

The Legal Model of Anticipatory Personal Data Governance in the Face of Generative Artificial Intelligence, with Emphasis on Alternative Futures of Privacy Law

Article Type: Research Article

Mohammad Sadegh Vasef^{1*}
Corresponding Author, Ph.D.
Student in Public Law, Qom Branch,
Islamic Azad University, Qom, Iran.
Email: dr.vasef@gmail.com

Zeinab Sheidayian²
Assistant Professor, Department of
Law, Qom Branch, Islamic Azad
University, Qom, Iran.
Email: m_sheidaieian@ut.ac.ir

Mohammad Hosein Khaki³
Ph.D. in Public Administration -
Human Resource Management, Qom
Branch, Islamic Azad University,
Qom, Iran.
Email: m.khaki5017@iau.ir

Received: February 9, 2026
Revised: May 15, 2026
Accepted: May 24, 2026

Abstract

The capacity of generative artificial intelligence to produce content, infer latent information, analyze vast volumes of data, and engage in continuous interaction with users has exposed classical privacy law mechanisms—particularly those based on individual consent and ex post control—to serious limitations. Under such circumstances, a transition from reactive approaches toward anticipatory personal data governance emerges as a legal necessity. The present study aims to design a legal model for anticipatory personal data governance in the face of generative artificial intelligence, with emphasis on alternative futures of privacy law. Employing a legal-analytical method with a futures-studies approach, the study examines the emerging challenges posed by intelligent technologies and identifies the components necessary for the formation of a legal system compatible with future developments. The findings indicate that effective protection of personal data in the era of generative artificial intelligence requires redefining the concept of privacy, developing ex ante risk assessment mechanisms, strengthening algorithmic transparency, establishing a multi-level accountability system, and moving toward adaptive regulation. Based on the results, the proposed model rests on five principal components: legal anticipation, data risk management, technological accountability, protection of individual and collective data rights, and regulatory flexibility. By offering a forward-looking framework, this study seeks to provide the theoretical groundwork for transforming privacy law from a merely protective system into an active and anticipatory governance system, and to propose pathways for legal policymaking in the face of data-driven technologies, particularly within developing legal systems.

Keywords: Anticipatory Data Governance, Generative Artificial Intelligence, Legal Futures Studies, Privacy Law, Technology Regulation.

Cite this article: Sheidayian, Gz., Khaki, M. H. & Vasef, M. S. (2025). Future Studies of the Political Crisis between Iran and the United States Based on Mearsheimer's Views. *Strategic Management & Futures Studies*, 8 (2), 23-42.



© The Author(s).

Online ISSN: 2821-0069

الگوی حقوقی حکمرانی پیش‌نگر داده‌های شخصی در مواجهه با هوش مصنوعی مولد با تأکید بر آینده‌های بدیل حقوق حریم خصوصی

چکیده

قابلیت فناوری هوش مصنوعی مولد در تولید محتوا، استنتاج اطلاعات پنهان، تحلیل حجم گسترده‌ای از داده‌ها و ایجاد تعامل مستمر با کاربران موجب شده است که سازوکارهای کلاسیک حقوق حریم خصوصی، به‌ویژه مدل‌های مبتنی بر رضایت فردی و کنترل پسینی، با محدودیت‌های جدی مواجه شوند. در چنین شرایطی، گذار از رویکردهای واکنشی به سمت حکمرانی پیش‌نگر داده‌های شخصی به‌عنوان یک ضرورت حقوقی مطرح می‌شود. هدف پژوهش حاضر، طراحی الگوی حقوقی برای حکمرانی پیش‌نگر داده‌های شخصی در مواجهه با هوش مصنوعی مولد با تأکید بر آینده‌های بدیل حقوق حریم خصوصی است. پژوهش حاضر با روش تحلیل حقوقی و رویکرد آینده‌پژوهانه، ضمن بررسی چالش‌های نوظهور ناشی از فناوری‌های هوشمند، مؤلفه‌های لازم برای شکل‌گیری یک نظام حقوقی سازگار با تحولات آینده را شناسایی می‌کند. یافته‌ها نشان داد حمایت مؤثر از داده‌های شخصی در عصر هوش مصنوعی مولد نیازمند بازتعریف مفهوم حریم خصوصی، توسعه سازوکارهای ارزیابی پیشینی خطر، تقویت شفافیت الگوریتمی، ایجاد نظام پاسخگویی چندسطحی و حرکت به سمت تنظیم‌گری تطبیقی است. بر اساس نتایج، الگوی پیشنهادی پژوهش بر پنج مؤلفه اصلی شامل پیش‌بینی حقوقی، مدیریت ریسک داده، پاسخگویی فناورانه، حفاظت از حقوق فردی و جمعی داده‌ها و انعطاف‌پذیری مقرراتی استوار است. این پژوهش با ارائه چارچوبی آینده‌نگر تلاش می‌کند زمینه نظری لازم برای تحول حقوق حریم خصوصی از یک نظام صرفاً حمایتی به یک نظام حکمرانی فعال و پیش‌بین را فراهم کند و مسیرهایی برای سیاست‌گذاری حقوقی در مواجهه با فناوری‌های داده‌محور به‌ویژه در نظام‌های حقوقی در حال توسعه ارائه دهد.

واژگان کلیدی: آینده‌پژوهی حقوقی، تنظیم‌گری فناوری، حقوق حریم خصوصی، حکمرانی پیش‌نگر داده، هوش مصنوعی مولد.

نوع مقاله:

مقاله پژوهشی

محمدصادق واصف^۱

نویسنده مسئول: دانشجوی دکتری حقوق عمومی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران.

رایانامه: dr.vasefi@gmail.com

زینب شیدائیان^۲

استادیار، گروه حقوق، واحد قم، دانشگاه آزاد اسلامی، قم، ایران.

رایانامه: m_sheidaei@ut.ac.ir

محمدحسین خاکی^۳

دکتری تخصصی مدیریت دولتی - مدیریت منابع انسانی، واحد قم، دانشگاه آزاد اسلامی، قم، ایران.

رایانامه: m.khaki5017@iaui.ac.ir

تاریخ دریافت: ۱۴۰۴/۱۱/۲۰

تاریخ بازنگری: ۱۴۰۵/۰۲/۲۵

تاریخ پذیرش: ۱۴۰۵/۰۳/۰۳

استناد: شیدائیان، زینب، خاکی، محمدحسین و واصف، محمدصادق (۱۴۰۴). الگوی حقوقی حکمرانی پیش‌نگر داده‌های شخصی در مواجهه با هوش مصنوعی مولد با تأکید بر آینده‌های بدیل حقوق حریم خصوصی. مدیریت راهبردی و آینده‌پژوهی، ۸ (۲)، ۲۳-۴۲.

مقدمه

تحول بنیادین هوش مصنوعی مولد، فراتر از تولید صرف متن یا تصویر در تبدیل داده‌های نامرتبط و پراکنده به الگوها، استنتاج‌ها و پیش‌بینی‌های رفتاری نهفته است. این سامانه‌ها داده‌هایی را که در بدو امر فاقد حساسیت حقوقی به نظر می‌رسند، به مبنای سنجش شخصیت، اهلیت اعتباری و ارزیابی رفتار فرد تبدیل می‌کنند (Gstrein & Kochenov, 2020; Mantelero, 2020). توانایی این الگوها در هم‌افزایی داده‌ها و خلق «روایت‌های به‌ظاهر منسجم»، خطر تصمیم‌گیری‌های ناعادلانه بر پایه استنتاج‌های الگوریتمی را تشدید می‌کند؛ به‌ویژه در فرایندهایی نظیر بازرسی و ارزیابی خطر که صرف قرارگیری در یک طبقه آماری غیرعادی می‌تواند آثار زیان‌بار عملی به همراه داشته باشد، بی‌آنکه تخلفی واقعی محقق شده باشد.

این تحول، الگوهای سنتی حقوقی را در دو رکن بنیادین به چالش کشیده است: نخست، دگرگونی مفهوم رضایت، در الگوهای کلاسیک حریم خصوصی، شخص تا حد معقولی هدف پردازش را پیش‌بینی می‌کرد؛ اما در سامانه‌های مولد با استنتاج‌های چندمرحله‌ای و پیچیده، شکاف عمیقی میان اطلاعات ارائه‌شده در زمان اخذ رضایت و کاربرد نهایی داده ایجاد می‌شود (Hacker et al., 2023). افزون بر این، در محیط‌های نوین، آثار حقوقی ممکن است حاصل داده‌هایی باشد که فرد هرگز شخصاً ارائه نداده و حتی از فرایند استنتاج آن‌ها بی‌اطلاع بوده است. ازاین‌رو، دایره حمایت حقوقی دیگر نمی‌تواند صرفاً متوجه «داده ورودی» باشد، بلکه ناگزیر باید فرایند استنتاج، ساخت روایت و پیامد تصمیم را نیز در بر گیرد (Mantelero, 2020).

دوم؛ بحران در مفهوم پاسخگویی و زنجیره مسئولیت، در نظام سنتی مسئولیت، زیان‌دیده با اثبات انتساب رفتار و رابطه سببیت، خسارت را مطالبه می‌کرد. در سامانه‌های مولد، تصمیم‌گیری میان چرخه‌ای مرکب از تأمین‌کننده داده، توسعه‌دهنده مدل، بهره‌بردار سامانه و کاربر نهایی توزیع شده است. این توزیع‌شدگی، شناسایی منشأ خروجی زیان‌بار را دشوار ساخته و گذار از «مسئولیت پسینی جبران زیان» به «پاسخگویی پیشینی، مستمر و ساختاری» را الزامی می‌کند.

در پاسخ به این دگرگونی، نظام‌های پیشرو در حال گذار از قواعد صلب و تکلیفی یکسان به‌سوی «تنظیم‌گری مبتنی بر ریسک» هستند؛ رویکردی که در آن شدت مداخله هنجاری و دامنه تعهدات

متناسب با ماهیت پردازش، استقلال سامانه و میزان خطرات توزیع می‌شود (Kaminski, 2019; Zuiderveen Borgesius, 2021 & Mantelero, 2016; Veale). آینده حقوق حریم خصوصی سناریوی واحدی ندارد و در طیفی میان نظارت دائمی پیش‌بینی‌محور تا طراحی نهادی مشارکتی در نوسان است. فرامرزی شدن گردش داده و وابستگی تصمیم‌ها به محاسبات ماشینی، حکمرانی داده را به مقوله «توزیع قدرت در فضای دیجیتال» بدل کرده که فراتر از حفاظت فردی صرف است (Yeung, 2018).

ضرورت بررسی این تحولات در حقوق ایران از همین گلوگاه نشأت می‌گیرد؛ قواعد عمومی مسئولیت مدنی، قانون تجارت الکترونیکی و اصول سنتی حریم خصوصی، تنها پاسخگوی مرحله ورود و انتشار اطلاعات‌اند و خلأ سازوکاری منسجم برای پوشش مرحله پس از جمع‌آوری و پیش از اثرگذاری تصمیم به‌شدت محسوس است. بر این اساس، مسئله اصلی این پژوهش، فقدان چارچوب حقوقی جامعی است که بتواند تمام چرخه حیات داده—از گردآوری تا استنتاج و کاربرد در تصمیم‌گیری—را پوشش دهد؛ رویکردی که نوآوری آن در انتقال کانون توجه حقوق حریم خصوصی از «داده به‌عنوان موضوع حمایت» به «چرخه اثرگذاری داده بر موقعیت حقوقی فرد» تجلی می‌یابد.

مبانی نظری

تحلیل حقوقی سازوکارهای حاکم بر فناوری‌های خودکار نیازمند ابتدا بر چارچوب‌های تئوریک معتبر در حقوق عمومی، تنظیم‌گری و فقه اسلامی است:

۱. نظریه تنظیم‌گری مبتنی بر ریسک

نظریه تنظیم‌گری مبتنی بر ریسک^۱ که در حقوق اداری نوین ریشه دارد، فرض را بر این می‌گذارد که دولت‌ها و نهادهای تنظیم‌گر فاقد منابع نامحدود برای مهار تمام مخاطرات پیرامونی هستند؛ بنابراین منابع نظارتی باید متناسب با شدت و احتمال وقوع آسیب تخصیص یابد (Yeung, 2018). در حوزه هوش مصنوعی، رویکرد مبتنی بر ریسک مانع از تحمیل بوروکراسی بازدارنده بر

1. Risk-based Regulation

نوآوری‌های کم‌خطر می‌شود، در حالی که سامانه‌های محل امنیت یا واجد ریسک غیرقابل جبران بر حقوق اساسی را تحت نظارت‌های سخت‌گیرانه پیشینی قرار می‌دهد (Edwards, 2022).

۲. دکترین دادرسی منصفانه و شفافیت اداری

در حقوق عمومی، تصمیمات مؤثر بر سرنوشت شهروندان باید مستدل، مستند و قابل ارزیابی باشند. فناوری یادگیری ماشین به دلیل خصلت «جعبه سیاه»^۱ خطر اتخاذ تصمیمات بدون استدلال آشکار را افزایش می‌دهد (Mittelstadt & Wachter, 2019). در نظریه دادرسی منصفانه و شفافیت اداری^۲ مبنای نظری حق بر توضیح‌پذیری الگوریتمی بر دکترین حکمرانی قانون استوار است؛ به این معنا که حاکمیت یا نهادهای خصوصی واجد موقعیت مسلط نمی‌توانند تکالیفی را بر اشخاص بار کنند، بدون آنکه منطق و علل اتخاذ تصمیم را به شیوه‌ای مفهوم و در دسترس ارائه دهند (Kaminski, 2019).

۳. نظریه نهادگرایی تنظیمی و بازتوزیع مسئولیت مدنی

الگوهای کلاسیک مسئولیت مدنی مبتنی بر تقصیر، قابلیت اعمال مؤثر بر زنجیره‌های ارزش توزیع‌شده هوش مصنوعی (طراح، گردآورنده داده، بهره‌بردار) را ندارند (Hacker et al., 2023). بر اساس نظریه نهادگرایی تنظیمی، قانون‌گذار باید با معکوس‌سازی بار اثبات دلیل و استقرار امارات قانونی ناشی از نقض تکالیف فنی، توازن از دست‌رفته میان زیان‌دیده عامی و توسعه‌دهنده مقتدر فناوری را ترمیم کند (Migliorini, 2024).

۴. مبانی فقهی و حقوق اساسی ایران در مواجهه با مخاطرات نوین

در حقوق اساسی ایران، صیانت از کرامت انسانی (بند ۶ اصل دوم قانون اساسی) و برابری همگان در برابر قانون (اصل نوزدهم و بیستم) چارچوب بنیادین هرگونه خط‌مشی‌گذاری هستند. از منظر فقه امامیه نیز سه قاعده کلیدی راهگشاست:

– قاعده لاضرر: هرگونه ابزار فناورانه که زمینه اضرار ناموجه به حقوق، اموال یا حریم خصوصی افراد را فراهم آورد، مشروعیت اعمال نخواهد داشت و حاکمیت موظف به دفع ضرر محتمل است.

1. Black box

2. Right to explanation

- قاعده تسبیب: در الگوریتم‌های زنجیره‌ای، ایجاد بستری که نوعاً منتهی به خطا یا نقض حق دیگری گردد، انتساب ضمان به توسعه‌دهنده یا بهره‌بردار سهل‌انگار را توجیه می‌نماید.
- اصل وجوب حفظ نظام و دفع مفسده: اعمال حاکمیت و قضاوت، قائم به فرد واجد شرایط است و واگذاری صلاحیت انحصاری تصمیم‌گیری قضایی یا حاکمیتی به هوش مصنوعی بدون نظارت انسان، مغایر اصول حقوق عمومی اسلامی به شمار می‌آید.

پیشینه پژوهش

با فراگیری سامانه‌های هوشمند، بررسی ابعاد حقوقی هوش مصنوعی توجه پژوهشگران را در دو سطح داخلی و بین‌المللی به خود جلب کرده است. با این حال دامنه این مطالعات غالباً بر بخش‌های خاصی از حقوق متمرکز بوده و کمتر به الگوی جامع تنظیم‌گری پرداخته‌اند. در متون حقوقی ایران، توجه به پیامدهای حقوقی فناوری‌های خودکار عمدتاً با تمرکز بر مسئولیت مدنی و مالکیت فکری صورت گرفته است. ناطقی و بادینی (۱۴۰۳) با بررسی مبانی مسئولیت مدنی ناشی از سامانه‌های هوش مصنوعی، نشان دادند که رویکردهای سنتی تقصیرمحور نمی‌توانند ریسک‌های توزیع‌شده در سیستم‌های یادگیری ماشین را پوشش دهند و پیشنهاد نمودند که باید به سمت مسئولیت ناشی از خطر و الزام به پوشش‌های بیمه‌ای اجباری حرکت کرد.

ناطقی و بادینی (۱۴۰۳) چالش‌های مربوط به داده‌ها و برون داده‌های هوش مصنوعی را در پرتو نظام مالکیت فکری در پزشکی تحلیل کرده و استدلال نمودند که نظام سنتی نیازمند بازتعریف قواعد برای سازگاری با ماهیت خودکار الگوریتم‌هاست.

سایر مطالعات داخلی نیز غالباً نگاهی پسینی (تمرکز بر لحظه وقوع خسارت یا تولید اثر) داشته‌اند و خلأ یک چارچوب تنظیم‌گری پیشینی برای کل چرخه عمر داده و استنتاج‌های الگوریتمی در حقوق عمومی ایران همچنان مشهود است.

در سطح بین‌المللی، پژوهش‌ها از رویکرد صرفاً توصیفی فاصله گرفته و بر تحلیل چارچوب‌های هنجاری متمرکز شده‌اند.

وزال و بورخس^۱ (۲۰۲۱) در تحلیل پیش‌نویس قانون هوش مصنوعی اروپا نشان دادند که اتکای صرف به هنجارهای بازار داخلی بدون ابزارهای نظارتی بنیادین، ممکن است کارآمدی حقوق بنیادین را تضعیف کند. کامینسکی (۲۰۱۹) با طرح نظریه «شفافیت مشارکتی»، اثبات کرد که توضیح‌دهی الگوریتمی تنها در صورتی کارآمد است که همزمان متضمن طراحی سیستم پاسخگو و حق فردی بر نظارت باشد (Kaminski, 2019). همچنین، مانتلرو (۲۰۱۶؛ ۲۰۲۰) با نقد رویکرد فردگرایانه سنتی در قوانین حفاظت از داده، لزوم ارزیابی ریسک در سطح جمعی و اجتماعی را تبیین کرد (Mantelero, 2016; 2020).

مرور پژوهش‌های پیشین نشان می‌دهد که مطالعات داخلی عموماً به چالش‌های پسینی (مانند جبران خسارت پس از وقوع زیان) پرداخته و از سازوکارهای پیشگیرانه حقوق عمومی و نظارت نهادی غفلت کرده‌اند. از سوی دیگر پژوهش‌های غربی ساختار تنظیمی را متناسب با اسناد اتحادیه اروپا بررسی کرده‌اند، بدون آنکه قابلیت پیاده‌سازی آن را در یک نظام حقوقی مبتنی بر قانون اساسی و موازین فقهی بسنجند. نوآوری پژوهش حاضر در آن است که با پر کردن این خلأ، مدلی جامع و انطباقی ارائه می‌دهد که همزمان تکالیف پیشینی (مدیریت ریسک و نظارت انسانی) و ضمانت‌اجراهای پسینی را برای نظام حقوقی ایران صورتبندی می‌کند.

روش‌شناسی پژوهش

پژوهش حاضر از نظر هدف، پژوهشی کاربردی با ماهیت نظری و از نظر رویکرد، کیفی است. مسئله مورد بررسی، طراحی یک الگوی حقوقی برای حکمرانی پیش‌نگر داده‌های شخصی در مواجهه با هوش مصنوعی مولد است؛ از این رو پاسخ به پرسش پژوهش از طریق گردآوری داده‌های کمی یا سنجش آماری امکان‌پذیر نیست و نیازمند تحلیل مفاهیم، قواعد، اصول حقوقی و روندهای تنظیم‌گری مرتبط با فناوری‌های داده‌محور است. چارچوب پژوهش بر این فرض استوار نیست که آینده فناوری را می‌توان به صورت قطعی پیش‌بینی کرد بلکه تلاش می‌شود مجموعه‌ای از وضعیت‌های محتمل و پیامدهای حقوقی آنها شناسایی و بر مبنای آن، ظرفیت‌های لازم برای یک نظام حقوقی انعطاف‌پذیر استخراج شود.

1. Veale & Borgesius

روش اصلی پژوهش، تحلیل حقوقی - آینده‌پژوهانه است. در بخش حقوقی، مفاهیم حریم خصوصی، داده شخصی، پردازش داده، استنتاج الگوریتمی، شفافیت، پاسخگویی و تنظیم‌گری مبتنی بر ریسک مورد تحلیل قرار گرفته‌اند. هدف از این تحلیل صرفاً توصیف وضعیت موجود نیست، بلکه تعیین این مسئله است که هر یک از این مفاهیم در محیطی که هوش مصنوعی مولد قادر به تولید خروجی‌های جدید و ایجاد استنتاج درباره اشخاص است چه حدود و کارکردی خواهند داشت. از این حیث، پژوهش میان «داده اولیه»، «فرایند پردازش» و «پیامد تصمیم‌گیری» تمایز قائل می‌شود.

بخش آینده‌پژوهانه پژوهش بر مفهوم «آینده‌های بدیل» استوار است. در این رویکرد، یک آینده واحد و قطعی برای حقوق حریم خصوصی فرض نمی‌شود بلکه چند مسیر محتمل برای تحول رابطه میان داده، هوش مصنوعی و حقوق اشخاص در نظر گرفته می‌شود. در یک مسیر، سازوکارهای پیشگیرانه و پاسخگویی مؤثر گسترش می‌یابند و استفاده از داده در محدوده اصول حقوقی قرار می‌گیرد. در مسیر دیگر توسعه فناوری سریع‌تر از ظرفیت تنظیم‌گری پیش می‌رود و داده‌های شخصی به ابزار گسترده‌تری برای ارزیابی، طبقه‌بندی و نظارت تبدیل می‌شوند. هدف از طرح این وضعیت‌ها، پیش‌بینی قطعی آینده نیست، بلکه آزمون ظرفیت قواعد حقوقی در مواجهه با شرایط متفاوت است. برای تحلیل این آینده‌های بدیل، چهار مرحله در نظر گرفته شده است. در مرحله نخست، قابلیت‌های فناورانه‌ای که می‌توانند پیامد حقوقی داشته باشند، شناسایی می‌شوند از جمله تولید محتوا، ترکیب داده‌های پراکنده، استنتاج ویژگی‌های فردی، تولید توصیه یا گزارش و استفاده از خروجی در تصمیم‌گیری. قابلیت‌های مذکور صرفاً از منظر فنی مورد توجه قرار نمی‌گیرند بلکه آثار آنها بر حقوق اشخاص معیار تحلیل قرار می‌گیرد (Edwards, 2022; Wachter & Mittelstadt, 2019). در مرحله دوم، سوءجریان‌های محتمل در چرخه داده شناسایی می‌شوند. در این پژوهش سوءجریان به معنای هر فرایندی است که در آن داده شخصی، بدون تناسب با هدف مشروع، می‌تواند به تصمیم یا اقدامی علیه موقعیت حقوقی فرد منجر شود. کاهش بازده یا امتیازدهی نامتناسب بر اساس استنتاج الگوریتمی، قرار دادن شخص در معرض بازرسی بر اساس الگوهای مبهم، ایجاد سابقه یا روایت گمراه‌کننده از طریق ترکیب داده‌ها و استفاده ثانویه از اطلاعات خارج از زمینه اولیه،

نمونه‌هایی از این وضعیت‌ها هستند. این مرحله اهمیت ویژه‌ای دارد زیرا نشان می‌دهد که آسیب به حریم خصوصی الزاماً با افشای داده آغاز نمی‌شود و ممکن است در مرحله معناگذاری و استفاده از داده شکل گیرد (Gstrein & Kochenov, 2020; Mantelero, 2020).

در مرحله سوم، ظرفیت پاسخگویی و کنترل حقوقی ارزیابی می‌شود. در این مرحله پرسش‌هایی مانند امکان اطلاع شخص از پردازش، قابلیت فهم مبنای تصمیم، امکان اعتراض، قابلیت اصلاح داده یا خروجی، تعیین مسئولیت بازیگران و امکان نظارت مستقل مورد توجه قرار می‌گیرند. شفافیت الگوریتمی و حق توضیح در این مرحله اهمیت دارند اما پژوهش آنها را به‌عنوان اهداف مستقل تلقی نمی‌کند بلکه ارزش آنها را بر اساس میزان توانایی واقعی فرد برای اعمال حقوق خود ارزیابی می‌کند. در مرحله چهارم، مؤلفه‌های لازم برای الگوی پیشنهادی استخراج و در یک ساختار منسجم قرار می‌گیرند. این مؤلفه‌ها باید به گونه‌ای انتخاب شوند که هم قابلیت پیشگیری از سوءجریان را داشته باشند و هم در برابر تغییرات فناورانه انعطاف‌پذیر باشند. در این زمینه، رویکرد تنظیم‌گری مبتنی بر ریسک و حرکت از قواعد ثابت به سمت چارچوب‌های تطبیق‌پذیر مورد توجه قرار می‌گیرد (Hacker et al., 2023; Mantelero, 2016; Veale & Zuiderveen Borgesius, 2021).

از نظر تحلیل تطبیقی، تجربه‌های حقوقی و تنظیم‌گری بین‌المللی صرفاً به‌عنوان نمونه‌هایی برای اقتباس مستقیم بررسی نمی‌شوند. هدف، شناسایی اصول و سازوکارهایی است که می‌توانند در طراحی یک چارچوب حقوقی پیش‌نگر مورد استفاده قرار گیرند. تجربه اتحادیه اروپا در طبقه‌بندی ریسک‌های هوش مصنوعی، توجه به الزامات شفافیت و تعیین مسئولیت بازیگران، از این جهت اهمیت دارد که نشان می‌دهد تنظیم‌گری فناوری در حال حرکت به سمت رویکردهای پیشگیرانه و چندسطحی است (Kaminski, 2019; Mantelero, 2020). همچنین، بحث حاکمیت دیجیتال نشان می‌دهد که کنترل داده و فناوری تنها مسئله‌ای فردی نیست و با ظرفیت نهادهای عمومی و نظام حقوقی برای اعمال کنترل مؤثر بر زیرساخت‌های داده‌ای نیز ارتباط دارد (Yeung, 2018).

اعتبار تحلیلی پژوهش از طریق تطبیق مستمر میان مسئله، مبانی نظری، سناریوهای بدیل و مؤلفه‌های الگوی پیشنهادی تأمین می‌شود. به این معنا که هر مؤلفه پیشنهادی باید بتواند دست‌کم یکی از خلأهای شناسایی‌شده در چرخه داده را پوشش دهد و در برابر بیش از یک وضعیت آینده

قابلیت اعمال داشته باشد. از سوی دیگر، از تعمیم نتایج فراتر از قلمرو موضوع پژوهش اجتناب شده است؛ بنابراین، الگوی ارائه‌شده به‌عنوان چارچوبی حقوقی برای سیاست‌گذاری و تنظیم‌گری پیش‌نگر پیشنهاد می‌شود نه نسخه‌ای قطعی برای تمام نظام‌های حقوقی.

در نهایت، فرایند تحلیل به استخراج الگویی چندلایه منتهی می‌شود که رابطه میان پیش‌بینی خطر، مدیریت داده، کنترل استنتاج، پاسخگویی، حقوق اعتراض و انعطاف‌پذیری مقرراتی را در یک ساختار واحد قرار می‌دهد. این الگو در بخش یافته‌ها به‌صورت تفصیلی تشریح خواهد شد و هر یک از مؤلفه‌های آن از منظر قابلیت اجرا، نقش آن در جلوگیری از سوءجریان و میزان سازگاری با آینده‌های بدیل حقوق حریم خصوصی ارزیابی خواهد شد.

یافته‌های پژوهش

تحلیل مسئله نشان می‌دهد که یکی از مهم‌ترین کاستی‌های رویکردهای سنتی حریم خصوصی، تمرکز بیش از اندازه بر خود داده و غفلت نسبی از فرایندی است که داده طی آن به تصمیم و اثر حقوقی تبدیل می‌شود. در محیط هوش مصنوعی مولد، یک داده شخصی ممکن است به‌تنهایی فاقد اهمیت خاصی باشد اما هنگامی که با مجموعه‌ای از داده‌های دیگر ترکیب شود، بتواند اطلاعاتی جدید درباره شخص ایجاد کند. بنابراین نقطه‌ای که باید تحت حمایت حقوقی قرار گیرد، تنها لحظه جمع‌آوری یا افشای داده نیست بلکه تمام چرخه‌ای است که در آن داده به شناخت، ارزیابی و در نهایت، اقدام درباره شخص تبدیل می‌شود.

بر این اساس چرخه حقوقی داده را می‌توان در شش مرحله متوالی در نظر گرفت: گردآوری، ذخیره و سازمان‌دهی، پردازش، استنتاج، تصمیم‌سازی و اثرگذاری. هر یک از این مراحل می‌تواند منشأ یک سوءجریان مستقل باشد. ممکن است داده در مرحله گردآوری به‌صورت مشروع به دست آمده باشد اما در مرحله پردازش برای هدفی متفاوت مورد استفاده قرار گیرد. همچنین ممکن است پردازش صحیح باشد اما استنتاج حاصل از آن فاقد اعتبار کافی باشد. حتی اگر استنتاج نیز از نظر آماری قابل دفاع باشد، استفاده از آن در یک تصمیم حساس می‌تواند نامتناسب یا ناقض حقوق فرد باشد.

این تفکیک سبب می‌شود مفهوم حریم خصوصی از یک حق ایستا به یک حق پویا تبدیل شود. شخص نه فقط باید در برابر افشای اطلاعات خود حمایت شود بلکه باید بتواند در برابر فرایندهایی که از اطلاعات مربوط به او برای شکل‌دهی به موقعیت حقوقی‌اش استفاده می‌کنند نیز از حمایت برخوردار باشد.

شناسایی سوء جریان‌های داده‌ای و الگوریتمی

بررسی چرخه یادشده نشان می‌دهد که سوء جریان‌های مرتبط با هوش مصنوعی مولد را می‌توان در چند گروه اصلی دسته‌بندی کرد:

- سوء جریان‌های ناشی از استفاده خارج از هدف اولیه: در این وضعیت، داده برای ارائه یک خدمت یا انجام یک فعالیت مشخص گردآوری شده اما در ادامه برای ارزیابی، نظارت یا تصمیم‌گیری دیگری مورد استفاده قرار می‌گیرد. مشکل اصلی در اینجا نه لزوماً دروغ بودن داده بلکه گسست میان هدف اولیه و کاربرد ثانویه است.

- سوء جریان‌های استنتاجی: در این حالت، سامانه از داده‌هایی که ممکن است به‌ظاهر عادی باشند، ویژگی یا نتیجه‌ای درباره شخص استخراج می‌کند. اهمیت این وضعیت در آن است که فرد ممکن است هیچ‌گاه آن ویژگی را اظهار نکرده باشد اما سامانه آن را به‌عنوان بخشی از پروفایل وی تولید کند. از آنجا که خروجی استنتاجی می‌تواند در تصمیم‌های بعدی مورد استفاده قرار گیرد، لازم است میان «داده ارائه‌شده توسط شخص» و «ویژگی منتسب‌شده به شخص» تمایز حقوقی برقرار شود.

- سوء جریان‌های روایی: هوش مصنوعی مولد قادر است مجموعه‌ای از داده‌ها را به شکل یک متن یا گزارش منسجم ارائه کند. همین قابلیت در صورت استفاده نادرست می‌تواند زمینه ایجاد تصویری غیر واقعی از شخص را فراهم کند. برای مثال چند رخداد بی‌ارتباط ممکن است در یک گزارش به‌گونه‌ای کنار یکدیگر قرار گیرند که چنین به نظر برسد فرد دارای الگویی خاص از رفتار است. در اینجا، خطر از جعل داده ناشی نمی‌شود بلکه از نحوه ترکیب و تفسیر آن ناشی می‌شود.

- سوء جریان‌های تصمیمی: این وضعیت زمانی رخ می‌دهد که خروجی هوش مصنوعی مستقیماً یا غیرمستقیم در تصمیمی درباره فرد مورد استفاده قرار گیرد. کاهش امتیاز عملکرد، محدودیت

دسترسی به یک خدمت، اولویت‌بندی برای بازرسی، ارزیابی اعتبار یا اعمال محدودیت‌های اداری، نمونه‌هایی از تصمیم‌هایی هستند که در صورت اتکا به خروجی‌های غیرقابل راستی‌آزمایی می‌توانند حقوق شخص را تحت تأثیر قرار دهند.

- سوء جریان‌های کاهش بازده و مسئله مشروعیت تصمیم الگوریتمی: یکی از مصادیق شایان توجه، استفاده از هوش مصنوعی برای ارزیابی عملکرد افراد است. فرض شود یک سازمان برای افزایش بهره‌وری، سامانه‌ای را به کار گیرد که اطلاعات مربوط به ساعات حضور، حجم کار، مکاتبات، زمان پاسخ‌گویی و سایر داده‌های کاری را تحلیل کند. سامانه ممکن است بر اساس الگوهای موجود، عملکرد فرد را پایین‌تر از سطح مورد انتظار ارزیابی کند. مشکل حقوقی از جایی آغاز می‌شود که این ارزیابی بدون توجه به زمینه شکل‌گیری داده‌ها به تصمیم سازمانی تبدیل شود. برای مثال، ممکن است کاهش تعداد مکاتبات فرد ناشی از انتقال او به وظایف پیچیده‌تر باشد اما الگوریتم آن را کاهش بهره‌وری تفسیر کند. یا ممکن است فرد ساعات کمتری در سامانه ثبت حضور داشته باشد اما بخش قابل توجهی از فعالیت خود را خارج از سامانه انجام داده باشد. در چنین شرایطی، داده خام ممکن است صحیح باشد، ولی نتیجه حاصل از آن لزوماً صحیح نیست.

الگوی پیشنهادی پژوهش اقتضا می‌کند که هیچ استنتاج الگوریتمی که بتواند موقعیت حقوقی یا شغلی فرد را به‌طور معنادار تغییر دهد، بدون ارزیابی زمینه‌ای و امکان مداخله انسانی مؤثر، مبنای تصمیم نهایی قرار نگیرد. همچنین شخص باید بتواند نسبت به نتیجه اعتراض کند و داده‌ها یا زمینه‌هایی را که سامانه در نظر نگرفته است ارائه دهد.

بنابراین «کاهش بازده» در این الگو یک مفهوم صرفاً مدیریتی نیست بلکه زمانی که نتیجه آن به کاهش حقوق، فرصت شغلی یا اعتبار حرفه‌ای فرد منجر شود، به مسئله‌ای حقوقی تبدیل می‌شود.

- سوء جریان‌های پرونده‌سازی داده‌محور و تولید واقعیت حقوقی کاذب: یکی از پیچیده‌ترین سوء جریان‌های احتمالی، ایجاد پرونده یا روایت منفی درباره یک فرد از طریق ترکیب داده‌های واقعی و استنتاج‌های الگوریتمی است. تفاوت این وضعیت با جعل سنتی در آن است که ممکن است هیچ‌یک از داده‌های مورد استفاده به‌تنهایی جعلی نباشند. مشکل از نحوه کنار هم قرار گرفتن آن‌ها و معنایی ناشی می‌شود که سامانه به مجموعه داده‌ها نسبت می‌دهد.

فرض شود اطلاعاتی درباره تماس‌های فرد، سوابق کاری، حضور در مکان‌های مختلف، فعالیت‌های عمومی و ارتباطات دیجیتال او در منابع گوناگون وجود داشته باشد. یک سامانه مولد می‌تواند این داده‌ها را در قالب گزارشی درباره «الگوی رفتاری» فرد تنظیم کند. اگر گزارش مذکور بدون بررسی مستقل وارد فرایند بازرسی یا ارزیابی شود، امکان دارد ارتباط‌های تصادفی به‌عنوان نشانه یک رفتار هدفمند تفسیر شوند.

در چارچوب دکرین حقوقی چنین وضعیتی نیازمند اصل تفکیک میان «واقعیت ثبت‌شده» و «استنتاج تولیدشده» است. هر داده‌ای که در یک گزارش الگوریتمی ظاهر می‌شود، نباید ارزش اثباتی یکسان داشته باشد. داده اولیه، استنتاج آماری، تحلیل تفسیری و نتیجه تصمیمی باید از یکدیگر تفکیک شوند تا شخص بتواند دقیقاً بداند کدام قسمت از فرایند را مورد اعتراض قرار می‌دهد.

الگوی پیشنهادی حکمرانی پیش‌نگر داده‌های شخصی

برآیند تحلیل‌های انجام‌شده نشان می‌دهد که حکمرانی پیش‌نگر داده‌های شخصی در محیط هوش مصنوعی مولد نمی‌تواند بر یک قاعده منفرد استوار باشد. پیچیدگی چرخه داده و تنوع آثار احتمالی آن بر حقوق اشخاص، وجود یک ساختار چندلایه را ضروری می‌سازد. الگوی پیشنهادی پژوهش بر شش لایه به‌هم‌پیوسته استوار است: پیش‌بینی و شناسایی خطر، تعیین هدف و حدود استفاده، کنترل فرایند استنتاج، پاسخگویی و نظارت، تضمین حقوق شخص موضوع داده و سازوکار تطبیق و بازنگری مقررات.

این لایه‌ها در ارتباط با یکدیگر عمل می‌کنند و ضعف هر یک می‌تواند اثربخشی سایر لایه‌ها را کاهش دهد. برای مثال اگر ارزیابی خطر انجام شود اما فرد امکان اعتراض به تصمیم نداشته باشد، نظام حکمرانی همچنان با خلأ جدی مواجه خواهد بود. به همین ترتیب اگر حق اعتراض پیش‌بینی شود، اما هیچ سازوکاری برای ثبت و مستندسازی فرایند تصمیم‌گیری وجود نداشته باشد امکان اعمال این حق در عمل محدود خواهد شد.

لایه نخست؛ پیش‌بینی و ارزیابی پیشینی خطر: نخستین لایه الگو، شناسایی خطر پیش از آغاز یا توسعه پردازش داده است. هر سازمان یا نهادی که قصد استفاده از هوش مصنوعی مولد برای

پردازش داده‌های شخصی دارد باید پیش از استقرار سامانه مشخص کند که کاربرد مورد نظر چه نوع خطری برای حقوق افراد ایجاد می‌کند.

ارزیابی خطر باید صرفاً به امنیت فنی سامانه محدود نباشد. موضوعاتی مانند احتمال ایجاد پروفایل نادرست، استنتاج ویژگی‌های شخصی، تبعیض، تولید اطلاعات نادرست درباره افراد، استفاده ثانویه از داده و امکان تبدیل خروجی سامانه به تصمیم زیان‌بار نیز باید مورد بررسی قرار گیرد.

شدت ارزیابی باید متناسب با میزان مداخله باشد. استفاده از هوش مصنوعی برای یک پردازش کم‌اهمیت با استفاده از آن در ارزیابی شغلی، اعتبار مالی، بازرسی یا تصمیم‌هایی که می‌توانند موقعیت حقوقی فرد را تغییر دهند، یکسان نیست. هرچه پیامد بالقوه شدیدتر باشد، ارزیابی پیشینی نیز باید دقیق‌تر و مستندتر انجام شود.

لایه دوم؛ تعیین هدف، ضرورت و حدود استفاده از داده: دومین لایه به تعیین مرز استفاده مشروع از داده مربوط می‌شود. در این مرحله باید مشخص شود که داده برای چه هدفی جمع‌آوری شده، برای چه هدفی قرار است مورد استفاده قرار گیرد و آیا میان این دو هدف ارتباط حقوقی قابل دفاع وجود دارد یا خیر.

در محیط هوش مصنوعی مولد خطر استفاده ثانویه اهمیت بیشتری پیدا می‌کند زیرا قابلیت پردازش و ترکیب داده‌ها می‌تواند کاربردهای جدیدی برای اطلاعات ایجاد کند. از این‌رو صرف دسترسی قانونی به داده نباید به معنای مجاز بودن هر نوع استفاده از آن تلقی شود.

اصل محدودیت هدف باید با یک اصل مکمل همراه شود و آن «حداقل‌گرایی داده‌ای» است. هرچه اطلاعات بیشتری وارد فرایند شود، احتمال ایجاد استنتاج‌های ناخواسته و تولید پروفایل‌های پیچیده افزایش می‌یابد. بنابراین باید فقط داده‌هایی وارد سامانه شوند که برای هدف مشخص و مشروع ضروری هستند.

لایه سوم؛ حکمرانی استنتاج و کنترل خروجی مولد: نوآوری اصلی الگو در این لایه قرار دارد. نظام‌های سنتی حفاظت از داده عمدتاً بر داده‌های ورودی تمرکز می‌کنند؛ اما در محیط هوش مصنوعی مولد، بخش قابل توجهی از خطر در خروجی و استنتاج شکل می‌گیرد.

بر اساس الگوی پیشنهادی، هر استنتاجی که بتواند بر حقوق یا موقعیت فرد اثر بگذارد باید قابلیت شناسایی، ارزیابی و کنترل داشته باشد. بنابراین خروجی سامانه باید از نظر نوع، منبع، درجه اطمینان و میزان ارتباط با داده‌های پایه طبقه‌بندی شود.

برای نمونه اگر سامانه در ارزیابی عملکرد کارکنان نتیجه بگیرد که فرد دارای «کاهش بازده» است، این نتیجه نباید بدون بررسی مشخص شود که بر چه داده‌هایی استوار بوده و چه عوامل زمینه‌ای نادیده گرفته شده‌اند. همچنین باید روشن باشد که آیا نتیجه حاصل از داده مستقیم است یا یک استنتاج احتمالی.

در مورد پرونده‌سازی داده‌محور نیز همین اصل اعمال می‌شود. گزارش تولیدشده توسط سامانه باید میان داده قطعی، داده تأییدنشده، استنتاج و تحلیل تفسیری تفکیک قائل شود. این تفکیک، امکان آن را فراهم می‌کند که شخص یا مقام نظارتی بتواند بخش مورد مناقشه را شناسایی و اصلاح کند. **لایه چهارم؛ پاسخگویی چندسطحی:** پاسخگویی در سامانه‌های هوش مصنوعی مولد نباید تنها بر استفاده‌کننده نهایی متمرکز باشد. زنجیره داده ممکن است شامل تولیدکننده مدل، ارائه‌دهنده زیرساخت، عرضه‌کننده داده، توسعه‌دهنده کاربرد و نهاد بهره‌بردار باشد. بنابراین مسئولیت باید متناسب با نقش هر بازیگر در فرایند تعیین شود.

در الگوی پیشنهادی برای هر مرحله از چرخه داده باید یک مسئول مشخص وجود داشته باشد. مسئولیت مبهم، یکی از مهم‌ترین عوامل کاهش کارایی حمایت حقوقی است. اگر معلوم نباشد چه کسی مسئول صحت داده، چه کسی مسئول نحوه پردازش و چه کسی مسئول تصمیم نهایی است فرد زیان‌دیده عملاً با مانع جدی در پیگیری حقوق خود مواجه خواهد شد.

ثبت سوابق پردازش نیز بخشی از پاسخگویی است. تصمیم‌های مهم باید به‌گونه‌ای مستندسازی شوند که امکان بازسازی مسیر رسیدن به نتیجه وجود داشته باشد. این مستندسازی نه به معنای افشای اسرار تجاری یا انتشار جزئیات فنی مدل بلکه به معنای فراهم کردن حداقل اطلاعات لازم برای نظارت و اعتراض است.

لایه پنجم؛ حقوق فرد در برابر تصمیم داده‌محور: حکمرانی پیش‌نگر بدون تضمین حقوق

شخص موضوع داده ناقص خواهد بود. فرد باید بتواند بداند که آیا اطلاعات مربوط به او در یک فرایند هوش مصنوعی مورد استفاده قرار گرفته است، هدف استفاده چه بوده و آیا خروجی سامانه در تصمیمی درباره او نقش داشته است.

حق اعتراض در این الگو اهمیت ویژه‌ای دارد. اعتراض نباید صرفاً یک امکان صوری باشد بلکه فرد باید بتواند نسبت به داده، استنتاج، نحوه پردازش و نتیجه تصمیم اعتراض کند. این چهار سطح اعتراض از یکدیگر متفاوت‌اند و هر یک مستلزم سازوکار خاص خود است.

همچنین، باید امکان اصلاح وجود داشته باشد. اگر سامانه بر اساس داده نادرست یا استنتاج نادرست تصمیمی تولید کرده باشد، اصلاح صرف داده اولیه ممکن است کافی نباشد. ممکن است لازم باشد خروجی‌های بعدی که بر مبنای آن استنتاج شکل گرفته‌اند نیز شناسایی و اصلاح شوند.

لایه ششم؛ تنظیم‌گری تطبیقی و قابلیت بازنگری: قانون‌گذاری در حوزه فناوری‌های مولد نمی‌تواند کاملاً ایستا باشد. هرچه فناوری سریع‌تر تغییر کند، احتمال ایجاد فاصله میان قواعد موجود و واقعیت فناورانه بیشتر خواهد شد. از این‌رو الگوی پیشنهادی بر تنظیم‌گری تطبیقی تأکید می‌کند. تنظیم‌گری تطبیقی به معنای بی‌ثباتی قانون نیست بلکه به معنای ایجاد سازوکارهایی است که امکان بازنگری دوره‌ای قواعد را فراهم کنند. مقررات باید اصول بنیادین مانند تناسب، ضرورت، پاسخگویی و حمایت از حقوق اشخاص را ثابت نگه دارند اما ابزارهای اجرایی و الزامات فنی بتوانند متناسب با تغییر فناوری اصلاح شوند.

این رویکرد به‌ویژه در حوزه هوش مصنوعی مولد اهمیت دارد، زیرا ممکن است یک کاربرد در زمان تصویب مقررات کم‌خطر تلقی شود اما با توسعه قابلیت‌های مدل یا تغییر شیوه استفاده، آثار آن افزایش یابد. نظام حقوقی باید بتواند بدون انتظار برای وقوع بحران، سطح مداخله و الزامات را تغییر دهد.

بحث و نتیجه‌گیری

گسترش هوش مصنوعی مولد، مسئله حمایت از داده‌های شخصی را از چارچوب سنتی حفاظت در برابر جمع‌آوری و افشای اطلاعات فراتر برده است. قابلیت این فناوری در ترکیب داده‌های پراکنده،

تولید استنتاج‌های جدید و تبدیل این استنتاج‌ها به مبنای ارزیابی و تصمیم‌گیری، موجب شده است که بخش مهمی از تهدیدهای نوین حریم خصوصی در مرحله‌ای شکل گیرد که در نظام‌های سنتی کمتر مورد توجه قرار گرفته است. در چنین شرایطی، ممکن است داده‌های مورد استفاده صحیح باشند اما نحوه ترکیب، تفسیر یا استفاده از آنها به تصمیمی منجر شود که موقعیت حقوقی فرد را بدون توجه کافی تحت تأثیر قرار دهد.

پژوهش حاضر با تمرکز بر این تحول، نشان داد که الگوی واکنشی حمایت از حریم خصوصی برای مواجهه با همه اشکال سوءجریان‌های داده‌ای و الگوریتمی کافی نیست. مواردی مانند کاهش بازده بر اساس ارزیابی ناقص الگوریتمی، ایجاد پرونده یا روایت گمراه‌کننده از طریق ترکیب داده‌های پراکنده، اولویت‌بندی افراد برای بازرسی بر اساس الگوهای مبهم و ایجاد استنتاج‌هایی درباره ویژگی‌های افراد، همگی می‌توانند بدون افشای مستقیم اطلاعات شخصی، آثار واقعی بر حقوق اشخاص ایجاد کنند. از این‌رو موضوع حمایت حقوقی باید از خود داده به چرخه اثرگذاری آن گسترش یابد.

بر اساس یافته‌های پژوهش، الگوی مناسب حکمرانی پیش‌نگر باید سه سطح به هم پیوسته داشته باشد. در سطح نخست، پیشگیری از طریق شناسایی خطر، تعیین هدف و ضرورت پردازش، حداقل‌سازی داده و ارزیابی اثر حقوقی انجام می‌شود. در سطح دوم، کنترل فرایند با نظارت انسانی مؤثر، کنترل استنتاج، ثبت‌پذیری و محدود کردن استفاده‌های ثانویه دنبال می‌شود. در سطح سوم، حقوق اعتراض، اصلاح داده و استنتاج، بازبینی تصمیم و تعیین مسئولیت، امکان واکنش مؤثر به خطا یا سوءجریان را فراهم می‌کند.

اهمیت این الگو در آن است که مسئولیت را صرفاً به مرحله وقوع خسارت موکول نمی‌کند. توسعه‌دهنده، ارائه‌دهنده و بهره‌بردار سامانه باید متناسب با نقشی که در ایجاد و کنترل خطر دارند، دارای تکالیف مشخص باشند و تصمیم‌گیری درباره حقوق افراد نیز نتواند صرفاً به خروجی یک سامانه هوش مصنوعی واگذار شود. کنترل انسانی زمانی معنا پیدا می‌کند که تصمیم‌گیرنده امکان رد، اصلاح و ارزیابی مستقل خروجی را داشته باشد.

از منظر آینده‌پژوهی حقوقی نیز یافته‌ها نشان می‌دهد که قانون‌گذاری نباید بر یک تصویر ثابت از آینده فناوری استوار شود. ممکن است توسعه هوش مصنوعی با افزایش ظرفیت نظارت و تصمیم‌گیری داده‌محور همراه شود یا نظام حقوقی بتواند همگام با تحول فناوری، سازوکارهای مؤثر کنترل را توسعه دهد. در هر دو وضعیت و در میان آینده‌های بدیل، قواعد حقوقی باید قابلیت بازنگری و تطبیق داشته باشند.

در نهایت پژوهش حاضر پیشنهاد می‌کند که حریم خصوصی در عصر هوش مصنوعی مولد به‌عنوان حقی برای جلوگیری از شکل‌گیری و استفاده ناموجه از تصویری داده‌محور درباره شخص نیز مورد توجه قرار گیرد. چنین برداشتی، امکان مواجهه حقوقی با خطرهایی را فراهم می‌کند که در آنها نقض حق نه از افشای مستقیم داده بلکه از استنتاج، طبقه‌بندی، ارزیابی یا تصمیم‌گیری بر مبنای داده ناشی می‌شود. حکمرانی پیش‌نگر، در این معنا، سازوکاری برای محدود کردن نوآوری نیست بلکه چارچوبی برای تضمین آن است که توسعه فناوری در فضایی صورت گیرد که حقوق اشخاص، پاسخگویی تصمیم‌گیرندگان و امکان اصلاح خطا از ابتدا در طراحی فرایندهای داده‌محور لحاظ شده باشد.

یافته‌های پژوهش آن است که حمایت مؤثر از حریم خصوصی در عصر هوش مصنوعی مولد با توسعه صرف قواعد مربوط به محرمانگی یا رضایت فردی حاصل نمی‌شود. مسئله اصلی در مرحله‌ای شکل می‌گیرد که داده از یک اطلاعات خام به یک استنتاج و سپس به یک تصمیم تبدیل می‌شود.

از این رو نظام حقوقی آینده باید موضوع حمایت خود را از «داده شخصی» به «فرایند تولید و استفاده از معنا درباره شخص» گسترش دهد. در این چارچوب، هر جا داده بتواند مبنای ارزیابی، طبقه‌بندی، بازرسی، نظارت یا تصمیم‌گیری درباره فرد قرار گیرد باید مجموعه‌ای از ضمانت‌های پیشینی و پسینی فعال شود.

بر این اساس الگوی پیشنهادی پژوهش بر این اصل بنیادین استوار است که هیچ سامانه هوش مصنوعی نباید صرفاً به دلیل توانایی فنی خود، اختیار تعیین موقعیت حقوقی افراد را به دست آورد.

فناوری می‌تواند ابزار تحلیل باشد اما مشروعیت تصمیم همچنان باید از قواعد حقوقی، تناسب، پاسخگویی و امکان اعتراض ناشی شود.

در نتیجه، حکمرانی پیش‌نگر داده را می‌توان رویکردی دانست که هدف آن توقف تحول فناورانه نیست بلکه جلوگیری از آن است که سرعت و پیچیدگی فناوری از ظرفیت حقوق برای حمایت از اشخاص پیشی گیرد. در چنین الگویی، حقوق پیش از وقوع سوءجریان مداخله می‌کند، در زمان پردازش بر مسیر داده نظارت دارد و پس از بروز خطا امکان اصلاح مؤثر را فراهم می‌کند. این سه ویژگی، بنیان اصلی الگوی پیشنهادی برای مواجهه با آینده‌های بدیل حقوق حریم خصوصی را تشکیل می‌دهند.

منابع

- ناطق، زهرا و بادینی، حسن (۱۴۰۳). نگرشی تحلیلی بر مسئولیت مدنی ناشی از به‌کارگیری هوش مصنوعی در پزشکی با مطالعه تطبیقی. حقوق پزشکی، ۱۸ (۵۹)، ۹۹-۱۱۲.
- Edwards, L. (2022). The EU Artificial Intelligence Act: A summary of the legal framework for artificial intelligence. *Artificial Intelligence and Law*, Hacker et al., 20230, 1-2Hacker et al., 2023.
- Gstrein, O. J. & Kochenov, D. V. (2020). Digital sovereignty: A concept for the digital age. *Journal of European Public Policy*, 2Miglorini, 2024(11), 1Mantelero, 2020Miglorini, 2024Miglorini, 2024-1Mantelero, 202095.
- Hacker, P., Engel, A. & Mauer, M. (202Hacker et al., 2023). Regulating ChatGPT and other Large Generative AI Models. *Proceedings of the 202Hacker et al., 2023 ACM Conference on Fairness, Accountability, and Transparency*, 1-8.
- Kaminski, M. E. (2019). The right to explanation, explained. *Berkeley Technology Law Journal*, Hacker et al., 20234(1), 189-218.
- Mantelero, A. (201Mantelero, 2020). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Review*, Hacker et al., 20232(2), 2Hacker et al., 20238-255.
- Mantelero, A. (2020). The future of data protection: Gold standard vs. global standard. *Computer Law & Security Review*, Hacker et al., 2023Mantelero, 2020, Yeung, 20185500.
- Miglorini, S. (2024). "More than Words": A Legal Approach to the Risks of Commercial Chatbots Powered by Generative Artificial Intelligence. *European Journal of Risk Regulation*, 15(2), 1-18.
- Veale, M. & Zuiderveen Borgesius, F. (2021). Demystifying the Draft EU Artificial Intelligence Act. *Computer Law Review International*, 22(4), 9Miglorini, 2024-112.
- Wachter, S. & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, 2019 (2), 494-Mantelero, 202020.
- Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505-52Hacker et al., 2023.