



Data Colonialism Inquiry: From Explaining New Forms of Domination to the Necessity of National Data Governance

Mahdieh Latifzadeh*

PhD in Private Law; Assistant Professor of Private Law;
Department (The Research Group) of Islamic Jurisprudence
and Law; Institute for Islamic Studies in Humanities; Ferdowsi
University of Mashhad; Mashhad, Iran Email: latifzadeh@um.ac.ir

Received: 02, Feb. 2025

Accepted: 16, May 2025

Abstract: In the current era, where data is recognized as a strategic asset of nations, large technology companies, by leveraging advanced tools, seize users' data instead of conquering lands and natural resources. This study demonstrates how big tech companies have shaped a new concept of domination-data colonialism- by creating data-centric structures. This study employs a qualitative content analysis method to conduct a multifaceted examination of the phenomenon of data colonialism. Although the scope of data colonialism transcends geographical boundaries and has become a global challenge with international dimensions, this study focuses on the national domain, especially proposing solutions to strengthen the country's capacity to confront this phenomenon. The findings identify four main factors as foundational elements of data colonialism: legal gaps and weaknesses in legal requirements, lack of technical infrastructure, weak supervisory mechanisms, and low levels of data literacy. These factors interact to weaken data sovereignty and ultimately undermine the data governance system. Therefore, to counter this phenomenon, the present study emphasizes the necessity of adopting a comprehensive and systematic approach and offers corresponding solutions, including specific legislation and strengthening legal frameworks, developing technical infrastructure, enhancing supervisory mechanisms, and increasing digital literacy. The results also show that these solutions, through their interaction, can reinforce national data sovereignty and solidify the data governance system. Ultimately, the study confirms that effectively addressing this phenomenon requires defining a new legal framework in which data sovereignty is recognized and supported as one of the fundamental pillars of national sovereignty.

Keywords: Data Colonialism, Data Governance, Digital Literacy, Cyber Power, General Data Protection Regulation (GDPR)

* Corresponding Author

واکاوی استعمار داده: از تبیین سلطه‌گری نوین تا ضرورت حکمرانی ملی بر داده (استعمار داده)

مهدیه لطیف‌زاده

دکتری حقوق خصوصی؛ استادیار؛ گروه پژوهشی فقه
و حقوق اسلامی؛ پژوهشکده مطالعات اسلامی در علوم
انسانی؛ دانشگاه فردوسی مشهد؛ مشهد، ایران؛
latifzadeh@um.ac.ir



مقاله برای اصلاح به مدت ۹ روز نزد پدیدآور بوده است.

پذیرش: ۱۴۰۴/۰۲/۲۷

دریافت: ۱۴۰۳/۱۱/۱۴

تشریح علمی | رتبه بین‌المللی
پژوهشگاه علوم و فناوری اطلاعات ایران
(ایرانداک)

شاخه (چاپی) ۲۲۵۱-۸۲۲۳

شاخه (الکترونیکی) ۲۲۵۱-۸۲۳۱

نمایه در SCOPUS، ISI، و LISTA

jipm.irandoc.ac.ir

دوره ۴۰ | شماره ۴ | صص ۱۱۴۶-۱۱۱۳

تابستان ۱۴۰۴

<https://doi.org/10.22034/jipm.2025.2052402.1927>



چکیده: در عصر حاضر که داده به‌عنوان سرمایه راهبردی کشورها شناخته می‌شود، شرکت‌های بزرگ فناوری با بهره‌گیری از ابزارهای پیشرفته به‌جای تسخیر سرزمین‌ها و منابع طبیعی، داده‌های کاربران را تصاحب می‌کنند. در این راستا، پژوهش حاضر نشان می‌دهد که چگونه شرکت‌های بزرگ فناوری با ایجاد ساختارهای داده‌محور، مفهوم جدیدی از سلطه‌گری (استعمار داده) را شکل داده‌اند. در این مسیر، مطالعه حاضر با بهره‌گیری از روش تحلیل محتوای کیفی به واکاوی چندجانبه پدیده استعمار داده پرداخته است. به‌رغم اینکه دامنه نفوذ استعمار داده از مرزهای جغرافیایی فراتر رفته و به چالشی جهانی تبدیل شده و ابعاد بین‌المللی نیز یافته است، دامنه این پژوهش بر حوزه ملی به‌ویژه ارائه راهکارهایی برای تقویت توان کشور در رویارویی با این پدیده متمرکز است. در این خصوص یافته‌های پژوهش نشان می‌دهد که چهار عامل اصلی شامل خلأ قانونی و ضعف در الزامات حقوقی، فقدان زیرساخت‌های فنی، ضعف سازوکار نظارتی، و پایین بودن سطح سواد داده به‌عنوان عناصر زمینه‌ساز استعمار داده شناسایی شده‌اند. این عوامل در تعامل با یکدیگر به تضعیف حاکمیت داده و سرانجام، تضعیف نظام حکمرانی بر داده می‌انجامند. بدین جهت پژوهش حاضر در راستای مقابله با این پدیده، با تأکید بر ضرورت اتخاذ رویکردی جامع و نظام‌مند، راهکارهایی متناظر با عوامل زمینه‌ساز ارائه می‌دهد که شامل قانون‌گذاری خاص و تقویت چارچوب‌های حقوقی، توسعه زیرساخت‌های فنی، ارتقای سازوکارهای نظارتی، و افزایش سطح سواد دیجیتال است. نتایج همچنین نشان می‌دهند که این راهکارها در تعامل با یکدیگر می‌توانند ضمن تقویت حاکمیت ملی نسبت به داده،

به استحکام نظام حکمرانی داده بینجامند. سرانجام اینکه نتایج این مطالعه مؤید آن است که مواجهه مؤثر با این پدیده، مستلزم تعریف چارچوب حقوقی نوینی است که در آن، حاکمیت داده به مثابه یکی از ارکان بنیادین حاکمیت ملی مورد شناسایی و حمایت قرار گیرد

کلیدواژه‌ها: استعمار داده، حکمرانی داده، سواد دیجیتال، قدرت سایبری، مقررات عمومی حفاظت از داده اتحادیه اروپا

۱. مقدمه

در عصری که مرزهای حاکمیت ملی به فضای دیجیتال توسعه یافته، تبیین و تضمین حقوق حاکمیتی کشورها بر داده‌ها، نه تنها ضرورتی اقتصادی، بلکه ضرورتی حقوقی برای حفظ استقلال، امنیت و توسعه پایدار در نظام بین‌المللی است. به‌رغم این امر، آمارها در خصوص کشور ما حاکی از وضعیت نگران‌کننده‌ای است. کشور ما با بیش از ۷۳ میلیون کاربر اینترنت و ضریب نفوذ ۸۱/۷ درصدی، یکی از بزرگ‌ترین تولیدکنندگان داده در منطقه است و در این میان، ۴۸ میلیون کاربر فعال شبکه‌های اجتماعی، روزانه ۳/۵ ساعت به تولید داده در پلتفرم‌های خارجی می‌پردازند (DataReportal 2024). این حجم عظیم داده که ارزش اقتصادی آن در سطح جهانی در سال ۲۰۲۳ به ۲۷۳/۴ میلیارد دلار رسیده و پیش‌بینی می‌شود تا سال ۲۰۲۷ به ۴۲۶/۲ میلیارد دلار افزایش یابد (Statista 2024)، در واقع، بخشی از سرمایه ملی محسوب می‌شود که بدون هیچ‌گونه چارچوب حقوقی الزام‌آور، به خارج از مرزهای حاکمیتی کشور منتقل می‌گردد.

این جریان بی‌وقفه انتقال داده‌های ملی به خارج از مرزهای دیجیتال کشور، مصداق پدیده‌ای است که در حال حاضر با عنوان استعمار داده^۱ شناخته می‌شود. استعمار داده به معنای تسلط نظام‌مند بر داده‌های کاربران و بهره‌برداری یک‌جانبه از آن‌ها از سوی قدرت‌های فراملیتی فناوری است که با ارائه خدمات به‌ظاهر رایگان، در عمل به استخراج و کنترل این منبع راهبردی می‌پردازند. این مفهوم، از منظر حقوقی با اصل «حاکمیت دائمی بر منابع و ثروت‌های ملی»^۲ که یکی از اصول بنیادین حقوق بین‌الملل است، در تعارض آشکار است. برای درک عمیق‌تر این چالش، تمایز مفهومی میان

1. data colonialism

2. permanent sovereignty over natural resources

«حکمرانی داده»^۱ و «حاکمیت داده»^۲ نیز دارای اهمیت است. حکمرانی داده به چارچوب‌های حقوقی، سیاستی و فنی اشاره دارد که نحوه مدیریت، استفاده و حفاظت از داده‌ها را در یک نظام حقوقی مشخص تنظیم می‌کند. در مقابل، حاکمیت داده به حق انحصاری یک دولت برای اعمال صلاحیت قانونی بر داده‌های تولیدشده در قلمرو سرزمینی خود و توسط شهروندانش اشاره دارد. استعمار داده، نقض هر دو مفهوم است؛ زیرا هم چارچوب‌های حکمرانی داده را تضعیف می‌کند و هم حق حاکمیتی دولت‌ها بر داده‌های ملی را نادیده می‌گیرد (Oderkirk 2021).

از سوی دیگر، اهمیت این پدیده از آن روست که داده‌ها در عصر دیجیتال، اطلاعات صرفاً بی‌ارزشی نیستند، بلکه منابعی راهبردی محسوب می‌شوند که قدرت اقتصادی، سیاسی و امنیتی را شکل می‌دهند. به گفته دقیق‌تر، تسلط بر داده‌ها به معنای توانایی تأثیرگذاری بر جریان‌های اقتصادی، اجتماعی و حتی سیاسی است. با وجود این، تحلیل وضعیت ایران در مواجهه با استعمار داده بیانگر چالش‌های متعددی است. در این راستا، پژوهش حاضر با رویکردی تحلیلی به بررسی ابعاد حقوقی استعمار داده و راهکارهای مقابله با آن در چارچوب نظام حقوقی ایران می‌پردازد. در این پژوهش، ابتدا به تحلیل دقیق ماهیت حقوقی این پدیده پرداخته شده و ابعاد مختلف آن بررسی خواهد شد. سپس، با تحلیل عوامل زمینه‌ساز این پدیده در سطح ملی، چارچوبی حقوقی برای تقویت حاکمیت داده و به تبع آن حکمرانی داده ارائه خواهد شد. بر این اساس، مسائل اصلی پژوهش حاضر عبارت‌اند از شناسایی خلأها و چالش‌های نظام حقوقی ایران در مواجهه با پدیده استعمار داده، ارائه راهکارهای مقابله با این پدیده و تقویت حاکمیت داده، و همچنین بررسی تجارب موفق کشورهای پیشرو در زمینه مقابله با استعمار داده و چگونگی بهره‌گیری از این تجارب در تدوین الگوی بومی.

۲. پیشینه پژوهش

قبل از ورود به مباحث اصلی با توجه به هدف و رویکرد پیش گفته، نگاهی به پیشینه نیز لازم است. در میان منابع فارسی، اگرچه مطالعات ویژه درباره استعمار داده محدود است، اما پژوهش‌های مرتبط با حاکمیت و حکمرانی داده در سال‌های اخیر رشد چشمگیری داشته

1. data governance

2. data sovereignty

است. به عنوان نمونه «احمدی و توانا» در مقاله «رویکرد فازی جدید برای سنجش استقرار حاکمیت داده و مدیریت عوامل مربوط به آن» با استفاده از مفاهیم فازی روشی کمی برای سنجش میزان استقرار حاکمیت داده در سازمان‌ها ارائه داده‌اند. این پژوهش عوامل مؤثر بر حاکمیت داده را شناسایی و اولویت‌بندی کرده، اما بیشتر بر سطح سازمانی متمرکز است و به ابعاد ملی و راهکارهای حقوقی کمتر پرداخته است (۱۴۰۱). همچنین «مرتضوی معینی و ساجدی‌نژاد» در مقاله «چارچوب حکمرانی داده در مراکز تبادل داده» چارچوبی برای حکمرانی داده در مراکز تبادل داده ارائه کرده‌اند. پژوهش آن‌ها به طور خاص بر ساختارهای تبادل داده تمرکز دارد و ابعاد حقوقی و سیاستی حاکمیت داده را در سطح ملی به طور جامع بررسی نکرده است (۱۴۰۳). افزون بر این، «نقشینه، فهیم‌نیا و احمدیان» در مقاله «ارائه چارچوبی برای دادگان ملی با تمرکز بر توسعه حاکمیت داده» چارچوبی برای دادگان ملی ارائه کرده‌اند که بر توسعه حاکمیت داده تأکید دارد (۱۴۰۰). پژوهش آن‌ها گامی مهم در جهت تبیین ساختار دادگان ملی است، اما به طور خاص به موضوع استعمار داده و راهکارهای مقابله با آن پرداخته است. از سوی دیگر، در منابع لاتین آثار متعددی وجود دارد که به استعمار داده و ابعاد مختلف آن پرداخته‌اند. به عنوان نمونه، «کالزاتی» در مقاله خود با عنوان «استعمارزدایی از استعمار داده» به بررسی مفهوم استعمار داده و پیامدهای آن در بستر شبکه‌ای می‌پردازد. این اثر بیشتر بر ابعاد سیاسی-اجتماعی استثمار داده تمرکز دارد و بر راهبردهای استعمارزدایی تأکید می‌کند (Calzati 2021). تفاوت اصلی این مقاله با اثر حاضر در این است که رویکرد «کالزاتی» نظری بوده و فاقد راهکارهای عملی و چارچوب‌های حقوقی ملی برای مقابله با استعمار داده است. همچنین «لئون» در پایان‌نامه خود با عنوان «استعمار داده در کانادا: استعمارزدایی داده از طریق حاکمیت داده بومی» به بررسی استعمار داده‌ای در کانادا و تلاش‌های مردمان بومی برای حاکمیت بر داده‌های خود می‌پردازد. او مفهوم استعمار داده را به عنوان «مدلی استعماری از سلب مالکیت و سلطه که از طریق کنترل اطلاعات و داده‌هایی که درباره یا توسط مردمان بومی ایجاد شده‌اند» تعریف می‌کند. این پژوهش اگرچه بر تجربه کانادا متمرکز است، اما بینش‌های ارزشمندی درباره ارتباط بین حاکمیت داده و استقلال فرهنگی و هویت ملی ارائه می‌دهد (Leone 2021). اثر دیگر مربوط به «مامفورد» است که در مقاله «استعمار داده: قانع‌کننده و مفید، اما تکلیف نظام‌های شناختی چه می‌شود؟» نقدی بر مفهوم استعمار داده ارائه می‌دهد. «مامفورد» معتقد است که حاکمیت داده صرفاً یک مسئله فنی یا اقتصادی نیست،

بلکه مسئله‌ای مرتبط با نظام‌های شناختی و جهان‌بینی است. این دیدگاه اهمیت توجه به ابعاد فرهنگی و معرفتی در تدوین راهکارهای حقوقی و سیاستی برای حاکمیت داده را برجسته می‌سازد (Mumford 2022). همچنین «کولدبری و مجیاس» در کتابی با عنوان «بهای ارتباط: چگونه داده‌ها زندگی انسان را مستعمره می‌کنند و آن را در خدمت سرمایه‌داری قرار می‌دهند» به بررسی چگونگی استعمار زندگی انسان توسط داده‌ها می‌پردازند و آن را به‌عنوان منبعی برای سود سرمایه‌داری تحلیل می‌کنند. این اثر بر پیامدهای اجتماعی-اقتصادی استثمار داده تمرکز دارد (Couldry and Mejias 2019b)؛ در حالی که پژوهش حاضر بر چارچوب‌های حقوقی و حاکمیتی برای مقابله با استعمار داده متمرکز است. افزون بر این‌ها، «هانگلادارم» در مقاله‌ای با عنوان «شوشانا زوباف، عصر سرمایه‌داری نظارتی: نبرد برای آینده‌ای انسانی در مرز جدید قدرت» به بررسی مفهوم سرمایه‌داری نظارتی ارائه‌شده توسط «شوشانا زوباف»^۱ می‌پردازد و بر پویایی قدرت در جمع‌آوری و استفاده از داده‌ها تأکید دارد (Hongladarom 2023). تفاوت اصلی این مقاله با پژوهش حاضر در این است که بیشتر بر پیامدهای اجتماعی نظارت تمرکز دارد و راهکارهای حقوقی ملی ارائه نمی‌دهد. اثر دیگر از «هامل» و همکاران با عنوان «مروری بر حاکمیت داده» است. این مطالعه به بررسی حاکمیت داده پرداخته و اهمیت آن را در زمینه کلان‌داده، همچنین پیامدهای اجتماعی این پدیده را مورد واکاوی قرار داده است (Hummel et al. 2021). این مقاله به موضوع پژوهش حاضر نزدیک است، لیکن بیشتر توصیفی بوده و فاقد راهکارهای حقوقی و سیاستی مشخص است. سرانجام، «سینگی» و همکاران در مقاله خود با عنوان «چارچوب حکمرانی حاکمیت داده» ساختاری برای حاکمیت داده پیشنهاد می‌دهند و بر نیاز به رویکردهای ساختارمند برای مدیریت داده در سطح ملی تأکید می‌کنند (Singi et al. 2020). این اثر به موضوع مقاله حاضر نزدیک بوده و بر ایجاد مدل حاکمیتی متمرکز است، لیکن پژوهش حاضر به‌طور خاص به عوامل زمینه‌ساز استعمار داده و راه‌حل‌های عملی برای مقابله با آن نیز می‌پردازد.

به‌طور کلی، بررسی پیشینه پژوهش نشان می‌دهد که اگرچه مطالعاتی در زمینه حاکمیت و حکمرانی داده انجام شده، اما شکاف قابل توجهی در زمینه ارائه راهکارهای حقوقی و سیاستی برای مقابله با استعمار داده در سطح ملی وجود دارد. تمایز اصلی پژوهش

1. Shoshana Zuboff

حاضر با مطالعات پیشین در رویکرد کاربردی آن است که نه تنها به تحلیل پدیده استعمار داده می‌پردازد، بلکه راهکارهای عملی و چارچوب‌های حقوقی مشخصی برای مقابله با آن در بستر ایران ارائه می‌دهد. این پژوهش با تلفیق مفاهیم حاکمیت داده، حکمرانی داده و استعمار داده از یک سو، و با تمرکز بر ارائه راهکارهای حقوقی و سیاسی در سطح ملی از سوی دیگر، نوآوری قابل توجهی در مقایسه با آثاری دارد که بیشتر به تحلیل و توصیف این پدیده‌ها می‌پردازند.

۳. روش پژوهش

پژوهش حاضر با بهره‌گیری از روش تحلیل محتوای کیفی^۱ به بررسی پدیده استعمار داده و راهکارهای مقابله با آن می‌پردازد. در راستای تبیین دقیق فرایند پژوهش، روش مطالعه در ادامه تشریح می‌گردد. این پژوهش از نظر هدف، بنیادی بوده و با اتخاذ رویکردی توصیفی-تحلیلی، امکان شناسایی لایه‌های پنهان پدیده استعمار داده و تحلیل عمیق آن را فراهم می‌آورد. روش گردآوری اطلاعات در این پژوهش، اسنادی و کتابخانه‌ای است و بررسی آثار علمی معتبر از پایگاه‌های داده موثق را شامل است. فرایند جست‌وجو و انتخاب منابع با استفاده از کلیدواژه‌های فارسی و انگلیسی مرتبط با موضوع پژوهش انجام شده است. کلیدواژه‌های فارسی مورد استفاده شامل «استعمار داده»، «استعمار دیجیتال»، «حاکمیت داده»، «حکمرانی داده»، «حفاظت از داده» و «حاکمیت ملی بر داده» است. همچنین «Data Colonialism»، «Digital Colonialism»، «Data Sovereignty»، «Data Governance» و «National Data Sovereignty» به عنوان کلیدواژه‌های انگلیسی در فرایند جست‌وجو مورد استفاده قرار گرفته‌اند. پایگاه‌های داده مورد جست‌وجو شامل Web of Science، ScienceDirect، Semantic Scholar، SID (پایگاه مرکز اطلاعات علمی جهاد دانشگاهی)، Noormags (پایگاه مجلات تخصصی نور) و Magiran (بانک اطلاعات نشریات کشور) است.

در فرایند تحلیل کیفی، مراحل متعددی به منظور استخراج و تحلیل مفاهیم مرتبط با موضوع پژوهش طی شده است. این مراحل شامل کدگذاری اولیه، کدگذاری محوری و کدگذاری انتخابی است. در مرحله کدگذاری اولیه، پس از مطالعه منابع گردآوری شده،

1. qualitative content analysis

مفاهیم و گزاره‌های مرتبط با پدیده استعمار داده شناسایی و استخراج گردیده است. در این مرحله، ۸۷ کد اولیه از متون مورد مطالعه استخراج شد. برخی از این کدهای اولیه از جمله «استخراج غیرشفاف داده‌های کاربران»، «نابرابری قدرت میان متصدیان پلتفرم‌ها و کاربران»، «فقدان قوانین حمایتی از داده‌های شخصی»، «انتقال داده‌های ملی به خارج از مرزهای کشور»، «عدم آگاهی کاربران از ارزش داده‌ها» و «سلطه الگوریتمی شرکت‌های فراملیتی» است. در مرحله کدگذاری محوری، کدهای اولیه بر اساس قرابت مفهومی و ارتباط موضوعی دسته‌بندی شده و ۱۸ مقوله فرعی شکل گرفت. برخی از مقوله‌های فرعی که در فرایند کدگذاری محوری شناسایی شدند، شامل «استخراج داده»، «نابرابری دیجیتالی»، «خلاف‌های قانونی»، «چالش‌های حفاظت از داده» هستند. سرانجام، در مرحله کدگذاری انتخابی، مقوله‌های فرعی در قالب ۴ مقوله اصلی سازماندهی شده و الگوی نظری پژوهش تدوین گردید. این مقوله‌های اصلی «خلاف قانونی و ضعف در الزامات حقوقی»، «فقدان زیرساخت‌های فنی»، «ضعف سازوکار نظارتی» و «پایین بودن سطح سواد داده» هستند.

از سوی دیگر، چارچوب تحلیلی پژوهش در سه سطح مفهومی، ساختاری و راهبردی طراحی شده است. این سه سطح بر اساس نتایج حاصل از فرایند کدگذاری استخراج گردیده است. در سطح مفهومی به تبیین مفهوم استعمار داده و شناسایی مؤلفه‌های آن پرداخته می‌شود. این سطح از تحلیل، مبتنی بر کدهای مرتبط با ویژگی‌ها و مصادیق استعمار داده است. در سطح ساختاری، عوامل زمینه‌ساز و سازوکارهای استعمار داده تحلیل می‌شوند. این سطح از تحلیل بر اساس کدهای مرتبط با علل، زمینه‌ها و سازوکارهای شکل‌گیری و تداوم استعمار داده استخراج شده است. سرانجام اینکه در سطح راهبردی، چارچوب مقابله با استعمار داده و راهکارهای آن تدوین می‌گردد. این سطح از تحلیل، مبتنی بر کدهای مرتبط با راهکارها، سیاست‌ها و اقدامات مقابله‌ای با پدیده استعمار داده است.

به‌منظور تضمین کیفیت علمی پژوهش، راهبردهای متعددی برای افزایش روایی و پایایی به کار رفته است. در راستای ارتقای روایی پژوهش، از روش مثلث‌سازی منابع داده^۱ استفاده شده که بر گردآوری و تحلیل داده‌ها از منظرهای مختلف مبتنی است. این رویکرد از طریق بهره‌گیری از طیف متنوعی از منابع شامل مقالات علمی معتبر، کتب تخصصی،

1. data triangulation

اسناد قانونی و حقوقی و آمارهای رسمی محقق شده است. تنوع منابع مورد استفاده امکان مقایسه و تطبیق یافته‌ها را فراهم آورده و به کاهش سوگیری‌های احتمالی کمک کرده است. در خصوص تضمین پایایی پژوهش، مستندسازی نظام‌مند و دقیق تمامی مراحل پژوهش انجام شده است. این مستندسازی شامل ثبت دقیق فرایندهای جمع‌آوری داده‌ها، مراحل کدگذاری، شیوه استخراج مفاهیم و مقوله‌ها، و روند تحلیل و تفسیر یافته‌هاست. سرانجام، به‌رغم اتخاذ رویکردهای روش‌شناختی فوق، پژوهش حاضر با محدودیت‌هایی نیز مواجه است. نوظهور بودن پدیده استعمار داده، کمبود منابع علمی به زبان فارسی و پیچیدگی‌های ذاتی موضوع به دلیل ماهیت میان‌رشته‌ای آن از جمله چالش‌های اصلی این پژوهش بوده‌اند. با وجود این، تلاش شده است با اتخاذ رویکردی نظام‌مند و روش‌شناسی دقیق علمی، این محدودیت‌ها تا حد امکان مدیریت شده و تحلیلی جامع از پدیده مورد مطالعه ارائه گردد.

۴. ماهیت استعمار داده: نگاهی بر مفهوم، ساختار و سازوکار

در این بند ابتدا مفهوم این پدیده، و سپس ساختار و سازوکار آن مورد توجه قرار خواهد گرفت.

۴-۱. مفهوم استعمار داده

استعمار داده^۱ را نخستین بار «نیک کولدري و اولریش مجیاس»^۲ مطرح کردند. از نظر آن‌ها، این مفهوم به فرایندی اشاره دارد که در آن، زندگی انسان‌ها به داده تبدیل شده و این داده‌ها توسط شرکت‌های بزرگ فناوری تصاحب می‌شوند (Couldry & Mejias 2019c, 337). استعمار داده پدیده‌ای است چندوجهی که در آن، شرکت‌ها یا نهادهای قدرتمند با استفاده از برتری فناوری خود، داده‌های کاربران را جمع‌آوری، پردازش و به کالا تبدیل می‌کنند؛ بدون آنکه منافع حاصل از این فرایند به‌طور عادلانه با صاحبان اصلی داده (اشخاص موضوع داده)^۳ تقسیم شود. عناصر و ارکان اصلی این مفهوم را می‌توان در چهار محور اساسی خلاصه کرد. نخست، وجود یک رابطه نابرابر قدرت بین جمع‌آوری‌کنندگان

1. data colonialism

2. Nick Couldry, Ulises A. Mejias

3. data subjects

و صاحبان داده؛ دوم، فقدان یا نقص در رضایت آگاهانه کاربران؛ سوم، عدم شفافیت در نحوه استفاده و پردازش داده‌ها؛ و چهارم، توزیع ناعادلانه منافع حاصل از ارزش افزوده داده‌ها. این عناصر در کنار یکدیگر، چارچوب مفهومی جامعی را برای درک و تحلیل پدیده استعمار داده فراهم می‌آورند (Sadowski 2019).

این مفهوم با استعمار سنتی (متعارف) از جنبه‌های متفاوتی شباهت‌های ساختاری دارد. این موارد از جمله تصاحب منابع است؛ یعنی همان‌طور که در استعمار به معنای متعارف، منابع طبیعی کشورهای مستعمره غارت می‌شد، در استعمار داده‌ها نیز داده‌های شخصی کاربران بدون پرداخت عوض منصفانه تصاحب می‌شود (Ricaurte 2019, 355). روابط نابرابر قدرت نیز وجود دارد. این امر بدین معناست که شرکت‌های بزرگ فناوری با در اختیار داشتن زیرساخت‌های دیجیتال، در موقعیتی برتر نسبت به کاربران قرار دارند. مورد دیگر، وابستگی ساختاری است؛ یعنی همانند وابستگی کشورهای مستعمره به قدرت‌های استعماری، امروزه نیز وابستگی عمیقی به خدمات و پلتفرم‌های شرکت‌های فناوری ایجاد شده است (Couldry & Mejias 2019c, 340). شباهت مهم دیگر این است که استعمار داده -مانند سلف تاریخی‌اش- خود را به‌عنوان نیروی برای پیشرفت معرفی می‌کند؛ چه از طریق پیشرفت علمی، خدمات شخصی‌سازی‌شده، یا مدیریت خردمندانه^۱؛ درست همان‌طور که استعمار سنتی مدعی مأموریت متمدن‌سازی بود (Verständig 2021). به‌دیگر سخن، ویژگی مشترک میان هر دو شکل استعمار، توانایی آن‌ها در عادی‌سازی بهره‌کشی از طریق عقلانی‌سازی است. همان‌طور که استعمار تاریخی، تصاحب سرزمینی را طبیعی و ضروری جلوه می‌داد، استعمار داده نیز جمع‌آوری و پردازش مداوم داده‌های شخصی را به‌عنوان جنبه‌ای اجتناب‌ناپذیر و مفید از زندگی امروزی ارائه می‌کند (Roberts & Montoya 2022, 10).

با وجود شباهت‌های ساختاری، تفاوت‌های بین استعمار سنتی و استعمار داده بسیار

1. rational management

مدیریت خردمندانه در این متن به رویکردی انتقادی اشاره دارد که در آن صاحبان فناوری با استفاده از داده‌ها، الگوریتم‌ها و روش‌های نظارتی امروزی، تصمیم‌گیری و کنترل را توجیه می‌کنند. این شیوه مدیریتی که در ظاهر با هدف بهینه‌سازی و کارایی انجام می‌شود، در واقع ابزاری برای کنترل بیشتر و بهره‌برداری از کاربران است

عمیق و چندوجهی است. در استعمار سنتی، قدرت‌های استعماری از طریق نیروی نظامی و خشونت فیزیکی، سرزمین‌ها را اشغال می‌کردند و منابع طبیعی آن‌ها را به غارت می‌بردند. این نوع استعمار به‌طور کامل، آشکار و ملموس بود و مرزهای جغرافیایی مشخصی داشت. اما استعمار داده به شکلی کاملاً متفاوت عمل می‌کند. این نوع استعمار از طریق جلب رضایت ظاهری کاربران و با ارائه خدمات به‌ظاهر رایگان صورت می‌گیرد. در استعمار داده، مرزهای جغرافیایی معنای خود را از دست داده‌اند و استعمارگران دیجیتال (شرکت‌های بزرگ فناوری) می‌توانند همزمان در تمام نقاط جهان حضور داشته باشند. از سوی دیگر، برخلاف استعمار سنتی که در آن استعمارشدگان از استثمار خود آگاه بودند، در استعمار داده، کاربران اغلب نه‌تنها از استثمار خود آگاه نیستند، بلکه داوطلبانه در این فرایند مشارکت و حتی از آن استقبال می‌کنند (Coleman 2019, 424-426). نکته مهم دیگر اینکه منابع مورد استعمار در استعمار سنتی، محدود و پایان‌پذیر بودند، اما در این استعمار داده‌ها به‌عنوان منبع اصلی، به‌طور دائم در حال تولید و بازتولید هستند. همچنین، در استعمار سنتی، استعمارگران برای بهره‌برداری از منابع باید هزینه‌های زیادی صرف می‌کردند، اما در استعمار داده، هزینه جمع‌آوری و پردازش داده‌ها بسیار پایین است و با پیشرفت فناوری به‌طور مداوم در حال کاهش است. تفاوت دیگر در شیوه مقاومت است. در استعمار سنتی، مقاومت به‌طور عمده، شکل فیزیکی و نظامی داشت، در حالی که در استعمار داده، مقاومت پیچیده‌تر خواهد بود و شامل اقدامات حقوقی، فنی و فرهنگی است. همچنین، برخلاف استعمار سنتی که پس از استقلال کشورها به پایان می‌رسید، استعمار داده ماهیتی مستمر و پویا دارد و حتی با قطع ارتباط کاربر با سرویس‌های دیجیتال، داده‌های قبلی همچنان در اختیار شرکت‌ها باقی می‌ماند. نکته قابل توجه دیگر این است که در استعمار سنتی، روابط قدرت به‌طور کامل، یک‌طرفه بود، اما در استعمار داده، روابط پیچیده‌تر است و گاهی کاربران نیز از مزایای خدمات دیجیتال بهره‌مند می‌شوند، هرچند این بهره‌مندی در مقایسه با سود شرکت‌های فناوری بسیار ناچیز است (Couldry & Mejias 2019a, 3 & 4).

به‌دنبال وجوه متمایز متعدد بین دو شکل استعمار، از نظر برخی، قیاس استعمار سنتی با استعمار داده صحیح نیست؛ چرا که استعمار داده تکرار الگوی استعمار سنتی نیست، بلکه دگرگونی عمیق‌تری را نمایان می‌سازد که آن تسخیر حیات انسانی و مناسبات اجتماعی از طریق استخراج و بهره‌برداری نظام‌مند از داده‌هاست (Dijck & Rieder 2019).

5). در واقع، این چارچوب نظری، دیدگاه سطحی رایج را که داده را صرفاً به‌عنوان یک منبع ارزشمند (مانند نفتِ عصر حاضر) می‌بیند، به چالش می‌کشد و در عوض، داده را به‌عنوان ابزاری نوین برای سلب مالکیت و کنترل اجتماعی معرفی می‌کند (Katzenbach & Bächle 2019, 5). عنصر کلیدی در این چارچوب، ایده «همزاد داده‌ای»^۱ است. این مفهوم به نسخه‌ای دیجیتال از هویت افراد اشاره دارد که از طریق جمع‌آوری و تحلیل داده‌های مختلف زندگی روزمره شکل می‌گیرد. در واقع، وقتی افراد در فضای مجازی فعالیت می‌کنند - از خرید آنلاین گرفته تا استفاده از شبکه‌های اجتماعی - از خود رد پای دیجیتال به جای می‌گذارند که شرکت‌ها و سازمان‌های مختلف آن را جمع‌آوری و تحلیل می‌کنند. بدین ترتیب، همزاد داده‌ای صرفاً یک مجموعه اطلاعات ساده نیست، بلکه تصویری جامع از رفتارها، علایق و الگوهای زندگی افراد است که می‌تواند بر تصمیم‌گیری‌های مهم درباره آن‌ها تأثیر بگذارد. برای مثال، وقتی شرکت‌ها از مشتریان خود پروفایل‌های دیجیتال می‌سازند یا وقتی سوابق آنلاین افراد در شبکه‌های اجتماعی پردازش می‌شود، در واقع، بخشی از این همزاد داده‌ای در حال شکل‌گیری است. اهمیت این مفهوم زمانی بیشتر می‌شود که درک شود چگونه این امر می‌تواند به‌عنوان ابزاری برای اعمال قدرت و کنترل اجتماعی استفاده شود. بدین دلیل است که تأثیر این امر از حریم خصوصی فردی فراتر رفته و می‌تواند بر ابعاد اجتماعی نیز اثرگذار باشد (Dijck & Rieder 2019, 5).

۴-۲. تبیین ساختار و سازوکار استعمار داده

استعمار داده از دو لایه اصلی تشکیل شده است. بخش نخست، لایه زیرساختی (فنی) است. این امر شامل تمامی عناصر فیزیکی و زیرساختی است که امکان پردازش داده‌ها را فراهم می‌کند (Cohen 2017, 231). بخش دوم، لایه الگوریتمی (پردازشی) است. الگوریتم‌ها مغز متفکر دنیای دیجیتال هستند که نحوه پردازش، تحلیل و استفاده از داده‌ها را تعیین می‌کنند. تعامل این دو لایه با یکدیگر موجب شکل‌گیری نظام سلطه دیجیتال می‌شود که در آن، کنترل جریان داده‌ها و استخراج ارزش از آن‌ها به شکل‌دهی رفتارها و تصمیمات منجر شده و سرانجام، به ایجاد وابستگی دیجیتال می‌انجامد (Bucher 2016, 32). وابستگی در لایه الگوریتمی منجر به انحصار الگوریتمی (انحصار در پردازش داده‌ها) است که یکی از

1. data double

مهم‌ترین چالش‌های عصر دیجیتال است. این امر ماهیتی چندوجهی و پیچیده دارد و فراتر از مفهوم سنتی انحصار است. این پدیده با ایجاد حلقه‌های تقویت‌کننده خودکار، به‌طور مداوم قدرت انحصاری شرکت‌های فناوری را افزایش می‌دهد. هنگامی که یک شرکت فناوری به حجم انبوهی از داده‌های کاربران دسترسی پیدا می‌کند، می‌تواند با استفاده از الگوریتم‌های پیشرفته، الگوهای پنهان در این داده‌ها را کشف و از آن‌ها برای بهبود خدمات خود استفاده کند. این بهبود خدمات به جذب کاربران بیشتر منجر می‌شود که خود منجر به تولید داده‌های بیشتر و در نتیجه، بهبود بیشتر الگوریتم‌ها می‌گردد (Zuboff, 2015, 79). این انحصار به شکل‌گیری نوعی «استبداد الگوریتمی»^۱ منجر می‌شود که در آن، تصمیم‌گیری‌های مهم زندگی افراد توسط سیستم‌های غیرشفاف و غیرپاسخگو صورت می‌گیرد. الگوریتم‌های انحصاری با تأثیرگذاری بر جریان اطلاعات، شکل‌گیری افکار عمومی و حتی رفتارهای اجتماعی، به‌نوعی «مهندسی اجتماعی نامرئی»^۲ دست می‌زنند. این وضعیت زمانی پیچیده‌تر می‌شود که در نظر گرفته شود بسیاری از این الگوریتم‌ها از فناوری‌های «یادگیری عمیق»^۳ استفاده می‌کنند که حتی برای طراحان خود نیز به‌طور کامل، قابل درک و توضیح نیست. از سوی دیگر، چالش شفافیت الگوریتمی در این میان، مسئله‌ای چندبعدی است. در سطح نخست، شرکت‌های فناوری به بهانه حفظ اسرار تجاری و مالکیت معنوی، از افشای جزئیات عملکرد الگوریتم‌هایشان خودداری می‌کنند. در لایه عمیق‌تر، ماهیت پیچیده و تکاملی الگوریتم‌های یادگیری ماشین، امکان بازرسی و نظارت سنتی را دشوار می‌سازد. این عدم شفافیت، زمانی نگران‌کننده‌تر می‌شود که افراد بدانند این الگوریتم‌ها می‌توانند به‌طور ناخواسته الگوهای تبعیض‌آمیز موجود در داده‌های ورودی (آموزشی) را تقویت و بازتولید کنند. در واقع، جعبه سیاه الگوریتم‌های یادگیری عمیق با

1. algorithmic tyranny/ algorithmic despotism

استبداد الگوریتمی به فرایندی اشاره دارد که در آن الگوریتم‌ها و فناوری‌های هوش مصنوعی بدون شفافیت و نظارت انسانی مناسب، تصمیمات مهمی می‌گیرند و ممکن است باعث تبعیض، کنترل، یا محدود کردن حقوق و آزادی‌های فردی شوند

2. invisible social engineering / covert social engineering

مهندسی اجتماعی نامرئی به تکنیک‌ها و راهبردهایی اشاره دارد که در آن از ابزارهای غیرمستقیم نظیر داده‌کاوی، الگوریتم‌ها و فناوری‌های مبتنی بر هوش مصنوعی، برای تأثیرگذاری بر رفتار، تصمیم‌گیری، یا باورهای افراد استفاده می‌شود، بدون آنکه آن‌ها از این تأثیرگذاری آگاه باشند.

3. deep learning

لایه‌های متعدد پردازشی خود، حتی برای طراحان نیز به‌طور کامل قابل درک نیست. این ابهام ذاتی در ترکیب با محرمانگی تجاری، به ایجاد نوعی حجاب الگوریتمی منجر می‌شود که امکان نظارت مؤثر بر عملکرد این سیستم‌ها را محدود می‌کند (Couldry & Mejias 2019b). به‌طور کلی، تحقق لایه استعمار فنی و لایه الگوریتمی، موجبات پیامدهای متفاوتی را فراهم خواهد آورد. از مهم‌ترین این موارد، استعمار داده از طریق کنترل محتوا و الگوریتم‌های توصیه‌گر^۱ است که به یکسان‌سازی فرهنگی در مقیاس جهانی می‌انجامد. این فرایند با تغییر تدریجی ارزش‌ها، باورها و سبک زندگی، هویت‌های فرهنگی را تضعیف می‌کند. پلتفرم‌های جهانی با ترویج الگوهای فرهنگی خاص، به‌نوعی امپریالیسم فرهنگی دیجیتال دامن می‌زنند. این تغییرات فرهنگی عمیق، چالش‌های جدی برای هویت ملی، ارزش‌های بومی و پیامدهای سیاسی متعدد نیز ایجاد می‌کند (Calzati 2021, 917).

سرانجام اینکه پرداختن به سازوکارهای استعمار داده ضروری است. سازوکار این پدیده، پیچیده و هوشمندانه است که چند لایه^۲ مختلف دارد. در لایه نخست، شرکت‌های فناوری کاربران را با ارائه خدمات به‌ظاهر رایگان مانند موتورهای جست‌وجو، شبکه‌های اجتماعی و پیام‌رسان‌ها جذب می‌کنند. این خدمات در ظاهر هیچ هزینه‌ای ندارد، اما در واقعیت، کاربران با داده‌های شخصی خود هزینه‌ای پنهان می‌پردازند که ارزش آن بسیار بیشتر از یک پرداخت مستقیم مالی است. در واقع، داده‌های کاربران به‌عنوان «بهای پنهان»^۳ خدمات محسوب می‌شود (Scholz 2018, 5). در لایه دوم، اقتصاد توجه^۴ عمل می‌کند که با استفاده از طراحی اعتیادآور و الگوریتم‌های پیچیده، کاربران را تشویق می‌کند که زمان بیشتری را در این پلتفرم‌ها صرف کنند. هرچه کاربران زمان بیشتری را صرف استفاده از این خدمات می‌کنند، داده‌های بیشتری تولید می‌کنند و این داده‌ها به منبعی ارزشمند برای شرکت‌ها تبدیل می‌شود. الگوریتم‌های هوشمند با تحلیل رفتار کاربران، محتوا و تبلیغات را به‌گونه‌ای شخصی‌سازی می‌کنند که باعث افزایش وابستگی و زمان استفاده می‌شود. لایه سوم، نظارت دیجیتال است که از آن با عنوان «سرمايه‌داری نظارتی»^۴ یاد می‌شود. در این لایه، فعالیت‌های آنلاین و حتی آفلاین کاربران به‌طور مداوم رصد و

1. recommendation algorithms

2. hidden cost

3. attention economy

4. surveillance capitalism

ثبت می‌شود. این نظارت فراگیر تنها محدود به فعالیت‌های آنلاین نیست؛ با گسترش اینترنت اشیا و دستگاه‌های هوشمند، حتی فعالیت‌های روزمره فیزیکی نیز به داده تبدیل می‌شوند. شرکت‌ها با تحلیل این داده‌ها می‌توانند الگوهای رفتاری کاربران را پیش‌بینی کرده و حتی در جهت منافع تجاری خود هدایت کنند (Couldry & Mejias 2019b).

۵. عوامل زمینه‌ساز و تسهیل‌کننده استعمار داده

تحلیل نظام‌مند عوامل مؤثر بر حکمرانی داده نشان می‌دهد که مجموعه‌ای از عوامل زمینه‌ای شامل ضعف در قانون‌گذاری و الزامات حقوقی، محدودیت‌های زیرساختی و فنی، ناکارآمدی نظام نظارتی و پایین بودن سطح سواد دیجیتال در جامعه، در گام نخست به تضعیف حاکمیت ملی بر داده‌ها منجر می‌شوند. این عوامل زمینه‌ای در کنار ضعف حاکمیت داده، سرانجام به تضعیف کل نظام حکمرانی بر داده می‌انجامد. بدین ترتیب در ادامه، ضمن بررسی عوامل زمینه‌ای چهارگانه، چگونگی تأثیر آن‌ها بر تضعیف حاکمیت داده و سرانجام، تضعیف نظام حکمرانی داده مورد تحلیل قرار می‌گیرد.

۵-۱. تبیین عوامل زمینه‌ای چهارگانه

عناصر تسهیل‌کننده استعمار داده به‌عنوان عوامل زمینه‌ای به‌شرح زیر است:

۵-۱-۱. خلأ قانونی و ضعف در الزامات حقوقی

در بسیاری از کشورها و نظام‌های حقوقی، نبود قوانین جامع و به‌روز در حوزه حفاظت از داده شخصی، حریم خصوصی اطلاعاتی دیجیتال و مالکیت داده، زمینه استعمار داده را فراهم آورده است. این خلأ قانونی شامل فقدان تعاریف دقیق از مفاهیم کلیدی، عدم تعیین حدود مسئولیت‌های شرکت‌های فناوری و فقدان ضمانت اجرای مؤثر است. همچنین، عدم انطباق قوانین موجود با تحولات سریع فناوری و پیچیدگی‌های فضای دیجیتال، شکاف‌های قانونی را تشدید می‌کند (Ilyas 2022, 35). در این راستا نظام حقوقی ایران نیز در حوزه حفاظت از داده‌های شخصی با خلأهای قانونی عمیقی مواجه است. البته ایران با ارائه پیش‌نویس‌های قانونی [طرح حمایت و حفاظت از داده و اطلاعات شخصی

این مفهوم در سال ۲۰۱۴ توسط Shoshana Zuboff نظریه‌پرداز اجتماعی معرفی شد. او این مفهوم را ابتدا در مقاله‌های خود توضیح داد و سپس در کتاب مشهورش با عنوان The Age of Surveillance Capitalism که در سال ۲۰۱۹ منتشر شد، به تفصیل به این موضوع پرداخت.

مرکز پژوهش‌های مجلس شورای اسلامی (۱۴۰۰)، و طرح حفاظت از داده شخصی مرکز پژوهش‌های مجلس شورای اسلامی (۱۴۰۳) در این خصوص گام برداشته است. این امر، در خصوص حمایت از داده‌های شخصی کافی نیست. بدین جهت فقدان قانون جامع حمایت از داده شخصی، از مهم‌ترین عوامل زمینه‌ای نسبت به استعمار داده است. این امر موجب شده است که برای حمایت از اشخاص موضوع داده، به مفاد پراکنده از سایر قوانین و مقررات مختلف مانند قانون تجارت الکترونیکی^۱، قانون جرائم رایانه‌ای^۲ و آیین دادرسی کیفری^۳، استناد شود. این پراکندگی نه تنها باعث سردرگمی در جریان حمایت‌ها می‌شود، بلکه خلأهای متعددی را در حمایت از حقوق شهروندان ایجاد می‌کند. همچنین عدم تعریف دقیق مفاهیم کلیدی مانند «داده شخصی» و «رضایت آگاهانه یا صریح» در قوانین موجود نیز چالش‌های جدی در تفسیر و اجرای این قوانین ایجاد نموده است (لطیف‌زاده و همکاران ۱۴۰۱).

۵-۱-۲. فقدان زیرساخت‌های فنی مناسب

این مورد یکی از مهم‌ترین عوامل زمینه‌ساز استعمار داده‌ها محسوب می‌شود. ضعف زیرساختی در لایه‌های مختلف فنی و فناوریانه قابل مشاهده است. در لایه نخست، کمبود مراکز داده پیشرفته و سیستم‌های ذخیره‌سازی با ظرفیت بالا، توانایی کشورها را برای نگهداری و پردازش داده‌های بومی محدود می‌کند. این محدودیت باعث می‌شود بخش قابل توجهی از داده‌های تولیدشده توسط کاربران در مراکز داده خارجی ذخیره شود که خود زمینه‌ساز وابستگی و آسیب‌پذیری است (Thatcher, O'Sullivan, and Mahmoudi 2016, 4). در لایه دوم، ضعف در توسعه پلتفرم‌های بومی و برنامه‌های کاربردی، منجر به وابستگی شدید به سرویس‌های خارجی می‌شود. این وابستگی تنها محدود به استفاده از نرم‌افزارها نیست، بلکه به معنای واگذاری کنترل جریان داده‌ها به شرکت‌های خارجی است. نبود جایگزین‌های بومی قدرتمند برای سرویس‌های پرکاربرد مانند موتورهای

۱. صریح‌ترین مواد در خصوص حمایت از داده‌های شخصی در قانون تجارت الکترونیکی مواد ۵۸ و ۵۹

است و ضمانت اجرای نقض چنین حمایت‌هایی نیز در ماده ۷۱ مقرر شده است

۲. این قانون در ماده ۱۷ و برخی مواد دیگر مانند ماده ۱، ۳، ۴، ۸ و ۱۲ به داده‌ها و داده‌های سری اشاره کرده و برای نقض داده‌ها ضمانت اجرا مقرر نموده است

۳. برخی مواد در این قانون، مانند ماده ۴ و ۴۰، در مورد حمایت از داده شخصی قابل استفاده است.

جست‌وجو، شبکه‌های اجتماعی و پیام‌رسان‌ها کاربران را ناگزیر به استفاده از پلتفرم‌های خارجی می‌کند (Subramani 2023, 94). در سطح پیشرفته‌تر، کمبود زیرساخت‌های لازم برای توسعه و پیاده‌سازی فناوری‌های نوین مانند هوش مصنوعی، یادگیری ماشین و پردازش کلان‌داده‌ها شکاف فناوری را عمیق‌تر می‌کند. این فناوری‌ها امروزه در استخراج ارزش از داده‌ها نقش کلیدی دارند، و عدم دسترسی به آن‌ها به معنای محرومیت از بخش مهمی از زنجیره ارزش در اقتصاد دیجیتال است (Kwet 2019, 3). همچنین، ضعف در زیرساخت‌های امنیت سایبری و سیستم‌های حفاظت از داده، آسیب‌پذیری در برابر تهدیدات سایبری را افزایش می‌دهد. این مسئله به‌ویژه در مورد داده‌های حساس اهمیت بیشتری می‌یابد. عدم توانایی در تأمین امنیت داده‌های بومی، اعتماد کاربران را کاهش داده و آن‌ها را به سمت استفاده از سرویس‌های خارجی سوق می‌دهد. از سوی دیگر، محدودیت در دسترسی به فناوری‌های پیشرفته، تحریم فناوری و موانع انتقال دانش فنی نیز این وضعیت را پیچیده‌تر می‌کند. کشورهای در حال توسعه اغلب با محدودیت‌های جدی در دسترسی به قطعات، نرم‌افزارها و دانش فنی مورد نیاز برای توسعه زیرساخت‌های بومی مواجه هستند. این محدودیت‌ها روند توسعه فناوری‌های بومی را کند کرده و وابستگی به سرویس‌های خارجی را تشدید می‌کند (Coudry & Mejias 2019b, 23- 25). این مجموعه از ضعف‌های زیرساختی سرانجام، به ایجاد یک چرخه معیوب منجر می‌شود؛ بدین صورت که عدم توسعه زیرساخت‌های بومی به وابستگی بیشتر به سرویس‌های خارجی می‌انجامد. این وابستگی به‌نوبه خود انگیزه و منابع لازم برای توسعه زیرساخت‌های داخلی را کاهش می‌دهد و این چرخه همچنان ادامه می‌یابد.

در کنار ضعف‌های زیرساختی مذکور که به‌طور کلی مورد توجه است، در مورد ایران به‌طور خاص لازم به ذکر است که نهادهای متولی امنیت سایبری و حفاظت از داده‌ها در کشور، به‌ویژه سازمان فناوری اطلاعات و امنیت فضای تولید و تبادل اطلاعات (افتا) در مقابله با استعمار داده با چالش‌های متعددی مواجه هستند. «افتا» به‌عنوان مرجع اصلی تنظیم‌گری امنیت فضای تبادل اطلاعات کشور، وظیفه تدوین سیاست‌ها، استانداردها و چارچوب‌های حقوقی-فنی برای حفاظت از داده‌های ملی را بر عهده دارد، اما کارآمدی این سازمان در این مورد با محدودیت‌های قابل توجهی روبه‌روست. از یک‌سو، چارچوب‌های تنظیم‌گری «افتا» به‌طور عمده بر جنبه‌های امنیتی و حفاظتی متمرکز بوده و کمتر به ابعاد راهبردی استقلال داده و مقابله با سلطه دیجیتال پرداخته است. این رویکرد

تک‌بعدی، توانایی کشور در مواجهه با پدیده چندوجهی استعمار داده را محدود می‌سازد. به‌عنوان مثال، مجوزهای صادره توسط «افتا» به‌طور عمده بر الزامات امنیتی تمرکز دارند و کمتر به مسائلی چون حاکمیت داده، مالکیت معنوی الگوریتم‌ها و استقلال زیرساخت‌های پردازشی توجه می‌کنند. از سوی دیگر، فقدان هماهنگی میان سیاست‌های «افتا» با سایر نهادهای تنظیم‌گر و سیاست‌گذار در حوزه فناوری اطلاعات، منجر به پراکندگی و گاه تعارض در رویکردهای مقابله با استعمار داده شده است. این ناهماهنگی، اثربخشی اقدامات حفاظتی را کاهش داده و زمینه را برای نفوذ و سلطه خارجی بر جریان داده‌های ملی فراهم می‌آورد. سرانجام اینکه رویکرد غالباً واکنشی «افتا» در مواجهه با تهدیدات امنیتی، به‌جای اتخاذ رویکردی پیشگیرانه و راهبردی، کارآمدی اقدامات این سازمان را در مقابله با استعمار داده کاهش داده است. تجربه کشورهایی که در مقابله با استعمار داده موفق‌تر بوده‌اند، نشان می‌دهد که رویکردی جامع، پیش‌دستانه و مبتنی بر آینده‌پژوهی برای مقابله با این پدیده ضروری است. بنابراین، بازنگری در ساختار، مأموریت‌ها و رویکردهای «افتا»، با هدف تقویت نقش این سازمان در مقابله با استعمار داده، یکی از ضرورت‌های اساسی برای کاهش آسیب‌پذیری‌های زیرساختی کشور در این حوزه به‌شمار می‌رود.

۳-۱-۵. ضعف سازوکار نظارتی

یکی از چالش‌های اساسی در برخی از کشورها مانند ایران، فقدان نهاد تخصصی مستقل برای نظارت بر حفاظت از داده‌هاست. این خلأ سازمانی باعث شده که نظارت بر رعایت حقوق داده به‌صورت پراکنده و ناکارآمد انجام شود. سیستم‌های نظارتی موجود نیز از کارایی لازم برخوردار نیستند و نبود دستورالعمل‌های استاندارد برای حفاظت از داده‌ها باعث شده که هر سازمان به‌صورت سلیقه‌ای عمل کند. ضعف در هماهنگی بین نهادهای مختلف درگیر نیز مشکل دیگری است که باعث موازی کاری و اتلاف منابع می‌شود. این ناهماهنگی‌ها سرانجام، به کاهش اثربخشی اقدامات حفاظتی منجر می‌شود. به دیگر سخن، ناکارآمدی سیستم‌های نظارتی در پایش و کنترل جریان داده‌ها، نبود نهادهای تخصصی با اختیارات کافی برای نظارت بر عملکرد شرکت‌های فناوری و فقدان سازوکارهای مؤثر برای رصد و مقابله با نقض حقوق دیجیتال شهروندان از جمله عناصر مؤثر در این

خصوص است (Subramani 2023, 92 & 93)

۵-۱-۴. پایین بودن سطح آگاهی عمومی (ضعف در سواد داده)^۱

عدم آگاهی عمومی به عنوان یکی از عوامل زمینه‌ساز استعمار داده‌ها، چالشی فراگیر و عمیق در جوامع معاصر است. این مسئله در عصر دیجیتال که داده‌ها به عنوان سرمایه‌ای ارزشمند شناخته می‌شود، بسیار مهم است. پایین بودن سطح سواد دیجیتال در جامعه، شکافی جدی نسبت به درک و مدیریت مخاطرات فضای مجازی ایجاد کرده است. ناآگاهی عمومی نسبت به ارزش واقعی داده‌های شخصی، منجر به رفتارهای پرخطر در فضای دیجیتال می‌شود (ibid 91). کاربران اغلب بدون درک پیامدهای بلندمدت، داده‌های شخصی خود را در اختیار پلتفرم‌ها و سرویس‌های مختلف قرار می‌دهند. این داده‌ها که شامل اطلاعات هویتی، رفتاری، مالی و حتی زیست‌سنجی است، می‌تواند برای اهداف مختلف تجاری و غیرتجاری مورد سوء استفاده قرار گیرد. همچنین عدم درک صحیح از سازوکارهای جمع‌آوری و پردازش داده‌ها توسط شرکت‌های فناوری باعث می‌شود که کاربران از میزان و عمق نظارتی که بر فعالیت‌های آنلاین آن‌ها اعمال می‌شود، بی‌اطلاع باشند (Ricaurte 2019, 357). افزون بر این، ناآشنایی با حقوق دیجیتال، مانع از مطالبه‌گری مؤثر شهروندان در این حوزه است (حتی در نظام‌های حقوقی که قانونگذاری خاص وجود دارد). بسیاری از کاربران از حقوق اساسی خود مانند حق دسترسی به داده‌های شخصی، حق اصلاح یا حذف داده‌ها و حق انتقال داده آگاهی ندارند. این ناآگاهی باعث می‌شود که شرکت‌های فناوری با آزادی عمل بیشتری به استخراج و بهره‌برداری از داده‌های کاربران بپردازند. سرانجام اینکه نبود درک درست از ارتباط میان داده‌های به ظاهر بی‌اهمیت و امکان استفاده از آن‌ها برای استخراج الگوهای رفتاری و شخصیتی، یکی دیگر از ابعاد این مسئله است. کاربران اغلب تصور می‌کنند که داده‌های روزمره آن‌ها ارزش چندانی ندارد، در حالی که ترکیب و تحلیل این داده‌ها می‌تواند به بینش‌های عمیقی درباره شخصیت، علایق و رفتار آن‌ها منجر شود. این ناآگاهی عمومی سرانجام، به تقویت چرخه استعمار داده‌ها کمک می‌کند. کاربرانی که از ارزش داده‌های خود و مخاطرات فضای دیجیتال آگاه نیستند، به راحتی در دام سرویس‌های رایگان اما داده‌محور می‌افتند و ناخواسته به تداوم این چرخه کمک می‌کنند (Zuboff 2015, 83).

1. data literacy

۵-۲. پیامدهای وجود عوامل زمینه‌ساز و تسهیل‌کننده

عوامل پیش‌گفته در مرحله نخست منجر به ضعف در حاکمیت داده می‌شود و سرانجام، در قالب پنج عنصر (عوامل زمینه‌ای همراه با ضعف در حاکمیت داده) حکمرانی بر داده را تضعیف می‌نماید. توضیح این دو پیامد به‌ترتیب به‌شرح زیر است.

۵-۲-۱. ضعف حاکمیت داده (چارچوب حقوقی)

در عصر حاضر، حاکمیت داده به‌مثابه یک حق حاکمیتی بنیادین برای کشورها مطرح است (Hummel et al. 2021, 7). این مفهوم که به معنای اقتدار قانونی و انحصاری یک کشور بر داده‌های تولیدشده در قلمرو سرزمینی خود است، امروزه در ایران با چالش‌های جدی است. تحلیل نظام‌مند این چالش‌ها نشان می‌دهد که چگونه عوامل زمینه‌ای چهارگانه در یک تعامل پیچیده و سیستمی، به تضعیف حاکمیت داده می‌انجامند. توضیح اینکه در مرحله نخست، ضعف در نظام حقوقی و قانونی، همچون حلقه‌ای مفقوده، توان کشور در اعمال حاکمیت بر داده‌ها را محدود می‌کند. نبود چارچوب‌های قانونی جامع و روزآمد، خلأهای قانونی در حوزه داده‌های فرامرزی و ناکارآمدی ضمانت اجرا، در عمل، امکان کنترل مؤثر بر چرخه حیات داده‌ها را از بین می‌برد (Singi et al. 2020). در مرحله دوم، محدودیت‌های زیرساختی فنی همچون شمشیری دولبه عمل می‌کند. از یک‌سو، وابستگی به زیرساخت‌های خارجی، کشور را در موقعیت آسیب‌پذیری قرار می‌دهد و از سوی دیگر، ناتوانی در ایجاد و توسعه زیرساخت‌های داخلی، این وابستگی را تشدید می‌کند. این چرخه معیوب، به‌تدریج توان کشور در ذخیره‌سازی و پردازش داده‌های ملی را تضعیف می‌کند (Wang et al. 2022). مرحله سوم، یعنی ضعف در نظام نظارتی همچون روزه‌ای است که امکان خروج بی‌ضابطه داده‌ها را فراهم می‌آورد. ناتوانی در رصد جریان‌های داده‌های فرامرزی و عدم کنترل مؤثر بر فعالیت پلتفرم‌های خارجی در عمل، حاکمیت داده را به چالش می‌کشد (Toliupa et al. 2023). سرانجام، پایین بودن سطح سواد دیجیتال در جامعه همچون عامل تشدیدکننده‌ای عمل می‌کند که اثرات منفی سایر عوامل را افزون خواهد کرد. در واقع، عدم آگاهی از اهمیت حفظ داده‌های ملی و استفاده غیرایمن از خدمات دیجیتال خارجی، زمینه را برای تضعیف بیشتر حاکمیت داده فراهم می‌آورد (Oderkirk 2021).

در این راستا، مطالعات متعدد این روابط متقابل و پیچیده میان عوامل تضعیف‌کننده حاکمیت داده را تأیید می‌کنند. به‌عنوان مثال، برخی از محققان در پژوهش خود نشان

داده‌اند که عوامل مؤثر بر حاکمیت داده در یک تعامل پیچیده و سیستمی با یکدیگر قرار دارند و ضعف در هر یک از آن‌ها می‌تواند به شکل‌گیری چرخه‌های معیوب منجر شود. این پژوهشگران با طبقه‌بندی عوامل به چهار گروه بر اساس میزان تأثیرگذاری و تعامل با سایر عوامل تأکید می‌کنند که برخی عوامل نقش کلیدی در شکل‌دهی به کل نظام حاکمیت داده دارند و ضعف در آن‌ها می‌تواند پیامدهای گسترده‌ای در سطح سازمان ایجاد کند. این یافته‌ها با تحلیل سیستمی ارائه‌شده در خصوص تضعیف حکمرانی بر داده همخوانی دارد و نشان می‌دهد که چگونه تعامل پیچیده میان عوامل زمینه‌ای به شکل‌گیری یک همگرایی منفی و سرانجام، ناکارآمدی نظام‌مند می‌انجامد (احمدی و توانا ۱۴۰۱)

۲-۲-۵. تضعیف حکمرانی بر داده (چارچوب راهبردی)

حکمرانی بر داده به معنای چارچوب جامع مدیریت، کنترل و بهره‌برداری از داده‌ها در یک سازمان یا کشور است. این مفهوم شامل مجموعه‌ای از الزامات، سیاست‌ها، فرایندها، استانداردها و ساختارهایی است که برای مدیریت مؤثر داده‌ها طراحی می‌شوند. به‌طور کلی، این مفهوم عام‌تر از حاکمیت داده^۱ است. تحلیل تضعیف حکمرانی داده نشان می‌دهد که این پدیده در بستر یک زیست‌بوم پیچیده و چندلایه شکل می‌گیرد. در این بستر، عوامل زمینه‌ای چهارگانه در تعامل با ضعف حاکمیت داده، به شکل‌گیری یک سندروم ناکارآمدی نظام‌مند می‌انجامد که می‌توان آن را در سه لایه تحلیلی بررسی کرد (Bueger 2021, 399). در لایه نخست، سازوکار شکل‌گیری ناکارآمدی وجود دارد. در این لایه، تعامل پیچیده میان عوامل زمینه‌ای به ایجاد یک همگرایی منفی می‌انجامد؛ ضعف در قانونگذاری، توان نظارتی سیستم را محدود می‌کند؛ محدودیت‌های زیرساختی فنی، ظرفیت اجرایی را کاهش می‌دهد و سطح پایین سواد دیجیتال، امکان مشارکت مؤثر بهره‌داران را تضعیف می‌کند. این عوامل در یک چرخه منفی، یکدیگر را تقویت می‌کنند. لایه دوم، تشکیل چرخه معیوب است. در این لایه، ناکارآمدی اولیه به شکل‌گیری یک چرخه معیوب می‌انجامد. ناتوانی در سیاست‌گذاری مناسب، به ضعف در اجرا منتهی می‌شود. این ضعف اجرایی، نظام ارزیابی را مختل می‌کند و نبود بازخورد مؤثر به‌نوبه خود چالش‌های سیاست‌گذاری را تشدید می‌کند. این چرخه معیوب با هر دور تکرار، عمیق‌تر و پیچیده‌تر می‌شود. لایه سوم، پیامدهای نظام‌مند است. تحلیل عمیق پیامدهای

1. data sovereignty

نظام‌مند مبین آن است که تضعیف حکمرانی بر داده منجر به شکل‌گیری یک زیست‌بوم ناکارآمد می‌شود که در سه بُعد اصلی قابل بیان است (Kwet 2019). ابتدا، بُعد ساختاری است. این امر یعنی نظام یکپارچه مدیریت داده به تدریج دچار فرسایش می‌شود. این فرسایش با ازهم‌گسیختگی ارتباطات بین بخشی آغاز شده و به تدریج به ایجاد جزایر اطلاعاتی منجر می‌شود. در نتیجه، ساختارهای موازی و ناهماهنگ شکل می‌گیرند که نه تنها کارایی سیستم را کاهش می‌دهند، بلکه هزینه‌های مدیریتی را نیز افزایش می‌دهند. این وضعیت به تدریج به یک ساختار سازمانی ناکارآمد می‌انجامد که در آن، هماهنگی بین سازمانی به حداقل می‌رسد. جنبه دیگر، بُعد کارکردی است. در این بُعد، اثربخشی سیاست‌های حوزه داده به شدت کاهش می‌یابد. سیستم‌های مدیریتی قادر به پیاده‌سازی مؤثر سیاست‌ها نیستند و هزینه‌های عملیاتی به‌طور فزاینده‌ای افزایش می‌یابد. کیفیت خدمات داده‌محور افت می‌کند و سیستم در یک چرخه معیوب از ناکارآمدی گرفتار می‌شود (Couldry & Mejias 2019a). این وضعیت منجر به نارضایتی بهره‌داران و کاهش اعتماد به سیستم می‌شود. سرانجام، بُعد راهبردی قابل اشاره است. در سطح راهبردی، سیستم توان رقابتی در اقتصاد دیجیتال را از دست می‌دهد. وابستگی به سیستم‌های خارجی افزایش می‌یابد و این وابستگی به نوبه خود، توان نوآوری و توسعه فناوری‌های بومی را تضعیف می‌کند. در نتیجه، سیستم در یک چرخه وابستگی فزاینده گرفتار می‌شود که خروج از آن به تدریج دشوارتر می‌شود (Vardanyan & Kocharyan 2022, 117).

به دیگر سخن، آنچه بیان شد - یعنی عوامل زمینه‌ای چهارگانه و ضعف حاکمیت داده- در تعامل با یکدیگر به شکل‌گیری یک ناکارآمدی نظام‌مند می‌انجامد که مشخصه اصلی آن، ناتوانی در مواجهه با چالش‌های نوظهور است. بررسی‌ها حکایت از این دارد که تضعیف حکمرانی داده نه یک رویداد مجزا، بلکه نتیجه یک فرایند تدریجی و نظام‌مند است که در آن، تعامل پیچیده عوامل مختلف به شکل‌گیری یک وضعیت ناکارآمد و خودتقویت‌کننده می‌انجامد. در انتها باید گفت که برآیند این عوامل در یک تعامل نظام‌مند، به شکل‌گیری پیامدهای چندوجهی می‌انجامد؛ از جمله، در بُعد امنیتی، آسیب‌پذیری در برابر تهدیدات سایبری افزایش می‌یابد؛ در حوزه اقتصادی، ارزش افزوده داده‌ها به نفع شرکت‌های خارجی مصادره می‌شود؛ در عرصه اجتماعی، حریم خصوصی اطلاعاتی شهروندان، داده‌های شخصی و هویت دیجیتال ملی تضعیف می‌شود؛ و در بُعد ژئوپلیتیک، استقلال دیجیتال کشور به مخاطره می‌افتد. این وضعیت سرانجام،

به شکل‌گیری استعمار داده می‌انجامد که در آن، کشور نه تنها کنترل مؤثر بر داده‌های خود را از دست می‌دهد، بلکه در چرخه معیوبی از وابستگی دیجیتال گرفتار می‌شود (Hongladarom 2023, 2359)

۶. چگونگی مقابله با استعمار داده

راهکارهای مقابله با استعمار داده مستلزم رویکردی جامع و نظام‌مند است که متناظر با عوامل زمینه‌ساز ارائه شده باشد. در این راستا، چهار حوزه راهبردی شامل قانون‌گذاری خاص و تقویت چارچوب‌های حقوقی، توسعه زیرساخت‌های فنی، ارتقای سازوکارهای نظارتی، و افزایش سطح سواد دیجیتال به‌عنوان ارکان اصلی مقابله با استعمار داده شناسایی می‌شوند. این راهکارهای چهارگانه در تعامل با یکدیگر، ضمن تقویت حاکمیت ملی بر داده‌ها به استحکام نظام حکمرانی داده می‌انجامند. در ادامه، ضمن تشریح این راهکارها، بر تقویت حاکمیت داده و استحکام نظام حکمرانی بر داده نیز تأکید خواهد شد.

۶-۱. مقابله با عوامل زمینه‌ساز و تسهیل‌کننده

یکی از راهکارهایی که تاکنون کمتر بدان توجه شده، حمایت‌های قانونی است که مبتنی بر ایجاد نظام حقوقی چندسطحی در خصوص حفاظت از داده باشد. این رویکرد، حمایت از داده را در سه سطح مکمل انجام می‌دهد. سطح نخست، حمایت بنیادین مبتنی بر اصلاح قوانین موجود و افزودن مفاد مستقل در مورد «حقوق بر داده»^۱ است. در این لایه، حمایت از داده به‌عنوان یک حق بنیادین شهروندی تعریف می‌شود و ضمانت‌های قانونی قوی برای حفاظت از آن ایجاد می‌گردد. این حمایت بنیادین پایه‌های اصلی حقوقی را برای تضمین امنیت و حریم خصوصی داده فراهم می‌آورد و اطمینان می‌دهد که حقوق شهروندان در فضای دیجیتال به‌خوبی حفظ می‌شود. در لایه دوم، حمایت عام یعنی تدوین قانون جامع حفاظت از داده و ایجاد نظام جبران خسارت باید مورد توجه قرار گیرد. این لایه شامل پوشش خسارات مادی و معنوی ناشی از نقض حقوق داده است و با تدوین قوانین جامع، چارچوب قانونی موسّعی برای مقابله با تخلفات فراهم خواهد شد. لایه سوم، حمایت خاص است که به تدوین الزامات حقوقی ویژه برای داده‌های خاص مانند داده‌های شخصی حساس، داده‌های کودکان و داده‌های کیفری می‌پردازد. این لایه با ایجاد نظام

1. data rights

اولویت‌بندی نسبت به حساسیت داده‌ها و تعیین ضمانت اجرای متناسب با سطح حساسیت تضمین می‌کند که داده‌های خاص با بیشترین دقت و امنیت حفاظت شوند. فارغ از چارچوب‌های قانونی، حمایت قضایی نیز به‌عنوان رکن مکمل، نقشی حیاتی در مقابله با استعمار داده ایفا می‌کند. دستگاه قضایی با تفسیر پویا از قوانین موجود، ایجاد رویه قضایی منسجم و صدور آرای بازدارنده می‌تواند خلأهای قانونی را پوشش داده و ضمانت اجرای مؤثری برای حمایت از حقوق دیجیتال شهروندان و مقابله با سوء استفاده از داده فراهم آورد. در این راستا سازوکار جبران خسارت پیشینی با محاسبه و تعیین خسارات احتمالی قبل از وقوع و ایجاد صندوق تضمین جبران خسارات داده، اطمینان بیشتری برای حمایت از حقوق داده ایجاد می‌کند. افزون بر این، تعیین خسارات تنبیهی برای نقض‌های عمدی، جنبه بازدارندگی نظام حقوقی را تقویت می‌نماید و از وقوع تخلفات جلوگیری می‌کند (Subramani 2023, 94-97).

از سوی دیگر، توجه به سازوکار مناسب فنی-نظارتی نیز لازم است. در گام نخست این مورد، پیاده‌سازی راهکارهای فنی کوتاه‌مدت اهمیت ویژه‌ای دارد. استقرار سامانه‌های پایش هوشمند جریان داده و سیستم‌های تشخیص نفوذ، اولین خط دفاعی در برابر تهدیدات محسوب می‌شود. این سیستم‌ها باید با دستورالعمل‌های رمزنگاری پیشرفته تقویت شده و با قابلیت پاسخ سریع پشتیبانی شوند. تجربه نشان داده است که واکنش سریع به تهدیدات، نقش کلیدی در کاهش خسارات احتمالی دارد. همزمان با تقویت زیرساخت‌های فنی، راهکارهای نظارتی نیز باید عملیاتی شوند. تشکیل کارگروه تخصصی نظارت بر داده و تدوین دستورالعمل‌های اجرایی شفاف، زیربنای نظام نظارتی کارآمد را تشکیل می‌دهند. این ساختار نظارتی باید با سامانه گزارش‌دهی تخلفات و سازوکار بازرسی‌های دوره‌ای تکمیل شود تا امکان شناسایی و مقابله سریع با تخلفات فراهم آید. از سوی دیگر، در افق میان‌مدت، توسعه زیرساخت‌های ذخیره‌سازی امن و سیستم‌های ممیزی خودکار ضروری است. افزون بر این، تقویت ساختار اجرایی از طریق تعیین متولی واحد با اختیارات مشخص و ایجاد واحدهای تخصصی، گام بعدی در این مسیر است. در این ساختار باید از پراکندگی و موازی کاری جلوگیری نمود و زمینه پاسخگویی مؤثر نسبت به چالش‌های حوزه داده را فراهم آورد. این امر مستلزم تدوین آیین‌نامه‌های اجرایی شفاف، تعیین سلسله‌مراتب سازمانی مشخص و برقراری نظام ارتباطی کارآمد میان واحدهای مختلف است (Balkin 2018, 1155). ناگفته نماند که در این مسیر، آموزش و آگاهی‌بخشی عمومی

نیز عنصری کلیدی برای مقابله با استعمار داده است. این امر بدین معناست که شهروندان باید از ارزش داده‌های خود و اهمیت حفاظت از آن‌ها آگاه باشند (Calzati 2021, 927)

۲-۶. استقرار نظام ملی حاکمیت داده و تقویت حاکمیت و حکمرانی بر داده

تحقق حاکمیت ملی مؤثر بر داده مستلزم دو گام اساسی است. گام نخست، ایجاد نظام ملی حاکمیت داده است که چارچوب‌های حقوقی، فنی و نهادی لازم برای اعمال حاکمیت بر داده را تعیین می‌کند. در گام دوم، تقویت و استحکام بخشی به این نظام از طریق سازوکارهای اجرایی و نظارتی مورد توجه قرار می‌گیرد. در ادامه، ضمن تبیین اجزا و عناصر اصلی نظام ملی حاکمیت داده، راهکارهای عملیاتی برای تقویت حاکمیت و حکمرانی بر داده مورد بررسی قرار می‌گیرد

۲-۶-۱. ضرورت ایجاد نظام ملی حاکمیت داده (پایه‌گذاری استقلال داده‌محور)

در عصر دگرگونی، استقرار نظام ملی حاکمیت داده به مثابه زیربنای حاکمیت سایبری کشورها از ضرورت‌های انکارناپذیر به شمار می‌رود. این ضرورت از آنجا ناشی می‌شود که داده‌ها در نقش سرمایه‌های راهبردی، نه تنها بنیان اقتصاد دیجیتال را شکل می‌دهند، بلکه به عنوان عامل قدرت ساز در معادلات ژئوپلیتیک نوین نیز ایفای نقش می‌کنند (Shoker 2022). تجربه کشورهای پیشرو نشان می‌دهد که نظام حاکمیت داده باید بر پایه ساختاری سه لایه استوار باشد که هر لایه کارکردی متمایز، اما مکمل دارد. لایه راهبردی به عنوان لایه فوقانی با تمرکز بر حفظ استقلال دیجیتال و تأمین امنیت داده‌ای، نقش سپر محافظتی در برابر استعمار داده ایفا می‌کند. این لایه با تدوین سیاست‌های کلان و تعیین خطوط قرمز راهبردی، چارچوب اصلی حرکت کل نظام را مشخص می‌سازد (Rebro et al. 2021). لایه میانی که ماهیت اقتصادی دارد، بر خلق ارزش از داده‌های ملی متمرکز است. این لایه با ایجاد زیست بوم نوآوری داده‌محور، زمینه را برای شکل‌گیری اقتصاد دیجیتال بومی و کاهش وابستگی به پلتفرم‌های خارجی فراهم می‌آورد. کارکرد اصلی این لایه، تبدیل داده‌های خام به ثروت ملی از طریق فرایندهای هوشمند ارزش آفرینی است (Chen 2021). لایه زیرین که در تعامل مستقیم با شهروندان است، مسئولیت حفاظت از حقوق دیجیتال، حریم خصوصی اطلاعاتی شهروندان و داده‌های شخصی را بر عهده دارد. این لایه با تضمین امنیت داده‌های شخصی و ارائه خدمات عمومی داده‌محور، پایه‌های اعتماد دیجیتال را در جامعه مستحکم می‌سازد. تعامل پویا و هم‌افزای این سه لایه، زیست بومی

یکپارچه شکل می‌دهد که در آن، ضمن حفظ منافع ملی و حقوق شهروندی، زمینه برای توسعه اقتصاد دیجیتال فراهم می‌شود. فقدان چنین نظامی می‌تواند به آسیب‌پذیری‌های جدی از جمله از دست رفتن حاکمیت بر داده‌های ملی، وابستگی فزاینده به قدرت‌های خارجی و تضعیف حقوق دیجیتال شهروندان منجر شود

بنابراین، استقرار نظام ملی حاکمیت داده نه یک گزینه اختیاری، بلکه الزامی راهبردی برای حفظ استقلال و منافع ملی در عصر داده است. این امر از آن جهت دارای اهمیت است که داده‌ها به‌عنوان دارایی‌های راهبردی کشور، نقش تعیین‌کننده‌ای در قدرت ملی، توسعه اقتصادی و امنیت سایبری ایفا می‌کنند. بر این اساس، نظام ملی حاکمیت داده باید مبتنی بر دو اصل کلیدی باشد. نخست، برخورداری از چارچوب‌های حقوقی-نهادی مستحکم برای مقابله مؤثر با چالش‌های نوظهور در حوزه حفاظت از داده‌های ملی، و دوم، دارا بودن سازوکارهای انعطاف‌پذیر برای انطباق با تحولات مستمر در عرصه فناوری. تلفیق این دو اصل، ضمن تأمین اقتدار حاکمیتی در فضای داده، زمینه بهره‌برداری بهینه از فرصت‌های اقتصاد داده‌محور را نیز فراهم می‌آورد (Pohle & Thiel 2020; Leone 2021)

در راستای آنچه بیان شد، نتایج پژوهش‌های داخلی به‌خوبی مؤید ضرورت اتخاذ رویکرد چندلایه‌ای در طراحی چارچوب حاکمیت داده است. به‌عنوان نمونه «مرتضوی، معینی و ساجدی‌نژاد» با بهره‌گیری از روش نظریه داده‌بنیاد، پانزده مؤلفه کلیدی در قالب سه گروه اصلی شامل مؤلفه‌های اصلی حکمرانی، مؤلفه‌های کسب و کار و مؤلفه‌های پشتیبان شناسایی و طبقه‌بندی کرده‌اند (۱۴۰۳). در همین راستا، پژوهش «نقشینه، فهم‌نیا و احمدیان» نیز با شناسایی ده مؤلفه کلیدی در سه لایه اصلی بر اهمیت استانداردسازی، مدیریت و شفافیت در استقرار نظام ملی حاکمیت داده تأکید می‌کند. این مطالعه نشان می‌دهد که توجه به این محورهای سه‌گانه نقش مهمی در تحقق استقلال دیجیتال و حفظ حاکمیت ملی بر داده‌ها ایفا می‌کند (۱۴۰۰). نتایج این پژوهش‌ها حاکی از آن است که چارچوب چندلایه‌ای حاکمیت داده، ضمن فراهم آوردن امکان مدیریت یکپارچه داده‌های ملی، از پراکندگی و ناهماهنگی در سیاست‌گذاری و اجرا جلوگیری می‌کند. این مهم به‌ویژه در شرایط کنونی که حجم و تنوع داده‌ها به‌طور مستمر در حال افزایش است، اهمیتی دوچندان می‌یابد. همچنین، یافته‌های این مطالعات بر ضرورت توجه همزمان به ابعاد راهبردی، اقتصادی و حقوق شهروندی در طراحی و استقرار نظام حاکمیت داده تأکید دارد. این رویکرد جامع و چندبعدی می‌تواند تضمین‌کننده موفقیت در پیاده‌سازی نظام حاکمیت داده و دستیابی به

اهداف کلان آن باشد.

فارغ از آنچه بیان شد توجه به نکته‌ای دیگر نیز لازم است. برخی از محققان در تحلیل انتقادی خود از مفهوم استعمار داده استدلال می‌کنند که حاکمیت داده فراتر از یک موضوع صرفاً فنی یا اقتصادی است. از این منظر، این پدیده به‌طور بنیادین با نظام‌های معرفتی و الگوهای شناختی^۱ مرتبط است. بدین جهت استعمار داده به‌عنوان چارچوبی که استخراج داده را شکل نوینی از استعمار تلقی می‌کند، درک عمیق‌تری از پیامدهای دیجیتال شدن ارائه می‌دهد. با این حال، دستیابی به استقلال واقعی در حوزه داده مستلزم به چالش کشیدن دو فرض اساسی ادعای برتری‌انگاری دانش غربی، و فرض جهان‌شمولی الگوهای غربی نسبت به مدیریت داده است. از این دیدگاه، توسعه نظام‌های دانشی بومی یک ضرورت راهبردی است. این امر به این دلیل است که پذیرش بی‌چون‌وچرای مدل‌های غربی مدیریت داده می‌تواند به شکل جدیدی از وابستگی شناختی منجر شود. بنابراین، در استقرار نظام ملی حاکمیت داده -فارغ از ابعاد بیان‌شده- بعد معرفت‌شناختی (توسعه الگوهای بومی فهم و مدیریت داده) نیز لازم است. این رویکرد تضمین می‌کند که استقلال در عصر داده صرفاً به استقلال فنی و اقتصادی محدود نشده و استقلال شناختی را نیز دربرمی‌گیرد (Mumford 2022)

۲-۲-۶. تقویت حاکمیت داده و زمینه‌سازی برای استحکام حکمرانی بر داده

تقویت حاکمیت داده و استحکام حکمرانی بر آن مستلزم درک عمیق از تحولات عصر دیجیتال و بازتعریف مفهوم قدرت در فضای سایبری است. در این عصر، توانایی کنترل و مدیریت جریان داده‌ها به عنصر کلیدی اقتدار ملی تبدیل شده و حاکمیت مؤثر بر داده‌ها، پیش‌شرط اساسی استقلال دیجیتال کشور محسوب می‌شود (Couture & Toupin 2019). ساختار تقویت حاکمیت داده باید بر پایه نگرشی راهبردی به مفهوم قدرت دیجیتال شکل گیرد. این ساختار از یک‌سو باید توانایی حفظ و صیانت از داده‌های ملی را داشته باشد و از سوی دیگر، ظرفیت خلق ارزش از این دارایی راهبردی را فراهم آورد (Glasze et al. 2022). چنین ساختاری با تکیه بر توانمندی‌های درونی و بهره‌گیری هوشمندانه از فناوری‌های نوین، زمینه را برای شکل‌گیری اقتدار دیجیتال فراهم می‌آورد. همچنین چارچوب حقوقی این ساختار باید متناسب با پویایی‌های فضای دیجیتال طراحی شود و

1. epistemic

ضمن حفظ انسجام درونی، قابلیت انطباق با تحولات فناورانه را داشته باشد. این چارچوب با تعریف دقیق حقوق و تکالیف تمامی کنشگران، مشروعیت اقدامات حاکمیتی در حوزه داده را تضمین می‌کند و بستر لازم برای مشارکت مؤثر بخش خصوصی و نهادهای علمی را فراهم می‌آورد. افزون بر این، تقویت عملیاتی این ساختار مستلزم ایجاد سازوکارهای اجرایی پایدار و کارآمد است. این سازوکارها باید ضمن تضمین امنیت داده‌ها، امکان بهره‌برداری بهینه از آن‌ها را نیز فراهم آورند. توسعه زیرساخت‌های فناورانه بومی، تربیت نیروی انسانی متخصص و ایجاد شبکه ملی نوآوری در حوزه فناوری‌های داده‌محور، ارکان اصلی این استحکام عملیاتی را تشکیل می‌دهند. سرانجام اینکه موفقیت این ساختار در گرو تعامل سازنده میان تمامی ارکان حاکمیتی و مشارکت فعال جامعه علمی و فناوری کشور است. این تعامل باید در چارچوب یک نظام یکپارچه مدیریت دانش شکل گیرد تا امکان یادگیری مستمر و تکامل تدریجی ساختار فراهم شود. چنین رویکردی، ضمن تقویت حاکمیت داده، زمینه را برای شکل‌گیری اقتدار پایدار در عصر دیجیتال فراهم می‌آورد (Kukutai 2023).

۷. نتیجه‌گیری و پیشنهادها

در عصر حاضر که داده به مثابه منبع راهبردی و عنصر کلیدی قدرت ملی محسوب است، مقابله با استعمار داده به ضرورتی حاکمیتی مبدل شده است. در این راستا پژوهش حاضر با تحلیل پدیده استعمار داده به عنوان شکل نوینی از سلطه‌گری، تبیین نموده است که بر خلاف اشکال سنتی استعمار، این پدیده از طریق سازوکارهای پیچیده‌تر و کم‌هزینه‌تری عمل می‌کند و تأثیرات عمیق‌تری بر حاکمیت ملی کشورها بر جای می‌گذارد. یافته‌های پژوهش مؤید آن است که چهار عامل اصلی شامل خلأهای قانونی، ضعف زیرساختی فنی، نقص در نظام نظارتی، و پایین بودن سطح آگاهی عمومی در شکل‌گیری و تداوم استعمار داده نقش محوری ایفا می‌کنند. این عوامل در تعامل با یکدیگر، بستر مناسبی را برای تسلط بر داده‌های ملی و استثمار ارزش نهفته در آن‌ها فراهم می‌آورند. بدین جهت تحلیل‌های صورت گرفته نشان می‌دهند که مقابله با این پدیده مستلزم رویکردی جامع و نظام‌مند برای مقابله است. توضیح اینکه، در این مسیر ایجاد نظام حقوقی چندسطحی حفاظت از داده لازم است که به عنوان راهکاری اساسی برای مقابله با استعمار داده در سه سطح متمایز، اما مرتبط عمل کند. در سطح نخست، حمایت‌های بنیادین از طریق اصلاح قوانین

موجود و گنجانیدن اصول مستقل در خصوص «حق حاکمیت بر داده» صورت می‌پذیرد. در سطح دوم، حمایت‌های عام از طریق تدوین قانون جامع حفاظت از داده و استقرار نظام جبران خسارت محقق می‌گردد. در سطح سوم، حمایت‌های خاص با تمرکز بر تدوین الزامات حقوقی ویژه برای داده‌های حساس نظیر داده‌های شخصی خاص و تعیین ضمانت اجرای متناسب صورت می‌پذیرد. این نظام حقوقی باید با استقرار نظام ملی حاکمیت داده تکمیل گردد؛ نظامی که بر پایه ساختاری سه‌لایه شامل لایه راهبردی (سیاست‌گذاری)، لایه اقتصادی (خلق ارزش) و لایه حمایتی (تأمین امنیت و حفظ حقوق) استوار باشد. نتایج پژوهش همچنین مبین آن است که تقویت حاکمیت داده مستلزم بازتعریف مفهوم قدرت در فضای سایبری است. در این عصر، قدرت ملی از انحصار ابزارهای سنتی خارج شده و توانایی کنترل و مدیریت جریان داده‌ها به عنصر کلیدی برای حاکمیت و اقتدار ملی تبدیل گردیده است؛ به گونه‌ای که تسلط بر داده‌های ملی و توانمندی تحلیل و بهره‌برداری از آن‌ها شاخص نوینی از قدرت محسوب می‌شود.

فارغ از برآمد پژوهش - که مورد توجه قرار گرفت - راهکارهای پیشنهادی مبتنی بر یافته‌های پژوهش که خواهد آمد نیز می‌تواند مورد استفاده باشد. از منظر حقوقی - فنی تعیین نظام حقوقی مشخص برای مالکیت داده از اهمیت به‌سزایی برخوردار است. در این راستا، قانون‌گذار باید با تفکیک میان انواع مختلف داده (شخصی، عمومی، تجاری و غیره)، نظام حقوقی متناسب با هر دسته را تعیین نماید. این امر مستلزم بازنگری در قوانین مالکیت فکری و توسعه مفاهیم نوینی چون «حق حاکمیت بر داده» است که در نظام حقوقی کنونی کمتر مورد توجه قرار گرفته‌اند. همچنین، ایجاد شبکه ملی مراکز داده با ظرفیت کافی برای ذخیره‌سازی و پردازش داده‌های تولیدشده در کشور از ضروریات زیرساختی محسوب می‌گردد. این مراکز باید با «معماری توزیع‌شده» طراحی شوند تا افزون بر افزایش تاب‌آوری، امکان پردازش محلی داده‌ها را فراهم آورند. توسعه زیرساخت‌های ارتباطی پرسرعت و کم‌تأخیر برای اتصال این مراکز داده نیز از الزامات تکمیلی این رویکرد است.

در بُعد نظارتی، تأسیس نهاد تنظیم‌گر مستقل در حوزه داده با اختیارات قانونی کافی ضرورت دارد. این نهاد باید از استقلال سازمانی و مالی برخوردار بوده و صلاحیت نظارت بر عملکرد تمامی پردازشگران داده را داشته باشد. همچنین، اختیار صدور دستورالعمل‌های الزام‌آور و اعمال ضمانت اجرایی متناسب از جمله صلاحیت‌های ضروری این نهاد محسوب

می‌گردد. افزون بر این، استقرار نظام پایش ملی جریان داده با هدف شناسایی و مدیریت نقاط خروج داده‌های حساس ملی نیز از دیگر اقدامات نظارتی ضروری است. این نظام باید با رعایت اصول حقوقی بنیادین شهروندان، امکان رصد جریان کلان‌داده‌ها را فراهم آورده و از خروج غیرمجاز داده‌های حساس جلوگیری نماید. تحقق این هدف مستلزم تعریف دقیق مفهوم «داده‌های حساس» و تعیین چارچوب حقوقی خاص برای آن‌هاست

همچنین از منظر آموزشی-فرهنگی، ضرورت دارد که فراتر از برنامه‌های آموزشی موجود، در برخی دوره‌ها و دانشگاه‌ها رویکردی عملیاتی و کاربردی برای ارتقای سواد دیجیتال طراحی گردد. در گام نخست، می‌توان با تشکیل کارگروه مشترک میان وزارتخانه‌های ارتباطات و فناوری اطلاعات، علوم و آموزش و پرورش نسبت به بازنگری محتوای آموزشی موجود و شناسایی خلأهای آموزشی در زمینه حکمرانی داده اقدام نمود. این اقدام می‌تواند به تدوین «سند ملی سواد دیجیتال» با تمرکز ویژه بر مفاهیم حاکمیت داده و امنیت اطلاعات منجر شود. بر اساس این سند، تدوین بسته‌های آموزشی متناسب با سطوح مختلف تحصیلی صورت گرفته و در مرحله بعد، آموزش مربیان و معلمان در قالب دوره‌های ضمن خدمت با محوریت مفاهیم پایه حاکمیت داده و امنیت اطلاعات می‌تواند زمینه‌ساز انتقال این مفاهیم به دانش‌آموزان و دانشجویان باشد. همچنین، برگزاری کارگاه‌های آموزشی کوتاه‌مدت برای مدیران میانی و ارشد دستگاه‌های اجرایی با تمرکز بر شناسایی مصادیق استعمار داده در حوزه کاری مربوط و راهکارهای عملی مقابله با آن می‌تواند به ارتقای آگاهی تصمیم‌گیرندگان کمک‌شایانی نماید. در سطح عمومی نیز تولید محتوای آموزشی ساده و کاربردی با محوریت اصول حفاظت از داده‌های شخصی و انتشار گسترده آن از طریق رسانه‌های عمومی و شبکه‌های اجتماعی می‌تواند گامی مؤثر در جهت افزایش آگاهی عمومی و ترویج فرهنگ خودمراقبتی دیجیتال باشد

در عرصه بین‌المللی نیز فراتر از مشارکت منفعلانه در معاهدات موجود، باید رویکردی فعال و پیشگامانه اتخاذ نمود. محور اصلی این امر می‌تواند تأسیس ائتلاف کشورهای در حال توسعه برای حاکمیت داده با هدف تدوین اصول و استانداردهای مشترک در مقابله با استعمار داده باشد. این ائتلاف می‌تواند پیشنهاد تدوین پروتکل الحاقی حمایت از حاکمیت داده ملی در چارچوب معاهدات بین‌المللی موجود را مطرح نموده و زمینه‌ساز ایجاد مراکز پایش داده با مشارکت کشورهای همسایه برای شناسایی و مقابله با تهدیدات نوظهور در این حوزه گردد. چنین ساختاری بستر مناسبی برای همکاری میان کشورهای در حال توسعه

فراهم خواهد آورد که هدف آن انتقال فناوری و دانش فنی در حوزه زیرساخت‌های ذخیره‌سازی و پردازش داده خواهد بود

سرانجام اینکه باید تأکید نمود که هدف از مقابله با استعمار داده، نه انزوای دیجیتالی، بلکه دستیابی به استقلال داده است. این مهم از طریق تقویت زیرساخت‌های ملی، ارتقای توانمندی‌های فنی داخلی و مشارکت فعال در شکل‌دهی به نظام حکمرانی جهانی داده محقق می‌گردد. پژوهش حاضر با تبیین ماهیت استعمار داده، شناسایی سازوکارهای آن، تبیین چالش‌های این حوزه و ارائه راهکارهایی برای مقابله، چارچوبی راهبردی برای تصمیم‌گیرندگان حوزه حکمرانی داده فراهم آورده و می‌تواند زمینه‌ساز پژوهش‌های آتی در این حوزه راهبردی باشد. نتیجه نهایی این امر، تحقق حاکمیت مؤثر بر داده‌های ملی و صیانت از حقوق دیجیتال شهروندان خواهد بود

فهرست منابع

- احمدی، صدرا، و محمد مهدی توانا. ۱۴۰۱. ارائه رویکرد فازی جدید برای سنجش استقرار حاکمیت داده و مدیریت عوامل مربوط به آن. *چشم‌انداز مدیریت صنعتی* ۱۲ (۱، پیاپی ۴۵): ۸۳-۱۰۸. شناسه برنمود دیجیتال: 10.52547/jimp.12.1.83
- لطیف‌زاده، مهدیه، سید محمد مهدی قبولی درافشان، سعید محسنی، و محمد عابدی. ۱۴۰۱. تبیین اسباب مشروعیت پردازش داده شخصی از منظر حقوق اتحادیه اروپا و ایران. *مطالعات حقوقی* ۱۴ (۳): ۳۶۴-۳۲۵. شناسه برنمود دیجیتال: 10.22099/jls.2022.40620.4390
- مرتضوی، محمدرضا، علی معینی، و آرمان ساجدی‌نژاد. ۱۴۰۳. چارچوب حکمرانی داده در مراکز تبادل داده. *علوم و فنون مدیریت اطلاعات* ۱۰ (۱): ۸۹-۱۱۶. شناسه برنمود دیجیتال: 10.22091/stim.2022.7668.1700
- مرکز پژوهش‌های مجلس شورای اسلامی. ۱۴۰۳. طرح حفاظت از داده‌های شخصی. تهران: مرکز پژوهش‌های مجلس شورای اسلامی. https://rc.majlis.ir/fa/legal_draft/show/1816729 (دسترسی در ۲ بهمن ۱۴۰۳)
- نقشینه، نادر، فاطمه فهم‌نیا، و حمیدرضا احمدیان. ۱۴۰۰. ارائه چارچوبی برای دادگان ملی با تمرکز بر توسعه حاکمیت داده. *فناوری اطلاعات و ارتباطات ایران* ۱۳ (۴۹-۵۰): ۵۷-۸۴. شناسه برنمود دیجیتال: 20.1001.1.27170411.1400.13.49.2.7

References

- Ahmadi, Sadra, and Mohammad Mahdi Tavana. 2022. A New Fuzzy Approach to Assess the Implementation of Data Governance and Management of Related Factors. *Journal of Industrial Management Perspective* 12 (1): 83-108. <https://doi: 10.52547/jimp.12.1.83> [In Persian]
- Balkin, Jack M. 2018. Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *UC Davis Law Review* 51: 1149-1214.

- Bucher, Taina. 2016. The algorithmic imaginary: exploring the ordinary effects of Facebook algorithms. *Information, Communication & Society* 20 (1): 30-44. <https://doi.org/10.1080/1369118X.2016.1154086>
- Bueger, Christian, and Tobias Liebetrau. 2021. Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy* 42: 391-413. <https://doi.org/10.1080/13523260.2021.1907129>
- Calzati, Stefano. 2021. Decolonising "Data Colonialism" Propositions for Investigating the Realpolitik of Today's Networked Ecology. *Television & New Media* 22 (8): 914-929. <https://doi.org/10.1177/1527476420957267>
- Chen, Si. 2021. Research on data sovereignty rules in cross-border data flow and Chinese solution. *US-China Law Review* 18: 261. <https://doi.org/10.17265/1548-6605/2021.06.001>
- Cohen, Julie E. 2017. The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy. *Philosophy & Technology* 31 (2): 213-233. <https://doi.org/10.1007/s13347-017-0258-2>
- Coleman, Danielle. 2019. Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. *Michigan Journal of Race & Law* 24: 417-439. <https://doi.org/10.36643/mjrl.24.2.digital>
- Couldry, Nick, and Ulises A. Mejias. 2019a. Making data colonialism liveable: How might data's social order be regulated? *Internet Policy Review* 8 (2): 1-16. <https://doi.org/10.14763/2019.2.1411>
- _____. 2019b. The costs of connection: How data is colonizing human life and appropriating it for capitalism. *Stanford University Press*. <https://doi.org/10.1515/9781503609754>
- _____. 2019c. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. *Television & New Media* 20 (4): 336-349. <https://doi.org/10.1177/1527476418796632>
- Couture, Stéphane, and Sophie Toupin. 2019. What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society* 21: 2305-2322. <https://doi.org/10.1177/1461444819865984>
- DataReportal. 2024. Digital 2024: Iran. <https://datareportal.com/reports/digital-2024-iran> (accessed Dec. 25, 2024)
- Dijk, José van, and Bernhard Rieder. 2019. The recursivity of internet governance research. *Internet Policy Review* 8 (2). <https://doi.org/10.14763/2019.2.1418>
- Glasse, Georg, Amaël Cattaruzza, Frédéric Douzet, Finn Dammann, Marie Bertran, Clément Bômont, Mareike Braun, Didier Danet, Alix Desforges, Aude Géry, Stéphane Grumbach, Patrice Hummel, Kevin Limonier, Maximilian Münßinger, Felix Nicolai, Louis Pétiniaud, Jantje Winkler, and Clarisse Zanin. 2022. Contested Spatialities of Digital Sovereignty. *Geopolitics* 28: 919-958. <https://doi.org/10.1080/14650045.2022.2050070>
- Hongladarom, Soraj. 2023. Shoshana Zuboff, The age of surveillance capitalism: The fight for a human future at the new frontier of power. *AI & SOCIETY* 38 (6): 2359-2361. <https://doi.org/10.1007/s00146-020-01100-0>
- Hummel, Patrik, Matthias Braun, Max Tretter, and Peter Dabrock. 2021. Data sovereignty: A review. *Big Data & Society*: 1-17. <https://doi.org/10.1177/2053951720982012>
- Ilyas, Muhammad. 2022. Terrorism Industry and Data Coloniality in Southeast Asia. *Journal of Contemporary Governance and Public Policy* 331-46 : (1) . <https://doi.org/10.46507/jcgp.v3i1.65>
- Islamic Parliament Research Center. 2024. Personal Data Protection Bill. Tehran: Islamic Parliament Research Center. https://rc.majlis.ir/fa/legal_draft/show/1816729 (accessed January 2, 2025) [In Persian]
- Katzenbach, Christian, and Thomas Christian Bächle. 2019. Defining concepts of the digital society. *Internet Policy Review* 84)). <https://doi.org/10.14763/2019.4.1430>
- Kukutai, Tahu. 2023. Indigenous data sovereignty-A new take on an old theme. *Science* 382 (6674): eadl4664. <https://doi.org/10.1126/science.adl4664>

- Kwet, Michael. 2019. Digital colonialism: Implications for the Global South. *Critical Studies in Media Communication* 36 (2): 1-18. <https://doi.org/10.1080/15295036.2019.1594776>
- Latifzadeh, Mahdieh, Seyed Mohammad Mahdi Ghabooli Dorafshan, Saeed Mohseni, and Mohammad Abedi. 2022. Explain the reasons for the legitimacy of personal data processing from the perspective of EU and Iranian law. *Journal of Legal Studies* 14 (3): 325-364. <https://doi.org/10.22099/jls.2022.40620.4390> [In Persian]
- Leone, Deanna. 2021. Data colonialism in Canada: Decolonizing data through Indigenous data governance [master's thesis, Carleton University]. Carleton University Research Virtual Environment (CURVE). <https://doi.org/10.22215/etd/2021-14697>
- Mortazavi, Mohammad Reza, Ali Moeini, and Arman Sajedinejad. 2024. Data Governance Framework in Data Exchange Centers. *Sciences and Techniques of Information Management* 10 (1): 89-116. <https://doi.org/10.22091/stim.2022.7668.1700> [In Persian]
- Mumford, Deborah. 2022. Data colonialism: compelling and useful, but whither epistemes. *Information, Communication & Society* 25 (10): 1511-1516. <https://doi.org/10.1080/1369118X.2021.1986103>
- Naghshineh, Nader, Fatemeh Fahimnia, and Hamidreza Ahmadian. 2021. A framework for establishing a national data vault for Data Governance institution. *Journal of Information and Communication Technology* 57-84 : (49-50) 13 . <https://dori.net/dor/20.1001.1.27170411.1400.13.49.2.7> [In Persian]
- Oderkirk, Jillian. 2021. Survey results: National health data infrastructure and governance. *OECD Health Working Papers*. <https://doi.org/10.1787/55D24B5D-EN>
- Pohle, Julia, and Thorsten Thiel. 2020. Digital sovereignty. *Internet Policy Review* 9. <https://doi.org/10.14763/2020.4.1532>
- Rebro, Oleg, Anna Gladysheva, Maxim Suchkov, and Andrey Sushentsov. 2021. The Notion of "Digital Sovereignty" in Modern World Politics. *International Trends/Mezhdunarodnye protsessy*. <https://doi.org/10.17994/it.2021.19.4.67.6>
- Ricaurte, Paola. 2019. Data Epistemologies, The Coloniality of Power, and Resistance. *Television & New Media* 20: 350-365. <https://doi.org/10.1177/1527476419831640>
- Roberts, Jessica Saunders, and Luis Noel Montoya. 2022. Decolonisation, global data law, and indigenous data sovereignty. *arXiv*. <https://doi.org/10.48550/arXiv.2208.04700>
- Sadowski, Jathan. 2019. When data is capital: Datafication, accumulation, and extraction. *Big Data & Society* 6: 1-12. doi: 10.1177/2053951718820549
- Scholz, L. H. 2018. Big data is not big oil: the role of analogy in the law of new technologies. *Tennessee Law Review* 86: 863-884. <https://dx.doi.org/10.2139/ssrn.3252543>
- Shoker, Sarah. 2022. Digital Sovereignty Strategies for Every Nation. *ArXiv*. <https://doi.org/10.5604/01.3001.0016.0943>
- Singi, Kalapriya, Sukriti Choudhury, Vibhu Kaulgud, Roshni Bose, Sanjay Podder, and Alfred Burden. 2020. Data Sovereignty Governance Framework. *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*. <https://doi.org/10.1145/3387940.3392212>
- Statista. 2024. Big data market size revenue forecast worldwide from 2011 to 2027. <https://www.statista.com/statistics/254266/global-big-data-market-forecast/> (accessed Dec. 25, 2024)
- Subramani, R. 2023. Data Colonialism and Data Localization: Issues and Challenges. *Shanlax International Journal of Arts, Science and Humanities* 11 (2): 91-98. <https://doi.org/10.34293/sijash.v11i2.6657>
- Thatcher, Jim, David O'Sullivan, and Dillon Mahmoudi. 2016. Data colonialism through accumulation by dispossession: New metaphors for daily data. *Environment and Planning D: Society and Space* 34 (6): 990-1006. <https://doi.org/10.1177/0263775816633195>

- Toliupa, Serhii, Anatolii Shevchenko, Serhii Buchyk, Ihor Pampukha, and Andrii Kulko. 2023. Managing the security of the critical infrastructure information network. In V. Sokolov, T. Radivilova, V. Ustimenko, & M. Nazarkevych (Eds.), *Proceedings of the Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II 2023)*: 131-142
- Vardanyan, Liana, and Heghine Kocharyan. 2022. Critical views on the phenomenon of EU digital sovereignty through the prism of global data governance reality: main obstacles and challenges. *European Studies* 9: 110-132. <https://doi.org/10.2478/eustu-2022-0016>
- Verständig, Dan. 2021. Critical data studies and data science in higher education. *Seminar.net* 173). <https://doi.org/10.7577/seminar.4397>
- Wang, Yajie, Ruiheng Fan, Xingcheng Liang, Peng Li, and Xinxin Hei. 2022. Trusted Data Storage Architecture for National Infrastructure. *Sensors (Basel, Switzerland)* 22. <https://doi.org/10.3390/s22062318>
- Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology* 30 (1): 75–89. <https://doi.org/10.1057/jit.2015.5>

مهدیه لطیف‌زاده

متولد سال ۱۳۷۱، دکتری حقوق خصوصی از دانشگاه فردوسی مشهد است. ایشان هم‌اکنون استادیار حقوق خصوصی گروه پژوهشی فقه و حقوق اسلامی دانشگاه فردوسی مشهد است.

حقوق فناوری به‌ویژه حکمرانی داده و تنظیم‌گری هوش مصنوعی با تمرکز بر مطالعه تطبیقی نظام حقوقی اتحادیه اروپا و ایران از جمله علایق پژوهشی و حوزه‌های تخصصی مطالعاتی وی به‌شمار می‌رود.



پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

پژوهش نامه
پژدازش و
مدیریت
اطلاعات

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی