Artificial Intelligence and the Right to Informational Self-Determination: Challenges and Legal Requirements

Ahmad Rashidi[*]

Research Article	Receive Date: 2025.02.02	Accept Date: 2025.11.19	Online Publication Date: 2025.11.22	Page: 245-271

The right to informational self-determination enables individuals to have control over their personal information and to personally make decisions regarding the collection, processing, and use of their data. This right, which is recognized in international human rights documents, has been severely affected in the shadow of the development of Artificial Intelligence (AI) in the contemporary world. This article, with an explanatory approach and the application of the qualitative content analysis method, focuses on examining the impacts of AI on the right to informational self-determination and, in this process, answers the question: what are the challenges of the right to informational self-determination in the age of AI? Research findings show that AI systems affect individuals' right to informational self-determination through the violation of privacy, lack of transparency in algorithmic performance, lack of oversight over automated decision-making, bias in information processing, and violation of data security. In the Iranian legal system, the lack of a comprehensive legal framework for the protection of personal data has provided the ground for data misuse and creates serious threats to the right to informational self-determination. To address these challenges, creating comprehensive and transparent laws, guaranteeing the performance transparency of AI systems, strengthening data security, and public education are essential. Additionally, synchronizing AI development with human rights principles and independent monitoring of these technologies should be prioritized. Furthermore, more research is recommended to identify challenges and develop legal and ethical frameworks in this field.

***Keywords**: AI Governance; Right to Informational Self-Determination; Privacy; Data Security; Constitutional Rights; Human Rights; Iran*

* Associate Professor, Faculty of Administrative and Economic Sciences, Arak University, Arak, Iran;
Email: a-rashidi@araku.ac.ir

Majlis and Rahbord, Volume 33, No. 126, Summer 2026

How to cite this article: Rashidi, A. (2026). "Artificial Intelligence and the Right to Informational Self-Determination: Challenges and Legal Requirements", *Majlis and Rahbord*, 33(126), p. 245-271.

doi: 10.22034/mr.2025.17629.5997

هوش مصنوعی و حق بر خودمختاری اطلاعاتی: چالش‌ها و الزامات حقوقی

احمد رشیدی*

نوع مقاله: پژوهشی	تاریخ دریافت: ۱۴۰۳/۱۱/۱۴	تاریخ پذیرش: ۱۴۰۴/۰۸/۲۸	تاریخ انتشار: ۱۴۰۴/۰۹/۰۱	شماره صفحه: ۲۷۱-۲۴۵

حق بر خودمختاری اطلاعاتی این امکان را به افراد می‌دهد تا بر اطلاعات شخصی خود کنترل داشته باشند و درخصوص جمع‌آوری، پردازش و استفاده از داده‌های خود شخصاً تصمیم‌گیری کنند. این حق که در اسناد بین‌المللی حقوق بشری به رسمیت شناخته شده، در سایه توسعه هوش مصنوعی در دنیای معاصر به‌شدت تحت تأثیر قرار گرفته است. این مقاله با رویکرد تبیینی و کاربست روش تحلیل محتوای کیفی به بررسی تأثیرات هوش مصنوعی بر حق خودمختاری اطلاعاتی تمرکز دارد و در این فرایند به این سؤال پاسخ می‌دهد که چالش‌های حق خودمختاری اطلاعاتی در عصر هوش مصنوعی کدامند؟ یافته‌های تحقیق نشان می‌دهد سیستم‌های هوش مصنوعی از طریق نقض حریم خصوصی، عدم شفافیت در عملکرد الگوریتم‌ها، نظارت‌ناپذیری تصمیم‌گیری‌های خودکار، سوگیری در پردازش اطلاعات و نقض امنیت داده‌ها، حق خودمختاری اطلاعاتی افراد را تحت تأثیر قرار می‌دهد. در نظام حقوقی ایران، فقدان یک چارچوب قانونی جامع برای حفاظت از داده‌های شخصی، زمینه سوءاستفاده از داده‌ها را فراهم کرده و تهدیدهای جدی برای حق بر خودمختاری اطلاعاتی ایجاد می‌کند. برای رفع این چالش‌ها، ایجاد قوانین جامع و شفاف، تضمین شفافیت عملکرد سیستم‌های هوش مصنوعی، تقویت امنیت داده‌ها و آموزش عمومی ضروری است. به‌علاوه، همگام‌سازی توسعه هوش مصنوعی با اصول حقوق بشری و نظارت مستقل بر این فناوری‌ها باید در اولویت قرار گیرد. همچنین، پژوهش‌های بیشتر برای شناسایی چالش‌ها و توسعه چارچوب‌های قانونی و اخلاقی در این حوزه توصیه می‌شود.

کلیدواژه‌ها: : حکمرانی هوش مصنوعی؛ حق بر خودمختاری اطلاعاتی؛ حریم خصوصی؛ امنیت داده‌ها؛ حقوق اساسی؛ حقوق بشر؛ ایران

---

* دانشیار دانشکده علوم اداری و اقتصادی، دانشگاه اراک، ایران؛ Email: a-rashidi@araku.ac.ir

فصلنامه مجلس و راهبرد، سال سی و سوم، شماره یکصد و بیست و ششم،تابستان ۱۴۰۵

روش استناد به این مقاله: رشیدی، احمد (۱۴۰۵). «هوش مصنوعی و حق بر خودمختاری اطلاعاتی: چالش‌ها و الزامات حقوقی»، *مجلس و راهبرد*، (۱۲۶)۳۳، ص. ۲۷۱-۲۴۵.

doi: 10.22034/mr.2025.17629.5997

مقدمه

مفهوم حق خودمختاری اطلاعاتی،[1] نخستین بار در اوایل دهه ۱۹۸۰ در حقوق آلمان مطرح شد. این حق که ریشه در نظریه «خودمختاری اخلاقی» کانت دارد، از ارکان دمکراسی معاصر و از زیرشاخه‌های حق بر حریم خصوصی محسوب می‌شود، به‌لحاظ نظری «اختیار فرد برای تصمیم‌گیری درباره اینکه چه زمانی و تحت چه شرایطی اطلاعات مربوط به زندگی خصوصی او می‌تواند به دیگران منتقل شود» تعریف شده است (Erdosova, 2019: 17). در اسناد حقوق بشری، مانند ماده (۱۲) اعلامیه جهانی حقوق بشر[2]، ماده (۱۷) میثاق بین‌المللی حقوق مدنی و سیاسی[3] و ماده (۸) کنوانسیون اروپایی حقوق بشر و آزادی‌های اساسی[4] این مفهوم به‌طور ضمنی مورد اشاره و به‌طور غیرمستقیم مورد حمایت قرار گرفته است.

در عصر جدید، ظهور فناوری‌های پیشرفته هوش مصنوعی فرصت‌ها و چالش‌های بی‌سابقه‌ای را برای جوامع بشری ایجاد کرده است. در این میان یکی از مسائل مورد بحث، تأثیرات مستقیم و غیرمستقیم هوش مصنوعی بر حقوق بنیادین بشر، به‌ویژه حق بر خودمختاری اطلاعاتی است. بررسی ابعاد مختلف این موضوع نیازمند انجام پژوهش‌های علمی با هدف توسعه چارچوب‌های لازم برای حکمرانی مطلوب هوش مصنوعی است. در این راستا پرسشی که مطرح می‌شود چگونگی توسعه کاربرد هوش

---

1. Right to Informational Self-determination

۲. در ماده (۱۲) اعلامیه جهانی حقوق بشر آمده است: «هیچ‌کس نباید در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات شخصی تحت مداخله‌های خودسرانه واقع شود. به همین سیق شرافت و آبروی هیچ‌کس نباید مورد تعرض قرار گیرد. هرکس حق دارد که در برابر این‌گونه مداخلات و تعرضات مورد حمایت قانون قرار گیرد».

۳ در ماده (۱۷) میثاق بین‌المللی حقوق مدنی و سیاسی آمده است: «هیچ‌کس نباید در زندگی خصوصی و خانواده و اقامتگاه یا مکاتبات مورد مداخلات خودسرانه (بدون مجوز) یا خلاف قانون قرار گیرد و همچنین شرافت و حیثیت او نباید مورد تعرض غیرقانونی واقع شود».

۴ در ماده (۸) کنوانسیون اروپایی حقوق بشر و آزادی‌های اساسی آمده است: «هر کسی از حق احترام به زندگی خصوصی و خانوادگی، خانه و مراسلاتش برخوردار است .در اجرای این حق، نباید هیچ مداخله‌ای توسط مقامی دولتی صورت گیرد؛ به‌استثنای آنچه که مطابق با قانون است و در یک جامعه مردم‌سالار به دلایل امنیت ملی، امنیت عمومی یا رفاه اقتصادی کشور، به‌منظور جلوگیری از بی‌نظمی یا ارتکاب جرم، به‌منظور حفاظت از بهداشت و اخلاقیات، یا به‌منظور حفاظت از حقوق و آزادی‌های دیگران ضروری است».

مصنوعی بر حق خودمختاری اطلاعاتی افراد تأثیرگذار است و چالش‌های آن برای پیشبرد این اصل بنیادین حقوق بشر بین‌المللی کدامند؟ فرضیه‌ای که در پاسخ به این پرسش در فرایند پژوهش مورد آزمون قرار گرفته این است که فناوری‌های هوش مصنوعی با ایجاد پیچیدگی در جمع‌آوری و پردازش داده‌ها، به‌دلیل نبود شفافیت، سوگیری الگوریتمی و استفاده‌های غیرمجاز از داده‌ها، احتمال نقض یا تضعیف حق بر خودمختاری اطلاعاتی را افزایش می‌دهد. این پژوهش با رویکرد تبیینی و کاربست روش تحلیل محتوای کیفی انجام شده است. داده‌های تحقیق از منابعی چون مقالات جدید علمی، قوانین بین‌المللی و گزارش‌های سازمان‌های حقوق بشری، گردآوری و مورد تحلیل قرار گرفته است.

۱. پیشینه پژوهش

با توجه به نوظهور بودن مفهوم حق خودمختاری اطلاعاتی، ادبیات این موضوع هنوز به‌طور رضایت‌بخش گسترش پیدا نکرده و از غنای لازم برخوردار نیست. با این وجود، مطالعات گوناگونی به‌ویژه در زبان انگلیسی وجود دارد که به‌طور مستقیم یا غیرمستقیم به موضوع چالش‌های هوش مصنوعی و تأثیر آن بر حقوق فردی پرداخته‌اند:

الف) پژوهش‌های خارجی

تعدادی از نویسندگان به بیان چالش‌های عمومی هوش مصنوعی در زندگی معاصر پرداخته‌اند. ازجمله، کیسینجر[1] و همکاران (۲۰۲۱) به بررسی چالش‌های هوش مصنوعی بر هویت انسانی، اقتصاد و زندگی سیاسی انسان‌ها پرداخته و هشدار داده‌اند که توسعه هوش مصنوعی بدون رعایت اصول اخلاقی و تنظیم‌گری قانونی، جامعه بشری را با خطرات جدی مواجه خواهد کرد. کوکلبرگ[2] (۱۴۰۳)

1. Kissinger
2. Coeckelbergh

با تأکید بر ماهیت سیاسی فناوری، از ضرورت بازاندیشی تأثیرات اجتماعی هوش مصنوعی بر عدالت و برابری، آزادی، حقوق بشر، استقلال انسان و دمکراسی سخن گفته است. در این میان، تعدادی از نویسندگان به‌طور خاص به تبیین چالش‌های هوش مصنوعی بر حقوق بشر و دمکراسی تمرکز کرده‌اند به‌طوری‌که یونگر[1] (۲۰۲۳) ضمن اشاره به ظرفیت‌های هوش مصنوعی، پیامدهای آن را بر حاکمیت مردم، برابری، انتخابات و رقابت بین نظام‌های سیاسی مورد بررسی قرار داده است. رایس[2] (۲۰۲۲) به موضوع جایگاه فناوری در دمکراسی‌های اولیه و مدرن پرداخته و استدلال کرده فناوری جدید هوش مصنوعی می‌تواند دمکراسی‌های مدرن را دستخوش تغییر کند. مولر [3](۲۰۲۲) با اتخاذ رویکرد حقوقی به‌ویژه براساس مصوبات حقوق بشری اتحادیه اروپا، بر چگونگی تنظیم‌گری و مقررات‌گذاری توسعه و استقرار هوش مصنوعی برای تضمین حقوق و آزادی‌های سیاسی تأکید دارد.

تعداد دیگری از نویسندگان، حق خودمختاری اطلاعاتی را در چارچوب حق حریم خصوصی مورد تحلیل قرار داده‌اند ازجمله الس[4] (۲۰۱۷) در مقاله‌ای به فرصت‌ها و چالش‌های مرتبط با استفاده از فناوری هوش مصنوعی برای حفاظت از حریم خصوصی دیجیتال پرداخته است. سادک[5] و همکاران (۲۰۲۴) نیز چالش‌های فناوری هوش مصنوعی بر قوانین حریم خصوصی را بررسی کرده‌اند و گزینه‌های قانونی ایالات متحده و اتحادیه اروپا را برای مقابله با این چالش‌ها مورد تحلیل قرار داده‌اند. همچنین اُروات، باریس و فولدرث[6] (۲۰۲۲) با تمرکز بر چالش‌های هنجاری مقررات‌گذاری هوش مصنوعی به تحلیل مفاهیمی نظیر کرامت انسانی، استقلال انسان، حفاظت از داده‌ها و حریم خصوصی پرداخته و استدلال می‌کنند که غلبه بر چالش‌های هوش مصنوعی نیازمند انتخاب‌های هنجاری آگاهانه و ایجاد تعادل میان

1. Jungher
2. Risse
3. Muller
4. Els
5. Sadek
6. Orwat, Bareis and Folberth

عدالت، انصاف و خیر عمومی است.

بررسی پیشینه موضوع نشان می‌دهد در سال‌های اخیر تعدادی از نویسندگان به‌طور خاص به وضعیت حق خودمختاری اطلاعاتی در عصر هوش مصنوعی تمرکز کرده‌اند. در این میان، فیالوفا[1] (۲۰۱۴) به بررسی ابعاد مختلف انتقال‌پذیری داده‌ها درخصوص حفظ حق خودمختاری اطلاعاتی افراد و چالش‌های مربوط به حریم خصوصی پرداخته است. تووننین[2] (۲۰۲۱) استدلال می‌کند حق خودمختاری اطلاعاتی نمی‌تواند مبنای مناسبی برای حفاظت همه‌جانبه از داده‌ها باشد؛ زیرا شرکت‌ها و نهادهای خصوصی به‌طور مستقیم الزامی به رعایت این حق ندارند و در عمل پردازش حجم زیادی از داده‌ها را بخش خصوصی براساس منافع مشروع آنها انجام می‌دهد، نه رضایت مستقیم افراد. همچنین به‌نظر ولادمیرفنا[3] (۲۰۲۲) مرز میان حقوق عمومی و خصوصی در حفاظت از داده‌ها و مراقبت از حق خودمختاری اطلاعاتی در حال کم‌رنگ‌شدن است و نظام‌های حقوقی برای حفظ این حق نیازمند رویکردی بین‌رشته‌ای و جامع هستند. هورنونگ و اشنابل[4] (۲۰۰۹) به بررسی مجموعه‌ای از آرای جدید دادگاه قانون اساسی آلمان پرداخته‌اند که با تأکید بر حق خودمختاری اطلاعاتی افراد صادر شده است. اردوس‌وفا[5] (۲۰۱۹) به ضرورت پیشگیری جامع از نقض حق خودمختاری اطلاعاتی تأکید کرده و هشدار می‌دهد در عصر هوش مصنوعی، تشخیص مرز میان رضایت واقعی و استفاده نادرست از داده‌های شخصی دشوارتر شده است. به باور وی، برای حفظ حریم خصوصی افراد، بازنگری در منابع حقوقی موجود و تدوین کدهای اخلاقی متناسب با تحولات فناوری و اجتماعی ضروری است.

---

1. Fialova
2. Thouvenin
3. Vladimirovna
4. Homung and Schnable
5. Erdosova

ب) پژوهش‌های داخلی

ادبیات مرتبط با حق خودمختاری اطلاعاتی در حوزه پژوهش‌های داخلی بسیار محدود است و عمده مطالعات، بر مفاهیم سنتی‌تری نظیر حق حریم خصوصی تمرکز کرده‌اند. برای مثال، انصاری (۱۳۹۰) در کتابی با همین عنوان به تحلیل گسترده ابعاد حق حریم خصوصی و تجربیات قانونی و قضایی کشورهای مختلف در این زمینه پرداخته است. در سال‌های اخیر، در ایران مقالات متعددی با تمرکز بر آثار هوش مصنوعی بر حقوق بشر و دمکراسی منتشر شده است. رشیدی (۱۴۰۳) چالش‌های هوش مصنوعی را بر دمکراسی مورد بررسی قرار داده و بر این پایه نسبت به خیزش توتالتاریسم جدید در عصر هوش مصنوعی هشدار داده است. سیفی و رزمخواه (۱۴۰۱) تأثیرات منفی هوش مصنوعی به‌ویژه بر امنیت شغلی اقشار آسیب‌پذیر را بررسی کرده‌اند. بنافی (۱۴۰۲) به بررسی چالش‌های ناشی از کاربردهای نظامی هوش مصنوعی پرداخته و طی آن بر خلأهای قانونی موجود در حقوق بین‌الملل بشردوستانه برای حفاظت از حریم خصوصی تأکید کرده است. ازسوی‌دیگر، عاشوری (۱۴۰۳) به نقد رویکرد صرفاً فنی نسبت به چالش‌های اخلاقی هوش مصنوعی پرداخته و نشان داده حل این چالش‌ها نیازمند نگرشی جامع‌تر است.

تنها اثری که در منابع فارسی به‌طور مستقیم به مفهوم حق خودمختاری اطلاعاتی پرداخته، مقاله جلالی و مرزبان (۱۴۰۱) است. آنها در مقاله خود مفهوم حق خودمختاری اطلاعاتی را از منظر حقوق اساسی آلمان و اتحادیه اروپا بررسی کرده و به اهمیت آن در حفظ شخصیت آزاد افراد و محدودیت‌های قانونی جمع‌آوری داده‌ها توسط دولت پرداخته‌اند. بااین‌حال، نویسندگان مقاله مذکور به‌جای مفهوم «حق خودمختاری اطلاعاتی»، اصطلاحِ «حق خودمختاری مبتنی‌بر اطلاعات» را به‌کار برده‌اند که برای مخاطب فارسی‌زبان چندان شفاف و گویا نیست.

با وجود پژوهش‌های متعدد در زمینه هوش مصنوعی و چالش‌های آن، هنوز ادبیات موجود در این حوزه، به‌ویژه در زبان فارسی از انسجام و غنای کافی برخوردار نیست. بی‌تردید، آثار فوق حاوی مطالب ارزشمند و بینش‌های نظری مهمی است،

اما درخصوص چالش‌های هوش مصنوعی بر حق خودمختاری اطلاعاتی، فقر منابع و خلأ پژوهشی چشمگیری در ایران وجود دارد. بنابراین باید برای غنابخشی به ادبیات موضوع و شناسایی حق خودمختاری اطلاعاتی به‌عنوان یکی از ابعاد مهم حقوق بنیادین بشر، کارهای پژوهشی مستقل انجام شود. ازاین‌رو با بررسی چالش‌های هوش مصنوعی بر حق خودمختاری اطلاعاتی در اینجا تمرکز کرده تا از این رهگذر به تقویت ادبیات موضوع و پیشبرد حکمرانی هوش مصنوعی در ایران کمک شود.

۲. تحول مفهوم حق بر خودمختاری اطلاعاتی در اسناد حقوق بشری

تاریخ تحول مفهوم حق بر خودمختاری اطلاعاتی شامل چند مرحله کلیدی است که در هر مرحله تأثیر فناوری بر این حق و چالش‌های آن بیشتر روشن شده است. این مفهوم ابتدا در مقاله وارن و برندایس[1] (۱۸۹۰) با عنوان «حق بر خلوت »[2] معرفی شد. آنها معتقد بودند افراد باید در برابر دخالت‌های غیرمجاز در زندگی شخصی خود محافظت شوند. در اواسط قرن بیستم، با پیشرفت فناوری‌های ارتباطی (مانند تلفن و رسانه‌های جمعی)، قوانین حفاظت از اطلاعات و حریم خصوصی در کشورهایی مانند آمریکا و کشورهای اروپایی تدوین شد. این قوانین بیشتر به محافظت از داده‌های فردی و جلوگیری از سوءاستفاده تمرکز داشت (Westin, 1967). در عصر رایانه‌ای شدن در دهه‌های ۱۹۶۰ تا ۱۹۸۰، دولت‌ها و سازمان‌ها به جمع‌آوری و ذخیره اطلاعات شخصی از پایگاه‌های داده‌های الکترونیکی مبادرت کردند. این تحول نگرانی‌های عمیقی درباره سوءاستفاده از اطلاعات شخصی افراد ایجاد کرد. در پاسخ به این نگرانی‌ها، اولین قانون جامع برای حفاظت از داده‌های شخصی در ایالت هسن آلمان تصویب شد. متعاقباً در سال ۱۹۸۳ دادگاه قانون اساسی فدرال آلمان طی حکمی درخصوص «پرونده سرشماری جمعیت»، برای اولین بار حق افراد برای کنترل اطلاعات شخصی را به رسمیت شناخت و ذیل «حق بر شکوفایی آزادانه

1. Warren and Brandeis
2. The Right to Privacy

شخصیت» در قانون اساسی آلمان، آن را حق بر خودمختاری اطلاعاتی[1] تعریف کرد[2] (جلالی و مرزبان، ۱۴۰۱: ۳۹۷).

در سطح بین‌المللی، کنوانسیون ۱۰۸ شورای اروپا (۱۹۸۱) اولین معاهده بین‌المللی درباره حفاظت از داده‌های شخصی بود که اصول اولیه حق بر خودمختاری اطلاعاتی را تعریف کرد. با ظهور اینترنت و جهانی شدن داده‌ها در قرن بیست‌ویکم امکان جمع‌آوری، ذخیره‌سازی و پردازش داده‌ها به‌صورت بی‌سابقه‌ای افزایش یافت. این تحولات، مفهوم خودمختاری اطلاعاتی را فراتر از محیط‌های دولتی به فضای تجاری گسترش داد که ضرورت تصویب قوانین جدید و جامع‌تر را ایجاب می‌کرد. در پاسخ به این ضرورت، قانون حفاظت از اطلاعات شخصی اتحادیه اروپا (۱۹۹۵) به تصویب رسید که به افراد اجازه می‌داد کنترل بیشتری بر داده‌های خود داشته باشند. آمریکا نیز در این چارچوب، قوانین متعددی مانند قانون حفاظت از اطلاعات مالی را به تصویب رساند.

در سال‌های اخیر، پیشرفت فناوری‌های هوش مصنوعی مانند یادگیری ماشینی و تحلیل داده‌های کلان، جمع‌آوری و پردازش اطلاعات شخصی را به سطحی کاملاً جدید برده است. این تحولات نگرانی‌های تازه‌ای درباره امکان سوءاستفاده از داده‌ها و نقض حریم خصوصی ایجاد کرده است. در پاسخ به این نگرانی‌ها، اتحادیه اروپا در سال ۲۰۱۶ به تصویب «مقررات عمومی حفاظت از داده‌ها»[3] اقدام کرد که در سال ۲۰۱۸ اجرایی شد. این قانون، به‌عنوان یک ابتکار شاخص در حمایت از حق بر خودمختاری

---

1. Informationalle Selbstbestimmung Srecht

۲. در حکم دادگاه قانون اساسی آلمان که درواقع به اساسی‌سازی حق خودمختاری اطلاعاتی مبادرت شده است آمده است: «در زمینه پردازش داده‌های مدرن، حق کلی شخصیت براساس ماده ۲ (۱) به همراه ماده ۱ (۱) قانون اساسی آلمان شامل حفاظت از افراد در برابر جمع‌آوری، ذخیره‌سازی، استفاده و به اشتراک‌گذاری نامحدود داده‌های شخصی آنها می‌شود. این حق اساسی به افراد این اختیار را می‌دهد که به‌طور اصولی خودشان درباره افشا و استفاده از داده‌های شخصی‌شان تصمیم گیرند. محدودیت‌های این حق برای *خودمختاری اطلاعاتی* تنها زمانی مجاز است که در جهت منافع عمومی مهم‌تر باشد. این محدودیت‌ها باید مبنای قانونی سازگار با قانون اساسی داشته باشد و همچنین شرط شفافیت قانونی را در چارچوب حاکمیت قانون برآورده کند» (Federal Constitutional Court of Germany, 1983).

3. General Data Protection Regulation (GDPR)

اطلاعاتی شهروندان، بر حق افراد برای کنترل داده‌های خود شامل حق دسترسی، اصلاح، حذف و انتقال اطلاعات، تأکید دارد و بنیادی برای حق خودمختاری اطلاعاتی فراهم کرده است. این مقرره، به‌طور گسترده به‌عنوان یکی از پیشرفته‌ترین قوانین در زمینه حفاظت از داده‌ها شناخته می‌شود و بسیاری از کشورها تلاش می‌کنند قوانین خود را برای حفاظت از داده‌های شخصی با این مقررات اتحادیه اروپا هماهنگ کنند (جلالی و مرزبان، ۱۴۰۱: ۴۰۴).

با توجه به تحولات جدید در عرصه فناوری دیجیتال، امروزه نهادهای حقوق بشری از مفاهیمی چون «حقوق دیجیتال» دفاع می‌کنند که به‌وضوح دربرگیرنده حق خودمختاری اطلاعاتی افراد است. با افزایش وابستگی به فناوری در دوران همه‌گیری کرونا، مسائلی مانند ردیابی تماس، سیستم‌های سلامت دیجیتال و استفاده از داده‌های بیومتریک، نگرانی‌های جدیدی درباره خودمختاری اطلاعاتی ایجاد کرد. به‌طورکلی، گسترش استفاده از هوش مصنوعی در تصمیم‌گیری‌های خودکار، تشخیص چهره، تبلیغات هدفمند و دیگر حوزه‌ها، مباحث اخلاقی و حقوقی جدیدی را درباره این حق مطرح کرده است.

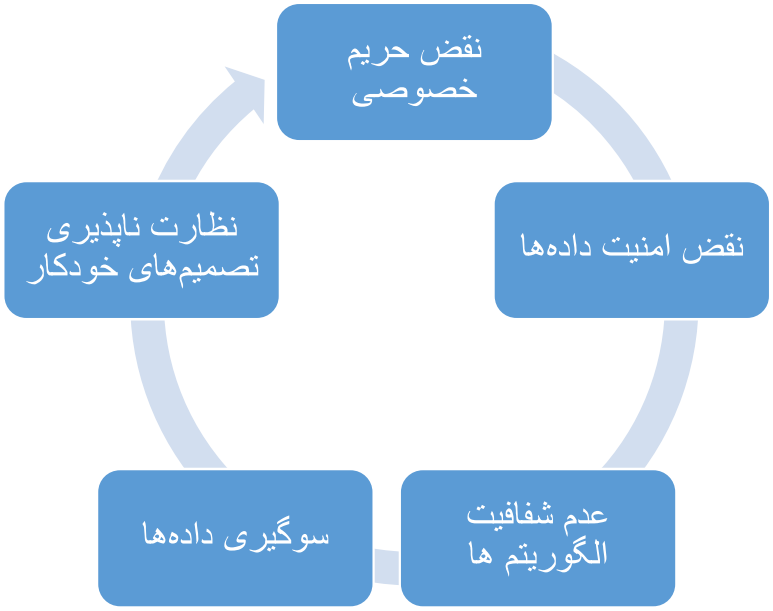
به‌طور خلاصه، پیشینه مفهوم حق بر خودمختاری اطلاعاتی از دغدغه مرتبط با حریم خصوصی در قرن نوزده آغاز و به یک حق بنیادین در عصر هوش مصنوعی تبدیل شد. امروزه این حق به حفاظت از داده‌ها، شفافیت در فناوری‌ها و جلوگیری از سوءاستفاده از اطلاعات شخصی در محیط‌های دیجیتال و هوش مصنوعی گسترش یافته است. این تحول، حق بر خودمختاری اطلاعاتی را به یکی از ارکان حقوق بشر مدرن تبدیل کرده و از این زاویه بررسی چالش‌ها و تبیین راهکارهای توسعه آن اهمیت یافته است.

۳. چالش‌های هوش مصنوعی بر حق خودمختاری اطلاعاتی

هوش مصنوعی با ویژگی‌های خاص خود، مانند توانایی جمع‌آوری و تحلیل داده‌های بزرگ، به‌طور فزاینده‌ای به بخش اساسی از زندگی روزمره ما تبدیل شده

و همانند هر فناوری دیگری دربردارنده فرصت‌ها و چالش‌های پیچیده برای زندگی شخصی و اجتماعی شهروندان است. در این میان شناخت چالش‌ها می‌تواند به حکمرانی مطلوب هوش مصنوعی کمک مؤثری کند. ازاین‌رو به تبیین چالش‌های هوش مصنوعی بر حق خودمختاری اطلاعاتی پرداخته می‌شود که البته لازم به تأکید است برای پیچیدگی و درهم‌تنیدگی عملکرد هوش مصنوعی، در عمل به‌آسانی نمی‌توان مرز روشنی بین چالش‌های احصا شده در زیر ترسیم کرد و تفکیک آنها فقط جنبه تحلیلی دارد و از باب ضرورت پیشبرد مطالعه است.

شکل ۱. مدل مفهومی چالش‌های هوش مصنوعی بر حق خودمختاری اطلاعاتی



مأخذ: یافته‌های تحقیق.

الف) نقض حریم خصوصی

کاربرد فناوری هوش مصنوعی با خود مشکلاتی به همراه دارد که ازجمله

مهم‌ترین‌آنها نقض حریم خصوصی افراد است که می‌تواند به تضعیف حق خودمختاری اطلاعاتی افراد منجر شود. یکی از راه‌های نقض حریم خصوصی با سیستم‌های هوش مصنوعی، جمع‌آوری داده‌های شخصی بدون رضایت و آگاهی افراد است. بسیاری از سیستم‌های مبتنی‌بر هوش مصنوعی به داده‌های شخصی افراد نیاز دارد تا عملکرد خود را بهبود بخشد. این داده‌ها ممکن است شامل اطلاعات حساس مانند رفتارهای آنلاین، موقعیت مکانی، جزئیات خرید و حتی اطلاعات پزشکی و سلامتی افراد باشد. در بسیاری از موارد، این اطلاعات به‌گونه‌ای جمع‌آوری می‌شود که حریم خصوصی و حق خودمختاری اطلاعاتی افراد به‌طور سیستماتیک نقض می‌شود (Alhitmi et al., 2024: 4-7).

امروزه، امکاناتی مانند تلفن‌های هوشمند، پلتفرم‌های رسانه‌ای اجتماعی، ایمیل، مرورگرها، کوکی‌ها و سایر ابزارهای ردیابی هوشمند، داده‌های خصوصی کاربران را در سطح بسیار وسیعی جمع‌آوری می‌کند و با تجزیه و تحلیل آنها جزئی‌ترین اطلاعات را به‌دست می‌آورد (Risse, 2022: 102). حتی در جایی‌که سیستم‌های هوش مصنوعی برای ارائه خدمات عمومی مورد استفاده قرار می‌گیرد، بیش از آنکه بر وظیفه خدمت‌رسانی به مردم تمرکز داشته باشد، اغلب ازطریق دوربین‌های نظارتی و نرم‌افزارهای تشخیص چهره، تشخیص صدا و ... بر انجام کارویژه نظارتی تمرکز دارد.

بسیاری از دستگاه‌ها و برنامه‌های هوشمندی که روزانه استفاده می‌شود، از ردیاب‌های هوش مصنوعی برای شناسایی مکان و نظارت بر فعالیت‌های ما برخوردارند. این ابزارها می‌تواند داده‌های مربوط به موقعیت مکانی، عادات خرید و حتی تعاملات اجتماعی ما را جمع‌آوری کند. به‌ویژه در دنیای مدرن که اینترنت اشیا[1] در حال گسترش است، دستگاه‌های مختلف نظیر ساعت‌های هوشمند، تلویزیون‌های هوشمند و حتی لوازم خانگی قادرند اطلاعات گسترده‌ای درباره زندگی روزمره کاربران جمع‌آوری کند. این اطلاعات ممکن است بدون آگاهی افراد به‌منظور بهبود عملکرد سیستم‌ها جمع‌آوری شود، درحالی‌که در بسیاری از موارد به‌طور عمدی یا غیرعمدی حریم خصوصی کاربران

1. Internet of Things (IoT)

خود را نقض می‌کند(Mestari, Lenzini and Demirci, 2024: 5). در این میان یکی از خطرات عمده، تحلیل داده‌ها برای استخراج الگوهای پنهان است. برای مثال، این الگوریتم‌ها می‌تواند رفتارهای آنلاین افراد را تحلیل کند و پیش‌بینی‌هایی در مورد علایق، وضعیت سلامتی یا حتی گرایش‌های سیاسی آنها ارائه دهد. در برخی موارد، این تحلیل‌ها به‌گونه‌ای انجام می‌شود که کاربران حتی از آن مطلع نیستند یا براساس داده‌هایی است که خود آنها هرگز به اشتراک نگذاشته‌اند. این امر می‌تواند به سوءاستفاده از این داده‌ها در تصمیمات تجاری یا حتی سیاسی منجر شود (King and Meinhardt, 2024: 7-16). بنابراین، هوش مصنوعی می‌تواند به ابزار جدیدی برای ورود به حریم خصوصی تبدیل شود که در چارچوب آن دیگر احساسات و انتخاب‌های انسانی منطقه ممنوعه نیست و همواره در معرض خطر هک شدن و دستکاری قرار دارد؛ وضعیتی که عده‌ای از دانش‌پژوهان آن را «تمامیت‌خواهی پست‌مدرن» نام نهاده‌اند (کوکلبرگ، ۱۴۰۳: ۱۶۲).

درمجموع، هوش مصنوعی با ظرفیت‌های بی‌نظیر خود، تهدیدهای جدی برای حریم خصوصی افراد به همراه دارد. بنابراین، نیاز به تنظیم مقررات دقیق و شفاف برای محافظت از حریم خصوصی در برابر هوش مصنوعی بیش از پیش ضرورت دارد تا استفاده از این فناوری‌ها هم‌زمان با رعایت حقوق فردی و حفظ حریم خصوصی توسعه یابد.

ب) عدم شفافیت در عملکرد الگوریتم‌ها

عدم شفافیت در الگوریتم‌ها یکی از چالش‌های عمده‌ای است که در عصر هوش مصنوعی فراروی حق خودمختاری اطلاعاتی افراد قرار دارد. این مسئله زمانی که الگوریتم‌ها به‌طور خودکار در حال تحلیل و تصمیم‌گیری براساس داده‌های شخصی افراد هستند، اهمیت بیشتری پیدا می‌کند. در این چارچوب، عدم شفافیت به‌معنای ناتوانایی افراد در درک نحوه پردازش داده‌ها و تأثیراتی است که این پردازش‌ها می‌تواند روی زندگی آنها داشته باشد. در دنیای مدرن که هوش مصنوعی نقش

پررنگی در تصمیمات شخصی و عمومی ایفا می‌کند، این مسئله به‌طور جدی می‌تواند حق خودمختاری اطلاعاتی افراد را نقض کند.

مهم‌ترین تأثیری که عدم شفافیت الگوریتم‌ها بر خودمختاری اطلاعاتی دارد، از رهگذر محدود شدن توانایی افراد در کنترل اطلاعات شخصی است. به‌طور معمول، لازم است افراد بدانند اطلاعاتشان چگونه جمع‌آوری، پردازش و مورد استفاده قرار می‌گیرد. هنگامی که الگوریتم‌ها غیرشفاف عمل می‌کند، افراد نمی‌توانند از فرایندها آگاهی یابند که روی داده‌های شخصی آنها انجام می‌شود. الگوریتم‌های هوش مصنوعی که تصمیمات خود را براساس داده‌های شخصی اتخاذ می‌کند، اغلب به‌عنوان «جعبه سیاه» شناخته می‌شود. به این معنا که نحوه تصمیم‌گیری این الگوریتم‌ها برای کاربران یا حتی توسعه‌دهندگان آنها نامشخص است. این فقدان شفافیت باعث می‌شود افراد نتوانند به‌طور کامل از فرایند تصمیم‌گیری آگاهی یابند و درصورتی‌که تصمیمات غیرعادلانه یا نادرستی علیه آنها اتخاذ شود از حقوق خود دفاع کنند. برای مثال، زمانی که یک سیستم هوش مصنوعی برای تصمیم‌گیری در مورد پذیرش شغلی یا اعطای اعتبار مالی به یک فرد مورد استفاده قرار می‌گیرد، آن فرد باید درک روشنی از نحوه پردازش داده‌های شخصی خود داشته باشد. اما در بسیاری از موارد، افراد نمی‌دانند که چه داده‌هایی جمع‌آوری شده، چگونه تجزیه و تحلیل شده و برپایه چه الگوریتم‌هایی تصمیم‌گیری می‌شود. بنابراین آنها نمی‌توانند به‌طور مؤثر اعتراضی مطرح کنند یا در صورت بروز اشتباه‌ها، اصلاحات لازم را درخواست کنند (Pasquale, 2015: 83). روشن است که این مسئله به‌طور مستقیم بر حق خودمختاری اطلاعاتی افراد تأثیر منفی می‌گذارد.

یکی دیگر از آثار منفی عدم شفافیت الگوریتم‌ها برای خودمختاری اطلاعاتی، توانایی افراد در کنترل چگونگی استفاده از داده‌هایشان برای اهداف مختلف است. در بسیاری از سیستم‌های هوش مصنوعی، به‌علت غیرشفاف بودن الگوریتم‌ها، افراد از جزئیات آن درباره اینکه داده‌هایشان چگونه و برای چه اهدافی مورد استفاده قرار می‌گیرد، بی‌اطلاع هستند. این ناآگاهی نه‌تنها باعث می‌شود افراد نتوانند در مورد نحوه استفاده از

اطلاعاتشان تصمیم‌گیری کنند، بلکه حتی ممکن است این استفاده‌ها درنهایت به ضرر منافع و خواسته‌های آنها تمام شود (Rodgers et al., 2023:16). برای مثال، اطلاعات یک فرد ممکن است برای تبلیغات هدفمند مورد استفاده قرار گیرد، بدون آنکه او بداند داده‌هایش در کجا و چگونه به فروش می‌رسد یا برای کدام کمپین تجاری استفاده می‌شود.

بنابراین، می‌توان نتیجه گرفت عدم شفافیت در الگوریتم‌ها حق خودمختاری اطلاعاتی افراد را نقض می‌کند. برای مقابله با این چالش، ضروری است سیستم‌های هوش مصنوعی به‌گونه‌ای طراحی شود که شفافیت بیشتری در فرایندهای خود داشته باشد تا افراد بتوانند به‌طور مؤثر بر نحوه استفاده از داده‌های خود اعمال نظارت و کنترل داشته باشند.

ج) سوگیری الگوریتم‌ها

اساساً داده‌های هوش مصنوعی سوگیری‌های ساختاری و پنهان دارد. این سوگیری‌ها ممکن است در داده‌های آموزشی، الگوریتم، داده‌هایی که الگوریتم روی آنها اعمال می‌شود و در تیم‌هایی وجود داشته باشد که فناوری را برنامه‌ریزی می‌کند (Muller, 2020: 10). به‌طورکلی، عملکرد سیستم‌های مبتنی‌بر هوش مصنوعی به‌گونه‌ای است که صرفاً به دنبال پیدا کردن رابطه همبستگی یا ویژگی‌های مشترک بین متغیرها است و به همین دلیل از درک معنا و دلایل آن عاجز است. در چنین رویکردی، انواع سوگیری‌ها به‌راحتی می‌تواند منشأ عمل قرار گیرد. سوگیری‌هایی که به تعبیر نوبل به «سرکوب الگوریتمی» منتهی می‌شود (Nobel, 2018: 9).

زمانی که الگوریتم‌ها برای پردازش داده‌های شخصی و تصمیم‌گیری‌های مهم در حوزه‌هایی همچون استخدام، اعطای وام، ارزیابی عملکرد یا حتی تصمیم‌گیری‌های مرتبط با سلامت به‌کار می‌رود، ممکن است براساس داده‌ها و الگوریتم‌های طراحی شده، تصمیمات ناعادلانه و تبعیض‌آمیز اتخاذ کند. سوگیری‌های الگوریتمی معمولاً ناشی از داده‌های نادرست یا پیش‌فرض‌های اشتباهی است که در فرایند یادگیری

الگوریتم‌ها ایجاد می‌شود. این سوگیری‌ها شاید به نتایج ناعادلانه در تصمیم‌گیری‌هایی منجر شود که براساس ویژگی‌هایی نظیر جنسیت، نژاد، سن یا حتی ویژگی‌های اقتصادی‌ـاجتماعی افراد صورت می‌گیرد. در بسیاری از مواقع، الگوریتم‌ها براساس داده‌های تاریخی و رفتاری آموزش می‌بینند که دربرگیرنده تبعیض‌های اجتماعی و فرهنگی است. این تبعیض‌ها به‌طور خودکار در الگوریتم‌ها وارد می‌شود و شاید به تصمیمات تبعیض‌آمیز و ناعادلانه منجر شود. به‌عنوان مثال، اگر بررسی پرونده‌های درخواست شغل یا وام و دیگر خدمات درخواستی افراد به الگوریتم هوش مصنوعی واگذار شود، ممکن است براساس داده‌های پیشین به‌طور غیرمنصفانه اعضای گروه‌های قومی، جنسیتی یا سنی خاصی را از کسب این امتیازات محروم کند، بدون آنکه فرصت درک یا اعتراض به نحوه پردازش داده‌هایشان را داشته باشد (کوکلبرگ، ۱۴۰۳: ۸۳-۸۲).

بنابراین، سوگیری‌های الگوریتمی می‌تواند به یک حلقه معیوب از نابرابری‌های اجتماعی و اقتصادی منجر شود. زمانی که الگوریتم‌ها از داده‌های تاریخی برای پیش‌بینی یا تصمیم‌گیری استفاده می‌کند، این پیش‌بینی‌ها می‌تواند الگوهای تبعیض‌آمیز گذشته را تکرار کند و این خود باعث بازتولید نابرابری‌ها شود. این روند نه‌تنها موجب بی‌عدالتی خواهد شد، بلکه حق خودمختاری اطلاعاتی افراد را نیز به‌طور جدی نقض می‌کند؛ زیرا افراد نمی‌توانند این تصمیم‌گیری‌های تبعیض‌آمیز الگوریتم‌های هوش مصنوعی را به چالش کشند یا از آنها جلوگیری کنند (رشیدی، ۱۴۰۳: ۳۷۷-۳۷۱). برای مقابله با این چالش، ضروری است الگوریتم‌ها به‌طور مداوم مورد ارزیابی قرار گیرد تا از سوگیری‌های ناعادلانه جلوگیری شود.

د) نظارت‌ناپذیری تصمیم‌گیری‌های خودکار

تصمیم‌گیری‌های خودکار هوش مصنوعی می‌تواند به‌طور زیادی حق خودمختاری اطلاعاتی افراد را نقض کند. نقض حق خودمختاری اطلاعاتی در تصمیم‌گیری‌های خودکار، عمدتاً از فقدان هرگونه دخالت و نظارت انسانی بر فرایند تصمیم‌گیری

ناشی می‌شود. اغلب سیستم‌های هوش مصنوعی در تصمیم‌گیری‌های خودکار بسیار پیچیده عمل می‌کند. این پیچیدگی می‌تواند به این معنا باشد که بسیاری از افراد به درک چگونگی یا دلایل تصمیمات اتخاذ شده از این سیستم‌ها قادر نیستند. برای مثال، در مواقعی که یک سیستم هوش مصنوعی به‌طور خودکار تصمیم می‌گیرد که فردی واجد شرایط برای دریافت خدمات خاص نیست، آن فرد ممکن است نتواند علت این تصمیم را بفهمد یا راهی برای اصلاح یا اعتراض به آن بیابد (عامری، مقدسی و حبیب‌نژاد، ۱۴۰۴)؛ زیرا سیستم‌های خودکار جزئیات دقیق فرایندهای تصمیم‌گیری خود را ارائه نمی‌دهد (O'Neil, 2016: 38).

همچنین، سیستم‌های تصمیم‌گیری خودکار می‌تواند به کاهش آزادی انتخاب افراد منجر شود. زمانی که یک سیستم هوش مصنوعی به‌طور خودکار تصمیمات را اتخاذ می‌کند، افراد از داشتن گزینه‌های مختلف و توانایی انتخاب از میان آنها محروم می‌شود. درنتیجه، تصمیم‌گیری به‌دست سیستم‌هایی می‌افتد که افراد در آن هیچ نقشی ندارند و این امر به‌طور مستقیم بر عاملیت افراد و توانایی آنها در انتخاب یا تعیین مسیر زندگی‌شان تأثیر منفی می‌گذارد (Prunkl, 2024).

به‌طور خلاصه، فقدان دخالت انسانی، پیچیدگی‌های غیرقابل درک، بی‌اطلاعی از فرایندها و عدم کنترل بر داده‌ها در تصمیم‌گیری‌های خودکار، ازجمله عواملی است که موجب می‌شود افراد نتوانند به‌طور مؤثر بر نحوه استفاده از اطلاعات شخصی خود نظارت داشته باشند. این مسئله تهدیدی جدی بر حق خودمحتاری اطلاعاتی افراد به‌شمار می‌آید و مقابله با آن نیازمند انجام اصلاحات اساسی در زمینه طراحی و اجرای سیستم‌های تصمیم‌گیری خودکار است.

هـ) نقض امنیت داده‌ها

هوش مصنوعی می‌تواند تهدیدهای جدی برای امنیت داده‌ها ایجاد کند و از این رهگذر حق خودمختاری اطلاعاتی افراد را نقض کند. امنیت داده‌ها به‌معنای حفاظت از داده‌های شخصی در برابر دسترسی‌های غیرمجاز، تغییرات غیرمجاز یا از بین رفتن

اطلاعات است. استفاده نادرست یا ناکافی از تکنولوژی‌های هوش مصنوعی می‌تواند به نقض امنیت داده‌ها منجر شود. این نقض‌ها می‌تواند از روش‌های مختلفی شامل دسترسی غیرمجاز به داده‌های شخصی، ذخیره‌سازی نامطمئن داده‌ها یا سوءاستفاده از داده‌های شخصی برای اهداف غیرمجاز ناشی شود.

یکی از اصلی‌ترین زمینه‌های نقض امنیت داده‌ها از طریق هوش مصنوعی، استفاده از الگوریتم‌های یادگیری ماشین است که به‌طور پیوسته داده‌های شخصی را برای آموزش و بهبود عملکرد خود به‌کار می‌گیرد. زمانی که داده‌های جمع‌آوری‌شده به‌طور غیرمجاز یا نادرست پردازش شود، ممکن است اطلاعات حساس افراد به خطر افتد. به‌عنوان مثال، در سیستم‌های مبتنی‌بر هوش مصنوعی که برای تحلیل داده‌ها یا پیش‌بینی نتایج استفاده می‌شود، ممکن است اطلاعات افراد خارج از کنترل آنها قرار گیرد. زمانی که این داده‌ها بدون نظارت مناسب ذخیره و پردازش شود، خطراتی از قبیل افشای اطلاعات شخصی و سوءاستفاده از آنها افزایش می‌یابد (Ye et al., 2024) این شرایط تهدیدی جدی برای حق خودمختاری اطلاعاتی افراد ایجاد می‌کند، زیرا آنها دیگر به کنترل اطلاعات شخصی خود قادر نخواهند بود و نمی‌توانند بر نحوه استفاده از این داده‌ها نظارت کنند.

همچنین، ممکن است داده‌های شخصی جمع‌آوری شده از طریق سیستم‌های هوش مصنوعی در سرورهای غیرمطمئن و با استانداردهای امنیتی پایین ذخیره شود که در صورت نفوذ هکرها یا حملات سایبری در معرض خطر جدی قرار می‌گیرد. این تهدیدهای سایبری به‌ویژه زمانی شدیدتر می‌شود که سیستم‌های هوش مصنوعی در سازمان‌ها یا کسب‌وکارهای بزرگ به‌کار گرفته شود. در چنین شرایطی، امکان افشای گسترده اطلاعات شخصی وجود دارد که می‌تواند تبعات جبران‌ناپذیری برای افراد داشته باشد (Cremer et al., 2022: 716-718). برای مثال، درصورتی‌که اطلاعات مربوط به سلامت، وضعیت مالی یا موقعیت مکانی افراد در معرض سرقت یا افشا قرار گیرد، این افراد ممکن است از نظر اجتماعی، اقتصادی و حتی روانی آسیب جدی ببینند. زمانی که داده‌های شخصی افراد به‌طور ناخواسته به‌دست اشخاص

ثالث می‌افتد، آنها درخصوص استفاده از اطلاعات خود در زمینه‌های مختلف بی‌خبر خواهند بود. ممکن است این اطلاعات به‌طور غیرمجاز در مقاصد تجاری یا تبلیغاتی به‌کار گرفته شود. برای مثال، سیستم‌های هوش مصنوعی بدون اجازه صریح فرد از اطلاعات شخصی او پیشنهادهای تجاری یا خدمات خاصی را برای او ایجاد کند (Pasquale, 2015: 110)؛ این فرایند می‌تواند به نقض حق خودمختاری اطلاعاتی افراد منجر شود.

مسئله دیگری که درخصوص نقض امنیت داده‌ها و به‌تبع در نقض حق خودمختاری اطلاعاتی افراد گفتنی است، خطرات مربوط به اشتراک‌گذاری و انتقال داده‌ها است. در دنیای امروز، سیستم‌های هوش مصنوعی به‌طور گسترده در فرایندهای کسب‌وکارهای مختلف به‌کار می‌رود و این داده‌ها ممکن است از یک سازمان به سازمان دیگر منتقل شود. این انتقال داده‌ها که ممکن است فراتر از مرزهای ملی انجام شود، می‌تواند امنیت اطلاعات شخصی را تهدید کند. بسیاری از کشورها قوانین مختلفی برای حفاظت از داده‌های شخصی دارند، اما وقتی داده‌ها به کشورهایی منتقل می‌شود که استانداردهای امنیتی پایین‌تر دارند، این خطر به‌وجود می‌آید که اطلاعات شخصی افراد در معرض سوءاستفاده قرار گیرد؛ به‌ویژه در شرایطی که این اطلاعات به‌طور گسترده در فضای آنلاین یا سرورهای عمومی ذخیره می‌شود، خطر هک شدن یا سوءاستفاده از آنها بیشتر است. این تهدیدها به‌طور مستقیم بر توانایی فرد در کنترل و مدیریت داده‌های شخصی تأثیر می‌گذارد و موجب تضعیف حق خودمختاری اطلاعاتی افراد می‌شود (O’Neil, 2016: 71).

۴. زمینه‌ها و خلأهای قانونی در نظام حقوقی ایران

با توسعه سیستم‌های هوش مصنوعی، چالش‌های متعددی در زمینه حقوق اطلاعات و حفاظت از حریم خصوصی افراد به‌وجود آمده است که در بالا به آنها اشاره شد. این چالش‌ها به‌طور خاص در کشورهای در حال توسعه مانند ایران بیشتر نمایان می‌شود که هنوز ساختارهای حقوقی و نظارتی لازم برای مواجهه با تهدیدهای مربوط

به داده‌ها و اطلاعات خصوصی را به‌طور کامل توسعه نداده‌اند. ازاین‌رو بی‌تردید، کاربرد هوش مصنوعی مبتنی‌بر منطق فازی در نظام حقوقی ایران می‌تواند در این مسیر راهگشا باشد (ابوذری، ۱۳۹۶). لذا در اینجا زمینه‌های قانونی حمایت از حق خودمختاری اطلاعاتی و خلأهای قانونی آن در ایران به تفکیک و مختصر بررسی خواهد شد.

الف) زمینه‌های قانونی

در نظام حقوقی ایران، حق بر خودمختاری اطلاعاتی به‌طور پراکنده در قوانین و مقررات مختلف مورد توجه قرار گرفته است. در قانون اساسی جمهوری اسلامی ایران، هرچند مستقیم اشاره‌ای به حق بر خودمختاری اطلاعاتی افراد نشده است، اما برخی اصول می‌تواند مبنای حمایت از این حق تلقی شود؛ ازجمله، اصل بیست‌ودوم که به حفاظت از حیثیت، زندگی و حقوق افراد اشاره می‌کند و اصل بیست‌وپنجم که بر عدم تجسس در زندگی افراد تأکید دارد. همچنین، قانون حمایت از حقوق مصرف‌کنندگان (مصوب ۱۳۹۲) نیز به‌ویژه در زمینه قراردادهای خرید و فروش و جمع‌آوری اطلاعات در بازارهای آنلاین بر حقوق افراد در برابر سوءاستفاده‌های احتمالی از داده‌ها و اطلاعات شخصی آنها تأکید دارد. اما قانون جرائم رایانه‌ای (مصوب ۱۳۸۸) مهم‌ترین قانون حاکم در حال حاضر است که در ایران به‌طور خاص به حفاظت از داده‌های شخصی و اطلاعات افراد پرداخته است. براساس این قانون، استفاده نادرست از داده‌های شخصی، نظیر هک کردن، سرقت اطلاعات یا استفاده از اطلاعات بدون رضایت صاحب داده، جرم تلقی می‌شود. بااین‌حال، این قانون بیشتر به مقابله با جرائم سایبری و تهدیدهای مرتبط با فضای مجازی پرداخته و از حقوق حریم خصوصی و خودمختاری اطلاعاتی افراد به‌طور کافی حمایت نمی‌کند. در این شرایط، به‌منظور کاهش بخشی از مخاطرات مرتبط با نقض حریم خصوصی کاربران و الزام اشخاص حقوقی غیردولتی و دستگاه‌های اجرایی کشور به رعایت شرایط مرتبط با شیوه‌های جمع‌آوری، پردازش و نگهداری داده‌های کاربران در سامانه‌ها و سکوهای

فضای مجازی، کمیسیون عالی تنظیم مقررات فضای مجازی کشور (۱۴۰۲) به صدور دستورالعمل اجرایی صرفاً برای ارائه‌دهندگان خدمات اقدام کرده که سازوکارهای اجرایی و ضمانت‌های قانونی آن به‌شدت ناکافی است.

ب) خلأهای قانونی و چالش‌های حقوقی

با عنایت به‌مراتب فوق می‌توان ادعا کرد در حال حاضر ایران هیچ قانون جامع و مستقلی ندارد که به‌طور اختصاصی به موضوع حفاظت از داده‌های شخصی و حق بر خودمختاری اطلاعاتی در عصر دیجیتال پرداخته باشد. چنانکه گفته شد، قوانین موجود پراکنده و به‌طور جزئی به این موضوع پرداخته است. در شرایط وجود خلأهای قانونی و فقدان سازوکارهای تنظیم‌گری کارآمد، نظارت بر نحوه جمع‌آوری، استفاده و پردازش داده‌ها در ایران بسیار ناکافی است. به‌علاوه، اجرایی شدن قوانین موجود در مورد حفاظت از داده‌های شخصی و جلوگیری از سوءاستفاده از آنها، ممکن است به‌شدت ضعیف و تبعیض‌آمیز باشد. در بسیاری از موارد، شرکت‌ها و سازمان‌های دولتی و خصوصی در ایران ممکن است بدون اطلاع‌رسانی شفاف به کاربران، داده‌های شخصی آنها را جمع‌آوری و پردازش کنند. این امر می‌تواند موجب نقض حق بر خودمختاری اطلاعاتی افراد شود. این مسئله به‌وضوح نیاز به تنظیم قوانین روشن و شفاف برای مدیریت داده‌ها و نظارت دقیق‌تر بر آنها را ایجاب می‌کند. برای نیل به این مقصود باید با استانداردهای بین‌المللی عمل شود. عدم رعایت این استانداردها ممکن است به سوءاستفاده از اطلاعات شخصی منجر شود و افراد نتوانند از حقوق خود در این زمینه به‌درستی دفاع کنند.

همچنین گفتنی است برای ضرورت تقنینی در ایران، لایحه قانونی با عنوان «لایحه حفاظت از داده‌های شخصی» در حال تهیه و تدوین است که انتظار می‌رود تا حدودی زمینه‌های حقوقی لازم برای حفاظت از حق بر خودمختاری اطلاعاتی را فراهم کند (کمیسیون حقوقی و قضایی هیئت دولت، ۱۴۰۳). بااین‌حال، این لایحه هنوز نهایی نشده و نمی‌توان آن را به‌عنوان ابزار حقوقی کامل برای حمایت از حق بر

خودمختاری اطلاعاتی شهروندان تلقی کرد. درنهایت ممکن است در فرایند تبدیل این لایحه به قانون، بیشتر بر موضوع‌های امنیتی و مقابله با جرائم سایبری تمرکز شود تا بر حقوق حریم خصوصی و خودمختاری اطلاعاتی افراد.

۵. جمع‌بندی و نتیجه‌گیری

حق بر خودمختاری اطلاعاتی به‌معنای حق هر فرد برای تصمیم‌گیری درباره این است که کدام‌یک از داده‌های شخصی او می‌تواند افشا یا مورد استفاده دیگران قرار گیرد. این حق، مفهوم نسبتاً جدیدی است که در سال ۱۹۸۳ طی رأی معروف به «حکم سرشماری» دادگاه قانون اساسی فدرال آلمان به منصه ظهور رسید. از آن زمان، با افزایش جمع‌آوری و پردازش دیجیتالی داده‌ها، حفاظت از داده‌های شخصی اهمیت بیشتری یافته و فراتر از قانون اساسی آلمان، در قالب «مقررات عمومی حفاظت از داده‌ها» در اتحادیه اروپا جایگاه ویژه‌ای پیدا کرده است. این قانون چارچوب حقوقی جامعی را برای حفاظت از داده‌های شخصی فراهم می‌کند و حق خودمختاری اطلاعاتی افراد را تقویت می‌کند.

در این مقاله، چالش‌های مختلفی مورد بررسی قرار گرفته که هوش مصنوعی می‌تواند بر حق خودمختاری اطلاعاتی افراد ایجاد کند، ازجمله نقض حریم خصوصی، نظارت‌ناپذیری تصمیم‌گیری‌های خودکار، عدم شفافیت الگوریتم‌ها، سوگیری در پردازش داده‌ها و نقض امنیت داده‌ها است. این مشکلات به‌ویژه زمانی شدت می‌گیرد که افراد به کنترل و نظارت بر استفاده از داده‌های شخصی خود قادر نیستند، یا در بسیاری از مواقع از نحوه جمع‌آوری، پردازش و استفاده از داده‌های خود بی‌اطلاع هستند. به‌طورکلی، این چالش‌ها به تهدیدهایی برای استقلال اطلاعاتی افراد منتهی می‌شود و نظارت افراد بر داده‌های شخصی را کاهش می‌دهد.

برای مقابله با چالش‌های فوق، برخی راهکارهای مهم وجود دارد که می‌تواند تأثیرات منفی هوش مصنوعی بر حق خودمختاری اطلاعاتی را کاهش دهد. یکی از مهم‌ترین آنها، ارتقای شفافیت در سیستم‌های هوش مصنوعی است. توسعه و

پیاده‌سازی الگوریتم‌هایی که قابلیت توضیح‌پذیری داشته باشد، به‌ویژه در زمینه‌هایی مانند تصمیم‌گیری‌های خودکار، می‌تواند از اهمیت بالایی برخوردار باشد. علاوه بر این، می‌توان با ایجاد مدل‌های قانونی و حقوقی ویژه، نظارت بر جمع‌آوری و استفاده از داده‌ها را تقویت کرد. سازوکار این نظارت باید به‌گونه‌ای باشد که افراد بتوانند دسترسی و کنترل بیشتری بر داده‌های خود داشته باشند و از این رهگذر از سوءاستفاده‌های احتمالی جلوگیری شود. راهکار دیگر، تضمین امنیت داده‌ها در سیستم‌های هوش مصنوعی است. شرکت‌ها و نهادهای توسعه‌دهنده این فناوری‌ها لازم است اقدام‌های قوی‌تری برای حفاظت از داده‌های حساس افراد انجام دهند و از ایجاد شکاف‌های امنیتی جلوگیری کنند که می‌تواند به نقض حریم خصوصی منجر شود. همچنین استفاده از تکنولوژی‌های رمزنگاری و افزایش تدابیر امنیتی در حین پردازش داده‌های شخصی، می‌تواند به کاهش آسیب‌های احتمالی کمک کند.

بنابراین، به‌منظور تنظیم و نظارت بر سیستم‌های هوش مصنوعی، توسعه قوانین دقیق و شفاف ضروری است. این قوانین باید به‌گونه‌ای طراحی شود که تمام جنبه‌های حقوقی مرتبط با جمع‌آوری، پردازش و استفاده از داده‌های شخصی را پوشش دهد. همچنین، نظارت مستمر بر سیستم‌های هوش مصنوعی باید ازسوی نهادهای مستقل و تخصصی انجام پذیرد تا اطمینان حاصل شود که این سیستم‌ها به‌طور منصفانه و بدون سوگیری عمل می‌کنند. در این راستا باید مسئولیت‌های هرکدام از نهادها و سازمان‌های استفاده‌کننده از این فناوری‌ها به‌طور شفاف مشخص شود. به‌علاوه، قوانین و مقررات به‌گونه‌ای تنظیم شود که از حقوق افراد پشتیبانی کند تا آنها بتوانند در صورت نقض حقوق‌شان، از مسیرهای قانونی نسبت به تأمین آن اقدام کنند. به‌طورکلی، با توجه به پیشرفت‌های سریع در زمینه هوش مصنوعی و کاربردهای گسترده آن در زندگی روزمره، همگام‌سازی این فناوری با اصول حقوق بشری از اهمیت ویژه‌ای برخوردار است. توسعه هوش مصنوعی باید به‌گونه‌ای صورت گیرد که حقوق افراد، شامل حق خودمختاری اطلاعاتی آنها محترم شمرده شود. در این راستا، توجه به حریم خصوصی و امنیت داده‌ها، تضمین شفافیت و پاسخگویی

سیستم‌های هوش مصنوعی، و مقابله با سوگیری‌های احتمالی در پردازش داده‌ها، ازجمله مهم‌ترین اقدام‌های ضروری است.

در ایران، با توجه به پیشرفت روزافزون فناوری هوش مصنوعی و تهدیدهایی که این فناوری‌ها برای حریم خصوصی و حق بر خودمختاری اطلاعاتی افراد ایجاد می‌کند، پیشنهاد می‌شود: اولاً حق خودمختاری اطلاعاتی افراد به‌عنوان یک حق اساسی به رسمیت شناخته شود؛ ثانیاً در راستای توسعه حکمرانی هوش مصنوعی یک چارچوب قانونی جامع و منسجم برای حفاظت از داده‌های شخصی ایجاد شود، به‌نحوی‌که خلأهای قانونی موجود به‌ویژه در زمینه تضمین شفافیت را پوشش دهد و ثالثاً از طریق کاربست سازوکارهای مختلف کوشش شود دانش و مهارت عمومی شهروندان در زمینه حفاظت از داده‌های شخصی در کاربرد ابزارهای مبتنی‌بر هوش مصنوعی افزایش یابد.

درنهایت، پژوهش‌های بیشتر در این حوزه لازم است تا چالش‌ها و تهدیدهای بالقوه فناوری‌های نوین درخصوص حقوق بشر شناسایی و راهکارهای عملی‌تری برای حفاظت از حقوق فردی توسعه یابد. نتایج این تحقیقات می‌تواند در توسعه چارچوب‌های قانونی و اخلاقی برای هوش مصنوعی و ایجاد سیستم‌های نظارتی مؤثر، نقشی حیاتی ایفا کند.

منابع و مآخذ

۱. ابوذری، مهرنوش (۱۳۹۶). *کاربرد منطق فازی در حقوق کیفری ایران*، تهران، بنیادحقوقی میزان.

۲. انصاری، باقر (۱۳۹۰). *حقوق حریم خصوصی*، تهران، انتشارات سمت.

۳. بنافی، فرشته (۱۴۰۲). «حفاظت از حق حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی»، *پژوهش حقوق خصوصی*، دوره ۱۲، ش ۴۵.

۴. جلالی، محمد و پگاه مرزبان (۱۴۰۱). «تضمین خودمختاری مبتنی‌بر اطلاعات در نظام حقوق اساسی جمهوری فدرال آلمان با نگاهی به رویه اتحادیه اروپا»، *فصلنامه تحقیقات حقوقی*، دوره ۲۵، ش ۱.

۵. رشیدی، احمد (۱۴۰۳). «هوش مصنوعی و چالش‌های دمکراسی»، *فصلنامه پژوهش سیاست نظری*، دوره ۱۹، ش ۳۶. https://rimag.ir/fa/Article/48240

۶. سیفی، آناهیتا و نجمه رزمخواه (۱۴۰۱). «هوش مصنوعی و چالش‌های پیش رو در قلمرو حقوق بین‌الملل بشر، با رویکردی بر حقِ کار»، *دوفصلنامه بین‌المللی حقوق بشر*، دوره ۱۷، ش ۱.

۷. عاشوری کیسمی، محمدعلی (۱۴۰۳). «همگرایی حریم خصوصی و شفافیت، محدودیت‌های طراحی هوش مصنوعی»، *حکمت و فلسفه*، دوره ۲۰، ش ۷۸.

۸. عامری، زهرا، محمدباقر مقدسی و سیداحمد حبیب‌نژاد (۱۴۰۴). «حق اعتراض به تصمیم‌گیری‌های خودکار مبتنی‌بر هوش مصنوعی: جلوه‌ای از الزامات حقوق بشری عصر فناوری»، *فصلنامه پژوهش‌های نوین حقوق اداری*، دوره ۷، ش ۲۵.

۹. کمیسیون حقوقی و قضایی هیئت دولت جمهوری اسلامی ایران (۱۴۰۳). «تصویب لایحه حفاظت از داده‌های شخصی»، پایگاه اطلاع‌رسانی دولت، https://dolat.ir/detail/447326.

۱۰. کمیسیون عالی تنظیم مقررات فضای مجازی کشور (۱۴۰۲). «ابلاغ دستورالعمل اجرایی بهبود حفاظت از حریم خصوصی کاربران و شیوه جمع‌آوری، پردازش و نگهداری اطلاعات کاربران در سامانه‌ها و سکوهای فضای مجازی»، پایگاه الکترونیکی مرکز پژوهش‌های مجلس شورای اسلامی، https://rc.majlis.ir/fa/law/show/1797869.

۱۱. کوکلبرگ، مارک (۱۴۰۳). *درآمدی بر فلسفه سیاسی هوش مصنوعی*، ترجمه علی‌اصغر رئیس‌زاده، تهران، مؤسسه فرهنگی دکسا.

12. Alhitmi, H.K., A. Mardiah, K.I. Al-Sulaiti and J. Abbas (2024). "Data Security and Privacy Concerns of AI-driven Marketing in the Context of Economics and Business Field", *Cogent Business and Management*, Vol. 11, No. 1. Available at: https://doi.org/10.1080/23311975.2024.2393743. [accessed on: 20/1/2025].
13. Cremer, F., B. Sheehan, M. Fortmann, A. Kia, M. Mullins, F. Murphy and S. Materne (2022). "Cyber Risk and Cybersecurity: A Systematic Review of Data Availability", *Geneva Pap Risk Insur Issues Pract*, Vol. 47, No. 3.
14. Els, A.S. (2017). "Artificial Intelligence as a Digital Privacy Protector", *Harvard Journal of Law & Technology*, Vol. 3, No. 1. Available at: https://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech217.pdf. [accessed on: 15/2/2025].
15. Erdosova, A. (2019). "The Right to Informational Self-determination in the Context of Selected Judicial Decisions and Practical Background, *Public Governance, Administration and Finances Law Review*, Vol. 4, No. 2.
16. Federal Constitutional Court of Germany (1983). "Headnots to the Judgment of the First Senate of 15 December 1983", Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/1983/12/rs19831215_1bvr020983en.html. [accessed on: 29/1/2025].
17. Fialová, E. (2014). "Data Portability and Informational Self-determination", *Masaryk University Journal of Law and Technology*, Vol. 8, No. 1. Available at: https://journals.muni.cz/mujlt/article/view/2645/2209.
18. Garvie, C. (2016). *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Washington D.C., Georgetown Law Center on Privacy & Technology.
19. Hornung, G. and C. Schnabel (2009). "Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-determination", *Computer Law & Security Review*, Vol. 25, No. 1.
20. Jungherr, A. (2023). "Artificial Intelligence and Democracy: A Conceptual Framework", *Social Media+Society*, 5 (31).
21. King, J. and C. Meinhardt (2024). "Rethinking Privacy in the AI Era", *White Paper of The Stanford Institute for Human-centered Artificial Intelligence*. Available at: https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf. [accessed on: 13/1/2025].
22. Kissinger, H., E. Schmidt, D.P. Huttenlocher and S. Schouten (2021). *The age of AI: and our Human Future*, New York, Little Brown and Company.
23. Mestari, S.Z., G. Lenzini and H. Demirci (2024). "Preserving Data Privacy in Machine Learning Systems", *Computers and Security*, Vol. 137, No. 1.
24. Muller, C. (2020). "The Impact of Artificial Intelligence on Human Rights,

Democracy and the Rule of Law", *ALLAI*., Online Published. Available at: https://allai.nl/wp-content/uploads/2020/06/The-Impact-of-AI-on-Human-Rights-Democracy-and-the-Rule-of-Law-draft.pdf. [accessed on: 19/8/2024].

25. Nobel, S.U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York University Press.
26. O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New Yourk, Crown Publishing Group.
27. Orwat, C., J. Bareis and A. Folberth (2024). "Normative Challenges of Risk Regulation of Artificial Intelligence", *Nanoethics*, Vol. 18, No. 11.
28. Pasquale, F. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambrige, Harvard University Press, Available at: http://www.jstor.org/stable/j.ctt13x0hch. [accessed on: 17/2/2025].
29. Prunkl, C. (2024). "Human Autonomy at Risk? An Analysis of the Challenges from AI", *Minds and Machines*, Vol. 34, No. 26.
30. Risse, M. (2022). "Artificial Intelligence and the Past, Present, and Future of Democracy", In S. Voeneky, P. Kellmeyer, O. Mueller and W. Burgard (eds) *The Responsible Artificial, Published Online by Cambridge University Press*. Available at: https://doi.org/10.1017/9781009207898.009. [accessed on: 22/7/2024].
31. Rodgers, W., J.M. Murry, A. Stefaniadis and S. Tarbam (2023)."An Artificial Intelligence Algorithmic Approach to Ethical Decision-making in Human Resource Management Processes", *Human Resource Management Review*, Vol. 33, No. 1.
32. Sadek, T., K.D. Stanley, G. Smith, K. Marcinek, P. Cormarie and S. Gunashekar (2024). "Artificial Intelligence Impacts on Privacy Law", *RAND Corporation*. Available at: https://www.rand.org/pubs/research_reports/RRA3243-2.html. [accessed on: 20/2/2025].
33. Sartor, G. (2020). "The Impact of the General Data Protection Regulation on Artificial Intelligence", *European Parliamentary Research Servic,* PE641.530. doi: 10.2861/293.
34. Thouvenin, F. (2021). "Informational Self-determination: A Convincing Rationale for Data Protection Law?", *JIPITEC*., Vol. 12, No. 4. Available at: https://www.jipitec.eu/issues/jipitec. [accessed on: 20/4/2025].
35. Vladimirovna, T.E. (2022). "The Right to Informational Self-determination: On the Edge of Public and Private", *Legal Issues in the Digital Age*, No. 4.
36. Westin, A. (1967). *Privacy and Freedom*, New York, Atheneum.
37. Ye, X., Y. Yan, J. Li and B. Jiang (2024). "Privacy and Personal Data Risk Governance for Generative Artificial Intelligence"*, Telecommunications Policy*, Vol. 48, No. 10.