Iranian Journal of Public Policy
2026 , Vol. 12 , No. 2 , 367-382
Online ISSN: 2538-5089
Home Page: jppolicy.ut.ac.ir

RESEARCH ARTICLE

Requirements for Artificial Intelligence Policymaking with an Emphasis on the Comparative Advantage of Data in Iran

Nafiseh Seifi[1], Ali khajehnaieni[2*], Kioomars Ashtarian[3]

1. Master of Public Policy, Faculty of Law & Political Science, Allameh Tabatabai University, Tehran, Iran
Email: nafise.seifi@gmail.com
2. Assistant Professor of Public Policy, Faculty of Law & Political Science, Allameh Tabataba'i University, Tehran, Iran
* Corresponding Author's Email: naieniali@atu.ac.ir
3. Associate Professor of Public Policy, Faculty of Law & Political Science, University of Tehran, Tehran, Iran
Email: ashtrian@ut.ac.ir

https://doi.org/10.22059/jppolicy.2026.107845

Received: 19 February 2026
Accepted: 21 April 2026

ABSTRACT

As a transformative technology, artificial intelligence has significant potential to improve governance, public services, and economic development. However, its effective use depends on efficient data policymaking. In Iran, the relative advantage in accessing indigenous data—especially legal, health, and public service data—has provided an unparalleled opportunity to develop proprietary algorithms. This qualitative study, based on document analysis and expert interviews, shows that the main problem in the country is not a lack of data, but rather a weakness in data governance, a lack of standardization, and a lack of legal and institutional mechanisms for the release, exchange, and protection of data. The experience of leading countries shows that "data policy" is the main foundation for the development of artificial intelligence, and without it, technological investments will not achieve the desired results. The research findings indicate the need to establish national data infrastructures, anonymize and standardize sensitive data, strengthen public trust, and design legal frameworks for data ownership and exchange. The main conclusion is that data governance should be placed as a policy priority on the Iranian governance agenda. Achieving this goal requires the government to play an active role in establishing national data centers, supporting data-driven businesses, and developing transparent regulations to balance public interest, privacy, and technological development.

Keywords:. Policy making, Artificial Intelligence, Comparative Advantage, Data, Data Governance.

Citation: Seifi,Nafiseh; khajehnaieni, Ali; Ashtarian, Kioomars (2026). Requirements for Artificial Intelligence Policymaking with an Emphasis on the Comparative Advantage of Data in Iran. *Iranian Journal of Public Policy*, 12 (2), 367-382.
DOI: https://doi.org/10.22059/jppolicy.2026.107845

Published by University of Tehran

فصلنامه سیاستگذاری عمومی

دوره ۱۲، شماره ۲، تابستان ۱۴۰۵. صفحات ۳۸۲-۳۶۷

شاپا الکترونیکی: ۵۰۸۹ - ۲۵۳۸

آدرس سایت: jppolicy.ut.ac.ir

مقاله پژوهشی

الزامات سیاستگذاری هوش مصنوعی با تأکید بر مزیت نسبی داده‌ها در ایران

نفیسه سیفی[۱]، علی خواجه نائینی[۲*]، کیومرث اشتریان[۳]

۱. کارشناسی ارشد سیاستگذاری عمومی، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبائی، تهران، ایران

رایانامه: nafise.seifi@gmail.com

۲. استادیار سیاستگذاری عمومی، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبائی، تهران، ایران

* رایانامهٔ نویسنده مسئول: naieniali@atu.ac.ir

۳. دانشیار سیاستگذاری عمومی، دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران

رایانامه: ashtrian@ut.ac.ir

تاریخ دریافت: ۳۰ بهمن ۱۴۰۴
تاریخ پذیرش: ۱ اردیبهشت ۱۴۰۵

https://doi.org/10.22059/jppolicy.2026.107845

چکیده

با وجود تمرکز بخش قابل توجهی از مطالعات مرتبط با هوش مصنوعی بر ابعاد فناورانه، اخلاقی و تنظیم‌گری هوش مصنوعی، نقش داده‌های بومی به‌عنوان مزیت نسبی کشورها کمتر مورد توجه قرار گرفته است. هدف این پژوهش، شناسایی الزامات حکمرانی داده در توسعه هوش مصنوعی با تأکید بر بهره‌برداری از ظرفیت داده‌های بومی ایران است. این پژوهش با رویکرد کیفی و بر اساس مصاحبه‌های نیمه‌ساختاریافته با خبرگان حوزه هوش مصنوعی و سیاست‌گذاری انجام شده و داده‌ها با استفاده از تحلیل مضمون بررسی شده‌اند. یافته‌ها نشان داد که هشت مؤلفه شامل تقویت اعتماد عمومی به زیست‌بوم داده، ایجاد زیرساخت‌های تنظیم‌گری داده، توسعه نظام‌های مالکیت داده، تقویت امنیت داده، استانداردسازی داده، افزایش دسترسی‌پذیری داده، انباشت و ذخیره‌سازی داده و گمنام‌سازی و ناشناس‌سازی داده‌ها از مهم‌ترین الزامات حکمرانی داده در توسعه هوش مصنوعی ایران به شمار می‌روند. نتایج پژوهش بیانگر آن است که داده‌های بومی می‌توانند به‌عنوان یک دارایی راهبردی و مزیت رقابتی کشور در توسعه هوش مصنوعی ایفای نقش کنند، مشروط بر آنکه حکمرانی داده به‌صورت یکپارچه و مبتنی بر چارچوب‌های حقوقی، فنی و نهادی مناسب استقرار یابد.

واژگان کلیدی: سیاستگذاری، هوش مصنوعی، مزیت نسبی، داده، حکمرانی داده.

استناد: سیفی، نفیسه؛ خواجه نائینی، علی؛ اشتریان، کیومرث (۱۴۰۵). الزامات سیاستگذاری هوش مصنوعی با تأکید بر مزیت نسبی داده‌ها در ایران. *فصلنامه سیاستگذاری عمومی*، ۱۲ (۲)، ۳۸۲-۳۶۷.

DOI: https://doi.org/10.22059/jppolicy.2026.107845

ناشر: دانشگاه تهران

مقدمه

هوش مصنوعی به یک پدیده سودمند در دنیای تکنولوژی تبدیل شده و کاربردهای گسترده‌ای در تسهیل فعالیتهای دولتی، خدمات دولت الکترونیک و خدمات عمومی پیدا کرده (Al marri et al, 2019:2-3) و توجهات زیادی را در بین محققان و متصدیان امور با گستره وسیعی از مزایا و سودمندی در بخش دولتی کسب کرده است (Wirtz et al , 2019: 1072). بخش عمده مطالعات حوزه هوش مصنوعی بر موضوعاتی همچون توسعه الگوریتم‌ها، پیشرفت‌های فناورانه، ملاحظات اخلاقی، تنظیم‌گری، حاکمیت الگوریتمی و پیامدهای اجتماعی هوش مصنوعی متمرکز بوده‌اند (Russell & Norvig, 2021؛ Floridi & Cowls, 2019). همچنین در سال‌های اخیر نیز با گسترش هوش مصنوعی مولد، پژوهش‌های متعددی به تدوین چارچوب‌های تنظیم‌گری، مدیریت ریسک، شفافیت، عدالت الگوریتمی و حکمرانی هوش مصنوعی پرداخته‌اند(OECD, 2024, UNESCO,2021) . اگرچه این مطالعات سهم ارزشمندی در توسعه دانش هوش مصنوعی داشته‌اند، اما کمتر به این پرسش بنیادین پرداخته‌اند که مزیت نسبی کشورها در توسعه هوش مصنوعی از چه منابع و ظرفیت‌هایی ناشی می‌شود و چگونه می‌توان این مزیت را در فرآیند سیاست‌گذاری تقویت کرد .در واقع، تمرکز غالب ادبیات بر «چگونگی تنظیم و کنترل هوش مصنوعی» بوده است، نه بر «منابع راهبردی و مزیت‌های رقابتی کشورها» در این حوزه. از طرفی رویکرد عقلانی در سیاستگذاری و تلاش برای افزایش قدرت تحلیل و پردازش داده‌ها در مقیاس کلان و سریع در حوزه سیاستگذاری به اهمیت کار بست هوش مصنوعی افزوده است (Pourezat & Abdi, 2019: 54-55). از منظر سیاستگذاری، این خلأ برای کشورهایی مانند ایران اهمیت بیشتری می‌یابد؛ زیرا محدودیت در دسترسی به سرمایه، زیرساخت‌های پردازشی و محاسباتی، ضرورت اتکا به مزیت‌های درون‌زا را دوچندان می‌کند. در این میان، داده‌های بومی می‌توانند به‌عنوان یک دارایی راهبردی و منبع بالقوه مزیت رقابتی در توسعه هوش مصنوعی مطرح شوند، مشروط بر آنکه در قالب یک نظام کارآمد حکمرانی داده مدیریت شوند. در این چارچوب، مزیت نسبی ایران را نیز باید فراتر از توسعه صرف الگوریتم‌ها جست‌وجو کرد. وجود حجم گسترده‌ای از داده‌های بومی در حوزه‌هایی همچون سلامت، حقوق، آموزش، خدمات عمومی و ...، ظرفیتی راهبردی برای توسعه مدل‌های هوش مصنوعی بومی ایجاد کرده است؛ ظرفیتی که به دلیل ویژگی‌های منحصربه‌فرد خود، به‌سادگی توسط رقبا قابل جایگزینی نیست. مزیت داده‌ها در حوزه‌های مختلف در ایران، ابعاد برجسته‌ای دارد. به عنوان مثال داده‌های حقوقی می‌توانند نقش کلیدی در توسعه الگوریتم‌های بومی هوش مصنوعی ایفا کنند، زیرا ایران به دلیل داشتن نظام حقوقی منحصربه‌فرد مبتنی بر حقوق اسلامی و مدنی، ظرفیت ویژه‌ای برای ایجاد مزیت رقابتی در حوزه هوش مصنوعی دارد. نظام حقوقی ایران، مبتنی بر شریعت اسلامی و اصول حقوق مدنی، الگویی خاص ارائه می‌دهد که می‌تواند الگوریتم‌های هوش مصنوعی متفاوت و بومی تولید کند. داده‌های حقوقی ایران شامل دعاوی مدنی، کیفری، خانواده، تجاری و دیوان عدالت اداری است که تنوع موضوعی بالایی دارند. وجود منابع گسترده‌ای مانند آرای قضایی، قوانین مصوب مجلس، و آیین‌نامه‌های اجرایی، مزیتی برای توسعه مدل‌های تحلیل حقوقی است. در ایران، با توجه به ویژگی‌های خاص سیستم بهداشت و درمان و داده‌های موجود در زمینه سلامت نیز، می‌توان از مزیت نسبی داده‌های سلامت برای توسعه الگوریتم‌های بومی هوش مصنوعی بهره برد. در حال حاضر، هوش مصنوعی در برخی زمینه‌ها مانند رادیولوژی، تحلیل تصاویر پزشکی، پیش‌بینی بیماری‌ها و مدل‌سازی اپیدمیولوژیک در ایران در حال استفاده است. الگوریتم‌های یادگیری ماشین و هوش مصنوعی برای تحلیل داده‌های سلامت به‌ویژه در زمینه‌های تشخیص بیماری‌های مزمن، مراقبت‌های پیشگیرانه، و بهینه‌سازی منابع بیمارستانی به‌کار گرفته می‌شوند. داده‌های سلامت در ایران به‌طور کلی شامل اطلاعات بیماران، سوابق پزشکی، نتایج آزمایشات، تصاویر پزشکی و گزارش‌های بیمارستانی است. این داده‌ها معمولاً در سیستم‌های مختلف از جمله بیمارستان‌ها، مراکز بهداشتی و درمانی، آزمایشگاه‌ها و مطب‌های خصوصی جمع‌آوری می‌شوند. با این حال، هنوز چالش‌هایی در این زمینه وجود دارد که نیاز به تقویت و به‌روزرسانی قوانین و مقررات دارند (Behzadifar et al,2025: 336-337). با توجه به این ملاحظات، پرسش اصلی این پژوهش آن است که تحقق این مزیت (استفاده از داده‌های بومی در توسعه هوش مصنوعی) مستلزم چه الزامات حکمرانی داده است؟ پاسخ

به این پرسش، علاوه بر افزودن بر غنای ادبیات سیاستگذاری هوش مصنوعی، می‌تواند مبنایی برای طراحی راهبردهای ملی در بهره‌برداری از ظرفیت‌های داده‌ای کشور فراهم آورد.

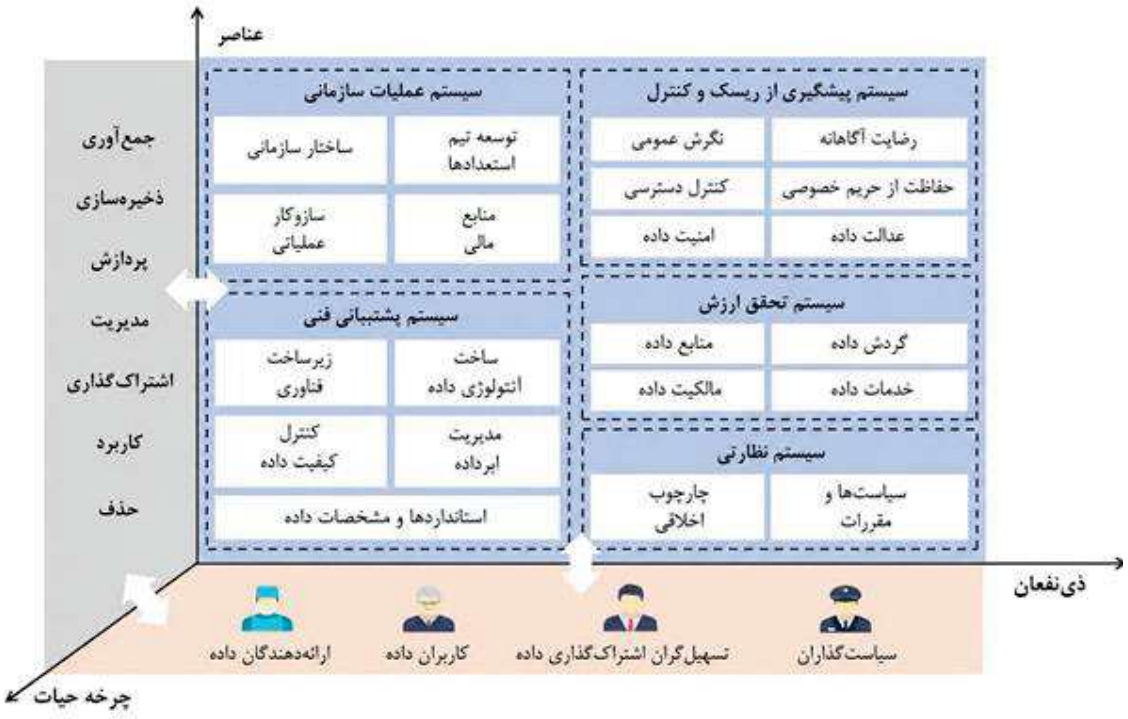
مبانی نظری

ادبیات نظری هوش مصنوعی دامنه گسترده‌ای را در بر می گیرد. از آنجا که موضوع این مقاله اهمیت داده‌ها به مثابه یکی از مزیت‌های نسبی فعالیت‌ها و سیاست‌های هوش مصنوعی در ایران است ما بر این بعد از ادبیات نظری تأکیدی بیشتری می‌نماییم. اهمیت فراوان هوش مصنوعی و لزوم سیاستگذاری در این حوزه باعث شده است تا سازمان‌های بین‌المللی، پژوهشهای متعددی را انجام دهند؛ از جمله سازمان همکاری و توسعه اقتصادی(OECD) که دارای واحدی ویژه با نام رصدخانه هوش مصنوعی است که بر موضوع هوش مصنوعی و سیاست‌هایش متمرکزند (OECD, 2024). سیاست‌های هوش مصنوعی به گسترش و تولید فناوری‌ها در سراسر جامعه می‌پردازد (Cave et al, 2021:38). این سیاست‌ها در مورد ابتکارات دولت برای تشویق توسعه فناوری هوش مصنوعی به منظور حفظ حاکمیت دیجیتال، اطمینان از مکانیسم‌های موثر حفاظت از داده‌ها، امنیت سایبری و حاکمیت اینترنت است. در همین راستا در حوزه سیاستگذاری، شش روایت مجزا برای سیاست هوش مصنوعی دیده شده است: روایت اول بر ایجاد و تقویت بازار داخلی هوش مصنوعی، حمایت از شرکت‌های نوآور و ارتقای رقابت‌پذیری اقتصادی کشور تأکید دارد و دولت در آن نقش تسهیل‌گر ایفا می‌کند. روایت دوم بر مقابله با انحصار داده از طریق اشتراک‌گذاری داده‌ها، جلوگیری از تمرکز آن در اختیار شرکت‌های بزرگ و استفاده از داده در جهت منافع عمومی متمرکز است و دولت نقش تنظیم‌گر را بر عهده دارد. روایت سوم توسعه اکوسیستم هوش مصنوعی را در گرو همکاری راهبردی میان دولت، دانشگاه و صنعت دانسته و دولت را به‌عنوان رهبر و هماهنگ‌کننده این همکاری‌ها معرفی می‌کند. روایت چهارم بر توسعه هوش مصنوعی اخلاق‌محور و قابل اعتماد با تأکید بر حقوق بنیادین، ارزش‌های انسانی، شفافیت و چارچوب‌های قانونی استوار است و دولت نقش تنظیم‌گر دارد. روایت پنجم بر تربیت نیروی انسانی متخصص و تقویت نظام آموزشی برای پاسخگویی به نیازهای بازار کار هوش مصنوعی تأکید می‌کند و دولت در جایگاه تسهیل‌گر قرار می‌گیرد. روایت ششم نیز بر گسترش استقرار و کاربرد هوش مصنوعی از طریق توسعه زیرساخت‌ها، حمایت از پژوهش و نوآوری و فراهم‌سازی شرایط مناسب برای به‌کارگیری گسترده این فناوری تأکید دارد و دولت نقش تسهیل‌گر را ایفا می‌کند. در مجموع، این روایت‌ها نشان می‌دهند که توسعه هوش مصنوعی نیازمند ترکیبی از سیاست‌های اقتصادی، تنظیم‌گری، همکاری بین‌بخشی، توسعه سرمایه انسانی و حکمرانی مسئولانه است (Guenduez & Mettler, 2023: 5). نامبو در رابطه با ابعاد مدنی و قانونی، حسابرسی و حق مالکیت و سو استفاده از هوش مصنوعی و چالش مستندات آن جهت رسیدگی قانونی سخن گفته است و در بخشی دیگر به چگونگی جلوگیری از طراحی فناوری جدید که تبدیل به رویه‌ای جهت رسیدن به اهداف مخرب نشود پرداخته است (Nambu, 2016: 490). با این وجود دویودی استفاده از فناوری بلاکچین در آموزش، سنجش و حفاظت از سواستفاده در استفاده از هوش مصنوعی را به عنوان مکانیزمی معتبر برای تأیید ایمنی و مطلوبیت اجتماعی می‌داند (Dwivedi et al, 2019: 31). تایهاق معتقد است که اطلاعات نامتقارن بین شرکت‌های فناوری و تنظیم‌کنندگان، برای درک و به کارگیری قوانین جدید و موجود برای برنامه‌های هوش مصنوعی مشکل‌زا است (Taeihagh, 2021: 140). پژوهشگران رشد تصاعدی داده را یکی از مهمترین چالشهای پیشروی توسعه این تکنولوژی می‌دانند و بیان می‌کنند که با وجود اینکه از این تغییرات به خوبی استقبال شده‌است، تاثیر افزایش این مقدار داده بر سازمان‌ها نیازمند عکس‌العمل جدی است و سازمان‌ها احتیاج به زیرساخت برای مدیریت این حجم از داده هستند؛ از طرف دیگر، میزان تأثیر هوش مصنوعی بستگی به میزان دسترسی به منابع داده‌ها دارد. داده‌ها باید بدون تبعیض و کامل باشند و برای داشتن یک حکمرانی داده موفق، تمامی دپارتمان‌های مربوط به داده‌ها باید از چهارچوب مربوطه پیروی کنند. در همین راستا اندرسون نیز رعایت حریم خصوصی و حمایت از داده‌ها را به عنوان محتمل‌ترین دغدغه هوش مصنوعی می‌داند (Anderson, 2019: 676). جانسن نیز در نظر دارد که حکمرانی داده یک موضوع

کلیدی حول مباحث پیرامون حکمرانی هوش مصنوعی است و با چالش‌های متعدد سازمانی و فناورانه مواجه است (Janssen et al., 2016: 5-8).

نظریه حکمرانی داده

امروزه در ادبیات سیاستگذاری هوش مصنوعی، «حکمرانی داده» نه صرفاً به‌عنوان یکی از مؤلفه‌های فنی، بلکه به‌عنوان زیرساخت نهادی توسعه هوش مصنوعی شناخته می‌شود. کیفیت، دسترس‌پذیری، استانداردسازی، قابلیت اشتراک‌گذاری و اعتمادپذیری داده‌ها، تعیین‌کننده توان کشورها در توسعه مدل‌های هوش مصنوعی و خلق ارزش اقتصادی و عمومی است. از این منظر، مزیت رقابتی کشورها بیش از آنکه به الگوریتم‌ها وابسته باشد، به توانایی آنها در سازماندهی و حکمرانی بر منابع داده‌ای بستگی دارد (Khatri & Brown, 2010). کیو و هیو (Qiu & Hu, 2026: 4) بر این باورند که «تعریف حکمرانی داده باید عناصر اساسی از جمله موضوعات حکمرانی، فرآیندهای حکمرانی و اهداف حکمرانی را در بر گیرد. حکمرانی داده به عنوان اجرای مدیریت و کنترل مؤثر در سراسر چرخه حیات کامل دسته‌های مختلف داده – شامل داده‌های شخصی، داده‌های سازمانی، داده‌های دولتی و داده‌های عمومی – از طریق چارچوبی نظام‌مند متشکل از قوانین و مقررات، نظام‌های مدیریتی، مشخصات استاندارد و ابزارهای فناورانه مفهوم‌سازی [می‌شود]. این چارچوب حکمرانی با هدف تأمین نیازهای کاربرد داده در سناریوهای متعدد از جمله مدیریت سازمانی، نظارت صنعتی، حکمرانی ملی و همکاری بین‌المللی طراحی شده است. بر این اساس، حکمرانی داده‌های علمی را می‌توان به عنوان مدیریت و کنترل مؤثر بر کل چرخه حیات داده‌های علمی از طریق چارچوبی نظام‌مند متشکل از قوانین و مقررات، نظام‌های مدیریتی، مشخصات استاندارد و ابزارهای فناورانه، به منظور تأمین نیازهای کاربرد داده در سناریوهای پژوهش علمی تعریف کرد. حکمرانی داده؛ مجموعه‌ای از قواعد، نهادها، استانداردها و سازوکارهای هماهنگ‌کننده است که نحوه تولید، ذخیره‌سازی، پردازش، اشتراک‌گذاری و استفاده از داده را در بخش‌های عمومی و خصوصی تنظیم می‌کند (OECD, 2021). فقدان چنین چارچوبی موجب شکل‌گیری جزایر داده‌ای، کاهش قابلیت تعامل میان سازمان‌ها، افت کیفیت داده‌ها و در نهایت کاهش کارایی سامانه‌های هوش مصنوعی خواهد شد.(Janssen et al., 2020) . در سال‌های اخیر، بسیاری از دولت‌ها سیاست‌های ملی هوش مصنوعی را با راهبردهای حکمرانی داده تلفیق کرده‌اند؛ زیرا بدون وجود داده‌های استاندارد، قابل اعتماد و قابل تبادل، حتی پیشرفته‌ترین الگوریتم‌های هوش مصنوعی نیز عملکرد مطلوبی نخواهند داشت (World Bank, 2021) . از سوی دیگر، حکمرانی داده صرفاً ناظر بر مدیریت فنی داده نیست، بلکه ابعاد حقوقی، اخلاقی، امنیتی و نهادی آن نیز اهمیت اساسی دارد. تضمین حریم خصوصی، تعیین مالکیت داده، ایجاد اعتماد عمومی، شفافیت در استفاده از داده‌ها و پاسخگویی نهادهای متولی از مهم‌ترین ارکان این نظام حکمرانی به شمار می‌روند .(United Nations, 2023) . به همین دلیل، در بسیاری از کشورها، سرمایه‌گذاری در زیرساخت‌های داده و تدوین چارچوب‌های حکمرانی داده، پیش از توسعه کاربردهای گسترده هوش مصنوعی در دستور کار قرار گرفته است. در ادامه برخی از چارچوبهای نظری حکمرانی داده معرفی شده و در انتهای این بخش، چارچوب مفهومی تلفیقی که مبنای این مقاله قرار گرفته است معرفی می‌شود.



شکل ۱ . چارچوب حکمرانی داده (Qiu & Hu, 2026)

شکل ۲ . چارچوب جامع حکمرانی داده (Panian,2010)

با تلفیق ابعاد و مؤلفه‌های موجود در دو چارچوب بیان شده، می‌توان مدل مفهومی زیر را طراحی کرد.

شکل ۳ . مدل مفهومی الزامات حکمرانی داده در توسعه هوش مصنوعی ((Panian,2010, Qiu & Hu, 2026))

روش‌شناسی تحقیق

این پژوهش کیفی بوده و جمع‌آوری داده‌ها از طریق با مصاحبه با خبرگان حوزه حکمرانی داده و هوش مصنوعی به شرح جدول ۱ انجام شده است.

جدول ۱ . مشارکت‌کنندگان در تحقیق

کد	سمت	زمان مصاحبه(دقیقه)
۱	دانشیار مهندسی کامپیوتر دانشگاه مالک اشتر	۴۰
۲	مسئول کارگروه ستاد اقتصاد دیجیتال معاونت علمی و فناوری ریاست جمهوری	۴۰
۳	رئیس مرکز هوشمندسازی دانشگاه الزهرا	۴۵
۴	مشاور ستاد هوش مصنوعی معاونت علمی و فناوری ریاست جمهوری	۵۵
۵	دانشیار گروه سیاستگذاری عمومی دانشگاه تهران	۶۰
۶	سرپرست معاونت مرکز نوآوری و توسعه هوش مصنوعی پژوهشگاه ارتباطات و فناوری اطلاعات	۵۵
۷	معاون مرکز نوآوری و کارآفرینی پردیس فارابی دانشگاه تهران/ سرپرست آزمایشگاه سیاستگذاری علم، فناوری و نوآوری	۴۵
۸	کارشناس ارشد دانشگاه عالی دفاع ملی و دبیر گروه سایبری	۶۰
۹	دبیر ستاد توسعه فناوری های هوش مصنوعی و رباتیک معاونت علمی، فناوری و اقتصاد دانش بنیان	۴۰
۱۰	هیأت علمی دانشگاه امیرکبیر	۶۰

کد	سمت	زمان مصاحبه(دقیقه)
۱۱	کارشناس ارشد در مرکز آمار قوه قضاییه	۱۲۰
۱۲	رئیس مرکز آمار قوه قضاییه	۴۰
۱۳	عضو هیئت علمی دانشگاه عالی دفاع ملی و رئیس مرکز توسعه فرهنگ و هنر در فضای مجازی وزارت فرهنگ و ارشاد اسلامی	۴۵
۱۴	استاد سیاستگذاری سلامت	۶۰

تحلیل داده‌های کیفی با بهره‌گیری از رویکرد کدگذاری اشتراوس و کوربین (۱۹۹۸) انجام شد. در این رویکرد، تحلیل داده‌ها به‌صورت نظام‌مند و طی سه مرحله کدگذاری باز، کدگذاری محوری و کدگذاری انتخابی صورت می‌گیرد. در مرحله کدگذاری باز، مفاهیم اولیه از متن مصاحبه‌ها استخراج و بر اساس شباهت‌های مفهومی دسته‌بندی شدند. سپس در مرحله کدگذاری محوری، ارتباط میان مفاهیم و مقوله‌ها شناسایی و سازمان‌دهی شد و در نهایت، در مرحله کدگذاری انتخابی، مقوله‌های اصلی در قالب مضامین محوری یکپارچه شدند. این فرآیند امکان شناسایی الگوهای مفهومی، تبیین روابط میان مقوله‌ها و دستیابی به چارچوبی منسجم از الزامات حکمرانی داده در توسعه هوش مصنوعی را فراهم ساخت (Strauss & Corbin, 1998; Corbin & Strauss, 2015).

یافته‌های پژوهش

تحلیلی مضامین حاصل از مصاحبه‌ها بر اساس ابعاد مختلف مدل مفهومی پژوهش به شرح جدول زیر است:

جدول ۲ . تحلیل مضامین حاصل از مصاحبه‌ها

ردیف	بعد اصلی	زیرمؤلفه	کدهای اولیه (نمونه)
۱	**اعتمادسازی داده**	اعتماد عمومی اعتماد بین‌سازمانی	شفافیت در استفاده از داده، رضایت آگاهانه کاربران، پاسخگویی نهادها، مشارکت ذی‌نفعان، افزایش مشروعیت، اعتماد به خدمات دیجیتال، اطلاع‌رسانی عمومی، رعایت اصول اخلاقی، تبادل امن داده، همکاری نهادی، توافق‌نامه‌های اشتراک داده، قابلیت اعتماد سازمان‌ها، مسئولیت‌پذیری مشترک، مدیریت ریسک، هماهنگی نهادی، اعتماد متقابل
۲	**تنظیم‌گری داده**	چارچوب‌های تنظیم‌گری نظام‌های مالکیت فکری	قوانین داده، سیاست‌های حاکمیتی، نهاد تنظیم‌گر، نظارت قانونی، ضمانت اجرا، انطباق مقررات، سیاستگذاری تطبیقی، ارزیابی اثرات مقررات، کپی رایت ، مجوز های مربوط به مالکیت، سازمان مالکیت فکری
۳	**مالکیت داده**	تعیین حقوق مالکیت حکمرانی حقوق داده	مالکیت فردی داده، مالکیت سازمانی، حق کنترل داده، تعیین مسئولیت، حقوق بهره‌برداری، قراردادهای داده، انتقال مالکیت، مدیریت حقوق داده، مدیریت مجوز دسترسی، حقوق استفاده مجدد، مسئولیت قانونی، مدیریت چرخه عمر داده، حل تعارضات مالکیت، سیاست‌های اشتراک، حق حذف داده، ثبت حقوق
۴	**امنیت داده**	حفاظت فنی مدیریت مخاطرات	رمزنگاری داده، کنترل دسترسی، احراز هویت، امنیت شبکه، پشتیبان‌گیری، ثبت وقایع امنیتی، مدیریت آسیب‌پذیری، پایش امنیت ارزیابی ریسک، پاسخ به رخداد، تداوم کسب‌وکار، بازیابی اطلاعات، مدیریت تهدیدات، ممیزی امنیت، آموزش امنیت، تاب‌آوری سایبری
۵	**استانداردسازی داده**	استانداردهای فنی استانداردهای مدیریتی	رمزنگاری داده، کنترل دسترسی، احراز هویت، امنیت شبکه، پشتیبان‌گیری، ثبت وقایع امنیتی، مدیریت آسیب‌پذیری، پایش امنیت ارزیابی ریسک، پاسخ به رخداد، تداوم کسب‌وکار، بازیابی اطلاعات، مدیریت تهدیدات، ممیزی امنیت، آموزش امنیت، تاب‌آوری سایبری
۶	**دسترس‌پذیری داده**	تسهیم داده استانداردهای مدیریتی	قالب‌های استاندارد، کیفیت داده، فراداده، یکپارچگی داده، قابلیت تعامل، واژگان مشترک، استانداردهای تبادل، مستندسازی، مدیریت کیفیت، کنترل نسخه، حاکمیت فراداده، ممیزی کیفیت، اعتبارسنجی داده، استانداردهای سازمانی، راهنماهای اجرایی، شاخص‌های کیفیت

ردیف	بعد اصلی	زیرمؤلفه	کدهای اولیه (نمونه)
۷	ذخیره‌سازی و انباشت داده	زیرساخت ذخیره‌سازی	مراکز داده، رایانش ابری، مخازن ملی داده، پایگاه‌های توزیع‌شده، ظرفیت ذخیره، پایداری زیرساخت، افزونگی داده، مدیریت منابع، جمع‌آوری مستمر، یکپارچه‌سازی داده، آرشیو بلندمدت، چرخه عمر داده، نگهداری داده، طبقه‌بندی داده، پاک‌سازی داده، مدیریت حجم داده
		مدیریت انباشت داده	
۸	گمنام‌سازی و ناشناس‌سازی داده	حفاظت از حریم خصوصی	حذف شناسه‌های فردی، کاهش قابلیت شناسایی، محرمانگی اطلاعات، حفاظت از داده‌های حساس، رضایت کاربران، حداقل‌سازی داده، تفکیک هویت، کنترل افشا ناشناس‌سازی آماری، مستعارسازی ، تجمیع داده، نویزافزایی، حذف ویژگی‌های حساس، ارزیابی ریسک بازشناسایی
		فناوری‌های ناشناس‌سازی	

بحث

بر اساس تحلیل مصاحبه‌ها، الزامات توسعه هوش مصنوعی بر اساس مزیت نسبی داده‌ها در ایران به شرح زیر هستند:

ایجاد زیرساختهای تنظیم‌گری داده

توسعه هوش مصنوعی مستلزم استقرار زیرساخت‌های تنظیم‌گری داده است؛ زیرساخت‌هایی که از طریق تدوین قوانین شفاف، تعیین حقوق و مسئولیت ذی‌نفعان و ایجاد نهادهای ناظر، تعادل میان نوآوری، حفاظت از حقوق افراد و بهره‌برداری مؤثر از داده‌ها را برقرار کنند. رویکردهای نوین در این حوزه نشان می‌دهد که تنظیم‌گری داده در حال حرکت به سمت الگوهای مشارکتی و انعطاف‌پذیر است. گزارش سمپوزیوم جهانی تنظیم‌گران در سال ۲۰۲۵، رویکردی نوآورانه برای رفتار با داده به عنوان یک «خدمات عمومی تنظیم‌شده» (regulated utility) ارائه می‌دهد که بر این اصل استوار است که داده‌ها مانند آب و برق، زیرساختی حیاتی هستند که باید تحت نظارت عمومی و با رعایت استانداردهای مشخص مدیریت شوند (ITU, 2025). این گزارش همچنین بر «تعبیه اعتماد در طراحی» (embed trust by design) به عنوان یکی از اصول کلیدی تنظیم‌گری تأکید دارد که به معنای لحاظ کردن ملاحظات امنیتی و حریم خصوصی از مرحله طراحی سیستم‌های داده است. ایجاد زیرساخت‌های تنظیم‌گری داده محور دیگر مورد تأکید در مصاحبه‌ها است: «در ایران قوانین مشخصی برای استفاده از داده‌های حقوقی در الگوریتم‌های هوش مصنوعی وجود ندارد، که باعث تردید در بهره‌گیری از این داده‌ها می‌شود. بسیاری از داده‌های حقوقی ممکن است تحت قوانین مالکیت فکری قرار بگیرند و بدون مجوز نمی‌توان از آن‌ها استفاده کرد» (مصاحبه شونده کد ۱). همچنین «داده که در همه دنیا بحث چالشی مستمر و دائم هست. ما در حوزه قوانین داده و مالکیت داده و تبادل داده‌ها بیشتر از بیست سال است که داریم کار می‌کنیم از وقتی دولت الکترونیک صورت گرفت. به نظرم باید رویکرد سیاست را تغییر بدهیم. در مورد بحث داده‌ها قانون خیلی زیاد داریم اما عملی نمی‌شود. مجازات بر آنها صورت می‌گیرد اما باز هم اجرا نمی‌شوند. به نظر می‌رسد سیاستی غیر از تصویب قوانین باید داشته باشیم؛ به جای تصویب زیاد، پیگیر اجرا شدن آن باشیم» (مصاحبه شونده کد ۲). مفهوم «مشارکت داده» (Data Commons) به عنوان یک رویکرد نوین در حکمرانی داده مطرح شده است که به یک منبع داده مشترک و حاکم‌شده با قوانین دسترسی روشن و نظارت عمومی اشاره دارد و می‌تواند به عنوان زیرساخت تنظیم‌گری عمل کند (Council on Business & Society Insights, 2025). این رویکرد ضمن خدمت به صنعت، تنظیم‌گران و محققان، امکان نظارت عمومی بر جریان داده‌ها را فراهم می‌کند و به کاهش تمرکز قدرت داده در دستان تعداد محدودی از شرکت‌های بزرگ کمک می‌نماید. چارچوب ارزیابی حاکمیت داده (Data Sovereignty Assessment Framework) نیز ابزاری عملی برای کمک به سازمان‌ها به منظور ایجاد تعادل بین انطباق با مقررات و نوآوری مبتنی بر داده ارائه می‌دهد (Holmström & Magnusson, 2025). این چارچوب شامل پنج بعد ارزیابی است که انطباق با قوانین و مقررات و مالکیت و کنترل داده از مهم‌ترین ابعاد آن محسوب می‌شوند. مصاحبه شونده دیگر بر لزوم تدوین قوانین مرتبط با آزادسازی داده‌ها تأکید می‌کند: «ما اگر قانون داشته باشیم، اینکه چه داده‌هایی آزادند و چه

داده‌هایی آزاد نیستند، نحوه جمع‌آوری داده‌ها و موارد دیگر استانداردسازی شده‌اند که می‌توان آن را خصوصی کرد و نیز استفاده نمود. اما اینکه ما خودمان داده‌های خودمان را نداشته باشیم، این فاجعه است. آمریکا بیشتر از خودمان از ما داده دارد. بنابراین اگر داده‌ای نداشته باشیم در هوش مصنوعی عملاً ما بازنده‌ایم. راهکار این است که اولاً دولت قانون داشته باشد. ما در بخش خصوصی سه نوع داده داریم: ۱. داده‌های خصوصی که کسی حق انتشار آن را ندارد؛ ۲. داده‌هایی که می‌تواند در اختیار کسی دیگر قرار بگیرد و در ازای آن پول دریافت شود؛ ۳. داده‌های آزاد که داده‌هایی هستند که برای همه است و در دسترس همه است. خیلی از داده‌های دولتی open data هستند و اگر در اختیار قرار بگیرند، می‌توانند استفاده کنند؛ چه خارجی و چه داخلی. اما share data را نمی‌خواهیم در اختیار خارجی‌ها قرار بگیرد و با پروتکل‌هایی در اختیار داخلی‌ها قرار داده می‌شود تا بتوانند استفاده کنند و خدمات ارائه دهند. اگر داده‌ها در اختیار قرار ندهند، بازخواست می‌شوند و می‌توان از آن‌ها شکایت کرد. وقتی ما قوانین آن را نداریم اینگونه می‌شود». به نظر مصاحبه شونده کد ۴: «بعضی داده‌ها فقط مجوز پردازش دارد یا فقط مجوز تبادل دارد یا فقط مجوز ذخیره‌سازی دارد و یا فقط مجوز تهیه دارد و یا همه را با هم دارد ولی آنکه مجوز پردازش دارد، حق ذخیره‌سازی را ندارد. نظارت بر این حوزه با قوانین قدیمی تا حدی ممکن است. مثلاً در حوزه نظامی سفارشی است و تعداد کم تولید می‌شود و نظامی‌ها توجیه دارند. دانشی که به دست آمد باید سرریز بشود در حوزه صنعت و جاهای دیگر تا بتواند توسعه پیدا بکند. تقریباً کاری که چینی‌ها انجام می‌دهند». مسئله مهم دیگر در زمینه داده‌های مرتبط با هوش مصنوعی در ایران، عدم وجود یک چارچوب قانون‌گذار تحت نظارت یک مرجع سیاستگذار است. «مراجع ملی هوش مصنوعی در ایران در جایگاه و نقش سیاستگذار نیستند. مرجع ملی سیاستگذاری هوش مصنوعی در ایران باید صرفاً نقش سیاستگذار داشته باشند تا بتوانند از این سردرگمی درآمده و جهت تسریع در ریل‌گذاری زیرساخت‌های هوش مصنوعی من جمله سر و سامان دادن به زیرساخت‌های داده‌محور در ایران جهت نزدیک شدن به اهداف جهانی در این زمینه اقدامات مؤثری انجام دهند» (مصاحبه‌شونده کد ۱۰).

توسعه نظام‌های شفاف مالکیت داده

یکی از الزامات اساسی حکمرانی داده، توسعه نظام‌های شفاف مالکیت داده است؛ نظامی که با تعیین حقوق، مسئولیت‌ها و حدود بهره‌برداری از داده‌ها برای اشخاص، سازمان‌ها و نهادهای عمومی، زمینه تولید، اشتراک‌گذاری، سرمایه‌گذاری و استفاده مسئولانه از داده‌ها را فراهم کرده و از بروز تعارضات حقوقی جلوگیری کند. نظام‌های سنتی مالکیت داده که عمدتاً بر مالکیت نهادی تأکید دارند، با انتقادات جدی مواجه شده‌اند و رویکردهای نوین به سمت مدل‌های کاربرمحور و مبتنی بر رضایت در حال حرکت هستند. «در هوش مصنوعی اگر بحث‌های مالکیت داده و دسترسی به داده‌های بومی حل نشود، خیلی از این مدل‌های زیرساختی که لازم است را اساساً نمی‌شود داشت. بنابراین من فکر می‌کنم بخش‌هایی از حاکمیت که در این حوزه کار می‌کنند مثلاً پژوهشکده‌هایی که دولتی هستند، کمک کنند که هرکسی که یک دیتاستی دارد یا می‌تواند یک داده‌ای را جمع کند، این داده‌ها را آنجا ثبت کند و هزینه‌های این کار را به او بدهند» (مصاحبه شونده کد ۳). رویکرد «کپسول داده» (Data Capsule) تحولی اساسی در مفهوم مالکیت داده ایجاد کرده است. این رویکرد با استفاده از فناوری بلاک‌چین و هستی‌شناسی (ontology)، امکان تغییر مالکیت داده از نهادها به افراد را فراهم می‌آورد ((Baraku et al., 2024)). در این مدل، افراد می‌توانند شرایط استفاده از داده‌های خود را تعیین کنند و بر شفافیت و امنیت داده‌های خود نظارت داشته باشند. همچنین پژوهشی به چالش مدیریت رضایت در مقیاس بزرگ در زیرساخت‌های دیجیتال عمومی می‌پردازد و مدلی برای نمایش حالت‌های مالکیت داده و پیامدهای آن برای جریان‌های داده مبتنی بر رضایت ارائه می‌دهد (arXiv, 2025). هدف این مدل، ایجاد سیستم‌های شفاف، امن و کاربرمحور برای مدیریت رضایت است که با قوانین در حال تحول حریم خصوصی همخوانی داشته باشد. از نظر مصاحبه شونده کد ۷: «تا زمانی که تکلیف مالکیت داده مشخص نباشد، هیچ انگیزه‌ای برای تولید، اشتراک‌گذاری یا سرمایه‌گذاری روی داده ایجاد نمی‌شود. وقتی افراد و سازمان‌ها ندانند حقوقشان نسبت به داده چیست، طبیعی است که داده‌های خود را در اختیار دیگران قرار ندهند. بنابراین، حاکمیت باید یک چارچوب

روشن برای مالکیت و بهره‌برداری از داده‌ها طراحی کند». مطالعه‌ای دیگر نشان می‌دهد که اصول FAIR (قابل یافتن، قابل دسترس، قابل هم‌کاری و قابل استفاده مجدد) صرفاً استانداردهای فنی نیستند، بلکه به عنوان رویه‌های اجتماعی، روابط قدرت را در شبکه‌های علمی تغییر می‌دهند و بر مفاهیم مالکیت و دسترسی‌پذیری داده تأثیر می‌گذارند (Schwarzfuch,2025).

تقویت امنیت داده

حکمرانی اثربخش داده مستلزم تقویت امنیت داده از طریق توسعه زیرساخت‌های فنی، استانداردهای امنیتی و نظام‌های مدیریت ریسک است تا ضمن حفاظت از داده‌های حساس، زمینه بهره‌برداری ایمن و پایدار از داده‌ها در توسعه هوش مصنوعی فراهم شود. با افزایش تهدیدات سایبری و پیچیده‌تر شدن حملات، رویکردهای سنتی امنیت داده دیگر کافی نیستند. راهنمای امنیت داده با رویکرد اعتماد صفر در دولت فدرال ایالات متحده، چارچوبی برای عملیاتی‌سازی امنیت داده ارائه می‌دهد (U.S. Federal CDO Council & CISO Council, 2025). این رویکرد بر اصل «هرگز اعتماد نکن، همیشه تأیید کن» استوار است و به سازمان‌ها کمک می‌کند تا در برابر تهدیدات داخلی و خارجی مقاوم‌تر شوند. همچنین مقاله دیگری به ارتقاء هم‌زمان امنیت و ارزش داده می‌پردازد که به سازمان‌ها کمک می‌کند تا داده‌ها را بر اساس حساسیت طبقه‌بندی کرده و ریسک‌های انطباق‌پذیری را مدیریت کنند (Thangaraju, 2022). «ما در حکمرانی داده، اول قانون داده را می‌خواهیم، بعد از این کسب‌وکارها را شکل بدهیم. مثلاً کسب‌وکارهایی که در حوزه داده باز کار می‌کنند را حمایت کرده و رشد بدهیم، شرکت‌هایی که تسهیم داده را در اختیار قرار می‌دهند، کمک کنیم کسب‌وکار راه بیندازند و در حوزه داده‌های خصوصی، شرکت‌هایی حمایت شده و رشد پیدا می‌کنند که امنیت داده‌ها را تضمین می‌کنند تا داده‌ها لو نروند. دولت برای داده‌های خودش تضمین امنیت را قرار داده است اما باز هم لو می‌رود زیرا وقتی داده لو می‌رود که در تبادل داده دقت انجام نمی‌گیرد» (مصاحبه شونده کد ۸). همچنین در نقلی دیگر: «موضوع داده‌محوری ترکیب اقدامات فنی و مدیریتی است. مثل تنظیم مقررات، امنیت و موارد مرتبط دیگر تا بتوانند بشناسند و داده‌ها را با در نظر داشتن تمهیدات مرتبط واگذار کنند. بنابراین باید مراحل متناوبی در این حوزه انجام شود: چند مرحله برای تضمین امنیت داده‌ها وجود دارد: ۱. تهیه داده، ۲. نگهداشت داده، ۳. تبادل داده و ۴. پردازش داده. برای هر کدام پروتکل نیاز است» (مصاحبه شونده کد ۹). مراکز داده تحقیقاتی مانند RDC دانشگاه اورا، بر یکپارچگی، امنیت و تاب‌آوری داده‌ها در چارچوب اصول FAIR و قوانین حریم خصوصی تمرکز دارند و نشان می‌دهند که چگونه می‌توان امنیت داده را با دسترسی‌پذیری و قابلیت استفاده مجدد ترکیب کرد (University of Évora, 2025).

استانداردسازی داده

یکی از الزامات اساسی حکمرانی داده، استانداردسازی داده‌ها از طریق ارتقای کیفیت، یکپارچگی، سازگاری و قابلیت تعامل میان داده‌های تولیدشده در سازمان‌های مختلف است؛ زیرا داده‌های غیراستاندارد و کم‌کیفیت، کارایی مدل‌های هوش مصنوعی را کاهش داده و قابلیت اعتماد به خروجی‌های آن را با چالش مواجه می‌کند. تحولات اخیر در هوش مصنوعی، نیاز به استانداردهای جدید و پیشرفته‌تر را آشکار ساخته است. «یکی از مشکلات اصلی این است که هر دستگاهی داده‌های خودش را با یک قالب و استاندارد متفاوت تولید و نگهداری می‌کند. وقتی این داده‌ها قرار است کنار هم قرار بگیرند، تازه مشخص می‌شود که قابل تجمیع و استفاده نیستند. اگر استاندارد مشترکی برای تولید و مدیریت داده وجود نداشته باشد، بخش زیادی از زمان و هزینه توسعه هوش مصنوعی صرف پاک‌سازی و یکسان‌سازی داده‌ها خواهد شد، نه خودِ توسعه مدل‌ها» (مصاحبه‌شونده، کد ۱۱). «بسیاری از داده‌ها ممکن است نادرست، ناقص یا با خطا باشند. این مشکل می‌تواند به‌ویژه در استفاده از داده‌ها برای آموزش الگوریتم‌های هوش مصنوعی چالش‌برانگیز باشد، چرا که داده‌های اشتباه می‌توانند باعث نتایج نادرست و کاهش دقت مدل‌های هوش مصنوعی شوند» (مصاحبه شونده کد ۱۴). مقاله «فراتر از KIS: چرا هوش مصنوعی به قوانین جدید داده‌های SMART نیاز دارد» استدلال می‌کند

که استانداردهای سنتی «ساده نگه دار» (Keep It Simple) برای اکوسیستم‌های مبتنی بر هوش مصنوعی کافی نیستند و چارچوب جدید SMART را پیشنهاد می‌کند که شامل پنج ویژگی است: ساختاریافته (Structured)، غنی از فراداده (Metadata-rich)، انعطاف‌پذیر (Adaptable)، قابل استفاده مجدد (Reusable) و قابل ردیابی (Traceable). این استانداردها برای تضمین انطباق، قابلیت هم‌کاری و نوآوری در عصر هوش مصنوعی حیاتی هستند (Thomson Reuters Institute, 2025). مؤسسه استانداردهای اروپایی (ETSI) در ژوئیه ۲۰۲۵ از برنامه کاری جدید خود برای توسعه استانداردهایی جهت قابل کشف بودن (discoverable)، قابلیت هم‌کاری (interoperable) و قابل اعتماد بودن (trustworthy) داده‌ها خبر داد (ETSI, 2025). این استانداردها، زیربنای نوآوری در حاکمیت داده و تبادل امن داده در صنایع مختلف هستند و به ایجاد اکوسیستم‌های داده قابل اعتماد کمک می‌کنند. پروژه فهرست‌نویسی داده MECO در لوکزامبورگ نیز نمونه‌ای عملی از پیاده‌سازی استانداردهای فراداده‌ای (مانند DCAT-AP-LU) برای بهبود قابلیت کشف و دسترسی‌پذیری داده‌های بخش عمومی است (FAIR EDIH, 2025).

افزایش دسترسی‌پذیری داده

یکی از الزامات حکمرانی داده، افزایش دسترسی‌پذیری داده‌ها از طریق ایجاد سازوکارهای قانونی، فنی و نهادی برای اشتراک‌گذاری هدفمند و ایمن داده‌هاست؛ به‌گونه‌ای که ضمن حفظ محرمانگی و حقوق مالکیت، پژوهشگران، کسب‌وکارها و نهادهای عمومی بتوانند به داده‌های موردنیاز برای توسعه هوش مصنوعی دسترسی داشته باشند. دسترسی‌پذیری داده نه تنها یک مسئله فنی، بلکه یک رویه اجتماعی با پیامدهای قدرت و عدالت است. «الان مشکل این نیست که داده نداریم؛ مشکل این است که داده‌ها در سازمان‌های مختلف محبوس شده‌اند و دسترسی به آن‌ها بسیار دشوار است. اگر سازوکار مشخصی برای اشتراک‌گذاری داده میان دستگاه‌ها و بخش خصوصی ایجاد نشود، هر مجموعه مجبور است دوباره همان داده‌ها را تولید کند و این هم زمان را هدر می‌دهد و هم توسعه هوش مصنوعی را کند می‌کند» (مصاحبه‌شونده، کد ۱۰). مسئله اراده آزادسازی داده نیز مورد تأکید یکی دیگر از مصاحبه‌شوندگان است. او می‌گوید: «یکی از نکات مهم این است که باید انگیزه لازم برای آزادسازی داده‌ها وجود داشته باشد. بر این اساس هوش مصنوعی می‌تواند مؤثر واقع شود. توجه به اینکه سازمان‌ها بدانند باید داده‌های تمیز تولید، نگهداری و با سازوکاری مشخص به یکدیگر تحویل دهند. اساساً دو نوع داده داریم: یک دسته داده‌های دولتی یا خصولتی و یک دسته داده‌های شرکت‌های خصوصی و مردم. برای مثال داده‌های یک شرکت خصوصی مثل اسنپ که داده جابجایی مردم را در اختیار دارد و یک داده با ارزش است. می‌توان این داده‌ها را نگهداری و در اختیار دانشمندان بگذاریم» (مصاحبه شونده کد ۳). مطالعه‌ای که به بررسی اصول FAIR در علم شهروندی پرداخته، نشان می‌دهد که دسترسی‌پذیری داده نه تنها یک مسئله فنی، بلکه یک رویه اجتماعی است که مذاکرات درباره دسترسی‌پذیری داده، روابط قدرت را در شبکه‌های علمی بازتعریف می‌کند و بر مفهوم «داده منصفانه» (fair data) تأثیر می‌گذارد (Schwarzfuch,2025). همچنین پروفسور توماس هارتونگ بر اهمیت دسترسی‌پذیری و شفافیت داده‌ها برای حاکمیت علمی و کاهش وابستگی به زیرساخت‌های خارجی تأکید کرده و از مفهوم «تاب‌آوری داده» (Data Resilience) یاد می‌کند (Hartung, 2025). با توجه به این نکات، مصاحبه‌شوندگان راهکارهایی برای مواجهه با ابعاد مختلف مسئله زیرساخت داده مطرح کرده‌اند که در ادامه به آن اشاره می‌شود: «تسهیل دسترسی پژوهشگران، دانشگاه‌ها، مؤسسات پژوهشی و شرکت‌های فعال به داده‌های بومی جهت توسعه الگوریتم‌های هوش مصنوعی برای گسترش خدمات مربوط به آن» (مصاحبه شونده کد ۵). «ایجاد و عمومی‌کردن دیتاست‌های اختصاصی غنی در حوزه‌های دارای اولویت به منظور استفاده محققان و کسب‌وکارهای فعال در حوزه‌های مربوطه». یک مصاحبه شونده که مقام مسئول نیز هست می‌گوید: «اساساً فناوری هوش مصنوعی، یک فناوری داده‌محور است و عملاً با شکل‌گیری Big Data است که تکنولوژی هوش مصنوعی به توانایی بالایی می‌رسد. اگر زیرساخت داده در کشور شکل بگیرد، عملاً زیست‌بوم داده‌ها فعال شده و طی آن شرکت‌ها می‌توانند داده‌های خود را

به اشتراک بگذارند و مادامی که این مهم (زیرساخت داده) شکل نگیرد، نمی‌توان چندان به پیشرفت هوش مصنوعی امید بست» (مصاحبه شونده کد ۱۳).

انباشت و ذخیره سازی داده

یکی از الزامات حکمرانی داده، توسعه زیرساخت‌های انباشت و ذخیره‌سازی داده است تا از طریق ایجاد مخازن داده‌ای امن، یکپارچه و مقیاس‌پذیر، امکان حفظ، مدیریت و بهره‌برداری بلندمدت از داده‌های باکیفیت برای آموزش و توسعه سامانه‌های هوش مصنوعی فراهم شود. زیرساخت‌های ذخیره‌سازی و انباشت داده، ستون فقرات هر نظام حکمرانی داده محسوب می‌شوند و باید امن، مقیاس‌پذیر، کارآمد و مطابق با قوانین حریم خصوصی طراحی شوند. «در بسیاری از دستگاه‌ها داده‌ها به‌صورت پراکنده، موقت و بدون برنامه مشخص نگهداری می‌شوند و حتی بخشی از آن‌ها به مرور زمان از بین می‌رود. اگر زیرساخت مناسبی برای ذخیره‌سازی و انباشت داده ایجاد نشود، عملاً سرمایه داده‌ای کشور از دست خواهد رفت و امکان آموزش مدل‌های بزرگ هوش مصنوعی بر پایه داده‌های بومی نیز فراهم نخواهد شد» (مصاحبه‌شونده، کد ۵). گزارش نهایی مخزن داده‌های تحقیقاتی مؤسسه کارولینسکا (KI) در سوئد، نمونه‌ای از ایجاد یک مخزن نهادی امن، قانونی و پایدار برای داده‌های تحقیقاتی است که راه‌حلی برای ذخیره‌سازی و بایگانی مجموعه‌داده‌های باز و محافظت‌شده فراهم کرده و دسترسی‌پذیری را از طریق ثبت فراداده و شناسه‌های دیجیتال (DOI) در راستای اصول FAIR تضمین می‌کند (Karolinska Institutet, 2025). از نظر مصاحبه‌شونده دیگر مشکلات زیادی در خصوص این زیرساخت داده در حال حاضر در کشور وجود دارد: «مشکل دیگر در کشور این است که داده درست تهیه نشده و ناقص است. در دنیا سانسور داده وجود دارد، به صورت هوشمندانه هست اما ما داده‌های خودمان را هم به صورت درست نداریم؛ داده، زمینه اولیه هوش مصنوعی است و باید باشد تا هوش مصنوعی کار کند. داده، زیرساخت هوش مصنوعی است، نبود داده موجب می‌شود عقب بمانیم. آمریکا برتری‌اش برای این است که داده‌ها در اختیار دولت است و شرکت‌های خصوصی داده‌ها را تهیه می‌کنند. اروپا عقب‌ماندگی‌اش در این است که در داده‌ها سخت‌گیری‌اش زیاد است و در اختیار شرکت‌ها قرار نمی‌دهد» (مصاحبه شونده کد ۴). «ما در ایران سازوکاری برای توبیخ ایراد در داده‌ها وجود ندارد. نقص داده‌ها برایشان مهم نیست. نبود داده خطرناک است. در نهادهای دولتی و اجرایی ما، اینکه داده‌شان ناقص باشد، برایشان هیچ مسئله‌ای نیست. این مقدمه‌ای است برای اینکه هوش مصنوعی دچار چالش بشود. ما الان بخواهیم از هوش مصنوعی در حکمرانی استفاده بکنیم، نمی‌توانیم استفاده بکنیم؛ زیرا نقص داده وجود دارد. این چالش چون از گذشته هست، از دست‌دادن داده‌های گذشته موجب می‌شود که ما نتوانیم مدل‌هایمان را ایجاد بکنیم؛ برای مثال هند که از ما عقب‌تر بوده است، آمده است مسئله داده‌ها را حل کرده است؛ برای ما خیلی فاجعه‌بار است که هنوز این مسئله را حل نکرده‌ایم» (مصاحبه شونده کد ۶). به عنوان مثال در حوزه سلامت داده‌های زیادی داریم که خوب نگهداری نمی‌شوند و این پرونده‌ها الکترونیکی نشده‌اند و تلف می‌شوند.

ناشناس‌سازی و گمنام‌سازی داده

یکی دیگر از الزامات حکمرانی داده، استقرار سازوکارهای مؤثر برای گمنام‌سازی و ناشناس‌سازی داده‌هاست. این اقدام با حذف یا پنهان‌سازی اطلاعات هویتی افراد، امکان بهره‌برداری از داده‌ها برای توسعه هوش مصنوعی را فراهم می‌کند، بدون آنکه حریم خصوصی افراد به خطر افتد؛ ازاین‌رو، نقش مهمی در افزایش امنیت داده‌ها و جلب اعتماد عمومی به زیست‌بوم داده ایفا می‌کند. گمنام‌سازی و ناشناس‌سازی داده از تکنیک‌های کلیدی برای حفظ حریم خصوصی در عین حفظ کارایی داده‌ها هستند و به ویژه در حوزه‌های سلامت، مالی و تحقیقاتی کاربرد گسترده‌ای دارند. «اگر قرار باشد داده‌های سلامت، مالی یا آموزشی در اختیار پژوهشگران و شرکت‌ها قرار بگیرد، اولین شرط این است که هویت افراد کاملاً محفوظ بماند. با استفاده از روش‌های گمنام‌سازی و ناشناس‌سازی می‌توان از ارزش داده‌ها برای آموزش مدل‌های هوش مصنوعی استفاده کرد، بدون اینکه اطلاعات شخصی افراد

افشا شود. این موضوع باید به یک الزام جدی در حکمرانی داده تبدیل شود» (مصاحبه‌شونده، کد ۱۲). شرکت TrustArc مروری بر تکنیک‌های پیشرو گمنام‌سازی داده شامل پوشانندگی (Masking)، تعمیم‌دهی (Generalization)، نام‌گذاری مستعار (Pseudonymization)، داده‌های مصنوعی و تجمیع (Aggregation) ارائه می‌دهد و گمنام‌سازی را به عنوان سنگ بنای انطباق و اعتماد معرفی کرده و به چگونگی تعادل بین حفظ حریم خصوصی و کارایی داده می‌پردازد (TrustArc, 2025). همچنین arXiv به بررسی تکنیک‌های مختلف «نام‌گذاری مستعار» (Pseudonymization) برای حفظ حریم خصوصی در عین حفظ کارایی مدل‌های پردازش زبان طبیعی (NLP) پرداخته و نشان می‌دهد که چگونه می‌توان داده‌های متنی را بدون کاهش قابل توجه کیفیت مدل‌ها، ناشناس کرد (arXiv, 2025). از نظر مصاحبه شونده دیگر: «می‌شود داده‌هایی که مربوط به دولت هست را به شکل آزاد و قسمت‌هایی که مربوط به بحث حریم خصوصی‌شان است را حذف کنند و یا به‌اصطلاح گمنام‌سازی کنند یعنی داده‌های هویتی را حذف می‌کنند. مثلاً کسانی که در ۱۵ سال گذشته تا به الان بیماری سرطان گرفته‌اند. تمام فایل‌ها و داکیومنت‌های اینها که در بیمارستان‌ها است. برای مثال اسامی اینها را برمی‌داریم می‌شود یک شخص ایکسی که نمی‌دانیم چه کسی است. بعد می‌توانیم متوجه شویم که وزارت بهداشت چه داروهایی دارد و در ۵ سال آینده روی آنها سرمایه‌گذاری کرده است و مجوز ساخت دارو داده است. در حوزه اقتصاد و کشاورزی هم همینطور است» (مصاحبه شونده کد ۶). مشارکت فنلاند و لوکزامبورگ در حاکمیت داده‌های سلامت، نمونه‌ای از استفاده از داده‌های نام‌گذاری‌شده (Pseudonymised) در محیط‌های امن و محیط‌های آزمایشی (Sandbox) نظارتی هوش مصنوعی است که با هدف بهبود شفافیت و تقویت اعتماد عمومی به نحوه استفاده از داده‌های بخش عمومی برای تحقیق و نوآوری انجام می‌شود (FAIR EDIH, 2025).

تقویت اعتماد عمومی به زیست بوم داده

یکی از پیش‌نیازهای موفقیت حکمرانی داده، ایجاد و تقویت اعتماد عمومی به نحوه جمع‌آوری، نگهداری، پردازش و استفاده از داده‌هاست؛ زیرا بدون اعتماد، مشارکت شهروندان و سازمان‌ها در اشتراک‌گذاری داده‌ها با چالش جدی مواجه خواهد شد. اعتماد عمومی یکی از ارکان اساسی حکمرانی داده مؤثر است و بدون آن، حتی بهترین سیستم‌های حکمرانی داده نیز با شکست مواجه خواهند شد. «اگر مردم احساس کنند که داده‌هایشان ممکن است بدون ضابطه یا خارج از هدف اولیه مورد استفاده قرار گیرد، طبیعی است که تمایلی به اشتراک‌گذاری اطلاعات نخواهند داشت. حاکمیت باید با شفافیت، پاسخگویی و تضمین حفظ حریم خصوصی، اعتماد عمومی به زیست‌بوم داده را تقویت کند؛ چون بدون این اعتماد، توسعه هوش مصنوعی بر پایه داده‌های بومی با مانع جدی روبه‌رو می‌شود» (مصاحبه‌شونده، کد ۹). تحقیق مؤسسه تورینگ به اندازه‌گیری نگرش عمومی نسبت به پردازش داده‌های شخصی توسط آژانس‌های امنیت ملی می‌پردازد و نشان می‌دهد که حمایت گسترده است اما همگانی نیست و بخش قابل توجهی از مردم، به ویژه در میان بزرگسالان جوان و آسیب‌پذیر، مخالف هستند. این مطالعه بر نیاز به درک دقیق‌تر از ترجیحات عمومی برای حفظ اعتماد عمومی تأکید دارد (The Alan Turing Institute, 2025). «یک مسئله کلی در رابطه با مردم مهم است و آن بحث اعتمادسازی و کیفیت سرویس‌دهی است چون مردم اطلاعاتشان را در اختیار ما قرار می‌دهند نباید نگران باشند و باید یک مقدار حس کنند که این کار باعث خواهد شد که کیفیت سرویس‌دهی به آنها افزایش یابد» (مصاحبه شونده کد ۱). مشارکت داده به عنوان یک رویکرد نوین در حکمرانی، می‌تواند با ایجاد شفافیت و پاسخگویی در مدیریت داده‌ها، به تقویت اعتماد عمومی کمک کند (Council on Business & Society Insights, 2025).

نتیجه‌گیری

یافته‌های این پژوهش نشان داد که مزیت نسبی ایران در توسعه هوش مصنوعی را نمی‌توان صرفاً در زیرساخت‌های محاسباتی، الگوریتم‌ها یا توان پردازشی جست‌وجو کرد، بلکه داده‌های بومی و متنوع کشور به‌عنوان یک دارایی راهبردی، ظرفیت ایجاد مزیت

رقابتی در این حوزه را دارند. با این حال، بهره‌برداری از این ظرفیت بدون استقرار یک نظام کارآمد حکمرانی داده امکان‌پذیر نخواهد بود. نتایج تحلیل مصاحبه‌ها هشت الزام کلیدی شامل ایجاد زیرساخت‌های تنظیم‌گری داده، توسعه نظام‌های شفاف مالکیت داده، تقویت امنیت داده، استانداردسازی داده‌ها، افزایش دسترسی‌پذیری داده، انباشت و ذخیره‌سازی داده، گمنام‌سازی و ناشناس‌سازی داده‌ها و تقویت اعتماد عمومی به زیست‌بوم داده را به‌عنوان ارکان حکمرانی داده شناسایی کرد. بررسی تطبیقی یافته‌های مصاحبه‌ها با ادبیات بین‌المللی نشان می‌دهد که چالش‌های ایران در حوزه حکمرانی داده، اگرچه منحصربه‌فرد نیست، اما در برخی ابعاد دارای شدت و عمق بیشتری است. در حالی که کشورهای پیشرو در حال حرکت به سمت رویکردهای ترکیبی، مشارکتی و مبتنی بر اعتماد در حکمرانی داده هستند، ایران همچنان با مسائلی نظیر فقدان قوانین اجرایی مؤثر، پراکندگی داده‌ها در سازمان‌های مختلف، نبود استانداردهای یکپارچه و ضعف در زیرساخت‌های ذخیره‌سازی و امنیت داده مواجه است. با این حال، ظرفیت‌های قابل توجهی در حوزه داده‌های بومی و متنوع کشور وجود دارد که در صورت مدیریت صحیح، می‌تواند به منبعی برای تولید ارزش و مزیت رقابتی در توسعه هوش مصنوعی تبدیل شود. تحقق این الزامات می‌تواند زمینه شکل‌گیری یک زیست‌بوم داده کارآمد را فراهم کرده و بستر توسعه مدل‌های هوش مصنوعی مبتنی بر داده‌های بومی را تقویت کند. ازاین‌رو، سیاستگذاران باید حکمرانی داده را نه یک موضوع صرفاً فنی، بلکه یک اولویت راهبردی در سیاستگذاری هوش مصنوعی تلقی کنند؛ زیرا آینده رقابت کشورها در این حوزه، بیش از هر چیز به توانایی آن‌ها در مدیریت، حفاظت و بهره‌برداری هوشمندانه از داده‌های بومی وابسته خواهد بود. نکته قابل توجه آن است که حکمرانی داده صرفاً یک ابزار پشتیبان برای توسعه هوش مصنوعی نیست، بلکه خود به‌عنوان یکی از پیش‌شرط‌های شکل‌گیری ظرفیت‌های ملی در این حوزه محسوب می‌شود. کشورهایی که قادر به ایجاد نظام‌های منسجم حکمرانی داده هستند، توان بیشتری در تولید مدل‌های بومی، کاهش وابستگی فناورانه و افزایش رقابت‌پذیری بین‌المللی خواهند داشت. در مقابل، نبود سازوکارهای مؤثر برای مدیریت و بهره‌برداری از داده، موجب پراکندگی منابع داده‌ای، کاهش اعتماد ذی‌نفعان و محدود شدن ظرفیت نوآوری خواهد شد. از این‌رو، ضروری است سیاست‌های هوش مصنوعی هم‌زمان با سیاست‌های حکمرانی داده طراحی و اجرا شوند و این دو حوزه به‌صورت مکمل و یکپارچه مورد توجه قرار گیرند. در چنین شرایطی، داده‌های بومی می‌توانند از یک منبع اطلاعاتی صرف، به سرمایه‌ای راهبردی برای خلق ارزش اقتصادی، ارتقای کیفیت تصمیم‌گیری و تقویت اقتدار فناورانه کشور تبدیل شوند.

تعارض منافع

متن حاضر فاقد هرگونه تعارض منافع است.

References

1. Al Marri, A., Albloosh, F., Moussa, S., & Elmessiry, H. (2019). Study on the impact of artificial intelligence on government E-service in Dubai. In 2019 International Conference on Digitization (ICD) (pp. 153-159). IEEE.
2. Anderson, K. P. (2019). Artificial intelligence-augmented ECG assessment: The promise and the challenge. Journal of Cardiovascular Electrophysiology, 30(5).
3. arXiv. (2025). A General Pseudonymization Framework for Cloud-Based LLMs: Replacing Privacy Information in Controlled Text Generation. https://arxiv.org
4. Baraku, V., Paraskakis, I., Veloudis, S., & Yadav, P. (2024). Responsible Information Sharing in the Era of Big Data Analytics: Facilitating Digital Economy Through the Use of Blockchain Technology and Observing GDPR. Proceedings of the 14th International Conference on Cloud Computing and Services Science (CLOSER), pp. 257–264
5. Behzadifar, Meysam. Azari, Samad, Sajedimehr, Negin (2025). Challenges of using artificial intelligence in Iran's health system: a qualitative study. J PREV MED HYG 2025; 66
6. Cave, S., & ÓhÉigeartaigh, S. S. (2018). An AI race for strategic advantage: rhetoric and risks. In Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society (pp. 36-40).
7. Corbin, J., & Strauss, A. (2015). Basics of Qualitative Research (4th ed.). Sage.
8. Council on Business & Society Insights. (2025). Data commons, the new frontier. Council on Business & Society Insights
9. Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., ... & Williams, M. D. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International journal of information management, 57, 101994.

10. ETSI. (2025). ETSI work programme for trustworthy data ecosystems. European Telecommunications Standards Institute. https://www.etsi.org
11. FAIR EDIH. (2025). Findata and Luxembourg forge data governance alliance ahead of EU health data reforms. FAIR EDIH News. https://www.fairedih.eu
12. Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review. 1(1)
13. Guenduez, A. A., & Mettler, T. (2023). Strategically constructed narratives on artificial intelligence: What stories are told in governmental artificial intelligence policies?. Government Information Quarterly, 40(1), 101719.
14. Hartung, T. (2025). Data resilience and scientific sovereignty: An interview with Professor Thomas Hartung. https://www.frontiersin.org/news/2025/10/02
15. Holmström Jonny, Magnusson Johan. (2025). Balancing innovation and regulation: The Data Sovereignty Assessment Framework. The Journal of Strategic Information Systems. In press
16. Hummel, P., Braun, M., Augsberg, S., & Dabrock, P. (2018). Sovereignty and data sharing. ITU Journal on Future and Evolving Technologies, 1(2).
17. ITU. (2025). Global Symposium for Regulators 2025 - Chairman's report. International Telecommunication Union. https://www.itu.int
18. Janssen, M., & Kuk, G. (2016). Big and open linked data (BOLD) in research, policy, and practice. Journal of Organizational Computing and Electronic Commerce, 26(1-2), 3-13.
19. Janssen, M., et al. (2020). Data Governance: Organizing Data for Trustworthy AI. Government Information Quarterly, Volume 37, Issue 3,
20. Judiciary Statistics Center [In Persian].
21. Karolinska Institutet. (2025). Slutrapport KI Data Repository – Fas 1 Flaggskeppsprojekt inom Svensk Nationell Datatjänst. Zenodo. https://zenodo.org
22. Khatri, V., & Brown, C. V. (2010). Designing Data Governance. Communications of the ACM
23. Nambu, T. (2016). Legal regulations and public policies for next-generation robots in Japan. Ai & society, 31(4), 483-500.
24. OECD. (2024). OECD Framework for the Classification of AI Systems.
25. Panian, Z., (2010) Some Practical Experiences in Data Governance, World Academy of Science, Engineering and Technology.
26. Pour Ezzat, A. A; Abdi, B. (2019). Identifying Meta-process of Information and Communication Technology Trends in Defense Industry Future Planning Towards Achieving an Islamic-Iranian Model of Progress, Defense Futures Studies Quarterly, 3(10) [In Persian].
27. Qiu, Yanrui & Hu, Zhimin. 2026. Construction of a theoretical Framework for Scientific DataGovernance. Scientific Data
28. Rivas, H., & Wac, K. (Eds.). (2018). Digital health: scaling healthcare to the world. Springer.
29. Russell, S. J., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach (4th ed.). Pearson.
30. Schwarzfuchs, E. N. (2025). FAIR data, fair data: data management principles and data ownership in citizen science. Information, Communication & Society, 1–17
31. Siau, K. (2017). Impact of artificial intelligence, robotics, and automation on higher education. AMCIS.
32. Strauss, A., & Corbin, J. (1998). Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory (2nd ed.). Sage
33. Taeihagh, A. (2021). Governance of artificial intelligence. Policy and society, 40(2), 137-157.
34. Thangaraju, D. (2022). Data Classification: Enabling Robust Data Governance and Access Management in Enterprise Environments. International Journal of Innovative Research in Computer Technology (IJIRCT)
35. The Alan Turing Institute. (2025). AI will be key to future national security decision making but brings its own risks The Alan Turing Institute. https://www.turing.ac.uk
36. Thomson Reuters Institute. (2025). Outgrowing KIS: Why AI needs a new SMART data rulebook. Thomson Reuters Institute. https://www.thomsonreuters.com
37. U.S. Federal CDO Council & CISO Council. (2025). Federal Zero Trust Data Security Guide. Data.gov. https://www.data.gov
38. UNESCO. (2021). Recommendation on the Ethics of Artificial Intelligence
39. United Nations (2023). The Global Digital Compact. United Nations Office for Digital and Emerging Technologies
40. University of Évora. (2025). Alentejo Research Data Centre (RDC): Infrastructure for research data storage and access. University of Évora. https://www.uevora.pt
41. Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. Public Management Review, 21(7), 1076-1100.
42. World Bank (2021). World Development Report 2021: Data for Better Lives.