Research Institute for Security and Development Studies

Strategic Studies Quarterly

P-ISSN: 1735-0272 | E-ISSN: 2980-910X

Quarterly.risstudies.org

Received: May 20, 2026
Revised: June 27 , 2026
Accepted: August 7, 2026
Published: August 27, 2026

Rethinking "Just Intelligence Theory" in the Age of Artificial Intelligence: The Security Implications of the Transition to Algorithmic Governance

Alireza Ghazizadeh, Associate Professor and Faculty Member, Ministry of Science, Research and Technology, Tehran, Iran.

Corresponding AuthorEmail Address: ghazizadeh@isdsac.ir

Introduction

Rapid advances in artificial intelligence, big data, and algorithmic surveillance have fundamentally transformed the nature of intelligence power and the security practices of contemporary states. Under traditional security paradigms, intelligence activities were largely reactive, narrowly focused, and directed at specific targets, typically commencing only after a threat had emerged. In the contemporary digital order, however, society as a whole has become a continuous field of data extraction, analysis, and prediction. Using data-driven infrastructures, states collect and analyze vast quantities of information about citizens' communications, behavior, biometric characteristics, and geographical movements in real time. These developments have blurred the boundary between national security and pervasive surveillance, once again placing the ethical legitimacy of intelligence activities at the center of debates in security studies, political philosophy, and the ethics of technology.

In response to this theoretical gap, Ross Bellaby introduced "Just Intelli-

Article type: Original Research

How to cite this article: Ghazizadeh, A. (2026). Rethinking "Just Intelligence Theory" in the Age of Artificial Intelligence: The Security Implications of the Transition to Algorithmic Governance. Strategic *Studies Quarterly*, 29(2), 11-53. DOI: 10.22034/ssq.2026.582527.4378.

gence Theory" (JIT) in 2011, seeking to bring intelligence activities within the scope of ethical scrutiny. Drawing on the tradition of Just War Theory, Bellaby argues that, just as warfare must remain subject to ethical and legal constraints, intelligence activities cannot be justified solely by invoking security imperatives. Given their inherently intrusive nature, intelligence operations directly affect fundamental human rights, particularly the rights to privacy and individual autonomy. Their legitimacy must therefore be assessed in accordance with principles such as just cause, proportionality, necessity, discrimination, and legitimate authority.

A central limitation, however, is that Bellaby formulated his theory before algorithmic surveillance, artificial intelligence, and big-data-driven governance had reached their present levels of complexity and pervasiveness. Today, technology companies have become integral components of the intelligence and security ecosystem through their access to vast quantities of user data. Their growing role has weakened the boundaries between state surveillance, commercial surveillance, and social control. As a result, power in the digital age is no longer concentrated exclusively in the hands of the state. Instead, networks of state and non-state actors are involved in the generation, storage, and analysis of data. This transformation presents new challenges for Just Intelligence Theory and underscores the need to reconsider its underlying concepts.

Against this background, this study adopts an analytical-critical approach to reassess the explanatory and normative potential, as well as the limitations, of Just Intelligence Theory in the age of artificial intelligence. It addresses the following central research question: To what extent can this theory explain and provide an ethical assessment of algorithmic surveillance and the collection of security-related big data?

Methodology

This study is a theoretical investigation that, through a descriptive-analytical approach, critically examines Ross Bellaby's Just Intelligence Theory in light of the transformations associated with artificial intelligence, algorithmic surveillance, and security-related big data. The methodological framework comprises three levels of analysis. First, the study examines the conceptual foundations of Just Intelligence Theory and reconstructs its normative premises. Second, it critically analyzes technological developments relating to algorithmic security and data-driven governance. Third, it com-

paratively evaluates the theory's strengths and limitations in addressing the emerging structure of intelligence power. Data were collected through library-based and documentary research. The sources include books, scholarly articles, specialized reports, and relevant literature on intelligence ethics, surveillance studies, AI ethics, and data-driven governance.

Findings and Discussion

The findings suggest that the transition to data-driven governance requires a reassessment and redefinition of the core concepts of Just Intelligence Theory. The principal challenges facing the theory in the age of big data can be summarized as follows:

The theory's state-centric orientation: Although intelligence power is increasingly exercised through networks of states and technology companies, Bellaby's theory locates legitimate authority primarily within the framework of the nation-state. Consequently, it offers an inadequate conceptual basis for analyzing the hybrid relationship between states and digital platforms.

The erosion of the principle of discrimination: By turning society as a whole into a potential site of data collection, algorithmic surveillance undermines the distinction between suspects and ordinary citizens. Threat prediction requires algorithms to process vast quantities of publicly available data. As a result, intelligence gathering is no longer necessarily restricted to specific individuals or identified targets.

The challenge to proportionality in predictive security: In traditional security practices, proportionality required the scale of an intervention to correspond to the severity of an actual threat. Under algorithmic surveillance, however, interventions are frequently based on anticipated or probabilistic threats rather than established ones. This creates the possibility of an effectively unlimited expansion in the scope of security interventions.

The ambiguity of legitimate authority: The growing involvement of technology companies in security-related data infrastructures has exposed the limitations of a state-centric understanding of legitimate authority and contributed to the emergence of hybrid forms of authority.

The theory's limited account of algorithms as non-human agents: Bella-

by's framework rests on a traditional conception of human agency and does not provide a sufficiently developed account of moral responsibility for algorithms involved in security decision-making.

Despite these limitations, the findings indicate that Just Intelligence Theory retains considerable normative potential for critiquing digital securitization. Its emphasis on constraining power, accountability, transparency, and proportionality provides valuable conceptual tools for assessing and challenging the expansion of algorithmic surveillance.

Conclusion

This study concludes that the central problem with Just Intelligence Theory is not its loss of validity, but its failure to keep pace with the transformation of the structure of intelligence power. The theory emerged in a historical context in which the state was the principal security actor and data collection was relatively limited and targeted. In the age of artificial intelligence, however, the emergence of large-scale data infrastructures and automated algorithms, alongside the increasingly close interconnection between states and technology companies, has fundamentally altered the configuration of power.

Just Intelligence Theory therefore needs to be reformulated and expanded to accommodate developments such as algorithmic transparency, data rights, multilayered oversight, predictive ethics, and transnational accountability. Such a reconstruction could transform the theory from a predominantly state-centric framework into a critical approach capable of analyzing and regulating the exercise of power in a data-driven environment. By proposing an expanded framework for Just Intelligence Theory, this article highlights the importance of adapting its normative foundations to the changing realities of power in the age of artificial intelligence.

Keywords: *Just Intelligence Theory (JIT); Algorithmic Security; Data-Driven Surveillance; Artificial Intelligence; Big Data; Predictive Security; Intelligence Ethics; Digital Governance; Intelligence Power.*

Ethical Considerations

Compliance with Ethical Guidelines

This study was approved by the Ethics Committee of Research Institute for Security and Development Studies (ISDS), Tehran, Iran.

Funding Sources

This research received no external funding.

فصلنامه مطالعات راهبردی
شاپای چاپی: ۱۷۳۵-۰۷۲۷ | شاپای الکترونیکی: ۲۹۸۰-X۹۱۰
Quarterly.risstudies.org

تاریخ دریافت: ۱۴۰۵/۰۲/۳۰
تاریخ اصلاح: ۱۴۰۵/۰۴/۰۶
تاریخ پذیرش: ۱۴۰۵/۰۵/۱۶
تاریخ انتشار: ۱۴۰۵/۰۶/۰۵

بازاندیشی نظریه اطلاعات عادلانه در عصر هوش مصنوعی: پیامدهای امنیتی گذار به حکمرانی الگوریتمی

علیرضا قاضی‌زاده، گروه حکمرانی و نظام سیاسی، پژوهشکده مطالعات راهبردی، پژوهشگاه مطالعات امنیت و پیشرفت، تهران، ایران.
ایمیل نویسنده مسئول: ghazizadeh@isdsac.ir .

چکیده

تحولات شتابان در حوزه هوش مصنوعی، کلان‌داده و نظارت الگوریتمی موجب دگرگونی بنیادین در ماهیت قدرت اطلاعاتی و سازوکارهای امنیتی دولت‌های معاصر شده است. در چنین زمینه‌ای، نظریه اطلاعات عادلانهٔ راس بلابی، به‌مثابه یکی از چارچوب‌های مهم اخلاق اطلاعات، می‌کوشد فعالیت‌های اطلاعاتی را در نسبت با اصولی همچون تمایز، تناسب، ضرورت و اقتدار مشروع ارزیابی کند. بااین‌حال، گذار از الگوی امنیت سنتی به امنیت داده‌محور و پیش‌بینانه چالش‌های نظری و کاربردی جدیدی را برای این چارچوب اخلاقی ایجاد کرده است. مقاله حاضر، با رویکردی تحلیلی-انتقادی، به بازاندیشی ظرفیت‌ها و محدودیت‌های نظریه اطلاعات عادلانه در عصر هوش مصنوعی می‌پردازد و نشان می‌دهد که اگرچه این نظریه همچنان واجد توانمندی هنجاری برای نقد امنیت‌گرایی دیجیتال است، در تبیین ساختارهای شبکه‌ای قدرت اطلاعاتی و منطق الگوریتمی با کاستی‌های جدی مواجه است. یافته‌های پژوهش حاکی از آن است

نوع مقاله: پژوهشی اصیل
نحوه استناد به این مقاله: قاضی‌زاده، علیرضا. (۱۴۰۵). بازاندیشی نظریه اطلاعات عادلانه در عصر هوش مصنوعی: پیامدهای امنیتی گذار به حکمرانی الگوریتمی، فصلنامه مطالعات راهبردی، ۲۹ (۲)، ۱۱-۵۳، DOI: 10.22034/ssq.2026.582527.4378

که گذار به حکمرانی داده‌محور نیازمند بازتعریف مفاهیم بنیادین این نظریه ازجمله اقتدار مشروع، اصل تمایز و تناسب است. درنهایت، مقاله با ارائه الگویی توسعه‌یافته برای نظریه اطلاعات عادلانه، بر ضرورت انطباق آن با واقعیت‌های جدید قدرت در عصر هوش مصنوعی تأکید می‌کند.

واژگان کلیدی: نظریه اطلاعات عادلانه، امنیت الگوریتمی، نظارت داده‌محور، هوش مصنوعی، کلان‌داده، امنیت پیش‌بینانه، اخلاق اطلاعاتی، حکمرانی دیجیتال، قدرت اطلاعاتی.

مقدمه

تحولات فناورانه دهه‌های اخیر، به‌ویژه در حوزه هوش مصنوعی، کلان‌داده‌ها، یادگیری ماشین و سامانه‌های نظارت الگوریتمی، ساختار قدرت امنیتی و اطلاعاتی دولت‌ها را به شکلی بنیادین دگرگون کرده است. اگر در الگوهای کلاسیک امنیتی، فعالیت اطلاعاتی عمدتاً بر جمع‌آوری محدود اطلاعات درباره افراد، گروه‌ها یا دولت‌های مشخص متمرکز بود، در نظم دیجیتال معاصر کل جامعه به عرصه دائمی استخراج، تحلیل و پیش‌بینی داده تبدیل شده است. دولت‌ها و نهادهای امنیتی اکنون با اتکا به زیرساخت‌های داده‌محور، حجم عظیمی از اطلاعات ارتباطی، رفتاری، زیستی و مکانی شهروندان را در زمان واقعی جمع‌آوری و تحلیل می‌کنند. این تحول موجب شده است که مرز میان حفاظت ملی و نظارت فراگیر بیش‌از هر زمان دیگری مبهم شود و مسئله مشروعیت اخلاقی فعالیت اطلاعاتی بار دیگر به یکی از مسائل اساسی در مطالعات امنیتی، فلسفه سیاسی و اخلاق فناوری تبدیل گردد. گسترش نظارت دیجیتال پس‌از حملات ۱۱ سپتامبر، نقطه‌عطف مهمی در تحول دولت امنیتی مدرن به شمار می‌آید. دولت‌ها با توسل به گفتمان مبارزه با تروریسم، دامنه اختیارات اطلاعاتی خود را توسعه دادند و سازوکارهایی را پدید آوردند که امکان جمع‌آوری انبوه داده‌های شهروندان را فراهم می‌کرد. افشاگری‌های ادوارد اسنودن نشان داد که نظارت دولتی دیگر صرفاً معطوف به افراد مظنون نیست، بلکه بخش گسترده‌ای از ارتباطات و داده‌های شهروندان به‌صورت فراگیر ذخیره، طبقه‌بندی و تحلیل می‌شود. در چنین وضعیتی، بسیاری از مفاهیم سنتی مرتبط با حریم خصوصی، آزادی مدنی و حدود اقتدار دولت با بحران مواجه شده‌اند. آنچه پیش‌تر جاسوسی سنتی تلقی می‌شد، اکنون در قالب منطق عادی حکمرانی داده‌محور بازتولید و به بخشی از سازوکار روزمره دولت‌های مدرن تبدیل شده است.

ظهور هوش مصنوعی و تحلیل کلان‌داده‌ها ظرفیت سازمان‌های اطلاعاتی را از سطح شناسایی تهدید به سطح پیش‌بینی رفتار ارتقا داده است. الگوریتم‌های یادگیری ماشین می‌توانند الگوهای رفتاری افراد را بازسازی کنند، شبکه‌های ارتباطی را تحلیل نمایند و حتی احتمال گرایش‌های سیاسی، اجتماعی یا امنیتی را تخمین بزنند. این تحولْ مفهوم سنتی اطلاعات امنیتی را از فعالیتی واکنشی به نوعی حکمرانی پیش‌دستانه تبدیل کرده است؛ در این‌گونه حکمرانی، دولت صرفاً درپی کشف تهدیدهای بالفعل نیست، بلکه می‌کوشد تهدیدهای احتمالی آینده را نیز پیش‌بینی و مدیریت کند. پیامد چنین تغییری گسترش بی‌سابقه قدرت نظارتی و افزایش امکان مداخله در حریم خصوصی و خودمختاری شهروندان است. در این چارچوب، شهروندان بیش‌از آنکه به‌عنوان سوژه‌های حقوقی فهم شوند، به مجموعه‌ای از داده‌های با قابلیت پردازش و کنترل تقلیل می‌یابند.

با وجود این تحولات، بخش مهمی از ادبیات کلاسیک مطالعات اطلاعاتی و امنیتی همچنان تحت‌تأثیر رویکردهای واقع‌گرایانه قرار دارد؛ این رویکردها فعالیت اطلاعاتی را عمدتاً بر اساس کارآمدی عملیاتی، حفظ امنیت ملی و مدیریت تهدید تحلیل می‌کنند و مسائل اخلاقی را در حاشیه قرار می‌دهند (لوونتال، ۱۴۰۱: ۱۸۴). در این نگرش، ضرورت امنیتی اغلب توجیه‌کننده گسترش اختیارات اطلاعاتی تلقی می‌شود و پرسش از مشروعیت اخلاقی ابزارهای مورد استفاده اهمیت ثانویه می‌یابد. اما گسترش نظارت دیجیتال و جمع‌آوری انبوه داده‌ها نشان داده است که مسئله صرفاً مقابله با تهدیدهای امنیتی نیست، بلکه شکل‌گیری نوعی قدرت داده‌محور است که می‌تواند بر آزادی‌های مدنی، حریم خصوصی و حتی بنیان‌های دموکراسی اثر بگذارد. به همین دلیل، بسیاری از پژوهشگران معاصر بر این باور هستند که الگوهای سنتی مطالعات امنیتی دیگر قادر به تبیین پیچیدگی‌های اخلاقی قدرت اطلاعاتی در عصر دیجیتال نیستند.

در واکنش به این خلأ نظری، راس بلابی[1] در سال ۲۰۱۱ با طرح نظریه اطلاعات عادلانه[2] تلاش کرد فعالیت اطلاعاتی را وارد قلمرو قضاوت اخلاقی کند. بلابی با الهام از سنت نظریه جنگ عادلانه[3] استدلال می‌کند همان‌گونه که جنگ نمی‌تواند خارج از معیارهای اخلاقی

1. Ross Bellaby
2. Just Intelligence Theory
3. Just War Theory

و حقوقی قرار گیرد، فعالیت اطلاعاتی نیز نباید صرفاً بر مبنای ضرورت امنیتی توجیه شود. ازنظر او، عملیات اطلاعاتی به‌دلیل ماهیت مداخله‌گر خود- ازجمله شنود، نفوذ، جمع‌آوری داده و نظارت- به‌طور مستقیم با حقوق بنیادین انسان‌ها، به‌ویژه حق حریم خصوصی و خودمختاری فردی، در ارتباط است؛ بنابراین، مشروعیت آن باید تابع اصولی همچون علت عادلانه، تناسب، ضرورت، تمایز و اقتدار مشروع باشد (Bellaby, 2012:45). این نظریه را می‌توان یکی از نخستین تلاش‌های منسجم برای اخلاقی‌سازی قدرت اطلاعاتی در عصر دولت امنیتی دانست، تلاشی که درصدد ایجاد توازن میان الزامات امنیت و محدودیت‌های اخلاقی است.

بااین‌حال، مسئله اساسی آن است که نظریه بلابی در وضعیتی صورت‌بندی شده که نظارت الگوریتمی، هوش مصنوعی و حکمرانی مبتنی بر کلان‌داده هنوز به سطح کنونی از پیچیدگی و فراگیری نرسیده بود. در زمان طرح این نظریه، اگرچه مسئله شنود گسترده و جنگ علیه تروریسم مطرح بود، هنوز قدرت پلتفرم‌های دیجیتال، تحلیل پیش‌بینانه داده‌ها و همکاری عمیق دولت‌ها و شرکت‌های فناوری به شکل کنونی توسعه نیافته بود. امروزه شرکت‌های فناوری با در اختیار داشتن حجم عظیمی از داده‌های کاربران، به بخشی از اکوسیستم اطلاعاتی و امنیتی تبدیل شده‌اند و مرز میان نظارت دولتی، نظارت تجاری و کنترل اجتماعی را تضعیف کرده‌اند. درنتیجه، ساختار قدرت در عصر دیجیتال دیگر صرفاً دولت‌محور نیست، بلکه شبکه‌ای از بازیگران دولتی و فرادولتی در فرایند تولید، ذخیره و تحلیل داده مشارکت دارند. این وضعیت چالش‌های تازه‌ای برای نظریه اطلاعات عادلانه ایجاد کرده و ضرورت بازاندیشی مفاهیم بنیادین آن را آشکار ساخته است.

اهمیت پژوهش حاضر دقیقاً از همین تحول ناشی می‌شود. در جهان معاصر، داده به یکی از مهم‌ترین منابع قدرت سیاسی و امنیتی تبدیل شده است. دولت‌ها با استفاده از سامانه‌های هوشمند می‌توانند نه‌تنها تهدیدهای بالفعل، بلکه رفتارهای بالقوه و آینده‌محور را نیز شناسایی و مدیریت کنند. این وضعیت نوعی امنیت‌گرایی الگوریتمی را شکل داده که در آن، منطق پیش‌بینی و کنترل جایگزین منطق سنتی واکنش به تهدید شده است. پیامد چنین فرایندی، گسترش دامنه نظارت، تضعیف حریم خصوصی و شکل‌گیری اشکال جدید انضباط اجتماعی است. در برخی کشورها، فناوری‌هایی همچون تشخیص چهره، تحلیل احساسات، ردیابی مکانی و نظام‌های امتیازدهی اجتماعی به بخشی از ساختار

حکمرانی تبدیل شده است و این موضوع می‌تواند به ایجاد جامعه شفاف بینجامد، جامعه‌ای که در آن، شهروندان همواره در معرض مشاهده، تحلیل و ارزیابی قرار دارند.

ازلحاظ نظری، این پژوهش از این جهت می‌یابد که ادبیات موجود درباره نظریه اطلاعات عادلانه عمدتاً بر جاسوسی کلاسیک، شنود یا عملیات ضدتروریسم متمرکز بوده و کمتر به پیامدهای هوش مصنوعی و کلان‌داده برای این نظریه پرداخته است. حال‌آنکه تحول فناوری، مفاهیم بنیادینی همچون تناسب، تمایز، ضرورت و اقتدار مشروع را با چالش مواجه کرده است. برای مثال، هنگامی که الگوریتم‌ها به‌طور مستمر داده‌های میلیون‌ها شهروند را جمع می‌کنند، چگونه می‌توان اصل تمایز میان مظنون و شهروند عادی را حفظ کرد؟ یا زمانی که شرکت‌های فناوری در کنار دولت‌ها به بخشی از ساختار امنیت داده‌ای تبدیل می‌شوند، مفهوم اقتدار مشروع چگونه باید بازتعریف شود؟ همچنین تحلیل پیش‌بینانه داده‌ها مفهوم سنتی تناسب را نیز دگرگون می‌کند، زیرا مداخله امنیتی دیگر صرفاً مبتنی‌بر تهدید بالفعل نیست، بلکه بر مبنای احتمال و پیش‌بینی رفتار آینده صورت می‌گیرد.

تحولات یادشده نشان می‌دهد که نظریه بلابی، به‌رغم ظرفیت انتقادی مهم خود، برای مواجهه با اشکال نوین قدرت اطلاعاتی نیازمند توسعه مفهومی است. ضرورت عملی پژوهش نیز به پیامدهای اجتماعی و سیاسی نظارت الگوریتمی بازمی‌گردد. امروزه بسیاری از دولت‌ها به بهانه مقابله با تروریسم، جرائم سایبری یا تهدیدهای امنیتی، سامانه‌های گسترده پایش داده ایجاد کرده‌اند. این روند می‌تواند به عادی‌سازی مداخلات گسترده در زندگی شهروندان و تضعیف تدریجی آزادی‌های مدنی بینجامد. مسئله دیگر صرفاً امنیت نیست، بلکه آینده دموکراسی، نسبت میان دولت و شهروند و نیز امکان حفظ خودمختاری فردی در عصر حکمرانی داده‌ای است. از این منظر، بازخوانی نظریه اطلاعات عادلانه می‌تواند چارچوبی هنجاری برای نقد امنیت‌گرایی دیجیتال و ارزیابی اخلاقی قدرت داده‌ای معاصر فراهم سازد.

براین‌اساس، هدف اصلی پژوهش حاضر بررسی ظرفیت‌ها و محدودیت‌های نظریه اطلاعات عادلانه راس بلابی در مواجهه با نظارت الگوریتمی و جمع‌آوری کلان‌داده‌های امنیتی در عصر هوش مصنوعی است. پژوهش می‌کوشد نشان دهد که آیا اصول هنجاری مطرح‌شده در این نظریه همچنان می‌تواند مبنایی مؤثر برای سنجش مشروعیت اخلاقی

عملیات اطلاعاتی باشد یا اینکه تحولات فناورانه جدید مستلزم بازتعریف و توسعه این اصول است. افزون‌بر این، پژوهش درپی ارائه چارچوبی انتقادی برای تحلیل اخلاقی امنیت داده‌محور و پیوند میان اخلاق اطلاعات، فلسفه فناوری و مطالعات امنیتی است. اهداف فرعی پژوهش عبارت‌اند از: تبیین مبانی نظری و هنجاری نظریه اطلاعات عادلانه؛ بررسی ویژگی‌های نظارت الگوریتمی و حکمرانی مبتنی‌بر کلان‌داده؛ تحلیل چالش‌هایی که فناوری‌های نوین برای اصول تناسب، تمایز و اقتدار مشروع ایجاد کرده‌اند؛ و درنهایت، بیان خوانشی توسعه‌یافته از نظریه بلابی برای فهم پیچیدگی‌های اخلاقی قدرت اطلاعاتی در عصر دیجیتال. در همین راستا، پرسش اصلی پژوهش آن است که نظریه اطلاعات عادلانه تا چه میزان توانایی تبیین و ارزیابی اخلاقی نظارت الگوریتمی و جمع‌آوری کلان‌داده‌های امنیتی را دارد. همچنین پرسش‌های فرعی پژوهش بر مبانی فلسفی اصول هنجاری این نظریه، تحول ماهیت قدرت اطلاعاتی در نتیجهٔ نظارت الگوریتمی، چالش‌های ناشی از فناوری‌های هوشمند برای اصول اخلاقی کلاسیک، و تأثیر شرکت‌های فناوری بر مفهوم اقتدار مشروع متمرکز است.

فرضیه اصلی پژوهش بر این مبنا استوار است که نظریه اطلاعات عادلانه، به‌رغم ظرفیت مهم خود برای نقد امنیت‌گرایی دیجیتال، در مواجهه با سازوکارهای نوین نظارت الگوریتمی و قدرت پلتفرمی با محدودیت‌های مفهومی روبه‌روست و برای حفظ کارآمدی تحلیلی خود نیازمند بازتعریف اصول بنیادین به‌ویژه در حوزه تناسب، تمایز و اقتدار مشروع است. همچنین فرضیه‌های فرعی پژوهش بیان می‌کند که نظارت الگوریتمی با تبدیل کل جامعه به میدان بالقوه جمع‌آوری داده، اصل تمایز میان مظنون و شهروند عادی را تضعیف می‌کند؛ تحلیل پیش‌بینانه داده‌ها مفهوم سنتی تناسب را دچار بحران می‌سازد؛ ورود شرکت‌های فناوری به ساختار امنیت داده‌ای، مفهوم دولت‌محور اقتدار مشروع را ناکافی می‌کند؛ و درنهایت، پیوند نظریه اطلاعات عادلانه با اخلاق هوش مصنوعی و حقوق داده می‌تواند چارچوبی مناسب‌تر برای تحلیل قدرت اطلاعاتی معاصر فراهم سازد.

نوآوری اصلی این پژوهش در بازخوانی و توسعه نظریه اطلاعات عادلانه راس بلابی در بستر تحولات امنیتی عصر هوش مصنوعی و کلان‌داده است. اگرچه تاکنون مطالعات متعددی درباره اخلاق اطلاعات، نظارت دیجیتال و امنیت الگوریتمی انجام شده، اغلب این پژوهش‌ها یا در سطح فلسفه اخلاق باقی مانده‌اند یا صرفاً بر ابعاد فناورانه

و حقوقی تمرکز کرده‌اند. پژوهش حاضر می‌کوشد با ایجاد پیوند میان مطالعات امنیتی، اخلاق اطلاعات و حکمرانی الگوریتمی، چارچوبی تحلیلی را برای فهم دگرگونی ماهیت قدرت اطلاعاتی در عصر داده‌محور ارائه دهد. انتقال کانون تحلیل از امنیت واکنشی سنتی به امنیت پیش‌بینانه الگوریتمی از دیگر ابعاد نوآورانه است. در این مقاله نشان داده می‌شود که امنیت در عصر هوش مصنوعی دیگر صرفاً بر پاسخ به تهدیدهای بالفعل استوار نیست، بلکه بر مبنای تحلیل احتمالات رفتاری و پیش‌بینی داده‌محور عمل می‌کند. این تغییر، مفاهیم بنیادین نظریه بلابی همچون تناسب، تمایز و اقتدار مشروع را با چالش مواجه و ضرورت بازتعریف آن‌ها را آشکار می‌کند.

نوآوری دیگر پژوهشْ تحلیل نقش شرکت‌های فناوری به‌عنوان بازیگران جدید قدرت اطلاعاتی است. برخلاف چارچوب کلاسیک بلابی که عمدتاً دولت‌محور است، این مقاله نشان می‌دهد که ساختار قدرت امنیتی در عصر دیجیتال به شبکه‌ای ترکیبی از دولت‌ها، پلتفرم‌های فناوری و سامانه‌های هوش مصنوعی تبدیل شده است. از این منظر، مقاله حاضر مفهوم اکوسیستم چندلایه قدرت اطلاعاتی را برای توضیح نظم امنیتی جدید مطرح می‌کند؛ بنابراین، با ارائه الگویی توسعه‌یافته برای نظریه اطلاعات عادلانه، تلاش می‌شود چارچوبی هنجاری برای ارزیابی اخلاقی امنیت الگوریتمی ارائه گردد. در این چارچوب، مفاهیمی مانند شفافیت الگوریتمی، حق داده، نظارت چندلایه و اخلاق پیش‌بینانه در تحلیل قدرت اطلاعاتی معاصر جای می‌گیرند. این امر مقاله را از سطح بازخوانی نظری صرف فراتر برده، به پژوهشی دارای ظرفیت نظری و کاربردی در حوزه مطالعات راهبردی تبدیل می‌سازد.

پژوهش حاضر ازحیث هدف، در زمره پژوهش‌های بنیادی-نظری قرار دارد و با رویکردی توصیفی-تحلیلی به بررسی انتقادی نظریه اطلاعات عادلانه راس بلابی در بستر تحولات ناشی از هوش مصنوعی، نظارت الگوریتمی و کلان‌داده‌های امنیتی می‌پردازد. مسئله اصلی پژوهشْ تحلیل هنجاری و مفهومی نسبت میان اخلاق اطلاعات و اشکال نوین قدرت داده‌محور در عصر دیجیتال است؛ ازاین‌رو، روش تحقیق مبتنی‌بر تحلیل نظری، تفسیر مفهومی و نقد هنجاری انتخاب شده است. چارچوب روش‌شناختی پژوهش بر سه سطح تحلیلی استوار است: نخست، تحلیل مفهومی نظریه اطلاعات عادلانه و بازسازی مبانی هنجاری آن؛ دوم، تحلیل انتقادی تحولات فناورانه مرتبط با امنیت الگوریتمی و

حکمرانی داده‌محور؛ و سوم، ارزیابی تطبیقی ظرفیت‌ها و محدودیت‌های نظریه بلابی در مواجهه با ساختار جدید قدرت اطلاعاتی. روش گردآوری داده‌ها کتابخانه‌ای و اسنادی است و منابع پژوهش شامل کتاب‌ها، مقالات علمی، گزارش‌های تخصصی و ادبیات مرتبط با اخلاق اطلاعاتی، مطالعات نظارت، اخلاق هوش مصنوعی و حکمرانی داده‌محور است. پژوهش حاضر در چارچوب مطالعات میان‌رشته‌ای قرار می‌گیرد و تلاش می‌کند با تلفیق مطالعات امنیتی، فلسفه سیاسی و اخلاق فناوری، تصویری جامع از تحولات قدرت اطلاعاتی در عصر دیجیتال ارائه دهد.

الف) پیشینه پژوهش

ادبیات مربوط به اخلاق فعالیت اطلاعاتی و مشروعیت نظارت امنیتی، در مقایسه با حوزه‌هایی مانند اخلاق جنگ یا حقوق بین‌الملل، تا مدت‌ها از فقر نظری رنج می‌برد. بخش عمده مطالعات کلاسیک اطلاعاتی عمدتاً بر ابعاد عملیاتی، راهبردی و سازمانی سرویس‌های اطلاعاتی متمرکز بود و فعالیت اطلاعاتی را حوزه‌ای استثنایی می‌دانست که منطق بقا و امنیت ملی در آن بر ملاحظات اخلاقی غلبه دارد. در چنین بستری، به پرسش از مشروعیت اخلاقی جاسوسی، شنود، نفوذ و جمع‌آوری داده‌ها کمتر به‌مثابه مسئله‌ای مستقل توجه می‌شد. بااین‌حال، تحولات پس‌از جنگ سرد، گسترش جنگ علیه تروریسم، توسعه فناوری‌های نظارتی و افشاگری‌های مربوط به شنود گسترده دولت‌ها به‌تدریج موجب شکل‌گیری ادبیاتی شد که می‌کوشید فعالیت اطلاعاتی را از منظر اخلاق هنجاری ارزیابی کند.

نظریه اطلاعات عادلانه راس بلابی را باید در متن همین چرخش اخلاقی در مطالعات امنیتی و اطلاعاتی فهم کرد. یکی از نخستین جریان‌های نظری مرتبط با این حوزه، از دل سنت نظریه جنگ عادلانه پدید آمد. متفکرانی همچون مایکل والزر با طرح این ایده که حتی جنگ نیز نمی‌تواند خارج از قضاوت اخلاقی قرار گیرد، راه را برای تعمیم اصول هنجاری به سایر اشکال قدرت امنیتی هموار کردند (Walzer, 2015). اگرچه والزر مستقیماً بر فعالیت اطلاعاتی تمرکز نداشت، اما مفاهیمی چون تناسب، تمایز و ضرورت که در نظریه جنگ عادلانه مطرح شده بودند بعداً الهام‌بخش اصلی نظریه اطلاعات عادلانه شدند. درواقع، بلابی کوشید همان منطقی را به حوزه فعالیت اطلاعاتی منتقل کند که سنت جنگ عادلانه برای محدودکردن خشونت نظامی به کار می‌برد. از این منظر، آثار والزر را می‌توان یکی از

مبانی نظری غیرمستقیم شکل‌گیری نظریه اطلاعات عادلانه دانست.

در دهه‌های پایانی قرن بیستم، برخی پژوهشگران به‌طور محدود به مسئله اخلاق جاسوسی پرداختند. آثار افرادی مانند جان گلدمن و تونی اریکسون ازجمله نخستین تلاش‌ها برای ورود اخلاق به مطالعات اطلاعاتی بودند (Goldman, 2010; Erskine, 2008). تمرکز این پژوهش‌ها عمدتاً بر این پرسش بود که آیا جاسوسی ذاتاً غیراخلاقی است یا می‌توان در شرایطی آن را توجیه کرد؟ بخش مهمی از این ادبیات هنوز تحت‌تأثیر دوگانه کلاسیک میان واقع‌گرایی و آرمان‌گرایی قرار داشت. واقع‌گرایان امنیتی استدلال می‌کردند که دولت‌ها در محیطی آنارشیک و مبتنی‌بر تهدید عمل می‌کنند؛ بنابراین، فعالیت اطلاعاتی ضرورتی اجتناب‌ناپذیر برای بقاست و نمی‌توان آن را به‌طور کامل تابع اخلاق ساخت. درمقابل، برخی رویکردهای لیبرال و اخلاق‌گرا بر لزوم محدودسازی فعالیت اطلاعاتی ازطریق قواعد حقوقی و هنجاری تأکید کردند.

با وقوع حملات ۱۱ سپتامبر و آغاز جنگ علیه تروریسم، مسئله اخلاق اطلاعاتی وارد مرحله‌ای جدید شد. گسترش بازداشت‌های مخفی، شکنجه، شنود گسترده و عملیات فرامرزی موجی از نقدهای حقوق بشری و فلسفی را برانگیخت. در این دوره، آثار متعددی درباره نسبت میان امنیت و آزادی منتشر شد. پژوهشگرانی چون دیوید لیون با تمرکز بر مفهوم جامعه نظارتی نشان دادند که فناوری‌های جدید دولت‌ها را قادر ساخته است که شکل تازه‌ای از نظارت فراگیر ایجاد کنند؛ این شکل از نظارت دیگر محدود به مظنونان نیست، بلکه کل جامعه را در بر می‌گیرد. لیون استدلال می‌کرد که نظارت دیجیتال نه‌فقط ابزار امنیت، بلکه سازوکاری برای طبقه‌بندی، مدیریت و کنترل اجتماعی است. آثار او بر ادبیات انتقادی نظارت و مراقبت[1] تأثیر مهمی گذاشت و زمینه نظری مناسبی را برای تحلیل اخلاقی قدرت اطلاعاتی فراهم ساخت (Lyon, 2001).

پس‌از انتشار آثار بلابی، مجموعه‌ای از پژوهش‌ها در حوزه اخلاق اطلاعاتی[2] شکل گرفت که یا در جهت توسعه نظریه او بودند یا به نقد آن پرداختند. برخی پژوهشگران چارچوب بلابی را برای تحلیل عملیات ضدتروریسم، شنود گسترده و ترورهای هدفمند به کار گرفتند؛ آن‌ها کوشیدند نشان دهند که چگونه اصول تناسب و تمایز می‌تواند مبنایی

1. surveillance

2. ethics of intelligence

برای محدودسازی قدرت اطلاعاتی باشد. درمقابل، منتقدان واقع‌گرا استدلال کردند که فعالیت اطلاعاتی ذاتاً مبتنی‌بر پنهان‌کاری، فریب و نبود شفافیت است و بنابراین، نمی‌توان آن را به‌طور کامل در قالب اخلاق هنجاری محدود کرد. به باور این گروه، نظریه بلابی بیش‌ازحد آرمان‌گرایانه است و با منطق واقعی دستگاه‌های اطلاعاتی سازگاری کامل ندارد. در سال‌های اخیر، پژوهش‌هایی نیز درباره نسبت میان هوش مصنوعی و امنیت منتشر شده است. این مطالعات عمدتاً بر خطرهای ناشی از کنترل پلیسی، تشخیص چهره، تحلیل احساسات و الگوریتم‌های پیش‌بینی تهدید تمرکز دارند. بسیاری از این پژوهش‌ها نشان داده‌اند که الگوریتم‌های امنیتی می‌توانند به بازتولید تبعیض، نقض حریم خصوصی و تضعیف آزادی‌های مدنی بینجامد. بااین‌حال، بخش درخور توجهی از این ادبیات بیشتر ماهیت فنی یا حقوقی دارد و کمتر به توسعه نظریه‌های هنجاری موجود، ازجمله نظریه اطلاعات عادلانه، پرداخته است (گیل، ۱۳۸۹).

در ادبیات فارسی، مطالعات مربوط به نظریه اطلاعات عادلانه بسیار محدود است. بیشتر پژوهش‌های موجود در حوزه امنیت و اطلاعات یا رویکردی توصیفی و سازمانی دارند یا از منظر حقوقی به مسئله حریم خصوصی و نظارت (مانند مفادی از قانون مجازات اسلامی یا آئین دادرسی کیفری) می‌پردازند یا اخلاق اطلاعاتی را از منظر فضایل و رذایل اخلاقی در اسلام (ری‌شهری، ۱۳۹۷؛ منظرزاده، ۱۳۹۹؛ پژوهشکده تحقیقات اسلامی، ۱۳۸۶؛ مؤسسه آموزشی و پژوهشی امام خمینی(ره)، ۱۴۰۱) بررسی کرده اند که موضوع این پژوهش نیست. همچنین بخش عمده ادبیات فارسی درباره هوش مصنوعی و امنیتْ بر جنبه‌های فناورانه یا حقوق سایبری (مانیان و رونقی، ۱۴۰۰؛ محمدی و جعفری، ۱۳۹۷) متمرکز بوده و کمتر به پیوند میان اخلاق اطلاعات و نظارت الگوریتمی توجه کرده است. از همین روی، می‌توان گفت خلأ درخور توجهی درزمینهٔ تحلیل نظری و انتقادیِ نسبت میان نظریه اطلاعات عادلانه و تحولات جدید فناوری وجود دارد.

بررسی پیشینه پژوهش نشان می‌دهد که اگرچه نظریه بلابی توانسته است جایگاهی مهم در ادبیات اخلاق اطلاعاتی یابد، هنوز چند خلأ اساسی باقی مانده است. نخست آنکه بیشتر پژوهش‌ها نظریه اطلاعات عادلانه را در بستر جاسوسی کلاسیک یا عملیات ضدتروریسم تحلیل کرده و کمتر به چالش‌های ناشی از هوش مصنوعی و کلان‌داده پرداخته‌اند. دوم آنکه بخش عمده ادبیات موجود همچنان دولت را بازیگر اصلی قدرت

اطلاعاتی فرض می‌کند، درحالی‌که در نظم دیجیتال معاصر، شرکت‌های فناوری و پلتفرم‌های داده‌ای نیز نقش تعیین‌کننده‌ای یافته‌اند. سوم آنکه مفاهیمی مانند تناسب، تمایز و اقتدار مشروع در شرایط نظارت الگوریتمی دچار دگرگونی شده‌اند، اما بازخوانی نظری مناسبی درباره آن‌ها انجام نشده است.

بر همین اساس، مقاله حاضر می‌کوشد خلأ موجود در ادبیات را ازطریق بازخوانی انتقادی نظریه اطلاعات عادلانه در بستر نظارت الگوریتمی و کلان‌داده‌های امنیتی پر کند. نوآوری پژوهش در آن است که نظریه بلابی را نه صرفاً درزمینهٔ جاسوسی سنتی، بلکه در چارچوب حکمرانی داده‌ای، هوش مصنوعی امنیتی و قدرت پلتفرمی ارزیابی می‌کند؛ همچنین می‌کوشد امکان توسعه مفهومی این نظریه را در عصر امنیت الگوریتمی بررسی کند.

ب) مبانی نظری نظریه اطلاعات عادلانه و اخلاقی‌سازی قدرت اطلاعاتی

نظریه اطلاعات عادلانه راس بلابی را باید تلاشی دانست برای انتقال اخلاق هنجاری به حوزه‌ای که مدتی طولانی در وضعیت استثنایی و خارج از داوری اخلاقی قرار داشت. در سنت کلاسیک مطالعات امنیتی، فعالیت اطلاعاتی عمدتاً بر اساس منطق بقا، امنیت ملی و ضرورت استراتژیک تحلیل می‌شد و به همین دلیل، پرسش از مشروعیت اخلاقی آن یا نادیده گرفته می‌شد یا در مرتبه‌ای ثانویه قرار می‌گرفت. بلابی با الهام از سنت جنگ عادلانه استدلال می‌کند همان‌گونه که جنگ- با وجود پیوندش با خشونت و ضرورت امنیتی- نمی‌تواند از محدودیت‌های اخلاقی رها باشد، فعالیت اطلاعاتی نیز باید تابع اصول هنجاری مشخصی شود. ازنظر او، دستگاه‌های اطلاعاتی صرفاً ابزارهای فنی جمع‌آوری داده نیستند، بلکه نهادهایی هستند که به‌طور مستقیم در آزادی، حریم خصوصی و خودمختاری انسان‌ها مداخله می‌کنند؛ بنابراین، مشروعیت آن‌ها نمی‌تواند صرفاً از ضرورت امنیتی ناشی شود (Bellaby, 2012: 65).

بلابی نظریه خود را بر پایه نوعی اخلاق وظیفه‌گرا و حقوق‌محور بنا می‌کند. در این چارچوب، انسان نه ابژه‌ای برای حفاظت امنیتی، بلکه سوژه‌ای دارای کرامت و حقوق بنیادین تلقی می‌شود. به همین دلیل، دولت حتی در شرایط تهدید امنیتی نیز نمی‌تواند شهروندان را صرفاً وسیله‌ای برای تحقق امنیت جمعی در نظر بگیرد. این رویکرد به‌وضوح

متأثر از سنت کانتی است که بر اصل غایت بودن انسان تأکید می‌کند. بر اساس این منطق، هرگونه شنود، نظارت، نفوذ یا جمع‌آوری داده فقط زمانی مشروع است که با اصولی چون ضرورت، تناسب و احترام به حقوق بنیادین همراه باشد (Bellaby, 2016: 78).

در نظریه اطلاعات عادلانه، مشروعیت عملیات اطلاعاتی وابسته به چند اصل بنیادین است: نخست، علت عادلانه که بر اساس آن، فعالیت اطلاعاتی را فقط زمانی می‌توان توجیه کرد که برای مقابله با تهدیدی واقعی و جدی علیه امنیت عمومی انجام شود؛ دوم، اقتدار مشروع که تأکید می‌کند عملیات اطلاعاتی باید زیر نظارت قانونی و نهادهای پاسخ‌گو اجرا شود؛ سوم، تناسب که به محدود بودن دامنه مداخله در حریم خصوصی متناسب با سطح تهدید اشاره می‌کند؛ چهارم، تمایز که دولت را ملزم می‌کند میان افراد مظنون و شهروندان عادی تفاوت قائل شود (Bellaby, 2014: 115). این اصول برای محدودکردن گسترش نامحدود قدرت اطلاعاتی و جلوگیری از تبدیل امنیت به توجیهی برای نظارت فراگیر تلاش می‌کند.

بااین‌حال، چارچوب نظری بلابی عمدتاً در بستری صورت‌بندی شد که هنوز فناوری‌های داده‌محور و نظارت الگوریتمی به گستردگی امروز توسعه نیافته بودند. از همین روی، هرچند نظریه او بنیانی مهم برای اخلاقی‌سازی فعالیت اطلاعاتی فراهم می‌آورد، تحولات فناورانه جدید پرسش‌های تازه‌ای را پیش روی این نظریه قرار داده است. برای مثال، در وضعیتی که الگوریتم‌ها قادرند بدون هدف‌گذاری مشخص، داده‌های میلیون‌ها شهروند را جمع‌آوری و تحلیل کنند، مفهوم تمایز چگونه باید فهم شود؟ یا هنگامی که مداخله امنیتی بر اساس احتمال و پیش‌بینی انجام می‌گیرد، اصل تناسب چه معنایی می‌یابد؟ این پرسش‌ها نشان می‌دهد که نظریه اطلاعات عادلانه اگرچه همچنان ظرفیت انتقادی مهمی دارد، برای تحلیل قدرت اطلاعاتی در عصر دیجیتال نیازمند بازخوانی و توسعه مفهومی است.

۱. نظارت الگوریتمی و تحول ماهیت قدرت اطلاعاتی در عصر کلان‌داده

تحول دیجیتال در دهه‌های اخیر موجب شکل‌گیری الگوی جدیدی از قدرت شده که در آن، داده به یکی از اصلی‌ترین منابع کنترل سیاسی و امنیتی تبدیل شده است. در الگوهای سنتی امنیتی، فعالیت اطلاعاتی عمدتاً واکنشی بود، یعنی دستگاه‌های امنیتی

پس‌از شکل‌گیری تهدید وارد عمل می‌شدند. اما در عصر هوش مصنوعی و کلان‌داده، منطق امنیتی به‌سوی پیش‌بینی و پیشگیری حرکت کرده است. دولت‌ها و نهادهای اطلاعاتی اکنون می‌کوشند پیش‌از وقوع تهدید، ازطریق تحلیل داده‌های رفتاری و الگوریتم‌های پیش‌بینانه، الگوهای خطر را شناسایی و مدیریت کنند. این تحولْ مفهوم سنتی جاسوسی و نظارت را دگرگون و آن را به نوعی از حکمرانی داده‌محور تبدیل کرده است (برت، ۱۴۰۴: ۵۸). در این ساختار جدید، شهروندان نه‌فقط سوژه‌های حقوقی، بلکه منابع دائمی تولید داده هستند. گوشی‌های هوشمند، شبکه‌های اجتماعی، دوربین‌های نظارتی، سامانه‌های مکان‌یابی و پلتفرم‌های دیجیتال حجم عظیمی از داده‌های رفتاری تولید می‌کنند که می‌توان از آن‌ها برای اهداف امنیتی استفاده کرد. این وضعیتْ شکل تازه‌ای از قدرت مشاهده‌گر ایجاد کرده که دیگر به فضای فیزیکی محدود نیست، بلکه به درون زندگی روزمره و زیست دیجیتال انسان‌ها نفوذ کرده است. قدرت اطلاعاتی در عصر الگوریتمی نه‌فقط مبتنی‌بر مشاهده، بلکه بر پیش‌بینی و شکل‌دهی رفتار استوار است.

برای فهم این تحول، پژوهش حاضر از برخی مفاهیم نظری در مطالعات انتقادی نظارت بهره می‌گیرد؛ ازجمله مهم‌ترین آن‌ها ایده جامعه نظارتی[1] در آثار دیوید لیون است. لیون استدلال می‌کند که فناوری‌های نوین ارتباطی نظارت را از اقدامی استثنایی به بخشی از سازوکار عادی حکمرانی تبدیل کرده است. در چنین جامعه‌ای، افراد به‌طور مداوم طبقه‌بندی، ردیابی و تحلیل می‌شوند. این نظارت نه‌فقط امنیتی، بلکه اقتصادی و اجتماعی نیز هست و مرز میان دولت و بازار را در حوزه داده از میان می‌برد (Lyon, 2001: 48). در این پژوهش، نظریه اطلاعات عادلانه چارچوب نظری اصلی است و حکمرانی الگوریتمی نه چارچوب نظری مستقل، بلکه زمینه تحول‌یافته‌ای در نظر گرفته می‌شود که کفایت و محدودیت‌های این نظریه در مواجهه با آن ارزیابی می‌گردد.

۲. بازاندیشی مفاهیم تناسب، تمایز و اقتدار مشروع در عصر امنیت الگوریتمی

یکی از مهم‌ترین چالش‌های نظارت الگوریتمی برای نظریه اطلاعات عادلانه عبارت است از دگرگونی مفاهیم بنیادین آن. اصولی مانند تناسب، تمایز و اقتدار مشروع در بستر

1. Surveillance Society

جاسوسی سنتی و عملیات اطلاعاتی محدود شکل گرفته‌اند، اما در شرایطی که کل جامعه به میدان دائمی داده تبدیل شده، کاربست آن‌ها با دشواری‌های جدی مواجه می‌شود.

اصل تمایز[1] در نظریه بلابی بر این فرض استوار است که دولت باید میان افراد مظنون و شهروندان عادی تفاوت قائل شود و نظارت را صرفاً متوجه تهدیدهای مشخص کند. اما در منطق نظارت الگوریتمی، این تمایز به‌تدریج تضعیف می‌شود. الگوریتم‌ها برای پیش‌بینی تهدید به حجم عظیمی از داده‌های عمومی نیازمندند و بنابراین، جمع‌آوری اطلاعات دیگر محدود به افراد خاص نیست؛ درنتیجه، کل جامعه به موضوع بالقوه نظارت تبدیل می‌شود. این وضعیت، اصل برائت را نیز با بحران مواجه می‌سازد، زیرا افراد پیش‌از ارتکاب هرگونه جرم یا تهدید، بر اساس احتمال و الگوهای رفتاری تحلیل می‌شوند (Bellaby, 2012: 87). اصل تناسب[2] نیز در عصر امنیت پیش‌بینانه دچار تحول شده است. در الگوی سنتی، تناسب به معنای آن بود که میزان مداخله امنیتی باید متناسب با شدت تهدید بالفعل باشد. اما در نظارت الگوریتمی، مداخله اغلب بر مبنای تهدید احتمالی و پیش‌بینی‌شده صورت می‌گیرد. این امر سبب می‌شود دامنه مداخله امنیتی به‌طور بالقوه نامحدود شود، زیرا هر فردی می‌تواند در آینده به تهدید تبدیل شود. بنابراین، مفهوم تناسب دیگر صرفاً به رابطه میان تهدید موجود و میزان مداخله محدود نیست، بلکه به مسئله مدیریت ریسک و احتمال نیز گره خورده است (Bellaby, 2012: 95).

چالش دیگر به مفهوم اقتدار مشروع[3] مربوط می‌شود. در نظریه بلابی، اقتدار مشروع عمدتاً به دولت و نهادهای رسمی آن مربوط است (Bellaby, 2014: 114). اما در نظم داده‌محور معاصر، شرکت‌های فناوری و پلتفرم‌های دیجیتال نقش تعیین‌کننده‌ای در جمع‌آوری و تحلیل داده دارند. همکاری دولت‌ها و این شرکت‌ها نوعی ساختار هیبریدی قدرت اطلاعاتی ایجاد کرده که در آن، مرز میان نظارت دولتی و نظارت تجاری تضعیف شده است. در چنین وضعیتی، دیگر نمی‌توان صرفاً با ارجاع به دولتْ مشروعیت فعالیت اطلاعاتی را توضیح داد. مسئله اصلی این است که چه نهادی بر جریان داده و الگوریتم‌های تحلیلگر آن کنترل دارد و این کنترل تا چه اندازه پاسخ‌گو و شفاف است.

1. Principle of Distinction
2. Principle of Proportionality
3. Legitimate Authority

بر همین اساس، اگرچه نظریه اطلاعات عادلانه همچنان ظرفیت مهمی برای نقد امنیت‌گرایی دیجیتال دارد، برای حفظ کارآمدی تحلیلی خود نیازمند توسعه مفهومی است. این توسعه باید بتواند تحول قدرت اطلاعاتی از جاسوسی سنتی و محدود به حکمرانی الگوریتمی را توضیح دهد و مفاهیمی چون حریم خصوصی، تمایز، تناسب و اقتدار مشروع را متناسب با وضعیت جدید بازتعریف کند. در غیر این صورت، این خطر هست که چارچوب‌های کلاسیک اخلاق اطلاعات، دربرابر پیچیدگی‌های قدرت داده‌ای معاصر، ناکافی باقی بماند.

۳. امنیت پیش‌بینانه الگوریتمی

مفهوم امنیت پیش‌بینانه الگوریتمی[1] به نوعی از حکمرانی امنیتی اشاره می‌کند که در آن، تصمیم‌گیری‌های امنیتی نه بر اساس تهدیدهای بالفعل و رخ‌داده، بلکه بر مبنای تحلیل داده‌ها، الگوهای رفتاری، احتمالات آماری و پیش‌بینی الگوریتمیِ تهدیدات آینده انجام می‌گیرد. در این الگو، امنیت از وضعیت واکنشی سنتی- یعنی پاسخ به یک تهدید مشخص- به وضعیتی پیش‌دستانه و داده‌محور گذار می‌کند؛ وضعیتی که در آن، هدفِ اصلی شناسایی، پیش‌بینی و مدیریت خطرهای احتمالی پیش‌از وقوع آن‌هاست. براین‌اساس، امنیت پیش‌بینانه الگوریتمی در پژوهش حاضر صرفاً به معنای استفاده از فناوری در حوزه امنیت نیست، بلکه به معنای دگرگونی در منطق قدرت امنیتی است. در این ساختار، داده‌ها به مهم‌ترین منبع تولید دانش امنیتی تبدیل می‌شوند و الگوریتم‌ها با تحلیل کلان‌داده‌ها، الگوهای رفتاری افراد و گروه‌ها را ارزیابی و طبقه‌بندی می‌کنند. درنتیجه، مرز میان مظنون و شهروند عادی تضعیف می‌شود، زیرا هر فرد می‌تواند ریسکی بالقوه باشد و موضوع نظارت قرار گیرد. این وضعیتْ امنیت را از امر محدود و استثنایی به یک سازوکار دائم حکمرانی اجتماعی تبدیل می‌کند.

مبانی نظری این مفهوم در مقاله حاضر بر تلفیق چند سنت نظری استوار است. نخستین مبنا مطالعات انتقادی نظارت است، به‌ویژه آثار دیوید لیون که مفهوم جامعه نظارتی را مطرح می‌کند. از منظر لیون، فناوری‌های دیجیتال موجب شکل‌گیری نوعی نظارت دائمی و نامرئی شده‌اند که در آن، داده‌های روزمره افراد به ابزار مدیریت اجتماعی

1. Algorithmic Predictive Security

تبدیل می‌شود. این دیدگاه مبنای فهم گسترش نظارت داده‌محور در امنیت الگوریتمی است. دومین مبنای نظری ادبیات حکمرانی الگوریتمی[1] و اخلاق هوش مصنوعی است. در این چارچوب، الگوریتم‌ها صرفاً ابزارهای فنی تلقی نمی‌شوند، بلکه سازوکارهای تصمیم‌گیری سیاسی و امنیتی در نظر گرفته می‌شوند. این رویکرد نشان می‌دهد که چگونه تحلیل داده، یادگیری ماشین و سیستم‌های پیش‌بینی می‌توانند بر تخصیص منابع امنیتی، طبقه‌بندی تهدیدها و حتی محدودسازی آزادی‌های مدنی تأثیر بگذارند. بنابراین، امنیت پیش‌بینانه الگوریتمی در این مقاله در نسبت با نظریه اطلاعات عادلانه بلابی تحلیل می‌شود.

استدلال اصلی آن است که این الگوی جدیدِ امنیتی، اصول کلاسیک نظریه بلابی (به‌ویژه تمایز، تناسب و ضرورت) را با چالش مواجه کرده؛ زیرا در شرایطی که نظارت بر اساس احتمال و پیش‌بینی انجام می‌گیرد، تشخیص مرز تهدید واقعی و ریسک احتمالی دشوار می‌شود. از همین روی، پژوهش حاضر نتیجه می‌گیرد که ظهور امنیت پیش‌بینانه الگوریتمی مستلزم بازاندیشی در مبانی اخلاقی و هنجاری نظریه اطلاعات عادلانه است.

ج) تحلیل نقش اطلاعات عادلانه در حکمرانی الگوریتمی

در الگوی کلاسیک امنیتی، دولت‌ها تقریباً انحصار ابزارهای اطلاعاتی را در اختیار داشتند. دستگاه‌های امنیتی با استفاده از ابزارهایی مانند جاسوسی انسانی، شنود یا ردیابی ارتباطات و اطلاعات فعالیت می‌کردند و شهروندان نیز دولت را مرجع اصلی حفاظت امنیتی می‌دانستند. اما با گسترش اینترنت و اقتصاد داده، بخش بزرگی از اطلاعات انسانی در اختیار شرکت‌های خصوصی قرار گرفت. امروزه شرکت‌هایی مانند گوگل، متا، آمازون، هووایی، اپل و مایکروسافت حجم عظیمی از داده‌های رفتاری، ارتباطی و روان‌شناختی کاربران را ذخیره و تحلیل می‌کنند؛ این داده‌ها در بسیاری موارد از اطلاعات در اختیار دولت‌ها نیز گسترده‌تر و دقیق‌تر است. این تحول موجب شده است که قدرت اطلاعاتی از ساختار سنتی دولت‌محور خارج و به شبکه‌ای پیچیده از بازیگران دولتی و غیردولتی منتقل شود؛ بنابراین، توسعه حکمرانی الگوریتمی نشان می‌دهد که نظریه اطلاعات عادلانه در ابعاد مختلف به شرح زیر نیازمند بازاندیشی است.

1. Algorithmic Governance

۱. تحول ساختار قدرت اطلاعاتی در عصر نظارت الگوریتمی

تحولات فناورانه، در دهه‌های اخیر، ماهیت قدرت اطلاعاتی و سازوکارهای امنیتی را به‌صورت بنیادین دگرگون کرده است. اگر در الگوهای کلاسیک امنیتی، فعالیت اطلاعاتی عمدتاً به جمع‌آوری پنهان و مخفیانه اطلاعات درباره دشمنان، دولت‌های رقیب یا تهدیدهای بالفعل محدود می‌شد، در عصر دیجیتال قدرت اطلاعاتی به ساختاری فراگیر، شبکه‌ای و داده‌محور تبدیل شده است که بخش بزرگی از زندگی اجتماعی شهروندان در عرصه داخلی را نیز در بر می‌گیرد. ظهور فناوری‌هایی چون هوش مصنوعی، کلان‌داده، الگوریتم‌های یادگیری ماشین، اینترنت اشیا و زیرساخت‌های ابری موجب شده است که فعالیت اطلاعاتی از سطح کشف تهدید به سطح مدیریت و پیش‌بینی رفتار اجتماعی ارتقا یابد. در چنین شرایطی، قدرت اطلاعاتی دیگر صرفاً ابزاری در خدمت امنیت ملی نیست، بلکه به بخشی از منطق حکمرانی تبدیل شده است (قاضی زاده، ۱۳۹۱: ۱۴۹).

در ساختار سنتی امنیت، نظارت عمدتاً محدود، هدفمند و مبتنی‌بر تهدیدهای مشخص بود. دستگاه‌های اطلاعاتی معمولاً پس‌از ظهور بحران یا شکل‌گیری نشانه‌های روشن تهدید وارد عمل می‌شدند و فعالیت آنان بر مبنای اصل هدف‌گذاری مشخص انجام می‌گرفت. اما در عصر الگوریتمی این وضعیت تغییر کرده است. امروزه داده‌های انسانی به‌طور مستمر ازطریق گوشی‌های هوشمند، شبکه‌های اجتماعی، سامانه‌های پرداخت الکترونیک، موتورهای جست‌وجو، دوربین‌های شهری و پلتفرم‌های دیجیتال تولید می‌شوند. این داده‌ها نه‌فقط درباره رفتار آشکار افراد، بلکه درباره ترجیحات، روابط اجتماعی، الگوهای مصرف، موقعیت مکانی و حتی گرایش‌های روانی آنان اطلاعات فراهم می‌کنند؛ درنتیجه، نظارت دیگر به حوزه استثنایی امنیت محدود نیست، بلکه در متن زندگی روزمره انسان‌ها ادغام شده است.

این تحول را می‌توان گذار از قدرت اطلاعاتی سنتی به قدرت داده‌ای دانست. در الگوی سنتی، هدف اصلی دستیابی به اطلاعات محرمانه درباره تهدیدهای مشخص بود، اما در ساختار جدید، خود زندگی اجتماعی به منبع دائمی اطلاعات تبدیل شده است. اهمیت این تحول در آن است که قدرت اطلاعاتی دیگر صرفاً بر مشاهده استوار نیست، بلکه بر توانایی پیش‌بینی و هدایت رفتار نیز متکی شده است. الگوریتم‌های هوش مصنوعی می‌توانند ازطریق تحلیل داده‌های انبوه، الگوهای رفتاری افراد را

شناسایی و احتمال کنش‌های آینده آنان را پیش‌بینی کنند. به همین دلیل، امنیت در عصر دیجیتال ماهیتی پیش‌بینانه یافته است.

امنیت پیش‌بینانه یکی از مهم‌ترین ویژگی‌های نظم اطلاعاتی جدید است. در گذشته، دولت‌ها عمدتاً پس‌از وقوع تهدید واکنش نشان می‌دادند، اما اکنون می‌کوشند تهدید را پیش‌از تحقق، شناسایی و مدیریت کنند. این رویکرد بر این فرض استوار است که رفتار انسان‌ها الگوهای تحلیل‌پذیری دارد و ازطریق پردازش داده‌های کلان می‌توان احتمال وقوع رفتارهای خطرناک را پیش‌بینی کرد؛ بنابراین، امنیت دیگر صرفاً بر مقابله با تهدیدهای بالفعل استوار نیست، بلکه بر تحلیل احتمالات و پیش‌بینی خطرهای آینده مبتنی شده است. این تحول اگرچه از منظر کارآمدی امنیتی جذاب به نظر می‌رسد، در عمل مرز تهدید واقعی و احتمال آماری را تضعیف می‌کند (Andrejevic, 2013: 103).

در چنین ساختاری، مفهوم سنتی مظنون نیز تغییر یافته است. در الگوهای کلاسیک، افراد زمانی زیر نظارت قرار می‌گرفتند که شواهد مشخصی درباره رفتار مجرمانه یا تهدیدآمیز آنان وجود داشت، اما در امنیت پیش‌بینانه، افراد ممکن است صرفاً بر اساس الگوهای رفتاری، روابط اجتماعی یا تحلیل‌های آماری به‌عنوان تهدید بالقوه شناسایی شوند. این امر نشان‌دهنده گذار از مظنونیت مبتنی‌بر عمل به مظنونیت مبتنی‌بر احتمال است، گذاری که اصل تمایز میان شهروند عادی و فرد تهدیدزا را با بحران مواجه می‌سازد. درنتیجه، دامنهٔ نظارت از گروه‌های محدود به کل جامعه گسترش یافته است و همه افراد بالقوه موضوع تحلیل امنیتی قرار گرفته‌اند (Zoboff, 2015: 78).

نمونه‌های معاصر این تحول را می‌توان در برنامه‌های کنترل پلیسی مشاهده کرد. در برخی کشورهای غربی، الگوریتم‌های تحلیل داده برای پیش‌بینی مناطق یا افرادی به کار گرفته شده که احتمال وقوع جرم در آن‌ها بیشتر است. نرم‌افزارهایی مانند پرد پل[1] با تحلیل

---

۱. نرم‌افزار «loPderP» ازطریق هوش مصنوعی تلاش می‌کند احتمال وقوع جرم را پیش‌بینی کند. این سامانه ابتدا در ایالات متحده توسعه یافت و ازسوی برخی اداره‌های پلیس برای تخصیص نیرو و مدیریت گشت‌های امنیتی به کار گرفته شد. بعدها نام تجاری آن به acitiloeG تغییر یافت. ایده اصلی نرم‌افزار این است که جرائم کاملاً تصادفی نیستند، بلکه الگوهای زمانی و مکانی دارند. این نرم‌افزار داده‌های تاریخی جرائم مانند نوع جرم، زمان وقوع و موقعیت جغرافیایی را تحلیل می‌کند و سپس مناطقی را مشخص می‌سازد که احتمال وقوع جرم در آن‌ها بیشتر است. پلیس می‌تواند بر اساس این پیش‌بینی‌ها نیروهای خود را در آن مناطق مستقر کند.

داده‌های جرائم گذشته می‌کوشد الگوهای خطر را شناسایی کند. هرچند این فناوری‌ها با هدف افزایش کارآمدی امنیتی توسعه یافته، اما پژوهش‌ها نشان داده‌اند که الگوریتم‌ها اغلب تبعیض‌های موجود در داده‌های تاریخی را بازتولید می‌کند و موجب تمرکز نظارت بر اقلیت‌های قومی و طبقات فرودست می‌شود. این مسئله نشان می‌دهد که امنیت پیش‌بینانه صرفاً ابزار فنی بی‌طرف نیست، بلکه می‌تواند به بازتولید ساختارهای نابرابر قدرت بینجامد. گسترش فناوری تشخیص چهره و نظارت بی‌درنگ نیز بخشی از همین تحول است. برخی دولت‌ها با بهره‌گیری از شبکه‌های گسترده دوربین‌های هوشمند، امکان ردیابی مداوم شهروندان را فراهم کرده‌اند. از این فناوری‌ها نه‌تنها برای مقابله با جرائم، بلکه برای مدیریت اجتماعی و کنترل رفتار عمومی استفاده می‌شود. در چنین وضعیتی، امنیت از سطح واکنش به تهدید به سطح حکمرانی دائمی جامعه ارتقا می‌یابد و مرز امنیت، مدیریت اجتماعی و کنترل سیاسی به‌تدریج تضعیف می‌شود.

پس‌از حملات ۱۱ سپتامبر نیز بسیاری از دولت‌های غربی به‌سوی توسعه زیرساخت‌های نظارت دیجیتال حرکت کردند. افشاگری‌های ادوارد اسنودن نشان داد که نهادهای اطلاعاتی ایالات متحده حجم عظیمی از داده‌های ارتباطی شهروندان را ازطریق برنامه‌هایی مانند پریسم[1] جمع‌آوری می‌کردند. تماس‌های تلفنی، ایمیل‌ها، جست‌وجوهای اینترنتی و فعالیت‌های شبکه‌های اجتماعی به داده‌هایی تبدیل شدند که برای تحلیل الگوریتمی و شناسایی الگوهای تهدید مورد استفاده قرار می‌گرفتند. این تحول نشان داد که فعالیت اطلاعاتی دیگر محدود به جاسوسی سنتی و هدفمند نیست، بلکه بر جمع‌آوری گسترده داده‌های کل جامعه استوار شده است. دراین‌میان، شرکت‌های فناوری به بازیگران اصلی قدرت اطلاعاتی تبدیل شده‌اند. در الگوهای کلاسیک، دولت‌ها تقریباً انحصار ابزارهای اطلاعاتی را در اختیار داشتند، اما در نظم داده‌محور معاصر، شرکت‌هایی مانند گوگل، متا،

---

۱. «MSIRP» یک برنامه نظارت الکترونیکی فوق محرمانه متعلق به آژانس امنیت ملی آمریکا (ASN) بود که در سال ۳۱۰۲ ازطریق افشاگری‌های ادوارد اسنودن علنی شد. این برنامه بخشی از ساختار گسترده نظارت دیجیتال دولت آمریکا پس‌از حملات ۱۱ سپتامبر به شمار می‌رفت و هدف رسمی آن، جمع‌آوری اطلاعات برای مقابله با تروریسم و تهدیدهای امنیتی اعلام شده بود. بر اساس اسناد منتشرشده، MSIRP به ASN اجازه می‌داد با همکاری شرکت‌های بزرگ فناوری، به داده‌های کاربران اینترنتی دسترسی پیدا کند.

آمازون و اپل حجم عظیمی از داده‌های انسانی را ذخیره و تحلیل می‌کنند. این شرکت‌ها ازطریق الگوریتم‌های پیچیده، الگوهای رفتاری، علایق، روابط اجتماعی و گرایش‌های سیاسی کاربران را تحلیل می‌کنند. به همین دلیل، قدرت اطلاعاتی دیگر صرفاً در اختیار دولت‌ها نیست، بلکه در شبکه‌ای از روابط دولت‌ها، شرکت‌های فناوری و زیرساخت‌های دیجیتال توزیع شده است. اهمیت این مسئله زمانی آشکارتر می‌شود که دولت‌ها برای اهداف امنیتی به داده‌های این شرکت‌ها دسترسی پیدا می‌کنند. افشاگری‌های اسنودن نشان داد که همکاری گسترده‌ای میان نهادهای اطلاعاتی و شرکت‌های فناوری وجود داشته است. دولت‌ها در عصر دیجیتال دیگر نیازی ندارند همه زیرساخت‌های نظارتی را خود ایجاد کنند، بلکه می‌توانند از داده‌هایی بهره ببرند که پیش‌تر، شرکت‌های خصوصی آن‌ها را برای اهداف تجاری جمع کرده‌اند؛ درنتیجه، نوعی هم‌پوشانی میان نظارت تجاری و نظارت امنیتی شکل گرفته است.

این وضعیتْ ساختار جدیدی از قدرت اطلاعاتی ایجاد کرده است که می‌توان آن را قدرت اطلاعاتی هیبریدی[1] نامید؛ در این ساختار نو، مرز میان دولت و بازار، امنیت و اقتصاد، و نظارت عمومی و خصوصی تضعیف شده است. قدرت اطلاعاتی هیبریدی نوعی ساختار شبکه‌ای قدرت در عصر دیجیتال است که در آن، دولت‌ها، شرکت‌های فناوری و سامانه‌های الگوریتمی به‌صورت مشترک در تولید، پردازش، تحلیل و کنترل داده‌های انسانی مشارکت می‌کنند و از این طریق بر امنیت، اقتصاد و رفتار اجتماعی اثر می‌گذارند (Zuboff, 2015: 80). در این وضعیت، قدرت جمع‌آوری، تحلیل و کنترل اطلاعات دیگر فقط در اختیار دولت‌ها نیست، بلکه میان دولت، شرکت‌های فناوری، پلتفرم‌های دیجیتال و سامانه‌های هوش مصنوعی توزیع شده و این بازیگران به‌صورت شبکه‌ای و مشترک عمل می‌کنند. در این ساختار، امنیت، اقتصاد دیجیتال و فناوری به یکدیگر پیوند می‌خورند و مدیریت داده‌ها ازطریق همکاری یا هم‌پوشانی نهادهای دولتی و خصوصی انجام می‌شود. ویژگی‌های اصلی قدرت اطلاعاتی هیبریدی عبارت‌اند از:

- ادغام دولت و شرکت‌های فناوری؛
- بازیگران متکثر، نوظهور، دولتی و غیردولتی؛

1. Hybrid Intelligence Power

- وابستگی امنیت به کلان‌داده و هوش مصنوعی؛
- نظارت گسترده و الگوریتمی؛
- مبهم شدن مرز میان امنیت و اقتصاد دیجیتال؛
- انتقال بخشی از قدرت سیاسی به پلتفرم‌های داده‌محور.

شرکت‌های فناوری داده‌های کاربران را برای اهداف اقتصادی جمع‌آوری می‌کنند، اما همین داده‌ها می‌توانند برای تحلیل امنیتی و مدیریت اجتماعی نیز استفاده شوند؛ درنتیجه، حکمرانی داده‌محور نه‌فقط یک ساختار امنیتی، بلکه بخشی از منطق کلی قدرت در عصر دیجیتال است.

این تحول، مفهوم اقتدار مشروع را نیز با چالش مواجه کرده است. نظریه‌های کلاسیک امنیتی، ازجمله نظریه اطلاعات عادلانه راس بلابی، عمدتاً دولت را بازیگر اصلی قدرت اطلاعاتی فرض می‌کردند و مشروعیت فعالیت اطلاعاتی را به اقتدار قانونی دولت پیوند می‌دادند. اما در عصر پلتفرم‌ها، قدرت اطلاعاتی میان دولت و شرکت‌های فناوری توزیع شده است؛ بنابراین، دیگر نمی‌توان صرفاً با ارجاع به دولت، مشروعیت نظارت را توضیح داد. پرسش اصلی این است که چه نهادی کنترل داده‌ها و الگوریتم‌ها را در اختیار دارد و این قدرت تا چه اندازه شفاف و پاسخ‌گوست.

در کنار این مسئله، نظارت الگوریتمی بر مفهوم حریم خصوصی نیز تأثیر عمیقی گذاشته است. در دموکراسی‌های کلاسیک، شهروندان حوزه‌ای خصوصی و مصون از مداخله دولت داشتند، اما در نظم داده‌محور، بخش بزرگی از زندگی روزمره ازطریق پلتفرم‌های دیجیتال واسطه‌گری می‌شود. کاربران برای مشارکت در حیات اجتماعی ناگزیرند داده‌های شخصی خود را در اختیار پلتفرم‌ها قرار دهند و همین داده‌ها می‌توانند در فرایندهای امنیتی به کار گرفته شوند؛ درنتیجه، مرز میان رضایت داوطلبانه و اجبار ساختاری مبهم شده است.

ظهور هوش مصنوعی نیز این روند را تشدید کرده است. توسعه الگوریتم‌های یادگیری ماشین نیازمند دسترسی به حجم عظیمی از داده‌هاست و شرکت‌های فناوری به‌دلیل دسترسی گسترده به داده‌های کاربران، به بازیگران اصلی این حوزه تبدیل شده‌اند. دولت‌ها نیز برای بهره‌گیری از فناوری‌های پیشرفته امنیتی ناگزیر به همکاری با این شرکت‌ها هستند. این وابستگی قدرت نظارتی دولت‌ها را به زیرساخت‌های خصوصی

گره زده و نوعی ساختار ترکیبی از قدرت دولتی و قدرت پلتفرمی ایجاد کرده است. در چنین شرایطی، شهروندان به‌تدریج در وضعیت شفافیت اجباری قرار می‌گیرند. بخش عمده تعاملات اجتماعی، اقتصادی و فرهنگی آنان ازطریق سامانه‌هایی انجام می‌شود که داده‌هایشان را ثبت و تحلیل می‌کنند. هر کنش دیجیتال می‌تواند موضوع تحلیل امنیتی قرار گیرد و همین مسئله بر آزادی بیان، مشارکت سیاسی و خودمختاری فردی تأثیر می‌گذارد. شهروندان ممکن است به‌دلیل آگاهی از امکان نظارت دائمی، رفتار خود را کنترل و محدود کنند. بنابراین، نظارت الگوریتمی نه‌فقط یک مسئله امنیتی، بلکه مسئله‌ای سیاسی و اجتماعی است که بر ساختار دموکراسی و مفهوم آزادی تأثیر می‌گذارد.

تحول قدرت اطلاعاتی در عصر نظارت الگوریتمی نشان‌دهنده گذار از الگوی سنتی جاسوسی به نوعی حکمرانی داده‌محور است که در آن، قدرت نه‌فقط بر مشاهده، بلکه بر پیش‌بینی و هدایت رفتار اجتماعی استوار است. امنیت پیش‌بینانه، تحلیل کلان‌داده‌ها و نقش فزاینده شرکت‌های فناوری موجب شده‌اند که مرز میان امنیت، اقتصاد و حکمرانی به‌تدریج از میان برود. این وضعیتْ نظریه‌های کلاسیک اخلاق اطلاعات، ازجمله نظریه اطلاعات عادلانه بلابی، را با چالشی اساسی مواجه ساخته است؛ زیرا اصولِ شکل‌گرفته بر مبنای نظارت محدود و هدفمند اکنون باید دربرابر ساختاری بازتعریف شوند که در آن، کل جامعه به موضوع دائمی استخراج، تحلیل و مدیریت داده تبدیل شده است.

۲. چالش‌های هنجاری نظریه اطلاعات عادلانه در مواجهه با امنیت داده‌محور

تحولات عصر کلان‌داده، هوش مصنوعی و نظارت الگوریتمی بسیاری از بنیان‌های نظریه اطلاعات عادلانه راس بلابی را با بحران مواجه کرده است. یکی از مهم‌ترین این بنیان‌ها اصل تمایز است؛ این اصل بر ضرورت تفکیک میان افراد مظنون و شهروندان عادی تأکید می‌کند و مشروعیت مداخله اطلاعاتی را به وجود ظن معقول محدود می‌سازد. در الگوهای کلاسیک امنیتی، دستگاه‌های اطلاعاتی ابتدا تهدید را ازطریق قراین و شواهد می‌شناسانند و سپس اطلاعات را گرد می‌آورند، اما در نظام داده‌محور این منطق وارونه شده است. اکنون دولت‌ها ابتدا حجم عظیمی از داده‌های عمومی را جمع‌آوری می‌کنند و سپس الگوریتم‌ها از دل این داده‌ها الگوهای تهدید را بیرون می‌آورند؛ درنتیجه، نظارت دیگر بر مبنای سوءظن

قبلی آغاز نمی‌شود، بلکه خود داده‌ها منشأ تولید سوءظن هستند. این تحول موجب شده است مرز میان مظنون و شهروند عادی به‌تدریج از میان برود و نوعی مظنونیت فراگیر شکل گیرد که در آن، همه افراد بالقوه موضوع تحلیل امنیتی باشند.

گسترش فناوری‌های دیجیتال نقشی اساسی در این تغییر ایفا کرده است. گوشی‌های هوشمند، شبکه‌های اجتماعی، سامانه‌های مکان‌یابی، دوربین‌های شهری و پلتفرم‌های مالی روزانه حجم عظیمی از داده‌های رفتاری تولید می‌کنند. این داده‌ها نه‌تنها ارتباطات افراد، بلکه عادات روزمره، روابط اجتماعی، گرایش‌های سیاسی و حتی وضعیت روانی آنان را آشکار می‌سازد (Nissenbaum, 2022: 98).

در چنین شرایطی، دستگاه‌های اطلاعاتی بدون نیاز به جاسوسی کلاسیک می‌توانند تصویری دقیق از زندگی شهروندان ترسیم کنند. ازآنجاکه الگوریتم‌های هوش مصنوعی برای پیش‌بینی تهدید به داده‌های گسترده نیازمندند، جمع‌آوری انبوه اطلاعات به پیش‌شرط امنیت تبدیل شده است؛ بنابراین، اصل تمایز عملاً بی‌معنا می‌شود، زیرا تفکیک میان مظنون و غیرمظنون پس‌از جمع‌آوری داده‌ها انجام می‌گیرد، نه پیش‌از آن. افشاگری‌های ادوارد اسنودن نشان داد که آژانس امنیت ملی آمریکا داده‌های ارتباطی میلیون‌ها شهروند را ذخیره و تحلیل می‌کرد. دولت این اقدامات را برای پیشگیری از تروریسم ضروری می‌دانست، اما منتقدان استدلال کردند که چنین نظارتی اصل تمایز را نقض می‌کند، زیرا همه شهروندان بدون وجود ظن مشخص در معرض رصد قرار گرفته‌اند. در این الگو، نظارت از حالت مبتنی‌بر سوءظن به نظارت مبتنی‌بر داده تغییر یافته است؛ الگوریتم‌ها، بر اساس احتمالات آماری، افراد را به‌عنوان تهدید بالقوه طبقه‌بندی می‌کنند، نه بر اساس اعمال واقعی آنان. درنتیجه، افراد ممکن است بدون ارتکاب جرم صرفاً به‌دلیل شباهت‌های آماری تحت مراقبت قرار گیرند.

ازسوی‌دیگر، این وضعیت اصل برائت را نیز تضعیف می‌کند. در حقوق مدرن، افراد بی‌گناه فرض می‌شوند مگر آنکه جرمشان ثابت شود، اما امنیت پیش‌بینانه شهروندان را به سوژه‌های بالقوه خطر تبدیل می‌کند. هر رفتار دیجیتال می‌تواند موضوع تحلیل امنیتی قرار گیرد و همین امر نوعی وارونگی در منطق حقوقی ایجاد می‌کند. افزون‌بر این، الگوریتم‌های امنیتی اغلب حامل تبعیض‌های اجتماعی هستند. چون این الگوریتم‌ها بر اساس داده‌های گذشته آموزش می‌بینند، سوگیری‌های نژادی، قومی و طبقاتی موجود

در داده‌ها را بازتولید می‌کنند. در برخی سامانه‌های پلیسی آمریکا، محله‌های فقیرنشین و اقلیت‌های قومی به‌طور نامتناسب به‌عنوان مناطق پرخطر شناسایی شدند و همین امر به افزایش نظارت و حضور پلیس در این مناطق انجامید. در چین نیز سامانه‌های تشخیص چهره و تحلیل داده نظارت گسترده‌ای بر اقلیت اویغور اِعمال کرده و ویژگی‌های فرهنگی و مذهبی آنان را به شاخص‌های خطر امنیتی مبدل ساخته است.

در چنین فضایی، مفهوم حریم خصوصی نیز دگرگون شده است. مسئله دیگر فقط محرمانه بودن اطلاعات نیست، بلکه امکان رهایی از تحلیل دائمی داده‌هاست. حتی داده‌های ظاهراً کم‌اهمیت می‌توانند ازطریق الگوریتم‌ها به اطلاعات حساسی درباره هویت، گرایش سیاسی یا روابط شخصی افراد تبدیل شوند. دولت‌ها اغلب این نظارت گسترده را با استناد به ضرورت امنیتی توجیه می‌کنند و مدعی‌اند بدون دسترسی به داده‌های وسیع، امکان مقابله با تهدیدهای نوین وجود ندارد. اما منتقدان هشدار می‌دهند که چنین منطقی به عادی‌سازی نظارت دائمی می‌انجامد و اصل تمایز را از میان می‌برد.

اصل تناسب نیز در نظام‌های مبتنی‌بر هوش مصنوعی با بحران مشابهی روبه‌رو شده است. این اصل تأکید می‌کند که مداخله امنیتی باید متناسب با شدت تهدید باشد و دولت‌ها حق ندارند به بهانه امنیت، آزادی‌های بنیادین را به‌طور نامحدود محدود کنند. در الگوهای سنتی، تناسب را می‌شد در چارچوب عملیات محدود و هدفمند ارزیابی کرد، اما در عصر داده‌محور، کل جامعه به موضوع دائمی نظارت تبدیل شده است. هوش مصنوعی امنیتی، برای تحلیل الگوهای رفتاری، به حجم عظیمی از داده‌ها نیاز دارد و همین امر دامنه مداخله را فراتر از تهدیدهای واقعی گسترش می‌دهد.

امنیت پیش‌بینانه بر پایه احتمال تهدید عمل می‌کند، نه تهدید بالفعل. الگوریتم‌ها می‌کوشند آینده را پیش‌بینی کنند و به همین دلیل، هر فرد بالقوه می‌تواند زیر نظارت قرار گیرد. این منطق باعث می‌شود دامنه مداخله امنیتی همواره درحال گسترش باشد، زیرا دولت‌ها می‌توانند ادعا کنند که داده بیشتر به معنای امنیت بیشتر است. برنامه‌های نظارتی پس‌از ۱۱ سپتامبر نمونه‌ای روشن از این وضعیت بود؛ جایی که دولت آمریکا جمع‌آوری گسترده داده‌ها را با منطق پیشگیری توجیه کرد، درحالی‌که بسیاری از افراد زیر نظارت هیچ ارتباط مستقیمی با تروریسم نداشتند.

بحران تناسب فقط به گستردگی نظارت محدود نیست، بلکه به ماهیت خود

الگوریتم‌ها نیز مربوط می‌شود. بسیاری از سامانه‌های هوش مصنوعی به‌صورت جعبه سیاه عمل می‌کند؛ یعنی فرایند تصمیم‌گیری آن‌ها شفاف نیست و حتی طراحانشان نمی‌توانند دقیقاً توضیح دهند چرا فردی خطرناک تشخیص داده شده است. این نبود شفافیت موجب دشواری ارزیابی تناسب می‌شود. علاوه‌بر این، چون الگوریتم‌ها بر اساس داده‌های تاریخی آموزش می‌بینند، تبعیض‌های گذشته را بازتولید می‌کنند و نظارت نامتناسب بر گروه‌های خاص را تشدید می‌سازند.

در چین، شبکه‌های عظیم تشخیص چهره و تحلیل کلان‌داده نمونه‌ای از گسترش منطق امنیت مطلق به شمار می‌آید؛ در این منطق، هر سطحی از نظارت برای حفظ ثبات سیاسی توجیه‌پذیر است. همچنین، مفهوم ضرورت در عصر هوش مصنوعی تغییر یافته است. در گذشته، مداخله گسترده فقط زمانی موجه بود که هیچ راه کم‌ضررتری وجود نداشت، اما اکنون خود فناوری دامنه ضرورت را گسترش می‌دهد. هرچه توان تحلیل داده بیشتر می‌شود، دولت‌ها نیز داده‌های بیشتری را ضروری می‌دانند؛ درنتیجه، اصل تناسب دربرابر منطق کارآمدی فناورانه تضعیف می‌شود («سیستم اعتباری چین»، ۱۴۰۴: ۳۹).

مفهوم ضرورت امنیتی نیز در عصر کلان‌داده دگرگون شده است. در گذشته، ضرورت امنیتی به وضعیتی استثنایی و تهدیدهای جدی محدود بود، اما اکنون به توجیهی برای جمع‌آوری دائمی داده‌ها تبدیل شده است. دولت‌ها استدلال می‌کنند که تهدیدهای معاصر ماهیتی پنهان و پیش‌بینی‌ناپذیر دارند و فقط ازطریق تحلیل کلان‌داده می‌توان آن‌ها را شناسایی کرد؛ درنتیجه، ضرورت امنیتی از وضعیتی استثنایی به بخشی از ساختار عادی حکمرانی تبدیل شده است. افشاگری‌های اسنودن بار دیگر نشان داد که چگونه دولت آمریکا با استناد به مقابله با تروریسم، داده‌های میلیون‌ها نفر را ذخیره و تحلیل می‌کرد. منتقدان تأکید می‌کردند که در این حالت، مفهوم ضرورت به ابزاری برای مشروعیت‌بخشی به نظارت دائمی تبدیل شده است. هرچه ظرفیت تحلیل داده افزایش می‌یابد، دامنه اطلاعاتی که ضروری تلقی می‌شوند نیز گسترده‌تر می‌شود. در دوران همه‌گیری کووید-۱۹ هم بسیاری از دولت‌ها با استفاده از اپلیکیشن‌های ردیابی و داده‌های مکانی، زیرساخت‌های گسترده نظارتی ایجاد کردند که خطر تثبیت نظارت دائمی را به همراه داشت.

یکی دیگر از تحولات مهم، بحران مفهوم اقتدار مشروع است. بلابی اقتدار مشروع را در چارچوب دولت ملی تعریف می‌کرد و معتقد بود فقط نهادهای دارای مشروعیت سیاسی و

قانونی حق انجام فعالیت اطلاعاتی دارند. اما در عصر داده‌محور، قدرت اطلاعاتی دیگر در انحصار دولت‌ها نیست. شرکت‌های فناوری مانند گوگل، متا، اپل، هوآوی و آمازون حجم عظیمی از داده‌های انسانی را در اختیار دارند و به بازیگران اصلی ساختار اطلاعاتی تبدیل شده‌اند. این وضعیت موجب شده است قدرت اطلاعاتی میان دولت‌ها، شرکت‌های خصوصی و سامانه‌های الگوریتمی توزیع شود. اسناد اسنودن نشان دادند که آژانس امنیت ملی آمریکا ازطریق همکاری با شرکت‌های فناوری به داده‌های کاربران دسترسی گسترده داشته است. در چنین ساختاری، مرز میان نظارت دولتی و زیرساخت‌های خصوصی از میان رفته و نوعی اقتدار هیبریدی شکل گرفته است. دولت‌ها برای اعمال قدرت امنیتی به شرکت‌های فناوری وابسته‌اند و شرکت‌ها نیز برای حفظ منافع خود با دولت‌ها همکاری می‌کنند؛ درنتیجه، امنیت، سرمایه‌داری دیجیتال و حکمرانی داده‌ای به‌صورت ساختاری درهم‌تنیده شده‌اند.

اشاره شد که در چین نیز همکاری نزدیک دولت و شرکت‌های فناوری به ایجاد یکی از پیچیده‌ترین نظام‌های نظارت دیجیتال جهان انجامیده است. سامانه‌های تشخیص چهره، تحلیل رفتار و نظام اعتبار اجتماعی نشان می‌دهد که مشروعیت سیاسی به‌تدریج بر توانایی کنترل داده‌ها و مدیریت رفتار اجتماعی استوار می‌شود. در دموکراسی‌های غربی نیز شهروندان از یک سو خواهان امنیت‌اند و از سوی دیگر، درخصوص گسترش نظارت دیجیتال نگران‌اند. این وضعیت نوعی بحران اعتماد به وجود آورده است و بسیاری احساس می‌کنند کنترل واقعی داده‌هایشان نه در اختیار خودشان و نه حتی دولت، بلکه در دست پلتفرم‌های دیجیتال است.

ظهور حاکمیت الگوریتمی نیز یکی از مهم‌ترین ابعاد این تحول است. الگوریتم‌ها اکنون در تحلیل تهدید، طبقه‌بندی افراد و تصمیم‌گیری‌های امنیتی نقش دارند، اما فاقد مسئولیت‌پذیری اخلاقی و سیاسی هستند. تصمیمات آنان اغلب غیرشفاف است و شهروندان نمی‌دانند بر چه اساسی ارزیابی می‌شوند؛ درنتیجه، بخشی از قدرت اطلاعاتی به ساختارهایی منتقل شده است که خارج از نظارت دموکراتیک عمل می‌کنند. این وضعیت مفهوم مشروعیت را با بحران مواجه کرده، نشان می‌دهد نظریه اطلاعات عادلانه برای حفظ ظرفیت انتقادی خود ناگزیر است مفاهیمی چون تمایز، تناسب، ضرورت و اقتدار مشروع را متناسب با واقعیت جدید قدرت داده‌ای بازتعریف کند، واقعیتی که در آن، داده به مهم‌ترین منبع قدرت سیاسی و اجتماعی تبدیل شده است.

۳. پیامدهای سیاسی و اجتماعی نظارت الگوریتمی

در اندیشه سیاسی مدرن، حریم خصوصی همواره فراتر از یک حق فردی ساده تلقی می‌شود و نقشی اساسی در تضمین آزادی سیاسی، استقلال شهروندی و مشارکت آزادانه در حیات عمومی دارد. وجود حوزه‌ای خصوصی که فرد بتواند در آن بدون ترس از نظارت یا مداخله قدرت سیاسی بیندیشد، ارتباط برقرار کند و هویت سیاسی و اجتماعی خود را شکل دهد از مهم‌ترین پایه‌های دموکراسی به شمار می‌آید. اما گسترش فناوری‌های دیجیتال، کلان‌داده و نظارت الگوریتمی این برداشت را با تحولی عمیق مواجه کرده است. در عصر داده‌محور، حریم خصوصی به‌تدریج از حق سیاسی و مدنی به مسئله‌ای مدیریتی و فناورانه تقلیل یافته است و شهروندان در معرض نوعی شفافیت اجباری قرار گرفته‌اند که مرز میان حوزه خصوصی و قلمرو قدرت را تضعیف می‌کند.

نظارت در شکل سنتی خود معمولاً محدود، پرهزینه و مبتنی‌بر حضور مستقیم نهادهای امنیتی بود. دولت‌ها برای دسترسی به اطلاعات افراد نیازمند استفاده از ابزارهایی همچون شنود، تعقیب یا جاسوسی با مجوز قانونی بودند و به همین دلیل، دامنه نظارت اغلب محدود باقی می‌ماند. اما در نظم دیجیتال، بخش بزرگی از زندگی روزمره انسان‌ها به داده تبدیل شده است. استفاده از گوشی‌های هوشمند، شبکه‌های اجتماعی، موتورهای جست‌وجو، سامانه‌های پرداخت الکترونیک، دوربین‌های شهری و ابزارهای هوشمند خانگی، به‌طور مداوم اطلاعات گسترده‌ای درباره رفتار، علایق، روابط اجتماعی، موقعیت مکانی و حتی وضعیت روانی افراد تولید می‌کند. الگوریتم‌های هوش مصنوعی نیز این داده‌ها را تحلیل و از خلال آن‌ها، الگوهای پیچیده رفتاری و روان‌شناختی استخراج را می‌کند؛ درنتیجه، نظارت دیگر صرفاً مشاهده اعمال آشکار نیست، بلکه به فرایندی دائمی برای تحلیل و بازسازی هویت انسانی ازطریق داده‌ها تبدیل شده است (Zuboff, 2019: 92).

یکی از مهم‌ترین پیامدهای این تحولْ فرسایش مرز میان حوزه خصوصی و حوزه عمومی است. در جهان دیجیتال، شهروندان برای مشارکت در زندگی اجتماعی ناگزیر از استفاده از پلتفرم‌ها و خدماتی هستند که داده‌های آنان را جمع‌آوری می‌کنند. حضور در شبکه‌های اجتماعی، استفاده از خدمات آنلاین، خرید اینترنتی یا حتی تردد در شهرهای هوشمند همگی به تولید داده می‌انجامند. به همین دلیل، مفهوم سنتی حریم خصوصی

که بر پنهان نگه داشتن اطلاعات استوار بود، دیگر کارایی گذشته را ندارد، زیرا تقریباً همه کنش‌های روزمره افراد قابلیت ثبت و تحلیل پیدا کرده است.

مسئله اصلی اکنون این است که چه نهادهایی این داده‌ها را در اختیار دارند، چگونه آن‌ها را تحلیل می‌کنند و با چه اهدافی از آن‌ها استفاده می‌شود. در این شرایط، شرکت‌های فناوری به بازیگران اصلی قدرت داده‌ای تبدیل شده‌اند. مدل اقتصادی بسیاری از پلتفرم‌های دیجیتال بر پایه استخراج و تحلیل داده‌های کاربران شکل گرفته است. این شرکت‌ها- ازطریق تحلیل رفتار کاربران- علایق، ترجیحات و احساسات آنان را شناسایی و سپس از این اطلاعات برای پیش‌بینی و هدایت رفتار استفاده می‌کنند؛ درنتیجه، تجربه انسانی به منبعی برای استخراج داده و کسب سود اقتصادی تبدیل شده است. الگوریتم‌ها نه‌تنها محتوای مورد مشاهده کاربران را تعیین می‌کنند، بلکه می‌توانند به توجه، ترجیحات و حتی تصمیمات سیاسی و اجتماعی آنان جهت دهند. به‌این‌ترتیب، حریم خصوصی دیگر صرفاً حفاظت از اطلاعات شخصی نیست، بلکه مستقیماً با استقلال فکری و آزادی اراده پیوند می‌خورد.

رسوایی کمبریج آنالیتیکا نمونه‌ای روشن از این مسئله بود. این شرکت با استفاده از داده‌های میلیون‌ها کاربر فیسبوک، الگوهای روان‌شناختی آنان را تحلیل و تبلیغات سیاسی هدفمند طراحی کرد تا بر رفتار رأی‌دهندگان در انتخابات آمریکا و همه‌پرسی برگزیت تأثیر بگذارد. این ماجرا نشان داد که داده‌های شخصی می‌توانند به ابزاری برای مهندسی سیاسی جامعه تبدیل شوند. از این منظر، حریم خصوصی دیگر مسئله‌ای صرفاً فردی نیست، بلکه با سلامت دموکراسی و استقلال فرایندهای سیاسی ارتباط مستقیم دارد.

در کنار شرکت‌های فناوری، دولت‌ها نیز به‌طور فزاینده‌ای از ظرفیت‌های داده‌محور برای گسترش نظارت استفاده می‌کنند. در گذشته، حریم خصوصی یکی از ابزارهای محدودسازی قدرت دولت به شمار می‌رفت و شهروندان حق داشتند بخشی از زندگی خود را از مداخله حکومت مصون نگه دارند. اما در عصر امنیت داده‌محور، دولت‌ها به حجم عظیمی از داده‌های دیجیتال دسترسی دارند و از الگوریتم‌ها برای تحلیل رفتار اجتماعی و شناسایی تهدیدهای احتمالی استفاده می‌کنند. این تحول موجب شده است که نظارت به بخشی عادی از فرایند حکمرانی تبدیل شود. اشاره شد که افشاگری‌های ادوارد اسنودن درباره فعالیت‌های آژانس امنیت ملی آمریکا نشان داد که

دولت‌ها قادرند داده‌های ارتباطی میلیون‌ها شهروند را به‌طور گسترده جمع‌آوری و تحلیل کنند. هرچند این اقدامات با هدف مقابله با تروریسم توجیه می‌شد، اما منتقدان هشدار دادند که نظارت فراگیر می‌تواند آزادی‌های مدنی را تضعیف کند. هنگامی که افراد احساس کنند ارتباطات و فعالیت‌های آنان ممکن است زیر نظارت باشد، احتمال دارد از بیان آزادانه دیدگاه‌های سیاسی یا مشارکت در فعالیت‌های مدنی خودداری کنند. این وضعیت که از آن با عنوان اثر سرما یاد می‌شود، یکی از مهم‌ترین پیامدهای سیاسی نظارت الگوریتمی است؛ زیرا بدون نیاز به سرکوب مستقیم، فضای عمومی و آزادی بیان را محدود می‌کند. در برخی کشورها، این روند به شکل آشکارتری دیده می‌شود. در چین، دولت با استفاده از شبکه گسترده دوربین‌های تشخیص چهره، سامانه‌های تحلیل رفتار و نظام اعتبار اجتماعی، ساختاری فراگیر از نظارت داده‌ای ایجاد کرده است. در این نظام، رفتار اقتصادی، اجتماعی و سیاسی شهروندان به‌طور مداوم ارزیابی می‌شود و نتایج این ارزیابی می‌تواند بر دسترسی افراد به خدمات عمومی، فرصت‌های شغلی یا امکان سفر اثر بگذارد. چنین ساختاری شهروندان را به خودسانسوری و تبعیت از هنجارهای مطلوب حکومت سوق می‌دهد و نظارت را به ابزاری برای مدیریت و مهندسی رفتار اجتماعی تبدیل می‌کند (کاظمی و محمدزاده، ۱۴۰۲: ۷۰). در دموکراسی‌های غربی نیز پس‌از حملات ۱۱ سپتامبر، گسترش قوانین امنیتی و نظارتی موجب افزایش چشمگیر اختیارات نهادهای اطلاعاتی شد. دولت‌ها با توجیه مقابله با تروریسم، امکان جمع‌آوری و تحلیل انبوه داده‌های شهروندان را فراهم کردند. هرچند این اقدامات در چارچوب حفظ امنیت عمومی انجام می‌شد، اما بسیاری از منتقدان هشدار دادند که عادی‌سازی نظارت گسترده می‌تواند به تضعیف تدریجی حقوق مدنی بینجامد. تجربه تاریخی نشان داده است که قدرت‌های امنیتی ایجادشده در شرایط بحرانی، اغلب پس‌از پایان بحران نیز باقی می‌مانند و به بخشی دائمی از ساختار حکمرانی تبدیل می‌شوند.

امنیت داده‌محور همچنین رابطه سنتی امنیت و آزادی را دگرگون کرده است. در گذشته، محدودسازی آزادی‌ها معمولاً در شرایط اضطراری یا در قبال تهدیدهای مشخص صورت می‌گرفت، اما در ساختار جدید، نظارت دائمی و پیشگیرانه به بخشی از وضعیت عادی تبدیل شده است. دولت‌ها و نهادهای امنیتی با استفاده از الگوریتم‌های پیش‌بینانه می‌کوشند تهدیدها را پیش‌از وقوع شناسایی کنند و همین امر نیازمند تحلیل

رفتار کل جامعه است؛ بنابراین، همه شهروندان به‌طور بالقوه در معرض نظارت قرار می‌گیرند، حتی اگر هیچ ظن مشخصی متوجه آنان نباشد. این وضعیت مرز میان امنیت مشروع و کنترل فراگیر را تضعیف می‌کند (والش، ۱۴۰۲: ۱۸۵).

یکی دیگر از چالش‌های مهم در نظم داده‌محور، مسئله تبعیض الگوریتمی است. سامانه‌های هوش مصنوعی امنیتی اغلب بر اساس داده‌های تاریخی آموزش می‌بینند و همین امر می‌تواند به بازتولید نابرابری‌های اجتماعی منجر شود. برای مثال، برخی برنامه‌های پلیسی پیش‌بینانه در آمریکا محله‌های فقیرنشین و اقلیت‌های قومی را بیشتر به‌عنوان مناطق پرخطر شناسایی می‌کردند. درنتیجه، حضور پلیس و میزان نظارت در این مناطق افزایش می‌یافت و چرخه‌ای از تبعیض ساختاری شکل می‌گرفت. به‌این‌ترتیب، نظارت الگوریتمی نه‌تنها موجب محدود شدن آزادی‌های مدنی می‌شود، بلکه این محدودیت‌ها را به‌طور نابرابر بر گروه‌های مختلف اجتماعی تحمیل می‌کند.

مشکل مهم دیگر، نبود شفافیت در عملکرد الگوریتم‌هاست. بسیاری از سامانه‌های داده‌محور به‌صورت محرمانه عمل می‌کنند و شهروندان نمی‌دانند چه داده‌هایی از آنان جمع‌آوری می‌شود، چگونه تحلیل می‌گردد و چه تصمیماتی بر اساس آن گرفته می‌شود. این نبود شفافیتْ امکان نظارت دموکراتیک و اعتراض حقوقی را کاهش می‌دهد و موجب می‌شود بخشی از قدرت سیاسی به ساختارهایی منتقل شود که خارج از کنترل عمومی هستند. در چنین شرایطی، نابرابری قدرت میان شهروندان و نهادهای داده‌ای افزایش می‌یابد؛ زیرا دولت‌ها و شرکت‌های فناوری به ابزارهای پیچیده تحلیل داده دسترسی دارند، درحالی‌که شهروندان از سازوکار این سامانه‌ها آگاهی محدودی دارند.

حریم خصوصی دیگر فقط مسئله‌ای فردی نیست، بلکه به بخشی اساسی از آزادی سیاسی و استقلال شهروندی تبدیل شده است. در نظم داده‌محور، نظارت دیگر محدود و استثنایی نیست، بلکه به بخشی دائمی از حکمرانی روزمره تبدیل شده و امکان تحلیل، پیش‌بینی و هدایت رفتار اجتماعی را فراهم کرده است. به‌این‌ترتیب، حفاظت از آزادی‌های مدنی مستلزم بازاندیشی در مفاهیم سنتی حریم خصوصی، امنیت و مشروعیت سیاسی و ایجاد سازوکارهایی برای محدودسازی قدرت داده‌ای، شفافیت الگوریتمی و کنترل دموکراتیک بر ساختارهای نظارتی است.

۴. بازاندیشی نظریه اطلاعات عادلانه در عصر هوش مصنوعی

نظریه اطلاعات عادلانه راس بلابی تلاشی مهم برای اخلاقی‌سازی فعالیت‌های اطلاعاتی و امنیتی در جهان معاصر بود. بلابی با الهام از سنت جنگ عادلانه استدلال می‌کرد که فعالیت‌های اطلاعاتی نیز مانند جنگ نمی‌توانند خارج از محدودیت‌های اخلاقی و حقوقی عمل کنند و باید تابع اصولی چون ضرورت، تناسب، تمایز و اقتدار مشروع باشند. این نظریه در زمان شکل‌گیری خود پاسخی به رویکردهای واقع‌گرایانه‌ای بود که امنیت را فراتر از هر قید اخلاقی می‌دانستند. بااین‌حال، ظهور هوش مصنوعی، کلان‌داده و امنیت الگوریتمی ساختار قدرت اطلاعاتی را به‌گونه‌ای دگرگون کرده که بسیاری از مفروضات کلاسیک نظریه بلابی با چالش مواجه شده است. درعین‌حال، همین نظریه هنوز ظرفیت‌های مهمی برای نقد امنیت‌گرایی دیجیتال و بازاندیشی در اخلاق قدرت اطلاعاتی دارد، هرچند برای حفظ کارآمدی خود نیازمند توسعه و بازتعریف مفاهیم بنیادین خویش است.

یکی از مهم‌ترین محدودیت‌های نظریه اطلاعات عادلانه دولت‌محور بودن آن است. بلابی اقتدار مشروع را عمدتاً در چارچوب دولت ملی و نهادهای رسمی امنیتی تعریف می‌کرد؛ زیرا در زمان طرح نظریه، دولت‌ها بازیگران اصلی قدرت اطلاعاتی محسوب می‌شدند. اما در عصر دیجیتال، بخش عمده زیرساخت اطلاعاتی جهان در اختیار شرکت‌های فناوری قرار گرفته است. شرکت‌هایی مانند گوگل، متا، آمازون، هوآوی و مایکروسافت نه‌تنها داده‌های میلیاردها کاربر را جمع‌آوری می‌کنند، بلکه ازطریق الگوریتم‌های پیشرفته قادر به تحلیل رفتار، پیش‌بینی ترجیحات و هدایت کنش اجتماعی‌اند. افشاگری‌های ادوارد اسنودن نشان داد که نهادهای امنیتی دولت‌ها نیز برای اجرای برنامه‌های نظارتی خود به همکاری گسترده این شرکت‌ها وابسته‌اند. برنامه پریسم نمونه‌ای روشن از پیوند ساختاری دولت و شرکت‌های فناوری در مدیریت داده‌ها بود. این وضعیت نشان می‌دهد که قدرت اطلاعاتی در جهان معاصر دیگر صرفاً در اختیار دولت نیست، بلکه در شبکه‌ای از بازیگران دولتی و خصوصی توزیع شده است؛ ازاین‌رو، نظریه بلابی که اقتدار مشروع را عمدتاً در سطح دولت تعریف می‌کرد، برای تحلیل این ساختار شبکه‌ای با محدودیت جدی روبه‌روست.

محدودیت دیگر نظریه بلابی به اصل تمایز مربوط می‌شود. بلابی معتقد بود فعالیت اطلاعاتی باید میان افراد تهدیدکننده و شهروندان عادی تمایز قائل شود. اما امنیت

الگوریتمی بر پایه جمع‌آوری انبوه داده‌ها عمل می‌کند و الگوریتم‌ها برای پیش‌بینی تهدیدها به دسترسی به حجم عظیمی از اطلاعات اجتماعی نیازمندند؛ درنتیجه، همه شهروندان به موضوع بالقوه نظارت تبدیل می‌شوند و مرز میان مظنون و غیرمظنون به‌تدریج از میان می‌رود. سامانه‌های کنترل پلیسی در آمریکا و سایر کشورها نمونه‌ای روشن از این وضعیت هستند. این سامانه‌ها با تحلیل داده‌های تاریخی جرائم، مناطقی را پرخطر می‌شناسند، اما در عمل اغلب محله‌های فقیرنشین و اقلیت‌های قومی را هدف نظارت بیشتر قرار داده‌اند. چنین الگوریتم‌هایی به‌جای تمرکز بر افراد مشخص، کل الگوهای جمعیتی را موضوع تحلیل قرار می‌دهد و همین امر موجب بازتولید تبعیض ساختاری می‌شود؛ بنابراین، اصل تمایز در عصر الگوریتمی با بحران جدی مواجه شده است.

اصل تناسب نیز در ساختار جدید امنیت داده‌محور دچار ابهام شده است. بلابی استدلال می‌کرد که میزان مداخله امنیتی باید متناسب با سطح تهدید باشد، اما در امنیت الگوریتمی تهدید نه یک واقعیت بالفعل، بلکه یک احتمال آماری است. دولت‌ها و نهادهای امنیتی برای پیشگیری از تهدیدهای بالقوه همواره به داده‌های بیشتری نیاز دارند و همین امر دامنه نظارت را به‌طور مستمر گسترش می‌دهد. افشاگری‌های مربوط به نهادهای امنیتی ایالات متحده نشان داد که داده‌های میلیون‌ها شهروند عادی بدون وجود ظن مشخص جمع‌آوری شد. این اقدامات با هدف مقابله با تروریسم توجیه می‌شد، اما منتقدان آن را نامتناسب و ناقض آزادی‌های مدنی می‌دانستند. در امنیت الگوریتمی هیچ مرز روشنی برای میزان داده کافی وجود ندارد و هرچه ظرفیت تحلیل داده افزایش یابد، نیاز به داده نیز بیشتر تعریف می‌شود. این وضعیت اصل تناسب را به مفهومی مبهم و انعطاف‌پذیر تبدیل کرده است.

یکی دیگر از ضعف‌های نظریه بلابی، اتکای آن به الگوی تصمیم‌گیری انسانی است. در زمان تدوین این نظریه فرض بر آن بود عاملان انسانی تصمیمات اطلاعاتی را می‌گیرند و بنابراین، امکان نسبت‌دادن مسئولیت اخلاقی وجود دارد. اما امروزه بسیاری از تصمیمات امنیتی ازسوی الگوریتم‌ها و سامانه‌های هوش مصنوعی اتخاذ می‌شود. فناوری‌هایی مانند تشخیص چهره، تحلیل رفتار و ارزیابی خطر اغلب بدون مداخله مستقیم انسان عمل می‌کنند. این تحول مسئله مهمی درباره مسئولیت اخلاقی ایجاد می‌کند. اگر الگوریتم به‌اشتباه فردی را تهدید تشخیص دهد یا موجب تبعیض شود،

مسئولیت بر عهده چه کسی است؟ طراح الگوریتم، نهاد امنیتی یا شرکت توسعه‌دهنده؟ نظریه بلابی پاسخ روشنی به این مسئله ندارد، زیرا بر پایه تصور کلاسیک از عاملیت انسانی بنا شده است.

مشکل دیگر نظریه اطلاعات عادلانه ناتوانی آن در تحلیل منطق اقتصادی امنیت داده‌محور است. در عصر دیجیتال، داده‌ها فقط ابزار امنیت نیستند، بلکه به مهم‌ترین منبع قدرت اقتصادی تبدیل شده‌اند. شرکت‌های فناوری ازطریق استخراج و تحلیل داده‌ها سود کلانی به دست می‌آورند و همین امر موجب شکل‌گیری سرمایه‌داری نظارتی شده است. رسوایی کمبریج آنالیتیکا نشان داد که داده‌های کاربران شبکه‌های اجتماعی چگونه می‌توانند برای مهندسی سیاسی و تأثیرگذاری بر افکار عمومی استفاده شوند. این وضعیت مرز میان منافع اقتصادی، امنیتی و سیاسی را تضعیف کرده است. نظریه بلابی که عمدتاً بر رابطه دولت و شهروند تمرکز داشت، برای تحلیل این پیوند میان سرمایه‌داری دیجیتال و قدرت اطلاعاتی کفایت لازم را ندارد.

با وجود این محدودیت‌ها، نظریه اطلاعات عادلانه همچنان ظرفیت‌های مهمی برای نقد امنیت‌گرایی دیجیتال دارد. یکی از مهم‌ترین ظرفیت‌های آن، تأکید بر محدودیت‌پذیری قدرت اطلاعاتی است. برخلاف رویکردهایی که در آن‌ها، امنیت فراتر از اخلاق است، بلابی معتقد بود حتی در شرایط تهدید نیز قدرت امنیتی باید محدود شود. این اصل در عصر نظارت الگوریتمی اهمیت ویژه‌ای دارد، زیرا امنیت دیجیتال ذاتاً گرایش به گسترش نامحدود دارد. الگوریتم‌ها برای افزایش دقت خود به داده‌های بیشتری نیاز دارند و همین امر موجب می‌شود منطق امنیتی دائماً خود را بازتولید کند. نظریه بلابی از این جهت ابزاری هنجاری برای نقد این گسترش بی‌حد فراهم می‌کند.

اصل تمایز نیز همچنان ظرفیت انتقادی مهمی دارد. در جهانی که همه شهروندان به موضوع تحلیل داده‌ای تبدیل شده‌اند، تأکید بر ضرورت تفکیک میان افراد تهدیدکننده و شهروندان عادی می‌تواند ابزاری برای نقد نظارت فراگیر باشد. همچنین اصل تناسب امکان آن را فراهم می‌کند که مشروعیت جمع‌آوری انبوه داده‌ها مورد پرسش قرار گیرد. از منظر بلابی، امنیت نمی‌تواند به توجیهی برای مداخله نامحدود در زندگی شهروندان تبدیل شود. این دیدگاه دربرابر منطق رایج امنیت دیجیتال قرار می‌گیرد که فرض می‌کند داده بیشتر، امنیت بیشتر و هرگونه محدودیت بر نظارت را مانعی برای امنیت می‌داند.

یکی دیگر از ظرفیت‌های نظریه بلابی تأکید بر پاسخ‌گویی و مشروعیت قدرت اطلاعاتی است. در عصر دیجیتال، بخش بزرگی از قدرت اطلاعاتی در اختیار شرکت‌های خصوصی قرار گرفته که خارج از سازوکارهای سنتی پاسخ‌گویی دموکراتیک عمل می‌کنند. نظریه بلابی با تأکید بر اقتدار مشروع، امکان نقد این وضعیت را فراهم می‌سازد و این پرسش را مطرح می‌کند که آیا شرکت‌های فناوری می‌توانند بدون نظارت عمومی بخشی از ساختار قدرت اطلاعاتی باشند یا خیر. همچنین حساسیت این نظریه به خطر سوءاستفاده از قدرت اطلاعاتی، آن را به ابزاری مهم برای نقد نظام‌های نظارتی گسترده تبدیل می‌کند، نظام‌هایی که می‌توانند داده‌های رفتاری شهروندان را برای کنترل اجتماعی و مهندسی سیاسی به کار گیرند.

بااین‌حال، حفظ ظرفیت انتقادی نظریه بلابی در عصر هوش مصنوعی مستلزم توسعه و بازطراحی آن است. نخستین گام در این مسیر، گذار از دولت‌محوری به درک شبکه‌ای از قدرت اطلاعاتی است. در ساختار جدید، دولت‌ها، شرکت‌های فناوری، پلتفرم‌های دیجیتال و سامانه‌های هوش مصنوعی همگی بخشی از اکوسیستم قدرت اطلاعاتی به حساب می‌آیند و باید تابع اصول اخلاقی مشابهی باشند. اقتدار مشروع دیگر نمی‌تواند صرفاً به دولت محدود شود، بلکه باید همه نهادهای داده‌محور را در بر گیرد. گام دوم بازتعریف اصل تمایز در قالب تمایز الگوریتمی است. در امنیت الگوریتمی، تصمیم‌گیری‌ها بر پایه تحلیل آماری و پیش‌بینی رفتاری انجام می‌شود؛ بنابراین، لازم است الگوریتم‌ها قابلیت توضیح‌پذیری داشته باشند تا مشخص شود بر چه مبنایی افراد یا گروه‌ها در دسته‌های پرخطر قرار می‌گیرند. بدون شفافیت الگوریتمی، اصل تمایز عملاً بی‌معنا خواهد شد. همچنین اصل تناسب باید از حالت ایستا به مفهومی پویا تبدیل شود. در عصر کلان‌داده، تهدیدها به‌صورت احتمالاتی تعریف می‌شوند و بنابراین، مداخلات امنیتی باید به‌طور مداوم ارزیابی و بازبینی شوند. اگر یک سامانه امنیتی میزان زیادی از خطا یا تبعیض تولید کند، ادامه استفاده از آن نمی‌تواند ازنظر اخلاقی مشروع باشد. شفافیت الگوریتمی نیز باید به یکی از شروط اصلی مشروعیت قدرت اطلاعاتی تبدیل شود. الگوریتم‌های جعبه‌سیاه که منطق تصمیم‌گیری آن‌ها فهم‌پذیر نیست نمی‌توانند مبنای مشروعیت اخلاقی فعالیت‌های امنیتی باشند. علاوه‌بر این، مفهوم حریم خصوصی باید به حق داده گسترش یابد، یعنی شهروندان نه‌تنها حق

حفاظت از اطلاعات شخصی، بلکه حق آگاهی، دسترسی، اصلاح و حذف داده‌های خود را داشته باشند.

عصر هوش مصنوعی مستلزم شکل‌گیری سازوکارهای چندلایه نظارتی است. نظارت بر قدرت اطلاعاتی دیگر نمی‌تواند صرفاً در اختیار دولت‌ها باشد، بلکه نهادهای مستقل قضایی، مدنی و حتی بین‌المللی باید در ارزیابی و کنترل سامانه‌های الگوریتمی مشارکت داشته باشند. این‌گونه از بازاندیشی نشان می‌دهد که نظریه اطلاعات عادلانه، با وجود ریشه‌های کلاسیک خود، هنوز دارای ظرفیت تبدیل شدن به چارچوبی مؤثر برای نقد و تنظیم اخلاقی قدرت اطلاعاتی در عصر هوش مصنوعی است، مشروط بر آنکه خود را با واقعیت‌های جدید حکمرانی داده‌محور سازگار سازد.

نتیجه‌گیری

پژوهش حاضر با تمرکز بر بازاندیشی نظریه اطلاعات عادلانه راس بلابی در بستر تحول‌آفرین هوش مصنوعی و کلان‌داده، تلاش کرد نسبت میان اخلاق، امنیت و قدرت اطلاعاتی را در چارچوبی انتقادی و به‌روز بازخوانی کند. مسئله محوری تحقیق آن بود که آیا نظریه‌ای که در بستر امنیت سنتی و دولت‌محور شکل گرفته است همچنان توانایی تبیین و تنظیم اخلاقی سازوکارهای پیچیده امنیت الگوریتمی را دارد یا خیر. یافته‌های تحلیلی این پژوهش نشان می‌دهد که اگرچه نظریه بلابی ازنظر هنجاری همچنان واجد ظرفیت‌های درخور توجه برای نقد امنیت‌گرایی دیجیتال است، اما ازحیث تحلیلی و ساختاری با محدودیت‌های جدی در مواجهه با منطق شبکه‌ای و داده‌محور قدرت روبه‌روست.

در پاسخ به پرسش نخست پژوهش مبنی‌بر اینکه نظریه اطلاعات عادلانه تا چه اندازه با ساختار امنیت الگوریتمی سازگار است، می‌توان نتیجه گرفت که همچنان می‌توان از این نظریه در سطح اصول کلی استفاده کرد، اما در سطح کاربردی با شکاف‌های مفهومی مواجه است. اصولی مانند تناسب، تمایز، ضرورت و اقتدار مشروع همچنان می‌توانند به‌مثابه معیارهای اخلاقی ارزیابی فعالیت‌های اطلاعاتی به کار آیند، اما این اصول در شکل کلاسیک خود توان توضیح کامل نظام‌های مبتنی بر هوش مصنوعی، نظارت انبوه و تحلیل پیش‌بینانه را ندارند. دلیل اصلی این امر تغییر ماهیت قدرت اطلاعاتی از مدل واکنشی و هدفمند به مدل پیش‌بینانه، شبکه‌ای و الگوریتمی است.

در پاسخ به پرسش دوم پژوهش مبنی‌بر اینکه مهم‌ترین چالش‌های نظریه اطلاعات عادلانه در عصر کلان‌داده چیست؟ یافته‌ها نشان داد که پنج چالش اساسی وجود دارد: نخست، دولت‌محور بودن نظریه درحالی‌که قدرت اطلاعاتی به شبکه‌ای از دولت‌ها و شرکت‌های فناوری منتقل شده است؛ دوم، ناکارآمدی اصل تمایز در مواجهه با تحلیل‌های انبوه داده‌ای؛ سوم، بحران اصل تناسب در شرایط امنیت پیش‌بینانه؛ چهارم، ابهام در مفهوم اقتدار مشروع در ساختارهای هیبریدی دولت-پلتفرم؛ و پنجم، ناتوانی در تبیین نقش الگوریتم‌ها به‌عنوان کنشگران غیرانسانی در فرایند تصمیم‌گیری امنیتی. این چالش‌ها نشان می‌دهد که نظریه بلابی در شکل اولیه خود نمی‌تواند به‌طور کامل پاسخ‌گوی پیچیدگی‌های نظم اطلاعاتی معاصر باشد.

در پاسخ به پرسش سوم مبنی‌بر اینکه آیا نظریه اطلاعات عادلانه همچنان ظرفیت کارکردی برای نقد امنیت‌گرایی دیجیتال دارد یا خیر، نتایج پژوهش نشان می‌دهد که این نظریه به‌رغم محدودیت‌ها، همچنان از ظرفیت‌های انتقادی مهمی برخوردار است. تأکید آن بر محدودیت قدرت، پاسخ‌گویی، شفافیت و تناسب ابزارهای مفهومی مؤثری برای نقد گسترش نظارت الگوریتمی فراهم می‌کند. به‌ویژه در مواجهه با پدیده‌هایی مانند نظارت انبوه، سرمایه‌داری نظارتی و حکمرانی داده‌محور، این نظریه همچنان قادر است مرزهای اخلاقی قدرت اطلاعاتی را برجسته سازد و از طبیعی‌سازی امنیت‌گرایی دیجیتال جلوگیری کند.

بنابراین، مسئله اصلی نه بی‌اعتباری نظریه اطلاعات عادلانه، بلکه ناهم‌زمانی آن با ساختار جدید قدرت اطلاعاتی است. این نظریه در بستر تاریخی خاصی شکل گرفته که در آن، دولت بازیگر اصلی امنیتی بود و داده‌ها به‌صورت محدود و هدفمند جمع‌آوری می‌شدند. اما در عصر هوش مصنوعی، با ظهور زیرساخت‌های عظیم داده‌ای، الگوریتم‌های خودکار و هم‌پیوندی دولت و شرکت‌های فناوری، ساختار قدرت به‌طور بنیادین دگرگون شده است. براین‌اساس، پژوهش حاضر پیشنهاد می‌کند که نظریه اطلاعات عادلانه باید در قالبی توسعه‌یافته و بازاندیشی‌شده بازسازی شود، به‌گونه‌ای که شامل عناصر جدیدی همچون شفافیت الگوریتمی، حقوق داده، نظارت چندلایه، اخلاق پیش‌بینانه و مسئولیت‌پذیری فراملی باشد. چنین بازسازی‌ای می‌تواند این نظریه را از یک چارچوب کلاسیک دولت‌محور به نظریه‌ای انتقادی برای تحلیل و تنظیم قدرت در عصر داده‌محور تبدیل کند.

از منظر نظری، این پژوهش نشان داد که گذار از امنیت سنتی به امنیت الگوریتمی صرفاً یک تحول فناورانه نیست، بلکه تغییری در منطق حکمرانی و ماهیت قدرت است. در این منطق جدید، داده نه‌فقط ابزار تصمیم‌گیری، بلکه زیرساخت اصلی تولید قدرت سیاسی و اجتماعی محسوب می‌شود. بنابراین، هر نظریه‌ای که بخواهد در این حوزه کارآمد باقی بماند، باید بتواند رابطه میان داده، قدرت و اخلاق را به‌صورت یکپارچه تحلیل کند. می‌توان گفت که نظریه اطلاعات عادلانه، با وجود محدودیت‌هایش، همچنان یکی از مهم‌ترین منابع نظری برای نقد اخلاقی امنیت دیجیتال است، اما بقای کارکردی آن منوط به بازتعریف مفاهیم بنیادین آن در پرتو تحولات هوش مصنوعی و کلان‌داده است. این بازتعریف نه به معنای کنارگذاشتن نظریه، بلکه به معنای انطباق آن با واقعیت‌های جدید قدرت اطلاعاتی و حفظ نقش انتقادی آن دربرابر گسترش بی‌حد امنیت‌گرایی دیجیتال است.

تعارض منافع
تضاد منافع : در انجام مطالعه حاضر هیچ‌گونه تضاد منافعی وجود ندارد.
موازین اخلاقی : در انجام این پژوهش تمامی اصول و موازین اخلاقی رعایت گردیده است.
شفافیت داده‌ها: داده‌ها و مآخذ پژوهش حاضر در صورت درخواست از نویسنده مسئول و ضمن رعایت اصول کپی رایت ارسال خواهد شد.
حامی مالی: این پژوهش حامی مالی نداشته است.

منابع

برت، سالی (۱۴۰۴). امنیت ملی در عصر دیجیتال و اطلاعات. ترجمه علیرضا قاضی‌زاده. مرکز آموزشی و پژوهشی شهید سپهبد صیاد شیرازی.

پژوهشکده تحقیقات اسلامی نمایندگی ولی‌فقیه در سپاه (۱۳۸۶). اخلاق اطلاعاتی. زمزم هدایت.

«سیستم اعتباری چین: بازسازی اعتماد جمعی تا تحولات چندلایه در حکمرانی» (شهریور ۱۴۰۴). مجله گراف، ۱(۱).

قاضی‌زاده، علیرضا (۱۳۹۱). فناوری و قدرت اطلاعاتی: از افزایش شناخت تا ارتقای توان کنترل. فصلنامه مطالعات راهبردی، ۱۵(۲).

کاظمی، حجت و محمدزاده، مریم (۱۴۰۲). فناوری دیجیتال: شکل‌گیری نام پایش سراسری و آینده حکمرانی چینی. فصلنامه سیاست‌گذاری عمومی، ۹(۳).

گیل، پیتر (۱۳۸۹). سیاست‌های پلیسی: اطلاعات امنیتی و دولت لیبرال دموکراتیک. ترجمه معاونت پژوهش. دانشکده اطلاعات.

لوونتال، مارک (۱۴۰۱). اطلاعات: از اسرار تا سیاست. ترجمه معاونت پژوهش و تولید علم. مؤسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی.

مانیان، امیر و رونقی، محمدحسین (۱۴۰۰). اخلاق در سیستم‌های اطلاعاتی. دانشگاه تهران.

محمدی ری‌شهری، محمد (۱۳۹۷). اخلاق اطلاعاتی. دانشگاه افسری و تربیت پاسداری امام حسین(ع).

محمدی، مسلم و جعفری، سیدمحمد باقر (۱۳۹۷). اخلاق حرفه‌ای فناوری اطلاعات. جهاد دانشگاهی.

منظرزاده؛ مجید و صداقت، علیرضا (۱۳۹۹). اخلاق اطلاعاتی. پژوهشگاه علوم اسلامی امام صادق(ع).

مؤسسه آموزشی و پژوهشی امام خمینی(ره)(۱۴۰۱). اخلاق و امنیت: مبانی و اصول. موسسه آموزشی و پژوهشی امام خمینی(ره).

والش، پاتریک (۱۴۰۲). رهبری و حکمرانی اطلاعاتی: ایجاد جوامع اطلاعاتی کارآمد در قرن بیست‌ویکم. ترجمه مهدی پیروز و پیمان حسنی. مؤسسه چاپ و انتشارات دانشگاه اطلاعات و امنیت ملی.

Andrejevic, M. (2013). Infoglut: How Too Much Information Is Changing the Way We Think and

Know. Routledge.

Bellaby, R. (2012). The Ethics of Intelligence: A New Framework. London: Routledge.

Bellaby, R. (2014). What's the Harm? The Ethics of Intelligence Collection. Intelligence and National Security, 29(1), 108–124.

Bellaby, R. (2016). Just Intelligence: A Capability Perspective. Journal of Global Ethics.

Erskine, T. (ed.) (2008). Can Institutions Have Responsibilities? Collective Moral Agency and International Relations. New York: Palgrave Macmillan.

Goldman, Jan. (2010). Ethics of Spying: A Reader for the Intelligence Professional (2nd ed.). Scarecrow Press.

Lyon, D. (2001). Surveillance Society: Monitoring Everyday Life. Open University Press.

Nissenbaum, H. (2022). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

Walzer, M. (2015). Just and Unjust Wars: A Moral Argument with Historical Illustrations (5th ed.). New York: Basic Books.

Zuboff, S. (2015). Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology, 30(1), 75–89.

Zuboff, S. (2019). The Age of Surveillance Capitalism. Public Affairs