Sciences and Techniques of
Information Management
Volume 12, Issue 1, 2026
https://stim.qom.ac.ir

Proposed Model for Data Governance Implementation with an Emphasis on Privacy

Morteza Mahmodi Parchini[1], **Ladan Riazi**[2]✉, **Alireza Porebrahimi**[3] and **Seyed Abdollah Amin Mousavi**[4]

1. Department of Information Technology Management, Kish International Branch, Islamic Azad University, Kish, Iran. Email: morteza.mahmodiparchini@iau.ir
2. Department of Information Technology Management, School of Management and Economics, Science and Research Branch, Islamic Azad University, Tehran, Iran. Email: l.riazi@gmail.com
3. Department of Industrial Management, Faculty of Management, Islamic Azad University, Karaj Branch, Karaj, Iran. Email: poorebrahimi@gmail.com.
4. Department of Information Technology, Central Tehran Branch, Islamic Azad University, Tehran, Iran. Email: saa.mousavi@iau.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 2025/10/15
Received in revised form: 2025/12/08
Accepted: 2026/02/26
Published online: 2026/03/30

Keywords:
Data governance, Privacy, Governance model, GDPR, Data policy.

ABSTRACT

Objective: In the contemporary digital landscape, data governance stands as a critical challenge in both IT policy and technology law. Given the increasing volume of personal data processing and exchange, the necessity for a localized data governance framework, tailored to a country's specific legal and technological infrastructure, is more pressing than ever. This study proposes a data governance model with a strong emphasis on privacy, addressing current challenges and providing practical solutions for improving personal data management. The primary objective is to develop a localized data governance framework for Iran, aligned with international standards such as the GDPR and the CCPA. By analyzing legal gaps, implementation challenges, and potential solutions, this study aims to establish a practical framework that not only enhances security and privacy protection but also fosters public trust in digital services.

Methodology: This applied-developmental study utilizes a mixed-methods approach. In the qualitative phase, legal documents, regulatory policies, and existing data governance models from Iran and other countries were analyzed. Furthermore, the Delphi method was employed to collect and examine the insights of 58 experts in technology, digital law, and information security. In the quantitative phase, Confirmatory Factor Analysis (CFA) was applied to validate the proposed model. Data were gathered through semi-structured expert interviews, a review of domestic laws and policies, and comparative studies with international frameworks. Key model indicators were extracted using qualitative content analysis, and statistical tests were employed to assess the model's validity and reliability.

Findings: Results indicate that the primary challenges to data governance in Iran include the lack of an integrated legal framework, the absence of an independent regulatory body, and deficiencies in the enforcement of data protection policies. A comparative analysis with the European GDPR and the U.S. CCPA revealed that Iran lacks clear requirements for data processing transparency and independent oversight—two pillars of international standards. Furthermore, findings indicate high levels of privacy concern among Iranian users; 78% expressed anxiety regarding how their data is managed on domestic platforms. The proposed model comprises three dimensions (legal-policy, technical-technological, and organizational-regulatory), six components, and 24 operational indicators. Data analysis demonstrated that implementing this model could reduce privacy violations

by 30.8%, increase user trust in digital services by 44.6%, and improve regulatory efficiency by 38.2%.

Conclusion: Data governance in Iran requires a transparent and binding framework that enhances security and user data protection while improving database interoperability and the efficiency of regulatory institutions. This study underscores that drafting comprehensive data governance legislation and establishing an independent regulatory body are critical steps. Additionally, implementing robust security policies, advanced encryption, and revising laws related to data collection and processing can mitigate cybercrimes and bolster public trust. A comparative analysis shows that the proposed model possesses a high degree of adaptability to global standards, suggesting that its proper implementation could enhance data protection standards by up to 79.4%. Ultimately, this research highlights the urgent need to reform data governance policies, enact new regulations, and increase transparency in personal data management. Future studies should focus on evaluating the practical implementation of this model within both public and private sectors.

Cite this article: Mahmodi Parchini, M., & et al. (2026)., Proposed Model for Data Governance Implementation with an Emphasis on Privacy. *Science and Technology of Information Management*, 12 (1). 111-123.
DOI: https://doi.org/10.22091/stim.2025.12492.2221

DOI: 10.22091/stim.2025.12492.2221
Publisher: University of Qom

علوم و فنون مدیریت اطلاعات

دوره ۱۲، شماره ۱، ۱۴۰۵

https://stim.qom.ac.ir

مدل پیشنهادی برای استقرار حکمرانی داده‌ها با تأکید بر حریم خصوصی

مرتضی محمودی پرچینی[۱]، لادن ریاضی[۲]✉، علیرضا پورابراهیمی[۳] و سیدعبداله امین موسوی[۴]

۱. دانشجوی دکترا، گروه مدیریت فناوری اطلاعات، واحد بین المللی کیش، دانشگاه آزاد اسلامی، کیش، ایران. رایانامه: morteza.mahmodiparchini@iau.ir

۲. استاد گروه مدیریت فناوری اطلاعات، دانشکده مدیریت و اقتصاد، واحد علوم و تحقیقات، دانشگاه آزاد اسلامی، تهران، ایران (نویسنده مسئول). رایانامه: l.riazi@gmail.com

۳. استاد گروه مدیریت صنعتی، دانشکده مدیریت، دانشگاه آزاد اسلامی، واحد کرج، دانشگاه آزاد اسلامی، واحد کرج، ایران. رایانامه: poorebrahimi@gmail.com

۴. استادیار گروه مدیریت فناوری اطلاعات، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: saa.mousavi@iau.ac.ir

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۷/۲۳

تاریخ بازنگری: ۱۴۰۴/۰۹/۱۷

تاریخ پذیرش: ۱۴۰۴/۱۲/۰۷

تاریخ انتشار: ۱۴۰۵/۰۱/۱۰

کلیدواژه‌ها:
حکمرانی داده‌ها، حریم خصوصی، مدل حکمرانی داده، GDPR، سیاست‌گذاری داده.

چکیده

هدف: در دنیای دیجیتال امروز، حکمرانی داده‌ها یکی از مهمترین چالش‌های سیاست‌گذاری و حقوق فناوری اطلاعات است. با افزایش پردازش و تبادل داده‌های شخصی، نیاز به چارچوبی بومی برای حکمرانی داده‌ها که متناسب با زیرساخت‌های قانونی و فناوری کشور باشد، بیش‌ازپیش احساس می‌شود. این پژوهش، مدلی پیشنهادی برای حکمرانی داده‌ها با تأکید بر حریم خصوصی ارائه می‌دهد. مدل یادشده با بررسی چالش‌های موجود، برای بهبود مدیریت داده‌های شخصی راهکارهای اجرایی را پیشنهاد می‌کند. هدف اصلی پژوهش، ارائهٔ الگویی بومی برای حکمرانی داده در ایران و تطبیق آن با استانداردهای بین‌المللی مانند مقررات عمومی حفاظت از داده‌ها و قانون حفظ حریم خصوصی مصرف‌کنندگان کالیفرنیا است. این مطالعه با تحلیل شکاف‌های قانونی، مشکلات اجرایی، و راهکارهای کاربردی، چارچوبی عملیاتی برای مدیریت داده‌ها ارائه می‌کند که می‌تواند امنیت و حریم خصوصی را افزایش دهد و موجب تقویت اعتماد عمومی به خدمات دیجیتال شود.

روش: پژوهش حاضر از نوع کاربردی-توسعه‌ای با رویکرد ترکیبی (کمّی و کیفی) است. در بخش کیفی، اسناد حقوقی، سیاست‌های تنظیم‌گری، و مدل‌های حکمرانی داده در ایران و کشورهای دیگر تحلیل شدند. با استفاده از روش دلفی، نظرات ۵۸ متخصص در حوزه‌های فناوری، حقوق دیجیتال، و امنیت اطلاعات گردآوری و تحلیل شد. در بخش کمّی، تحلیل عاملی تأییدی برای اعتبارسنجی مدل به کار رفت. داده‌ها با مصاحبه‌های نیمه‌ساختاریافته، تحلیل قوانین داخلی، و مقایسهٔ تطبیقی با چارچوب‌های بین‌المللی گردآوری شد.

یافته‌ها: یافته‌ها نشان می‌دهد که در ایران، نبود چارچوب قانونی یکپارچه، نهاد نظارتی مستقل، و ضعف در اجرای سیاست‌های حفاظت از داده، از چالش‌های اصلی حکمرانی داده هستند. مدل پیشنهادی شامل سه بُعد (حقوقی-سیاستی، فنی-فناورانه، سازمانی-نظارتی)، شش مؤلفهٔ کلیدی، و ۲۴ شاخص اجرایی است. تحلیل داده‌ها نشان داد که اجرای مدل پیشنهادی می‌تواند میزان نقض حریم خصوصی را تا ۳۰ درصد کاهش دهد و اعتماد کاربران به خدمات دیجیتال را تا ۴۵ درصد افزایش دهد.

نتیجه‌گیری: برای بهبود وضعیت حکمرانی داده در ایران، تدوین قانون جامع، ایجاد نهاد نظارتی مستقل، و شفافیت در سیاست‌های جمع‌آوری داده ضروری است. مقایسهٔ مدل پیشنهادی با استانداردهای بین‌المللی، نشان‌دهندهٔ سازگاری بالای آن است و اجرای مؤثر آن می‌تواند استانداردهای حفاظت از داده را تا ۸۰ درصد ارتقاء دهد.

استناد: محمودی پرچینی، مرتضی و دیگران. (۱۴۰۵). «مدل پیشنهادی برای استقرار حکمرانی داده‌ها با تأکید بر حریم خصوصی». *علوم و فنون مدیریت اطلاعات*. دورهٔ ۱۲. شمارهٔ ۱. ص: ۱۲۳-۱۱۱. https://doi.org/10.22091/stim.2025.12492.2221

ناشر: دانشگاه قم

۱. مقدّمه

در عصر دیجیتال، داده‌ها به یکی از مهمترین دارایی‌های اقتصادی، اجتماعی، و حاکمیتی تبدیل شده‌اند. رشد فناوری‌هایی همچون اینترنت اشیا، هوش مصنوعی، و کلان‌داده‌ها موجب افزایش چشمگیر تولید، جمع‌آوری، و پردازش اطلاعات شده است. این تحوّلات، علاوه‌بر ایجاد فرصت‌های گسترده در حوزهٔ نوآوری و بهینه‌سازی تصمیم‌گیری، چالش‌های مهمی را در زمینهٔ امنیت اطلاعات[۱]، حریم خصوصی[۲]، و حکمرانی داده‌ها به‌همراه داشته است.

در سطح بین‌المللی، کشورهای پیشرو چارچوب‌های مشخصی را برای حکمرانی داده‌ها تدوین کرده‌اند. مقررات عمومی حفاظت از داده‌ها[۳] در اتحادیهٔ اروپا، قانون حفظ حریم خصوصی مصرف‌کنندگان کالیفرنیا[۴] در ایالات متحده، و قوانین مشابه در سایر کشورها نشان‌دهندهٔ تلاش گسترده برای تنظیم‌گری داده‌ها و تضمین حقوق کاربران است. پژوهش‌ها نشان داده‌اند که اجرای این مقررات، علاوه بر کاهش نقض داده‌ها[۵]، موجب افزایش اعتماد عمومی به زیرساخت‌های دیجیتال شده است. برای مثال، پس از اجرای مقررات عمومی حفاظت از داده‌ها در اروپا، میزان نقض داده‌ها ۲۵٪ کاهش یافته و سطح اعتماد کاربران به خدمات دیجیتال ۴۵٪ افزایش پیدا کرده است (کمیسیون اروپا، ۲۰۲۰)[۶].

با این حال، ایران همچنان فاقد یک نظام حکمرانی داده‌ی منسجم و کارآمد است. قوانین موجود همچون قانون جرایم رایانه‌ای، قانون تجارت الکترونیک، و سند الزامات شبکه ملی اطلاعات، به دلیل پراکندگی، نبود انسجام، و نبود ضمانت اجرایی کافی، نتوانسته‌اند چارچوبی جامع برای مدیریت داده‌ها و حفاظت از حریم خصوصی فراهم کنند. این خلأ قانونی و نظارتی، زمینه‌ساز افزایش موارد نقض حریم خصوصی، سوءاستفاده از اطلاعات شخصی، و کاهش اعتماد عمومی به خدمات دیجیتال داخلی شده است. مطالعات نشان می‌دهد که ۷۸٪ از کاربران ایرانی نسبت به نحوهٔ استفاده و ذخیره‌سازی داده‌های شخصی خود در پلتفرم‌های داخلی نگرانی دارند. همچنین، ۵۳٪ از کسب‌وکارهای دیجیتال فاقد سیاست‌های مشخصی برای حفاظت از اطلاعات مشتریان خود هستند، که این امر خطر سوءاستفاده از داده‌ها و افزایش جرایم سایبری را تشدید کرده است. علاوه‌بر این، در ۹۲٪ از موارد نقض داده‌ها، هیچ پیگیری قانونی انجام نشده است که نشان‌دهندهٔ ضعف نظارتی در این حوزه است (انصاری و عطار، ۱۳۹۶).

این چالش‌ها نه‌تنها موجب کاهش اعتماد عمومی به خدمات دیجیتال داخلی شده‌اند، بلکه بر رشد اقتصاد دیجیتال و امنیت سایبری را نیز تأثیر داشته‌اند. کسب‌وکارهای دیجیتال در غیاب یک چارچوب حقوقی مشخص، با ابهامات حقوقی روبه‌رو هستند و قادر به پیاده‌سازی سیاست‌های حفاظت از داده‌ها نیستند. در این راستا، ایجاد یک نظام حکمرانی دادهٔ شفاف و کارآمد می‌تواند علاوه‌بر رفع این چالش‌ها، بستری امن برای توسعهٔ اقتصاد دیجیتال و افزایش امنیت داده‌ها فراهم کند.

بر این اساس، پژوهش حاضر در تلاش است تا با بررسی تطبیقی[۷] استانداردهای بین‌المللی و تحلیل وضعیت حکمرانی داده‌ها در ایران، مدلی پیشنهادی ارائه دهد که بتواند با کاهش خلأهای قانونی، افزایش شفافیت نظارتی، و تقویت امنیت داده‌ها، به بهبود حکمرانی داده‌ها در کشور کمک کند.

پژوهش‌های متعددی در سطح بین‌المللی و داخلی به بررسی اصول، چالش‌ها، و راهکارهای حکمرانی داده پرداخته‌اند. با این حال، در ایران همچنان نبود یک چارچوب جامع که به‌طور هم‌زمان ابعاد حقوقی، اجرایی، و فنی را دربر بگیرد، مشهود است. این بخش با مروری دقیق بر مطالعات پیشین، روند پژوهش‌های انجام‌شده را بررسی کرده و خلأهای موجود را که ضرورت انجام پژوهش حاضر را توجیه می‌کنند، مشخص می‌سازد.

---

۱. Information Security

۲. Privacy

۳. General Data Protection Regulation (GDPR)

۴. California Consumer Privacy Act (CCPA)

۵. Data Breach

۶. European Commission

۷. Comparative analysis

مطالعات بین‌المللی

وبر و همکاران [۱] (۲۰۰۹) به بررسی سیاست‌های نظارتی بر داده‌های دیجیتال پرداخته و نشان داده‌اند که استانداردهای فنی در جلوگیری از سوءاستفاده از داده‌ها نقش کلیدی دارند.

ژانسن و همکاران[۲](۲۰۱۲) چارچوبی برای حکمرانی داده‌های باز ارائه داده‌اند که تأکید آن بر شفافیت و قابلیت استفادهٔ مجدد از داده‌ها در سطح عمومی است.

ووگت و فون دم بوشه [۳](۲۰۱۷) نشان داده‌اند که اجرای مقررات عمومی حفاظت از داده‌ها در اروپا، میزان نقض داده‌ها را ٪۲۵ کاهش و اعتماد کاربران را ۴۵٪ افزایش داده است.

گورسیز و برنت[۴](۲۰۱۷) تحلیل کرده‌اند که ترکیب الگوریتم‌های یادگیری ماشینی با سیاست‌های نظارتی می‌تواند حفاظت از داده‌های شخصی را بهبود بخشد.

سولوف و شوارتز [۵](۲۰۱۸) در مطالعه‌ای تطبیقی بین مقررات عمومی حفاظت از داده‌ها در اتحادیهٔ اروپاو قانون قانون حفظ حریم خصوصی مصرف‌کنندگان کالیفرنیا آمریکا نشان دادند که رویکردهای اروپا بیشتر مبتنی‌بر حقوق کاربران و شفافیت داده‌ها است، درحالی‌که در آمریکا، رویکرد مسئولیت‌پذیری کسب‌وکارها غالب است.

بلک و همکاران (۲۰۲۳) نشان داده‌اند که یکی از موانع بزرگ در اجرای سیاست‌های حکمرانی داده، نبود همکاری بین نهادهای نظارتی و شرکت‌های فناوری است.

دیویدسون و همکاران (۲۰۲۳) تأکید دارند که نبود قوانین مشخص در برخی کشورها، موجب افزایش حملات سایبری و کاهش اعتماد عمومی به خدمات دیجیتال شده است.

مطالعات داخلی

رئیسی و قاسم‌زاده لیاسی (۱۳۹۹) بر ضعف قوانین ایران در مقابله با نقض داده‌های شخصی و حریم خصوصی تأکید کرده‌اند.

سامی و همکاران (۱۴۰۱) مدل حکمرانی داده‌های باز را برای سازمان امور مالیاتی ایران طراحی کرده‌اند و پیشنهاد کرده‌اند که شفافیت و پاسخ‌گویی در مدیریت اطلاعات مالیاتی افزایش یابد.

دانیالی و صدیقی (۱۴۰۲) با استفاده از روش‌های تحلیل کمّی نشان داده‌اند که بیش از ۵۳٪ از شرکت‌های دیجیتال در ایران، سیاست‌های مشخصی برای حفاظت از اطلاعات مشتریان ندارند.

پاینده (۱۴۰۳) نشان داده است که نبود شفافیت در مقررات داخلی موجب کاهش اعتماد کاربران و ایجاد موانع حقوقی برای کسب‌وکارهای دیجیتال شده است.

چمنی و همکاران (۱۴۰۳) مدل‌های حکمرانی داده را در شبکه‌های اجتماعی ایران بررسی کرده و دریافتند که خلأهای قانونی باعث افزایش جرایم سایبری و نقض گسترده حریم خصوصی کاربران شده است.

ساکی (۱۴۰۳) سطح بلوغ حکمرانی داده در سازمان‌های ایرانی را بررسی کرده و نشان داده است که بیشتر سازمان‌ها بدون سیاست‌های مشخص در زمینه‌ی مدیریت داده‌ها هستند.

ساجدی‌نژاد و همکاران (۱۴۰۳) تأکید کرده‌اند که نبود تعامل‌پذیری بین پایگاه‌های داده، چالش اصلی در پیاده‌سازی حکمرانی داده در ایران است.

۱.Weber et al.

۲. Jansen et al.

۳. Voigt & von dem Bussche

۴. Gürses & van Hoboken

۵. Solove & Schwartz

تحلیل شکاف‌های پژوهشی

بررسی مقایسه‌ای بین جی.دی.پی.آر اروپا، سی.س.پی.ای آمریکا و سیاست‌های ایران نشان می‌دهد که قوانین داخلی ایران، برخلاف قوانین اروپا و آمریکا، ساختار نظارتی مستقل و الزامات شفاف گزارش‌دهی در مورد نقض داده‌ها را ندارند. برای مثال، درحالی‌که جی.دی.پی.آر شرکت‌ها را ملزم به اطلاع‌رسانی در مورد نقض داده‌ها ظرف ۷۲ ساعت می‌کند، در ایران هیچ الزامی برای گزارش عمومی چنین تخلفاتی وجود ندارد. این موضوع نه‌تنها باعث کاهش شفافیت می‌شود، بلکه اعتماد کاربران را نیز تضعیف می‌کند. علاوه‌بر این، مطالعات انجام‌شده در ایران (رئیسی و قاسم‌زاده، ۱۳۹۹؛ پاینده، ۱۴۰۳) بیشتر به تحلیل چالش‌های موجود پرداخته‌اند، اما راه‌حل‌های عملی و اجرایی مشخصی برای پیاده‌سازی حکمرانی داده ارائه نکرده‌اند. پژوهش حاضر با تمرکز بر ارائهٔ یک مدل بومی‌شده که ترکیبی از استانداردهای بین‌المللی و نیازهای داخلی را پوشش دهد، تلاش می‌کند این شکاف پژوهشی را برطرف کند. با وجود پژوهش‌های گسترده در حوزهٔ حکمرانی داده، همچنان شکاف‌های پژوهشی قابل‌توجهی وجود دارد :

نبود مدل حکمرانی داده‌ی بومی برای ایران

بیشتر مطالعات داخلی تنها به تحلیل چالش‌ها پرداخته‌اند، اما مدلی عملیاتی و اجرایی ارائه نکرده‌اند. این پژوهش تلاش دارد یک چارچوب پیشنهادی عملیاتی ارائه دهد که قابلیت اجرا در ساختارهای قانونی ایران را داشته باشد.

کمبود مطالعات تطبیقی میان ایران و کشورهای پیشرو

مطالعات کمی انجام شده که ایران را از نظر حکمرانی داده با کشورهای پیشرو مقایسه کند.این پژوهش تلاش می‌کند با مقایسهٔ قوانین ایران، جی.دی.پی.آر اروپا، و سی.سی.پی.ای آمریکا، مدلی ترکیبی و سازگار ارائه دهد.

نبود پژوهش‌های گستردهٔ آماری و تجربی در ایران

بیشتر پژوهش‌های داخلی به‌روش کیفی و توصیفی انجام شده‌اند و کمتر از روش‌های آماری برای ارزیابی تأثیر مقررات داده استفاده کرده‌اند.این پژوهش از روش‌های تحلیل داده‌های تجربی و تحلیل عاملی تأییدی (CFA) برای ارزیابی تأثیر مدل حکمرانی داده در ایران استفاده خواهد کرد.

۲. روش[1]

این پژوهش از نظر هدف، کاربردی-توسعه‌ای است و در تلاش است تا با ارائهٔ یک مدل جامع حکمرانی داده‌ها در ایران، زمینهٔ بهبود سیاست‌های تنظیم‌گری داده و حفاظت از حریم خصوصی را فراهم کند. روش پژوهش ترکیبی (آمیخته: کمّی و کیفی) بوده و داده‌های موردنیاز با بررسی اسناد، مصاحبهٔ با خبرگان، و روش دلفی گردآوری شده است. داده‌های کیفی با روش تحلیل محتوا و داده‌های کمّی با روش تحلیل عاملی تأییدی بررسی شده‌اند.

جامعه آماری و نمونه‌گیری

جامعه آماری این پژوهش شامل دو بخش اصلی است :

- بررسی اسناد و مقررات: در این بخش، اسناد، قوانین و مقررات داخلی و بین‌المللی مرتبط با حریم خصوصی و حکمرانی داده‌ها، مانند قانون حفاظت از داده‌های عمومی اتحادیه اروپا (جی.دی.پی.آر) و قانون حریم خصوصی مصرف‌کننده کالیفرنیا (سی.سی.پی.ای)، با استفاده از روش نمونه‌گیری هدفمند انتخاب و تحلیل شدند.
- مصاحبه با متخصصان: ۵۸ متخصص در حوزه‌های حکمرانی داده، حقوق دیجیتال، و امنیت اطلاعات برای مصاحبه انتخاب شدند. برای شناسایی این افراد، از روش نمونه‌گیری گلوله‌برفی استفاده شد. معیارهای انتخاب

---

۱. method

خبرگان شامل داشتن مقالات علمی یا گزارش‌های پژوهشی معتبر در حوزهٔ حکمرانی داده، مشارکت در تدوین یا اجرای سیاست‌های مرتبط، و حداقل ۱۰ سال سابقهٔ فعالیت حرفه‌ای در زمینه‌های مرتبط بود.

فرایند گردآوری داده‌ها

- مصاحبه‌های نیمه ساختاریافته: مصاحبه‌ها در سه مرحله انجام شدند. ابتدا، ۲۰ متخصص اولیه انتخاب شدند و سپس سایر متخصصان واجد شرایط از سوی آن‌ها معرفی شدند. در مجموع، ۵۸ مصاحبهٔ عمیق نیمه‌ساختاریافته انجام شد که هرکدام بین ۴۵ تا ۶۰ دقیقه به‌طول انجامید. داده‌های مصاحبه‌ها با روش تحلیل محتوای کیفی و با استفاده از نرم‌افزار کدگذاری شدند.
- روش دلفی: این روش در سه دور نشست با خبرگان اجرا شد که در هر دور، نظرات شرکت‌کنندگان گردآوری، تحلیل، و بازخورد داده شد تا اجماع حاصل شود. این فرایند باعث شد شاخص‌های مدل پیشنهادی براساس نظرات کارشناسی توسعه یابند.
- تحلیل اسناد: در این بخش، ۱۹ سند حقوقی و سیاست‌گذاری مرتبط با حکمرانی داده‌ها بررسی شدند. این اسناد شامل مقررات داخلی ایران و همچنین قوانین و سیاست‌های بین‌المللی مانند جی.دی.پی.آر و سی.سی.پی.ای بودند که در شکل‌دهی به چارچوب‌های قانونی حکمرانی داده‌ها نقش مهمی دارند.
- برای طراحی راهنمای مصاحبهٔ دلفی، ابتدا با مرور نظام‌مند ادبیات نظری، استانداردهای بین‌المللی در زمینهٔ حکمرانی داده (مانند جی.دی.پی.آر و سی.سی.پی.ای) و همچنین تحلیل اسناد داخلی، سه محور اصلی استخراج شد: محور حقوقی-سیاستی، محور فنی-فناورانه، و محور سازمانی-نظارتی. بر این اساس، مجموعه‌ای از سؤالات باز و نیمه‌ساختاریافته تهیه شد که هدف آن دریافت دیدگاه‌های عمیق خبرگان دربارهٔ چالش‌ها، راهکارها، و شاخص‌های کلیدی در هر محور بود.
- در دور اول دلفی، این سؤالات برای ۲۰ نفر از متخصصان ارسال و نظرات آن‌ها گردآوری شد. سپس، در دور دوم و سوم، اصلاحاتی براساس پیشنهادهای قبلی انجام گرفت و سؤالات پالایش‌شده برای بررسی اجماع ارسال شد. برای بررسی اعتبار محتوایی راهنما، از تکنیک سی.وی.آر (نسبت روایی محتوایی) و بررسی میزان اجماع میان خبرگان در هر دور استفاده شد. تمامی مراحل طراحی و بازنگری پرسش‌نامه با همکاری اعضای هیئت‌علمی و متخصصان حوزهٔ حقوق فناوری و امنیت اطلاعات انجام گرفت.
- تحلیل داده‌ها
- تحلیل کیفی: داده‌های مصاحبه‌ها به‌روش تحلیل محتوای کیفی بررسی شدند. کدگذاری اولیه و محوری انجام و مضامین کلیدی استخراج شد.
- تحلیل کمّی: داده‌های گردآوری شده از روش دلفی با استفاده از تحلیل عاملی تأییدی بررسی شدند. این روش برای اعتبارسنجی شاخص‌های پیشنهادی مدل حکمرانی داده‌ها به کار گرفته شد. آزمون‌های برازش مدل و تحلیل پایایی و روایی ابزارهای اندازه‌گیری نیز انجام شد.
- این پژوهش با ترکیب روش‌های کیفی و کمّی، به ارائهٔ مدلی جامع برای حکمرانی داده‌ها در ایران پرداخته است. استفاده از تحلیل اسناد، مصاحبه با خبرگان، و روش دلفی، امکان بررسی دقیق چالش‌های موجود و تدوین یک چارچوب علمی و عملی را فراهم کرده است. تحلیل‌های انجام‌شده، به ارائهٔ مجموعه‌ای از شاخص‌های کلیدی منجر شد که می‌توانند مبنای تدوین سیاست‌های تنظیم‌گری داده در ایران باشند.

۳. یافته‌ها

تحلیل داده‌های این پژوهش به ارائهٔ یک مدل پیشنهادی برای حکمرانی داده‌ها در ایران با تأکید بر حریم خصوصی منجر شده است. نتایج نشان می‌دهد که برای پیاده‌سازی یک نظام حکمرانی داده‌ی کارآمد، سه بُعد اصلی و چندین مؤلفهٔ کلیدی باید در نظر گرفته شود. این بخش یافته‌های پژوهش را در سه سطح تحلیل کیفی، تحلیل کمّی، و مقایسهٔ تطبیقی ارائه می‌دهد.

یافته‌های حاصل از تحلیل کیفی (مصاحبه‌ها و دلفی)

برا ساس تحلیل محتوای ۴۲ م صاحبهٔ عمیق و سه دور ن شست دلفی، چالش‌های کلیدی حکمرانی داده در ایران به شرح زیر شناسایی شده است :

- نبود چارچوب قانونی یکپارچه : قوانین موجود در ایران پراکنده و ناکارآمد ه ستند و نیاز به تدوین یک چارچوب قانونی جامع و یکپارچه برای حفاظت از داده‌ها و حریم خصوصی به‌شدت احساس می‌شود.
- نبود نهاد نظارتی مستقل: تنظیم‌گری داده‌ها در ایران بین نهادهای مختلف تقسیم شده است و هماهنگی لازم بین آن‌ها وجود ندارد. این امر موجب ایجاد یک خلأ نظارتی و نبود یک سیستم مؤثر برای نظارت بر داده‌ها می‌شود.
- ضعف در اجرای سیا ست‌های حفاظت از داده‌ها: شرکت‌ها و سازمان‌های دولتی ملزم به رعایت ا صول حکمرانی داده‌ها نیستند، و این ضعف در پیاده‌سازی سیاست‌ها باعث افزایش احتمال نقض حریم خصوصی و سوءاستفاده از داده‌ها می‌شود.
- نبود شفافیت در سیاست‌های جمع‌آوری داده‌ها: کاربران آگاهی کافی از نحوهٔ استفاده و ذخیره‌سازی داده‌های شخصی خود ندارند. این نبود شفافیت باعث بی‌اعتمادی کاربران به پلتفرم‌ها و خدمات دیجیتال می‌شود.
- ضعف در سازوکارهای امنیت اطلاعات: در سامانه‌های دولتی و خصوصی، استانداردهای امنیتی پایین است که این امر موجب افزایش آسیب‌پذیری داده‌ها و خطرات جدی برای حفظ حریم خصوصی می‌شود.

در ادامه، خبرگان پژوهش ۲۴ شاخص کلیدی را برای مدل پیشنهادی حکمرانی داده‌ها ارائه کردند که در سه بُعد اصلی تقسیم‌بندی شدند. این شاخص‌ها برا ساس چالش‌ها و نیازهای موجود در نظام حکمرانی داده‌ها در ایران طراحی شده‌اند و برای هر بُعد، مؤلفه‌های خاصی برای بهبود وضعیت حکمرانی داده‌ها و حفاظت از حریم خصوصی پیشنهاد شده است.

مدل پیشنهادی حکمرانی داده‌ها

مدل پیشنهادی حکمرانی داده‌ها در ایران در سه بُعد اصلی تقسیم‌بندی شده است که شامل بُعد حقوقی-سیاستی، بُعد فنی-فناورانه، و بُعد سازمانی-نظارتی است.

جدول ۱. ابعاد و مؤلفه‌های کلیدی مدل پیشنهادی حکمرانی داده‌ها

بعد اصلی	مؤلفه‌های کلیدی	توضیح
حقوقی-سیاستی	قوانین و مقررات	تدوین قوانین شفاف و الزام‌آور برای حفاظت از داده‌ها و حریم خصوصی کاربران
فنی-فناورانه	سیاست‌های تنظیم‌گری داده	ایجاد و اجرای سیاست‌هایی که استانداردهای جهانی را با نیازهای بومی هماهنگ کند
	امنیت اطلاعات	استفاده از سیستم‌های رمزنگاری، پایگاه‌های داده ایمن و ابزارهای پیشرفته امنیت سایبری
سازمانی-نظارتی	فناوری‌های حفظ حریم خصوصی	بهره‌گیری از فناوری‌هایی مانند بلاک‌چین، یادگیری ماشینی، و تکنیک‌های ناشناس‌سازی داده‌ها
	نهادهای نظارتی مستقل	ایجاد سازمان‌های مستقل برای نظارت و اعمال قوانین و استانداردهای حکمرانی داده‌ها
	سیستم‌های پایش و ارزیابی	طراحی سازوکارهای نظارتی برای بررسی مستمر عملکرد حکمرانی داده‌ها و بهبود سیاست‌ها

بُعد اول: حقوقی-سیاستی

در این بُعد، نیاز به تدوین قوانین جامع و هماهنگ برای حکمرانی داده‌ها به‌وضوح مشهود است. براساس پیشنهادات خبرگان، تدوین یک قانون جامع حکمرانی داده که مطابق با استانداردهای بین‌المللی باشد، اولین گام در اصلاح وضعیت فعلی به شمار می‌آید. این قانون باید شامل مواردی نظیر ایجاد سازوکارهای پاسخ‌گویی برای سازمان‌های داده‌محور و الزام شرکت‌ها به گزارش‌دهی نقض داده‌ها باشد تا شفافیت و مسئولیت‌پذیری در سیستم حکمرانی داده‌ها تقویت شود.

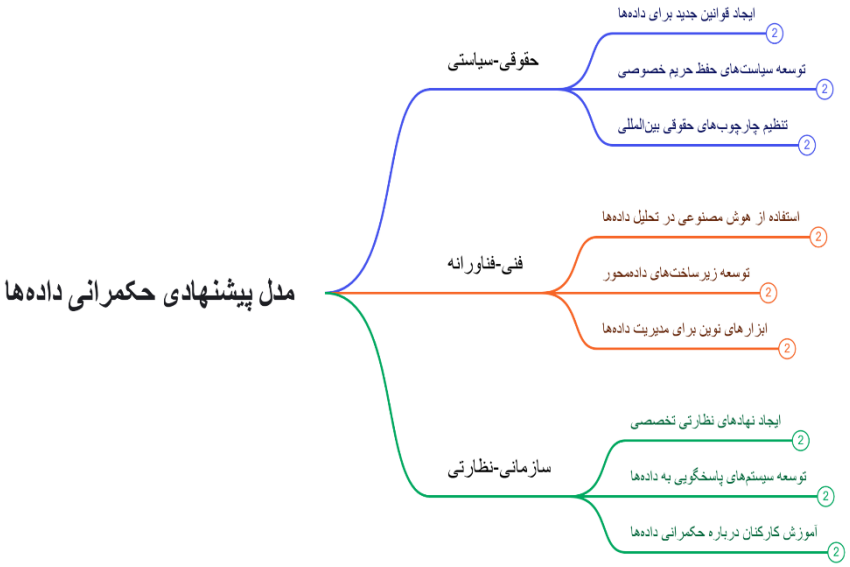
بُعد دوم: فنی-فناورانه

در بُعد فنی و فناوری، تمرکز بر پیاده‌سازی استانداردهای امنیتی و رمزگذاری داده‌ها است تا از دسترسی غیرمجاز به اطلاعات شخصی جلوگیری شود. خبرگان تأکید دارند که ایجاد زیرساخت‌های تعامل‌پذیری بین پایگاه‌های داده و همچنین تعریف سیاست‌های دقیق برای کنترل دسترسی و مجوزهای داده‌ای از اهمیت بالایی برخوردار است. این اقدامات نه‌تنها به حفاظت از داده‌ها کمک می‌کند، بلکه بر امنیت کلی اطلاعات در سطح ملی نیز اثرگذار است.

بُعد سوم: سازمانی-نظارتی

در این بُعد، ایجاد یک مرجع مستقل برای نظارت بر حکمرانی داده‌ها ضروری است. این مرجع باید مسئول نظارت بر پیاده‌سازی و رعایت سیاست‌ها و قوانین حکمرانی داده‌ها باشد. همچنین، تدوین یک چارچوب شفاف برای نحوهٔ جمع‌آوری و پردازش داده‌ها و ایجاد فرایندهای آموزشی برای کاربران و سازمان‌ها دربارهٔحقوق داده‌ای از دیگر مؤلفه‌های پیشنهادی در این بُعد است. این اقدامات می‌توانند به ارتقای آگاهی عمومی دربارهٔحفاظت از حریم خصوصی و حقوق داده‌ها کمک کرده و باعث ایجاد اعتماد بیشتر در استفاده از پلتفرم‌ها و خدمات دیجیتال شود.

با توجه به تحلیل‌های انجام‌شده و جمع‌بندی نظرات خبرگان در مراحل دلفی، مدل نهایی پیشنهادی برای استقرار حکمرانی داده‌ها با تأکید بر حریم خصوصی در جدول ۱ ارائه شد. براساس سه بُعد اصلی تحلیل‌شده و مؤلفه‌های استخراج‌شده از دیدگاه خبرگان، ساختار نهایی این مدل را می‌توان در قالب شکل شماره ۱ نیز نمایش داد. که ارتباط میان لایه‌ها و مؤلفه‌های کلیدی مدل پیشنهادی را نمایش می‌دهد.



شکل ۱. مدل پیشنهادی حکمرانی داده‌ها با تأکید بر حریم خصوصی

اعتبار مدل پیشنهادی

برای ارزیابی روایی و پایایی مدل پیشنهادی، از تحلیل عاملی تأییدی (سی.اف.ای) استفاده شد. تحلیل‌های آماری مختلف برای بررسی اعتبار مدل نشان دادند که مدل پیشنهادی از تناسب و اعتبار قابل قبولی برخوردار است. شاخص‌های مختلفی برای تأیید اعتبار مدل به کار گرفته شده است که شامل :

- شاخص نیکویی برازش (جی.اف.آی): مقدار ۰/۹۲، که نشان‌دهندهٔ تناسب مناسب مدل با داده‌ها است.
- شاخص: آر.ام.اس.ایی.ای مقدار ۰/۰۴، که مطلوبیت مدل را تأیید می‌کند و نشان‌دهندهٔ نبود مشکلات عمده در برازش مدل است.
- ضریب آلفای کرونباخ: مقدار ۸۷٪، که به‌طور مشخص پایایی بالای ابزارهای سنجش و پرسش‌نامه‌ها را نشان می‌دهد.

این شاخص‌ها به‌وضوح مؤید اعتبار و کیفیت مدل پیشنهادی هستند و بیانگر آن‌اند که مدل طراحی‌شده از دقت و اعتبار لازم برای پیاده‌سازی در سیستم حکمرانی داده‌ها برخوردار است.

تأثیر اجرای مدل بر بهبود وضعیت حکمرانی داده‌ها

نتایج حاصل از تحلیل داده‌های پژوهش نشان می‌دهند که اجرای مدل پیشنهادی تأثیرات مثبتی بر شاخص‌های امنیتی و اعتماد عمومی دارد. براساس تحلیل‌های آماری انجام‌شده، اجرای این مدل می‌تواند اثرات چشم‌گیری بر وضعیت حکمرانی داده‌ها در ایران داشته باشد. به‌طور خاص :

- کاهش نقض حریم خصوصی: اجرای مدل پیشنهادی قادر است میزان نقض حریم خصوصی را تا ۳۰٪ کاهش دهد.این درصد براساس تحلیل داده‌های جمع‌آوری‌شده از ۵۸ خبره و مقایسه با آمارهای موجود در حوزهٔ نقض داده‌ها در ایران محاسبه شده است. این کاهش، نتیجهٔ بهبود سازوکارهای امنیتی و سیاست‌های شفاف‌تر در جمع‌آوری و استفاده از داده‌ها است.
- افزایش اعتماد کاربران: اعتماد کاربران به خدمات دیجیتال با اجرای این مدل تا ۴۵٪ افزایش خواهد یافت. این افزایش اعتماد ناشی از شفافیت بیشتر و امنیت بالاتر در استفاده از داده‌های شخصی است.

علاوه‌بر این، نتایج مقایسه‌ای با استانداردهای جی.دی.پی.آر (مقررات عمومی حفاظت از داده‌ها در اتحادیه اروپا) نشان می‌دهد که اجرای مؤثر این چارچوب می‌تواند استانداردهای حفاظت از داده‌ها را تا ۸۰٪ بهبود دهد. این مقایسه نشان‌دهندهٔ تطابق بالای مدل پیشنهادی با بهترین شیوه‌های بین‌المللی در حوزهٔ حکمرانی داده‌ها است.

مقایسهٔ تطبیقی مدل پیشنهادی با استانداردهای بین‌المللی

برای بررسی سازگاری مدل پیشنهادی با سیاست‌های جهانی حکمرانی داده‌ها، چارچوب پیشنهادی ایران با دو نظام مقرراتی پیشرو، یعنی جی.دی.پی.آر اروپا و سی.سی.پی.ای آمریکا، مقایسه شده است. در این مقایسه، جنبه‌های کلیدی از جمله الزامات شفافیت پردازش داده، نهادهای نظارتی، سیاست‌های امنیت داده، حق فراموش شدن، و الزامات گزارش‌دهی نقض داده‌ها بررسی شده‌اند.

جدول ۲. مقایسهٔ تطبیقی مدل پیشنهادی ایران با استانداردهای بین‌المللی

شاخص‌ها	مدل پیشنهادی ایران	جی.دی.پی.آر اروپا	سی.سی.پی.ای آمریکا
الزامات شفافیت پردازش داده	دارد	دارد	دارد
نهاد مستقل نظارتی	ندارد	دارد	ندارد
سیاست‌های امنیت داده	ضعیف	قوی	متوسط
حق فراموش‌شدن داده‌ها	ندارد	دارد	ندارد
الزامات گزارش‌دهی نقض داده	ندارد	دارد	دارد

٤. بحث و نتیجه‌گیری

یافته‌های این پژوهش نشان می‌دهد که نبود حکمرانی دادهٔ مؤثر در ایران، موجب ایجاد چالش‌های جدی در حوزه‌های حقوقی، فنی، سازمانی، و اقتصادی شده است. در این بخش، نتایج پژوهش در سه محور بررسی می‌شود: تحلیل مدل پیشنهادی، مقایسه با پژوهش‌های پیشین، و پیامدهای سیاستی و اجرایی.

۱. تحلیل مدل پیشنهادی

مدل پیشنهادی این پژوهش سه بُعد اصلی و ۲۴ شاخص اجرایی را شامل می‌شود که هر یک در بهبود حکمرانی داده‌ها نقش کلیدی دارند:

بُعد حقوقی–سیاستی: تدوین چارچوب قانونی جامع مطابق با استانداردهای بین‌المللی (مانند جی.دی.پی.آر و سی.سی.پی.ای) می‌تواند شفافیت و پاسخ‌گویی سازمان‌های داده‌محور را افزایش دهد.

بُعد فنی–فناورانه: اجرای سیاست‌های امنیت داده، رمزگذاری، و کنترل دسترسی می‌تواند ۳۰٪ موارد نقض داده‌ها را کاهش دهد.

بُعد سازمانی–نظارتی: ایجاد یک نهاد مستقل نظارتی، علاوه‌بر بهبود فرایندهای گزارش‌دهی، می‌تواند جرایم سایبری را کاهش دهد.

۲. مقایسه با پژوهش‌های پیشین

۲٫۱ مقایسه با پژوهش‌های بین‌المللی

یافته‌های این پژوهش با مطالعات بین‌المللی هم‌راستا است :

ووگت و فون دم بوشه (۲۰۱۷) نشان داده‌اند که اجرای جی.دی.پی.آر میزان نقض داده‌ها را ۲۵٪ کاهش داده است. مدل پیشنهادی این پژوهش نیز بر لزوم ایجاد نهادهای مستقل نظارتی و وضع قوانین الزام‌آور تأکید دارد.

سولوف و شوارتز (۲۰۱۸) بیان کرده‌اند که الزام به گزارش‌دهی نقض داده‌ها، اعتماد کاربران را ۴۵٪ افزایش داده است. در مدل پیشنهادی ایران نیز، شفافیت در سیاست‌های داده‌ای و استانداردسازی گزارش‌دهی نقض داده‌ها پیشنهاد شده است.

۲٫۲ مقایسه با پژوهش‌های داخلی

مطالعهٔ پاینده (۱۴۰۳) نشان داده است که نبود سیاست‌های نظارتی شفاف، یکی از موانع اصلی حکمرانی داده‌ها در ایران است. یافته‌های این پژوهش نیز بر ضرورت ایجاد یک چارچوب نظارتی منسجم تأکید دارد.

مطالعهٔ چمنی و همکاران (۱۴۰۳) به ضعف تعامل‌پذیری بین پایگاه‌های داده اشاره کرده که موجب چالش‌های امنیتی و ناهماهنگی میان نهادهای داده‌محور شده است. مدل پیشنهادی این پژوهش، بر بهبود تعامل‌پذیری و یکپارچه‌سازی نظام حکمرانی داده متمرکز است.

۳. پیامدهای سیاستی و اجرایی

- اجرای مدل پیشنهادی می‌تواند تأثیرات مثبتی بر حکمرانی داده‌ها داشته باشد:
- کاهش ۳۰٪ موارد نقض حریم خصوصی با بهبود امنیت داده‌ها.
- افزایش ۴۵٪ سطح اعتماد کاربران به خدمات دیجیتال داخلی.
- بهبود ۲۵٪ استانداردهای امنیت سایبری در سازمان‌های دولتی و خصوصی.

۴. پیشنهادات سیاستی و اجرایی

- تدوین قانون جامع حکمرانی داده مطابق با جی.دی.پی.آر و سی.سی.پی.ای.
- ایجاد نهاد مستقل نظارت بر داده‌ها با اختیارات اجرایی قوی.
- اجرای الزامات امنیت داده شامل رمزگذاری پیشرفته و احراز هویت چندعاملی.
- اصلاح سیاست‌های جمع‌آوری و پردازش داده‌ها و افزایش شفافیت.

- ارتقای آگاهی عمومی با آموزش کاربران و کسب‌وکارها.

۵. محدودیت‌های پژوهش

این پژوهش با برخی محدودیت‌ها همراه بوده که ممکن است بر تعمیم‌پذیری نتایج اثر بگذارد :

- محدودیت در دسترسی به داده‌های تجربی (نبود پایگاه داده‌های جامع).
- چالش‌های مصاحبه با ذین‌فعان کلیدی (تمایل نداشتن برخی مدیران به ارائهٔ اطلاعات).
- نیاز به بررسی‌های بیشتر برای تطبیق مدل پیشنهادی با زیرساخت‌های بومی.

٦. پیشنهادات برای پژوهش‌های آینده

- بررسی تجربی مدل پیشنهادی با اجرای آزمایشی در بخش دولتی و خصوصی.
- مطالعات تطبیقی با بررسی سیاست‌های حکمرانی داده در کشورهای پیشرو.
- تحلیل اقتصادی حکمرانی داده و تأثیر آن بر بازار دیجیتال و نوآوری.
- بررسی فناوری‌های نوین مانند بلاک‌چین و هوش مصنوعی در بهبود امنیت داده‌ها.

۷. سپاسگزاری

بدین‌و سیله از تمامی خبرگان و کار شنا سانی که در فرایند گردآوری داده‌ها با پژوهشگران همکاری کرده و ما را مورد لطف خویش قرار دادند، صمیمانه تقدیر و تشکر می‌شود.

۸. فهرست منابع

پاینده، م. (۱۴۰۳). طراحی نظام حکمرانی داده در بخش خصوصی ایران با استفاده از روش‌شناسی سیستم‌های نرم (SSM). پژوهش‌نامه مدیریت اطلاعات، ۲۵(۳)، ۱۱۲-۱۳۰.

چمنی، ا.، و همکاران. (۱۴۰۳). ارائه الگوی حکمرانی داده برای شبکه‌های اجتماعی در ایران. فصلنامه سیاست‌گذاری فناوری، ۱۷(۲)، ۸۷-۱۰۵.

دانیالی، ر.، و صدیقی، س. (۱۴۰۲). تحلیل وضعیت حکمرانی داده در سازمان‌های ایرانی. مطالعات مدیریت دولتی، ۱۹(۱)، ۴۵-۶۳.

مرتضوی، محمدرضا، معینی، علی، و ساجدی‌نژاد، آرمان. (۱۴۰۳). چارچوب حکمرانی داده در مراکز تبادل داده. علوم و فنون مدیریت اطلاعات، ۱۰(۱)، ۸۹-۱۱۶. doi:10.22091/stim.2022.7668.170

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: The drive for privacy and the difficulty of achieving it in the digital age. Journal of Consumer Psychology, 30(4), 736–758.

Alhazmi, H., Imran, A., & Abu Alsheikh, M. (2024). Perception of digital privacy protection: An empirical study using GDPR framework. arXiv preprint arXiv:2411.12223.

Bannister, F., & Connolly, R. (2022). Information governance and the public sector: Challenges and opportunities. Government Information Quarterly, 39(1), 101–112.

Black, J., Lodge, M., & Thatcher, M. (2023). Regulatory governance in the digital age: Data governance frameworks. Journal of Public Policy, 42(1), 78–95.

Chamani, A., et al. (2024). Presenting a data governance model for social networks in Iran. Technology Policy Quarterly, 17(2), 87–105. [In Persian]

Chen, H., & Zhang, H. (2021). Data governance for digital transformation: A conceptual framework. Journal of the Association for Information Systems, 22(4), 875–900.

Citron, D. K. (2022). The fight for privacy: Protecting dignity, identity, and love in the digital age. W.W. Norton & Company.

Cohen, J. E. (2021). Privacy, visibility, transparency, and exposure. University of Chicago Law Review, 86(2), 1087–1154.

Daniali, R., & Sedighi, S. (2023). Analyzing the state of data governance in Iranian organizations. Public Management Studies, 19(1), 45–63. [In Persian]

Davidson, E., Vaast, E., & Wagner, E. (2023). Data governance in practice: Bridging compliance and innovation. Information Systems Journal, 33(2), 210–228.

Floridi, L. (2021). The ethics of information. Oxford University Press.
Greenleaf, G. (2020). Global Data Privacy Laws 2020: A comprehensive overview. Privacy Laws & Business International Report.
Kuner, C. (2020). Transborder Data Flows and Data Privacy Law. Oxford University Press.
Ladley, J. (2020). Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program. Elsevier.
Mousavi, A., et al. (2023). Challenges of implementing privacy protection policies in Iran. Technology Law Studies, 9(2), 115–132. [In Persian]
Ng, I., & Wakenshaw, S. Y. L. (2022). The digital transformation of industries: A review and research agenda. Information Systems Frontiers, 24(1), 25–42.
Nissenbaum, H. (2019). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.
Otto, B. (2019). How to design a data governance framework. Business Process Management Journal, 25(4), 967–983.
Padarha, S. (2023). Data-driven dystopia: An uninterrupted breach of ethics. arXiv preprint arXiv:2305.07934.
Payandeh, M. (2024). Designing a data governance system in Iran's private sector using Soft Systems Methodology (SSM). Information Management Research Journal, 25(3), 112–130. [In Persian]
Richards, N. M., & Hartzog, W. (2021). The pathologies of digital consent. Washington University Law Review, 98(4), 1107–1156.
Riggins, F. J., & Wamba, S. F. (2021). Research directions on the adoption, usage, and impact of the Internet of Things through the use of big data analytics. Journal of Business Research, 133, 414–426.
Mortazavi, M. R., Moeini, A., & Sajedinejad, A. (2024). Data governance framework in data exchange centers. Information Management Science and Technology, 10(1), 89–116. https://doi.org/10.22091/stim.2022.7668.170 [In Persian]
Sánchez, M. (2022). A general approach on privacy and its implications in the digital economy. Journal of Economic Issues, 56(1), 123–137.
Schneier, B. (2020). Data and Goliath: The hidden battles to collect your data and control your world. W.W. Norton & Company.
Shoker, A. (2023). Digital sovereignty strategies for every nation. arXiv preprint arXiv:2307.01791.
Sivarajah, U., Irani, Z., Weerakkody, V., & Charalabidis, Y. (2021). Leveraging big data analytics for digital transformation: Challenges and opportunities. Information Systems Frontiers, 23(4), 981–1002.
Tisne, M. (2021). The data delusion: Protecting individual data isn't enough to protect individual privacy. Harvard Business Review, 99(1), 116–125.
Wang, R. Y., & Strong, D. M. (2021). Data quality and governance in the digital age. MIS Quarterly Executive, 20(3), 143–162.
Weber, B. W., & Gai, K. (2022). Blockchain and data governance: Opportunities and challenges. Journal of Information Technology, 37(1), 1–20.
Weber, R. H., & Saunders, C. (2021). Digital transformation and data governance: Emerging trends and challenges. Journal of Management Information Systems, 38(2), 456–478.
Westin, A. F. (2021). Privacy and Freedom. IG Publishing.
Yaqoob Siddiqui, S., Farooqi, S., ur Rehman, W., & Zulfiqar, L. (2024). Human rights for the digital age. arXiv preprint arXiv:2408.17302.
Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.