Journal Website

Article history:
Received 27 May 2026
Revised 12 September 2026
Accepted 19 September 2026
Initial Publication 06 November 2026
Final Publication 22 December 2027

Dynamic Management and Business Analysis

Volume 6, Issue 5, pp 1-25

E-ISSN: 3041-8933

Assessing the Role of Data Governance in Managing Legal Risks and Combating Privacy Violations in Digital Businesses

Salam. Hadi Jasem[1], Reza. Nikkhah[2*], Siamak. Jafarzadeh[2]

[1] PhD Student in Private Law, Urmia University, Urmia, Iran
[2] Associate Professor, Department of Islamic Jurisprudence and Law, Faculty of Literature and Humanities, Urmia University, Urmia, Iran

*** Corresponding author email address**: r.nikkhah@urmia.ac.ir

A r t i c l e I n f o

Article type:
Original Research

How to cite this article:
Hadi Jasem, S., Nikkhah, R., & Jafarzadeh, S. (2027). Assessing the Role of Data Governance in Managing Legal Risks and Combating Privacy Violations in Digital Businesses. *Dynamic Management and Business Analysis*, *6*(5), 1-25.
https://doi.org/10.61838/dmbaj.524

© 2027 the author(s). Published by Knowledge Management Scientific Association. This is an open access article under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) License.

A B S T R A C T

Objective: This study aimed to assess the role of data governance in managing legal risks and combating privacy violations in digital businesses in Tehran.

Methodology: This applied study employed a quantitative, cross-sectional, descriptive-correlational design. The study population consisted of managers, specialists, and professionals working in digital businesses in Tehran in the fields of data management, information technology, information security, legal affairs, compliance, and risk management. The final sample included 384 participants selected through purposive and convenience sampling. Data were collected using a structured questionnaire measuring three main constructs: data governance, legal risk management, and combating privacy violations. The validity and reliability of the measurement model were assessed using factor loadings, Cronbach's alpha, composite reliability, and average variance extracted. Data were analyzed using SPSS version 29 and SmartPLS version 4 through Pearson correlation, structural equation modeling, and bootstrapping procedures.

Findings: Data governance had a significant positive effect on legal risk management ($\beta = 0.692$, $t = 16.878$, $p < 0.001$). It also had a significant direct effect on combating privacy violations ($\beta = 0.529$, $t = 11.021$, $p < 0.001$). Legal risk management significantly predicted combating privacy violations ($\beta = 0.287$, $t = 5.519$, $p < 0.001$). The indirect effect of data governance on combating privacy violations through legal risk management was 0.199 and statistically significant ($t = 5.237$, $p < 0.001$), confirming partial mediation. The R^2 values were 0.479 for legal risk management and 0.598 for combating privacy violations, while the SRMR value was 0.057.

Conclusion: The findings indicate that data governance is a strategic mechanism for reducing legal risks and strengthening privacy protection in digital businesses, with part of its effect operating through improved legal risk management. Integrating data governance, legal compliance, information security, and organizational accountability can therefore enhance personal-data protection and reduce organizational legal exposure.

Keywords: *Data Governance; Legal Risk Management; Privacy; Digital Businesses; Data Protection; Legal Compliance*

EXTENDED ABSTRACT

Introduction

The rapid expansion of digital businesses, platform-based services, artificial intelligence, big-data analytics, cloud computing, digital banking, e-commerce, and algorithmic decision-making has fundamentally transformed the role of data in contemporary organizations. Data are no longer merely operational by-products; rather, they constitute strategic assets that support customer profiling, personalization, innovation, risk assessment, market forecasting, and value creation. At the same time, the increasing dependence of organizations on personal, behavioral, financial, transactional, and biometric data has intensified concerns regarding privacy, accountability, regulatory compliance, and legal liability. Recent research suggests that data can enhance firm value when organizations operate within effective privacy and regulatory frameworks, indicating that data protection and economic value creation should not necessarily be regarded as conflicting objectives (Yan & Cai, 2026). Consequently, data governance has become a central organizational mechanism for determining how data are collected, classified, accessed, processed, shared, retained, and deleted.

The legal complexity of data governance is particularly evident in digital businesses operating across multiple regulatory environments. Digital data flows frequently cross organizational and national boundaries, while privacy regulations remain jurisdiction-specific and may impose different or overlapping obligations. The coexistence of local privacy laws within a globalized digital economy therefore creates significant compliance challenges for organizations that collect and process data across jurisdictions (Sharma et al., 2026). Similar challenges have emerged in relation to artificial intelligence, where large-scale data use raises questions regarding provenance, quality, consent, ownership, access control, accountability, and lawful processing. Effective AI data governance has consequently been identified as a fundamental requirement for reducing the legal, ethical, and technical risks associated with large language models and other data-intensive AI applications (Pahune et al., 2025). Moreover, voluntary ethical commitments alone may be insufficient when they are not accompanied by enforceable accountability, monitoring, and governance mechanisms (Haidar, 2026).

A major challenge for contemporary digital businesses is therefore to maintain a workable balance between commercial data utilization and the protection of consumer rights. AI-driven services, online lending, digital marketing, behavioral profiling, and personalized services increasingly depend on extensive datasets, yet such practices may create risks of excessive data collection, secondary use, inadequate consent, opaque profiling, and unauthorized disclosure. Research concerning the relationship between AI data use and consumer rights emphasizes the need for governance mechanisms that reconcile technological innovation with privacy protection and accountability (Vásquez & Alvarez-Orozco, 2026). Similarly, research in plural legal contexts indicates that privacy cannot be understood solely through formal legal rules; contextual expectations, informational norms, and institutional arrangements also shape what constitutes legitimate data use (Kadiri & Boamah, 2025).

These issues are particularly important in digitally mediated financial and commercial services. Studies of online loan services have shown that uncontrolled collection and use of personal information may expose consumers to substantial privacy risks (Ramadhan et al., 2024; Widi et al., 2021). In digital banking, personal data protection has similarly become a core component of responsible governance

because financial institutions process highly sensitive identity, transaction, and behavioral information (Yuspin et al., 2023). E-commerce and social media environments also create complex relationships between organizational interests, advertising practices, information use, consumer protection, and individual privacy (Akbar et al., 2023; Mujtaba & Cavico, 2023). Accordingly, business law increasingly plays a central role in ensuring transparency, accountability, consumer protection, and legal remedies in digital markets (Widiarty & Tehupeiory, 2024).

Data governance is also closely connected with cybersecurity and organizational risk management. Security breaches can generate not only technical disruptions but also contractual disputes, regulatory penalties, reputational damage, and civil liability. Comparative research on cybersecurity policies demonstrates that effective organizational responses require integrated policies that clearly define responsibilities, security controls, and incident-response procedures (Mishra et al., 2022). Similarly, studies of smart-city environments indicate that data security and privacy are strengthened when compliance requirements are incorporated into technical and managerial systems rather than treated as separate legal obligations (Aslam et al., 2022). Enterprise architecture research further demonstrates that legal requirements can be translated into operational roles, processes, controls, and data-flow mechanisms, thereby enhancing organizational capacity to comply with data-protection requirements in complex information environments (Georgiadis & Poels, 2021).

Another important dimension concerns data sharing across organizational boundaries. Industrial privacy frameworks emphasize that privacy risks frequently arise not only within an organization but also through data exchange with business partners, vendors, cloud providers, and other third parties (Ghorashi et al., 2023). Stakeholder-based analyses likewise indicate that effective protection of data rights depends on the interaction among organizations, users, regulators, and other actors whose incentives and responsibilities may differ (Li & Guo, 2023). In this context, co-regulation and industry participation can complement governmental regulation by developing sector-specific standards and monitoring mechanisms (Suleiman et al., 2022). The concept of reasonable expectations of privacy is also relevant because the legitimacy of data processing depends partly on the purpose, context, and expectations under which information is disclosed and used (Shen & Teng, 2022).

The need for integrated data governance is increasingly evident in highly sensitive domains such as health, biometric identification, tourism, and public administration. The use of AI chatbots in health-related services, for example, raises important issues concerning confidentiality, data storage, access, developer responsibility, and compliance with health-information requirements (Rezaeikhonakdar, 2023). Privacy concerns have also been documented in medical tourism and other contexts involving cross-border movement of sensitive information (Roy, 2021). Likewise, biometric identification systems may generate not only individual privacy risks but also broader structural risks involving surveillance, exclusion, discrimination, and asymmetries of power (Wodajo, 2024a, 2024b). The growing use of consumer data in tourism and hospitality further illustrates the importance of integrating data ethics with organizational data governance (Yallop et al., 2021).

Despite substantial research on cybersecurity, personal-data protection, privacy regulation, AI governance, and digital consumer protection, fewer empirical studies have examined how data governance simultaneously affects legal risk management and organizational capacity to prevent privacy violations. This gap is particularly important in digital businesses, where legal, technical, and managerial risks are

E-ISSN: 3041-8933

strongly interconnected. Accordingly, the present study aimed to assess the role of data governance in managing legal risks and combating privacy violations in digital businesses in Tehran.

Methods and Materials

This applied, quantitative, cross-sectional, descriptive-correlational study was conducted among managers, specialists, and professionals working in digital businesses located in Tehran. The final sample consisted of 384 participants who were professionally involved in data management, information technology, information security, legal affairs, compliance, risk management, digital platforms, or related organizational functions. Participants were recruited through purposive and convenience sampling. Eligibility criteria included employment in a digital business in Tehran, at least one year of relevant professional experience, practical familiarity with data processing or protection processes, and informed consent to participate.

Data were collected using a structured questionnaire consisting of demographic and professional characteristics and three principal constructs: data governance, legal risk management, and combating privacy violations. Data governance covered dimensions including data policies and accountability, data quality and integrity, access control and security, transparency and accountability in data processing, and data lifecycle management. Legal risk management included identification and assessment of legal risks, compliance with legal and contractual obligations, management of liability arising from data breaches, and third-party risk management. Combating privacy violations included control over the collection and use of personal data, consent and user-rights management, protection of information confidentiality, and management of privacy-breach incidents. Items were scored on a five-point Likert scale.

Content validity was assessed by experts in information technology law, data privacy, information security, and digital business management. Construct reliability and validity were evaluated using Cronbach's alpha, composite reliability, factor loadings, average variance extracted, and discriminant validity. Descriptive analyses and preliminary assumption testing were performed using SPSS version 29. Structural equation modeling was conducted using SmartPLS version 4. Pearson correlations were used to examine bivariate associations, while bootstrapping was applied to evaluate direct and indirect structural effects. Statistical significance was set at 0.05.

Findings

The final analysis included 384 participants, of whom 226 were men (58.9%) and 158 were women (41.1%). The mean age was 36.84 years with a standard deviation of 7.29 years. The mean scores for data governance, legal risk management, and combating privacy violations were 3.71 ± 0.63, 3.62 ± 0.67, and 3.68 ± 0.65, respectively. Among data-governance dimensions, access control and data security had the highest mean score (3.83), whereas transparency and accountability in data processing had the lowest mean (3.57). Within legal risk management, compliance with legal and contractual requirements recorded the highest mean (3.74), whereas third-party risk management showed the lowest mean (3.48). Within privacy protection, information confidentiality had the highest mean (3.87), while consent and user-rights management had the lowest mean (3.55).

Data governance was positively and significantly correlated with legal risk management ($r = 0.692$, $p < 0.01$) and combating privacy violations ($r = 0.728$, $p < 0.01$). Legal risk management was also positively associated with combating privacy violations ($r = 0.653$, $p < 0.01$). Measurement-model assessment demonstrated satisfactory reliability and validity. Cronbach's alpha values for data

governance, legal risk management, and combating privacy violations were 0.912, 0.903, and 0.918, respectively. Composite reliability values were 0.927, 0.922, and 0.936, while average variance extracted values were 0.615, 0.642, and 0.666, respectively.

Structural modeling showed that data governance had a strong positive effect on legal risk management ($\beta = 0.692$, $t = 16.878$, $p < 0.001$). Data governance also had a significant direct effect on combating privacy violations ($\beta = 0.529$, $t = 11.021$, $p < 0.001$). Legal risk management significantly predicted combating privacy violations ($\beta = 0.287$, $t = 5.519$, $p < 0.001$). The indirect effect of data governance on combating privacy violations through legal risk management was 0.199 ($t = 5.237$, $p < 0.001$), demonstrating partial mediation. The total effect of data governance on combating privacy violations was 0.728 ($p < 0.001$). Data governance explained 47.9% of the variance in legal risk management, while data governance and legal risk management jointly explained 59.8% of the variance in combating privacy violations. Predictive relevance values were $Q^2 = 0.331$ for legal risk management and $Q^2 = 0.407$ for combating privacy violations. The SRMR value of 0.057 indicated satisfactory overall model fit.

Discussion and Conclusion

The findings demonstrate that data governance is a central organizational mechanism for reducing legal exposure and strengthening privacy protection in digital businesses. The strong effect of data governance on legal risk management indicates that organizations with clearer policies, accountability structures, access controls, data-quality mechanisms, and lifecycle-management procedures are better equipped to identify, document, evaluate, and control legal risks associated with data processing. This finding also suggests that legal risk cannot be managed effectively through legal review alone; rather, risk reduction requires organizational structures that define responsibility for data throughout its entire lifecycle.

The significant direct effect of data governance on combating privacy violations further indicates that privacy protection depends on more than formal legal compliance. Governance mechanisms can directly improve privacy performance by restricting unnecessary access, clarifying permissible uses of information, improving transparency, strengthening confidentiality, and establishing procedures for incident detection and response. The persistence of this direct effect after legal risk management was entered into the model suggests that some of the privacy benefits of data governance operate independently through technical, managerial, and operational mechanisms.

Legal risk management also significantly improved the ability of organizations to combat privacy violations. This result shows that systematic identification of legal obligations, contractual exposure, third-party responsibilities, and potential liabilities contributes directly to stronger privacy protection. In practical terms, organizations that translate legal requirements into operational controls are more likely to prevent misuse, unauthorized disclosure, and non-compliant processing of personal information.

The significant indirect effect additionally demonstrates that legal risk management partially mediates the relationship between data governance and privacy protection. Therefore, data governance appears to operate through two complementary pathways. One pathway is direct, involving technical and managerial controls over data processing. The second pathway is indirect, in which governance strengthens legal risk management, which in turn improves organizational privacy performance. This dual

E-ISSN: 3041-8933

mechanism provides a more comprehensive explanation of how organizational governance structures can produce measurable privacy outcomes.

The relatively high explained variance in both endogenous constructs reinforces the practical importance of the proposed model. Data governance alone accounted for nearly half of the variance in legal risk management, while data governance together with legal risk management explained almost 60% of the variance in combating privacy violations. These findings indicate that strengthening governance structures can have substantial organizational consequences and should be considered a strategic priority rather than a narrowly technical compliance function.

Overall, the study concludes that effective data governance significantly enhances legal risk management and organizational capacity to prevent and respond to privacy violations in digital businesses. Legal risk management also serves as a partial mediating mechanism through which data governance contributes to privacy protection. Digital businesses should therefore integrate data governance, legal compliance, cybersecurity, accountability, and privacy management into a unified organizational framework. Such integration can reduce legal exposure, improve transparency and responsibility, strengthen user trust, and provide a more sustainable foundation for data-driven digital operations.



شاپای الکترونیکی: ۸۹۳۳-۳۰۴۱

مدیریت پویا و تحلیل کسب و کار

دوره ۶، شماره ۵، صفحه ۲۵-۱

وبسایت مجله

تاریخچه مقاله
دریافت شده در تاریخ ۶ خرداد ۱۴۰۵
اصلاح شده در تاریخ ۲۱ شهریور ۱۴۰۵
پذیرفته شده در تاریخ ۲۸ شهریور ۱۴۰۵
اولین انتشار در تاریخ ۱۵ آبان ۱۴۰۵
انتشار نهایی در تاریخ ۱ دی ۱۴۰۶

ارزیابی نقش حکمرانی داده در مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی در کسب‌وکارهای دیجیتال

سلام هادی جاسم[۱]، رضا نیکخواه[۲*]، سیامک جعفرزاده[۲]

۱. دانشجوی دکتری حقوق خصوصی، دانشگاه ارومیه، ارومیه، ایران
۲. دانشیار، گروه فقه و حقوق اسلامی، دانشکده ادبیات و علوم انسانی، دانشگاه ارومیه، ارومیه، ایران

[*] **ایمیل نویسنده مسئول:** r.nikkhah@urmia.ac.ir

اطلاعات مقاله

نوع مقاله
پژوهشی اصیل

نحوه استناد به این مقاله:
هادی جاسم، سلام.، نیکخواه، رضا.، و جعفرزاده، سیامک. (۱۴۰۶). ارزیابی نقش حکمرانی داده در مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی در کسب‌وکارهای دیجیتال. *مدیریت پویا و تحلیل کسب و کار*، ۶(۵)، ۲۵-۱.

© ۱۴۰۶ تمامی حقوق انتشار این مقاله متعلق به نویسنده(گان) است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY 4.0) صورت گرفته است.

چکیده

هدف: هدف این پژوهش ارزیابی نقش حکمرانی داده در مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی در کسب‌وکارهای دیجیتال شهر تهران بود. **روش‌شناسی:** این پژوهش کاربردی با رویکرد کمی، مقطعی و توصیفی–همبستگی انجام شد. جامعه پژوهش شامل مدیران، کارشناسان و متخصصان شاغل در کسب‌وکارهای دیجیتال شهر تهران در حوزه‌های مدیریت داده، فناوری اطلاعات، امنیت اطلاعات، امور حقوقی، انطباق و مدیریت ریسک بود. نمونه نهایی شامل ۳۸۴ نفر بود که با روش نمونه‌گیری هدفمند و در دسترس انتخاب شدند. داده‌ها با استفاده از پرسشنامه ساختاریافته شامل سه سازه اصلی حکمرانی داده، مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی گردآوری شد. روایی محتوایی و سازه‌ای ابزار و پایایی آن با استفاده از بارهای عاملی، آلفای کرونباخ، پایایی ترکیبی و میانگین واریانس استخراج‌شده بررسی شد. تحلیل داده‌ها با نرم‌افزارهای SPSS نسخه ۲۹ و SmartPLS نسخه ۴ و با استفاده از همبستگی پیرسون، مدل‌سازی معادلات ساختاری و روش بوت‌استرپ انجام شد. **یافته‌ها:** حکمرانی داده اثر مثبت و معناداری بر مدیریت ریسک‌های حقوقی داشت (β = ۰.۶۹۲، t = ۱۶.۸۷۸، p < ۰.۰۰۱). همچنین، حکمرانی داده به‌طور مستقیم بر مقابله با نقض حریم خصوصی اثر معناداری نشان داد (β = ۰.۵۲۹، t = ۱۱.۰۲۱، p < ۰.۰۰۱). مدیریت ریسک‌های حقوقی نیز اثر مثبت و معناداری بر مقابله با نقض حریم خصوصی داشت (β = ۰.۲۸۷، t = ۵.۵۱۹، p < ۰.۰۰۱). اثر غیرمستقیم حکمرانی داده بر مقابله با نقض حریم خصوصی از طریق مدیریت ریسک‌های حقوقی برابر با ۰.۱۹۹ و معنادار بود (t = ۵.۲۳۷، p < ۰.۰۰۱) و نقش میانجی جزئی مدیریت ریسک‌های حقوقی را تأیید کرد. مقدار R^2 برای مدیریت ریسک‌های حقوقی ۰.۴۷۹ و برای مقابله با نقض حریم خصوصی ۰.۵۹۸ به دست آمد و مقدار SRMR برابر با ۰.۰۵۷ بود. **نتیجه‌گیری:** یافته‌ها نشان دادند که حکمرانی داده یکی از سازوکارهای راهبردی برای کاهش مخاطرات حقوقی و تقویت حفاظت از حریم خصوصی در کسب‌وکارهای دیجیتال است و بخشی از اثر آن از طریق بهبود مدیریت ریسک‌های حقوقی منتقل می‌شود؛ بنابراین، ادغام حکمرانی داده، انطباق حقوقی، امنیت اطلاعات و پاسخگویی سازمانی می‌تواند به ارتقای حفاظت از داده‌های شخصی و کاهش مواجهه حقوقی سازمان کمک کند.

کلیدواژگان: *حکمرانی داده؛ مدیریت ریسک‌های حقوقی؛ حریم خصوصی؛ کسب‌وکارهای دیجیتال؛ حفاظت از داده؛ انطباق حقوقی*

مقدمه

گسترش شتابان اقتصاد دیجیتال، توسعه پلتفرم‌های آنلاین، استفاده فراگیر از هوش مصنوعی، کلان‌داده، خدمات ابری، بانکداری دیجیتال، تجارت الکترونیکی و سامانه‌های مبتنی بر داده، ساختار تصمیم‌گیری و خلق ارزش در کسب‌وکارها را به‌طور اساسی دگرگون کرده است. در چنین محیطی، داده دیگر صرفاً یک محصول جانبی فعالیت‌های سازمانی محسوب نمی‌شود، بلکه به یکی از مهم‌ترین دارایی‌های راهبردی کسب‌وکارهای دیجیتال تبدیل شده است که بر تصمیم‌گیری، نوآوری، شناخت مشتری، شخصی‌سازی خدمات، توسعه محصولات و ایجاد مزیت رقابتی اثر مستقیم دارد. بااین‌حال، افزایش وابستگی سازمان‌ها به داده، به‌ویژه داده‌های شخصی و رفتاری کاربران، هم‌زمان دامنه مسئولیت‌های حقوقی و مخاطرات مرتبط با حریم خصوصی را گسترش داده است. یافته‌های پژوهشی نشان می‌دهند که خلق ارزش اقتصادی از داده در فضای مقرراتی جدید تنها زمانی پایدار است که استفاده از داده با سازوکارهای مؤثر حفاظت از حریم خصوصی، پاسخگویی و انطباق حقوقی همراه شود؛ زیرا مقررات حریم خصوصی می‌توانند هم محدودیت ایجاد کنند و هم در صورت حکمرانی صحیح داده، به ارتقای اعتماد و ارزش بنگاه کمک کنند (Yan & Cai, 2026). ازاین‌رو، حکمرانی داده به‌عنوان مجموعه‌ای از ساختارها، سیاست‌ها، مسئولیت‌ها، استانداردها و فرایندهای سازمانی برای هدایت نحوه تولید، دسترسی، نگهداری، استفاده، اشتراک‌گذاری و حذف داده، به یکی از مؤلفه‌های اساسی حکمرانی شرکتی در محیط دیجیتال تبدیل شده است.

پیچیدگی این مسئله زمانی افزایش می‌یابد که کسب‌وکارهای دیجیتال در محیط‌هایی فعالیت کنند که در آن قوانین محلی حریم خصوصی، قواعد فرامرزی پردازش داده و الزامات متفاوت حوزه‌های قضایی به‌طور هم‌زمان بر فعالیت سازمان اثر می‌گذارند. جهانی‌شدن خدمات دیجیتال موجب شده است که داده‌ها به‌سادگی از مرزهای ملی عبور کنند، درحالی‌که قوانین حریم خصوصی عمدتاً در قلمروهای حقوقی خاص طراحی و اجرا می‌شوند. این ناهمگونی می‌تواند سازمان‌ها را با مجموعه‌ای از الزامات هم‌پوشان یا حتی متعارض مواجه کند و هزینه انطباق را افزایش دهد (Sharma et al., 2026). در کنار این مسئله، توسعه سامانه‌های هوش مصنوعی و استفاده از حجم عظیمی از داده‌های آموزشی و عملیاتی، ضرورت شکل‌گیری مدل‌های روشن حکمرانی داده را دوچندان کرده است. در مدل‌های زبانی بزرگ و سامانه‌های مبتنی بر هوش مصنوعی، نبود استانداردهای روشن درباره منشأ داده، کیفیت داده، رضایت، حقوق مالکیت، دسترسی و مسئولیت می‌تواند به بروز مخاطرات حقوقی، اخلاقی و امنیتی منجر شود (Pahune et al., 2025). از سوی دیگر، صرف تدوین اعلامیه‌های اخلاقی یا اصول داوطلبانه برای تنظیم رفتار پلتفرم‌ها کافی نیست و بدون سازوکارهای اجرایی، نظارتی و پاسخگویی مؤثر، این چارچوب‌ها ممکن است اثر عملی محدودی بر کاهش ریسک داشته باشند (Haidar, 2026).

یکی از چالش‌های اساسی حکمرانی داده در کسب‌وکارهای دیجیتال، ایجاد تعادل میان بهره‌برداری اقتصادی از داده و صیانت از حقوق مصرف‌کنندگان است. خدمات مبتنی بر هوش مصنوعی، اعتبارسنجی دیجیتال، تبلیغات هدفمند، تحلیل رفتار کاربران و شخصی‌سازی تجربه مشتری به داده‌های گسترده‌ای وابسته‌اند، اما همین فرایندها ممکن است زمینه استفاده بیش از حد از داده، پردازش بدون رضایت مؤثر، پروفایل‌سازی غیرشفاف یا نقض محرمانگی را فراهم کنند. در این زمینه، ضرورت برقراری تعادل میان منافع حاصل از بهره‌گیری از داده و حقوق مصرف‌کننده، به‌ویژه در بستر توسعه هوش مصنوعی، به یکی از موضوعات مهم سیاست‌گذاری تبدیل شده است (Vásquez & Alvarez-Orozco, 2026). همچنین، بررسی تجربه کشورهای دارای نظام‌های حقوقی متکثر نشان می‌دهد که حفاظت از حریم خصوصی صرفاً از طریق اعمال قواعد رسمی قابل تحقق نیست و باید هنجارهای اجتماعی، انتظارات زمینه‌ای کاربران و ویژگی‌های نهادی محیط نیز مورد توجه قرار

گیرند (Kadiri & Boamah, 2025). بنابراین، حکمرانی داده در کسب‌وکارهای دیجیتال باید فراتر از رعایت حداقلی قانون عمل کرده و سازوکاری برای درونی‌سازی اصول حریم خصوصی در تصمیمات سازمانی باشد.

تجربه شرکت‌های بزرگ فعال در اقتصاد دیجیتال نیز نشان می‌دهد که ضعف در حکمرانی داده می‌تواند پیامدهای جدی حقوقی، مالی و اعتباری به همراه داشته باشد. بررسی نظام‌های مقرراتی سخت‌گیرانه، از جمله مقررات حاکم بر حفاظت و امنیت داده در چین، نشان داده است که شرکت‌های فعال در بازارهای فرامرزی باید از همان مرحله طراحی مدل کسب‌وکار، الزامات مربوط به جمع‌آوری، نگهداری، انتقال و پردازش داده را در ساختارهای سازمانی خود ادغام کنند (Conde et al., 2025). مدیریت داده در اقتصاد دیجیتال همچنین با سیاست‌های رقابتی و کنترل قدرت بازار پیوند خورده است؛ زیرا دسترسی گسترده به داده می‌تواند به تمرکز اقتصادی، رفتارهای ضد رقابتی یا سوءاستفاده از موقعیت مسلط منجر شود و به همین دلیل، تنظیم مقررات داده باید با ملاحظات حقوق رقابت نیز هماهنگ باشد (Mushtaq et al., 2024). در این معنا، حکمرانی داده تنها موضوعی فنی یا امنیتی نیست، بلکه به قلمرو گسترده‌تری از حقوق تجارت، رقابت، مسئولیت مدنی، حمایت از مصرف‌کننده و تنظیم‌گری دیجیتال مرتبط است.

تحول دیجیتال همچنین موجب شده است که مفهوم داده شخصی از اطلاعات هویتی سنتی فراتر رود و انواع گسترده‌ای از داده‌های رفتاری، زیستی، مکانی، مالی، سلامت و داده‌های حاصل از تعاملات آنلاین را شامل شود. در مطالعات مربوط به حفاظت از داده‌های شخصی در محیط دیجیتال، بر این نکته تأکید شده است که افزایش ظرفیت جمع‌آوری، ذخیره و ترکیب داده‌ها، تشخیص مرز میان داده عادی و داده حساس را دشوارتر کرده و ضرورت تدوین سیاست‌های روشن برای پردازش قانونی داده را افزایش داده است (Nguyen & Le, 2024). در حوزه‌هایی مانند شناسه‌های زیست‌سنجی، مخاطرات صرفاً محدود به افشای اطلاعات نیست، بلکه ممکن است شامل نظارت گسترده، تبعیض، حذف اجتماعی و عدم توازن قدرت میان شهروند و سازمان باشد (Wodajo, 2024a, 2024b). از همین رو، ارزیابی خطرات حریم خصوصی باید علاوه بر پیامدهای فردی، آثار ساختاری و اجتماعی پردازش داده را نیز در نظر گیرد.

یکی از ابعاد اساسی مدیریت ریسک‌های حقوقی، حفاظت از حقوق مصرف‌کنندگان در بازارهای دیجیتال است. تحول شیوه‌های ارائه خدمات و گسترش قراردادهای آنلاین موجب شده است که مصرف‌کنندگان در بسیاری از موارد بدون آگاهی کامل از نحوه پردازش اطلاعات خود، با شرایط استفاده از داده موافقت کنند. در چنین شرایطی، حقوق کسب‌وکار نقش مهمی در ایجاد سازوکارهای شفافیت، مسئولیت‌پذیری، جبران خسارت و حفاظت از مصرف‌کننده دارد (Widiarty & Tehupeiory, 2024). این موضوع در خدمات مالی دیجیتال اهمیت بیشتری می‌یابد؛ زیرا ارائه‌دهندگان خدمات وام آنلاین، بانکداری دیجیتال و فین‌تک به حجم گسترده‌ای از داده‌های هویتی، مالی و رفتاری افراد دسترسی پیدا می‌کنند. مطالعات نشان داده‌اند که توسعه خدمات وام آنلاین بدون کنترل مناسب جمع‌آوری و پردازش اطلاعات می‌تواند به سوءاستفاده از داده‌های شخصی و نقض حریم خصوصی منجر شود (Ramadhan et al., 2024). پژوهش‌های پیشین درباره حفاظت حقوقی از داده‌های شخصی در معاملات وام آنلاین نیز بر ضرورت وجود سازوکارهای روشن رضایت، محدودیت استفاده از داده و پاسخگویی ارائه‌دهندگان خدمات تأکید کرده‌اند (Widi et al., 2021).

در حوزه بانکداری دیجیتال نیز حفاظت از داده شخصی به یکی از ارکان اصلی اعتماد عمومی تبدیل شده است. داده‌های بانکی به دلیل ماهیت حساس خود در معرض مجموعه‌ای از تهدیدهای امنیتی، حقوقی و سوءاستفاده‌های تجاری قرار دارند و ضعف در حکمرانی آن‌ها می‌تواند مسئولیت گسترده‌ای برای مؤسسات مالی ایجاد کند. بررسی چارچوب‌های حکمرانی بانکداری دیجیتال نشان داده است که حفاظت از داده باید در کنار قواعد دسترسی، انتقال، ذخیره‌سازی و پاسخگویی سازمانی قرار گیرد و صرفاً به اقدامات امنیت سایبری محدود نشود (Yuspin et al., 2023). به همین ترتیب، سیاست‌های تجارت الکترونیکی و شبکه‌های اجتماعی نیز نیازمند ترکیبی از تدابیر مدیریتی و

E-ISSN: 3041-8933

حقوقی هستند؛ زیرا استفاده تجاری از اطلاعات کاربران در این فضاها می‌تواند موجب تعارض میان اهداف بازاریابی، آزادی فعالیت اقتصادی و الزامات حفاظت از حقوق کاربران شود (Mujtaba & Cavico, 2023). سوءاستفاده از اطلاعات در شبکه‌های اجتماعی نیز می‌تواند به نقض حریم خصوصی، آسیب‌های اعتباری و مسئولیت حقوقی منجر شود و ضرورت مداخله حقوقی و تقویت سازوکارهای حفاظتی را برجسته سازد (Akbar et al., 2023).

مدیریت ریسک حقوقی در محیط‌های داده‌محور به‌طور جدی با سیاست‌های امنیت سایبری سازمان پیوند دارد. نقض امنیت داده می‌تواند به افشای اطلاعات محرمانه، توقف خدمات، از دست رفتن اعتماد مشتریان و ایجاد مسئولیت مدنی یا قراردادی منجر شود. ازاین‌رو، سیاست‌های امنیت سایبری مؤثر باید با ساختار حکمرانی داده هماهنگ باشند و مسئولیت‌ها، کنترل‌ها و فرایندهای واکنش به حادثه را به‌طور دقیق مشخص کنند (Mishra et al., 2022). بررسی حوزه شهرهای هوشمند نیز نشان می‌دهد که افزایش اتصال میان سامانه‌ها و تمرکز داده در زیرساخت‌های دیجیتال بدون رعایت الزامات انطباق می‌تواند مخاطرات جدی حریم خصوصی و امنیتی ایجاد کند (Aslam et al., 2022). چنین شواهدی بیانگر آن است که انطباق حقوقی، امنیت اطلاعات و حکمرانی داده سه حوزه جداگانه نیستند، بلکه اجزای یک نظام یکپارچه مدیریت ریسک محسوب می‌شوند.

این یکپارچگی در حوزه معماری سازمانی نیز اهمیت دارد. مطالعات نشان داده‌اند که معماری سازمانی می‌تواند ابزاری برای تبدیل الزامات قانونی مرتبط با حفاظت از داده به فرایندها، نقش‌ها و کنترل‌های عملیاتی باشد و به‌ویژه در محیط کلان‌داده امکان ردیابی جریان داده و تعیین مسئولیت را فراهم آورد (Georgiadis & Poels, 2021). چارچوب‌های صنعتی حریم خصوصی نیز بر لزوم مشخص شدن قواعد اشتراک‌گذاری داده میان سازمان‌ها و شرکای تجاری تأکید دارند، زیرا بخش قابل توجهی از مخاطرات حریم خصوصی نه در داخل یک سازمان، بلکه در جریان انتقال داده میان بازیگران مختلف ایجاد می‌شود (Ghorashi et al., 2023). همچنین، مدل‌های مبتنی بر تعامل ذی‌نفعان نشان داده‌اند که حفاظت مؤثر از حقوق داده نیازمند درنظرگرفتن انگیزه‌ها و رفتار بازیگران مختلف، از جمله سازمان، کاربر و نهاد تنظیم‌گر است (Li & Guo, 2023).

از منظر سیاست‌گذاری عمومی نیز داده به منبعی برای پاسخ به مسائل اجتماعی تبدیل شده است و استفاده مسئولانه از آن می‌تواند ظرفیت دولت‌ها و سازمان‌ها را برای حل مشکلات عمومی افزایش دهد. بااین‌حال، بهره‌گیری از داده باید در چارچوب سازوکارهایی انجام شود که اعتماد، شفافیت و حقوق افراد را حفظ کند (Oecd, 2022). در فضای دولت دیجیتال نیز حاکمیت قانون باید هم‌زمان با توسعه فناوری تقویت شود و فرایندهای تصمیم‌گیری مبتنی بر داده تحت نظارت قواعد روشن قرار گیرند (Wang & Liu, 2023). تحول ارتباطات دیجیتال در حوزه حقوق عمومی نیز نشان می‌دهد که مرز میان ارتباط خصوصی و عمومی در فضای دیجیتال پیچیده‌تر شده و این امر می‌تواند در تعیین مسئولیت‌ها و حدود مداخله تنظیم‌گر چالش ایجاد کند (Zubko et al., 2024). افزون بر آن، سرعت تحول فناوری موجب شده است که حقوق موجود در برخی موارد از فناوری عقب بماند و نیاز به رویکردهای انعطاف‌پذیرتر برای تنظیم پدیده‌های جدید، به‌ویژه هوش مصنوعی، احساس شود (Ruan, 2024).

یکی دیگر از چالش‌های مهم، توسعه نظام‌های خودتنظیمی و تنظیم‌گری مشترک است. با توجه به پیچیدگی فناوری و سرعت تحول مدل‌های کسب‌وکار، دولت به‌تنهایی ممکن است توانایی تدوین قواعد جزئی و به‌روز برای همه حوزه‌های پردازش داده را نداشته باشد. ازاین‌رو، مشارکت انجمن‌های صنعتی و سازمان‌های حرفه‌ای در تدوین استانداردها، نظارت بر اعضا و ارتقای انطباق می‌تواند مکمل تنظیم‌گری دولتی باشد (Suleiman et al., 2022). این رویکرد به‌ویژه زمانی مؤثر است که قواعد خودتنظیمی با ضمانت‌های پاسخگویی، ممیزی و نظارت مستقل همراه باشند. همچنین، ایجاد توازن میان حفاظت از اطلاعات شخصی و منافع مشروع ناشی از استفاده از داده مستلزم توجه به مفهوم

انتظار معقول افراد از حریم خصوصی است؛ بدین معنا که مشروعیت پردازش داده باید با زمینه، هدف و انتظارات منطقی کاربران سنجیده شود (Shen & Teng, 2022).

در حوزه‌های حساس مانند سلامت، ضعف در حکمرانی داده می‌تواند پیامدهای حقوقی گسترده‌تری ایجاد کند. استفاده از چت‌بات‌های هوش مصنوعی در خدمات سلامت، برای مثال، پرسش‌هایی درباره محرمانگی، ذخیره‌سازی اطلاعات، مسئولیت توسعه‌دهندگان و انطباق با الزامات حفاظت از اطلاعات سلامت ایجاد کرده است (Rezaeikhonakdar, 2023). در حوزه گردشگری سلامت نیز نگرانی‌های مربوط به حریم خصوصی دیجیتال اهمیت ویژه‌ای دارد؛ زیرا اطلاعات پزشکی افراد ممکن است میان کشورها، ارائه‌دهندگان خدمات و پلتفرم‌های مختلف جابه‌جا شود (Roy, 2021). تجربه همه‌گیری کووید-۱۹ نیز نشان داد که حتی زمانی که اهداف سلامت عمومی مشروع و فوری هستند، استفاده از فناوری‌های ردیابی و تحلیل داده باید با تکنیک‌های حفاظت از حریم خصوصی همراه باشد تا از پردازش بیش از حد یا سوءاستفاده بعدی از اطلاعات جلوگیری شود (Majeed & Hwang, 2021). این نمونه‌ها نشان می‌دهند که حکمرانی داده باید براساس ماهیت داده و میزان حساسیت آن، سطوح متفاوتی از کنترل و پاسخگویی را تعریف کند.

موضوع اخلاق داده نیز بخش جدایی‌ناپذیر این چارچوب است. در صنایع گردشگری و مهمان‌نوازی، افزایش استفاده از داده‌های مسافران برای شخصی‌سازی خدمات، تحلیل رفتار و بازاریابی، مسائل مهمی درباره رضایت، مالکیت اطلاعات و استفاده ثانویه ایجاد کرده است و به همین دلیل، اخلاق داده و حکمرانی داده باید هم‌زمان مورد توجه قرار گیرند (Yallop et al., 2021). در نظام‌های اداری نیز حفاظت از امنیت داده و حریم خصوصی افراد باید بخشی از مسئولیت سازمانی و پاسخگویی عمومی محسوب شود، نه صرفاً یک مسئله فنی مرتبط با واحد فناوری اطلاعات (Sari et al., 2024). این دیدگاه سبب می‌شود که مدیریت داده از سطح کنترل‌های فنی به سطح راهبرد سازمانی ارتقا یابد و نقش مدیران ارشد، واحدهای حقوقی، مدیریت ریسک و امنیت اطلاعات در آن به‌صورت یکپارچه تعریف شود.

افزون بر مسائل داخلی سازمان، توسعه تجارت جهانی و استفاده از هوش مصنوعی در زنجیره‌های فرامرزی، پیچیدگی‌های جدیدی در زمینه مسئولیت حقوقی، مالکیت داده و انطباق ایجاد کرده است. مقررات مربوط به هوش مصنوعی و داده می‌توانند بر روابط تجاری بین‌المللی اثر بگذارند و سازمان‌ها را با الزامات متفاوت در بازارهای متعدد مواجه کنند (Igbinenikaro & Adewusi, 2024). این وضعیت ضرورت ایجاد چارچوب‌های حکمرانی داده منعطف اما قابل ممیزی را برجسته می‌کند. از سوی دیگر، ویژگی‌های ساختاری اقتصاد داده‌محور موجب شده است که مسائل حریم خصوصی نه صرفاً از منظر حق فردی، بلکه در قالب روابط قدرت میان پلتفرم‌ها، کاربران و نهادهای تنظیم‌گر نیز تحلیل شوند. بنابراین، حکمرانی داده باید بتواند میان منافع سازمانی، الزامات قانونی و حقوق کاربران سازوکاری پایدار ایجاد کند.

با وجود گسترش پژوهش‌ها در زمینه حفاظت از داده، امنیت اطلاعات، حریم خصوصی، تنظیم‌گری هوش مصنوعی و انطباق حقوقی، بخش قابل توجهی از مطالعات موجود هر یک بر یک حوزه خاص تمرکز داشته‌اند و کمتر به بررسی هم‌زمان نقش حکمرانی داده در مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی در سطح سازمان پرداخته‌اند. به‌ویژه در فضای کسب‌وکارهای دیجیتال، لازم است مشخص شود که آیا وجود سیاست‌های روشن داده، مسئولیت‌پذیری، کنترل دسترسی، مدیریت چرخه عمر داده و شفافیت می‌تواند به‌طور مستقیم ریسک‌های حقوقی را کاهش دهد و هم‌زمان ظرفیت سازمان برای حفاظت از حریم خصوصی را افزایش دهد. اهمیت این موضوع از آن جهت بیشتر است که ریسک‌های حقوقی ناشی از داده ممکن است از مسیرهای مختلفی مانند نقض قرارداد، عدم رعایت رضایت کاربران، افشای غیرمجاز، انتقال نامشروع داده، ضعف در کنترل اشخاص ثالث یا فقدان مستندسازی تصمیمات ایجاد شوند. در نتیجه، تحلیل رابطه میان حکمرانی داده و مدیریت ریسک حقوقی می‌تواند تصویری یکپارچه‌تر از نحوه تبدیل اصول حکمرانی به پیامدهای عملی حفاظت از حریم خصوصی ارائه دهد.

E-ISSN: 3041-8933

بر همین اساس، هدف پژوهش حاضر ارزیابی نقش حکمرانی داده در مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی در کسب‌وکارهای دیجیتال شهر تهران است.

روش پژوهش

پژوهش حاضر از نظر هدف کاربردی و از نظر روش، مطالعه‌ای کمی، مقطعی و توصیفی–همبستگی بود که با هدف ارزیابی نقش حکمرانی داده در مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی در کسب‌وکارهای دیجیتال انجام شد. جامعه آماری پژوهش را مدیران، کارشناسان و متخصصان شاغل در کسب‌وکارهای دیجیتال مستقر در شهر تهران تشکیل دادند که در حوزه‌های مدیریت داده، فناوری اطلاعات، امنیت اطلاعات، امور حقوقی، مدیریت ریسک، انطباق سازمانی، حفاظت از داده‌ها و مدیریت پلتفرم‌های دیجیتال فعالیت داشتند. با توجه به گستردگی جامعه آماری و به‌منظور دستیابی به حجم نمونه‌ای مناسب برای انجام تحلیل‌های چندمتغیره و مدل‌سازی روابط میان متغیرهای پژوهش، تعداد ۳۸۴ نفر به‌عنوان نمونه نهایی مطالعه در نظر گرفته شد. نمونه‌گیری به شیوه هدفمند و در دسترس و با تمرکز بر افرادی انجام شد که به دلیل موقعیت شغلی و مسئولیت حرفه‌ای خود دارای تجربه مستقیم در زمینه جمع‌آوری، ذخیره‌سازی، پردازش، اشتراک‌گذاری، حفاظت یا نظارت حقوقی بر داده‌های کاربران و مشتریان بودند. معیارهای ورود به پژوهش شامل اشتغال در یکی از کسب‌وکارهای دیجیتال فعال در تهران، داشتن حداقل یک سال سابقه فعالیت حرفه‌ای مرتبط با داده‌ها، فناوری اطلاعات، امور حقوقی، امنیت اطلاعات یا مدیریت ریسک، آشنایی عملی با فرایندهای پردازش و حفاظت از داده‌های دیجیتال و اعلام رضایت آگاهانه برای شرکت در پژوهش بود. پرسشنامه‌هایی که بیش از ۱۰ درصد گویه‌های آن‌ها بدون پاسخ باقی مانده بود یا الگوی پاسخ‌دهی غیرقابل اعتماد و یکنواخت داشتند، از فرایند تحلیل کنار گذاشته شدند. گردآوری داده‌ها به‌صورت حضوری و الکترونیکی انجام شد و پیش از تکمیل ابزارها، هدف پژوهش، محرمانه بودن اطلاعات، ناشناس ماندن پاسخ‌دهندگان و اختیاری بودن مشارکت برای آنان توضیح داده شد. هیچ‌گونه اطلاعات هویتی مستقیم از مشارکت‌کنندگان دریافت نشد و داده‌های گردآوری‌شده صرفاً به‌صورت تجمیعی و برای اهداف علمی مورد استفاده قرار گرفت.

داده‌های پژوهش با استفاده از یک پرسشنامه ساختاریافته متناسب با چارچوب مفهومی پژوهش گردآوری شد. ابزار مورد استفاده از چهار بخش اصلی تشکیل شده بود. بخش نخست به اطلاعات جمعیت‌شناختی و حرفه‌ای مشارکت‌کنندگان، از جمله سن، جنسیت، سطح تحصیلات، سابقه فعالیت حرفه‌ای، حوزه تخصصی، نوع کسب‌وکار دیجیتال و سطح مسئولیت سازمانی اختصاص داشت. بخش دوم برای سنجش حکمرانی داده طراحی شد و ابعادی نظیر تدوین سیاست‌ها و مسئولیت‌های مرتبط با داده، تعیین مالکیت و پاسخگویی در قبال داده‌ها، کیفیت و یکپارچگی داده، کنترل دسترسی، امنیت و حفاظت از داده، شفافیت در پردازش داده‌ها، مدیریت چرخه عمر داده، نظارت بر اشتراک‌گذاری داده و سازوکارهای انطباق و پاسخگویی سازمانی را مورد ارزیابی قرار داد. بخش سوم به سنجش مدیریت ریسک‌های حقوقی در کسب‌وکارهای دیجیتال اختصاص یافت و مؤلفه‌هایی از قبیل شناسایی و ارزیابی ریسک‌های ناشی از پردازش داده، انطباق فعالیت‌های سازمان با الزامات حقوقی و قراردادی، مدیریت مسئولیت‌های ناشی از دسترسی یا افشای غیرمجاز اطلاعات، کنترل ریسک‌های مربوط به اشخاص ثالث، مستندسازی تصمیمات مرتبط با داده و آمادگی سازمان برای پاسخگویی به دعاوی و اختلافات حقوقی را پوشش داد. بخش چهارم نیز مقابله با نقض حریم خصوصی را با تمرکز بر اقداماتی مانند محدودسازی جمع‌آوری داده به میزان ضروری، مدیریت رضایت کاربران، کنترل دسترسی به اطلاعات شخصی، جلوگیری از استفاده ثانویه و غیرمجاز از داده، حفاظت از محرمانگی اطلاعات، شناسایی و مدیریت رخدادهای نقض داده، اطلاع‌رسانی مناسب در هنگام وقوع رخداد و ایجاد سازوکارهای پاسخگویی به درخواست‌ها و اعتراض‌های مرتبط با حریم خصوصی ارزیابی کرد. گویه‌های اصلی ابزار بر اساس طیف پنج‌درجه‌ای لیکرت از «کاملاً مخالفم» با نمره ۱ تا «کاملاً موافقم» با نمره ۵ امتیازگذاری شدند؛ به‌گونه‌ای

که نمرات بالاتر در هر سازه بیانگر استقرار مطلوب‌تر حکمرانی داده، اثربخشی بیشتر مدیریت ریسک‌های حقوقی یا توان بالاتر کسب‌وکار در پیشگیری و مقابله با نقض حریم خصوصی بود.

برای اطمینان از روایی ابزار، نسخه اولیه پرسشنامه در اختیار گروهی از صاحب‌نظران حوزه‌های حقوق فناوری اطلاعات، حقوق داده و حریم خصوصی، مدیریت فناوری اطلاعات، امنیت اطلاعات و مدیریت کسب‌وکارهای دیجیتال قرار گرفت و تناسب، شفافیت، ضرورت و ارتباط گویه‌ها با سازه‌های مورد اندازه‌گیری بررسی شد. اصلاحات پیشنهادی متخصصان در زمینه حذف گویه‌های مبهم، رفع هم‌پوشانی مفهومی و بهبود وضوح عبارات در نسخه نهایی اعمال شد. روایی محتوایی ابزار با استفاده از نسبت روایی محتوا و شاخص روایی محتوا ارزیابی شد و تنها گویه‌هایی که مقادیر قابل قبول داشتند در نسخه نهایی باقی ماندند. همچنین، برای بررسی اولیه قابلیت فهم و ثبات ابزار، پرسشنامه به‌صورت آزمایشی در گروهی مستقل از افراد دارای ویژگی‌های مشابه جامعه هدف اجرا شد. پایایی درونی سازه‌ها با استفاده از ضریب آلفای کرونباخ و پایایی ترکیبی بررسی شد و مقادیر ۰.۷۰ و بالاتر به‌عنوان سطح قابل قبول پایایی در نظر گرفته شد. برای بررسی روایی سازه نیز بارهای عاملی، میانگین واریانس استخراج‌شده و روایی واگرا مورد ارزیابی قرار گرفتند. میانگین واریانس استخراج‌شده بیشتر از ۰.۵۰ به‌عنوان شواهد مناسب روایی همگرا در نظر گرفته شد و برای بررسی تمایز تجربی میان سازه‌های حکمرانی داده، مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی، روایی واگرا نیز پیش از آزمون مدل ساختاری بررسی شد.

پس از تکمیل فرایند گردآوری داده‌ها، پرسشنامه‌ها از نظر کامل بودن، وجود داده‌های مفقود، پاسخ‌های پرت و الگوهای پاسخ‌دهی نامعتبر بررسی شدند و سپس داده‌های قابل قبول برای تحلیل آماری آماده شدند. در مرحله نخست، آمار توصیفی شامل فراوانی، درصد، میانگین، انحراف معیار، حداقل و حداکثر نمرات برای توصیف ویژگی‌های مشارکت‌کنندگان و متغیرهای اصلی پژوهش محاسبه شد. پیش از اجرای تحلیل‌های استنباطی، مفروضه‌های آماری شامل توزیع داده‌ها، وجود داده‌های پرت، خطی بودن روابط، هم‌خطی چندگانه و استقلال خطاها مورد بررسی قرار گرفت. برای ارزیابی هم‌خطی چندگانه از شاخص عامل تورم واریانس و مقدار تحمل استفاده شد و مقادیر شاخص عامل تورم واریانس کمتر از ۵ به‌عنوان نشانه نبود مشکل جدی هم‌خطی در نظر گرفته شد. علاوه بر این، ضرایب چولگی و کشیدگی متغیرها برای بررسی ویژگی‌های توزیع داده‌ها محاسبه شدند.

در مرحله بعد، روابط دو متغیره میان حکمرانی داده، مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی با استفاده از ضریب همبستگی پیرسون بررسی شد. برای آزمون هم‌زمان روابط پیش‌بینی‌شده در مدل مفهومی و تعیین میزان تأثیر حکمرانی داده بر مدیریت ریسک‌های حقوقی و توانایی کسب‌وکارهای دیجیتال در مقابله با نقض حریم خصوصی، از مدل‌سازی معادلات ساختاری استفاده شد. ابتدا مدل اندازه‌گیری از نظر بارهای عاملی، پایایی درونی، پایایی ترکیبی، روایی همگرا و روایی واگرا ارزیابی و پس از تأیید کفایت آن، مدل ساختاری مورد آزمون قرار گرفت. ضرایب مسیر استانداردشده برای تعیین جهت و شدت اثر میان سازه‌ها محاسبه شد و مقدار ضریب تعیین برای مشخص کردن میزان واریانس تبیین‌شده متغیرهای وابسته مورد استفاده قرار گرفت. همچنین، معناداری ضرایب مسیر و اثرات مستقیم و غیرمستقیم با استفاده از روش بازنمونه‌گیری بوت‌استرپ بررسی شد. تحلیل‌های توصیفی و بررسی مقدماتی داده‌ها با استفاده از نرم‌افزار SPSS نسخه ۲۹ و آزمون مدل اندازه‌گیری و ساختاری با استفاده از نرم‌افزار SmartPLS نسخه ۴ انجام شد. سطح معناداری آماری در تمامی آزمون‌ها برابر با ۰.۰۵ در نظر گرفته شد و مقادیر کمتر از این سطح به‌عنوان شواهد وجود رابطه یا اثر آماری معنادار تفسیر شدند. این رویکرد تحلیلی امکان بررسی هم‌زمان کیفیت سنجش سازه‌ها و میزان اثرگذاری حکمرانی داده بر دو پیامد اصلی پژوهش، یعنی کاهش و مدیریت ریسک‌های حقوقی و تقویت سازوکارهای پیشگیری و مقابله با نقض حریم خصوصی در کسب‌وکارهای دیجیتال را فراهم کرد.

E-ISSN: 3041-8933

یافته‌ها

در مجموع، داده‌های مربوط به ۳۸۴ نفر از مدیران، کارشناسان و متخصصان فعال در کسب‌وکارهای دیجیتال شهر تهران وارد تحلیل نهایی شد. از کل مشارکت‌کنندگان، ۲۲۶ نفر معادل ۵۸.۹ درصد مرد و ۱۵۸ نفر معادل ۴۱.۱ درصد زن بودند. میانگین سنی مشارکت‌کنندگان ۳۶.۸۴ سال با انحراف معیار ۷.۲۹ سال بود و دامنه سنی آنان از ۲۴ تا ۵۸ سال متغیر بود. از نظر تحصیلات، ۴۶ نفر معادل ۱۲.۰ درصد دارای مدرک کارشناسی، ۲۴۱ نفر معادل ۶۲.۸ درصد دارای مدرک کارشناسی ارشد و ۹۷ نفر معادل ۲۵.۲ درصد دارای مدرک دکتری یا تحصیلات حرفه‌ای معادل بودند. از نظر سابقه فعالیت حرفه‌ای، ۷۳ نفر معادل ۱۹.۰ درصد بین ۱ تا ۴ سال، ۱۴۶ نفر معادل ۳۸.۰ درصد بین ۵ تا ۹ سال، ۱۰۳ نفر معادل ۲۶.۸ درصد بین ۱۰ تا ۱۴ سال و ۶۲ نفر معادل ۱۶.۲ درصد دارای ۱۵ سال یا بیشتر سابقه فعالیت مرتبط بودند. ترکیب تخصصی نمونه نیز نشان داد که ۹۲ نفر معادل ۲۴.۰ درصد در حوزه فناوری اطلاعات و مدیریت داده، ۷۴ نفر معادل ۱۹.۳ درصد در حوزه امنیت اطلاعات و امنیت سایبری، ۶۶ نفر معادل ۱۷.۲ درصد در امور حقوقی و انطباق، ۵۹ نفر معادل ۱۵.۴ درصد در مدیریت ریسک، ۴۸ نفر معادل ۱۲.۵ درصد در مدیریت پلتفرم‌ها و محصولات دیجیتال و ۴۵ نفر معادل ۱۱.۷ درصد در سایر حوزه‌های مرتبط فعالیت داشتند. از نظر سطح سازمانی، ۱۰۸ نفر معادل ۲۸.۱ درصد در سطح مدیریت ارشد یا میانی، ۱۸۹ نفر معادل ۴۹.۲ درصد در سطح کارشناسی تخصصی و ۸۷ نفر معادل ۲۲.۷ درصد در سمت‌های نظارتی، مشاوره‌ای یا مسئولیت‌های مرتبط با انطباق و حفاظت از داده مشغول به فعالیت بودند. این ترکیب نشان داد که نمونه پژوهش از نظر تجربه، تخصص حرفه‌ای و سطح سازمانی از تنوع کافی برای ارزیابی روابط میان حکمرانی داده، مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی برخوردار بود.

جدول ۱

شاخص‌های توصیفی متغیرهای اصلی پژوهش

متغیر	میانگین	انحراف معیار	حداقل	حداکثر	چولگی	کشیدگی
حکمرانی داده	۳.۷۱	۰.۶۳	۱.۸۲	۴.۹۳	−۰.۴۱	−۰.۱۸
سیاست‌ها و مسئولیت‌پذیری داده	۳.۷۶	۰.۶۸	۱.۶۰	۵.۰۰	−۰.۴۶	−۰.۱۱
کیفیت و یکپارچگی داده	۳.۶۹	۰.۶۶	۱.۷۵	۵.۰۰	−۰.۳۲	−۰.۲۴
کنترل دسترسی و امنیت داده	۳.۸۳	۰.۶۴	۱.۸۰	۵.۰۰	−۰.۵۱	۰.۰۷
شفافیت و پاسخگویی در پردازش داده	۳.۵۷	۰.۷۲	۱.۴۰	۵.۰۰	−۰.۲۷	−۰.۳۱
مدیریت چرخه عمر داده	۳.۶۵	۰.۶۹	۱.۵۰	۵.۰۰	−۰.۳۵	−۰.۱۹
مدیریت ریسک‌های حقوقی	۳.۶۲	۰.۶۷	۱.۵۴	۴.۹۶	−۰.۲۹	−۰.۲۲
شناسایی و ارزیابی ریسک حقوقی	۳.۵۹	۰.۷۱	۱.۴۰	۵.۰۰	−۰.۲۶	−۰.۲۸
انطباق با الزامات حقوقی و قراردادی	۳.۷۴	۰.۶۸	۱.۵۰	۵.۰۰	−۰.۴۳	−۰.۰۹
مدیریت مسئولیت ناشی از نقض داده	۳.۵۱	۰.۷۵	۱.۲۰	۵.۰۰	−۰.۲۱	−۰.۳۶
مدیریت ریسک اشخاص ثالث	۳.۴۸	۰.۷۳	۱.۳۰	۵.۰۰	−۰.۱۷	−۰.۲۹
مقابله با نقض حریم خصوصی	۳.۶۸	۰.۶۵	۱.۶۱	۴.۹۷	−۰.۳۸	−۰.۱۵
کنترل جمع‌آوری و استفاده از داده شخصی	۳.۷۲	۰.۶۹	۱.۵۰	۵.۰۰	−۰.۴۱	−۰.۱۰
مدیریت رضایت و حقوق کاربران	۳.۵۵	۰.۷۴	۱.۲۰	۵.۰۰	−۰.۲۵	−۰.۳۳
حفاظت از محرمانگی اطلاعات	۳.۸۷	۰.۶۲	۱.۸۰	۵.۰۰	−۰.۵۵	۰.۱۴
مدیریت رخدادهای نقض حریم خصوصی	۳.۵۸	۰.۷۱	۱.۳۰	۵.۰۰	−۰.۳۰	−۰.۲۶

بر اساس نتایج جدول ۱، میانگین نمره کلی حکمرانی داده برابر با ۳.۷۱ و انحراف معیار آن ۰.۶۳ بود که نشان‌دهنده ارزیابی نسبتاً مطلوب مشارکت‌کنندگان از میزان استقرار سازوکارهای حکمرانی داده در کسب‌وکارهای دیجیتال مورد بررسی است. در میان ابعاد حکمرانی داده، بالاترین میانگین به کنترل دسترسی و امنیت داده با میانگین ۳.۸۳ اختصاص داشت، در حالی که شفافیت و پاسخگویی در پردازش داده با میانگین ۳.۵۷ پایین‌ترین مقدار را در میان ابعاد این سازه نشان داد. این الگو بیانگر آن است که کسب‌وکارهای دیجیتال مورد بررسی در حوزه کنترل‌های فنی و امنیتی عملکرد نسبتاً قوی‌تری داشته‌اند، اما در زمینه شفاف‌سازی تصمیمات مربوط به پردازش داده و ایجاد سازوکارهای پاسخگویی همچنان ظرفیت بهبود وجود داشته است. میانگین مدیریت ریسک‌های حقوقی برابر با ۳.۶۲ بود. در این سازه، انطباق با الزامات حقوقی و قراردادی با میانگین ۳.۷۴ بالاترین مقدار را به خود اختصاص داد، در حالی که مدیریت ریسک اشخاص ثالث با میانگین ۳.۴۸ و مدیریت مسئولیت ناشی از نقض داده با میانگین ۳.۵۱ از مقادیر پایین‌تری برخوردار بودند. همچنین، میانگین کلی مقابله با نقض حریم خصوصی ۳.۶۸ به دست آمد که در میان ابعاد آن، حفاظت از محرمانگی اطلاعات با میانگین ۳.۸۷ بالاترین مقدار و مدیریت رضایت و حقوق کاربران با میانگین ۳.۵۵ پایین‌ترین مقدار را نشان داد. مقادیر چولگی تمامی متغیرها بین -۰.۵۵ و -۰.۱۷ و مقادیر کشیدگی بین -۰.۳۶ و ۰.۱۴ قرار داشت؛ بنابراین، هیچ‌یک از متغیرهای اصلی انحراف شدید از توزیع متقارن نشان ندادند و داده‌ها از نظر شکل توزیع برای انجام تحلیل‌های همبستگی و مدل‌سازی روابط ساختاری مناسب ارزیابی شدند.

جدول ۲

ماتریس همبستگی میان سازه‌های اصلی پژوهش و شاخص‌های روایی واگرا

متغیر	حکمرانی داده	مدیریت ریسک‌های حقوقی	مقابله با نقض حریم خصوصی
حکمرانی داده	۰.۷۸۴		
مدیریت ریسک‌های حقوقی	۰.۶۹۲**	۰.۸۰۱	
مقابله با نقض حریم خصوصی	۰.۷۲۸**	۰.۶۵۳**	۰.۸۱۶

نتایج جدول ۲ نشان داد که میان حکمرانی داده و مدیریت ریسک‌های حقوقی رابطه مثبت و معناداری وجود داشت و ضریب همبستگی میان این دو متغیر برابر با ۰.۶۹۲ بود. همچنین، حکمرانی داده با مقابله با نقض حریم خصوصی دارای رابطه مثبت و نسبتاً قوی با ضریب همبستگی ۰.۷۲۸ بود. این یافته نشان می‌دهد که هرچه ساختارها، سیاست‌ها، مسئولیت‌ها و فرایندهای مرتبط با حکمرانی داده در کسب‌وکارهای دیجیتال منسجم‌تر و توسعه‌یافته‌تر باشند، ظرفیت سازمان برای پیشگیری از نقض حریم خصوصی و واکنش مناسب به رخدادهای مرتبط با داده‌های شخصی نیز افزایش می‌یابد. رابطه بین مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی نیز مثبت و معنادار بود و مقدار ۰.۶۵۳ برای آن به دست آمد؛ بنابراین، کسب‌وکارهایی که در شناسایی، ارزیابی و کنترل پیامدهای حقوقی فعالیت‌های داده‌محور عملکرد مناسب‌تری داشتند، در زمینه کنترل مخاطرات حریم خصوصی نیز وضعیت مطلوب‌تری نشان دادند. تمام ضرایب همبستگی در سطح کمتر از ۰.۰۱ معنادار بودند. از سوی دیگر، جذر میانگین واریانس استخراج‌شده برای حکمرانی داده، مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی به‌ترتیب ۰.۷۸۴، ۰.۸۰۱ و ۰.۸۱۶ بود که در هر مورد از ضرایب همبستگی آن سازه با سایر سازه‌ها بیشتر بود. این نتایج از کفایت روایی واگرای سازه‌ها حمایت کرد و نشان داد که با وجود ارتباط مفهومی میان متغیرهای اصلی، هر سازه مفهوم متمایزی را در مدل پژوهش اندازه‌گیری می‌کند. همچنین، هیچ‌یک از ضرایب همبستگی به سطحی نرسید که نشان‌دهنده هم‌پوشانی شدید یا مشکل بالقوه هم‌خطی میان سازه‌ها باشد.

E-ISSN: 3041-8933

جدول ۳

نتایج ارزیابی مدل اندازه‌گیری، پایایی و روایی همگرای سازه‌ها

سازه	دامنه بارهای عاملی	آلفای کرونباخ	پایایی ترکیبی	میانگین واریانس استخراج‌شده
حکمرانی داده	۰.۷۱۱تا ۰.۸۶۴	۰.۹۱۲	۰.۹۲۷	۰.۶۱۵
سیاست‌ها و مسئولیت‌پذیری داده	۰.۷۲۳تا ۰.۸۵۱	۰.۸۴۶	۰.۸۸۷	۰.۶۱۱
کیفیت و یکپارچگی داده	۰.۷۱۶تا ۰.۸۳۹	۰.۸۲۱	۰.۸۷۴	۰.۵۸۲
کنترل دسترسی و امنیت داده	۰.۷۴۱تا ۰.۸۸۲	۰.۸۷۳	۰.۹۰۹	۰.۶۶۶
شفافیت و پاسخگویی در پردازش داده	۰.۷۰۴تا ۰.۸۴۳	۰.۸۳۴	۰.۸۸۳	۰.۶۰۲
مدیریت چرخه عمر داده	۰.۷۱۸تا ۰.۸۵۷	۰.۸۵۱	۰.۸۹۵	۰.۶۳۱
مدیریت ریسک‌های حقوقی	۰.۷۲۶تا ۰.۸۷۵	۰.۹۰۳	۰.۹۲۲	۰.۶۴۲
شناسایی و ارزیابی ریسک حقوقی	۰.۷۱۹تا ۰.۸۵۴	۰.۸۳۸	۰.۸۸۴	۰.۶۰۵
انطباق با الزامات حقوقی و قراردادی	۰.۷۴۴تا ۰.۸۷۳	۰.۸۶۴	۰.۹۰۲	۰.۶۴۸
مدیریت مسئولیت ناشی از نقض داده	۰.۷۳۱تا ۰.۸۶۱	۰.۸۵۲	۰.۸۹۵	۰.۶۳۱
مدیریت ریسک اشخاص ثالث	۰.۷۰۸تا ۰.۸۴۶	۰.۸۱۷	۰.۸۷۱	۰.۵۷۶
مقابله با نقض حریم خصوصی	۰.۷۳۸تا ۰.۸۸۹	۰.۹۱۸	۰.۹۳۶	۰.۶۶۶
کنترل جمع‌آوری و استفاده از داده شخصی	۰.۷۲۶تا ۰.۸۶۲	۰.۸۴۷	۰.۸۹۰	۰.۶۱۸
مدیریت رضایت و حقوق کاربران	۰.۷۱۱تا ۰.۸۵۱	۰.۸۳۲	۰.۸۸۱	۰.۵۹۷
حفاظت از محرمانگی اطلاعات	۰.۷۵۹تا ۰.۸۹۱	۰.۸۸۱	۰.۹۱۵	۰.۶۸۳
مدیریت رخدادهای نقض حریم خصوصی	۰.۷۳۳تا ۰.۸۷۲	۰.۸۵۸	۰.۸۹۹	۰.۶۴۱

بر اساس یافته‌های جدول ۳، مدل اندازه‌گیری از سطح مطلوبی از پایایی و روایی همگرا برخوردار بود. تمامی بارهای عاملی گویه‌ها و ابعاد مورد بررسی بالاتر از ۰.۷۰ قرار داشتند و دامنه کلی بارهای عاملی بین ۰.۷۰۴ و ۰.۸۹۱ متغیر بود. این مقادیر نشان می‌دهد که شاخص‌های مشاهده‌شده ارتباط کافی با سازه‌های مربوط به خود داشته و هیچ‌یک از گویه‌های اصلی به دلیل ضعف بار عاملی نیازمند حذف از مدل نبود. ضریب آلفای کرونباخ برای تمامی سازه‌ها و ابعاد بالاتر از ۰.۸۰ بود و برای سه سازه اصلی حکمرانی داده، مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی به‌ترتیب ۰.۹۱۲، ۰.۹۰۳ و ۰.۹۱۸ به دست آمد. همچنین، مقادیر پایایی ترکیبی برای تمامی سازه‌ها بالاتر از ۰.۸۷ بود و در سازه‌های اصلی به‌ترتیب ۰.۹۲۷، ۰.۹۲۲ و ۰.۹۳۶ محاسبه شد. این یافته‌ها نشان‌دهنده همسانی درونی مطلوب و ثبات مناسب ابزار سنجش بودند. میانگین واریانس استخراج‌شده نیز برای تمامی سازه‌ها بیش از مقدار معیار ۰.۵۰ بود و در سه سازه اصلی به‌ترتیب ۰.۶۱۵، ۰.۶۴۲ و ۰.۶۶۶ به دست آمد. از میان ابعاد مورد بررسی، حفاظت از محرمانگی اطلاعات با مقدار ۰.۶۸۳ و کنترل دسترسی و امنیت داده با مقدار ۰.۶۶۶ بالاترین میزان واریانس تبیین‌شده توسط شاخص‌های مربوط به خود را نشان دادند. در مقابل، مدیریت ریسک اشخاص ثالث با مقدار ۰.۵۷۶ پایین‌ترین میانگین واریانس استخراج‌شده را داشت، اما این مقدار نیز همچنان بالاتر از آستانه قابل قبول قرار داشت. در مجموع، ترکیب بارهای عاملی مطلوب، ضرایب آلفای کرونباخ بالا، پایایی ترکیبی مناسب و مقادیر قابل قبول میانگین واریانس استخراج‌شده نشان داد که مدل اندازه‌گیری از کیفیت روان‌سنجی کافی برخوردار بوده و می‌توان روابط ساختاری میان متغیرهای پژوهش را با اتکا به این مدل مورد آزمون قرار داد.

جدول ۴

نتایج مدل ساختاری و آزمون روابط میان متغیرهای پژوهش

مسیر ساختاری	ضریب مسیر استانداردشده β	خطای استاندارد	مقدار t	مقدار p	نتیجه
حکمرانی داده ← مدیریت ریسک‌های حقوقی	۰.۶۹۲	۰.۰۴۱	۱۶.۸۷۸	<۰.۰۰۱	معنادار
حکمرانی داده ← مقابله با نقض حریم خصوصی	۰.۵۲۹	۰.۰۴۸	۱۱.۰۲۱	<۰.۰۰۱	معنادار
مدیریت ریسک‌های حقوقی ← مقابله با نقض حریم خصوصی	۰.۲۸۷	۰.۰۵۲	۵.۵۱۹	<۰.۰۰۱	معنادار
حکمرانی داده ← مدیریت ریسک‌های حقوقی ← مقابله با نقض حریم خصوصی	۰.۱۹۹	۰.۰۳۸	۵.۲۳۷	<۰.۰۰۱	اثر غیرمستقیم معنادار
اثر کل حکمرانی داده بر مقابله با نقض حریم خصوصی	۰.۷۲۸	۰.۰۳۷	۱۹.۶۷۶	<۰.۰۰۱	معنادار

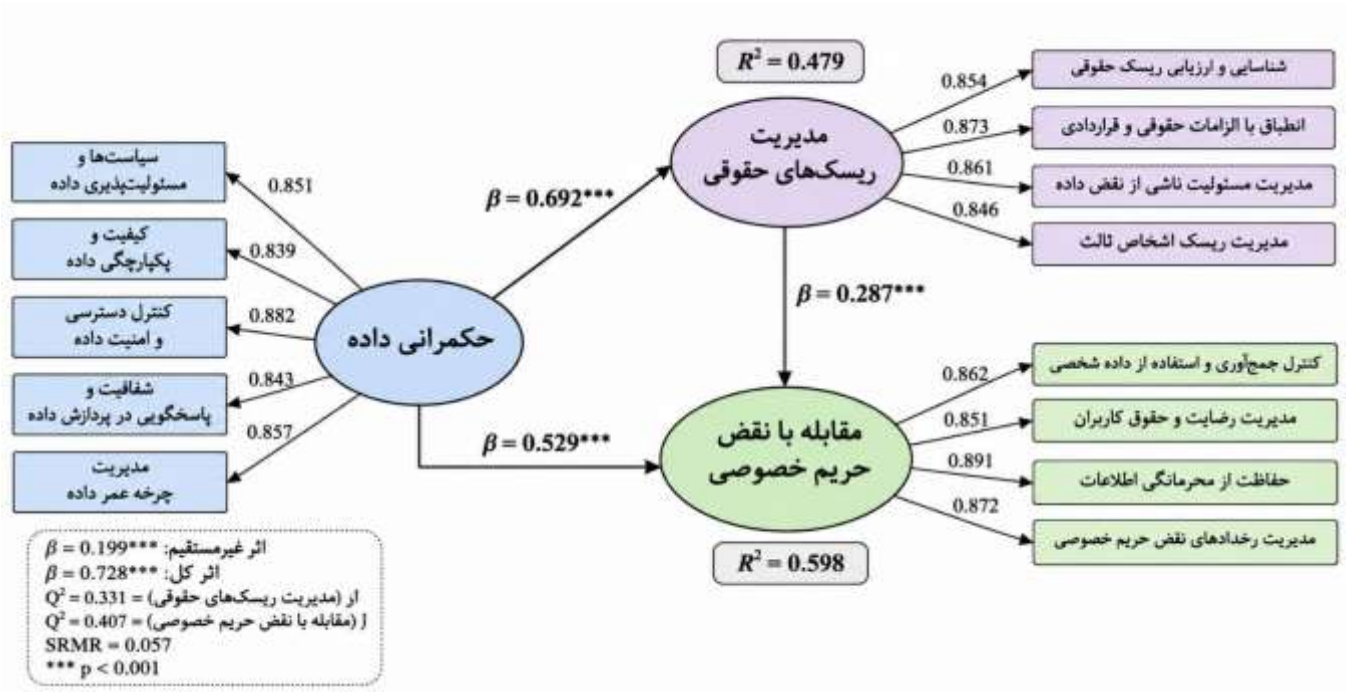
شاخص‌های تبیین و پیش‌بینی مدل: R^2 مدیریت ریسک‌های حقوقی = ۰.۴۷۹؛ R^2 مقابله با نقض حریم خصوصی = ۰.۵۹۸؛ Q^2 مدیریت ریسک‌های حقوقی = ۰.۳۳۱؛ Q^2 مقابله با نقض حریم خصوصی = ۰.۴۰۷؛ SRMR = ۰.۰۵۷.

نتایج مدل ساختاری ارائه‌شده در جدول ۴ نشان داد که حکمرانی داده اثر مثبت، مستقیم و معناداری بر مدیریت ریسک‌های حقوقی داشت. ضریب مسیر استانداردشده این رابطه برابر با ۰.۶۹۲ و مقدار t برابر با ۱۶.۸۷۸ بود که در سطح کمتر از ۰.۰۰۱ معنادار شد. این یافته نشان می‌دهد که بهبود ساختارهای حکمرانی داده با افزایش توان کسب‌وکارهای دیجیتال در شناسایی، ارزیابی، کنترل و مستندسازی ریسک‌های حقوقی همراه است. همچنین، حکمرانی داده اثر مستقیم معناداری بر مقابله با نقض حریم خصوصی داشت و ضریب مسیر آن برابر با ۰.۵۲۹ به دست آمد. این رابطه نیز با مقدار t برابر با ۱۱.۰۲۱ در سطح کمتر از ۰.۰۰۱ معنادار بود. بنابراین، حتی پس از در نظر گرفتن نقش مدیریت ریسک‌های حقوقی، حکمرانی داده به‌طور مستقل توان پیشگیری، کنترل و پاسخگویی سازمانی در برابر نقض حریم خصوصی را افزایش داد. مدیریت ریسک‌های حقوقی نیز اثر مثبت و معناداری بر مقابله با نقض حریم خصوصی داشت و ضریب مسیر آن ۰.۲۸۷ بود. این نتیجه نشان می‌دهد که سازمان‌هایی که دارای فرایندهای منسجم‌تر برای مدیریت مسئولیت‌های حقوقی، الزامات انطباق و ریسک‌های ناشی از پردازش داده هستند، در زمینه کنترل نقض‌های حریم خصوصی نیز عملکرد مؤثرتری دارند. افزون بر اثر مستقیم، اثر غیرمستقیم حکمرانی داده بر مقابله با نقض حریم خصوصی از طریق مدیریت ریسک‌های حقوقی برابر با ۰.۱۹۹ بود و این اثر با مقدار t برابر با ۵.۲۳۷ در سطح کمتر از ۰.۰۰۱ معنادار شد. با توجه به معناداری هم‌زمان اثر مستقیم و غیرمستقیم، مدیریت ریسک‌های حقوقی نقش میانجی جزئی در رابطه میان حکمرانی داده و مقابله با نقض حریم خصوصی ایفا کرد. اثر کل حکمرانی داده بر مقابله با نقض حریم خصوصی برابر با ۰.۷۲۸ به دست آمد که بیانگر نقش قابل توجه این سازه در تبیین ظرفیت سازمان برای حفاظت از داده‌های شخصی و کاهش احتمال نقض حریم خصوصی است. مقدار R^2 برای مدیریت ریسک‌های حقوقی برابر با ۰.۴۷۹ بود؛ به این معنا که ۴۷.۹ درصد از واریانس این متغیر توسط حکمرانی داده تبیین شد. مقدار R^2 مقابله با نقض حریم خصوصی نیز ۰.۵۹۸ به دست آمد و نشان داد که ۵۹.۸ درصد از تغییرات این متغیر به‌وسیله حکمرانی داده و مدیریت ریسک‌های حقوقی قابل تبیین بود. مقادیر Q^2 برابر با ۰.۳۳۱ برای مدیریت ریسک‌های حقوقی و ۰.۴۰۷ برای مقابله با نقض حریم خصوصی نیز نشان‌دهنده توان پیش‌بینی مناسب مدل بودند. همچنین، مقدار SRMR برابر با ۰.۰۵۷ بود که از برازش مطلوب مدل کلی حمایت کرد.

E-ISSN: 3041-8933

شکل ۱

مدل ساختاری نقش حکمرانی داده در مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی در کسب‌وکارهای دیجیتال



نتایج نمایش‌داده‌شده در شکل ۱ نشان می‌دهد که حکمرانی داده در مدل نهایی پژوهش دارای دو مسیر اثرگذاری بر مقابله با نقض حریم خصوصی است. نخست، یک مسیر مستقیم با ضریب استانداردشده ۰.۵۲۹ که بیانگر اثر مستقل حکمرانی داده بر ظرفیت سازمان برای حفاظت از داده‌های شخصی، مدیریت رضایت کاربران، کنترل دسترسی، کاهش استفاده غیرمجاز از داده و واکنش مناسب به رخدادهای نقض حریم خصوصی است. دوم، یک مسیر غیرمستقیم که از طریق مدیریت ریسک‌های حقوقی عمل می‌کند؛ به‌گونه‌ای که حکمرانی داده ابتدا با ضریب ۰.۶۹۲ مدیریت ریسک‌های حقوقی را تقویت کرده و مدیریت ریسک‌های حقوقی نیز با ضریب ۰.۲۸۷ موجب افزایش توان مقابله با نقض حریم خصوصی می‌شود. حاصل این مسیر غیرمستقیم برابر با ۰.۱۹۹ بود. ترکیب اثر مستقیم و غیرمستقیم موجب شد اثر کل حکمرانی داده بر مقابله با نقض حریم خصوصی به ۰.۷۲۸ برسد. این ساختار نشان می‌دهد که حکمرانی داده صرفاً مجموعه‌ای از کنترل‌های فنی یا سیاست‌های اجرایی مرتبط با داده نیست، بلکه از طریق ایجاد مسئولیت‌پذیری سازمانی، روشن کردن حدود صلاحیت و دسترسی، افزایش قابلیت مستندسازی تصمیمات، بهبود انطباق با الزامات حقوقی و ایجاد سازوکارهای پاسخگویی، زمینه لازم برای کاهش مخاطرات حقوقی مرتبط با داده را فراهم می‌کند. در عین حال، باقی ماندن اثر مستقیم معنادار حکمرانی داده پس از ورود مدیریت ریسک‌های حقوقی به مدل نشان می‌دهد که بخشی از نقش حکمرانی داده در حفاظت از حریم خصوصی از مسیرهایی فراتر از مدیریت رسمی ریسک حقوقی، از جمله کنترل‌های فنی، کیفیت داده، شفافیت در پردازش، محدودسازی دسترسی و مدیریت چرخه عمر داده اعمال می‌شود. در مجموع، الگوی نهایی مدل نشان داد که توسعه حکمرانی داده می‌تواند به‌عنوان یک سازوکار سازمانی مرکزی، هم به کاهش مواجهه کسب‌وکارهای دیجیتال با ریسک‌های حقوقی کمک کند و هم به‌طور مستقیم و غیرمستقیم احتمال وقوع و پیامدهای نقض حریم خصوصی را کاهش دهد.

بحث و نتیجه‌گیری

پژوهش حاضر با هدف ارزیابی نقش حکمرانی داده در مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی در کسب‌وکارهای دیجیتال انجام شد. نتایج نشان داد که حکمرانی داده اثر مثبت و معناداری بر مدیریت ریسک‌های حقوقی دارد و ضریب مسیر استانداردشده این رابطه برابر با ۰.۶۹۲ بود. همچنین، حکمرانی داده به‌طور مستقیم اثر مثبت و معناداری بر مقابله با نقض حریم خصوصی داشت و ضریب مسیر این رابطه ۰.۵۲۹ به دست آمد. از سوی دیگر، مدیریت ریسک‌های حقوقی نیز با ضریب ۰.۲۸۷ اثر مثبت و معناداری بر مقابله با نقض حریم خصوصی نشان داد. افزون بر این، اثر غیرمستقیم حکمرانی داده بر مقابله با نقض حریم خصوصی از طریق مدیریت ریسک‌های حقوقی برابر با ۰.۱۹۹ بود و معناداری آن نشان داد که مدیریت ریسک‌های حقوقی نقش میانجی جزئی در این رابطه ایفا می‌کند. اثر کل حکمرانی داده بر مقابله با نقض حریم خصوصی نیز ۰.۷۲۸ به دست آمد. مقدار ضریب تعیین نشان داد که حکمرانی داده ۴۷.۹ درصد از واریانس مدیریت ریسک‌های حقوقی را تبیین می‌کند و حکمرانی داده همراه با مدیریت ریسک‌های حقوقی قادر به تبیین ۵۹.۸ درصد از واریانس مقابله با نقض حریم خصوصی است. مقادیر Q^2 برای مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی نیز به‌ترتیب ۰.۳۳۱ و ۰.۴۰۷ بود که بیانگر توان پیش‌بینی مطلوب مدل است و مقدار SRMR برابر با ۰.۰۵۷ نیز از برازش مناسب مدل حمایت کرد.

نخستین یافته مهم پژوهش، اثر قوی حکمرانی داده بر مدیریت ریسک‌های حقوقی بود. این نتیجه نشان می‌دهد که هرچه کسب‌وکارهای دیجیتال دارای سیاست‌های روشن‌تر در زمینه مالکیت داده، مسئولیت‌پذیری، کنترل دسترسی، کیفیت داده، مدیریت چرخه عمر اطلاعات و شفافیت پردازش باشند، احتمال مواجهه آنان با مخاطراتی مانند استفاده غیرمجاز از داده، عدم انطباق قراردادی، ضعف در مستندسازی، نقض تعهدات مرتبط با داده و مسئولیت ناشی از افشای اطلاعات کاهش می‌یابد. این یافته با مطالعاتی همسو است که حکمرانی داده را نه صرفاً یک سازوکار فنی، بلکه بخشی از ساختار مدیریت ریسک و انطباق سازمانی می‌دانند. برای مثال، در مطالعات مربوط به انطباق مقرراتی در محیط‌های داده‌محور، تأکید شده است که سازمان‌ها باید الزامات حقوقی حفاظت از داده را به نقش‌ها، فرایندها و معماری سازمانی تبدیل کنند تا امکان ردیابی جریان داده و تعیین مسئولیت فراهم شود (Georgiadis & Poels, 2021). همچنین، چارچوب‌های امنیت سایبری نشان داده‌اند که سیاست‌های مؤثر سازمانی زمانی می‌توانند ریسک را کاهش دهند که به‌صورت هماهنگ با ساختار حکمرانی داده و قواعد پاسخگویی اجرا شوند (Mishra et al., 2022). از این منظر، نتیجه حاضر نشان می‌دهد که حکمرانی داده می‌تواند به‌عنوان لایه‌ای سازمانی عمل کند که کنترل‌های فنی، حقوقی و مدیریتی را در یک سازوکار منسجم به یکدیگر متصل می‌سازد.

این یافته همچنین با نتایج پژوهش‌هایی که بر نقش انطباق در محیط‌های دیجیتال تأکید دارند، سازگار است. در مطالعات مربوط به شهرهای هوشمند، نشان داده شده است که حفاظت از داده و امنیت اطلاعات زمانی اثربخش‌تر است که الزامات انطباق از مرحله طراحی در ساختارهای داده‌ای لحاظ شوند (Aslam et al., 2022). به همین ترتیب، در نظام بانکداری دیجیتال، وجود چارچوب‌های روشن برای جمع‌آوری، ذخیره، دسترسی و انتقال داده به‌عنوان یکی از عناصر اصلی کاهش مخاطرات حقوقی شناخته شده است (Yuspin et al., 2023). نتایج پژوهش حاضر نیز همین منطق را در بستر کسب‌وکارهای دیجیتال تأیید می‌کند؛ به این معنا که حکمرانی داده می‌تواند از طریق تعریف روشن مسئولیت‌ها، ایجاد کنترل‌های قابل ممیزی و مستندسازی تصمیمات، احتمال وقوع تخلف یا اختلاف حقوقی را کاهش دهد.

یافته دوم پژوهش نشان داد که حکمرانی داده به‌طور مستقیم بر مقابله با نقض حریم خصوصی اثر مثبت و معناداری دارد. این نتیجه از این دیدگاه حمایت می‌کند که حفاظت از حریم خصوصی صرفاً به اقدامات فنی مانند رمزنگاری یا کنترل دسترسی محدود نیست، بلکه نیازمند وجود ساختارهای حکمرانی است که تعیین کنند چه داده‌ای، با چه هدفی، توسط چه شخصی، برای چه مدتی و تحت چه شرایطی

E-ISSN: 3041-8933

پردازش شود. مطالعات انجام‌شده در زمینه داده‌های شخصی نیز بر اهمیت چنین رویکردی تأکید کرده‌اند. برای نمونه، پژوهش‌های مربوط به داده‌های شخصی در عصر دیجیتال نشان داده‌اند که توسعه ظرفیت‌های جمع‌آوری و ترکیب داده، بدون وجود چارچوب‌های شفاف پردازش، می‌تواند مرزهای حریم خصوصی را تضعیف کند (Nguyen & Le, 2024). در همین راستا، بررسی چارچوب‌های صنعتی حریم خصوصی نیز نشان داده است که مدیریت اشتراک‌گذاری داده و تعیین قواعد دسترسی میان سازمان‌ها از عناصر کلیدی حفاظت از حریم خصوصی محسوب می‌شود (Ghorashi et al., 2023).

اثر مستقیم حکمرانی داده بر حریم خصوصی با نتایج پژوهش‌های حوزه اخلاق داده نیز هماهنگ است. در صنایع گردشگری و مهمان‌نوازی، افزایش استفاده از داده‌های مشتریان برای تحلیل رفتار و شخصی‌سازی خدمات باعث شده است که اخلاق داده و حکمرانی داده به‌عنوان عناصر مکمل یکدیگر مطرح شوند (Yallop et al., 2021). در سطح اداره عمومی نیز بر این نکته تأکید شده است که امنیت داده و حریم خصوصی باید بخشی از ساختار پاسخگویی سازمانی باشد و مسئولیت آن تنها بر عهده واحد فناوری اطلاعات قرار نگیرد (Sari et al., 2024). یافته حاضر همین دیدگاه را تقویت می‌کند؛ زیرا نشان می‌دهد که سازوکارهای حکمرانی داده، مستقل از مدیریت ریسک حقوقی، می‌توانند به‌طور مستقیم ظرفیت سازمان را برای حفاظت از حریم خصوصی افزایش دهند.

این نتیجه همچنین با پژوهش‌های مربوط به خدمات مالی و پلتفرم‌های دیجیتال همخوان است. در مطالعات مربوط به خدمات وام آنلاین، ضعف در کنترل جمع‌آوری و استفاده از داده‌های شخصی به‌عنوان یکی از مهم‌ترین عوامل تهدیدکننده حریم خصوصی کاربران شناخته شده است (Ramadhan et al., 2024; Widi et al., 2021). همچنین، در حوزه تجارت الکترونیک و شبکه‌های اجتماعی، بر ضرورت تدوین سیاست‌های روشن برای استفاده از اطلاعات مشتریان و جلوگیری از بهره‌برداری غیرمجاز از داده تأکید شده است (Akbar et al., 2023; Mujtaba & Cavico, 2023). این یافته‌ها با نتیجه پژوهش حاضر سازگارند و نشان می‌دهند که حکمرانی داده می‌تواند با ایجاد محدودیت‌های روشن بر جمع‌آوری، استفاده و انتقال داده، احتمال نقض حریم خصوصی را کاهش دهد.

یافته سوم پژوهش نشان داد که مدیریت ریسک‌های حقوقی نیز به‌طور مثبت و معناداری بر مقابله با نقض حریم خصوصی اثر دارد. این نتیجه حاکی از آن است که سازمان‌هایی که دارای سازوکارهای مؤثر برای شناسایی ریسک، ارزیابی پیامدهای حقوقی، کنترل تعهدات قراردادی، مدیریت اشخاص ثالث و مستندسازی تصمیمات هستند، در مواجهه با مخاطرات حریم خصوصی نیز عملکرد بهتری دارند. این یافته با مطالعاتی که بر پیوند میان حقوق، حریم خصوصی و مدیریت سازمانی تأکید دارند، همسو است. پژوهش‌های حوزه حمایت از مصرف‌کننده در عصر دیجیتال نشان داده‌اند که حقوق کسب‌وکار می‌تواند از طریق ایجاد الزامات شفافیت، مسئولیت‌پذیری و جبران خسارت، نقش مؤثری در کاهش نقض حقوق کاربران ایفا کند (Widiarty & Tehupeiory, 2024). از سوی دیگر، مطالعات مرتبط با حفاظت از اطلاعات شخصی نشان داده‌اند که مشروعیت پردازش داده باید با انتظارات معقول افراد و منافع مشروع سازمان‌ها متوازن شود (Shen & Teng, 2022). بنابراین، مدیریت ریسک‌های حقوقی می‌تواند به‌عنوان حلقه واسطی میان سیاست‌های کلان حکمرانی داده و اجرای عملی الزامات حریم خصوصی عمل کند.

نقش میانجی مدیریت ریسک‌های حقوقی نیز یکی از مهم‌ترین نتایج پژوهش حاضر بود. اثر غیرمستقیم ۰.۱۹۹ نشان داد که بخشی از اثر حکمرانی داده بر مقابله با نقض حریم خصوصی از طریق کاهش و مدیریت مخاطرات حقوقی منتقل می‌شود. این یافته بدان معناست که حکمرانی داده علاوه بر اثر مستقیم بر کنترل‌های حریم خصوصی، از طریق تقویت انطباق، مستندسازی، پاسخگویی و کنترل مسئولیت‌های حقوقی، به بهبود حفاظت از حریم خصوصی کمک می‌کند. این نتیجه با دیدگاه‌هایی همسو است که حفاظت از داده را نتیجه تعامل هم‌زمان سازوکارهای حقوقی، مدیریتی و فنی می‌دانند. برای نمونه، در بررسی نظام‌های داده‌محور در شرکت‌های بین‌المللی، تأکید شده است که انطباق

حقوقی باید از مرحله طراحی مدل کسب‌وکار در فرایندهای داده‌ای گنجانده شود (Conde et al., 2025). همچنین، در چارچوب‌های هوش مصنوعی، نبود ساختار روشن برای منشأ داده، دسترسی، مسئولیت و رضایت می‌تواند همزمان به ریسک‌های حقوقی و نقض حریم خصوصی منجر شود (Pahune et al., 2025). بنابراین، میانجی‌گری مدیریت ریسک‌های حقوقی از نظر نظری نیز قابل توجیه است؛ زیرا انطباق حقوقی سازوکاری است که اصول کلی حکمرانی را به رفتارهای عملیاتی قابل کنترل تبدیل می‌کند.

اثر کل بالای حکمرانی داده بر مقابله با نقض حریم خصوصی، یعنی ۰.۷۲۸، اهمیت راهبردی این سازه را برجسته می‌کند. این مقدار نشان می‌دهد که حکمرانی داده نه یک عامل فرعی، بلکه یکی از مهم‌ترین متغیرهای تعیین‌کننده ظرفیت سازمان برای حفاظت از حریم خصوصی است. این نتیجه با مطالعاتی که بر ضرورت ایجاد تعادل میان استفاده اقتصادی از داده و حقوق کاربران تأکید کرده‌اند، همخوان است. در پژوهش‌های مربوط به مقررات حریم خصوصی، نشان داده شده است که استفاده صحیح از داده در چارچوب حکمرانی مناسب می‌تواند هم ارزش بنگاه را افزایش دهد و هم ریسک ناشی از مقررات را کاهش دهد (Yan & Cai, 2026). همچنین، در زمینه تعادل میان هوش مصنوعی، داده و حقوق مصرف‌کننده، بر این نکته تأکید شده است که بهره‌برداری اقتصادی از داده بدون حفاظت مؤثر از حقوق کاربران نمی‌تواند پایدار باشد (Vásquez & Alvarez-Orozco, 2026). این دیدگاه با یافته حاضر هماهنگ است و نشان می‌دهد که حکمرانی داده باید به‌عنوان یکی از عناصر اصلی راهبرد کسب‌وکارهای دیجیتال در نظر گرفته شود.

از سوی دیگر، معنادار بودن اثر مستقیم حکمرانی داده پس از ورود مدیریت ریسک‌های حقوقی به مدل نشان می‌دهد که تمامی اثرات حکمرانی داده از مسیر حقوقی عبور نمی‌کنند. بخشی از این اثر احتمالاً از طریق کنترل‌های فنی، کیفیت داده، محدودسازی دسترسی، نظارت بر چرخه عمر داده و شفافیت در پردازش اعمال می‌شود. این موضوع با مطالعات حوزه فناوری و حریم خصوصی سازگار است. در تحقیقات مربوط به حفاظت از حریم خصوصی در محیط‌های حساس، استفاده از تکنیک‌های فنی و معماری‌های مناسب در کنار الزامات حقوقی ضروری دانسته شده است (Majeed & Hwang, 2021). همچنین، در حوزه شناسه‌های زیست‌سنجی، تأکید شده است که مخاطرات حریم خصوصی صرفاً با قواعد حقوقی قابل کنترل نیستند و باید آثار ساختاری و فنی سامانه‌های داده نیز مدنظر قرار گیرند (Wodajo, 2024a, 2024b). ازاین‌رو، نتیجه حاضر بر ضرورت نگاه چندبعدی به حکمرانی داده تأکید دارد.

مقدار ۴۷.۹ درصد واریانس تبیین‌شده در مدیریت ریسک‌های حقوقی نیز نشان‌دهنده قدرت قابل توجه حکمرانی داده در توضیح این متغیر است. این نتیجه بیانگر آن است که تقریباً نیمی از تفاوت در توانایی کسب‌وکارهای دیجیتال برای مدیریت ریسک‌های حقوقی را می‌توان با تفاوت در کیفیت حکمرانی داده توضیح داد. این مقدار از منظر مدیریتی قابل توجه است و نشان می‌دهد که سیاست‌های داده، نقش‌ها و کنترل‌های داخلی می‌توانند مستقیماً بر عملکرد حقوقی سازمان اثر بگذارند. در مطالعات مربوط به رقابت و اقتصاد دیجیتال نیز بر اهمیت چارچوب‌های مدیریت داده برای جلوگیری از سوءاستفاده و کاهش تعارضات حقوقی تأکید شده است (Mushtaq et al., 2024). همچنین، در زمینه تنظیم‌گری داده و تجارت بین‌الملل، پیچیدگی‌های حقوقی ناشی از تفاوت حوزه‌های قضایی نشان داده‌اند که سازمان‌ها باید سازوکارهای داخلی منسجمی برای انطباق ایجاد کنند (Igbinenikaro & Adewusi, 2024; Sharma et al., 2026).

تبیین ۵۹.۸ درصد از واریانس مقابله با نقض حریم خصوصی نیز نشان‌دهنده قدرت نسبتاً بالای مدل پژوهش است. این نتیجه حاکی از آن است که حکمرانی داده و مدیریت ریسک‌های حقوقی در کنار یکدیگر می‌توانند بخش قابل توجهی از توان سازمان برای پیشگیری و مقابله با نقض حریم خصوصی را توضیح دهند. البته باقی ماندن حدود ۴۰ درصد واریانس تبیین‌نشده نشان می‌دهد که متغیرهای دیگری نظیر فرهنگ امنیتی، بلوغ فناوری، سطح آگاهی کارکنان، ساختار سازمانی، نوع صنعت و شدت نظارت مقرراتی نیز احتمالاً بر این متغیر اثر دارند. این برداشت با مطالعاتی که بر نقش تعامل میان بازیگران مختلف در حفاظت از حقوق داده تأکید کرده‌اند، همخوان است (Li & Guo, 2023).

E-ISSN: 3041-8933

همچنین، استفاده از تنظیم‌گری مشترک و مشارکت نهادهای صنعتی می‌تواند بخشی از عوامل بیرونی مؤثر بر حفاظت از داده را توضیح دهد (Suleiman et al., 2022).

در مجموع، نتایج این پژوهش نشان می‌دهد که حکمرانی داده باید به‌عنوان یک سازوکار راهبردی و چندبعدی در کسب‌وکارهای دیجیتال در نظر گرفته شود. این مفهوم هم‌زمان بر کیفیت تصمیم‌گیری، انطباق حقوقی، امنیت داده، پاسخگویی، اعتماد کاربران و حفاظت از حریم خصوصی اثر می‌گذارد. در شرایطی که توسعه هوش مصنوعی و پلتفرم‌های دیجیتال سرعت گرفته است، اتکا به چارچوب‌های اخلاقی بدون ضمانت اجرایی کافی نخواهد بود (Haidar, 2026). همچنین، تحولات سریع فناوری نشان می‌دهد که قواعد حقوقی باید همراه با ساختارهای انعطاف‌پذیر سازمانی به‌روز شوند (Ruan, 2024). بر این اساس، حکمرانی داده می‌تواند نقش حلقه اتصال میان فناوری، مدیریت و حقوق را ایفا کند و از این طریق به کاهش ریسک و افزایش اعتماد در محیط کسب‌وکار دیجیتال کمک نماید.

پژوهش حاضر با چند محدودیت همراه بود که باید در تفسیر یافته‌ها مورد توجه قرار گیرد. نخست، مطالعه به‌صورت مقطعی انجام شد و داده‌ها در یک مقطع زمانی گردآوری شدند؛ بنابراین، اگرچه روابط معناداری میان حکمرانی داده، مدیریت ریسک‌های حقوقی و مقابله با نقض حریم خصوصی مشاهده شد، استنباط قطعی روابط علّی باید با احتیاط صورت گیرد. دوم، جامعه پژوهش به مدیران، کارشناسان و متخصصان کسب‌وکارهای دیجیتال شهر تهران محدود بود و ممکن است ویژگی‌های محیط حقوقی، سازمانی و فناوری این کسب‌وکارها با سایر شهرها یا کشورها متفاوت باشد؛ ازاین‌رو، تعمیم نتایج به سایر محیط‌ها نیازمند احتیاط است. سوم، داده‌ها براساس پرسشنامه خودگزارشی جمع‌آوری شدند و احتمال وجود سوگیری مطلوبیت اجتماعی یا تفاوت میان ادراک پاسخ‌دهندگان و عملکرد واقعی سازمان وجود دارد. چهارم، مطالعه حاضر بر سه سازه اصلی تمرکز داشت و عواملی مانند فرهنگ امنیت اطلاعات، بلوغ دیجیتال، حمایت مدیریت ارشد، آموزش کارکنان، شدت مقررات‌گذاری، ساختار مالکیت و اندازه سازمان وارد مدل نشدند. افزون بر این، تفاوت میان صنایع مختلف دیجیتال نیز به‌صورت جداگانه مورد بررسی قرار نگرفت و ممکن است شدت روابط مشاهده‌شده در حوزه‌هایی مانند بانکداری دیجیتال، تجارت الکترونیک، سلامت دیجیتال و پلتفرم‌های مبتنی بر هوش مصنوعی متفاوت باشد.

پیشنهاد می‌شود در پژوهش‌های آینده از طرح‌های طولی استفاده شود تا تغییرات حکمرانی داده و پیامدهای حقوقی آن در طول زمان بررسی و جهت روابط میان متغیرها با دقت بیشتری مشخص شود. همچنین، تکرار این مطالعه در سایر شهرها، کشورها و محیط‌های حقوقی متفاوت می‌تواند امکان مقایسه میان نظام‌های مقرراتی و فرهنگی را فراهم سازد. بررسی مدل در صنایع خاص مانند بانکداری دیجیتال، فین‌تک، سلامت دیجیتال، تجارت الکترونیک، پلتفرم‌های شبکه اجتماعی و سامانه‌های هوش مصنوعی نیز می‌تواند تفاوت‌های بخشی را آشکار کند. پیشنهاد می‌شود متغیرهایی مانند بلوغ امنیت سایبری، فرهنگ سازمانی، سواد حریم خصوصی کارکنان، حمایت مدیریت ارشد، اعتماد کاربران، شدت مقررات‌گذاری و کیفیت کنترل‌های اشخاص ثالث به‌عنوان میانجی یا تعدیل‌گر در مدل‌های آینده وارد شوند. استفاده از داده‌های عینی، مانند تعداد رخدادهای نقض داده، شکایات حریم خصوصی، پرونده‌های حقوقی، نتایج ممیزی و میزان خسارت‌های مرتبط با داده، در کنار پرسشنامه می‌تواند اعتبار یافته‌ها را افزایش دهد. همچنین، انجام پژوهش‌های کیفی با مدیران حقوقی، مسئولان حفاظت از داده و کارشناسان امنیت اطلاعات می‌تواند به شناسایی سازوکارهای عمیق‌تر اثرگذاری حکمرانی داده بر ریسک‌های حقوقی کمک کند.

بر اساس یافته‌های پژوهش، پیشنهاد می‌شود کسب‌وکارهای دیجیتال حکمرانی داده را به‌عنوان بخشی از راهبرد کلان سازمان و نه صرفاً مسئولیت واحد فناوری اطلاعات در نظر گیرند. لازم است مسئولیت مالکیت، نگهداری، دسترسی، پردازش و حذف داده به‌طور شفاف میان واحدهای مختلف تعریف شود و برای هر فرایند داده‌ای فرد یا واحد پاسخگو تعیین گردد. تدوین سیاست‌های روشن برای طبقه‌بندی داده، کنترل دسترسی، مدیریت رضایت کاربران، نگهداری و حذف اطلاعات و اشتراک‌گذاری داده با اشخاص ثالث باید در اولویت قرار گیرد. همچنین،

پیشنهاد می‌شود واحدهای حقوقی، مدیریت ریسک، امنیت اطلاعات و فناوری به‌صورت یکپارچه در طراحی و ارزیابی فرایندهای داده مشارکت داشته باشند. انجام ارزیابی‌های دوره‌ای ریسک حریم خصوصی، ممیزی انطباق، ثبت و مستندسازی تصمیمات داده‌ای و طراحی سازوکارهای سریع برای پاسخ به رخدادهای نقض داده می‌تواند ریسک‌های حقوقی و عملیاتی را کاهش دهد. آموزش مستمر کارکنان درباره مسئولیت‌های مرتبط با داده و حریم خصوصی نیز ضروری است. علاوه بر این، سازمان‌ها باید قراردادهای خود با ارائه‌دهندگان خدمات ابری، پیمانکاران، پلتفرم‌های تبلیغاتی و سایر اشخاص ثالث را از نظر تعهدات مرتبط با حفاظت از داده بازبینی کنند و شاخص‌های مشخصی برای پایش عملکرد آنان در نظر گیرند. در نهایت، توصیه می‌شود اصول حریم خصوصی و حکمرانی داده از مرحله طراحی محصولات و خدمات دیجیتال در فرایندهای کسب‌وکار ادغام شوند تا حفاظت از داده به‌صورت پیشگیرانه و نه صرفاً پس از وقوع تخلف یا حادثه انجام گیرد.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

موازین اخلاقی

در انجام این پژوهش تمامی موازین و اصول اخلاقی رعایت گردیده است.

شفافیت داده‌ها

داده‌ها و مآخذ پژوهش حاضر در صورت درخواست از نویسنده مسئول و ضمن رعایت اصول کپی رایت ارسال خواهد شد.

حامی مالی

این پژوهش حامی مالی نداشته است.

References

Akbar, R. A., Mulyana, A., & Amalia, M. (2023). Legal Challenges in the Age of Social Media: Protecting Citizens From Misuse of Information. *Golden Ratio of Law and Social Policy Review*, *3*(1), 14-25. https://doi.org/10.52970/grlspr.v3i1.328

Aslam, M., Abbasi, M. A. K., Khalid, T., Shan, R. u., Ullah, S., Ahmad, T., Saeed, S., Alabbad, D. A., & Ahmad, R. (2022). Getting Smarter About Smart Cities: Improving Data Security and Privacy Through Compliance. *Sensors*, *22*(23), 9338. https://doi.org/10.3390/s22239338

Conde, I. C., Li, Y., & Vyas, R. P. (2025). Global Companies and China’s Data Privacy Laws: Analysing DIDI'S Case and Regulatory Compliance Implications. *Chinese Journal of Transnational Law*, *2*(1), 60-81. https://doi.org/10.1177/2753412x241288770

Georgiadis, G., & Poels, G. (2021). Enterprise Architecture Management as a Solution for Addressing General Data Protection Regulation Requirements in a Big Data Context: A Systematic Mapping Study. *Information Systems and e-Business Management*, *19*(1), 313-362. https://doi.org/10.1007/s10257-020-00500-5

E-ISSN: 3041-8933

Ghorashi, S. R., Zia, T., Bewong, M., & Jiang, Y. (2023). An Analytical Review of Industrial Privacy Frameworks and Regulations for Organisational Data Sharing. *Applied Sciences*, *13*(23), 12727. https://doi.org/10.3390/app132312727

Haidar, A. (2026). Ethics Without Teeth? Challenges and Opportunities in AI Declarations for Platform Governance. *Journal of Theoretical and Applied Electronic Commerce Research*, *21*(4), 103. https://doi.org/10.3390/jtaer21040103

Igbinenikaro, E., & Adewusi, A. O. (2024). Navigating the Legal Complexities of Artificial Intelligence in Global Trade Agreements. *International Journal of Applied Research in Social Sciences*, *6*(4), 488-505. https://doi.org/10.51594/ijarss.v6i4.987

Kadiri, A., & Boamah, E. F. (2025). Contextual Integrity in Africa's Plural-Legal Contexts: Fintech, Privacy, and Informational Norms in Ghana. *Big Data & Society*, *12*(2). https://doi.org/10.1177/20539517251351330

Li, X., & Guo, X. (2023). A Tripartite Evolutionary Game Analysis of Sports Data Rights Protection From the Perspective of Stakeholder. *PLoS One*, *18*(11), e0292914. https://doi.org/10.1371/journal.pone.0292914

Majeed, A., & Hwang, S. O. (2021). A Comprehensive Analysis of Privacy Protection Techniques Developed for COVID-19 Pandemic. *IEEE Access*, *9*, 164159-164187. https://doi.org/10.1109/access.2021.3130610

Mishra, A., Alzoubi, Y. I., Gill, A. Q., & Anwar, M. J. (2022). Cybersecurity Enterprises Policies: A Comparative Study. *Sensors*, *22*(2), 538. https://doi.org/10.3390/s22020538

Mujtaba, B. G., & Cavico, F. J. (2023). E-Commerce and Social Media Policies in the Digital Age: Legal Analysis and Recommendations for Management. *Journal of Entrepreneurship and Business Venturing*, *3*(1). https://doi.org/10.56536/jebv.v3i1.37

Mushtaq, S. A., Baig, K., Hassan, S., & Ahmad, W. (2024). The Importance of China's Competition Law in the Management of Data in the Country's Rapidly Developing Digital Economy: Policy Recommendations for Pakistan. *Current Trends in Law and Society*, *4*(1), 27-51. https://doi.org/10.52131/ctls.2024.0401.0030

Nguyen, L. M., & Le, T.-L. (2024). Personal Data in the Digital Age: An Overview Study in Vietnam. *Journal of Law and Sustainable Development*, *12*(3), e2623. https://doi.org/10.55908/sdgs.v12i3.2623

Oecd. (2022). Responding to Societal Challenges With Data. https://doi.org/10.1787/2182ce9f-en

Pahune, S. A., Akhtar, Z., Mandapati, V., & Siddique, K. (2025). The Importance of AI Data Governance in Large Language Models. *Big Data and Cognitive Computing*, *9*(6), 147. https://doi.org/10.3390/bdcc9060147

Ramadhan, M. T. A., Fitri, W., & Agustianto, A. (2024). Consumer Data Protection Amidst the Rise of Online Loan Services: Safeguarding Personal Data Privacy. *Legal Spirit*, *8*(2), 453-462. https://doi.org/10.31328/ls.v8i2.5502

Rezaeikhonakdar, D. (2023). AI Chatbots and Challenges of HIPAA Compliance for AI Developers and Vendors. *The Journal of Law Medicine & Ethics*, *51*(4), 988-995. https://doi.org/10.1017/jme.2024.15

Roy, D. G. (2021). Digital Privacy Concerns in India for Medical Tourism. *Journal of Public Affairs*, *22*(S1). https://doi.org/10.1002/pa.2762

Ruan, X. (2024). Analysis on the Predicament of Future Law and Its Solution Under the Background of Artificial Intelligence. https://doi.org/10.3233/faia231505

Sari, J. A., Yuliani, I., Akadira, T., Sunarya, A., & Ating, R. (2024). Data Security and Individual Privacy From the Perspective of Public Administration. *Ilomata International Journal of Social Science*, *5*(3), 818-830. https://doi.org/10.61194/ijss.v5i3.1297

Sharma, S., Myers, E., Carli, L. D., Banerjee, R., & Ray, I. (2026). Local Privacy Laws in a Globalized World. 193-204. https://doi.org/10.1145/3800506.3803491

Shen, Z., & Teng, X. (2022). Personal Information Protection and Interest Balance Based on Rational Expectation in the Era of Big Data. *International Review for Spatial Planning and Sustainable Development*, *10*(1), 1-23. https://doi.org/10.14246/irspsd.10.1_1

Suleiman, A., Audrine, P., & Dewaranu, T. (2022). Co-Regulation in Protecting Personal Data: The Role of Industry Associations as Potential Self-Regulatory Organizations. https://doi.org/10.35497/555905

Vásquez, J. W., & Alvarez-Orozco, R. (2026). Balancing AI Data and Consumer Rights: The Colombian Context. *Latin American Policy*, *17*(3). https://doi.org/10.1111/lamp.70062

Wang, S., & Liu, Y. (2023). A Study on the Optimisation of the Rule of Law Path for Digital Government. *Journal of Education Humanities and Social Sciences*, *20*, 142-150. https://doi.org/10.54097/ehss.v20i.11437

Widi, F., Qahar, A., & Aswari, A. (2021). Legal Protection Against Personal Data in Online Loan Transactions. *Golden Ratio of Law and Social Policy Review*, *1*(1), 17-25. https://doi.org/10.52970/grlspr.v1i1.152

Widiarty, W. S., & Tehupeiory, A. (2024). The Role of Business Law in Improving Consumer Protection in the Digital Age. *Journal of Law and Sustainable Development*, *12*(2), e3137. https://doi.org/10.55908/sdgs.v12i2.3137

Wodajo, K. K. (2024a). Societal and Structural Risks of Biometric ID: Towards People's Right to Privacy. https://doi.org/10.2139/ssrn.4993105

Wodajo, K. K. (2024b). Societal and Structural Risks of Biometric ID: Towards People's Right to Privacy. *Science Technology and Society*, *29*(4), 614-631. https://doi.org/10.1177/09717218241281941

Yallop, A. C., Gică, O. A., Moisescu, O. I., Coroș, M. M., & Séraphin, H. (2021). The Digital Traveller: Implications for Data Ethics and Data Governance in Tourism and Hospitality. *Journal of Consumer Marketing*, *40*(2), 155-170. https://doi.org/10.1108/jcm-12-2020-4278

Yan, Z., & Cai, X. (2026). How Big Data Enhances Firm Value Under Data Privacy Regulation. *Journal of Global Information Management*, *34*(1), 1-22. https://doi.org/10.4018/jgim.404387

Yuspin, W., Wardiono, K., Nurrahman, A., & Budiono, A. (2023). Personal Data Protection Law in Digital Banking Governance in Indonesia. *Studia Iuridica Lublinensia*, *32*(1), 99-130. https://doi.org/10.17951/sil.2023.32.1.99-130

Zubko, A., Sokiran, M., Danylenko, A., Левченко, Д., & Oksin, V. (2024). Determining the Nature of Digital Communication in Public Law Sphere. *International Journal of Religion*, *5*(5), 568-575. https://doi.org/10.61707/c4xc0981

E-ISSN: 3041-8933