدودیت‌های امنیتی می‌توانند به شفاف‌سازی مالکیت داده‌ها و کاهش مخاطرات ناشی از سوءاستفاده کمک کنند (Kuner, 2017; van der Sloot, 2019). علاوه بر این، مالکیت داده‌ها نقش مهمی در نوآوری و توسعه فناوری دارد. سازمان‌ها و افراد تنها زمانی تمایل به تولید و اشتراک‌گذاری داده‌ها دارند که مالکیت آن‌ها محفوظ بماند و از حقوق قانونی برخوردار باشند. حفاظت قانونی از داده‌ها، ایجاد انگیزه برای سرمایه‌گذاری در فناوری‌های نوین و توسعه محصولات مبتنی بر داده‌ها را تضمین می‌کند. در نتیجه، مالکیت داده‌ها نه تنها ابزاری برای مدیریت و بهره‌برداری اقتصادی است، بلکه نقش مهمی در تضمین رشد و توسعه پایدار فناوری‌های دیجیتال و اقتصاد اطلاعات محور ایفا می‌کند (Kitchin, 2014). می توان چنین بیان نمود که، مالکیت داده‌ها ترکیبی از حق قانونی، کنترل مدیریتی و حفاظت فناورانه است که به افراد و سازمان‌ها امکان می‌دهد از داده‌ها به صورت بهینه و ایمن استفاده کنند. تعیین مالکیت و حقوق استفاده، اعمال چارچوب‌های قانونی و قراردادی و استفاده از ابزارهای حقوق مالکیت فکری موجب می‌شود داده‌ها به عنوان یک دارایی استراتژیک مدیریت شوند و ارزش واقعی آن‌ها محقق گردد. اهمیت مالکیت داده‌ها در عصر دیجیتال نه تنها از منظر اقتصادی و فناورانه، بلکه از لحاظ اجتماعی، امنیتی و حقوقی نیز برجسته است و شناسایی و تثبیت آن یک ضرورت حیاتی برای سازمان‌ها، افراد و نظام‌های حقوقی محسوب می‌شود (Laney, 2001; Kitchin, 2014; Tene & Polonetsky, 2013; Goldman, 2020).

ابزارهای حقوق مالکیت فکری

ابزارهای حقوق مالکیت فکری نقش بسیار مهمی در حفاظت از داده‌ها و اطلاعات دیجیتال ایفا می‌کنند و به مالکان داده‌ها اجازه می‌دهند تا کنترل، بهره‌برداری و انتقال اطلاعات خود را به شکلی قانونی و مستند مدیریت کنند. حق مؤلف یا Copyright یکی از اصلی‌ترین ابزارهای حقوق مالکیت فکری است که مالکیت قانونی بر پایگاه‌های داده، نرم‌افزارها و محتوای دیجیتال را تضمین می‌کند. این حق به مالک داده اجازه می‌دهد تا تکثیر، توزیع، نمایش و تغییر داده‌ها را کنترل کند و هرگونه استفاده غیرمجاز از آن‌ها را منع نماید. حفاظت قانونی از پایگاه‌های داده و نرم‌افزارها اهمیت ویژه‌ای دارد، زیرا این داده‌ها اغلب حاصل سرمایه‌گذاری‌های قابل توجه در زمینه جمع‌آوری، پردازش و سازمان‌دهی اطلاعات هستند و بدون حمایت قانونی، امکان بهره‌برداری غیرمجاز توسط سایرین بسیار بالا می‌رود. علاوه بر این، حق مؤلف با ایجاد انگیزه اقتصادی برای تولیدکنندگان محتوا و داده‌های دیجیتال، موجب تشویق نوآوری و سرمایه‌گذاری در فناوری‌های داده‌محور می‌شود و نقش کلیدی در توسعه فناوری‌های دیجیتال دارد (Bainbridge, 2017).

پتنت یا Patent به عنوان ابزار دیگری از حقوق مالکیت فکری، حفاظت از اختراعات و فناوری‌های پردازش داده را فراهم می‌کند. پتنت به مخترع اجازه می‌دهد که از اختراعات خود برای مدت مشخصی محافظت کند و دیگران بدون مجوز او نتوانند از این فناوری‌ها بهره‌برداری کنند. در زمینه داده‌های بزرگ، پتنت می‌تواند شامل الگوریتم‌های نوین پردازش داده، روش‌های تحلیل اطلاعات، سیستم‌های ذخیره‌سازی و انتقال داده‌ها و فناوری‌های مرتبط با هوش مصنوعی و یادگیری ماشین باشد. این ابزار نه تنها مالکیت قانونی فناوری‌های نوین را تضمین می‌کند، بلکه انگیزه‌ای برای پژوهش و نوآوری در زمینه فناوری‌های داده‌محور ایجاد می‌کند. با توجه به اینکه داده‌های بزرگ نیازمند فناوری‌های پیشرفته برای پردازش، ذخیره و تحلیل هستند، حفاظت از این فناوری‌ها از طریق پتنت موجب می‌شود که سرمایه‌گذاری‌های سازمان‌ها و افراد در حوزه توسعه نرم‌افزار و الگوریتم‌های تحلیل داده محافظت شود و امکان رقابت سالم در بازار فناوری فراهم گردد (Hall & Harhoff, 2012).

یکی دیگر از ابزارهای حیاتی حقوق مالکیت فکری، اسرار تجاری یا Trade Secrets است که حفاظت از روش‌ها، فرمول‌ها، الگوریتم‌ها و رویه‌های پردازش و تحلیل داده‌ها را ممکن می‌سازد. اسرار تجاری به مالک داده امکان می‌دهد اطلاعات حساس و محرمانه خود را بدون افشای عمومی نگهداری کند و از بهره‌برداری غیرمجاز توسط رقبا جلوگیری نماید (مرعشی،۱۳۹۹، ص ۲۲). این ابزار به ویژه در محیط‌های رقابتی و فناوری‌محور اهمیت دارد، زیرا بسیاری از مزیت‌های اقتصادی و فناورانه سازمان‌ها ناشی از توانایی آن‌ها در نگهداری اطلاعات محرمانه و استفاده بهینه از آن‌هاست. حفاظت از اسرار تجاری نیازمند اقداماتی مانند محدود کردن دسترسی، رمزگذاری، نظارت داخلی و استفاده از قراردادهای محرمانگی است تا اطلاعات به شکل قانونی محفوظ بماند و در صورت نقض حقوق مالک، امکان پیگیری قانونی فراهم شود (Bainbridge, 2017).

ترکیب این سه ابزار یعنی حق مؤلف، پتنت و اسرار تجاری، چارچوبی کامل برای حفاظت از داده‌ها و فناوری‌های مرتبط با داده‌های بزرگ ایجاد می‌کند. هر یک از این ابزارها نقش مکمل دیگری را دارد و با همدیگر امکان مدیریت جامع حقوق مالکیت فکری را فراهم می‌سازند. برای مثال، داده‌های خام و نرم‌افزارهای پردازش آن‌ها ممکن است تحت حمایت حق مؤلف باشند، در حالی که الگوریتم‌های نوین تحلیل داده از طریق پتنت محافظت می‌شوند و روش‌های محرمانه پردازش داده‌ها تحت پوشش اسرار تجاری قرار می‌گیرند. این ترکیب موجب می‌شود که مالکیت داده‌ها و

فناوری‌های مرتبط به شکل قانونی و مستحکم تثبیت شود و امکان سوءاستفاده، تکثیر غیرمجاز یا دسترسی غیرمجاز به حداقل برسد.

علاوه بر بعد قانونی، استفاده از ابزارهای حقوق مالکیت فکری تأثیر مهمی بر توسعه اقتصادی و نوآوری دارد. سازمان‌ها و شرکت‌هایی که مالکیت قانونی داده‌ها و فناوری‌های مرتبط را تثبیت کرده‌اند، قادر به ایجاد محصولات و خدمات جدید، بهبود فرآیندهای عملیاتی و بهره‌برداری اقتصادی از داده‌ها هستند. حفاظت از مالکیت فکری موجب افزایش اعتماد سرمایه‌گذاران، ایجاد امنیت حقوقی و کاهش ریسک‌های ناشی از رقابت غیرقانونی می‌شود و در نتیجه محیطی پایدار برای توسعه فناوری‌های داده‌محور فراهم می‌آورد. در واقع، این ابزارها نه تنها از داده‌ها و فناوری‌ها حفاظت می‌کنند، بلکه محرک نوآوری، توسعه اقتصادی و رقابت سالم در بازارهای فناوری محسوب می‌شوند (Bainbridge, 2017; Hall & Harhoff, 2012).

با توجه به اهمیت بالای داده‌ها در اقتصاد دیجیتال و نقش آن‌ها در تصمیم‌گیری‌های مدیریتی، اقتصادی و فناورانه، ابزارهای حقوق مالکیت فکری امکان مدیریت و بهره‌برداری قانونی از این دارایی‌ها را فراهم می‌کنند. مالکیت داده‌ها و فناوری‌های مرتبط به وسیله حق مؤلف، پتنت و اسرار تجاری تثبیت می‌شود و تضمین می‌کند که بهره‌برداری از داده‌ها به نفع مالک اصلی و به صورت قانونی انجام گیرد. در نتیجه، این ابزارها علاوه بر حفاظت از حقوق قانونی مالک، موجب ایجاد امنیت اقتصادی و انگیزه برای تولید، پردازش و تحلیل داده‌ها می‌شوند و زمینه رشد پایدار فناوری‌های داده‌محور و توسعه اقتصاد دیجیتال را فراهم می‌آورند. اهمیت ابزارهای حقوق مالکیت فکری در حفاظت از داده‌ها، الگوریتم‌ها و فناوری‌های پردازش داده‌ها نشان می‌دهد که بدون وجود چارچوب‌های قانونی مناسب، ارزش واقعی داده‌های بزرگ و فناوری‌های مرتبط با آن‌ها به طور کامل محقق نخواهد شد و بهره‌برداری مؤثر و پایدار از داده‌ها با چالش‌های جدی مواجه خواهد شد (Bainbridge, 2017; Kuner, 2017).

چالش‌های حقوقی

چالش‌های حقوقی مرتبط با داده‌های بزرگ یکی از مهم‌ترین موانع بهره‌برداری مؤثر و قانونی از داده‌ها در عصر دیجیتال محسوب می‌شوند و به گونه‌ای عمل می‌کنند که بدون مدیریت صحیح می‌توانند موجب تضاد منافع، سوءاستفاده از اطلاعات و کاهش ارزش اقتصادی داده‌ها شوند. یکی از اساسی‌ترین این چالش‌ها تعیین مالکیت داده‌ها و انتقال آن‌ها است. داده‌ها معمولاً از منابع متعدد تولید می‌شوند و ممکن است چندین فرد یا سازمان در جمع‌آوری، پردازش و تحلیل آن‌ها مشارکت داشته باشند، بنابراین شناسایی مالک اصلی و تفکیک حقوق استفاده‌کنندگان به یک موضوع پیچیده تبدیل می‌شود. تعیین مالکیت داده‌ها اهمیت ویژه‌ای دارد زیرا حقوق مالک بر استفاده، بهره‌برداری اقتصادی، انتشار و انتقال داده‌ها را تثبیت می‌کند و اطمینان می‌دهد که بهره‌برداری از داده‌ها به نفع مالک اصلی انجام می‌شود. انتقال داده‌ها به محیط‌های ابری، سیستم‌های توزیع‌شده و پایگاه‌های داده بین‌المللی پیچیدگی‌های بیشتری ایجاد می‌کند و نیازمند چارچوب‌های قانونی روشن و قراردادهای شفاف است تا حقوق مالک حفظ شود و سوءاستفاده‌ها به حداقل برسد (Kuner, 2017). یکی دیگر از چالش‌های مهم، استفاده غیرمجاز از داده‌ها و مسئولیت قانونی ناشی از آن است. داده‌های بزرگ به دلیل قابلیت تکثیر بالا و امکان دسترسی آسان، در معرض سوءاستفاده‌های غیرمجاز قرار دارند و می‌توانند بدون مجوز مالک یا سازمان مورد استفاده قرار گیرند. این نوع سوءاستفاده‌ها می‌تواند شامل تکثیر، انتشار، تحلیل یا بهره‌برداری تجاری غیرمجاز باشد و پیامدهای حقوقی و اقتصادی گسترده‌ای برای مالک داده ایجاد کند.

مسئولیت قانونی در این زمینه به دو نوع مستقیم و غیرمستقیم تقسیم می‌شود. مسئولیت مستقیم مربوط به اقداماتی است که توسط خود متخلف انجام می‌شود، مانند استفاده غیرمجاز از داده‌ها یا نقض قراردادهای حقوق مالکیت فکری، و مسئولیت غیرمستقیم شامل فعالیت‌هایی است که تسهیل‌کننده نقض حقوق مالکیت داده‌ها توسط دیگران است، مانند فراهم کردن پلتفرم‌های پردازش داده یا ابزارهای تحلیلی بدون کنترل کافی. شناسایی و تعیین مسئولیت قانونی در این حوزه ضروری است تا مالک داده بتواند از حقوق خود دفاع کند و امکان جبران خسارت و پیشگیری از سوءاستفاده‌های آینده فراهم گردد (Goldman, 2020). حفظ محرمانگی و امنیت داده‌ها نیز یکی از چالش‌های اصلی حقوقی مرتبط با داده‌های بزرگ است. داده‌ها اغلب شامل اطلاعات شخصی، مالی، پزشکی یا اطلاعات حساس سازمانی هستند و هرگونه نقض امنیتی می‌تواند پیامدهای جدی قانونی، اقتصادی و اجتماعی داشته باشد. قوانین و مقررات بین‌المللی مانند GDPR اتحادیه اروپا، چارچوب‌هایی را برای حفاظت از داده‌های شخصی و حفظ محرمانگی آن‌ها ارائه می‌کنند و شرکت‌ها و سازمان‌ها را ملزم به اتخاذ اقدامات حفاظتی، رمزگذاری داده‌ها و نظارت مداوم می‌سازند. رعایت این مقررات نه تنها برای حفظ حقوق افراد ضروری است بلکه موجب کاهش ریسک‌های قانونی و افزایش اعتماد کاربران و سرمایه‌گذاران می‌شود. همچنین، حفاظت از محرمانگی داده‌ها و امنیت آن‌ها به ایجاد محیطی پایدار برای نوآوری و بهره‌برداری قانونی از داده‌های بزرگ کمک می‌کند و از وقوع نقض حقوق مالکیت فکری و سوءاستفاده‌های غیرقانونی جلوگیری می‌کند.

این چالش‌ها به ویژه در زمینه داده‌های بزرگ پیچیده‌تر هستند زیرا حجم عظیم داده‌ها، سرعت تولید بالا و تنوع منابع، امکان کنترل و پایش دقیق داده‌ها را دشوار می‌سازد. تعیین مالکیت و حقوق استفاده، مدیریت دسترسی‌ها، اعمال محدودیت‌های قانونی و قراردادی و اتخاذ فناوری‌های محافظتی از جمله اقداماتی هستند که برای مقابله با چالش‌های حقوقی داده‌ها لازم است. بدون توجه به این مسائل، بهره‌برداری از داده‌های بزرگ با ریسک‌های قانونی و اقتصادی فراوانی همراه خواهد بود و ارزش واقعی داده‌ها محقق نخواهد شد. در نتیجه، شناسایی مالکیت داده‌ها، تعیین مسئولیت قانونی و حفاظت از امنیت و محرمانگی داده‌ها برای بهره‌برداری مؤثر و قانونی از داده‌های بزرگ امری ضروری و اجتناب‌ناپذیر است (Kuner, 2017; Goldman, 2020; van der Sloot, 2019).

مسئولیت قانونی و مساعدت در نقض

مسئولیت قانونی در حوزه داده‌های بزرگ یکی از مهم‌ترین موضوعات حقوقی است که نقش حیاتی در حفاظت از مالکیت داده‌ها و جلوگیری از سوءاستفاده‌های غیرمجاز ایفا می‌کند و در عین حال پیچیدگی‌های خاص خود را دارد. مسئولیت ناشی از استفاده غیرمجاز داده‌ها به دو دسته اصلی تقسیم می‌شود که شامل مسئولیت مستقیم و مسئولیت غیرمستقیم است. مسئولیت مستقیم مربوط به اقداماتی است که توسط خود شخص یا سازمان متخلف صورت می‌گیرد و شامل تکثیر غیرمجاز، انتشار، تحلیل یا بهره‌برداری اقتصادی بدون مجوز مالک داده است. این نوع مسئولیت به وضوح در قوانین حقوق مالکیت فکری و مقررات حفاظت از داده‌ها مشخص شده است و امکان پیگیری قانونی و جبران خسارت را برای مالک فراهم می‌آورد. مسئولیت مستقیم اهمیت ویژه‌ای دارد زیرا نقض‌کننده داده‌ها مستقیماً با اقدام خود موجب تضییع حقوق مالک شده و پیامدهای قانونی و اقتصادی قابل توجهی ایجاد می‌کند (Goldman, 2020).

در مقابل، مسئولیت غیرمستقیم به فعالیت‌هایی اطلاق می‌شود که نقض حقوق مالکیت داده‌ها توسط شخص ثالث را تسهیل یا مساعدت می‌کنند، بدون آنکه خود اقدام مستقیم به نقض داده‌ها انجام دهند (کتابی،۱۴۰۰، ص ۳۱). این نوع

مسئولیت شامل ارائه فناوری‌ها، پلتفرم‌ها یا خدماتی است که امکان سوءاستفاده از داده‌ها را فراهم می‌کنند و مالک اصلی را در معرض خسارت قرار می‌دهند. مسئولیت غیرمستقیم از اهمیت ویژه‌ای برخوردار است زیرا بسیاری از فناوری‌ها و خدمات داده‌محور، از جمله سرویس‌های ابری، نرم‌افزارهای پردازش داده و ابزارهای تحلیلی، می‌توانند به صورت ناخواسته یا عمدی به نقض حقوق مالکیت داده‌ها کمک کنند. در این زمینه، شناسایی ارکان مسئولیت غیرمستقیم و تعیین میزان نقش افراد یا سازمان‌ها در تسهیل نقض حقوق مالک، برای اعمال مجازات قانونی و جبران خسارت ضروری است.

یکی از چالش‌های مرتبط با مسئولیت غیرمستقیم، تعیین حدود مساعدت و تسهیل است، زیرا برخی از فناوری‌ها و خدمات ممکن است کاربردهای قانونی و مشروع نیز داشته باشند. برای مثال، ارائه پلتفرم‌های ابری یا ابزارهای پردازش داده، به خودی خود نقض حقوق مالک محسوب نمی‌شود، اما در صورتی که استفاده‌کنندگان از آن‌ها اقدام به بهره‌برداری غیرمجاز از داده‌ها کنند و ارائه‌دهنده ابزار یا خدمات آگاهی داشته باشد یا اقدامات پیشگیرانه لازم را انجام نداده باشد، مسئولیت غیرمستقیم مطرح می‌شود. در این راستا، نظام‌های حقوقی پیشرفته چارچوب‌هایی برای شناسایی مسئولیت غیرمستقیم و تعیین شرایط لازم برای اعمال آن ارائه کرده‌اند تا هم از مالک داده محافظت شود و هم از ایجاد محدودیت‌های غیرضروری برای توسعه فناوری جلوگیری گردد (رضایی،۱۳۹۹ ص ۵۴).

حفظ امنیت و کنترل دسترسی به داده‌ها نیز ارتباط مستقیمی با مسئولیت قانونی و مساعدت در نقض دارد. ارائه ابزارها یا خدمات بدون مکانیزم‌های امنیتی کافی می‌تواند نقش مؤثری در تسهیل نقض حقوق مالک ایفا کند و مالک داده را در معرض خطرات قانونی و اقتصادی قرار دهد. از این رو، مسئولیت غیرمستقیم شامل الزام به اتخاذ اقدامات حفاظتی، نظارت بر استفاده از داده‌ها و اطمینان از رعایت قوانین و مقررات مرتبط با مالکیت داده‌ها می‌شود. این اقدامات می‌تواند شامل رمزگذاری داده‌ها، تعیین سطوح دسترسی، قراردادهای محرمانگی و پایش فعالیت کاربران باشد تا نقش ارائه‌دهندگان خدمات یا فناوری‌ها در مساعدت به نقض داده‌ها به حداقل برسد و مالکیت داده‌ها به شکل مؤثر حفظ شود. یکی دیگر از ابعاد مسئولیت قانونی و مساعدت در نقض، نقش اخلاقی و حرفه‌ای ارائه‌دهندگان فناوری و خدمات داده‌محور است. در بسیاری از موارد، افراد و سازمان‌هایی که ابزارها و خدمات پردازش داده را ارائه می‌کنند، می‌توانند با اتخاذ استانداردهای اخلاقی و اجرای سیاست‌های امنیتی، خطر نقض داده‌ها توسط شخص ثالث را کاهش دهند. این اقدام نه تنها موجب کاهش مسئولیت قانونی می‌شود بلکه اعتماد کاربران و سرمایه‌گذاران به محیط‌های داده‌محور را افزایش می‌دهد و شرایط توسعه پایدار فناوری‌های مبتنی بر داده را فراهم می‌کند. در واقع، مسئولیت غیرمستقیم نه تنها یک الزام حقوقی بلکه یک ضرورت مدیریتی و اخلاقی برای اطمینان از بهره‌برداری قانونی و امن از داده‌ها محسوب می‌شود (Goldman, 2020).

در مجموع، مسئولیت قانونی و مساعدت در نقض داده‌ها یک چارچوب جامع برای حفاظت از مالکیت داده‌ها فراهم می‌کند که شامل مسئولیت مستقیم متخلف و مسئولیت غیرمستقیم ارائه‌دهندگان فناوری و خدمات است. شناسایی، تعیین حدود و اعمال این مسئولیت‌ها، امکان مدیریت مؤثر حقوق مالکیت داده‌ها، کاهش سوءاستفاده‌های غیرمجاز و تضمین امنیت اقتصادی و فناورانه داده‌ها را فراهم می‌آورد. توجه به این جنبه‌ها برای توسعه پایدار فناوری‌های داده‌محور، افزایش اعتماد کاربران و سرمایه‌گذاران و ایجاد محیطی قانونی و امن برای بهره‌برداری از داده‌های بزرگ ضروری است و اهمیت آن در عصر دیجیتال هر روز بیشتر می‌شود (Goldman, 2020).

مطالعات موردی و تطبیقی

مالکیت داده‌های بزرگ به معنای حق کنترل، بهره‌برداری، انتشار و انتقال داده‌ها است و شناسایی مالک واقعی داده‌ها در محیط‌های دیجیتال پیچیده اهمیت بسیار بالایی دارد، زیرا داده‌ها معمولاً از منابع متعدد تولید می‌شوند و چندین فرد یا سازمان در جمع‌آوری، پردازش و تحلیل آن‌ها مشارکت دارند. تعیین مالکیت داده‌ها نقش مهمی در تضمین حقوق مالک، مدیریت بهره‌برداری اقتصادی و پیشگیری از سوءاستفاده‌های غیرمجاز ایفا می‌کند و امکان انتقال قانونی داده‌ها به محیط‌های ابری یا بین سازمانی را فراهم می‌آورد (Kuner, 2017). یکی از چالش‌های اساسی در مالکیت داده‌ها، موضوع مالکیت مشترک و هم‌افزایی داده‌ها است، زیرا بسیاری از پروژه‌های داده‌محور شامل داده‌هایی هستند که توسط چندین نهاد تولید شده‌اند و ترکیب این داده‌ها ارزش افزوده ایجاد می‌کند. در این شرایط، تعیین حقوق استفاده‌کنندگان و تقسیم منافع اقتصادی و مسئولیت‌های قانونی میان ذی‌نفعان امری پیچیده است که نیازمند چارچوب‌های قراردادی شفاف و مقررات دقیق است تا از بروز اختلافات حقوقی جلوگیری شود (Tene & Polonetsky, 2013). چالش دیگر انتقال و پردازش داده‌ها در محیط‌های ابری و سامانه‌های توزیع‌شده است. انتقال داده‌ها به مراکز داده مختلف و پردازش آن‌ها در فضای ابری موجب کاهش کنترل مستقیم مالک بر داده‌ها می‌شود و نیازمند مقررات حفاظتی، قراردادهای دقیق و فناوری‌های امنیتی پیشرفته است. استفاده غیرمجاز و نقض مالکیت داده‌ها نیز یکی دیگر از مسائل مهم است و می‌تواند شامل تکثیر غیرمجاز، انتشار، تحلیل یا بهره‌برداری تجاری بدون اجازه مالک باشد. این موضوع علاوه بر ایجاد خسارت اقتصادی، پیامدهای حقوقی قابل توجهی برای مالک داده دارد و نقش چارچوب‌های قانونی و مسئولیت‌های مستقیم و غیرمستقیم را پررنگ می‌کند. حفظ امنیت و محرمانگی داده‌ها نیز به دلیل حساسیت بالای اطلاعات شخصی، مالی و پزشکی اهمیت ویژه‌ای دارد و نقض آن می‌تواند پیامدهای جدی قانونی و اجتماعی ایجاد کند، به همین دلیل رعایت استانداردهای بین‌المللی و فناوری‌های محافظتی از الزامات حیاتی بهره‌برداری از داده‌های بزرگ است (تابش، ۱۳۹۰، ص ۲۴).

مطالعات موردی نشان می‌دهند که عدم حفاظت مناسب از داده‌ها می‌تواند پیامدهای گسترده‌ای داشته باشد. در صنعت مالی، پرونده Equifax Data Breach نمونه‌ای از استفاده غیرمجاز و افشای داده‌های حساس مشتریان است که موجب جریمه‌های قانونی و خسارت‌های مالی شد. در حوزه سلامت، مواردی وجود دارد که داده‌های بیماران بدون اجازه و برای مقاصد تجاری یا پژوهشی مورد استفاده قرار گرفته‌اند و این اقدام علاوه بر نقض حقوق بیماران، موجب کاهش اعتماد عمومی به سیستم‌های بهداشتی شد. همچنین در شبکه‌های اجتماعی، داده‌های کاربران شرکت‌هایی مانند Facebook و Google بارها بدون رضایت کافی کاربران جمع‌آوری و تحلیل شده است و این امر نگرانی‌های جدی درباره مالکیت، محرمانگی و بهره‌برداری اقتصادی داده‌ها ایجاد کرده است. این نمونه‌ها اهمیت تعیین مالکیت داده‌ها، حفاظت قانونی و کنترل استفاده را روشن می‌سازد و ضرورت تدوین مقررات جامع و چارچوب‌های مسئولیت قانونی را برجسته می‌کند.

تحلیل تطبیقی ایران و سایر کشورها

تحلیل تطبیقی ایران و سایر کشورها نشان می‌دهد که اقتباس اصول بین‌المللی و تدوین مقررات مشخص می‌تواند خلأ قانونی موجود در ایران را کاهش دهد و زمینه بهره‌برداری قانونی و ایمن از داده‌های بزرگ را فراهم آورد. در بسیاری از نظام‌های حقوقی پیشرفته، مالکیت داده‌ها، مسئولیت استفاده‌کنندگان، انتقال داده‌ها و حفاظت از محرمانگی داده‌ها به

صراحت تعریف شده و چارچوب‌های قانونی و قراردادی مشخصی برای مدیریت مالکیت مشترک و مسئولیت غیرمستقیم وجود دارد. در ایران، با وجود قوانینی مانند تجارت الکترونیک و حمایت از داده‌های شخصی، هنوز چارچوب جامع و صریحی برای مالکیت داده‌های بزرگ و مسئولیت‌های ناشی از استفاده غیرمجاز و مساعدت در نقض وجود ندارد (حبیبی،۱۳۹۶. ص ۲۴). اتخاذ استانداردهای بین‌المللی، تدوین قوانین مشخص، ایجاد قراردادهای دیجیتال و اعمال فناوری‌های حفاظتی می‌تواند به کاهش ریسک‌های حقوقی و افزایش امنیت اقتصادی و فناورانه داده‌ها کمک کند و زمینه توسعه پایدار فناوری‌های داده‌محور و اقتصاد دیجیتال را فراهم نماید (Kuner, 2017; Tene & Polonetsky, 2013; Goldman, 2020).

در مجموع، مالکیت داده‌های بزرگ و چالش‌های مرتبط با آن یک حوزه پیچیده و چندبعدی است که شامل تعیین مالکیت، مدیریت مالکیت مشترک، انتقال و پردازش ابری، استفاده غیرمجاز، امنیت و محرمانگی داده‌ها می‌شود. شناسایی مالک واقعی، اعمال چارچوب‌های قانونی و قراردادی، تعیین مسئولیت‌های مستقیم و غیرمستقیم و بهره‌گیری از فناوری‌های امنیتی، همگی از عوامل کلیدی برای مدیریت این چالش‌ها و تضمین بهره‌برداری قانونی، اقتصادی و اخلاقی از داده‌های بزرگ هستند و نقش مهمی در توسعه فناوری‌ها و اقتصاد اطلاعات محور ایفا می‌کنند.

حقوق مالکیت فکری و داده‌های بزرگ

حقوق مالکیت فکری در حوزه داده‌های بزرگ نقش بسیار حیاتی دارد و ابزارهایی مانند حق مؤلف، پتنت و اسرار تجاری مالک داده را قادر می‌سازند تا استفاده، بهره‌برداری اقتصادی و انتشار داده‌ها را کنترل کرده و از سوءاستفاده‌های غیرمجاز جلوگیری کنند. حق مؤلف یا Copyright یکی از اصلی‌ترین ابزارهای حقوق مالکیت فکری است که حفاظت از پایگاه‌های داده، نرم‌افزارها و محتواهای دیجیتال را تضمین می‌کند و به مالک این امکان را می‌دهد که تکثیر، توزیع و تغییر داده‌ها را کنترل کند. به عنوان مثال، پرونده SAS Institute v. World Programming Ltd نشان می‌دهد که نرم‌افزارهای تحلیلی و پایگاه‌های داده می‌توانند تحت حمایت حق مؤلف قرار گیرند و هرگونه استفاده غیرمجاز از آن‌ها مشمول مسئولیت قانونی خواهد شد. حفاظت قانونی از داده‌ها و نرم‌افزارها انگیزه‌ای برای سرمایه‌گذاری و توسعه فناوری‌های داده‌محور فراهم می‌کند و به مالک امکان می‌دهد ارزش اقتصادی داده‌ها و نرم‌افزارهای مرتبط با آن‌ها را حفظ نماید (Kuner, 2017; Bainbridge, 2017).

در زمینه داده‌های بزرگ، پتنت می‌تواند شامل الگوریتم‌های پیشرفته پردازش و تحلیل داده، سیستم‌های هوشمند ذخیره‌سازی و مدیریت داده و فناوری‌های مبتنی بر هوش مصنوعی باشد. این حفاظت حقوقی نه تنها انگیزه اقتصادی برای سرمایه‌گذاری و نوآوری ایجاد می‌کند، بلکه موجب توسعه پایدار فناوری‌های داده‌محور و ایجاد مزیت رقابتی برای مالکین می‌شود (Hall & Harhoff, 2012) واسرار تجاری به مالک داده اجازه می‌دهد اطلاعات حساس خود را بدون افشای عمومی نگهداری کند و از بهره‌برداری غیرمجاز توسط رقبا جلوگیری نماید. با این حال، پیگیری نقض حقوق اسرار تجاری و اثبات مساعدت یا تسهیل نقض توسط دیگران از چالش‌های عملی و حقوقی این ابزار محسوب می‌شود و نیازمند چارچوب‌های قانونی، قراردادی و فناوری‌های امنیتی دقیق است (Bainbridge, 2017).

تحلیل تطبیقی نشان می‌دهد که نظام‌های بین‌المللی حقوق مالکیت فکری، مسئولیت غیرمستقیم ناشی از مساعدت در نقض حقوق مالکیت داده‌ها را به کار می‌گیرند و چارچوب‌هایی برای مدیریت مالکیت مشترک، مسئولیت ارائه‌دهندگان خدمات ابری و ابزارهای تحلیلی ایجاد کرده‌اند. در ایران، هنوز چارچوب صریحی برای مسئولیت غیرمستقیم و حفاظت

جامع از داده‌های بزرگ وجود ندارد و این امر خلأ قانونی در حوزه بهره‌برداری، انتقال و انتشار داده‌ها ایجاد کرده است. بنابراین اقتباس اصول بین‌المللی و تدوین مقررات مشخص می‌تواند زمینه بهره‌برداری قانونی و ایمن از داده‌های بزرگ را فراهم آورد و ریسک‌های حقوقی و اقتصادی را کاهش دهد (Kuner, 2017).

چالش‌ها و محدودیت‌های حقوق مالکیت فکری در حوزه داده‌های بزرگ شامل پیچیدگی‌های حقوقی و فنی، مالکیت مشترک داده‌ها و قابلیت تکثیر سریع آن‌ها است. پیچیدگی حقوقی ناشی از تعامل قوانین حق مؤلف، پتنت و اسرار تجاری با مقررات حفاظت از داده‌ها و استانداردهای بین‌المللی است، در حالی که پیچیدگی فنی به حجم عظیم داده‌ها، تنوع فرمت‌ها و سرعت تولید بالای آن‌ها مربوط می‌شود. مالکیت مشترک و هم‌افزایی داده‌ها موجب می‌شود تعیین مالک واقعی و حقوق استفاده‌کنندگان پیچیده شود و قابلیت تکثیر داده‌ها ریسک سوءاستفاده و نقض حقوق مالک را افزایش می‌دهد.

راهکارهای پیشنهادی برای رفع این چالش‌ها شامل تدوین قوانین خاص برای مالکیت داده‌های بزرگ، شناسایی مسئولیت غیرمستقیم ناشی از مساعدت در نقض حقوق مالکیت، ایجاد استانداردهای امنیتی و حفاظت از محرمانگی داده‌ها و تدوین چارچوب‌های قراردادی و فناوری برای مدیریت مالکیت مشترک و انتقال داده‌ها است. این اقدامات موجب می‌شود مالک داده بتواند حقوق خود را به شکل قانونی و مؤثر اعمال کند و بهره‌برداری اقتصادی، فناورانه و قانونی از داده‌های بزرگ تضمین شود. همچنین، رعایت استانداردهای امنیتی و حفظ محرمانگی داده‌ها موجب افزایش اعتماد کاربران و سرمایه‌گذاران و ایجاد محیطی پایدار برای توسعه فناوری‌های داده‌محور می‌شود و نقش مهمی در توسعه اقتصاد دیجیتال دارد. در نتیجه، حقوق مالکیت فکری در حوزه داده‌های بزرگ نه تنها حفاظت قانونی ایجاد می‌کند بلکه انگیزه‌ای برای نوآوری، سرمایه‌گذاری و بهره‌برداری اخلاقی و مؤثر از داده‌ها فراهم می‌آورد و اهمیت آن در اقتصاد اطلاعات محور و فناوری‌های دیجیتال غیرقابل انکار است (Kuner, 2017; Bainbridge, 2017; Hall & Harhoff, 2012).

مالکیت داده‌های بزرگ در ایران: تحلیل حقوق مالکیت فکری و محدودیت‌های قانونی

مالکیت داده‌های بزرگ در ایران یک حوزه نوظهور و پیچیده در حقوق است و قوانین موجود به صورت مستقیم و صریح به آن اشاره نکرده‌اند، اما با استناد به اصول حقوقی و قوانین مرتبط می‌توان چارچوبی برای فهم مالکیت و حقوق بهره‌برداری از داده‌ها ترسیم کرد. قانون مدنی ایران مالکیت را عمدتاً برای اشیاء مادی و قابل تملک تعریف کرده و تصریح دارد که مالیت شامل اشیاء مادی و حقوق مشروع است، بنابراین داده‌ها و پایگاه‌های داده می‌توانند از طریق قرارداد، حق انحصاری یا حمایت حقوق معنوی قابل تملک شوند و این مالکیت به معنای حق مطلق استفاده نیست بلکه مشروط به قوانین آمره و محدودیت‌های قانونی است (ماده ۲۷۵ قانون مدنی). علاوه بر آن، قانون تجارت الکترونیکی مصوب ۱۳۸۲ به موضوع تبادل اطلاعات دیجیتال، صحت و اعتبار داده‌ها و معاملات مبتنی بر آنها پرداخته و برای داده‌ها و پایگاه‌های داده که قابلیت بهره‌برداری تجاری دارند، حمایت‌هایی در قالب حق تکثیر، حق استفاده محدود و اعتبار قانونی فراهم کرده است، به نحوی که استفاده غیرمجاز از داده‌ها می‌تواند مستلزم مسئولیت کیفری یا مدنی باشد (مواد ۶ و ۸ قانون تجارت الکترونیکی).

قانون حمایت از حقوق مؤلفان، مصنفان و هنرمندان مصوب ۱۳۴۸ و اصلاحات بعدی نیز آثار ادبی، هنری و علمی را شامل نرم‌افزارها و پایگاه داده‌ها می‌داند و پایگاه داده‌ها در صورتی که خلاقیت و انتخاب محتوا در آنها مشهود باشد،

تحت حمایت حقوق مؤلف یا مالکیت معنوی قرار می‌گیرند. تبصره یک ماده ۲ این قانون حق مؤلف را شامل هرگونه بهره‌برداری مادی یا معنوی از اثر دانسته است که می‌تواند برای پایگاه داده‌های ساختاریافته و داده‌های بزرگ با سازماندهی خلاقانه کاربرد داشته باشد. به این ترتیب، مجموعه داده‌ها در صورتی که صرفاً شامل داده خام و بدون ارزش خلاقانه باشند، امکان حمایت کامل حقوق مؤلف را ندارند، اما اگر طراحی پایگاه داده و انتخاب محتوا خلاقانه باشد، مالکیت معنوی قابل اعمال است.با این حال، مالکیت داده‌های بزرگ در ایران محدودیت‌هایی نیز دارد و قوانین آمره نقش اساسی در تعریف حدود مالکیت ایفا می‌کنند. قوانین آمره قابل توافق یا سلب از طریق قرارداد نیستند و شامل حفاظت از حریم خصوصی و داده‌های شخصی، حفاظت از اسرار تجاری و جلوگیری از انحصار و تخلف از رقابت می‌شوند. قانون جرائم رایانه‌ای مصوب ۱۳۸۸ و اصلاحات ۱۳۹۹، حفاظت از اطلاعات شخصی کاربران و جلوگیری از سوءاستفاده از داده‌ها را الزامی دانسته است و داده‌های بزرگ که شامل اطلاعات شخصی باشند تحت حمایت این قانون قرار دارند. بنابراین حتی مالکیت قانونی داده‌ها، حق استفاده مطلق را به مالک نمی‌دهد و استفاده از داده‌های شخصی همواره مشمول محدودیت‌های قانونی است (مواد ۱۷ تا ۲۱ قانون جرائم رایانه‌ای). استفاده بدون اجازه از داده‌های جمع‌آوری شده که به اسرار تجاری لطمه بزند، طبق قانون حمایت از اسرار تجاری مصوب ۱۳۹۰ قابل تعقیب است و این قانون به عنوان یک قانون آمره نمی‌تواند با قرارداد، حق مالکیت کامل بر پایگاه داده‌های شامل اسرار تجاری اعطا کند (مواد ۱ تا ۵ قانون حمایت از اسرار تجاری). علاوه بر این، قوانین مربوط به رقابت و ضدانحصار، از جمله قانون اجرای سیاست‌های کلی اصل ۴۴ و قانون ضدانحصار مصوب ۱۳۸۶، محدودیت‌هایی برای جلوگیری از استفاده انحصاری از داده‌ها که مانع رقابت شود، تعیین کرده‌اند (ماده ۱ و ۳ قانون ضدانحصار). در عمل، مالکیت داده‌های بزرگ در ایران عمدتاً از طریق ترکیب حقوق مؤلف، حقوق پایگاه داده، قراردادها و مجوزهای حقوقی قابل اعمال است و قوانین آمره محدودیت‌های جدی برای مالکیت کامل ایجاد می‌کنند. پایگاه داده‌ها در صورتی که دارای ساختار خلاقانه و انتخاب محتوا باشند، تحت حمایت حقوق معنوی قرار می‌گیرند، اما استفاده از داده‌های شخصی، داده‌های حساس یا داده‌های تجاری همواره مشمول محدودیت‌های قانونی و الزامات حفاظت و امنیت داده است. بنابراین هر گونه بهره‌برداری تجاری یا علمی از داده‌های بزرگ در ایران نیازمند رعایت همزمان قوانین مالکیت فکری، قوانین حریم خصوصی، حفاظت از اسرار تجاری و مقررات رقابت است و بدون رعایت این قوانین، مالکیت داده‌ها نمی‌تواند مطلق باشد و ممکن است مسئولیت کیفری، مدنی یا انتظامی برای مالک ایجاد شود. می توان گفت چارچوب حقوقی مالکیت داده‌های بزرگ در ایران مبتنی بر حمایت از خلاقیت، حقوق پایگاه داده، قراردادها و حقوق محدود قانونی است و قوانین آمره مانند حفاظت از داده‌های شخصی و اسرار تجاری، و جلوگیری از انحصار، نقش مهمی در تعریف محدوده مالکیت و بهره‌برداری از داده‌ها دارند. این چارچوب ترکیبی باعث می‌شود که مالکیت داده‌های بزرگ نه به صورت مطلق بلکه با رعایت محدودیت‌های قانونی و تضمین حقوق دیگران اعمال شود، و هرگونه بهره‌برداری بدون توجه به این محدودیت‌ها ممکن است تخلف محسوب شود و مسئولیت حقوقی ایجاد کند.

مسئولیت قانونی و راهکارها

مسئولیت قانونی ناشی از نقض مالکیت داده‌ها یکی از مهم‌ترین مسائل حقوقی در حوزه داده‌های بزرگ است و شامل مسئولیت مستقیم و غیرمستقیم می‌شود، که هر یک آثار حقوقی و اقتصادی گسترده‌ای دارند و نقش حیاتی در حفاظت از داده‌ها و تضمین بهره‌برداری قانونی ایفا می‌کنند. مسئولیت مستقیم به اقداماتی اطلاق می‌شود که توسط خود شخص یا

سازمان متخلف انجام می‌شود و شامل استفاده غیرمجاز، نقض اسرار تجاری، تکثیر غیرمجاز و بهره‌برداری تجاری بدون مجوز مالک داده است. نمونه‌ای بارز از این نوع مسئولیت، پرونده Equifax Data Breach است که در آن اطلاعات حساس میلیون‌ها مشتری افشا شد و موجب جریمه‌های قانونی، خسارت‌های مالی و کاهش اعتماد عمومی گردید. مسئولیت مستقیم اهمیت ویژه‌ای دارد زیرا نقض‌کننده به صورت مستقیم حقوق مالک داده را تضییع می‌کند و مالک می‌تواند از طریق قوانین حقوقی و قراردادی نسبت به جبران خسارت اقدام نماید (شکوری،۱۳۹۷، ص ۱۲).

مسئولیت غیرمستقیم شامل اقداماتی است که تسهیل یا مساعدت در نقض حقوق مالکیت داده‌ها توسط اشخاص ثالث را ایجاد می‌کنند، بدون آنکه خود متخلف اقدام مستقیم به نقض داده‌ها انجام دهد. این نوع مسئولیت معمولاً مرتبط با ارائه فناوری‌ها، پلتفرم‌ها یا خدمات پردازش داده است که امکان سوءاستفاده از داده‌ها را برای دیگران فراهم می‌کنند. نمونه‌های تاریخی مانند Napster نشان می‌دهد که ارائه پلتفرم اشتراک‌گذاری فایل‌ها می‌تواند مسئولیت غیرمستقیم ایجاد کند، حتی اگر ارائه‌دهنده خدمات خود نقض مستقیمی انجام نداده باشد. در حوزه داده‌های بزرگ، پلتفرم‌های ابری، ابزارهای تحلیلی و سیستم‌های مدیریت داده، در صورتی که کنترل کافی بر استفاده از داده‌ها نداشته باشند، می‌توانند نقش مؤثری در تسهیل نقض حقوق مالک ایفا کنند. شناسایی مسئولیت غیرمستقیم و تعیین شرایط لازم برای اعمال آن، امری حیاتی است تا مالک داده بتواند از حقوق خود دفاع کند و از سوءاستفاده‌های غیرمجاز جلوگیری شود (براتی،۱۳۹۹. ص ۲۳). چالش‌های مسئولیت قانونی در ایران به دلیل نبود قوانین مشخص برای مسئولیت غیرمستقیم و پیچیدگی مالکیت چندجانبه داده‌ها تشدید می‌شود. در بسیاری از پروژه‌های داده‌محور، داده‌ها توسط چندین نهاد جمع‌آوری و پردازش می‌شوند و تعیین مالک واقعی و حقوق استفاده‌کنندگان از داده‌ها با مشکل مواجه است. علاوه بر این، کمبود استانداردهای امنیت داده‌ها و چارچوب‌های فناورانه محافظتی، امکان سوءاستفاده و نقض حقوق مالک را افزایش می‌دهد و ریسک‌های قانونی و اقتصادی برای مالک داده ایجاد می‌کند. این محدودیت‌ها نشان می‌دهند که بدون اصلاحات قانونی و پیاده‌سازی استانداردهای امنیتی، مسئولیت قانونی داده‌ها در ایران ناقص و ناکارآمد است و بهره‌برداری قانونی و ایمن از داده‌های بزرگ را دشوار می‌سازد.

راهکارهای پیشنهادی برای مدیریت مسئولیت قانونی داده‌ها شامل اصلاحات قانونی، شناسایی مسئولیت غیرمستقیم و تدوین مقررات امنیتی و حفاظت از محرمانگی داده‌ها است. اصلاحات قانونی می‌تواند شامل تعریف دقیق مسئولیت مستقیم و غیرمستقیم، تعیین حدود مساعدت و تسهیل در نقض حقوق مالک و ایجاد چارچوب‌های حقوقی برای مالکیت مشترک داده‌ها باشد. علاوه بر چارچوب قانونی، راهکارهای قراردادی نیز اهمیت دارند و شامل تدوین قراردادهای شفاف بین تولیدکنندگان، پردازش‌کنندگان و کاربران داده‌ها و تعیین شرایط جبران خسارت در صورت نقض حقوق مالک است. این قراردادها نقش مؤثری در کاهش ریسک‌های حقوقی و افزایش اطمینان مالک از حفاظت داده‌ها دارند (حسینی،۱۳۹۵، ص ۳۴). راهکارهای فناوری و مدیریتی نیز مکمل اقدامات قانونی و قراردادی هستند و شامل استفاده از رمزگذاری داده‌ها، کنترل دقیق دسترسی کاربران، نظارت مداوم بر استفاده از داده‌ها و پیاده‌سازی سیاست‌های امنیتی و محرمانگی می‌شود. این اقدامات نه تنها مسئولیت قانونی ارائه‌دهندگان خدمات و کاربران داده را کاهش می‌دهند، بلکه امکان مدیریت مؤثر بهره‌برداری از داده‌ها، جلوگیری از سوءاستفاده غیرمجاز و حفظ مزیت رقابتی مالک را فراهم می‌آورند (علوی،۱۳۹۸، ص ۲۴). ترکیب این سه سطح یعنی چارچوب قانونی، قراردادهای شفاف و فناوری‌های محافظتی، محیطی پایدار، امن و قابل اعتماد برای استفاده و بهره‌برداری از داده‌های بزرگ ایجاد می‌کند و به مالک داده

اطمینان می‌دهد که حقوق او به شکل مؤثر حفظ می‌شود. در نتیجه، مدیریت مسئولیت قانونی، شناسایی مسئولیت غیرمستقیم و پیاده‌سازی راهکارهای قانونی، قراردادی و فناوری از الزامات حیاتی بهره‌برداری قانونی، ایمن و مؤثر از داده‌های بزرگ هستند و نقش مهمی در توسعه فناوری‌های داده‌محور و اقتصاد دیجیتال ایفا می‌کنند (Goldman, 2020).

مطالعات موردی در حوزه مالکیت داده‌ها و حقوق مالکیت فکری نشان می‌دهند که چالش‌های قانونی و مسئولیت استفاده غیرمجاز داده‌ها بسیار متنوع و پیچیده است. Napster نمونه‌ای از نقض حقوق مالکیت فکری در زمینه اشتراک‌گذاری موسیقی بود که مسئولیت غیرمستقیم پلتفرم را به بحث گذاشت و موجب تغییر قوانین مربوط به انتشار محتوا شد. سیستم YouTube Content ID نیز مثال موفقی از مدیریت حقوق مالکیت فکری در محیط دیجیتال است که با استفاده از فناوری تشخیص محتوا، مالکین را قادر می‌سازد از حقوق خود محافظت کنند و درآمد ناشی از استفاده از محتوایشان را دریافت نمایند. در حوزه پزشکی، پرونده‌های استفاده غیرمجاز از داده‌های بیماران در اروپا نشان می‌دهند که رعایت استانداردهای حفاظت از داده‌ها و محرمانگی برای جلوگیری از نقض حقوق افراد ضروری است و قوانین مانند GDPR چارچوب قانونی محکمی فراهم کرده‌اند. در حوزه مالی، افشای داده‌های مشتریان در پرونده‌هایی مانند Equifax، اهمیت مسئولیت مستقیم و مدیریت ریسک‌های امنیتی را برجسته می‌کند. در ایران، نمونه‌های مشابه محدودتر و عمدتاً مرتبط با پروژه‌های دیجیتال و قراردادهای فناوری اطلاعات است که نشان می‌دهد خلا قانونی و نبود چارچوب مشخص برای مالکیت داده‌ها و مسئولیت غیرمستقیم همچنان وجود دارد. این مطالعات موردی اهمیت تدوین قوانین مشخص، پیاده‌سازی فناوری‌های حفاظتی و استانداردهای امنیتی، و استفاده از قراردادهای شفاف برای مدیریت مالکیت داده‌ها را به وضوح نشان می‌دهند. آنها همچنین تأکید می‌کنند که حفاظت از داده‌ها نه تنها الزامی قانونی بلکه یک ضرورت اقتصادی و اخلاقی است و نقش مهمی در ایجاد اعتماد کاربران، سرمایه‌گذاران و توسعه فناوری‌های داده‌محور دارد. مطالعه تطبیقی این پرونده‌ها می‌تواند به سیاست‌گذاران و سازمان‌ها در تدوین مقررات مؤثر و بهره‌برداری قانونی از داده‌های بزرگ کمک کند. اهمیت فناوری‌های تشخیص خودکار محتوا، رمزگذاری، کنترل دسترسی و نظارت مداوم نیز در این نمونه‌ها آشکار است و نشان می‌دهد که ترکیب چارچوب قانونی، راهکارهای قراردادی و فناوری، کلید مدیریت موفق مالکیت داده‌ها است (Goldman, 2020; Bainbridge, 2017; Kuner, 2017).

نتیجه‌گیری و پیشنهادها

داده‌های بزرگ به عنوان دارایی‌های ارزشمند و حیاتی در عصر دیجیتال شناخته می‌شوند و حفاظت قانونی از آن‌ها اهمیت بالایی دارد، زیرا این داده‌ها نه تنها ارزش اقتصادی قابل توجهی دارند بلکه نقش کلیدی در توسعه فناوری، تصمیم‌گیری‌های هوشمند و ایجاد مزیت رقابتی برای سازمان‌ها ایفا می‌کنند. ابزارهای حقوق مالکیت فکری مانند حق مؤلف، پتنت و اسرار تجاری امکان مدیریت بهره‌برداری، کنترل انتشار و محافظت از داده‌ها و فناوری‌های مرتبط را فراهم می‌آورند و در ترکیب با مسئولیت‌های قانونی مستقیم و غیرمستقیم، چارچوبی جامع برای حفاظت از داده‌ها ایجاد می‌کنند. مسئولیت مستقیم، شامل استفاده غیرمجاز، نقض اسرار تجاری و بهره‌برداری بدون مجوز مالک است و امکان پیگیری قانونی و جبران خسارت را فراهم می‌آورد، در حالی که مسئولیت غیرمستقیم مرتبط با مساعدت یا تسهیل نقض حقوق مالک توسط اشخاص ثالث است و نیازمند شناسایی ارکان قانونی و تعریف دقیق حدود مساعدت می‌باشد.

ترکیب این ابزارهای قانونی و حقوقی به مالک داده اجازه می‌دهد که بهره‌برداری اقتصادی، امنیتی و فناورانه از داده‌ها را مدیریت کند و از سوءاستفاده‌های غیرمجاز جلوگیری نماید (Bainbridge, 2017; Kuner, 2017).

در ایران، با وجود قوانین مرتبط با تجارت الکترونیک و حمایت از داده‌های شخصی، چارچوب جامع مالکیت داده‌ها و مسئولیت غیرمستقیم هنوز ناقص است و خلاهای قانونی متعددی وجود دارد. فقدان قوانین اختصاصی برای مالکیت داده‌های بزرگ و مسئولیت غیرمستقیم، مشکلات ناشی از مالکیت چندجانبه داده‌ها و نبود استانداردهای امنیتی و محرمانگی، ریسک‌های حقوقی و اقتصادی قابل توجهی ایجاد کرده است و بهره‌برداری ایمن و قانونی از داده‌های بزرگ را دشوار می‌سازد. بنابراین، اصلاحات قانونی، تدوین مقررات مشخص برای مالکیت داده‌ها و شناسایی مسئولیت‌های مستقیم و غیرمستقیم، ضرورت دارد تا چارچوبی پایدار و قابل اعتماد برای مدیریت داده‌ها ایجاد شود و ارزش واقعی اقتصادی و فناورانه آن‌ها محقق گردد. این اصلاحات قانونی باید شامل تعریف دقیق مالکیت داده‌ها، شناسایی حدود مسئولیت غیرمستقیم، الزام به رعایت استانداردهای امنیتی و محرمانگی و ایجاد سازوکارهای قانونی برای جبران خسارت در صورت نقض حقوق مالک باشد.

راهکارهای قراردادی نیز از اهمیت بالایی برخوردار هستند و شامل تدوین قراردادهای شفاف بین تولیدکنندگان، پردازش‌کنندگان و کاربران داده‌ها، تعیین حقوق دسترسی و بهره‌برداری، و پیش‌بینی مکانیزم‌های جبران خسارت در صورت نقض حقوق مالک است. این قراردادها نقش مؤثری در کاهش اختلافات حقوقی و ایجاد اعتماد میان طرفین ایفا می‌کنند و چارچوبی روشن برای بهره‌برداری قانونی از داده‌ها فراهم می‌آورند. علاوه بر چارچوب قانونی و قراردادی، راهکارهای فناوری و مدیریتی نیز اهمیت حیاتی دارند و شامل استفاده از رمزگذاری داده‌ها، کنترل دقیق دسترسی کاربران، نظارت مداوم بر استفاده از داده‌ها، آموزش کارکنان و اعمال سیاست‌های امنیتی و محرمانگی می‌شوند. ترکیب این راهکارها با چارچوب‌های قانونی و قراردادی امکان مدیریت مؤثر مالکیت داده‌ها و جلوگیری از سوءاستفاده‌های غیرمجاز را فراهم می‌کند و محیطی ایمن و پایدار برای بهره‌برداری قانونی و اقتصادی از داده‌های بزرگ ایجاد می‌نماید.

تلفیق ابزارهای حقوق مالکیت فکری، مسئولیت قانونی و فناوری‌های حفاظتی، چارچوب مناسبی برای حفاظت از داده‌های بزرگ ایجاد می‌کند و علاوه بر تضمین حقوق مالک، مزیت اقتصادی و امنیتی قابل توجهی برای سازمان‌ها فراهم می‌آورد. رعایت این چارچوب موجب افزایش اعتماد کاربران و سرمایه‌گذاران، کاهش ریسک‌های حقوقی و اقتصادی و ایجاد زمینه توسعه پایدار فناوری‌های داده‌محور می‌شود. همچنین، ترکیب قانونی، قراردادی و فناورانه این ابزارها امکان بهره‌برداری هوشمندانه، امن و قانونی از داده‌ها را فراهم می‌آورد و ارزش واقعی داده‌های بزرگ را محقق می‌سازد. در نتیجه، تدوین اصلاحات قانونی، قراردادهای شفاف، استانداردهای امنیتی و محرمانگی داده‌ها و آموزش کاربران، عناصر کلیدی برای مدیریت مؤثر مالکیت داده‌ها و تضمین بهره‌برداری قانونی، ایمن و اقتصادی از داده‌های بزرگ هستند و اهمیت آن‌ها در اقتصاد دیجیتال و فناوری‌های اطلاعاتی غیرقابل انکار است (Bainbridge, 2017; Kuner, 2017).

در پایان، این مقاله با ارائه چارچوبی جامع برای مالکیت داده‌ها و مسئولیت قانونی، پیشنهادهایی عملی و کاربردی ارائه می‌دهد که می‌تواند به سیاست‌گذاران، سازمان‌ها و پژوهشگران کمک کند تا از داده‌های بزرگ به شکل قانونی، امن و اقتصادی بهره‌برداری نمایند و محیطی پایدار و قابل اعتماد برای توسعه فناوری‌های داده‌محور ایجاد کنند. توجه به این

چارچوب، نه تنها حفاظت حقوق مالک را تضمین می‌کند بلکه موجب افزایش بهره‌وری، کاهش ریسک‌های قانونی و اقتصادی و ایجاد مزیت رقابتی پایدار می‌شود و نقش مهمی در توسعه اقتصاد اطلاعات محور ایفا می‌کند.

منابع

مقالات فارسی:

جعفری، م. (۱۴۰۰). «مالکیت داده‌ها و حقوق مالکیت فکری در ایران». فصلنامه حقوق فناوری اطلاعات, ۱۵ (۳), ۱۲۳–۱۵۰.

نجفی، م. (۱۳۹۸). «حفاظت از اسرار تجاری و چالش‌های حقوقی آن در ایران». فصلنامه حقوق مالکیت فکری و فناوری‌های نوین, ۱۲ (۳), ۴۰–۵۵.

فیاضی، س. (۱۴۰۱). «چالش‌های حقوقی مالکیت داده‌های بزرگ و راهکارهای محافظتی». فصلنامه پژوهش‌های حقوق فناوری اطلاعات و داده‌های دیجیتال, ۴ (۲), ۴۰–۵۵.

مولایی، م. (۱۳۹۸). «چارچوب حقوقی مالکیت داده‌های بزرگ در ایران و تجربه تطبیقی با قوانین بین‌المللی». مجله حقوق فناوری اطلاعات و داده‌های دیجیتال ایران, ۳ (۱), ۳۰–۴۵.

مرعشی، ع. (۱۳۹۹). «نقش اسرار تجاری در حفاظت از داده‌ها و الگوریتم‌ها». مجله پژوهش‌های حقوقی فناوری اطلاعات, ۴ (۲), ۲۰–۳۵.

طالب‌زاده، م. (۱۳۹۷). «ابعاد حقوقی و اجتماعی مالکیت داده‌ها». مجله حقوق فناوری اطلاعات, ۳ (۱), ۱۰–۲۵.

تابش، ع. (۱۳۹۰). «چالش‌ها و الزامات حقوقی پردازش داده‌ها در محیط‌های ابری». فصلنامه حقوق فناوری اطلاعات و ارتباطات, ۲ (۳), ۲۰–۳۵.

علوی، م. (۱۳۹۸). «راهکارهای فناوری و مدیریتی در حفاظت از داده‌ها و مسئولیت حقوقی کاربران». فصلنامه مدیریت فناوری اطلاعات, ۵ (۲), ۲۰–۳۰.

حسینی، ع. (۱۳۹۵). «راهکارهای حقوقی و قراردادی مدیریت مسئولیت قانونی داده‌ها». مجله حقوق فناوری اطلاعات, ۳ (۱), ۳۰–۴۰.

کتابی، م. (۱۴۰۰). «مسئولیت غیرمستقیم در حقوق مالکیت داده‌ها». فصلنامه حقوق فناوری و اطلاعات, ۵ (۲), ۲۸–۳۶.

براتی، ع. (۱۳۹۹). «مسئولیت غیرمستقیم در بهره‌برداری از داده‌های بزرگ و پلتفرم‌های ابری». مجله حقوق فناوری اطلاعات و داده‌ها, ۵ (۱), ۲۰–۲۸.

شکوری، م. (۱۳۹۷). «مسئولیت مستقیم در حقوق مالکیت داده‌ها و راهکارهای جبران خسارت». فصلنامه حقوق دیجیتال و مالکیت فکری, ۳ (۲), ۱۰–۱۸.

حبیبی، س. (۱۳۹۶). «چارچوب حقوقی مالکیت داده‌های بزرگ در ایران و چالش‌های مسئولیت قانونی». مجله حقوق فناوری اطلاعات و داده‌های بزرگ, ۴ (۱), ۲۰–۳۰.

رضایی، م. (۱۳۹۹). «مسئولیت غیرمستقیم در بهره‌برداری از داده‌ها: تحلیل حقوقی و چالش‌ها». فصلنامه حقوق فناوری اطلاعات و اقتصاد دیجیتال, ۷ (۲), ۵۰–۶۰.

تراب‌نژاد، ع. (۱۳۹۹). «اهمیت مالکیت داده‌ها در عصر دیجیتال». مجله تحقیقات مدیریت و فناوری, ۱۲ (۳), ۴۲–۵۰.

۲. منابع انگلیسی

Books:

Laney, D. (2001). 3D Data Management: Controlling Data Volume, Velocity, and Variety. META Group Research Note.

Kitchin, R. (2014). The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences. SAGE Publications.

van der Sloot, B. (2019). Big Data and Privacy: Data Protection Impact Assessments and Beyond. Springer.

Bainbridge, D. (2017). Intellectual Property. 10th Edition, Pearson Education.

Articles:

Kuner, C. (2017). "Reality and Illusion in EU Data Transfer Regulation Post Schrems." Computer Law & Security Review, 33(2), 140–149.

Tene, O., & Polonetsky, J. (2013). "Big Data for All: Privacy and User Control in the Age of Analytics." Northwestern Journal of Technology and Intellectual Property, 11(5), 239–273.

Goldman, J. (2020). "Contributory Liability in the Age of Big Data: Legal Approaches to Indirect Infringement." Journal of Intellectual Property Law, 27(1), 45–78.

Hall, B. H., & Harhoff, D. (2012). "Recent Research on the Economics of Patents." Annual Review of Economics, 4, 541–565.

Cases and Legal Documents:

SAS Institute v. World Programming Ltd, Case C-406/10, \[2012] ECR I-0000.

Equifax Data Breach Case, United States, 2017.

Napster Case, A\&M Records, Inc. v. Napster, Inc., 239 F.3d 1004 (9th Cir. 2001).

YouTube Content ID Case, Viacom International Inc. v. YouTube, Inc., 676 F.3d 19 (2d Cir. 2012).
GDPR (General Data Protection Regulation), Regulation (EU) 2016/679.