Civil Law Knowledge Open Access

Autumn & Winter (2026) 14 (2): 175-193

DOI: 10.30473/clk.2026.76021.3419

ORIGINAL ARTICLE

The Requirements of Intellectual Property Rights for Big Data Generated within the Internet of Things Ecosystem

Amid Mohammadi[1]

1. Assistant Professor in Private Law, Department of Law, Faculty of humanity, Jahrom University, Jahrom, Iran.

Correspondence:
Amid Mohammadi
Email: amid_mohammadi@jahromu.ac.ir

Received: 02/Oct/2025
Revised: 24/Dec/2025
Accepted: 16/ May/2026
Published: 20/May/2026

How to cite:
Mohammadi, A. (2026). The Requirements of Intellectual Property Rights for Big Data Generated within the Internet of Things Ecosystem, Civil Law Knowledge, 14 (2), 175-193.
(DOI: 10.30473/clk.2026.76021.3419)

ABSTRACT

The emerging paradigm of the "Internet of Things" (IoT), by establishing an integrated network of physical objects equipped with advanced sensors, data processors, and communication infrastructures, has fundamentally dissolved the boundaries between the physical and digital environments, thereby generating data of unprecedented volume, variety, and velocity, commonly referred to as "big data." This study, focusing on an analysis of the supportive frameworks of intellectual property law within the IoT ecosystem, seeks to investigate the central question of how a legal status for the protection of big data generated in this domain can be defined within the confines of the intellectual property system. Adopting a descriptive-analytical approach and evaluating the capacities of classical intellectual property institutions—including copyright, the patent system, and the protection of trade secrets—this article argues that these mechanisms cover only limited facets of the complex reality of the IoT and face fundamental substantive challenges when confronted with the unique nature of big data, particularly its lack of originality for copyright, absence of a novelty requirement for patentability, and the difficulties in fulfilling the condition of confidentiality for trade secrets. The findings of this research indicate that the inherent inadequacy of these legal institutions in adapting to the intrinsic characteristics of big data inevitably compels legislators and jurists to create independent theoretical frameworks and design novel protective mechanisms capable of providing a fitting response to the unprecedented legal questions of this field.

KEYWORDS

Internet of Things, Big Data, Connected Technology, Intellectual Property, Sui generis System.

© 2026, by the author(s). Published by Payame Noor University, Tehran, Iran.
This is an open access article under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).
https://clk.journals.pnu.ac.ir/

Extended Abstract

Introduction and Problem Statement

This abstract examines the challenges and requisite adaptations within the intellectual property (IP) regime posed by the emergent phenomenon of the "Internet of Things" (IoT) and, specifically, the vast quantities of data—Big Data—generated within its ecosystem. The IoT, conceptualized as an integrated network of physical objects embedded with sensors, software, and connectivity technologies, is catalyzing the Fourth Industrial Revolution by merging the physical and digital worlds. Its pervasive applications across sectors such as healthcare, agriculture, industry, and smart cities, coupled with the automated, continuous, and mass generation of data, have engendered unprecedented legal complexities. Paramount among these is the challenge of delineating an appropriate legal framework for the protection of associated intellectual assets, particularly Big Data.

The central research question of this inquiry is: Given the inherent characteristics of Big Data (volume, velocity, variety) and the decentralized, interdisciplinary nature of the IoT, to what extent is the traditional IP regime capable of providing effective and comprehensive protection? Furthermore, what legal imperatives and frameworks are essential to address this legislative lacuna? To answer this, employing an analytical-descriptive methodology and drawing upon authoritative library sources, this study scrutinizes the three principal pillars of IP—copyright, patent law, and trade secrets—in their confrontation with this technology and its data.

Analysis of Traditional Intellectual Property Frameworks

Copyright: The copyright framework is designed to protect the original "expression" of an idea, not the idea itself. This legal instrument finds application in protecting embedded software within smart objects and, in some instances, the creative structure and arrangement of databases. However, when confronting "raw data" generated by sensors (e.g., temperature, positional, or health status data), the copyright system encounters a fundamental obstacle: the "lack of originality." Raw data, being predominantly the product of an automated process devoid of direct human creative authorship, fails to meet the threshold of originality required for copyright protection. Consequently, copyright can only afford a thin layer of protection to Big Data—covering its formatting and superficial structure—while the core, value-generating substance of the data remains outside its protective scope.

Patent Law: The patent system, which protects inventions possessing novelty, non-obviousness (inventive step), and industrial applicability, could ostensibly extend to innovative IoT processes, data processing algorithms, and analytical models. The principal challenge, however, lies in the substantive and procedural barriers within many legal systems—including that of Iran—against granting patents for "mathematical algorithms" and "software *per se*." While jurisdictions like the United States may permit the patenting of an algorithm if it yields a "specific, tangible, and practical application" beyond an abstract idea, establishing a "non-obvious inventive step" for algorithms operating on mass data analysis is often arduous. Furthermore, the protracted and costly patent registration process is fundamentally incompatible with the rapid pace of development and iteration characteristic of IoT technology.

Trade Secrets: Among the classical IP institutions, trade secrets emerge as the most efficacious mechanism for protecting many components of the IoT and Big Data, owing to their flexibility, absence of registration formalities, and broad scope of coverage. This instrument can protect a wide spectrum of items—from raw data and proprietary analytical algorithms to business models and customer lists—provided they derive economic value from not being generally known and reasonable efforts are undertaken to maintain their secrecy. This makes trade secrets an attractive option for companies operating in this domain. Nevertheless, this mechanism suffers from inherent limitations: vulnerability to breaches of confidentiality via cyber-attacks, reverse engineering, or employee malfeasance. Moreover, the non-disclosure nature of trade secrets can potentially stifle knowledge dissemination and impede the innovation cycle in an ecosystem intrinsically predicated on data sharing.

Synthesizing Deficiencies and the Imperative for a Novel Framework

The foregoing analysis demonstrates that none of the traditional IP institutions, in isolation, is capable of providing a comprehensive and proportionate response to the complexities of the IoT and Big Data. Copyright is impotent in protecting raw data; patent law grapples with substantive and temporal hurdles; and trade secrets are fraught with the inherent risks of disclosure and the restriction of information flow. This theoretical and legislative lacuna compellingly necessitates a fundamental re-examination of foundational principles and the creation of novel, flexible, and multi-layered protective frameworks.

Proposed Imperatives and Solutions

The ultimate conclusion of this research underscores the imperative of moving towards an "Integrated and Multi-Layered Governance Model" for intellectual property in the IoT domain. This model does not rely on a single, exclusive solution but operates through the simultaneous and intelligent deployment of various mechanisms and, in some instances, the development of new legal institutions:

1. **A Hybrid Approach:** This approach proposes the coordinated utilization of the strengths of existing IP institutions. For instance, patents can protect truly innovative hardware devices and processes; copyright can safeguard software and database structures; and trade secrets can be employed to preserve raw data, analytical algorithms, and predictive models whose value resides in their confidentiality.
2. **Development of Specific and Independent Frameworks:** In light of existing inadequacies, the formulation of a *sui generis* system for the protection of data-based assets could be instrumental. Such a regime could establish limited, time-bound exclusive rights for Big Data producers, while simultaneously guaranteeing fair access for other actors for competitive or research purposes, thereby striking a balance between innovation incentives and the public interest.
3. **Implementation of Flexible Regulatory Mechanisms:** Mechanisms such as industry "self-regulation" under governmental oversight, "stringent security standards" for data and algorithm protection, and "data governance" models emphasizing transparency, fairness, and accountability can serve as appropriate complements to IP frameworks.
4. **Emulation of Emerging Institutions:** Procedures such as "Post-Grant Review" in the U.S. system, which allows for the efficient and expedited re-examination of a patent's validity, can serve as a model for curbing frivolous patents and facilitating innovation within the dynamic IoT landscape.

Final Conclusion

Protecting intellectual assets in the realm of the IoT and its concomitant Big Data necessitates a departure from traditional paradigms and the adoption of a systemic, dynamic, and forward-looking perspective. The integrated, multi-layered framework proposed in this research can serve as a roadmap for legislators and policymakers—particularly within the Iranian legal context—to devise efficient, equitable regulations that are congruent with the exigencies of the Fourth Industrial Revolution. Only through such an approach can the dual objectives of preserving innovation incentives and preventing data from becoming an arena of anti-competitive exclusivity be achieved.

Keywords: Internet of Things (IoT), Big Data, Intellectual Property, Copyright, Patent Law, Trade Secrets, Data Governance, Sui Generis Legal System, Integrated Framework.

دانش حقوق مدنی

سال چهاردهم، شماره دوم، پیاپی ۲۸، پاییز و زمستان ۱۴۰۴ (۱۹۳-۱۷۵)

DOI: 10.30473/clk.2026.76021.3419

«مقاله پژوهشی»

بایسته‌های حقوق مالکیت فکری در حوزه کلان‌داده‌های ناشی از اکوسیستم «اینترنت اشیا»

عمید محمدی[۱]

۱. استادیار حقوق خصوصی، گروه حقوق، دانشکده علوم انسانی، دانشگاه جهرم، جهرم، ایران.

نویسنده مسئول:
عمید محمدی
رایانامه: amid_mohammadi@jahromu.ac.ir

تاریخ دریافت: ۱۴۰۴/۰۷/۱۰
تاریخ بازنگری: ۱۴۰۴/۱۰/۰۳
تاریخ پذیرش: ۱۴۰۵/۰۲/۲۶
تاریخ چاپ: ۱۴۰۵/۰۲/۳۰

چکیده

پارادایم نوظهور «اینترنت اشیا» با ایجاد شبکه‌ای یکپارچه از اجسام فیزیکی مجهز به حسگرهای پیشرفته، پردازشگرهای داده و زیرساخت‌های ارتباطی، مرزهای محیط واقعی و دیجیتال را درنوردیده و داده‌هایی با حجم، تنوع و سرعت بی‌سابقه موسوم به «کلان‌داده‌ها» تولید می‌نماید. پژوهش حاضر با تمرکز بر تحلیل چارچوب‌های حمایتی حقوق مالکیت فکری در اکوسیستم اینترنت اشیا، درصدد واکاوی این پرسش اساسی است که چگونه می‌توان در محدوده نظام مالکیت فکری، جایگاهی حقوقی برای حمایت از کلان‌داده‌های تولیدشده در این فضا تعریف کرد. با اتخاذ رویکردی توصیفی-تحلیلی و با ارزیابی ظرفیت‌های نهادهای کلاسیک مالکیت فکری از جمله کپی‌رایت، نظام حق اختراع و حمایت از اسرار تجاری، این مقاله استدلال می‌نماید که این مکانیسم‌ها، تنها وجوه محدودی از واقعیت پیچیده اینترنت اشیا را پوشش داده و در مواجهه با ماهیت منحصربه‌فرد کلان‌داده‌های حاصله از آنها که از حیث فقدان اصالت اثر، نبود شرط نوآوری و دشواری در تحقق شرط محرمانگی، با چالش‌های ماهوی بنیادینی روبه‌رو هستند. یافته‌های این تحقیق حاکی از آن است که نارسایی ذاتی این نهادهای حقوقی در تطبیق با ویژگی‌های ذاتی کلان‌داده‌ها، تقنین‌گذاران و حقوقدانان را ناگزیر از خلق چارچوب‌های نظری مستقل و طراحی سازوکارهای‌های حمایتی نوین می‌سازد که بتواند پاسخی درخور به مسائل حقوقی بی‌پیشینه این عرصه باشد.

واژه‌های کلیدی

اینترنت اشیا، کلان داده‌ها، فناوری متصل، مالکیت فکری، نظام حقوقی مستقل.

استناد به این مقاله:

محمدی، عمید (۱۴۰۴). بایسته‌های حقوق مالکیت فکری در حوزه کلان‌داده‌های ناشی از اکوسیستم «اینترنت اشیا»، دوفصلنامه علمی دانش حقوق مدنی، ۱۴ (۲)، ۱۹۳-۱۷۵.
(DOI: 10.30473/clk.2026.76021.3419)

حق انتشار این مستند، متعلق به نویسندگان آن است. ۱۴۰۴ ©. ناشر این مقاله، دانشگاه پیام نور است.

مجوز Creative Commons Attribution (CC BY 4.0) منتشر شده و استفاده از آن با ارجاع صحیح مجاز است.
(http://creativecommons.org/licenses/by/4.0/)
https://clk.journals.pnu.ac.ir/

مقدمه

در عصر حاضر، شتاب فزاینده پیشرفت‌های فناورانه در حوزه‌هایی نظیر هوش مصنوعی، چت‌بات‌ها، متاورس، بلاک‌چین و رایانش ابری، زمینه‌ساز دگرگونی‌های بنیادین در عرصه‌های مختلف حیات بشری شده است. در این میان، فناوری موسوم به «اینترنت اشیا» با ایفای نقش یک اکوسیستم یکپارچه و به‌هم‌پیوسته برای شبکه‌سازی دستگاه‌های هوشمند، کارکردی عملگرا و بی‌بدیل در فرایند دیجیتالی‌سازی جهان فیزیکی ایفا می‌کند. این نقش کاتالیزوری و تحول‌آفرین تا بدان حد برجسته است که از سوی بسیاری از صاحب‌نظران، به‌عنوان موتور محرک و بستر زیرساختی «چهارمین انقلاب صنعتی» توصیف شده است (Greenberg, 2020: 331).

اینترنت اشیا با فراهم‌آوردن بستر ارتباط خودکار میان اشیا و امکان پردازش و تحلیل داده‌ها بدون نیاز به مداخله مستقیم انسان، کارایی و بهره‌وری سیستم‌ها را در حوزه‌های گوناگونی از قبیل بهداشت و درمان، صنعت، کشاورزی و مدیریت شهرهای هوشمند، به‌طور چشمگیری افزایش داده است. با این حال، همین تعامل پیوسته و خودکار میان دستگاه‌های متصل، منجر به تولید حجم بی‌سابقه‌ای از داده‌ها شده که عمدتاً بدون دخالت انسان و از طریق فرایندهای مبتنی بر یادگیری ماشین و هوش مصنوعی تولید می‌شوند. این ویژگی ذاتی، به‌کارگیری فناوری اینترنت اشیا را با چالش‌ها و پرسش‌های حقوقی پیچیده‌ای مواجه ساخته که از جمله آنها می‌توان به مباحث مربوط به منبع و کیفیت داده، مسئله مالکیت و تعدد ذینفعان، حریم خصوصی اطلاعات و تعیین حدود و ثغور حمایت‌های مالکیت فکری اشاره کرد (Peppet, 2014: 117).

در خصوص چگونگی حمایت از فناوری اینترنت اشیا در پرتو حقوق مالکیت فکری، میان صاحب‌نظران و پژوهشگران اختلاف نظر وجود دارد. عده‌ای بر این عقیده‌اند که این فناوری با ایجاد بستری برای نوآوری و توسعه خلاقیت در عرصه صنایع وابسته، فرصت‌های بی‌سابقه‌ای فراهم می‌آورد (Robinson, 2015: 670).در مقابل، گروهی دیگر از محققان استدلال می‌کنند که نظام سنتی مالکیت فکری با ویژگی‌های متمایز اینترنت اشیا از جمله تولید انبوه داده‌ها، ارتباطات پیچیده و چندلایه و محدودیت‌های ذاتی منابع سخت‌افزاری ناسازگاری دارد و این امر، ضرورت بازاندیشی در مبانی و سازوکارهای حمایتی موجود را ایجاب می‌کند (Anwar Yelukar & Siddhi Vijay, 2023: 302). افزون بر این، پیاده‌سازی مکانیسم‌های حفاظتی، تضمین محرمانگی الگوریتم‌ها و تعیین مالکیت آنها، از دیگر مشکلات پیش‌روی این فناوری به‌شمار می‌روند. این موانع نه‌تنها توسعه و گسترش اینترنت اشیا را با دشواری مواجه ساخته، بلکه بر توانایی نظام‌های حاکمیتی حقوق مالکیت فکری در تنظیم‌گری و ساماندهی مؤثر این پدیده نوظهور تأثیر گذاشته است (Heer et al, 2011: 2).

این پژوهش با روش تحلیلی–توصیفی و با اتکا بر منابع کتابخانه‌ای، در پی تبیین بایسته‌های حقوق مالکیت فکری کلان‌داده‌ها با تمرکز بر اینترنت اشیا است. اگرچه در در ادبیات حقوقی ایران زوایای پراکنده‌ای از حقوق داده‌ها (انصاری و عطّار، ۱۴۰۰؛ حبیبا و نبوی، ۱۴۰۳) و حتی ارائه چارچوب کلی برای حمایت از اینترنت اشیا از منظرهای مختلف (صادقی و ناصر، ۱۳۹۹؛ معینی‌فر و وحیدزاده، ۱۴۰۱؛ فرهادخانی و دیگران، ۱۴۰۲) مدنظر نویسندگان بوده است، لیکن بررسی مبسوط و منسجم قابلیت اعمال حقوق مالکیت فکری به فناوری مزبور تاکنون مورد اقبال محققان واقع نشده است. بنابراین، هدف این تحقیق، مطالعه مراتب تعامل نظام مذکور با پیچیدگی‌های ذاتی کلان‌داده‌های اینترنت اشیا از رهگذر تأسیسات حقوقی چون کپی‌رایت، حق اختراع و اسرار تجاری است. در این راستا، سؤوال اصلی این است که کلان‌داده‌های تولیدشده توسط اینترنت اشیا، چه جایگاهی در نظام حقوق مالکیت فکری دارند و تحت چه شرایط و قالب‌هایی می‌توانند از حمایت انحصاری برخوردار شوند؟ پاسخ به این پرسش، مسیری راهبردی برای تنظیم‌گری این عرصه نوظهور ترسیم خواهد کرد. یافته‌ها مؤید از آن است که اگرچه نظام حقوق مالکیت فکری از پتانسیل لازم برای حکمرانی بر این فناوری برخوردار است، اما فعلیت‌یافتن این نقش، منوط به نوسازی چارچوب‌ها و توسعه‌ی سازوکارهای انعطاف‌پذیر، متناسب با اقتضائات خاص اینترنت اشیا و کلان‌داده‌هاست.

ملاحظات نظری پیرامون اینترنت اشیا

در ابتدا به بررسی مفهوم و سیر تکوین اینترنت اشیا، تحلیل اجزای تشکیل‌دهنده و ارکان اساسی آن و در نهایت، واکاوی

1. Internet of Thing (IoT)

مصادیق عینی و کاربردهای عملی این فناوری در حوزه‌های مختلف می‌پردازیم.

۱. مفهوم و سیر پیدایش

اینترنت اشیا به عنوان یک مفهوم میان‌رشته‌ای، بر پایه دانش‌های گوناگونی از جمله مهندسی مخابرات، الکترونیک، علوم کامپیوتر و دیگر شاخه‌های فناوری اطلاعات استوار است (Rose et al, 2015: 12). در این ترکیب، کلمه «اینترنت» بر ماهیت شبکه‌ای و واژه «شیء» بر قابلیت اتصال اشیای فیزیکی به شبکه مزبور دلالت دارد. به‌رغم کاربرد گسترده این اصطلاح، تعریف واحدی که مورد اتفاق صاحب‌نظران باشد، ارائه نشده است. فرهنگ لغت آکسفورد، اینترنت اشیا را «اتصال متقابل دستگاه‌های محاسباتی جاسازی‌شده در اشیا از طریق اینترنت که امکان ارسال و دریافت داده را فراهم می‌کنند» تعریف کرده است.[1]

به طور کلی، این فناوری به چگونگی تعامل رایانه‌ها، حسگرها و اشیا و اتصال آنها در بستر اینترنت برای پردازش اطلاعات در یک سناریوی ارتباطی می‌پردازد، به‌طوری که داده‌ها بدون نیاز به مداخله انسانی منتقل شده و دستورالعمل‌ها به اشیا ارسال می‌گردد، بی‌آنکه ملاحظات امنیتی و حریم خصوصی نادیده گرفته شود (De Araujo et al, 2020: 138; Robinson, 2015: 662). به عبارت دیگر، اینترنت اشیا ناظر بر این است که اشیا از طریق اینترنت بایکدیگر مرتبط می‌شوند. در این پارادایم، دستگاه‌ها کاربران اصلی محسوب می‌شوند و این باور غلط که اشیا دارای اینترنت هستند را باید از ذهن زدود (Bello & Zeadally, 2014: 2). بر همین بنیان، از این پدیده به عنوان «زیرساخت شبکه‌ای اشیای فیزیکی» یاد شده است (Kortuem et al, 2010: 44).

کاربردهای پیشرفته اینترنت اشیا اغلب با تلفیق الگوریتم‌های پیچیده، مؤلفه‌های هوش مصنوعی[2] و رایانش ابری[3] محقق می‌شوند. در این مدل، اینترنت اشیا داده‌های دستگاه‌های مختلف را جمع‌آوری کرده و این پلتفرم‌ها هستند که داده‌ها را تحلیل نموده و اطلاعات عملیاتی را برای رفع نیازهای خاص در زمان واقعی ارائه می‌کنند (Yuan, 2020: Online). هدف نهایی این فناوری، فراهم آوردن زیرساخت فناوری اطلاعات امن و قابل اعتماد برای ارتباط اشیا و پل زدن بین جهان مجازی و فیزیکی و بازنمایی دیجیتال آن در سیستم‌های اطلاعاتی است (Weber & Weber, 2010: 1).

تحقیقات در زمینه اشیای هوشمند و اینترنت اشیا، به بیش از دو دهه قبل باز می‌گردد و خاستگاه آن را می‌توان در آراء اولیه مارک وایزر[4] در مورد رایانش فراگیر جست‌وجو کرد. بروس استرلینگ[5] نیز ایده اشیای هوشمند و اینترنت اشیا را عمومی‌سازی کرده است؛ وی اصطلاح «اسپایم[6]» را برای توصیف طبقه‌جدیدی از اشیای فضازمانی ابداع کرد که از قابلیت آگاهی از محیط برخوردار بوده و توانایی ضبط رویدادهای جهان واقعی را دارا می‌باشند. به موازت این ایده، جولیان بلچر[7] نیز در «بیانیه اشیای متصل به شبکه»، مفهوم مشابهی تحت عنوان «بلاگجکت[8]» معرفی کرد که به اشیایی اشاره دارد که قادر به تولید محتوی و نگارش بلاک هستند. این آثار آینده‌نگرانه مبنایی برای حجم روزافزون پژوهش‌های کاربردی و فناورانه در زمینهٔ فرکانس رادیویی، اشیا و محصولات هوشمند فراهم آورده‌اند (Kortuem et al, 2010: 49). با این حال، این اصطلاح برای نخستین بار در سال ۱۹۹۹ از سوی «کوین اشتون[9]»، کارشناس فناوری اطلاعات بریتانیایی تبار و مدیر اجرایی شرکت «پروکتر اند گمبل»، به منصه ظهور رسید و بنیان‌های عصر جدیدی از تعاملات ماشینی را پی‌ریزی کرد. وی با استفاده از برچسب‌های «شناسایی فرکانس‌های (امواج) رادیویی»، زنجیره تأمین مبتنی بر اینترنت اشیا را بازطراحی کرد و بر نوآوری تجاری با هدف امکان شمارش و ردیابی خودکار اجسام بدون دخالت انسان تأکید کرد (Schoenberger, 2002: Online). در این پارادایم، هر شیء حتی اشیای بی‌جان هویت دیجیتالی خواهد داشت و رایانه‌ها قادر به سازماندهی و مدیریت آنها خواهند بود (Ferguson, 2016: 813).

---

1. Online Oxford Learners Dictunary: Under the entry of innernet of Things(IoT).
2. Artificial Intelligence
3. Cloud Computing

4. Mark Weiser
5. Bruce Sterling
6. Spime (Space & Time)
7. Julian Bleeker
8. Blogjects (objects that blog)
9. Kevin Ashton: The term “IoT” has been “invented” by Kevin Ashton in a presentation in 1998.

۲. ارکان و کارکرد

به طور کلی، اینترنت اشیا مشتمل بر شبکه‌ای از موجودیت‌های ناهمگون بوده که بر اساس الگوهای ارتباطی انسان با انسان[1]، انسان با شیء[2] شیء با شیء[3] و شیء با اشیا[4] در تماس هستند (Manzo, 2018: 5). در این وادی، برنامه‌ها به دو دسته اصلی نرم‌افزارهای نهفته[5] و غیرنهفته[6] تقسیم می‌شوند. نرم‌افزارهای نهفته به طور خاص و سفارشی برای یک سخت‌افزار معین (مانند یک تراشه یا ریزپردازنده) طراحی شده‌اند و به طور دائم در حافظه آن سخت‌افزار جاسازی می‌شوند. عملکرد این نرم‌افزارها به شدت به سخت‌افزار وابسته است و معمولاً وظایف خاص و محدودی را انجام می‌دهند. به‌عنوان نمونه، سیستم عامل داخلی یک یخچال هوشمند، یا نرم‌افزار کنترل موتور در خودروهای مدرن. در مقابل، نرم‌افزارهای غیرنهفته مستقل از سخت‌افزارهای خاص عمل می‌کنند و عموماً بر روی سکوهای عمومی و استاندارد (مانند سیستم عامل‌های ویندوز یا لینوکس) اجرا می‌شوند. در این زمینه می‌توان به یک اپلیکیشن موبایل برای کنترل لوازم خانگی، یک نرم‌افزار تحلیل کلان داده‌های کلان که روی یک سرور ابری اجرا می‌شود یا یک پلتفرم مدیریت مرکزی دستگاه‌های اینترنت اشیا در یک شهر هوشمند اشاره کرد (Oliveira et al, 2020: 146). بر این اساس، چارچوب فنی اینترنت اشیا بر سه رکن اصلی استوار است:

سخت‌افزار و دستگاه‌های هوشمند: این قسمت که هسته اصلی سیستم را تشکیل می‌دهد، شامل تجهیزات و حسگرهایی است که در خط مقدم تعامل با محیط فیزیکی قرار دارند. حسگرها وظیفه اندازه‌گیری پارامترهای مختلف مانند دما، فشار، موقعیت‌یابی و ضربان قلب را بر عهده دارند. در مقابل، کنشگرها با دریافت دستورات دیجیتال، اقدام به اعمال تغییرات فیزیکی در محیط می‌کنند؛ نمونه‌هایی از این اقدامات شامل باز و بسته کردن قفل، روشن و خاموش کردن موتورها یا تنظیم جریان شیر آب است. افزون بر این، پردازنده‌ها و محرک‌ها نیز از دیگر اجزای حیاتی این مجموعه به شمار می‌روند (Fan & Zhou, 2011: 532).

پروتکل‌ها و زیرساخت‌های ارتباطی: این بخش امکان تعامل بین دستگاه‌ها را از طریق فناوری‌هایی همچون سامانه بازشناسی با امواج رادیویی[7] و ارتباط میدان نزدیک[8] فراهم می‌کند.

سامانه‌های پردازش و تحلیل داده: این رکن متکی بر پیشرفت‌های نوینی مانند رایانش ابری[9] و هوش مصنوعی است که توانایی ذخیره‌سازی، پردازش و تحلیل حجم عظیمی از داده‌های تولیدشده را دارد. در حالی که روش‌های سنتی برای مدیریت این داده‌ها ناتوان هستند، الگوریتم‌های یادگیری ماشین این چالش را مرتفع می‌سازند (Kortuem et al, 2010: 44; Jacques, 2020: 6).

گفتنی است که در مقوله ارتباط ماشین با ماشین به عنوان مصداق نوین اینترنت اشیا، داده‌ها در مرحله اول جمع‌آوری شده و سپس به فضای ابری انتقال می‌یابند تا مورد پردازش قرار گیرند. سرورهای مبتنی بر رایانش ابری قادرند حجم عظیمی از داده‌های تولیدشده توسط دستگاه‌های متصل را ذخیره و تحلیل نمایند. نتیجه این فرایند، استخراج الگوها، شناسایی روندها و کشف ناهنجاری‌ها است که در نهایت می‌تواند منجر به بهبود عملیات، ارتقاء عملکرد و اتخاذ تصمیم‌گیری‌های اثربخش‌تر شود (Farkas, 2017: 6).

کاربرد این فناوری در مقیاس‌های مختلفی متجلی شده است. در مقیاس خرد از دستگاه‌های پوشیدنی مانند ساعت‌های هوشمند، تلفن‌های همراه، سطل‌های زباله متصل و قفسه‌های

---

1. Human-to-Human (H2H).
2. Human-to-Thing (H2T).
3. Thing-to-Thing (T2T).
4. Thing-to-Things (T2Ts).
5. Embedded Software
6. Nonembedded Software

۷. شناسایی با فرکانس رادیویی (Radio Frequency Identification (RFID)) عبارت است از استفاده بی‌سیم از امواج برای انتقال داده‌ها که سرعت بسیار بالایی دارد. برچسب‌گذاری کالاهای مختلف توسط داده به کاربران امکان می‌دهد موجودی و دارایی‌های خود را به‌طور خودکار و منحصربه‌فرد شناسایی و ردیابی کنند.

۸. ارتباط میدان‌نزدیک (Near Field Communication (NFC)) مجموعه‌ای از پروتکل‌های ارتباطی است که برای برقراری ارتباط بین دو دستگاه الکترونیکی در فاصله‌ای بسیار کوتاه (حداکثر ۴ سانتی‌متر یا ۱٫۵ اینچ) طراحی شده‌اند. این فناوری با ایجاد یک اتصال کم‌سرعت و ساده، اغلب به عنوان یک کلید راه‌انداز برای برپایی ارتباطات بی‌سیم پایدارتر و پرتوان‌تر (مانند وای‌فای یا بلوتوث) مورد استفاده قرار می‌گیرد.

۹. رایانش ابری مدلی از ارائه خدمات رایانشی است که بر پایهٔ شبکه‌های کامپیوتری مانند اینترنت بنا شده است. این مدل، الگویی نوین برای عرضه، مصرف و تحویل سرویس‌های مختلف شامل زیرساخت، نرم‌افزار، پلتفرم و سایر منابع را از طریق شبکه فراهم می‌کند. نام «رایانش ابری» از ترکیب دو واژهٔ «رایانش» و «ابـر» تشکیل شده است.

دارویی مجهز گرفته تا استفاده در مصادیق کلان نظیر شهرهای هوشمند[1] وسایل نقلیه خودران[2] سیستم‌های کنترل صنعتی و پهپادهای بدون سرنشین را شامل می‌شوند (Gertner, 2014: Online). زمینه‌های کاربردی این فناوری نیز تقریباً نامحدود است و موضوعاتی همچون مراقبت بهداشتی (از جمله دستگاه‌های پایش سلامت، قرص‌های هوشمند و ایمپلنت‌ها)، کشاورزی (نظارت بر رطوبت خاک، رشد محصولات و مدیریت آبیاری)، لجستیک (خلق صنایع جدید، بهبود کارایی و ارائه قابلیت سفارش‌سازی)، کسب و کار (تحلیل رفتار مشتریان، مدیریت سطح موجودی و بهینه‌سازی زنجیره تأمین) را در برگیرد (Rens, 2019: 6). این فراگیری برخی از محققان را بر آن داشته تا تعبیر «اینترنت همه چیز»[3] را برای معرفی آینده این تکنولوژی به کار گیرند (Thierer, 2015: 7).

کلان‌داده‌های اینترنت اشیا و چالش‌های حمایت از آنها در نظام حقوق مالکیت فکری

اینترنت اشیا از طریق یکپارچه‌سازی داده‌های فیزیکی و دیجیتال، به‌طور ذاتی با تولید کلان‌داده‌ها عجین شده است (سعادتی و مهرشاد، ۱۳۹۶: ۱۸). از این رو، کلان‌داده‌ها به‌عنوان هسته پردازشی و محصول اصلی اینترنت اشیا، در تقاطع با حقوق مالکیت فکری قرار می‌گیرند. با این حال، ماهیت پیچیده، پویا و ناملموس این داده‌ها و نیز روش‌های پردازش آنها، نظام‌های سنتی حمایت از مالکیت فکری را با چالش‌های بنیادین مواجه ساخته است. در این مجال، ضمن تحلیل حقوقی کلان‌داده‌های ناشی از اینترنت اشیا، به چالش‌های حمایت از آنها در رژیم حقوق مالکیت فکری می‌پردازیم.

۱. کلان‌داده‌های مرتبط با اینترنت اشیا و تمایز آنها از سایر مصادیق

در یک نگاه، کلان‌داده‌ها صرفاً به معنای حجم عظیمی از اطلاعات نیستند، بلکه به قابلیت گردآوری، پردازش و تحلیل مجموعه‌های بسیار بزرگ و متنوعی از داده‌ها اشاره دارند که از منابع گوناگون و با سرعت بالا تولید می‌شوند و غالباً ارزش آن با گذشت زمان تغییر می‌کند (Banterle, 2016: 19). این مفهوم عموماً با سه ویژگی اصلی حجم[4] تنوع[5] و سرعت[6] شناخته می‌شود. تنوع به معنی چندشکلی بودن داده‌ها از نظر قالب و منبع است که می‌توانند از پلتفرم‌ها و کاربران مختلف گردآوری شوند. سرعت نیز نه‌تنها به تولید پرشتاب داده‌ها، بلکه به ضرورت پردازش و تحلیل سریع آنها اشاره دارد؛ چرا که در غیر این صورت، داده‌ها بخش عمده‌ای از ارزش و تأثیرگذاری خود را از دست می‌دهند (رهبری، ۱۴۰۱: ۲۹۷). در برخی از دیدگاه‌های پیشرفته‌تر، دو ویژگی صحت[7] و ارزش[8] نیز به فهرست معیارهای تعریف کلان‌داده اضافه شده و مدل V5 را شکل داده‌اند. بر این اساس، اکوسیستم کلان‌داده متشکل از قابلیت‌های محاسباتی، الگوریتم‌ها و نرم‌افزارهای پیشرفته‌ای است که امکان مدیریت و تحلیل این حجم عظیم از داده‌های گوناگون و پویا را فراهم می‌کنند (Lubyová, 2018: 1-2). این ویژگی‌ها به‌ویژه در زمینه اینترنت اشیا اهمیت دوچندان می‌یابند؛ چرا که داده‌های تولیدشده توسط حسگرها و دستگاه‌های متصل، بسیار حجیم، متنوع و نیازمند پردازش بلادرنگ هستند و حمایت از توسعه فناوری‌های کلان‌داده، زیرساخت ضروری برای بهره‌برداری کامل از قابلیت‌های اینترنت اشیا به‌شمار می‌رود.

بنا به مراتب بالا، ممکن است این پرسش پیچیده مطرح شود که علت تمرکز بر کلان‌داده‌های ناشی از اینترنت اشیا چیست و وجه تمایز آن با کلان‌داده‌های سایر فناوری‌ها و از جمله هوش مصنوعی کدام است؟ در پاسخ باید اذعان داشت که برجسته‌ترین دلیل برای موضوعیت بخشیدن به اینترنت اشیا، خاستگاه کاملاً متمایز داده‌های تولیدشده در آن است. برخلاف هوش مصنوعی که غالباً به عنوان یک «ابزار پردازش» داده‌های موجود را تحلیل، استنتاج یا خلق می‌کند، اینترنت اشیا در جایگاه یک «منبع زایش اولیه» داده‌هایی را مستقیماً از دل جهان فیزیکی استخراج می‌نماید. این داده‌ها، «امضای دیجیتال» رویدادها و حالت‌های عینی هستند: از نوسان دمای یک توربین صنعتی و الگوی حرکت یک خودروی خودران گرفته تا ریتم فیزیولوژیک بدن یک بیمار.

---

1. Smart Cities
2. Self-driving Cars
3. Internet of Everything (IoE)

---

4. Volume
5. Variety
6. Velocity
7. Veracity
8. Value

بنابراین، دادهٔ برآمده از آن، صرفاً یک «عدد» دیجیتال نیست، بلکه بازنمایی دیجیتالی بی‌واسطه یک واقعیت فیزیکی است.

همچنین، یکی از تمایزات کلان داده‌های اینترنت اشیا با مصادیق مشابه مانند کلان‌داده‌های هوش مصنوعی، ساختار پیچیده و توزیع‌شده زنجیره ارزش آن است. وانگهی، نوآوری در این فناوری اغلب در قالب «نرم‌افزارهای نهفته» در درون یک شیء فیزیکی (از یخچال تا تراشه صنعتی) متجلی می‌شود. هوش مصنوعی به‌طور معمول به عنوان یک نرم‌افزار مستقل (غیرنهفته) تجلی می‌یابد و این مسئله حاد را ندارد. یک سیستم هوش مصنوعی ممکن است در یک محیط نسبتاً بسته (با مالک الگوریتم، داده‌ها و نتایج مشخص) عمل کند، اما در اینترنت اشیا، چرخه حیات داده از شبکه‌ای درهم‌تنیده از ذی‌نفعان عبور می‌کند: سازنده سخت‌افزار، برنامه‌نویس نرم‌افزار نهفته، اپراتور شبکه، ارائه‌دهنده پلتفرم ابری، تحلیلگر داده و در نهایت، کاربر نهایی. هر یک از این بازیگران ممکن است ادعایی نسبت به بخشی از داده یا ارزش افزودهٔ حاصل از آن داشته باشند. بر این اساس، تعیین «مالک اصلی» یک اختراع در اکوسیستم اینترنت اشیا که حاصل مشارکت دستگاه‌های خودمختار و سرویس‌های متعدد است، دشوار می‌باشد. همچنین، احتمال «نقض مشترک» پتنت هنگامی که یک فرایند بین چندین کنشگر مستقل تقسیم شده، از مسائل ویژه این حوزه است. مضافاً، هستی اینترنت اشیا بر پایه توانایی ارتباط بی‌درنگ اشیا با یکدیگر است. این امر آن را به شدت وابسته به پروتکل‌ها، قالب‌های داده و استانداردهای فنی می‌سازد. حفاظت از این استانداردها در قالب کپی‌رایت یا حق اختراع (Hamza & Pradana, 2022: 3-5)، می‌تواند به عاملی برای انحصار یا مانعی برای هم‌کاری‌پذیری تبدیل شود. این دغدغه در مرکز توجه حقوق مالکیت فکریِ اینترنت اشیا قرار دارد، حال آنکه برای یک مدل هوش مصنوعی ممکن است حاشیه‌ای باشد.

به هر روی، حوزه کلان‌داده، پدیده پیشرو و در حال ظهور در قلمرو اینترنت اشیا است. هرچند این پدیده با موضوعات مربوط به عناصر مالکیت داده‌های شخصی در اینترنت اشیا نیز بی‌ارتباط نیست (Janeček, 2018: 9)، اما تمرکز غالب پژوهش‌ها در این زمینه بر ارائه راه‌حل‌های امنیتی و فنی بوده است و ابعاد حقوقی، اجتماعی و مربوط به حکمرانی داده که مستقیماً به حریم خصوصی افراد می‌پردازد، کمتر مورد توجه قرار گرفته است. به همین ترتیب، سؤالاتی چون «داده‌های شخصی کاربران کجا ذخیره خواهد شد؟»، «چه کسی این داده‌ها را مدیریت می‌کند؟» و اینکه «چه نوع اقدامات امنیتی لازم است تا به کار گرفته شود؟» و اساساً «آیا می‌توان چنین سیستم هوشمندی را منطبق با قوانین حریم خصوصی دانست؟» ذهن فعالان این عرصه را به خود درگیر کرده است (Fabiano, 2017: 3). پاسخ به این پرسش‌ها به مدل طراحی استفاده‌شده در مرحله مقدماتی توسعه بستگی دارد. با این وجود، در ادبیات حقوقی، دو دیدگاه غالب وجود دارد: دیدگاهی که بر حق مالکیت مصرف‌کننده بر داده‌های شخصی خود تأکید دارد (مانند رویکرد مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا[1]) و دیدگاهی که با استناد به قراردادهای کاربری، حقوق را به ارائه‌دهندگان خدمت واگذار می‌کند. نگارنده با اتخاذ دیدگاه اول، فرض را بر این می‌گذارد که مصرف‌کنندگان باید از حق مالکیت فکری بر داده‌های تولیدشده توسط خویش برخوردار باشند.

با استناد به دلایل فوق، می‌توان نتیجه گرفت که اینترنت اشیا صرفاً یک «طریق» یا ابزار خنثی برای تولید کلان‌داده نیست. این فناوری یک «ساختار فنی–اجتماعی» پیچیده با ویژگی‌های ذاتیِ تولید داده، معماری چندلایه و تجلی فیزیکی است که مسائل حقوق مالکیت فکری را در قالبی منحصربه‌فرد و چندبعدی طرح می‌نماید. تمرکز این پژوهش بر «اینترنت اشیا» به‌طور عام و بر «کلان‌داده‌های تولیدشده در این فضا» به‌طور خاص، ناظر بر همین واقعیت است. در حالی که هوش مصنوعی می‌تواند به عنوان یکی از ابزارهای قدرتمند پردازش داده‌های اینترنت اشیا ظاهر شود، منبع، ماهیت، چرخه حیات و چارچوب‌های حقوقی حاکم بر خودِ داده‌های خام و زیرساخت تولیدکننده آن، ریشه در پارادایم اینترنت اشیا دارد.

۲. چالش‌های حمایت از کلان‌داده‌های ناشی از اینترنت اشیا در رژیم حقوق مالکیت فکری

پیدایش حجم انبوهی از داده‌ها در بستر اینترنت اشیا، نظام حقوق مالکیت فکری را با پرسش‌ها و چالش‌های بنیادین مواجه ساخته است. ماهیت حقوقی این داده‌ها و تعیین جایگاه آنان در منظومه مالکیت فکری، مستلزم عبور از تحلیلی

1. The General Data Protection Regulation (GDPR) (EU) 2016/679

ساده‌انگارانه و تشریح مراحل مختلف چرخه حیات داده، از تولید و پردازش تا بهره‌برداری، می‌باشد.

گفتنی است که داده‌های خام اولیه که مستقیماً و بدون دخالت خلاقانه انسانی از حسگرها و دستگاه‌های اینترنت اشیا گردآوری می‌شوند، عمدتاً در زمره «امور واقع» طبقه‌بندی می‌گردند. بر اساس آموزه‌های کلاسیک مالکیت فکری، این دسته از داده‌ها فاقد مؤلفه‌های ضروری برای حمایت، همچون «اصالت» در حقوق مؤلف یا «شرایط ثبت» در نظام اختراع هستند؛ چرا که حاصل یک فرایند اکتشافی (کشف امر موجود) محسوب شده و به‌عنوان یک «بیان» خاص قلمداد نمی‌گردند (عطار، ۱۴۰۴: ۵). این ویژگی، به همراه «رقابت‌ناپذیری»[1] و «انحصارناپذیری»[2]، باعث می‌شود داده‌های خام از خصلت «کالای عمومی»[3] برخوردار باشند (Manzo, 2018: 6-11).

با این همه، صحنه کلان‌داده‌های اینترنت اشیا منحصر به داده‌های خام نیست. سرمایه‌گذاری‌های عظیم و پردازش‌های مبتکرانه‌ای که بر روی این داده‌ها صورت می‌پذیرد، خود می‌تواند موجد دارایی‌های فکری کاملاً جدید و مستحقی برای حمایت باشد. این فرایند تبدیل، می‌تواند در قالب‌های متنوعی همچون پایگاه‌های داده غنی و ساختاریافته، الگوریتم‌های پردازشی نوآورانه، خروجی‌های خلاقانه مانند مدل‌های آموزش‌دیده هوش مصنوعی، و نیز طرح‌های ساختاری در سخت‌افزارهای هوشمند متبلور گردد (Anwar Yelukar & Siddhi Vijay, 2023: 303). این مصادیق، اگرچه از داده‌های خام منشأ می‌گیرند، اما به دلیل دربرگرفتن سرمایه، تلاش فکری و ابتکار بشری، واجد شرایط لازم برای تحت‌الحمایه قرار گرفتن در یکی از قالب‌های مالکیت فکری می‌باشند.

به دلیل ارزش اقتصادی فوق‌العاده کلان‌داده‌ها و محدودیت‌های قالب‌های سنتی، حمایت از آنان در عمل اغلب متکی بر چارچوب‌های حقوقی جایگزین یا مکمل می‌باشد. این چارچوب‌ها شامل «حقوق قراردادها» (برای تعیین شرایط استفاده از طریق موافقت‌نامه‌ها)، «قوانین حفاظت از داده‌ها»، «رژیم اسرار تجاری» (برای داده‌هایی که محرمانه نگه داشته می‌شوند) و «حقوق رقابت» می‌گردد. با این حال، اعمال این چارچوب‌ها نیز در محیط اینترنت اشیا به دور از اشکال نیست. برای مثال می‌توان عدم کنترل مؤثر کاربران بر داده‌های شخصی خود، عدم تقارن اطلاعاتی فاحش بین ارائه‌دهندگان خدمات و کاربران، ابهام در کیفیت و شرایط اخذ رضایت آگاهانه، مسائل حقوقی ناشی از استفاده از داده‌های استنتاجی، تغییر هدف از جمع‌آوری اولیه داده‌ها و کاستی‌ها و محدودیت‌های فنی در روش‌های ناشناس‌سازی را ذکر کرد (Noto La .Diega & Sappa, 2020: 8). بدیهی است که مسائلی از این دست به‌طور تصاعدی سطح مخاطراتی چون دسترسی غیرمجاز، سرقت و سوءاستفاده از داده‌ها را افزایش دهند.

جایگاه مصادیق حقوق مالکیت فکری در حفاظت از کلان‌داده‌های اینترنت اشیا

برخی از پژوهشگران به امکان‌سنجی حمایت از اینترنت اشیا در حیطه حقوق مالکیت فکری پرداخته‌اند. به اذعان آنها در تسرّی نظام حمایتی مالکیت فکری بر حوزه اینترنت اشیا می‌بایست بین دو بعد ملموس و ناملموس این گزاره قائل به تفکیک شد (Aggarwal & Verma, 2020: 134). ابعاد ناملموس اینترنت اشیا (یعنی داده‌ها) قابلیت انطباق با قالب‌های حقوقی نظیر کپی‌رایت، حق اختراع و اسرار تجاری را دارند و ابعاد ملموس آن را می‌توان در بستر تأسیسات حقوقی نظیر علامت تجاری و طرح صنعتی مورد حمایت قرار داد[4] (Oliveira et al, 2020: 146; Vohra & Mehta, 2021: 67). این نوشتار با تکیه بر ابعاد نامشهود در تلاش است تا بایسته‌ها حفاظت از داده‌ها را در پرتو این مصادیق بررسی کند.

۱. نظام کپی‌رایت

کپی‌رایت به مجموعه‌ای از حقوق انحصاری ناشی از تکثیر، توزیع، اجرا، نمایش، حق اجرای عمومی و بهره‌برداری مادی از

1. Non-rivalry
2. Non-excludability
3. Public Goods

۴. بررسی حمایت از ابعاد ملموس اینترنت اشیا در بستر علامت تجاری نشان می‌دهد که اگرچه ثبت علائم سه‌بعدی به طور نظری ممکن است، اما در عمل موانع ماهوی جدی وجود دارد. برای نمونه، شکل این محصولات معمولاً به عنوان نشانه تشخیص منشأ تجاری تلقی نمی‌گردد. از این‌رو، طرح صنعتی که مختص حمایت از ویژگی‌های ظاهری و زیبایی‌شناختی است، راهکار مناسب‌تری محسوب می‌شود. در صورت ثبت طرح صنعتی، دارنده حق می‌تواند از استفاده تجاری دیگران جلوگیری کند، اما این حق شامل استفاده‌های شخصی و غیرتجاری نخواهد شد.

آثار ادبی–هنری اشاره دارد که متعلق به پدیدآورنده یا خالق یک اثر اصیل است. در پرتو اصل حمایت‌ناپذیری ایده‌ها، صرفاً از ایده‌هایی که نمود عینی و تجسم خارجی یافته‌اند، حمایت به عمل می‌آید. به دیگر سخن، اصل موسوم به «دوگانگی ایده و بیان»[1] از اصول مسلم کپی‌رایت است که بر حمایت‌پذیری آثار اصیلی که ابراز (بیان) شده‌اند تمرکز دارد. بدین ترتیب، ایده‌ها، رویه‌ها، روش‌های عملیاتی و داده‌های خام[2] به خودی خود مشمول حمایت کپی‌رایت نمی‌شوند. به دیگر سخن، کپی‌رایت نسبت به «فرایندها» و «روش‌ها» حق انحصاری ایجاد نمی‌کند و حوزه حمایت این حق، صرفاً به «خروجی»ها و «آثار» نهایی ناشی از به‌کارگیری آن روش‌ها محدود می‌شود (Mishchenkom, 2016: 90). سؤالی که در اینجا مطرح می‌شود این است که آیا نظام کپی‌رایت قابلیت اعمال و حمایت از الگوریتم‌ها و کلان‌داده‌های اینترنت اشیا را دارد؟

چتر حمایتی کپی‌رایت به محض خلق یک اثر، به طور خودکار فعال می‌شود. این مکانیسم اگرچه دارای مزایای زیادی برای خالقان اثر است،[3] اما در محدوده دیجیتال و به ویژه داده‌ها، با پیچیدگی‌ها و چالش‌های منحصر به فردی روبه‌رو است. بر اساس معاهدات بین‌المللی مانند «کنوانسیون برن» و قوانین ملی اکثر کشورها (از جمله قانون حمایت از حقوق مؤلفان و مصنفان و هنرمندان ایران مصوب ۱۳۴۸)، یک اثر برای برخورداری از حمایت کپی‌رایت باید «اصیل» باشد. اصالت معمولاً به معنای «آفرینش مستقل مؤلف» و «دارای حداقلی از خلاقیت» است. از همین رو، داده‌های خام اینترنت اشیا (مثلاً دمای ثبت‌شده توسط یک سنسور، میزان تپش قلب از یک ساعت هوشمند، یا موقعیت جغرافیایی یک خودرو) فاقد این خلاقیت هستند. این داده‌ها عمدتاً محصول فرعی عملکرد حسگرها و دستگاه‌های متصل و نه بیان ذهنی و قصد هنری یک پدیدآورنده هستند. به تعبیر دیگر، آنها صرفاً «کشف» و «ثبت» یک واقعیت عینی توسط یک ماشین هستند و به‌تنهایی واجد شرایط لازم برای حمایت کپی‌رایت نمی‌باشند. افزون بر این، در محیط اینترنت اشیا، که داده‌ها اغلب به صورت خودکار و بر اساس پارامترهای از پیش تعریف شده گردآوری می‌شوند، احراز اصالت به دلیل فقدان عنصر خلاقیت انسانی که از ناحیه پدیدآورنده و شخص حقیقی میسر است، بسیار دشوار خواهد بود (شاکری، ۱۴۰۴: ۴۴). در مقابل، اگر داده‌ها در قالب خاصی «گزینش» یا «چینش» شوند به گونه‌ای که این گزینش و چینش حاوی خلاقیت و ابتکار باشد (مانند یک پایگاه داده)، آنگاه آن «ساختار» یا «قالب» پایگاه داده می‌تواند به عنوان یک اثر مستقل مشمول کپی‌رایت شود (Noto La Diega, 2023: 307). هرچند این سنسورها و الگوریتم‌ها هستند که بدون دخالت مستقیم و مداوم انسان، داده تولید می‌کنند، لیکن در خصوص نتایج حاصل از تحلیل کلان داده‌ها، الگوریتم‌های پیش‌بینی‌کننده و نمودارهای پیچیده، خروجی‌های تحلیلی و بصری‌سازی‌ها[4] باید اذعان کرد که چنانچه حاصل خلاقیت و اصالت باشند، به طور قطع مشمول حمایت کپی‌رایت خواهند بود. در این دیدگاه، نظام حقوقی کپی‌رایت می‌تواند در مواجهه با قالب‌های پیام، رابطها، پروتکل‌ها و سایر استانداردهای رایج که لزوم ارائه داده‌ها در قالبی مشخص را در دنیای کلان‌داده‌ها ایجاب می‌کنند، قابل استناد باشد (Hamza & Pradana, 2022: 4). با وجود این، سؤال دیگری که به ذهن خطور می‌کند این است که آیا یک ماشین می‌تواند «مؤلف» باشد؟ پاسخ فعلی حقوق اکثر نظام‌ها «خیر» است. در این انگاره، بر اساس تئوری «کارمند–کارفرما»[5] گفته شده است که انتساب اثر به شخصی که ماشین را برنامه‌ریزی، راه‌اندازی و مدیریت می‌کند، می‌تواند منصفانه باشد؛ یعنی مالک دستگاه اینترنت اشیا یا ارائه‌دهنده سرویس می‌تواند به عنوان صاحب حقوق شناخته شود، اما این نیز در مواردی که داده‌ها از تعامل چندین دستگاه و سرویس مختلف حاصل می‌شوند، به پیچیدگی منتهی می‌شود. اتحادیه اروپا برای حل این مشکل، حق خاصی به نام «پایگاه‌داده» تمهید کرده است. این حق مستقل از کپی‌رایت، از سرمایه‌گذاری قابل‌توجه (مالی، زمانی یا نیروی انسانی) در تهیه، تأیید و ارائه محتوای یک پایگاه داده حمایت می‌کند، حتی اگر محتوای آن فاقد خلاقیت باشد (Lu, 2020: 2). این مدل می‌تواند برای داده‌های حاصل از اینترنت اشیا بسیار مناسب باشد؛ زیرا تأکید آن بر «سرمایه‌گذاری» است، نه «خلاقیت». مالک یک شبکه

1. The Idea–Expression Dichotomy
2. Raw Data
۳. مزیت کلیدی اتکا به کپی‌رایت برای کلان‌داده‌های اینترنت اشیا، این است که حمایت مستلزم افشای الگوریتم‌های پردازش، منطق حاکم بر سنسورها یا متدولوژی‌های ترکیب داده‌های ناهمگون نیست. در نتیجه، می‌توان استنتاج کرد که نظام کپی‌رایت، مانع از شفاف‌سازی عملیات پیچیده اینترنت اشیا می‌شود.
4. Analytical Outputs & Visualizations
5. Work Made for Hire

بزرگ سنسورها می‌تواند با استناد به این حق، دیگران را از استخراج و استفاده مجدد بی‌اجازه از حجم عظیم داده‌هایش منع کند.

۲. نظام حق اختراع

نظام حق اختراع، با اعطای حق انحصاری موقت به مخترعان، نقش بسزایی در تحریک و تشویق نوآوری در عرصه فناوری‌های پیشرفته ایفا می‌نماید. با این حال، تطبیق چارچوب سنتی این نظام با پدیده‌های نوظهور فناورانه، از جمله «اینترنت اشیا»، مستلزم واکاوی دقیق مبانی نظری و حدود و ثغور شمول قواعد موجود است.

الف) شرایط حمایت

بر پایه اسناد بین‌المللی (همچون موافقت‌نامه تریپس) و قوانین ملی اکثر کشورها و از جمله قانون حمایت از مالکیت صنعتی ایران مصوب ۱۴۰۳، یک اختراع برای برخورداری از حمایت، باید واجد سه معیار ماهوی جدید بودن[1] (یعنی، عدم افشای پیشین)، دارا بودن گام ابتکاری[2] (بدین معنا که اختراع برای شخصی که در آن فن دارای مهارت معمولی است، بدیهی نباشد) و قابلیت کاربرد صنعتی[3] باشد (ماده ۱۲).

اینترنت اشیا، با تولید انبوه و پیوسته داده‌ها، پرسش‌های بنیادینی را در برابر نظام حق اختراع مطرح ساخته است. بر اساس یک اصل مسلّم در حقوق اختراعات، «ایده‌های انتزاعی»، «روش‌های ریاضی محض» و «الگوریتم‌های پایه» به‌خودی‌خود خارج از دایره موضوعات قابل ثبت محسوب می‌گردند (ماده ۴ قانون حمایت از مالکیت صنعتی ایران). از این‌رو، هسته‌های پردازشی و الگوریتم‌های ریاضی صرف که در تحلیل کلان‌داده‌های اینترنت اشیا به کار می‌روند، عموماً فاقد شرایط حمایت از طریق حق اختراع تشخیص داده می‌شوند (Jacques, 2020: 6; Althabhawi et al, 2025: 458). به‌علاوه، داده‌های خام تولیدشده توسط حسگرها و دستگاه‌های اینترنت اشیا (مانند رقم ثبت‌شده دمای هوا توسط یک سنسور) در مقام «کشف» یا «واقعیت طبیعی» قرار دارند و فاقد هرگونه «گام ابتکاری» هستند؛ در نتیجه به‌طور مستقیم تحت شمول حمایت‌های حق اختراع قرار نمی‌گیرند. افزون بر این، با توجه به تولید مداوم و خودکار این داده‌ها، شرط «جدید بودن» نیز در مواجهه با حجم عظیم و فزاینده «دانش پیشین» –که خود حاصل پردازش همین کلان‌داده‌هاست– به دشواری قابل احراز است (Campanile et al, 2025: 503). مضافاً اینکه، با گسترش کمّی داده‌ها، حجم دانش پیشین نیز با شتابی بی‌سابقه در حال فزونی است. برآوردها گواه این است که نرخ رشد تعداد اختراعات که به دشواری هر دو دهه دو برابر می‌شود، در برابر سرعت تصاعدی تولید دانش پیشین که ظرف تنها یک تا یک و نیم سال دوچندان می‌گردد، قادر به رقابت و تقابل نیست. این شکاف روزافزون، کارآمدی نظام کنونی اختراع را به پرسش کشیده و اعطای حق اختراع را در این مسیر با موانع ساختاری مواجه ساخته است (حبیبا و نبوی، ۱۴۰۳: ۲۶۹).

نقطه عطف تغییر نگرش، زمانی است که یک الگوریتم یا روش ریاضی، نه به‌صورت مجرد، بلکه در قالب بخشی از یک فرایند فناورانه خاص به کار گرفته شده و منجر به دستیابی به نتیجه ملموس، نوآورانه و فنی گردد. در چنین مواردی، حمایت نه از خود الگوریتم انتزاعی، بلکه به «کاربرد فنی» آن در حل یک مشکل مشخص اعطا می‌شود (Noto La Diega, 2017: 176). برای نمونه، «روش بهینه‌سازی مصرف انرژی در یک شبکه حسگر با بهره‌گیری از یک الگوریتم اختصاصی یادگیری ماشین، که به افزایش قابل‌ملاحظه طول عمر باتری‌ها منجر می‌گردد»، قابلیت ثبت به‌عنوان اختراع را داراست (Greenberg, 2020: 344). در رویه قضایی برخی نظام‌های حقوقی، از جمله ایالات متحده آمریکا، چارچوب‌های دقیق‌تری برای تشخیص حمایت‌پذیری ادعاهای نرم‌افزاری و الگوریتمی تبیین شده است. به‌عنوان مثال، در پرونده «شرکت آلیس»[4] دادگاه عالی آمریکا رویکردی سختگیرانه را اتخاذ کرد که بر اساس آن، ادعاهای مرتبط تنها در صورتی قابل پذیرش هستند که متضمن «ایده انتزاعی» نبوده یا در صورت انتزاعی بودن، واجد «گام ابتکاری» باشند؛ به این معنا که عناصری افزوده شوند که ادعا را به‌طور قابل‌ملاحظه‌ای فراتر از آن ایده انتزاعی اولیه قرار دهد (Harmon, 2015: 2355).

بنابراین، در مواجهه با داده‌های اینترنت اشیا، نظام حق اختراع بایست مرز میان «داده خام» (به‌عنوان یک کشف غیرقابل حمایت) و «فرایندها، سیستم‌ها و روش‌های فنی

1. Novelty
2. Inventive Step (Non-obviousness)
3. Industrial Applicability

4. Alice Corp. v. CLS Bank International (2014).

پردازش و تحلیل این داده‌ها» (به‌عنوان یک اختراع بالقوه) را به وضوح ترسیم نماید. آینده حمایت از نوآوری‌های این حوزه، در گرو تدوین ادعاهای اختراعی است که بر کاربردهای فنی ملموس و غیربدیهیِ حاصل از پردازش داده‌ها تأکید دارند.

ب) بایسته‌های حکمرانی

به منظور غلبه بر این چالش‌های پیش‌گفته، سه راهبرد کلیدی از سوی صاحب‌نظران این عرصه پیشنهاد شده است. نخست، توصیف عینی و دقیق ادعاهای مفاهیم اختراعی در اظهارنامه ثبت اختراع که با شفاف‌سازی دامنه حمایت، از بروز تفسیرهای نادرست و در نتیجه عدم انطباق جلوگیری می‌کند. دوم، نگارش استراتژیک ادعاها به منظور پرهیز از چالش‌های نقض مشترک که از طریق تحدید داوطلبانه قلمرو ادعاها، تطابق دقیق‌تری بین مفهوم ثبت‌شده و کاربرد عملی اختراع ایجاد می‌نماید. سوم، بهره‌گیری از مکانیسم‌های نوین نظیر بازبینی پس از اعطا توسط نهادهای متولی ثبت اختراع و حقوق مالکیت صنعتی که با اعمال استانداردهای کیفی فزون‌تر، به اصلاح پتنت‌های فاقد انطباق می‌پردازد (Robinson, 2015: 659). در این راستا، قانون اختراعات آمریکا مصوب ۲۰۱۱، به اداره ثبت اختراع اجازه داده است تا رویکردهایی را با هدف ارتقای کیفیت حقوق انحصاری اعطایی به کار بندد. این مکانیسم‌ها شامل «بازبینی بین‌الطرفین»[1]، «بازبینی پس از اعطا»[2] و «بازبینی روش‌های تجاری تحت پوشش»[3] هستند. این رویه‌ها بدون تردید نه تنها برای به چالش کشیدن شرایط احراز حق اختراع حاوی اینترنت اشیا، بلکه برای به تردید انداختن دامنه آنها نیز مورد توجه قرار می‌گیرند (Robinson, 2015: 660).

با این همه، مشوق‌های انحصاری ناشی از ثبت اختراع، انگیزه لازم را برای پردازشگران کلان‌داده به منظور ثبت فرایندهای پردازشی فراهم نمی‌آورد. فرایند طولانی و پرهزینه ثبت اختراع در تقابلی ذاتی با چرخه عمر کوتاه فناوری‌های دیجیتال قرار می‌گیرد؛ به‌گونه‌ای که یک روش پردازش، غالباً پیش از اخذ گواهی، منسوخ گشته و ارزش اقتصادی خود را از دست می‌دهد. به‌علاوه، افشای عمومی جزئیات فنی در اظهارنامه اختراع که ماهیتی ذاتی دارد، می‌تواند مخاطرات امنیتی و حقوقی قابل‌توجهی را به همراه داشته باشد. این افشاسازی نه‌تنها امکان نقض حریم خصوصی داده‌های شخصی موجود در پایگاه‌های داده را افزایش می‌دهد، بلکه زمینه سوءاستفاده و مهندسی معکوس توسط رقبا و ناقضان حق را نیز فراهم می‌سازد.

با توجه به سرشت ذاتاً تعاملی فناوری اینترنت اشیا، بازیگران متعدد و حتی دستگاه‌های خودمختار، در خلق داده و ابداعات مرتبط نقش‌آفرینی می‌کنند. این واقعیت، تعیین «مالک اصلی» برای ثبت اختراع را با چالش‌های جدی مواجه ساخته و ضرورت بازنگری در چارچوب‌های حقوقی موجود را عیان می‌سازد. برای حل این موضوع، توسعه دکترین «مخترع مشترک»[4] به گونه‌ای که مشارکت‌های غیرمتمرکز و پلتفرم‌محور را دربرگیرد و نیز تعریف معیارهای شفاف برای «سهم اساسی» پیشنهاد شده است (England & Murphy, 2014). از منظر دیگر، آنچه فناوری اینترنت اشیا را به‌صورت ویژه تهدید می‌کند، وجود بازیگران متعدد در فرایند شکل‌گیری حق اختراع است. در این راستا، ممکن است شرایطی پدیدار گردد که در آن فعالیت‌های چندین طرف مستقل، به نقض احتمالی یک پتنت واحد بینجامد. در چنین بستری، مسئولیت حقوقی اشخاص ثالث عمدتاً در چارچوب مفاهیم «تحریک به نقض»[5] و «نقض مشارکتی»[6] مندرج در قوانین پتنت مورد تحلیل قرار می‌گیرد. همچنین، «نقض مشترک»[7] به عنوان یک رویکرد متعارض، این امکان حقوقی را می‌سنجد که آیا در مواردی که اجرای یک روش بین چند کنشگر تقسیم شده است، می‌توان مسئولیت نقض را به آنها منتسب کرد؟ بر اساس رویه جاری دادگاه‌های فدرال آمریکا[8]، تحقق این مسئولیت منوط به تسلط جامع یک طرف واحد بر کل فرایند و روش است، به‌گونه‌ای که تمامی مراحل آن به وی قابل انتساب باشد. احراز معیار دشوار «کنترل یا هدایت» در رویه قضایی آمریکا، موجب شده است تا دارندگان پتنت‌های اینترنت اشیا در موقعیت حقوقی مطلوب‌تری قرار گیرند که

1. Inter Partes Review
2. Post Grant Review
3. Covered Business Methods Review

4. Joint Inventorship
5. The Patent Statute's Inducement
6. Contributory Infringement
7. Joint infringement
8. BMC Res., Inc. v. Paymentech, LP, 498 F.3d 1373, 1381 (Fed. Cir. 2007), overruled by Akamai Techs., Inc. v. Limelight Networks, Inc., 692 F.3d 1301 (Fed. Cir. 2012).

بتوانند بدون اتکا به نظریه نقض مشترک به اعمال حقوق خود مبادرت ورزند (Robinson, 2015: 668).

۳. نظام اسرار تجاری

الف) شرایط حمایت

ماهیت حمایت از اسرار تجاری، در تقابل با مبانی بنیادین حقوق مالکیت فکری قرار دارد که بر «افشای اطلاعات در ازای اعطای حقوق انحصاری» استوار است. حمایت در بستر این تأسیس حقوقی مستلزم آن است که مالک، خود اقدامات حفاظتی ضروری را برای جلوگیری از انتشار آن به کار بندد. در حالی که نظام‌های کپی‌رایت و حق اختراع به عنوان ابزارهای سنتی مالکیت فکری اغلب در کانون توجه حمایت از فناوری‌های نوین قرار می‌گیرند، اسرار تجاری به عنوان یک مکانیسم حقوقی انعطاف‌پذیر و قدرتمند، نقشی بی‌بدیل در حفاظت از دارایی‌های ناملموس در عرصه اینترنت اشیا و به‌ویژه کلان داده‌های حاصل از آن ایفا می‌کند.

همان‌طور که بارها گفته شد، اینترنت اشیا بر پایه گردآوری، انتقال، پردازش و تحلیل حجم عظیمی از داده‌ها بنا شده است. ارزش رقابتی شرکت‌ها در این فضا نه تنها در مالکیت بر داده‌ها، بلکه در توانایی استخراج اطلاعات و ارائه راه‌حل‌های هوشمندانه از طریق الگوریتم‌های اختصاصی، مدل‌های یادگیری ماشین و متدولوژی‌های تحلیلی تأثیرگذار است (López-Tarruella, 2016: 662). چنین داده‌هایی، به‌ویژه هنگامی که متضمن الگوریتم‌های تشکیل‌دهنده معماری و زیرساختی هستند، از ارزش اقتصادی فوق‌العاده‌ای برخوردارند. به‌طوری که بخش قابل‌توجهی از آن مستقیماً از ماهیت محرمانه و غیرعلنی این داده‌ها و الگوریتم‌ها سرچشمه می‌گیرد. بدین ترتیب، اسرار تجاری با سه ضابطه «محرمانه بودن»[1]، دارا بودن «ارزش اقتصادی»[2] و به‌کارگیری «اقدامات معقول»[3] برای حفظ محرمانگی، چارچوبی ایده‌آل برای محافظت از چنین دارایی‌هایی را فراهم می‌کنند (Gervais, 2019: 19). الگوریتم‌ها و کد منبع، مدل‌های تحلیلی و روش‌های کسب‌وکار، فرمول‌ها و دستورالعمل‌ها، روش‌ها و فرایندها، داده‌های خام و پردازش‌شده و استراتژی‌های بازارگردانی و داده‌های غیر پیش‌پاافتاده که خروجی فرایندهای بین ماشینی هستند از جمله طیف گسترده‌ای از مصادیقی می‌باشند که در حوزه اینترنت اشیا و کلان‌داده‌ها می‌توانند از مزایای حمایت اسرار تجاری بهره‌مند شوند (Holbrook, & Janis, 2018: 167).

ناگفته نماند که حفاظت از داده‌های تولیدشده از سوی اینترنت اشیا از طریق نظام اسرار تجاری، در مقایسه با مکانیسم حق اختراع، از مزایای زیادی برخوردار است. برخلاف حق اختراع که مستلزم افشای کامل دانش فنی است، اسرار تجاری هیچ اهرم الزام‌آور مبتنی بر افشا ندارند. همچنین، حمایت از اسرار تجاری مستلزم ثبت، پرداخت هزینه‌های دوره‌ای یا گذراندن مراحل ارزیابی نیست. این حمایت تا زمانی که اطلاعات محرمانه در انحصار دارنده آن باقی بماند و برای عموم افشا نشود، به‌صورت نامحدود تداوم خواهد یافت. با این حساب، اگرچه اسرار تجاری عموماً در چارچوب «قواعد خودتنظیمی»[4] مبتنی بر هنجارهای اجتماعی و حقوق قراردادها مورد حمایت قرار می‌گیرند و مراجع قضایی نیز به دعاوی مربوط به نقض آنها رسیدگی می‌کنند، اما اعمال این قالب حمایتی برای کلان‌داده‌های حاصل از اینترنت اشیا، دچار چالش‌های جدی خواهد بود. این رویکرد نه تنها دسترسی آزاد به داده‌ها را محدود می‌سازد، بلکه با ماهیت پویا و سیّال کلان‌داده‌ها نیز در تضاد قرار می‌گیرد. از دیگر نقاط ضعف اتکا به این سازوکار، عدم ایجاد حق انحصاری و وجود ریسک دائمی افشا است که می‌تواند از طرق مختلفی از قبیل حملات سایبری، سوءرفتار کارکنان، یا حتی مهندسی معکوس محقق شود. شایان توجه است که اطلاعات تجسم‌یافته در یک «شیء» فیزیکی به‌واسطه دسترسی اشخاص ثالث و امکان مهندسی معکوس، فاقد وصف محرمانگی می‌باشد. به‌رغم این دیدگاه، رویه قضایی آمریکا، رویگردان از این نظر، الگوریتم‌های تعبیه‌شده در «اشیا» را در پوشش اسرار تجاری مورد حمایت قرار داده است. در پرونده «فولکس واگن علیه گارسیا»[5]، دادگاه با صدور قرار تأمین، از افشای الگوریتمی که در یک ریزتراشه خودرو جاسازی شده بود، ممانعت به عمل آورد؛ حال آنکه خواندگان از طریق مهندسی معکوس یک برنامه کامپیوتری، به اطلاعات آن دست پیدا کرده بودند. بنابراین، اگرچه از منظر تئوریک می‌توان در خصوص قابلیت اعمال وصف تجاری محرمانه بر الگوریتم‌ها و داده‌های ماشینی

1. Secrecy
2. Commercial Value
3. Reasonable Steps
4. Self Regulation
5. Volkswagen v Garcia

اینترنت اشیا تردید نمود، اما از جنبه عملی، باید این واقعیت را مدنظر قرار داد که شرکت‌های فعال در این عرصه، این اطلاعات را محرمانه نگه می‌دارند و همین امر سهم بسزایی در خلق ارزش اقتصادی آنها دارد (Noto La Diega, Guido, 2023: 309-311).

مضاف بر اینها، در صورت نقض محرمانگی، اثبات ادعای نقض اسرار تجاری در مراجع قضایی فرایندی پیچیده و پرهزینه است؛ چرا که مستلزم ارائه‌ی مدارکی مستدل در خصوص مخفی بودن اطلاعات و همچنین کفایت اقدامات حفاظتی انجام‌شده می‌باشد. از جنبهٔ تجاری نیز، ارزش یک سرّ تجاری به‌طور ذاتی به استمرار محرمانگی آن گره خورده است. این ویژگی، واگذاری یا اعطای مجوز بهره‌برداری از آن را در مقایسه با حق اختراع، به مراتب حساس‌تر و پیچیده‌تر می‌سازد. نهایتاً، در بستر اینترنت اشیا، محرمانه نگه‌داشتن پروتکل‌های ارتباطی و استانداردهای فنی می‌تواند به عنوان یک مانع فنی عمل کرده و قابلیت همکاری و تعامل بی‌درنگ بین دستگاه‌ها و پلتفرم‌های ساخت تولیدکنندگان مختلف را مختل سازد (Sandeen, 2018: 210).

ب) بایسته‌های حمایت

به هر تقدیر، به منظور اعمال نظام حفاظت از اسرار تجاری بر کلان‌داده‌ها، ابتدا باید امکان احراز مالکیت بر این داده‌ها به‌صورت قانونی محقق گردد. یکی از بایسته‌های حمایت در این عرصه، تدوین چارچوب‌های حقوقی و سازوکارهای فنی برای مواجهه با چالش‌های ویژه این حوزه، از جمله مسئله مالکیت داده‌های تولیدشده توسط اشیای متصل و تعیین حدود مسئولیت در زنجیره تأمین چندلایه است. قابل تأمل آنکه در اکثر نظام‌های حقوقی مدرن، از جمله موافقت‌نامه تریپس، یکی از ارکان اساسی بهره‌مندی از حمایت اسرار تجاری، برخورداری دارنده از «حق قانونی» برای اعمال کنترل بر اطلاعات محرمانه است. این حق قانونی عمدتاً ریشه در مفاهیمی چون مالکیت یا وضعیت مسلط بر داده دارد (Banterle, 2016: 15). بر این اساس، هر یک از بازیگران عرصه فناوری اعم از کاربران، تولیدکنندگان سخت‌افزار یا ارائه‌دهندگان پلتفرم می‌توانند مشمول چنین حقی گردند.

شایان توجه است که در بسیاری از نظام‌های حقوقی، به‌ویژه در اتحادیه اروپا، تأکید اصلی نه بر مالکیت مطلق بر داده، بلکه بر «حق دسترسی و بهره‌برداری» از آن معطوف گشته است (Holbrook, & Janis, 2018: 168-169). از این منظر، حتی در صورت عدم احراز مالکیت مطلق بر داده‌ها، اشخاصی نظیر تولیدکنندگان پلتفرم یا پردازشگران داده، به واسطه سرمایه‌گذاری انجام‌شده، خلق ارزش افزوده و اعمال تدابیر حفاظتی متناسب، واجد حق قانونی برای کنترل و حفظ محرمانگی داده‌های پردازش‌شده خواهند بود. این حق قانونی می‌تواند مبنای مناسبی برای شناسایی و حمایت از داده به‌عنوان سرّ تجاری قلمداد گردد. در این میان، تمایز نهادن میان «داده‌های خام» و «داده‌های پردازش‌شده، تجمیع‌شده یا مشتق‌شده» حائز اهمیت است. در مورد داده‌های خام، مقوله مالکیت عمدتاً در هاله‌ای از ابهام باقی می‌ماند؛ حال آنکه در خصوص کلان‌داده‌های حاصل از پردازش و تحلیل، امکان بهره‌مندی از حمایت در قالب نهاد اسرار تجاری تقویت می‌یابد. با این همه، هرگاه شخص بتواند اثبات نماید که به‌رغم نامشخص بودن مالکیت داده، رفتاری معطوف به حفاظت و اعمال کنترل محرمانه بر اطلاعات داشته، احتمال وصول به حمایت قضایی برای وی فزونی می‌یابد.

بحث و نتیجه‌گیری

پدیده اینترنت اشیا، با ایجاد زیرساختی گسترده و بهم‌پیوسته، حجم انبوه و بی‌سابقه‌ای از داده‌ها را تولید می‌کند که در اقتصاد دیجیتال معاصر، به‌مثابه سرمایه‌ای راهبردی و ارزش‌آفرین تلقی می‌گردند. کلان‌داده‌های حاصل از این اکوسیستم، با اتکا بر ویژگی‌های «حجم»، «سرعت» و «تنوع»، پارادایم‌های سنتی حقوق مالکیت فکری را با چالش‌های نوظهور و پیچیده‌ای مواجه ساخته‌اند. این پژوهش نشان می‌دهد که سه رکن اصلی حمایتی، یعنی نظام کپی‌رایت، حق اختراع و اسرار تجاری، هر یک به‌شکلی ناقص و ناتمام در پوشش دادن به این دارایی‌های داده‌بنیان عمل می‌کنند. ماهیت بین‌رشته‌ای و چندبعدی این داده‌ها، ضرورت بازاندیشی در مبانی نظری و تدوین یک چارچوب حقوقی جامع و پیش‌بینی‌گر را ایجاب می‌نماید.

با عنایت به کاستی‌های شناسایی‌شده در نظام‌های سنتی مالکیت فکری، که دیگر پاسخگوی پیچیدگی‌های فناوری‌های نوظهور مانند اینترنت اشیا و کلان‌داده‌ها نیستند، بایسته‌های جدیدی برای قانون‌گذاری در این حوزه پیشنهاد می‌گردد. نخستین و اساسی‌ترین رهیافت، اتخاذ یک رویکرد تلفیقی و چندلایه است؛ چرا که حمایت مؤثر از دارایی‌های فکری در این

حوزه نه در قالب یک راه‌حل واحد، بلکه در پرتو چارچوبی ترکیبی قابل تحقق است. در این الگو، هر یک از ابزارهای مالکیت فکری نقش مکمل ایفا می‌کنند: حق اختراع از ایده‌ها و فرایندهای نوآورانه حفاظت می‌کند؛ حقوق پدیدآورنده به حمایت از بیان، قالب‌بندی و ساختارهای خاص داده‌ها و نرم‌افزارها می‌پردازد و اسرار تجاری از جنبه محرمانگی و ارزش اقتصادی ناشی از عدم افشای داده‌ها و الگوریتم‌ها صیانت می‌کند.

در کنار این چارچوب تلفیقی، تعادل‌بخشی بین نوآوری و دسترسی به عنوان یک اصل راهبردی ضروری است. یک چارچوب حقوقی نوین باید در یک توازن منطقی، میان تحریک انگیزه‌های نوآوری برای بازیگران اصلی و تضمین دسترسی عادلانه سایر ذی‌نفعان به داده‌ها عمل نماید. این تعادل حیاتی می‌تواند از طریق مکانیسم‌هایی هوشمندانه مانند الزام به افشای محدود داده‌های غیرحساس برای اهداف پژوهشی یا تعریف مجوزهای اجباری در مواردی که انحصار منجر به زیان عمومی می‌شود، محقق گردد. همزمان، توسعه مکانیسم‌های حکمرانی داده امری اجتناب‌ناپذیر است. مدیریت چرخه عمر داده‌ها، از تولید تا مصرف و انهدام، مستلزم به‌کارگیری ترکیبی از ابزارهای نظارتی است که می‌تواند شامل مقررات خودتنظیمی صنعتی، استانداردهای امنیتی سخت‌گیرانه و الگوهای منعطف حکمرانی داده باشد.

سرانجام، برای فائق آمدن بر چالش‌های پویا و سریع‌التغییر این فضا، نهادینه‌سازی سازوکارهای نظارتی چابک یک ضرورت انکارناپذیر است. این امر مستلزم ایجاد نهادهای ناظر تخصصی و بهره‌گیری از نهادهای حقوقی نوین است. نهادهایی مانند «رویه‌های بهینه بازبینی پس از اعطای پتنت» می‌توانند با فراهم آوردن امکان بازبینی سریع و کارآمد اعتبار اختراعات ثبت‌شده، از قفل شدن نوآوری در دام انحصارهای نامشروع جلوگیری کرده و پاسخگویی نظام حقوقی را در برابر تحولات شتابان فناوری تضمین نمایند. در مجموع، این بایسته‌ها در کنار یکدیگر، بنیان یک نظام مالکیت فکری پویا، عادلانه و کارآمد را برای حوزه اینترنت اشیا و کلان‌داده‌ها پی می‌ریزند. در نتیجه، دستاورد اصلی این تحقیق تأکید بر ناکارآمدی راه‌حل‌های انحصاری و لزوم حرکت به سمت یک «نظام خاص و مستقل[1]» است که مبتنی بر رویکردی تلفیقی عمل می‌کند. چنین نظامی با به رسمیت شناختن همزمان نقش مکمل نهادهای سنتی و ضرورت ایجاد ساز و کارهای جدید حکمرانی داده، قادر خواهد بود به‌طور همزمان ابعاد فنی، اقتصادی و حقوقی کلان‌داده‌های ناشی از اینترنت اشیا را پوشش دهد و به‌عنوان الگویی کاربردی و بومی‌پذیر برای تقنین در حوزه حمایت از ابداعات اینترنت اشیا در حقوق داخلی ایران نیز مورد توجه قرار گیرد.

References

Aggarwal, P., & Verma, R. (2020). "Intellectual property challenges in the era of the Internet of Things". *Journal of Intellectual Property Rights*, 25(2), 134-147.

Althabhawi, Nabeel M. & et al. (2025). "Application of Patent Law to Software in the IoT Context". *Sriwijaya Law Review*, 9(2), 457-479.

Ansari, Bagher & Attar, Sima. (2022). "Data Protection in China; A Comparative Study of the Data Protection Approach in the United States and the European Union". *Comparative Law Review*, 13(1), 91-113, (In Pesian).

Anwar Yelukar, Adv. Sadaf & Siddhi Vijay, Sawant. (2023). "The Impact of the Internet of Things (IoT) on Intellectual Property Law". *International Journal of Emerging Technologies and Innovative Research* (IJETIR), 3(11). ISSN (Online): 2583-0554.

Attar, Shima. (2025). "Uncertainty in the Concept of Data Ownership". *Journal of Legal Research*, Accepted Manuscript, 1-18, (In Pesian).

Banterle, Francesco. (2016). The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database Sui generis Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis: In book: Personal Data in

1. Sui generis System

Competition, Consumer Protection and Intellectual Property Law.

Bello, Oladayo & Zeadally, Sherali. (2014). "Intelligent Device-to-Device Communication in the Internet of Things". *IEEE SYSTEMS JOURNAL* 1, available at: http://syslog.co.in/files/eciot/Intelligent%20Device-to Device%20Communication.pdf

Campanile, Lelio & et al. (2025). *An AI-Driven Methodology for Patent Evaluation in the IoT Sector: Assessing Relevance and Future Impact*. Paper published under CC license (CC BY-NC-ND 4.0), In Proceedings of the 10th International Conference on Internet of Things, Big Data and Security (IoTBDS 2025), 501-508.

De Araujo, J.H., at al. (2020). "Smart cities: A prospective study on Internet of Things (IoT) applied to the urban mobility sector (In Portuguese)". *Prospect*. Notebooks, 13: 138-153.

England, Paul & Murphy, Kathleen. (2014). *Patent Issues and the Internet of Things*, TAYLORWESSING (Feb. 2014), http://www.taylorwessing.com/download/article_patent_iot.html.

Fabiano, Nicola. (2017). *The Internet of Things Ecosystem: The Blockchain and Privacy Issues*. The Challenge for a Global Privacy Standard, 978-1-5386-2064-9/17/$31.00 IEEE, 1-7.

Fan, Peng-fei & Zhou, Guang-zhao. (2011). *Analysis of the Business Model Innovation of the Technology of Internet of Things in Postal Logistics*, IEEE 532.

Farkas, Thomas, J. (2017). Data Created by the Internet of Things: The New Gold Without Ownership? (August 1, 2017). REVISTA LA PROPIEDAD INMATERIAL; No. 23; Enero–Junio 2017, Available at SSRN: https://ssrn.com/abstract=3012155

Farhadkhani, Zeinab & et al. (2023). "Civil Liability of IoT Manufacturer and Service Provider; A Comparative Study in the Laws of the European Union, the United States and Iran". *Civil Law Knowledge Journal*, 12(23), 1-18, (In Pesian).

Ferguson, Andrew Guthrie. (2016). "The Internet of Things and the Fourth Amendment of Effects". *California Law Review*, 104(4), 805-880.

Gertner, Jon. (2014). *Behind GE's Vision for the Industrial Internet of Things*. FAST COMPANY (June 18, 2014), http://www.fastcompany.com/3031272/can-jeff-immelt-really-make-the-world-1-better.

Gervais, Daniel J. (2019). "Exploring the Interfaces Between Big Data and Intellectual Property Law". *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 10(3), Available at: https://scholarship.law.vanderbilt.edu/faculty-publications/1095.

Greenberg, Anastasia. (2020). Protecting Virtual Things: Patentability of Artificial Intellhgence Technology for the Internet of Things, The Law Review of the Franklin Pierce Center for Intellectual Property IDEA, 60(2).

Habiba, Saeed & Nabavi, Maryam. (2025). "Protection of Intellectual Property Rights of Big Data". *Journal of Research and Development in Public Law*, 1(2).

Hamza, Rafik & Pradana, Hilmil. (2022). "A Survey of Intellectual Property Rights Protection in Big Data Applications". *Algorithms Journal*, 1-15. https://doi.org/10.3390/a15110418

Harmon, Daniel E. (2015). "Patents in the Balance? IP Analysts Continue to Ponder Alice Ramifications". *LAW*, PC

1, 32(12).

Heer, Tobias, et al. (2011). Security Challenges in the IP-Based Internet of Things, Authors Suppressed Due to Excessive Length, Wireless Personal Communications, 61(3).

Holbrook, T. R., & Janis, M. D. (2018). "The Internet of Things and Trade Secrecy". *Harvard Journal of Law & Technology*, 32(1), 167-220.

Jacques, Sabine. (2020). Patenting Algorithms in an Internet of Things and Artificial Intelligence World: Pathways to Harmonizing the Patentable Subject Matters and Evaluation of the Novelty Requirement: Patenting AI: Rethinking Eligible Subject-Matters and the Novelty Requirement in an IoT world. Japanese Institute of Intellectual Property.

Janeček, Václav. (2018). "Ownership of personal data in the Internet of Things". *Forthcoming in the Computer Law & Security Review* (ELSEVIER Ltd.). 1-22. https://doi.org/10.1016/j.clsr.2018.04.007

Kiaei, Farkhondeh. (2023). "Developments Arising from the Internet of Things in Administrative Law and the Realization of Smart Governance". *Administrative Law Quarterly*, 11(36), 72-91. (In Pesian).

Kortuem, Gerd et al. (2010). *Smart Objects as Building Blocks for the Internet of Things*, IEEE 30, 44 (Frederic Thiesse & Florian Michahelles eds., Jan./Feb. 2010), http://www.fahim-kawsar.net/papers/Kortuem.IEEEInternet2010.Camera.pdf.

López-Tarruella, A. (2016). "The Protection of Trade Secrets in the Age of Big Data". *IIC- International Review of Intellectual Property and Competition Law*, 47(6), 662-688.

Lu, Meng. (2020). "Intellectual Property Protection of Big Data". *Journal of Physics: Conference Series*, CISAI 2020, 1-5.

Lubyová, Linda Holková. (2018). *Big Data in the EU Competition Law*. Charles University Law Faculty, Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3128400, p. 1.

Manzo, Valentina. (2018). The Internet of Things and Intellectual Property rights: the protection of data, NIVERSITY OF TURIN - LAW SCHOOL, INTERNATIONAL LABOUR ORGANIZATION WIPO ACADEMY, LL.M. IN INTELLECTUAL PROPERTY.

Mishchenkom, Lidiya. (2016). The Internet of Things: Where Privacy and Copyright Collide, Santa Clara High Tech. L.J., 33, Available at: http://digitalcommons.law.scu.edu/chtlj/vol33/iss1/1

Moeinifar, Mohaddeseh & Vahidzadeh, Delaram. (2022). "Requirements for Exercising the Right to Privacy in the Field of Internet of Things in Iran's law". *Modern Technology Law*, 3(6), pp. 61-75. (In Pesian).

Noto La Diega, Guido. (2017). *Software Patents and the Internet of Things in Europe, the United States and India*. European Intellectual Property Review, 39, Thomson Reuters (Professional) UK Limited and Contributors

Noto La Diega, 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, Revue européenne de droit de la consommation / European Journal of Consumer Law*, 3, 419-458

Noto La Diega, Guido. (2023). The Internet of Things (You Don't Own) under Bourgeois Law: An Integrated Tactic to Rebalance Intellectual Property, Chapter

6 in Guido Noto La Diega, Internet of Things and the Law: Legal Strategies for Consumer-Centric Smart Technologies (Routeldge 2022) 275-340, Available at SSRN: https://ssrn.com/abstract=4240975.

Oliveira, Sergio Silva, et al. (2020). "Intellectual Property and the Internet of Things: A Bibliometric Search". *Int. Business Manage*, 14(4), 145-156.

Peppet, Scott R. (2014). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, TEX. L. REV., 85.

Rahbari, Ebrahim. (2022). "The Analysis of Big data Challenges for Competition Law". *Legal Research Quarterly*, 25(98), 295-320 (In Pesian).

Rens, Andrew. (2019). "Who Is in Charge Here? The Internet of Thing, Governance and The Global Intellectual Property Regime". *UCLA Journal of Law & Technology*, 23(2).

Robinson, W. Keith. (2015). "Patent Law Challenges for the Internet of Things". *Wake Forest J. Bus. & Intell. Prop. L*., Vol.15. 655-670.

Rose, Karen, Eldridge, Scott & Chapin, Lyman. (2015). *The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World, The Internet Society (ISOC).* licensed under the Creative Commons Attribution/NonCommercial/ShareAlike 4.0 Unported, Available at: https://www.internetsociety.org/iot

Saadati, Zeinab & Mehrshad, Batool. (2017). "The Internet of Things and big data Applications in Sustainable Smart Cities". *Science and Technology Policy Quarterly*, 7(3), 17-30 (In Pesian).

Sadeghi, Hossein & Naser, Mahdi. (2020). "Providing a legal framework for accountability in the operation of "Internet of Things" tools in the context of e-government". *Iranian Journal of Public Policy*, 6(3), 81-103, (In Persian).

Schoenberger, Chana R. (2002). The Internet of Things, FORBES (Mar. 18, 2002, 12:00 AM), https://www.forbes.com/global/2002/0318/092.html#33f75a713c3e.

Shakeri, Zahra. (2025). "The Literary and Artistic Property Law System in the Age of Artificial Intelligence; Considerations for Policymaking in Future Governance". *Iranian Journal of Public Policy*, 11(1), 41-55. (In Pesian).

Thierer, A. (2015). "The Internet of Things and Wearable Technology Addressing Privacy and Security Concerns without Derailing Innovation". *Richmond Journal of Law & Technology*, 21, 1-118.

Tusikov, Natasha. (2019). Precarious Ownership of the Internet of Things in the Age of Data, B. Haggart et al. (eds.), Information, Technology and Control in a Changing World, International Political Economy Series, https://doi.org/10.1007/978-3-030-14540-8_6

Vohra, N., & Mehta, S. (2021). "The Impact of IoT on Trademark Law: An Indian perspective". *Journal of Indian Law and Society*, 13(2), 67-79.

Weber, Rolf H. & Weber, Romana. (2010). Internet of Things: Legal Perspectives, Springer Heidelberg Dordrecht London New York. Copyright © Schulthess Juristische Medien AG, Zurich – Basel – Geneva 2010. DOI 10.1007/978-3-642-11710-7_1.

Yuan, Q., (2020). Research on new technology of power system automation based on ubiquitous Internet of Things technology. IOP Conf. Ser. Earth Environ. Sci., 440, DOI:10.1088/1755-1315/440/3/032101.