



Designing a Framework for Determining the Role of Data Governance in Mitigating Cognitive Threats

Mohammad-Sadegh Zoughi

Ph.D. Candidate, University of Tehran, Tehran, Iran.

Ali Alizadeh

Assistant Professor, Supreme National Defense University, Tehran, Iran.

Abstract

In an era of rapid digital transformation, cognitive threats have emerged as one of the most serious challenges to security, society, and governance. By leveraging vast amounts of data, advanced algorithms, and communication infrastructures, such threats can influence collective awareness, judgment, and behavior, thereby undermining the foundations of legitimacy and public trust. Against this backdrop, the role of data governance as a strategic safeguard for managing such threats has become increasingly salient. Accordingly, data-driven governance and the development of advanced legal and regulatory policies constitute an indispensable requirement for any intelligent governance system. This study is an applied developmental research project aimed at integrating theoretical foundations and abstract concepts with practical and strategic requirements in the domains of data governance and cognitive threat mitigation. A descriptive-analytical research design was adopted. In the first stage, a library-based research method was employed to examine authoritative sources in the fields of data governance, algorithmic control, and international law, from which relevant concepts were identified and extracted. Based on these findings, an initial conceptual framework was developed to analyze the relationship between data governance and cognitive threats. Subsequently, to assess the validity and credibility of the proposed conceptual framework, semi-structured interviews were conducted with three groups of experts, comprising specialists in data law, cognitive sciences, and digital governance. Qualitative content analysis of the interview responses played a significant role in strengthening and refining the theoretical framework of the study. Thus, while maintaining methodological coherence, the research process established a purposeful linkage between the theoretical approach and the empirical field. The findings indicate that an appropriate framework for determining the role of data governance in mitigating cognitive threats is a three-layer, cyclical framework. This framework is formed through the integration of legal governance of cognitive data, risk-based regulation of algorithms that influence perception, and macro-level big data policymaking aimed at enhancing cognitive resilience. The proposed framework underscores the need for an integrated governance architecture in which legal, regulatory, and strategic policy instruments operate in a continuous and mutually reinforcing cycle to mitigate cognitive threats.

Keywords: Data Governance; Cognitive Threats; Data Ownership; Algorithmic Control; Big Data Policies; Intelligent Governance; Cognitive Security; Data Law; Algorithmic Transparency; Technological Accountability.



طراحی الگویی برای تعیین نقش حاکمیت داده در مهار تهدیدهای شناختی

محمدصادق ذوقی

دانشجوی دکتری دانشگاه تهران، تهران، ایران

Email: mszoghi@gmail.com

علی علیزاده

استادیار دانشگاه عالی دفاع ملی، تهران، ایران

چکیده

در عصر تحولات پرشتاب فناوری‌های دیجیتال، تهدیدهای شناختی به یکی از جدی‌ترین چالش‌های امنیتی، اجتماعی و حکمرانی تبدیل شده‌اند؛ تهدیدهایی که با استفاده از داده‌های گسترده، الگوریتم‌های پیشرفته و زیرساخت‌های ارتباطی، قادرند بر آگاهی، قضاوت و رفتار جمعی اثرگذار شوند و بنیان‌های مشروعیت و اعتماد عمومی را به خطر اندازند. در این میان، نقش حاکمیت داده به‌عنوان سپری راهبردی برای مدیریت این تهدیدهای برجسته می‌شود، به‌گونه‌ای که حکمرانی داده‌محور و طراحی سیاست‌های حقوقی پیشرفته، ضرورت انکارناپذیر هر نظام حکمرانی هوشمند محسوب می‌شود. این پژوهش از نوع تحقیق توسعه‌ای کاربردی است که با هدف تلفیق مبانی نظری و مفاهیم انتزاعی با نیازهای عملی و راهبردی در حوزه حکمرانی داده و مهار تهدیدهای شناختی انجام گرفته است؛ روش تحقیق اتخاذ شده در این مطالعه توصیفی-تحلیلی بوده، به‌گونه‌ای که در مرحله نخست با بهره‌گیری از روش کتابخانه‌ای، منابع معتبر در حوزه‌های مرتبط با حاکمیت داده، کنترل الگوریتمی و حقوق بین‌الملل مورد بررسی و استخراج مفاهیم قرار گرفت و براساس آن، یک الگوی مفهومی اولیه برای تحلیل ارتباط میان حاکمیت داده و تهدیدهای شناختی تدوین شد، سپس برای ارزیابی روایی و سنجش اعتبار این الگوی مفهومی، مصاحبه‌های نیمه‌ساختاریافته‌ای با سه گروه از خبرگان شامل متخصصان حقوق داده، علوم شناختی و حکمرانی دیجیتال انجام شد که تحلیل محتوای کیفی پاسخ‌های آن‌ها نقش مهمی در تقویت و اصلاح چهارچوب نظری تحقیق ایفا کرد، به‌گونه‌ای که فرایند تحقیق ضمن حفظ انسجام روش‌شناختی، از پیوندی هدفمند میان رویکرد نظری و میدان تجربی برخوردار گردید. نتایج پژوهش نشان می‌دهد الگوی مناسب برای تعیین نقش حاکمیت داده در مهار تهدیدهای شناختی، الگویی سه‌لایه و چرخه‌ای است که از پیوند میان حاکمیت حقوقی بر داده‌های شناختی، تنظیم‌گری ریسک‌محور الگوریتم‌های اثرگذار بر ادراک و سیاست‌گذاری کلان‌داده‌ای برای تاب‌آوری شناختی شکل می‌گیرد.

کلیدواژه‌ها: حاکمیت داده، تهدیدهای شناختی، مالکیت داده، کنترل الگوریتمی، سیاست‌های کلان‌داده‌ای، حکمرانی هوشمند، امنیت شناختی، حقوق داده، شفافیت الگوریتمی، پاسخ‌گویی فناوریانه.

مقدمه

در دوران معاصر، مفهوم «جنگ شناختی»^۱، از یک مقوله به تنهایی مفهومی و نظری خارج شده و به یکی از حیاتی‌ترین، پیچیده‌ترین و درعین‌حال خطرناک‌ترین شکل‌های تقابل قدرت در عصر دیجیتال بدل شده است. این پدیده نه تنها با تغییر در محیط تهدید، بلکه با تحول در ساختار ذهن و ادراک انسان همراه است و بنابراین از جنگ نرم، «جنگ اطلاعاتی»^۲ و «عملیات روانی»^۳ متمایز می‌گردد. درحالی‌که جنگ نرم بیشتر به تغییر ذائقه فرهنگی و ساختار ارزش‌های اجتماعی توجه دارد و عملیات روانی بیشتر بر تحریک احساسات و بهره‌برداری از هیجانات جمعی تمرکز می‌کند، جنگ شناختی در لایه‌های عمیق‌تری از ذهن انسان نفوذ می‌کند و به تغییرهای پایدار در ادراک، شناخت و حتی هویت فرد می‌انجامد. در این الگوی جدید از تقابل، دیگر لازم نیست که قدرت مهاجم به تسلیحات فیزیکی یا حتی بمباران تبلیغاتی متوسل شود، بلکه کافی است که به وسیله مجموعه‌ای هوشمند از داده‌ها، الگوریتم‌ها و معماری‌های اطلاعاتی، مخاطب را به گونه‌ای شکل دهد که اول آن که خود از تغییر آگاه نباشد، دوم آن که تغییر را براساس اراده خود تلقی کند و سوم آن که در برابر هرگونه بازنگری مقاومت نشان دهد (Rosati, 2007: 1665).

باید توجه داشت که داده در این اکوسیستم نه تنها به عنوان منبعی برای تحلیل اطلاعات و هدایت تصمیم‌سازی مورد استفاده قرار می‌گیرد، بلکه خود به «زیرساخت ادراک» تبدیل شده است. درواقع، داده‌ها امروزه مانند مصالح خامی هستند که معماری ذهن انسان‌ها را بازسازی می‌کنند و به واسطه الگوریتم‌هایی ذهن افراد را در مسیرهای خاصی هدایت می‌کنند. این نقش بنیادین داده به ما نشان می‌دهد که در دوران جدید، عملیات شناختی از پایه بدون اشراف بر زیرساخت داده‌ای نه قابل طراحی است و نه قابل اجرا، چراکه کنشگر شناختی برای اعمال اراده خود بر ذهن مخاطب، نخست باید به آن دسترسی، احاطه و کنترل بر داده‌هایی داشته باشد که ذهن او را تغذیه می‌کنند.

-
1. Cognitive Warfare
 2. Information Warfare
 3. Psychological Operations



از همین رو، می توان ادعا کرد که کنترل بر داده ها، به ویژه داده های رفتاری و تجربی، معادل با کنترل بر آگاهی و ادراک فرد است (Linden et al., 2003: 78). براساس پژوهش های انجام شده در زمینه توانمندسازی ساختارهای ملی در برابر تهدیدهای شناختی، علوم و فناوری های شناختی می توانند از طریق تقویت عملکرد ذهن، ایجاد انعطاف پذیری شناختی، به کارگیری هوش مصنوعی و توسعه سامانه های شناختی دفاعی، به شکل گیری یک ساختار مقاوم در برابر عملیات ادراکی کمک کنند. به ویژه استفاده از تحلیل سریع و هوشمند داده های کلان می تواند در پیش بینی تهدیدهای نوپدید، شناسایی رفتارهای دشمن و مدیریت مخاطرات امنیتی نقش اساسی ایفا نماید (اسماعیلی و میارعباسی، ۱۴۰۳: ۴۴).

در عصر سلطه فناوری های هوش مصنوعی، یادگیری ماشین و تحلیل کلان داده ها، شکل بندی جدیدی از تهدیدهای علیه جوامع انسانی پدید آمده است که در سطوح عمیق تری از امنیت ملی، حاکمیت اجتماعی و استقلال روانی عمل می کند؛ تهدیدهایی که برخلاف تهدیدهای سنتی، نه با توسل به قدرت نظامی، اقتصادی یا حتی تبلیغاتی آشکار، بلکه از طریق نفوذ تدریجی، هدفمند و نظام مند در ساختارهای شناختی و فرایندهای تصمیم سازی ذهنی افراد و گروه ها اعمال می گردد. این دسته از تهدیدهای که در عنوان «تهدیدهای شناختی» طبقه بندی می شوند، از توانایی ترکیبی فناوری های داده محور، معماری های الگوریتمی و سیستم های هوشمند بهره می گیرند تا روایت ها، ادراک های، نظام های ارزشی و گرایش های تصمیم گیری عمومی را به گونه ای نامرئی، اما مؤثر، تغییر دهند. در چنین بستری، دیگر مفهوم امنیت به معنای کلاسیک آن پاسخگوی نیازهای یک جامعه دیجیتال زیست نیست؛ بلکه لازم است از مفهومی نوین با عنوان «امنیت شناختی» سخن گفته شود که ناظر به مصون سازی جوامع در برابر انواع مداخله های غیرمستقیم بر حیطه ادراک و ذهنیت جمعی است.

داده به عنوان ماده هرگونه پردازش ادراکی و شناختی، در قلب این سازوکار پیچیده جای دارد. اگر در گذشته، قدرت با کنترل منابع فیزیکی و زیرساخت های نظامی تعریف می شد، در دوران حاضر قدرت در گرو کنترل داده، مهندسی الگوریتم و تسلط بر فرایندهای

تولید، توزیع و تحلیل اطلاعات قرار گرفته است. این تحول اساسی، مرز میان سیاست، امنیت، فناوری و حقوق را به شدت مخدوش کرده و نظام‌های حقوقی کلاسیک را با چالش‌هایی مواجه ساخته است که از جنبه مفهومی، ساختاری و نهادی، نیازمند بازنگری و نوسازی عمیق‌اند. به عنوان نمونه، در حوزه مالکیت داده، هنوز اجماع مشخصی در سطح حقوق بین‌الملل عمومی و نظام‌های داخلی وجود ندارد که بتواند پاسخ روشنی به پرسش‌هایی از قبیل «مالک واقعی داده‌های رفتاری، زیستی یا شناختی کیست؟»، «آیا الگوریتم‌های تحلیل‌گر باید نسبت به تصمیم‌های شناختی تولیدشده پاسخ‌گو باشند؟» یا «آیا مداخله در ادراک عمومی بدون رضایت، مصداق نقض کرامت ذهنی است؟» ارائه دهد. این ابهامات نه تنها شکاف‌های حقوقی، بلکه خلأهای جدی در سیاست‌گذاری، تنظیم‌گری و حکمرانی نیز ایجاد کرده‌اند. جمع‌بندی بیان مسئله نشان می‌دهد که مشکل اصلی در مواجهه با تهدیدهای شناختی، فقدان یک چهارچوب منسجم و قابل اجرا برای حاکمیت داده است که بتواند هم‌زمان مالکیت و کاربری داده‌های رفتاری و شناختی را تعیین کند، بر عملکرد الگوریتم‌های اثرگذار بر ادراک عمومی نظارت حقوقی و نهادی اعمال کند، سیاست‌گذاری کلان داده‌ای را با ملاحظات امنیت شناختی هم‌راستا سازد. در وضعیت موجود، پراکندگی مقررات، ابهام در مسئولیت‌پذیری بازیگران داده‌محور، نبود سازوکارهای ممیزی و شفاف‌سازی الگوریتمی، موجب می‌شود مداخله‌های نامرئی در ذهنیت جمعی بدون ابزار بازخواست و جبران مؤثر تداوم یابد و مرزهای امنیت ملی و حاکمیت اجتماعی در سطح ادراک تضعیف شود. این تحقیق برای حل این خلأ، با تلفیق ادبیات نظری و تحلیل اسنادی با داده‌های کیفی حاصل از مصاحبه خبرگان، الگویی سه لایه ارائه می‌کند که در آن حدود حقوقی مالکیت داده تا سطح داده‌های شناختی روشن می‌شود، الزامات تنظیم‌گری و پاسخ‌گویی الگوریتمی به صورت ریسک محور صورت بندی می‌گردد، سیاست‌های کلان داده‌ای مبتنی بر شفافیت و حق کنترل سرنوشت داده‌ای طراحی می‌شود. پیامد این رویکرد، تبدیل مسئله از سطح توصیف تهدید به سطح ارائه راه‌حل سیاستی و حقوقی است، به گونه‌ای که دستگاه حکمرانی بتواند با معیارهای روشن، نهادهای متولی و ابزارهای نظارتی مشخص، تهدیدهای شناختی را مهار و امنیت ادراکی را تقویت



کند.

اهمیت این تحقیق در آن است که شکاف میان ادبیات نظری حاکمیت داده و واقعیت عملی تهدیدهای شناختی را در سطح یک چهارچوب حقوقی و سیاستی منسجم پر می‌کند؛ به این معنا که پژوهش حاضر به جای توصیف کلی تهدیدها یا تکرار ادبیات موجود، مستقیماً بر طراحی الگو برای پیوند میان مالکیت داده، کنترل الگوریتمی و امنیت شناختی متمرکز است و تلاش دارد نشان دهد چگونه می‌توان این سه حوزه را در قالب یک معماری حکمرانی داده‌محور قابل اجرا صورت بندی کرد.

۱. در صورت انجام این پژوهش نخستین پیامد آن فراهم شدن مبنای مفهومی و عملی برای تعریف «رابطه ساختاری میان حاکمیت داده و امنیت شناختی» است؛ در نتیجه نهادهای سیاست‌گذار می‌توانند به جای مواجهه موردی و واکنشی، از الگوی ارائه شده برای شناسایی حوزه‌های پُریسک، تعریف انواع داده با حساسیت بالا و تعیین جایگاه هر یک در منظومه امنیت ادراکی بهره ببرند؛ در صورت فقدان این تحقیق وضعیت کنونی تداوم می‌یابد که در آن حاکمیت داده بیشتر در سطح شعار و کلی گویی باقی می‌ماند و نسبت آن با تهدیدهای شناختی در سطح سیاست‌گذاری ملی روشن و قابل استناد نیست.

۲. پیامد مثبت دیگر انجام پژوهش حاضر، تولید چهارچوبی عملی برای تنظیم حقوقی مالکیت داده تا سطح داده‌های شناختی است؛ الگوی پیشنهادی تحقیق با تفکیک انواع داده و تعیین حقوق و تکالیف بازیگران، امکان طراحی مقررات مشخص درباره دسترسی، پردازش و توقف پردازش داده‌های ادراکی را فراهم می‌کند و به این ترتیب از یک‌سو از سوءاستفاده ساختاری سکوها نسبت به داده‌های ذهنی شهروندان جلوگیری می‌شود و از سوی دیگر ابزار حقوقی لازم برای صیانت از حاکمیت ادراکی فرد فراهم می‌گردد؛ در صورت انجام نشدن چنین پژوهشی، ابهام در حدود مالکیت داده‌های رفتاری و شناختی ادامه خواهد یافت و تعارض میان منافع اقتصادی سکوها، الزامات امنیتی و حقوق اساسی افراد بدون چهارچوب روشمند حل و فصل می‌شود.

۳. این تحقیق با طراحی سازوکارهای مشخص برای ممیزی و پاسخ‌گویی الگوریتم‌های اثرگذار بر ادراک عمومی، زمینه‌گذار از وضعیت «جعبه سیاه الگوریتمی» به وضعیت «الگوریتم شفاف و قابل حسابرسی» را فراهم می‌سازد؛ پیامد مثبت این امر برای نظام حکمرانی، امکان الزام ارائه دهندگان خدمات داده‌محور به ثبت مشخصات الگوریتم، انجام ارزیابی اثر ادراکی، پذیرش نظارت مستقل و پاسخ‌گویی در برابر آسیب‌های شناختی است، درحالی‌که در صورت فقدان چنین چهارچوبی الگوریتم‌ها همچنان به‌منزله کنشگرانی پنهان عمل می‌کنند، امکان انتساب مسئولیت حقوقی در برابر آثار ادراکی آن‌ها محدود می‌ماند و تهدیدهای شناختی در لایه‌ای نامرئی از ساختار تصمیم‌سازی عمومی بازتولید می‌شود.

۴. انجام پژوهش حاضر از منظر سیاست‌گذاری عمومی این مزیت را دارد که شاخص‌ها و محورهای لازم برای طراحی سیاست‌های داده‌محور با رویکرد شناختی را ارائه می‌کند؛ به این ترتیب دستگاه‌های مسئول می‌توانند برنامه‌های ارتقای سواد داده‌ای و سواد ادراکی، مقررات حکمرانی دیجیتال و راهبردهای امنیتی را بر پایه درک یکپارچه از داده، الگوریتم و ذهنیت جمعی تنظیم کنند؛ در نبود این تحقیق، سیاست‌گذاری در حوزه فضای مجازی و داده عمدتاً بر ابعاد فناورانه یا امنیتی سستی متمرکز خواهد ماند و اثرات عمیق داده و الگوریتم بر ساختار ادراک، هویت و تصمیم‌گیری جمعی تا حد زیادی نادیده گرفته می‌شود.

۵. از منظر نهادی، نتایج این پژوهش می‌تواند مبنایی برای طراحی نهاد تخصصی تنظیم‌گر الگوریتم‌های شناختی و تعیین حدود اختیارات، ابزارهای نظارتی و نسبت آن با سایر نهادهای حکمرانی دیجیتال باشد؛ استقرار چنین نهادی بر پایه الگوی ارائه شده در تحقیق، امکان اعمال نظارت پیشینی و پسینی بر سامانه‌های پُرسک، صدور مجوز زمان دار، تعلیق الگوریتم‌های آسیب‌زا و تدوین استانداردهای ملی شفافیت و ممیزی را فراهم می‌کند؛ در صورت فقدان این تحقیق، بحث نهاد تنظیم‌گر در سطح کلیات باقی می‌ماند، مرز مسئولیت میان نهادهای مختلف روشن نمی‌شود و خلأ نظارتی در حوزه



امنیت شناختی تداوم خواهد یافت.

۶. پژوهش حاضر با ارائه راهبردهای اجرایی برای تاب‌آوری شناختی جامعه، پیامدهای مثبتی در سطح توانمندسازی شهروندان و نخبگان دارد؛ الگوهای پیشنهادی برای آموزش‌های تخصصی، ارتقای سواد ادراکی، طراحی برنامه‌های حمایتی از گروه‌های حساس و استفاده هوشمندانه از داده‌ها برای تقویت روایت‌های ملی، به سیاست‌گذاران اجازه می‌دهد به‌جای تمرکز یک‌سویه بر محدودسازی، ترکیبی از اقدامات پیشگیرانه، توانمندساز و بازدارنده را به‌کار گیرند؛ در غیر این صورت، تهدیدهای شناختی عمده‌تاً با رویکردهای سلبی و مسدودساز مدیریت می‌شود، سرمایه اجتماعی و اعتماد عمومی تضعیف می‌گردد و جامعه بدون ابزارهای لازم برای تشخیص و مقاومت ادراکی در معرض شکل‌گیری خزنده روایت‌های تحمیلی قرار می‌گیرد.

۷. در نهایت، انجام این تحقیق از منظر توسعه دانش میان‌رشته‌ای نیز واجد ضرورت است، زیرا مدل ارائه شده می‌تواند مبنای مطالعات تکمیلی کمی و کیفی در حوزه سنجش تاب‌آوری ادراکی، ارزیابی اثربخشی سیاست‌های حاکمیت داده و طراحی شاخص‌های ملی امنیت شناختی قرار گیرد؛ در صورت عدم انجام آن، پژوهش‌های آتی ناچار خواهند بود بدون بهره‌گیری از یک چهارچوب مفهومی یکپارچه و بومی در این حوزه حرکت کنند و روند تولید دانش در تقاطع حقوق داده، علوم شناختی و حکمرانی هوشمند به‌صورت پراکنده و ناهمگون ادامه خواهد یافت.

سؤال‌های پژوهش

سؤال اصلی

الگوی مناسب برای تعیین نقش حاکمیت داده در مهار تهدیدهای شناختی در بستر حکمرانی هوشمند کدام است؟

سؤال‌های فرعی

♦ حدود و اصول حقوقی مالکیت داده در مواجهه با تهدیدهای ادراکی چگونه باید

تعریف و تنظیم شود تا از حاکمیت ذهنی افراد در برابر دستکاری شناختی محافظت

کند؟

- ❖ چه سازوکارهای حقوقی و نظارتی برای کنترل، شفاف‌سازی و پاسخ‌گویی الگوریتم‌های شناختی در فرایندهای تصمیم‌سازی داده‌محور قابل طراحی است؟
- ❖ چگونه می‌توان از طریق سیاست‌گذاری داده‌محور، بین امنیت شناختی، حاکمیت داده و حقوق ادراکی تعادل برقرار کرد؟

هدف‌های پژوهش

هدف اصلی

طراحی الگو و چهارچوبی حقوقی و سیاست‌گذارانه برای استقرار حاکمیت داده با هدف مهار تهدیدهای شناختی و تقویت امنیت ادراکی در بستر حکمرانی هوشمند.

هدف‌های فرعی

- ❖ بازشناسی و تبیین مبانی و حدود و اصول حقوقی مالکیت داده در تقاطع با حق حاکمیت ادراکی و تحدید تهدیدهای شناختی در فضای دیجیتال.
- ❖ ارائه سازوکارهای دقیق برای تنظیم‌گری الگوریتم‌های شناختی با تأکید بر شفافیت، ممیزی و مسئولیت‌پذیری در سطوح حکمرانی.
- ❖ الگویی برای سیاست‌گذاری داده‌محور جهت ارتقای تاب‌آوری شناختی و تضمین تعادل میان آزادی داده، امنیت ذهنی و منافع حاکمیتی.

۱. پیشینه پژوهش

پایان‌نامه دکتری محمدرضا مرتضوی (۱۳۹۴)، با عنوان طراحی چهارچوب حاکمیت داده در مراکز تبادل داده و اطلاعات ملی، مانند یکی از پیشگام‌ترین مطالعات داخلی در حوزه سیاست‌گذاری داده‌ها محسوب می‌شود.

پژوهش امیرحسین صدیقی (۱۳۹۶)، با عنوان ارائه رویکردی برای ارزیابی حکمرانی داده در کسب‌وکارها، تمرکز خود را بر ایجاد الگوی برای سنجش میزان بلوغ حکمرانی داده در



سازمان‌های اقتصادی گذاشته است.

در مقاله‌ای که توسط فتح اله زاده و همکاران (۱۳۹۶) با عنوان مروری بر الگوهای بلوغ حکمرانی داده‌ها، در بنگاه‌های اقتصادی در پنجمین همایش مدیران فناوری اطلاعات ارائه شده، تمرکز بر مروری بر الگوهای بلوغ حکمرانی داده در بنگاه‌های اقتصادی است و این مرور سعی دارد الگوهای موجود در فضای بین‌المللی همچون الگوی DGI و COBIT را به زمینه‌های بومی ایران تطبیق دهد.

مقاله علیرضا لگزائی و همکاران (۱۳۹۷)، با عنوان چهارچوبی جهت پیاده‌سازی حاکمیت داده در صنعت بانکداری ایران، با تمرکز بر طراحی سازوکارهای عملیاتی و اجرایی برای استقرار نظام حکمرانی داده در ساختار بانکی کشور، بیشتر به نیازمندی‌های فنی، زیرساختی و فرایندی بانک‌ها در مدیریت داده‌های مالی و مشتریان می‌پردازد.

در مقاله الگوریتم‌های داده‌کاوی در پایگاه داده (۱۳۹۸) که توسط سارا رجبی در قالب یک پژوهش فنی در حیطه علوم کامپیوتر در دانشگاه شهید بهشتی ارائه شده است، تمرکز اصلی بر بررسی الگوریتم‌های استخراج دانش از پایگاه‌های داده و کاربرد آن‌ها در بهبود فرایندهای تحلیلی و تصمیم‌سازی مبتنی بر داده است.

۲. مبانی نظری پژوهش

۲-۱. «حاکمیت داده»^۱

در نظام‌های حقوقی نوین، حاکمیت داده به‌مانند مفهومی چندبُعدی، بیانگر صلاحیت قانونی، فنی و حاکمیتی یک دولت در اعمال اقتدار مؤثر بر چرخه جمع‌آوری، پردازش، کنترل، انتقال و تنظیم داده‌ها در محدوده صلاحیت سرزمینی یا سایبری آن است. این مفهوم، ناظر بر تلاقی میان حق حاکمیت ملی و معماری دیجیتال است و به‌صورت مستقیم در برابر سلطه فراسرزمینی سکوها بزرگ داده‌محور قرار می‌گیرد. حاکمیت داده، نه‌تنها جنبه‌ای از استقلال راهبردی در زیست‌بوم دیجیتال است، بلکه پایه‌ای برای دفاع شناختی و حفظ تمامیت

1. Data Sovereignty

تصمیم‌سازی ملی در برابر الگوریتم‌های بی‌مرز تلقی می‌شود (Taylor 2017: 6).

۲-۲. «تهدیدهای شناختی»^۱

تهدید شناختی، به‌عنوان گونه‌ای از مخاطرات راهبردی غیرمرئی، حاصل بهره‌برداری نظام‌مند از کلان‌داده‌ها، تحلیل الگوریتمی و الگوسازی پیش‌بینی‌گر برای نفوذ و تأثیرگذاری در حوزه‌های ادراک، حافظه، قضاوت و هویت جمعی است. این تهدیدهای، برخلاف حملات سایبری مرسوم که زیرساخت‌های فنی را هدف می‌گیرند، به‌صورت مستقیم فرایندهای تصمیم‌سازی ذهنی را مورد تهاجم قرار می‌دهند و با ایجاد تغییر در بنیان‌های شناختی، فضای افکار عمومی را مهندسی می‌کنند. در چهارچوب حقوقی، تهدیدهای شناختی در سطحی فراتر از امنیت اطلاعات، به مقوله‌ای مرتبط با کرامت شناختی، آزادی فکری و حق حاکمیت ادراکی بدل شده‌اند (Bousquet et al. 2021: 431).

۳-۲. «حکمرانی الگوریتمی»^۲ و الزام‌های حقوقی آن

الگوی حکمرانی الگوریتمی که بر مبنای تعامل میان کلان‌داده، هوش مصنوعی و سامانه‌های تصمیم‌یار دیجیتال توسعه‌یافته، موجب بازتعریف بنیادهای سنتی اداره عمومی و حقوق عمومی شده است. در این الگو، فرایند سیاست‌گذاری به‌جای نهاد انسانی، از سوی الگوریتم‌ها و سازوکارهای یادگیرنده اجرا می‌شود که این امر چالش‌هایی جدی در حوزه شفافیت، عدالت داده‌ای و مسئولیت‌پذیری حقوقی ایجاد می‌کند. در غیاب سازوکارهای نظارتی و قواعد شفافیت الگوریتمی، خطر تبدیل حکمرانی هوشمند به ساختاری مستتر و تبعیض‌آفرین افزایش می‌یابد؛ بنابراین، حاکمیت داده‌محور نیازمند نهادینه‌سازی اصولی چون حق دانستن، مسئولیت‌پذیری تصمیم‌های ماشینی و امکان بازخواست از ساختارهای غیرانسانی است (Zuboff 2019: 181).

1. Cognitive Threats

2. Algorithmic Governance



۲-۴. حکمرانی هوشمند

حکمرانی هوشمند، الگویی نوین از اداره عمومی است که در آن فناوری‌های دیجیتال، داده‌های کلان، سامانه‌های هوش مصنوعی و سازوکارهای مشارکتی برای ارتقای کیفیت تصمیم‌گیری، افزایش شفافیت، پاسخ‌گویی، کارآمدی و انعطاف‌پذیری نهادی به کار گرفته می‌شوند. در این معنا، حکمرانی هوشمند تنها به معنای الکترونیکی کردن خدمات عمومی یا استفاده فنی از ابزارهای دیجیتال نیست، بلکه بیانگر بازآرایی رابطه دولت، شهروندان، داده‌ها و نهادهای تصمیم‌گیر در یک محیط داده‌محور و شبکه‌ای است. به همین دلیل، برخی نویسندگان حکمرانی هوشمند را نوعی همکاری انسانی و نهادی می‌دانند که با اتکا به فناوری‌های اطلاعات و ارتباطات، امکان دستیابی به نتایج بهتر و فرایندهای بازتر حکمرانی را فراهم می‌سازد (Meijer & Bolívar, 2016: 392).

در چهارچوب پژوهش حاضر، حکمرانی هوشمند بستری است که در آن حاکمیت داده، تنظیم‌گری الگوریتمی و سیاست‌گذاری کلان‌داده‌ای به یکدیگر پیوند می‌خورند. این نوع حکمرانی زمانی کارآمد خواهد بود که هوشمندی آن تنها در سرعت پردازش داده یا خودکارسازی تصمیم‌ها خلاصه نشود، بلکه بتواند هم‌زمان اصول شفافیت، عدالت داده‌ای، پاسخ‌گویی فناورانه، مشارکت عمومی و تاب‌آوری نهادی را نیز تضمین کند.

از این منظر، حکمرانی هوشمند با امنیت شناختی ارتباط مستقیم پیدا می‌کند؛ زیرا هرچه تصمیم‌گیری عمومی بیشتر به داده‌ها و الگوریتم‌ها وابسته شود، امکان اثرگذاری بر ادراک عمومی، جهت‌دهی به روایت‌ها و دست‌کاری شناختی نیز افزایش می‌یابد؛ بنابراین، در این پژوهش، حکمرانی هوشمند به عنوان بستر نهادی و فناورانه‌ای در نظر گرفته می‌شود که در آن الگوی حاکمیت داده باید بتواند میان بهره‌برداری از داده، کنترل الگوریتمی، حقوق ادراکی شهروندان و امنیت شناختی تعادل برقرار کند (Gil-Garcia et al., 2016: 524).

۳. روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف، توسعه‌ای-کاربردی و از نظر روش، کیفی با رویکرد توصیفی-تحلیلی و تحلیل مضمون انجام شده است. این انتخاب به آن جهت صورت گرفته است که پدیده مورد بررسی- یعنی نسبت میان حاکمیت داده، مالکیت داده، کنترل الگوریتمی و سیاست‌گذاری کلان‌داده‌ای با سطح تاب‌آوری شناختی- ماهیتی پیچیده، چندبُعدی و میان‌رشته‌ای دارد و در نتیجه برای تحلیل آن به‌تنهایی اتکای به روش‌های کمی یا تک‌بُعدی کفایت نمی‌کند. ترکیب روش توصیفی-تحلیلی با تحلیل محتوای کیفی و مصاحبه‌های نیمه‌ساختاریافته، این امکان را فراهم می‌سازد که هم از نظر مفهومی نظری و هم از نظر تجربی کاربردی، چهارچوبی جامع و منسجم تدوین گردد.

قلمرو پژوهش در سه بُعد موضوعی، زمانی و سازمانی تعریف شده است. قلمرو موضوعی تحقیق بر حاکمیت داده و نقش آن در مهار تهدیدهای شناختی با تمرکز بر سه مؤلفه اصلی مالکیت داده، کنترل الگوریتمی و سیاست‌های کلان‌داده‌ای است. قلمرو زمانی پژوهش سال‌های ۱۳۹۸ تا ۱۴۰۳ را در برمی‌گیرد، چراکه عمده تحولات و مقررات‌گذاری‌های ملی و بین‌المللی در حوزه داده و حکمرانی دیجیتال در این بازه رخ داده است و تحلیل آن می‌تواند نمایانگر وضعیت موجود و روندهای نوپدید باشد. قلمرو سازمانی نیز ناظر بر جمهوری اسلامی ایران است، با تأکید بر نهادهای متولی حکمرانی دیجیتال همچون شورای عالی فضای مجازی، وزارت ارتباطات و فناوری اطلاعات و مراکز پژوهشی و سیاست‌گذاری در عرصه حقوق فناوری؛ درعین‌حال برای مقایسه و غنا بخشی، اسناد و چهارچوب‌های بین‌المللی اتحادیه اروپا، سازمان ملل و سایر رژیم‌های حقوقی نیز مورد توجه قرار گرفته‌اند. جامعه آماری پژوهش شامل خبرگان و متخصصانی است که در سه حوزه اصلی پژوهش یعنی حقوق داده و حریم خصوصی، علوم شناختی و امنیت ادراکی و حکمرانی دیجیتال و سیاست‌گذاری داده دارای سابقه علمی یا اجرایی‌اند. این افراد به‌عنوان دارندگان تجربه عمیق و دانش تخصصی، بهترین منبع برای واکاوی ابعاد نظری و عملی مسئله محسوب می‌شوند.



جدول ۱: نمایه شرکت‌کنندگان مصاحبه

شناسه	حوزه تخصصی	نقش-مرتبه	سازمان-بخش	سابقه (سال)	جنسیت
E01	حقوق داده	استادیار	دانشگاه	۱۲	مرد
E02	حقوق داده	دانشیار	دانشگاه	۱۸	زن
E03	حقوق داده	پژوهشگر	پژوهشکده	۱۰	مرد
E04	حقوق داده	استادیار	دانشگاه	۱۴	مرد
E05	حقوق داده	دانشیار	دانشگاه	۲۰	مرد
E06	حقوق داده	استادیار	دانشگاه	۱۱	زن
E07	علوم شناختی	پژوهشگر	مرکز شناخت	۱۳	زن
E08	علوم شناختی	روان‌شناس ادراکی	بیمارستان/آزمایشگاه	۱۵	مرد
E09	علوم شناختی	پژوهشگر	پژوهشگاه	۱۰	مرد
E10	علوم شناختی	پژوهشگر ارشد	آزمایشگاه صنعتی	۱۶	مرد
E11	علوم شناختی	پژوهشگر	دانشگاه	۱۲	زن
E12	حکمرانی دیجیتال	مشاور ارشد سیاسی	نهاد تنظیم‌گر	۲۲	مرد
E13	حکمرانی دیجیتال	تنظیم‌گر	رگولاتوری	۲۵	مرد
E14	حکمرانی دیجیتال	مدیر	وزارتخانه	۱۷	زن
E15	حکمرانی دیجیتال	تحلیلگر	مرکز ملی	۱۰	مرد

ویژگی‌ها و تعداد اعضای نمونه به‌گونه‌ای تعیین شده است که تنوع رشته‌ای و حرفه‌ای در جامعه خبرگان پوشش داده شود. در مجموع ۱۵ نفر به‌عنوان نمونه پژوهش انتخاب شده‌اند که ترکیب آن‌ها شامل ۶ نفر استاد دانشگاه در حوزه‌های حقوق فناوری و حقوق بین‌الملل، ۵ نفر پژوهشگر و متخصص در علوم شناختی و روان‌شناسی ادراکی و ۴ نفر کارشناس ارشد اجرایی در نهادهای سیاست‌گذار و تنظیم‌گر حوزه حکمرانی دیجیتال است. علت انتخاب ۱۵ نفر فوق، تأمین تنوع رشته‌ای و حرفه‌ای کافی در نمونه تحقیق است. این افراد از نظر

جنسیت، ۱۰ مرد و ۵ زن و از نظر سابقه علمی اجرایی، بین ۱۰ تا ۲۵ سال فعالیت مستمر در حوزه تخصصی خود داشته‌اند. میانگین سنی آن‌ها ۴۵ سال است که بیانگر ترکیبی متوازن از تجربه و پویایی علمی است.

آمار توصیفی نمونه نشان می‌دهد که حدود ۶۰ درصد اعضای نمونه دارای مرتبه علمی استادیاری یا دانشیاری در دانشگاه‌های معتبر داخلی‌اند، ۲۶ درصد سابقه مدیریت اجرایی در سازمان‌های مرتبط با حکمرانی دیجیتال دارند و ۱۴ درصد نیز پژوهشگران مستقل با سوابق بین‌المللی در حوزه علوم شناختی‌اند. این تنوع موجب می‌شود داده‌های گردآوری‌شده از زوایای گوناگون مسئله را پوشش دهند و از غنای تحلیلی بالاتری برخوردار باشند.

شیوه انتخاب نمونه‌ها مبتنی بر روش «نمونه‌گیری هدفمند»^۱ بوده است؛ به این معنا که معیارهای مشخصی برای ورود به جامعه خبرگان تعریف شد: داشتن حداقل یک اثر علمی منتشرشده در موضوع‌های مرتبط، یا سابقه اجرایی و سیاست‌گذاری در نهادهای حکمرانی داده، یا فعالیت پژوهشی در عرصه علوم شناختی. افزون بر این، برای شناسایی و دسترسی به برخی متخصصان کم‌تر شناخته‌شده از روش «گلوله‌برفی»^۲ نیز استفاده شد، به این صورت که هر یک از خبرگان معرفی‌شده، سایر افراد واجد شرایط را نیز پیشنهاد دادند تا شبکه مصاحبه‌شوندگان تکمیل گردد.

روش گردآوری داده‌ها در دو مرحله انجام شد. نخست داده‌های نظری و اسنادی از طریق منابع کتابخانه‌ای معتبر (مقاله‌های علمی، اسناد سیاستی، متون حقوقی و گزارش‌های بین‌المللی) استخراج شد و به‌وسیله تحلیل محتوای کیفی، مضامین مفهومی و روابط علی میان آن‌ها شناسایی گردید. در مرحله دوم، داده‌های میدانی از طریق مصاحبه‌های نیمه‌ساختاریافته با ۱۵ نفر خبرگان گردآوری شد. پرسش‌های مصاحبه به‌گونه‌ای طراحی شده بود که افزون بر تأیید یا نقد چهارچوب نظری اولیه، امکان بروز دیدگاه‌های مستقل و ارائه مثال‌های عملی نیز فراهم گردد.

1. Purposive Sampling
2. Snowball Sampling



جدول ۲: ماتریس نگاشت سؤال‌های پژوهش به محورهای مصاحبه و پرسش‌های محرک

سؤال-فرض پژوهش	محور گفت‌وگو در مصاحبه	نمونه پرسش محرک (نیمه‌ساختار یافته)
نسبت حاکمیت داده و امنیت شناختی	سازوکارهای بازدارندگی ادراکی در حاکمیت داده	از منظر تجربه شما، چه اجزایی از حاکمیت داده به صورت مستقیم از القای روایت‌های مخرب جلوگیری می‌کند؟
حدود حقوقی مالکیت داده‌های شناختی	حق حاکمیت ادراکی، حق اعتراض شناختی	مالکیت بر داده‌های رفتاری-عاطفی در عمل چگونه باید تعریف و تضمین شود؟
کنترل/شفافیت الگوریتمی	تبیین‌پذیری، ممیزی مستقل، انسان‌در-حلقه	حداقل‌های شفافیت و حسابرسی برای الگوریتم‌های اثرگذار بر ادراک چیست؟
توازن سیاستی داده-امنیت ذهنی	تعادل آزادی داده، منافع عمومی، کرامت ذهنی	چه معیارهایی برای برقراری توازن میان آزادی داده و صیانت از ذهن لازم است؟

روش تحلیل داده‌ها بر پایه کدگذاری استقرایی و تحلیل مضمون کیفی قرار گرفت. به این معنا که داده‌های حاصل از مصاحبه‌ها ابتدا در قالب کدهای باز شناسایی شدند، سپس در مرحله کدگذاری محوری، پیوندهای میان مقولات استخراج گردید و در نهایت در قالب مقوله‌های محوری و مضامین اصلی سامان یافت. این فرایند موجب شد چهارچوب مفهومی نهایی نه تنها از ادبیات نظری، بلکه از شواهد تجربی نیز تغذیه شود.

جدول ۳: ویژگی‌های جمعیت‌شناختی خبرگان مصاحبه‌شونده

شاخص‌ها	دسته‌بندی	تعداد (نفر)	درصد (%)
جنسیت	مرد	۱۰	۶۶٫۷
	زن	۵	۳۳٫۳
جمع		۱۵	۱۰۰
سن	۳۵-۴۰ سال	۳	۲۰
	۴۱-۵۰ سال	۸	۵۳٫۳
	۵۱ سال و بالاتر	۴	۲۶٫۷
میانگین سنی		۴۵ سال	—

جدول ۴: ترکیب تخصصی و حرفه‌ای خبرگان

توضیحات	درصد	تعداد (نفر)	حوزه تخصصی-حرفه‌ای
استادان دانشگاه و پژوهشگران حقوق فناوری	۴۰	۶	حقوق داده و حریم خصوصی
متخصصان شناختی با سابقه پژوهش امنیت ادراکی	۳۳/۳	۵	علوم شناختی و روان‌شناسی ادراکی
مدیران و کارشناسان اجرایی در نهادهای سیاست‌گذار	۲۶/۷	۴	حکمرانی دیجیتال و سیاست‌گذاری
—	۱۰۰	۱۵	جمع کل

جدول ۵: شاخص‌های علمی و اجرایی خبرگان

درصد	تعداد (نفر)	دسته‌بندی	شاخص‌ها
۳۳/۳	۵	استادیار	مرتبه علمی
۲۶/۷	۴	دانشیار	
۱۳/۳	۲	پژوهشگر مستقل	
۲۶/۷	۴	مدیر اجرایی-کارشناس ارشد	
۴۰	۶	۱۰-۱۵ سال	سابقه کاری
۳۳/۳	۵	۱۶-۲۰ سال	
۲۶/۷	۴	بیش از ۲۰ سال	

۴. یافته‌های پژوهش

این بخش که به «یافته‌های پژوهش و تجزیه و تحلیل آن‌ها» اختصاص دارد، برآیند نهایی تلفیق داده‌های نظری، تحلیل‌های مفهومی و داده‌های کیفی حاصل از مصاحبه‌های نیمه‌ساختاریافته با خبرگان حوزه‌های حقوق داده، امنیت شناختی، علوم شناختی و حکمرانی دیجیتال است. یافته‌های به‌دست‌آمده از این پژوهش، به‌وضوح حاکی از آن است که در شرایط تحول‌یافته نظم اطلاعاتی جهانی، تهدیدهای شناختی نه‌تنها به یکی از شکل‌های غالب منازعه در فضای ژئوپلیتیک دیجیتال بدل شده‌اند، بلکه به‌واسطه نفوذ خزنده الگوریتم‌های تحلیلگر در حوزه



ادراک عمومی، ظرفیت بازتعریف هویت، ادراک‌ها و تصمیم‌های جمعی را در اختیار کنشگران فناورانه قرار داده‌اند. در این چهارچوب، نبود چهارچوب‌های جامع حقوقی برای تنظیم مالکیت داده، فقدان پاسخ‌گویی الگوریتمی و غیبت رژیم‌های مشخص نظارت و ممیزی شناختی، زمینه را برای تکوین تهدیدهای ادراکی پایدار، ناپیدا و ساخت‌یافته فراهم کرده است.

جدول ۶: کدبوک کیفی و مضامین برآمده از مصاحبه‌ها با شواهد متنی

مضمون نهایی	کد محوری	چند کد باز نمونه	فراوانی	شاهد کوتاه (نقل قول ناشناس)
پاسخ‌گویی فناورانه	شفافیت الگوریتمی	عدم تبیین‌پذیری، مستندسازی الگو، برچسب‌گذاری	۱۳	بدون کارت شناسنامه الگو، در عمل هیچ مرجع پاسخ‌گو پیدا نمی‌شود (E07)
کرامت-حاکمیت ادراکی	مالکیت-کنترل داده	حق اعتراض شناختی، حق فراموشی، دسترسی	۱۲	کاربر باید بتواند پردازش ادراکی را متوقف یا به چالش بکشد (E02)
تاب‌آوری شناختی	ریسک ادراکی	قطبی‌سازی روایتی، حلقه‌های خودتغذیه‌گر	۱۱	الگوریتم، سوگیری موجود را بازتولید و تشدید می‌کند (E10)
معماری نهادی	تنظیم‌گری هوشمند	ممیزی پیشینی-پسینی	۱۲	بدون نهاد ممیزی، سیاست‌نامه‌ها روی کاغذ می‌ماند (E12)

جدول ۷: ثبت روند «اشباع نظری» در کدگذاری مصاحبه‌ها

دسته مصاحبه‌ها	شناسه‌ها	کد تازه افزوده شده	کد تازه سطح مضمون	کل کدهای یکتا (تجمیعی)
نوبت ۱	E01-E03	۱۸	۳	۱۸
نوبت ۲	E04-E06	۱۱	۱	۲۹
نوبت ۳	E07-E09	۷	۱	۳۶
نوبت ۴	E10-E12	۴	۰	۴۰
نوبت ۵	E13-E15	۲	۰	۴۲

جدول ۸: شاخص‌های توافق میان‌کدگذاران و کنترل کیفیت تحلیل

مؤلفه	تعریف-دامنه	هدف-حداقل مطلوب	مقدار محاسبه‌شده
واحد تحلیل	گزاره/واحد معنایی	—	گزاره
درصد توافق (Po)	نسبت توافق خام در بخش دابل کدگذاری	$0/80 \leq$	$0/88$
ضریب κ - کدهای باز	$\kappa = (Po - Pe) / (1 - Pe)$ بر مبنای ۳ مصاحبه دابل	$0/75 \leq$	$0/79$
ضریب κ - کدهای محوری	همان	$0/70 \leq$	$0/72$
ضریب κ - مضامین نهایی	همان	$0/80 \leq$	$0/83$
روایی محتوایی	بازبینی هم‌تایان + بازگشت به مشارکت‌کننده	انجام/مستند	انجام شد

جدول ۹: نگاشت مضمون‌های برآمده از مصاحبه به توصیه‌های سیاستی قابل اجرا

مضمون مصاحبه	بینش/یافته کلیدی	اقدام-سیاست پیشنهادی
پاسخ‌گویی فناورانه	نبود تبیین‌پذیری و مستندسازی الگو	استقرار «کارت شناسنامه الگوریتم» و ممیزی دوره‌ای اجباری
کرامت/حاکمیت ادراکی	ابهام در حقوق داده‌های شناختی	تعریف حقوق «اعتراض شناختی» و «توقف پردازش» در قانون
تاب‌آوری شناختی	چرخه‌های تقویت سوگیری و قطبی‌سازی	انسان‌در-حلقه در حوزه‌های پُریسک و قطع خودکار تقویت سوگیری
معماری نهادی	خلأ رگولاتور ادراکی	ایجاد «مرجع ممیزی الگوریتم‌ها» با اختیار تعلیق- جریمه

نخستین یافته بنیادین این پژوهش، تأکید بر آن دارد که مفهوم حاکمیت داده در شرایط کنونی نمی‌تواند به‌تنهایی به‌عنوان یک گزاره فناورانه یا مالکیتی تلقی شود، بلکه باید در سطح راهبردی، به‌مانند پیش‌نیازی برای صیانت از «امنیت شناختی ملی» بازتعریف گردد. این بازتعریف مستلزم آن است که دولت‌ها ضمن طراحی و پیاده‌سازی چهارچوب‌های قانونی برای تعیین حدود مالکیت داده، از اصولی چون «حق بر حاکمیت ادراکی»، «تمامیت ذهنی»



و «اعتراض شناختی» نیز صیانت کنند. یافته‌ها نشان می‌دهد که در غیاب چنین چهارچوب‌هایی، شهروندان در عمل در معرض استخراج، تحلیل و بازنمایی داده‌های ادراکی و روان‌سنجی خود توسط سکوه‌های تجاری یا بازیگران فراملی قرار گرفته و از حق آگاهی، نظارت و کنترل بر فرایندهای شناختی خویش محروم می‌گردند.

یافته دوم، بر ضعف ساختاری در حوزه تنظیم‌گری الگوریتمی و فقدان پاسخ‌گویی حقوقی تمرکز دارد. تحلیل محتوای داده‌های کیفی به‌دست‌آمده از مصاحبه‌های تخصصی نشان می‌دهد که الگوریتم‌هایی که در فضای عمومی برای هدف‌گیری شناختی، تحلیل رفتار کاربران، طبقه‌بندی محتوایی و شخصی‌سازی اطلاعات به‌کار گرفته می‌شوند، بیشتر فاقد سازوکارهای شفاف‌سازی، مستندسازی و قابلیت ارزیابی ریسک شناختی هستند. درواقع، الگوریتم‌ها به‌عنوان «کنشگران پنهان و خودمختار» عمل می‌کنند و نظام حقوقی موجود نه تنها در شناسایی سازوکار عملکرد آن‌ها ناتوان است، بلکه در سطح تقنینی نیز ظرفیت کافی برای الزام آن‌ها به شفافیت، تبیین‌پذیری و پاسخ‌گویی ندارد. این وضعیت، به‌ویژه در حوزه‌هایی چون رسانه، تبلیغات سیاسی و سیاست‌گذاری اجتماعی، زمینه‌ساز دست‌کاری ادراک عمومی، تشدید قطب‌زدگی اجتماعی و تخریب تدریجی انسجام روانی و معرفتی جامعه شده است. سومین محور یافته‌ها، لزوم طراحی چهارچوب‌های سیاست‌گذاری داده‌محور با رویکردی شناختی حکمرانی است. بررسی سیاست‌های موجود و تحلیل ساختار نهادی نظام حکمرانی دیجیتال نشان می‌دهد که در اغلب موارد، سیاست‌گذاری‌ها فاقد درک ادراکی از تأثیرات داده‌ها و الگوریتم‌ها بر سازوکارهای ذهنی هستند و اغلب در سطحی به‌تنهایی فناورانه یا امنیتی باقی می‌مانند. یافته‌های این پژوهش نشان می‌دهد که برای مهار تهدیدهای شناختی، باید سیاست‌گذاری‌ها از سطح کنترل داده و زیرساخت، به سطح طراحی روایت، مهندسی ادراک و حمایت از استقلال ذهنی ارتقا یابد. این امر مستلزم آن است که حاکمیت داده نه به‌تنهایی در چهارچوب ذخیره‌سازی بومی یا منع دسترسی بیگانه، بلکه به‌مانند یک چهارچوب ترکیبی شامل حکمرانی الگوریتمی، عدالت شناختی و کرامت ذهنی انسان‌ها تلقی شود. در سطح تحلیلی، داده‌های گردآوری‌شده حاکی از آن است که هیچ‌یک از سه الگوی

حاکمیت داده متعارف - یعنی الگوی لیبرال فردمحور، الگوی جمع‌گرایانه رفاه‌محور و الگوی دولت‌محور امنیت‌گرا - به‌تنهایی توانایی پاسخ‌گویی به پیچیدگی‌های تهدیدهای شناختی را ندارند؛ بلکه نیاز به الگوی مفهومی جدیدی است که در آن، حاکمیت داده با حاکمیت ذهنی هم‌راستا شده و تنظیم‌گری، مسئولیت‌پذیری و مشارکت چندسطحی در فرایندهای ادراکی لحاظ گردد. این الگوی پیشنهادی باید بر سه پایه استوار باشد: نخست، تنظیم دقیق و چندسطحی مالکیت داده و اعمال حق نظارت فردی و جمعی بر داده‌های شناختی؛ دوم، الزام‌آوری تقنینی برای شفاف‌سازی، مستندسازی و پاسخ‌گویی الگوریتم‌های شناخت‌محور در فضای عمومی؛ و سوم، طراحی نهادهای حکمرانی ادراکی برای نظارت، ممیزی و مقابله با تخلقات ادراک‌زدا یا عملیات شناختی مخرب. یافته‌های تحقیق نشان می‌دهد که تحقق حکمرانی هوشمند داده‌محور بدون استقرار یک رژیم حقوقی سیاستی شناخت‌محور که بتواند مالکیت داده، کنترل الگوریتمی و تاب‌آوری شناختی را در ساختاری یکپارچه به هم پیوند دهد، امکان‌پذیر نخواهد بود. تهدیدهای شناختی، به‌مانند جدیدترین و عمیق‌ترین شکل تهدید علیه امنیت ملی و حاکمیت فرهنگی معرفتی جوامع، نیازمند رویکردی ترکیبی، میان‌رشته‌ای و آینده‌نگر است که در آن، حقوق داده نه به‌تنهایی ناظر بر اطلاعات، بلکه ضامن کرامت ذهن، هویت ادراکی و استقلال روانی انسان مدرن باشد.

۴-۱. الگوی پیشنهادی حاکمیت داده برای مهار تهدیدهای شناختی

براساس تحلیل مبانی نظری، بررسی اسناد مرتبط و تحلیل مضمون مصاحبه‌های انجام‌شده با خبرگان، الگوی پیشنهادی پژوهش برای تعیین نقش حاکمیت داده در مهار تهدیدهای شناختی در قالب یک الگوی سه‌لایه و چرخه‌ای قابل تبیین است. این الگو بر این فرض استوار است که تهدید شناختی زمانی امکان اثرگذاری پایدار پیدا می‌کند که سه حوزه اصلی، یعنی داده، الگوریتم و سیاست‌گذاری، فاقد نظام تنظیم‌گر منسجم باشند. ازاین‌رو، مهار تهدیدهای شناختی نیز نیازمند الگویی است که به‌صورت هم‌زمان مالکیت و کنترل داده، شفافیت و پاسخ‌گویی الگوریتمی و سیاست‌گذاری کلان‌داده‌ای را در ارتباط با امنیت شناختی



سامان دهد.

لایه نخست الگو، «لایه حقوقی-مالکیتی داده» است. در این لایه، داده‌ها برحسب میزان حساسیت و قابلیت اثرگذاری بر ادراک افراد و جامعه طبقه‌بندی می‌شوند. داده‌های فنی و عمومی در سطح پایه، داده‌های هویتی و رفتاری در سطح حساس و داده‌های شناختی، عاطفی و روان‌سنجی در سطح بسیار حساس قرار می‌گیرند. کارکرد اصلی این لایه، تعیین حدود مالکیت، دسترسی، پردازش، انتقال، توقف پردازش و حق اعتراض نسبت به داده‌هایی است که می‌توانند در شکل‌دهی یا دست‌کاری ادراک عمومی نقش داشته باشند؛ بنابراین، در این بخش از الگو، حاکمیت داده از سطح مدیریت اداری اطلاعات فراتر می‌رود و به ابزار صیانت از حاکمیت ادراکی افراد و جامعه تبدیل می‌شود.

لایه دوم الگو، «لایه تنظیم‌گری و ممیزی الگوریتمی» است. در این لایه، الگوریتم‌هایی که در تحلیل رفتار کاربران، پیشنهاد محتوا، طبقه‌بندی پیام‌ها، هدف‌گیری شناختی، تبلیغات سیاسی، مدیریت افکار عمومی و تصمیم‌سازی داده‌محور نقش دارند، براساس میزان ریسک ادراکی ارزیابی و طبقه‌بندی می‌شوند. ابزارهای اصلی این لایه شامل کارت‌شناسنامه الگوریتم، ارزیابی اثر ادراکی، ممیزی پیشینی و پسینی، ثبت رخدادهای ادراکی، الزام به تبیین‌پذیری و پیش‌بینی مداخله انسانی در حوزه‌های پُرخطر است. هدف این لایه آن است که الگوریتم‌ها از وضعیت کنشگران پنهان و غیرپاسخ‌گو خارج شوند و در برابر آثار شناختی و اجتماعی خود قابل نظارت، اصلاح و بازخواست باشند.

لایه سوم الگو، «لایه سیاست‌گذاری کلان‌داده‌ای و تاب‌آوری شناختی» است. در این لایه، سیاست‌های عمومی، مقررات ملی، برنامه‌های آموزشی، سازوکارهای نهادی و راهبردهای دفاع شناختی با محوریت داده طراحی می‌شوند. کارکرد اصلی این لایه، ایجاد تعادل میان جریان آزاد داده، امنیت شناختی، حقوق ادراکی شهروندان و منافع حاکمیتی است. در این سطح، سیاست‌گذار باید افزون بر کنترل فنی داده، به پیامدهای ادراکی، روایتی و اجتماعی داده‌ها نیز توجه کند و از طریق ارتقای سواد داده‌ای و ادراکی، حمایت از فناوری‌های شناختی بومی، تدوین استانداردهای شفافیت و ایجاد مرجع ممیزی الگوریتم‌ها، تاب‌آوری شناختی

جامعه را تقویت نماید.

براین اساس، الگوی نهایی پژوهش را می‌توان در قالب یک چرخه سه‌مرحله‌ای توضیح داد: نخست، شناسایی و طبقه‌بندی داده‌های اثرگذار بر ادراک؛ دوم، کنترل و ممیزی الگوریتم‌های پردازشگر و جهت‌دهنده به ادراک؛ سوم، تبدیل یافته‌های نظارتی به سیاست‌های کلان‌داده‌ای و برنامه‌های تقویت تاب‌آوری شناختی. خروجی این چرخه، شکل‌گیری نظامی از حاکمیت داده است که در آن داده، الگوریتم و سیاست به‌صورت جداگانه مدیریت نمی‌شوند، بلکه در قالب یک معماری یکپارچه برای صیانت از امنیت ادراکی و مهار تهدیدهای شناختی به‌کار گرفته می‌شوند.

درنتیجه، الگوی پیشنهادی این پژوهش دارای سه رکن اصلی است: رکن نخست، «حاکمیت حقوقی بر داده‌های شناختی»؛ رکن دوم، «تنظیم‌گری ریسک‌محور الگوریتم‌های اثرگذار بر ادراک» و رکن سوم، «سیاست‌گذاری کلان‌داده‌ای برای تاب‌آوری شناختی». رابطه میان این سه رکن، رابطه‌ای خطی و جداگانه نیست، بلکه رابطه‌ای چرخه‌ای و تکمیل‌کننده است؛ به این معنا که بدون تعیین حقوق و حدود مالکیت داده، امکان ممیزی مؤثر الگوریتم‌ها وجود ندارد؛ بدون شفافیت و پاسخ‌گویی الگوریتمی، سیاست‌گذاری کلان‌داده‌ای به سطح تصمیم‌های کلی و غیرقابل اجرا فروکاسته می‌شود و بدون سیاست‌گذاری کلان و نهادی، حقوق داده و ممیزی الگوریتمی نیز فاقد ضمانت اجرایی مؤثر خواهند بود؛ بنابراین، الگوی پیشنهادی پژوهش، حاکمیت داده را به‌عنوان سازوکاری سه‌لایه برای تبدیل کنترل داده به امنیت شناختی تبیین می‌کند.

۴-۲. راهبردهای اجرایی در کنترل ملی الگوریتم‌های اثرگذار بر امنیت شناختی

۱. تأسیس مرجع ممیزی الگوریتم‌ها به‌عنوان نهاد مستقل و چندرشته‌ای برای ارزیابی و نظارت و تدوین استانداردهای حکمرانی الگوریتمی؛
۲. طراحی سامانه ملی شناسایی و طبقه‌بندی الگوریتم‌های خطرآفرین شناختی بر پایه شاخص‌های ریسک ادراکی و پایش مستمر سکوها؛



۳. ایجاد چرخه بازخورد اصلاحی درون الگوریتم‌ها برای مهار تثبیت سوگیری‌های شناختی و جلوگیری از بازتولید قطبی‌سازی؛
۴. تدوین دستورنامه مداخله انسانی هوشمند در حوزه‌های حساس رسانه‌ای و تصمیم‌سازی عمومی برای کنترل خروجی‌های پُریسک؛
۵. تصویب مقررات و استانداردهای ملی حکمرانی دیجیتال و امنیت شناختی با تأکید بر شفافیت و مسئولیت‌پذیری و امکان تنظیم‌گری عمومی؛
۶. مرجع‌میزی الگوریتم‌ها باید اختیار بررسی پیشینی و پسینی و صدور مجوز و تعلیق الگوریتم‌های پُرخطر را داشته باشد و ترکیبی از حقوق دانان داده و متخصصان علوم شناختی و کارشناسان فنی را گرد هم آورد تا پاسخ‌گویی و عدالت شناختی از سطح توصیه به سطح الزام برسد. این راهبرد نقطه شروع راهبردسازی الگوریتمی ملی است و امکان حکمرانی مؤثر بر آثار شناختی را فراهم می‌کند (Niquet, 2021: 147)، همچنین با نهادهای گردن اِزارهای ممیزی و ارزیابی ریسک از شکل‌گیری خلأ نظارتی جلوگیری می‌شود (Roth & Murnighan, 1978: 194)؛
۷. سامانه ملی شناسایی الگوریتم‌های خطرآفرین باید شاخص‌هایی مانند نرخ تأثیر بر تصمیم‌گیری عمومی و شدت بازتولید روایت‌های انحرافی را به معیارهای عملیاتی تبدیل کند و براساس رتبه‌بندی ریسک، دستورهای نظارت و هشدار و مداخله را فعال سازد. خروجی این سامانه باید برای مرجع ممیزی و نهادهای سیاست‌گذار قابل استفاده باشد تا تصمیم‌ها به‌موقع و مبتنی بر داده اتخاذ شوند و از تداوم عملیات ادراکی پنهان پیشگیری گردد؛
۸. چرخه بازخورد اصلاحی به معنای افزودن سازوکارهای فنی و نهادی است که الگوریتم را از حالت خودتغذیه‌گر خارج کند و امکان اصلاح سوگیری و توقف تقویت روایت تک‌بعدی را فراهم آورد. این چرخه می‌تواند با داده‌های تطبیقی تولیدشده توسط نهادهای مستقل یا کاربران آگاه تغذیه شود تا مسیر تصمیم‌گیری الگوریتمی به سمت تعادل و کاهش خطای ادراکی هدایت گردد؛

۹. دستورنامه مداخله انسانی هوشمند باید مشخص کند در چه موضوع‌هایی و با چه آستانه‌ای از حساسیت، تأیید انسانی شرط اعتبار خروجی الگوریتمی است و چه مسیرهایی برای اصلاح یا حذف فوری پیش‌بینی می‌شود. این مداخله در بحران‌های سیاسی و امنیت ملی و مسائل قومیتی مانع از وقوع آسیب‌های جمعی می‌شود و الگوی حکمرانی انسان ماشین را در حوزه‌های پُریسک تثبیت می‌کند (Pana, 2006: 15)؛

۱۰. مقررات ملی حکمرانی دیجیتال و امنیت شناختی باید حق جامعه برای آگاهی از سازوکارهای اثرگذاری الگوریتمی را تضمین کند و مسئولیت توسعه دهندگان و بهره‌برداران را در برابر پیامدهای اجتماعی روشن سازد و امکان اعمال تنظیم‌گری عمومی را فراهم کند. این استانداردها باید به حوزه‌هایی مانند تبلیغات سیاسی و پیشنهاددهی رسانه‌ای و تحلیل داده‌های سلامت روان توجه ویژه داشته باشد تا کنترل ملی الگوریتم‌ها از سطح سیاست‌نامه به سطح قاعده اجرایی ارتقا یابد (Emmanuel et al., 2021: 11)، شواهد میدانی نیز نشان می‌دهد نبود تنظیم‌گری مؤثر می‌تواند به تهدید جدی برای امنیت روانی و شناختی ملت‌ها تبدیل شود (محمدی‌الستی و فولادی، ۱۴۰۰: ۵۸).

۳-۴. سیاست‌های تقنینی و اجرایی برای تاب‌آوری ادراکی جامعه در بستر داده

۱. ارتقای بنیادین سواد داده‌ای و ادراکی در نظام آموزش رسمی و غیررسمی به‌عنوان نخستین سیاست کلیدی، به این معنا که آموزش عمومی فراتر از مهارت‌های فنی و سواد رایانه‌ای رفته و مفاهیمی چون تشخیص روایت‌های فریبنده، شناسایی سوگیری‌های شناختی، درک سازوکارهای الگوریتمی رسانه‌ها و بازشناسی عملیات روانی در بستر داده‌ها را در برگیرد تا شهروندان بتوانند در برابر مداخله‌های ادراکی هدفمند، مقاوم و فعال عمل کنند (Linden et al., 2003: 83).

۲. طراحی و اجرای سیاست‌های حمایتی و تشویقی برای توسعه فناوری‌های شناختی



بومی به گونه‌ای که با ایجاد انگیزه برای شرکت‌های دانش‌بنیان و تیم‌های پژوهشی فعال در حوزه فناوری‌های شناختی، زمینه تولید الگوریتم‌های تحلیل ادراکی، سامانه‌های تشخیص عملیات شناختی و الگوهای بومی روایت‌پردازی فراهم شود و این روند با ابزارهایی مانند حمایت‌های مالیاتی، اعتبارات پژوهشی، اولویت در پروژه‌های ملی و تسهیلات سرمایه‌گذاری پشتیبانی گردد تا اکوسیستمی فناورانه و مقاوم در برابر تهدیدهای شناختی شکل گیرد (Roth & Murnighan, 1978: 197).

۳. استفاده هوشمندانه و هدفمند از «داده‌های بازتعریف‌شده روایت‌محور» به عنوان سیاست مکمل، به این معنا که به جای اکتفا به داده‌های خام، از داده‌هایی بهره گرفته شود که حاوی ساختارهای معنایی، چهارچوب‌های استنباطی و جهت‌گیری‌های ارزشی هستند و می‌توانند در خدمت تقویت و ترویج «روایت‌های ادراکی ملی» قرار گیرند تا درک مردم از خود، ملت، دشمن، تهدید و آینده بازتعریف شده و انسجام روانی و ادراکی جامعه در برابر پویش‌های شناختی مهاجم تقویت شود (McGrath, 2016: 20).

۴. اجرای برنامه‌های هدفمند ارتقای تاب‌آوری ادراکی در میان «کارکنان دولت» و «نخبگان سیاسی» به عنوان گروه‌های دروازه‌بان ادراک عمومی، به این صورت که این اقشار از طریق دوره‌های تخصصی، آموزش راهبردهای مقابله با عملیات شناختی، آشنایی با تکنیک‌های اثرگذاری ادراکی و تمرین‌های سناریومحور در سطوح مختلف تصمیم‌گیری مجهز شوند تا در برابر نفوذ ادراکی و تصمیم‌سازی تحمیلی مصونیت بیشتری پیدا کنند و بتوانند از جایگاه خود، سپری برای جامعه ایجاد نمایند (Niquet, 2021: 145).

۵. اعمال سیاست‌های «تحریم داده‌ای هوشمند» علیه سکوها و کشورهایی که مدیریت یا پشتیبانی تهدیدهای شناختی را برعهده دارند، به عنوان ابزار بازدارندگی و مدیریت ریسک، به این معنا که با استفاده از محدودیت دسترسی به داده‌های عمومی، ممنوعیت برخی تعاملات فنی یا مسدودسازی الگوریتم‌های مشکوک و از طریق سازوکارهای همکاری بین‌المللی، امکان صیانت مشروع از امنیت شناختی ملی فراهم شود، درحالی‌که هم‌زمان با مجموعه‌ای از سیاست‌های تقنینی، تربیتی، فناورانه و روایتی، تاب‌آوری ادراکی جامعه به صورت

چندبُعدی و پایدار تقویت می‌گردد (Jensen et al., 2020: 537).



۵. نتیجه‌گیری و پیشنهاد

پاسخ به سؤال فرعی نخست: حدود و اصول حقوقی مالکیت داده در مواجهه با تهدیدهای ادراکی چگونه باید تعریف و تنظیم شود تا از حاکمیت ذهنی افراد در برابر دست‌کاری شناختی محافظت کند؟ جمع‌بندی مضامین برآمده از گفت‌وگو با خبرگان حقوق داده و علوم شناختی نشان می‌دهد که تعریف کارآمد مالکیت داده، نیازمند تفکیک صریح طبقات داده (فنی، هویتی، رفتاری و شناختی)، ارتقای سطح حمایت برای طبقه شناختی به عنوان «داده‌های بسیار حساس»، گنجاندن حقوق چهارگانه دسترسی، قابلیت حمل، حذف - فراموشی و مهم‌تر



از همه «اعتراض و توقف پردازش شناختی» در قانون و نیز برقراری تکالیف امانی برای سکوها در مقام «امین داده» است؛ دوازده نفر از پانزده مصاحبه‌شونده شفاف و روشن بر لزوم شناسایی «حق حاکمیت ادراکی» به عنوان حق مستقل و قابل استناد قضایی تأکید کردند و این نکته را افزودند که این حق بدون سازوکارهای اجرایی روشن - مانند دفتر ثبت پردازش‌های با ریسک ادراکی، ارزیابی اثر ادراکی پیشینی برای پروژه‌های کلان‌داده‌ای و امکان مطالبه توضیح قابل فهم از الگوهای تصمیم‌یار- ضمانت تحقق نخواهد یافت، به این ترتیب مرزهای حقوقی لازم باید از سطح رضایت شکلی فراتر رود و به سطح «قابلیت کنترل واقعی فرد بر سرنوشت داده‌های ادراکی» برسد، به گونه‌ای که فرد بتواند در نقاط حساس چرخه پردازش، از حق تعلیق، محدودسازی دامنه استفاده، یا انتقال امن به امین جایگزین استفاده کند و درعین حال سازوکارهای جبران خسارت ادراکی، امکان اثبات رابطه سببیت میان پردازش و آسیب شناختی را از طریق بار اثبات معکوس برای پردازشگر تسهیل نماید.

پاسخ به سؤال فرعی دوم: چه سازوکارهای حقوقی و نظارتی برای کنترل، شفاف‌سازی و پاسخ‌گویی الگوریتم‌های شناختی در فرایندهای تصمیم‌سازی داده‌محور قابل طراحی است؟ مضمون غالب در گفت‌وگوها که از سوی سیزده نفر از مشارکت‌کنندگان تکرار شد این بود که کنترل مؤثر الگوریتم‌ها تنها با ترکیب ابزارهای پیشینی و پسینی و استقرار یک رژیم ریسک‌محور قابل اتکا می‌شود؛ در وجه پیشینی، لازم است «کارت‌شناسنامه الگوریتم» شامل هدف، دامنه، داده‌های تمرین، سنجه‌های سوگیری، حدود تبیین‌پذیری و نقاط مداخله انسانی پیش از استقرار عمومی ثبت و افشا شود و هر سامانه پُرسیک فرایند ارزیابی اثر ادراکی را بگذراند و مجوز زمان‌دار دریافت کند؛ در وجه پسینی، ممیزی دوره‌ای مستقل، ثبت و گزارش حوادث ادراکی، بازآفرینی تصمیم برای موارد شکایت و امکان تعلیق فوری الگوهای پُرخطر باید در اختیار مرجع ممیزی قرار گیرد و در حوزه‌های پُرسیک، حضور انسان در حلقه مانند شرط قانونی اعتبار تصمیم الزام‌آور شود، همچنین طبقه‌بندی ریسک از «کم» تا «غیرقابل قبول» باید به الزام‌های متناسب گره بخورد تا شفافیت صرف جایگزین مسئولیت واقعی نشود و در نهایت پاسخ‌گویی از سطح توسعه‌دهنده تا بهره‌بردار توزیع گردد و ابزارهای جبرانی مانند

صندوق خسارت ادراکی برای پاسخ‌های سریع و بی‌هزینه در دسترس عموم قرار گیرد. پاسخ به سؤال فرعی سوم: چگونه می‌توان از طریق سیاست‌گذاری داده‌محور، بین امنیت شناختی، حاکمیت داده و حقوق ادراکی تعادل برقرار کرد؟ برآیند تحلیل‌ها و تأکید یازده تا دوازده نفر از خبرگان در دو خوشه «تاب‌آوری شناختی» و «سیاست‌گذاری کلان‌داده» حکایت از آن دارد که تعادل پایدار تنها در صورتی حاصل می‌شود که سیاست‌ها هم‌زمان سه اصل را پی بگیرند: نخست، اصل تناسب و ضرورت که به‌موجب آن هر محدودیت بر جریان داده یا بر خروجی الگوریتمی باید به‌طور دقیق متناسب با سطح ریسک ادراکی و محدود به حداقل لازم باشد تا آزادی داده و تنوع روایات فدا نشود؛ دوم، اصل شفافیت معنادار که از سطح افشاگری‌های نمادین فراتر می‌رود و به ارائه توضیحات قابل فهم و قابل اعتراض برای افراد، برچسب‌گذاری خروجی‌های حساس و آموزش سواد ادراکی عمومی منتهی می‌شود؛ سوم، اصل مشارکت ذی‌نفعان که از طریق درگیرکردن جامعه مدنی، دانشگاه و بخش خصوصی در تدوین استانداردها، آزمایش‌های میدانی در محیط‌های امن و ایجاد اکوسیستم پژوهش‌های ممیزی مستقل، مشروعیت و کارآمدی سیاست‌ها را تضمین می‌کند؛ این تعادل در افق زمانی کوتاه‌مدت با شیوه نامه‌های شفافیت و برچسب‌گذاری و در میان‌مدت با تأسیس مرجع ممیزی و آیین‌نامه‌های ارزیابی اثر ادراکی و در بلندمدت با تقنین جامع «حقوق داده ادراک» و نهادهای سازوکارهای جبران و نظارت اجتماعی استوار می‌شود، به‌گونه‌ای که هم حق حاکمیت ادراکی فرد پاس داشته شود، هم منافع عمومی و امنیت شناختی صیانت گردد و هم ظرفیت نوآوری و بهره‌وری داده‌ای در چهارچوب‌های پیش‌بینی‌پذیر و عادلانه حفظ بماند.

پاسخ به سؤال اصلی پژوهش: الگوی مناسب برای تعیین نقش حاکمیت داده در مهار تهدیدهای شناختی در بستر حکمرانی هوشمند کدام است؟

بر مبنای تحلیل مضمون مصاحبه‌های نیمه‌ساختاریافته با ۱۵ نفر از خبرگان و تلفیق آن با مبانی نظری و اسناد مرتبط، الگوی مناسب برای تعیین نقش حاکمیت داده در مهار تهدیدهای شناختی، «الگوی سه‌لایه و چرخه‌ای حاکمیت داده شناخت‌محور» است. این الگو بر سه لایه



اصلی استوار است: نخست، لایه حقوقی - مالکیتی داده؛ دوم، لایه تنظیم‌گری و ممیزی الگوریتمی و سوم، لایه سیاست‌گذاری کلان‌داده‌ای و تاب‌آوری شناختی. در این الگو، داده، الگوریتم و سیاست‌گذاری به‌عنوان سه حوزه جداگانه و منفک در نظر گرفته نمی‌شوند، بلکه در قالب یک معماری یکپارچه برای صیانت از امنیت ادراکی و کنترل تهدیدهای شناختی سامان می‌یابند.

در لایه نخست، حاکمیت داده از طریق طبقه‌بندی داده‌ها به داده‌های فنی، هویتی، رفتاری و شناختی، زمینه تعیین حدود مالکیت، دسترسی، پردازش، انتقال، توقف پردازش و حق اعتراض نسبت به داده‌های اثرگذار بر ادراک را فراهم می‌سازد. در این سطح، داده‌های شناختی، عاطفی و روان‌سنجی به‌عنوان داده‌های بسیار حساس تلقی می‌شوند و باید مشمول حمایت حقوقی شدیدتر قرار گیرند؛ زیرا این دسته از داده‌ها می‌توانند در شکل‌دهی، جهت‌دهی یا دست‌کاری ادراک فردی و جمعی نقش مستقیم داشته باشند؛ بنابراین، نقش حاکمیت داده در این لایه، تبدیل مدیریت داده به سازوکار صیانت از حاکمیت ادراکی افراد و جامعه است.

در لایه دوم، الگو بر تنظیم‌گری ریسک‌محور الگوریتم‌های اثرگذار بر ادراک عمومی تأکید دارد. یافته‌های پژوهش نشان داد که الگوریتم‌های پیشنهاددهنده، تحلیل‌گر رفتار، طبقه‌بندی‌کننده محتوا و هدف‌گیر شناختی، در صورت فقدان شفافیت و ممیزی، می‌توانند به کنشگرانی پنهان در تولید سوگیری، قطبی‌سازی و دست‌کاری ادراک عمومی تبدیل شوند. از این‌رو، ابزارهایی مانند کارت‌شناسنامه الگوریتم، ارزیابی اثر ادراکی، ممیزی پیشینی و پسینی، ثبت رخدادهای ادراکی، الزام به تبیین‌پذیری و مداخله انسانی در حوزه‌های پُرخطر، اجزای اصلی این لایه را تشکیل می‌دهند. نقش حاکمیت داده در این سطح، خارج‌کردن الگوریتم‌ها از وضعیت جعبه سیاه و تبدیل آن‌ها به سازوکارهای قابل نظارت، اصلاح و پاسخ‌گویی است.

در لایه سوم، سیاست‌گذاری کلان‌داده‌ای با هدف تقویت تاب‌آوری شناختی جامعه سازمان‌دهی می‌شود. در این لایه، حاکمیت داده باید میان جریان آزاد داده، امنیت شناختی،

حقوق ادراکی شهروندان و منافع حاکمیتی تعادل برقرار کند. این تعادل از طریق تدوین استانداردهای شفافیت، ارتقای سواد داده‌ای و ادراکی، حمایت از فناوری‌های شناختی بومی، ایجاد مرجع ممیزی الگوریتم‌ها و طراحی سازوکارهای جبران خسارت ادراکی تحقق می‌یابد؛ بنابراین، نقش حاکمیت داده در این لایه، تبدیل داده و تحلیل داده به ابزار سیاست‌گذاری پیشگیرانه، توانمندساز و بازدارنده در برابر تهدیدهای شناختی است.

براین اساس، الگوی نهایی پژوهش، الگوی خطی و ایستا نیست، بلکه چرخه‌ای و تکمیل‌کننده است. این چرخه از شناسایی و طبقه‌بندی داده‌های اثرگذار بر ادراک آغاز می‌شود، سپس به کنترل و ممیزی الگوریتم‌های پردازشگر و جهت‌دهنده به ادراک می‌رسد و در نهایت به سیاست‌گذاری کلان‌داده‌ای برای تقویت تاب‌آوری شناختی منتهی می‌شود. در این چرخه، هر لایه پیش‌شرط کارآمدی لایه بعدی است؛ به این معنا که بدون تعیین حقوق و حدود مالکیت داده، ممیزی الگوریتمی مؤثر نخواهد بود؛ بدون شفافیت و پاسخ‌گویی الگوریتمی، سیاست‌گذاری کلان‌داده‌ای به تصمیم‌های کلی و غیرقابل اجرا فروکاسته می‌شود؛ و بدون سیاست‌گذاری نهادی و ضمانت اجرایی، حقوق داده و ممیزی الگوریتمی نیز اثر عملی کافی نخواهد داشت.

بنابراین، پاسخ نهایی پژوهش آن است که حاکمیت داده زمانی می‌تواند در مهار تهدیدهای شناختی نقش‌آفرینی کند که در قالب یک الگوی سه‌لایه شامل «حاکمیت حقوقی بر داده‌های شناختی»، «تنظیم‌گری ریسک‌محور الگوریتم‌های اثرگذار بر ادراک» و «سیاست‌گذاری کلان‌داده‌ای برای تاب‌آوری شناختی» مستقر شود. این الگو، حاکمیت داده را از سطح مدیریت فنی اطلاعات فراتر می‌برد و آن را به سازوکاری حقوقی، فناورانه و سیاستی برای تبدیل کنترل داده به امنیت شناختی و صیانت از حاکمیت ادراکی جامعه تبدیل می‌کند.

جمع‌بندی نهایی پژوهش نشان می‌دهد که مهار تهدیدهای شناختی در عصر حکمرانی هوشمند، تنها با کنترل محتوا، محدودسازی سکوها یا سیاست‌های امنیتی سنتی امکان‌پذیر نیست، بلکه نیازمند استقرار نظامی از حاکمیت داده است که بتواند هم‌زمان بر داده‌های اثرگذار بر ادراک، الگوریتم‌های جهت‌دهنده به ذهنیت عمومی و سیاست‌های کلان‌داده‌ای



ناظر بر تاب‌آوری شناختی اعمال اقتدار کند. از این منظر، الگوی پیشنهادی پژوهش، تلاشی برای پیوند میان حقوق داده، حکمرانی الگوریتمی و امنیت شناختی است و می‌تواند مبنایی برای طراحی مقررات، نهادهای تنظیم‌گر و سیاست‌های اجرایی در حوزه صیانت از امنیت ادراکی جامعه قرار گیرد.

۵-۱. پیشنهادهای پژوهش

۱. تدوین «منشور ملی حاکمیت ادراکی و داده‌محور» در دستور کار نهادهای قانون‌گذار و سیاست‌گذار (مجلس شورای اسلامی، شورای عالی فضای مجازی و مرکز ملی فضای مجازی) قرار گیرد که در آن اصولی چون مالکیت شناختی، شفافیت الگوریتمی و حق اعتراض شناختی به‌عنوان حقوق بنیادین دیجیتال شناسایی شوند.
۲. لازم است نهادهای حکمرانی دیجیتال با همکاری میان‌رشته‌ای متخصصان علوم داده، حقوق فناوری، علوم شناختی و سیاست عمومی، اقدام به طراحی «نهاد تنظیم‌گر الگوریتم‌های شناختی» نمایند که ضمن ارزیابی ریسک‌های ادراکی سکوها و سامانه‌های تحلیل‌گر، مسئولیت پاسخ‌گویی آن‌ها را در قبال تأثیرگذاری شناختی الزامی سازد.
۳. سیاست‌گذاری در حوزه حکمرانی داده از سطح کنترل زیرساختی و امنیتی فراتر رفته و به سطح «سیاست‌گذاری شناختی» ارتقا یابد، به‌گونه‌ای که از طریق تنظیم‌گری داده‌های ذهنی، محافظت از ساختارهای معرفتی و مقابله با راهبردهای دست‌کاری ادراک، تاب‌آوری شناختی جامعه تقویت شود.
۴. توسعه چهارچوب‌های حقوقی جدید برای تفکیک میان انواع داده‌ها (داده‌های فنی، هویتی، رفتاری و شناختی) و تعیین سطوح مختلف حق مالکیت و مداخله دولت یا سکوها در هر دسته، می‌تواند مبنایی برای نظام حقوق داده‌ای پیشرفته در مواجهه با تهدیدهای ادراکی باشد.
۵. در افق پژوهش‌های آینده، انجام مطالعات تجربی و کمی برای طراحی شاخص‌های سنجش‌پذیر تاب‌آوری ادراکی و ارزیابی رابطه میان حاکمیت داده، تنظیم‌گری

الگوریتمی و سطح تهدیدهای شناختی در میان گروه‌های مختلف کاربران فضای مجازی پیشنهاد می‌شود.

۶. پیشنهاد می‌شود پژوهش‌های تطبیقی میان نظام حقوقی جمهوری اسلامی ایران و رژیم‌های حقوق داده و امنیت شناختی در سایر کشورها (مانند اتحادیه اروپا و برخی کشورهای آسیایی و منطقه‌ای) انجام گیرد تا الگوهای موفق در حوزه حقوق داده و حکمرانی الگوریتمی شناسایی و امکان بومی‌سازی آن‌ها بررسی شود.
۷. انجام مطالعات موردپژوهی عمیق بر روی سکوها و سامانه‌های مشخص (ازجمله شبکه‌های اجتماعی پُرکاربر یا سامانه‌های تصمیم‌یار دولتی) برای واکاوی عملی سازوکارهای پردازش داده، سطح شفافیت الگوریتمی و میزان رعایت حقوق ادراکی کاربران به‌عنوان مسیر دیگری برای تحقیقات آتی پیشنهاد می‌گردد.



فهرست منابع

اسماعیلی، حمید؛ ابوذر میرزاعباسی «بررسی قابلیت‌های علوم و فناوری‌های شناختی برای کاربردهای دفاعی-امنیتی جمهوری اسلامی ایران». فصلنامه علمی راهبرد دفاعی، سال ۲۲، شماره ۸۶.

اصلی‌پور، حسین؛ میرهاشمی، علی؛ نهادی، هادی. «تبیین فرایند تصمیم‌گیری حاکمیتی دفاع مقدس با رویکرد نظریه‌پردازی داده‌بنیاد». فصلنامه علمی راهبرد دفاعی، سال ۱۸، شماره ۷۲.

پورهادی، ابراهیم؛ قباد نوری. «تأثیر عملیات روانی رسانه‌های غربی بر امنیت سیاسی-اجتماعی (مطالعه موردی: نظامیان مستقر در غرب کشور)». فصلنامه راهبرد دفاعی، سال ۱۳، شماره ۵۰.

شاملوی، رضا؛ رضا زاده، مصطفی. «شناسایی و اولویت‌بندی کارکردهای سیاسی فضای مجازی (شبکه‌های اجتماعی) در جنگ شناختی». فصلنامه علمی راهبرد دفاعی، سال ۲۲، شماره ۸۵.

عقیلی، سید وحید؛ اسدی، عباس؛ فریادپور، داوود. «طراحی الگوی آگاهی‌بخشی سازمانی ارتش جمهوری اسلامی ایران مبتنی بر بیانات مقام معظم رهبری». فصلنامه راهبرد دفاعی، سال ۱۶، شماره ۶۱.

محمدی‌الستی، مسعود؛ فولادی، قاسم؛ نهادی، هادی. «الگوی آمریکا در جنگ مردم‌محور علیه نظام جمهوری اسلامی ایران». فصلنامه علمی راهبرد دفاعی، سال ۱۹، شماره ۷۶.

References

- Bousquet, Antoine, Simon Curtis, and Alister Miskimmon. 2021. *Cognitive Security: Examining the New Strategic Contest over Information*. Contemporary Security Policy 42 (4): 427–449.
- Emmanuel, Thato, T. Maupong, D. Mpoeleng, T. Semong, B. Mphago, and O. Tabona. "A Survey on Missing Data in Machine Learning." Journal of Big Data 8, no. 1 (2021): 1–37.
- Jensen, Benjamin M., Christopher Whyte, and Scott Cuomo. "Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence." International Studies Review 22, no. 3 (2020): 526–550.
- Lind, William S., Keith Nightengale, John F. Schmitt, and Joseph W. Sutton. "The Changing Face of War: Into the Fourth Generation." Marine Corps Gazette 73, no. 10 (1989): 22–26.
- Linden, Greg, Brent Smith, and Jeremy York. "Amazon.com Recommendations: Item-to-Item Collaborative Filtering." IEEE Internet Computing 1, no. 5 (2003): 76–80.
- McGrath, John R. "Twenty-First Century Information Warfare and the Third Offset Strategy." Joint Force Quarterly 82, no. 3 (2016): 16–23.
- Niquet, Valérie. "Chapitre 5. La Chine: Une Modernisation des Pratiques de Guerre de l'Information." In Les Guerres de l'Information à l'Ère Numérique, edited by Clément Marange and Marc Quessard, 137–158. Paris: Presses Universitaires de France, 2021.
- Pana, Lukasz. "Artificial Intelligence and Moral Intelligence." tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society 4, no. 2 (2006): 254–264.
- Rosati, Alexandra, J. Stevens, Brian Hare, and Marc Hauser. "The Evolutionary Origins of Human Patience: Temporal Preferences in Chimpanzees, Bonobos, and Human Adults." Current Biology 17 (2007): 1663–1668.
- Roth, Alvin E., and J. Keith Murnighan. "Equilibrium Behavior and Repeated Play of the Prisoner's Dilemma." Journal of Mathematical Psychology 17, no. 2 (1978): 189–198.
- Taylor, Linnet. 2017. *What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally*. Big Data & Society 4 (2): 1–14.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.
- Gil-Garcia, J. Ramon, Jing Zhang, and Gabriel Puron-Cid. "Conceptualizing Smartness in Government: An Integrative and Multi-Dimensional View." Government Information Quarterly 33, no. 3 (2016): 524–534.
- Meijer, Albert, and Manuel Pedro Rodríguez Bolívar. "Governing the Smart City: A Review of the Literature on Smart Urban Governance." International Review of Administrative Sciences 82, no. 2 (2016): 392–408.