دامنه و آثار تعهد محرمانگی در حمایت از اسرار تجاری در عصر هوش مصنوعی: مطالعه تطبیقی در نظام حقوقی ایران، اتحادیه اروپا و ایالات متحده آمریکا

علی ساعتچی * | دکتری حقوق خصوصی، استادیار گروه حقوق خصوصی ، دانشکده حقوق و علوم سیاسی، دانشگاه فردوسی مشهد، مشهد، ایران

جواد فهیمی تبار | دانشجو دکتری حقوق خصوصی، دانشگاه فردوسی مشهد، مشهد، ایران

دریافت: ۱٤۰٤/۱۰/۰۲ | **پذیرش:** ۱٤۰۵/۰۵/۳۱ | مقاله برای اصلاح به مدت ۷ روز نزد پدیدآوران بوده است.

چکیده:

امروزه داده‌ها به حیاتی‌ترین دارایی شرکت‌ها تبدیل شده و تعهد به حفظ محرمانگی، نقشی بنیادین در صیانت از این سرمایه‌ها ایفا می‌کند. ظهور هوش مصنوعی مولد، چالش‌هایی مانند ورود داده‌های حساس به مدل‌های زبانی بزرگ و بازتولید اطلاعات پژوهشی، نظام‌های حقوقی را با پرسش‌هایی نوین درباره حدود و ماهیت محرمانگی روبه‌رو کرده است. هدف این پژوهش، تبیین دامنه و آثار تعهد محرمانگی در حمایت از اسرار تجاری در عصر هوش مصنوعی و ارزیابی ظرفیت‌های نظام حقوقی ایران در قیاس با اتحادیه اروپا و ایالات متحده است. ضرورت این بررسی از آن روست که دکترین سنتی مبتنی بر منع افشای مستقیم، در برابر مخاطرات پردازش‌های الگوریتمی و ازدست‌رفتن کنترل داده‌ها ناکافی به نظر می‌رسد. پژوهش با روش توصیفی-تحلیلی و با رویکرد تطبیقی انجام شده و داده‌ها به شیوه کتابخانه‌ای از قوانین و دیدگاه‌های حقوقی سه‌نظام مذکور گردآوری و با تحلیل محتوای کیفی بررسی شده‌اند. یافته‌ها نشان می‌دهد ایالات متحده استمرار حمایت از اسرار تجاری را به اثبات اقدامات معقول حفاظتی مشروط می‌کند و ورود داده‌های محرمانه به پلتفرم‌های غیرقابل‌کنترل، زوال حمایت را در پی دارد. درحالی‌که اتحادیه اروپا حمایت از اسرار تجاری را در کنار الزامات حفاظت از داده، شفافیت، حقوق بنیادین، رقابت و منافع عمومی تنظیم می‌کند.در ایران، به‌رغم فقدان قانون جامع، ظرفیت‌های گسترده‌ای در قالب اصل آزادی قراردادها، قواعد

نشریهٔ علمی (رتبه ین المللی)
پژوهشگاه علوم و فنّاوری اطلاعات ایران
شاپا(چاپی) ۸۲۲۳-۲۲۵۱
شاپا(الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISTA، SCOPUS و ISC
http://jipm.irandoc.ac.ir
دوره XX | شمارهٔ X | ص ص XX-XX
۱۳XX X

نوع مقاله: پژوهشی

به این مقاله به شکل زیر استناد کنید:
درون متن:
(ساعتچی و فهی‌می تبار ، زودآیند)
در فهرست منابع:
ساعتچی، علی. فهی‌می تبار، جواد. زودآیند. دامنه و آثار تعهد محرمانگی در حمایت از اسرار تجاری در عصر هوش مصنوعی: مطالعه تطبی‌قی در نظام حقوقی ای‌ران، اتحادی‌ه اروپا و ای‌الات متحده آمری‌کا. *پژوهشنامه پردازش و مدیریت اطلاعات*. http://Jipm.irandoc.ac.ir (دسترسی در روز/ماه/سال)

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات

x ۱۳ | دورهٔ xx | شمارهٔ x

مسئولیت مدنی و مفاهیم فقهی مانند امانت، تفریط و اتلاف وجود دارد، اما تمرکز بر مفهوم سنتی افشا و دشواری اثبات ، حمایت مؤثر را با چالش مواجه ساخته است. نتیجه‌گیری پژوهش آن است که تعهد محرمانگی در عصر هوش مصنوعی باید به تعهد مراقبتی ویژه بازتعریف شود که اتخاذ تدابیر فنی و سازمانی را نیز در برگیرد. پذیرش معیار ازدست‌رفتن کنترل مؤثر به‌عنوان مصداق افشا، جابه‌جایی محدود بار اثبات به نفع زیان‌دیده و راهکارهایی چون تعهد مراقبت دیجیتال می‌تواند نظام حقوقی ایران را به در برابر تحولات فناوری سازگار نماید.

کلیدواژه‌ها: تعهد، محرمانگی، عدم افشا، داده، اسرار تجاری، هوش مصنوعی

*پدیدآور رابط alisaatchi@um.ac.ir

۱. مقدمه پژوهش

امروزه داده‌ها از دارایی‌هایی ایستا و صرفاً قابل‌ذخیره‌سازی، به سوخت حیاتی موتورهای پردازشی و زیربنای اصلی فعالیت‌های علمی، اقتصادی و تجاری تبدیل شده‌اند. نشریات و پلتفرم‌های دیجیتال امروز نه‌تنها مخزن ذخیره داده، بلکه پردازشگر، تحلیل‌گر و بازتولیدکننده اطلاعات هستند (*Kwakye, 2022, p. 117*). این تحول موجب شده است که ارزش اطلاعات دیگر صرفاً به محتوای اولیه آن محدود نباشد، بلکه نحوه پردازش، ترکیب، تحلیل و بازتولید آن نیز بتواند ارزش اقتصادی و فکری مستقلی ایجاد کند. ظهور هوش مصنوعی مولد، این روند را شتاب بخشیده و چالش‌های حقوقی مدیریت اطلاعات را از مفاهیمی مانند عدم افشا فراتر برده و با پدیده‌های نوظهوری همچون توهم‌زایی هوش مصنوعی مواجه ساخته است. در چنین شرایطی، چالش اساسی آن است که هنگامی که داده‌های حساس پژوهشی یا تجاری وارد هوش مصنوعی می‌شوند، مرز میان الهام‌گیری مشروع و بازتولید غیرمجاز چگونه باید ترسیم شود. امروزه مفهوم اسرار تجاری دیگر صرفاً به فرمول‌های تولید، فرایندهای صنعتی یا اطلاعات تجاری محدود نیست، بلکه طیف گسترده‌ای از داده‌های دارای ارزش اقتصادی، از جمله داده‌های پژوهشی، مجموعه‌داده‌های آموزشی، متادیتا، الگوریتم‌ها و مدل‌های یادگیری ماشین را نیز در بر می‌گیرد. وجه مشترک این اطلاعات، برخورداری از ارزش اقتصادی ناشی از محرمانگی و اتخاذ تدابیر معقول برای حفظ آن‌هاست؛ ازاین‌رو، تحلیل مدیریت داده‌های پژوهشی

در این پژوهش نه به‌عنوان موضوعی مستقل، بلکه به‌عنوان یکی از مصادیق نوین اسرار تجاری و اطلاعات محرمانه در محیط‌های مبتنی بر هوش مصنوعی انجام شده است .اهمیت این مسئله زمانی آشکارتر می‌شود که ماهیت و جایگاه اسرار تجاری و اطلاعات محرمانه موردتوجه قرار گیرد. سازمان جهانی مالکیت فکری، اسرار تجاری را دانش فنی یا تجاری محرمانه و مجموعه‌ای از اطلاعات تعریف کرده است که برای اجرای فعالیت‌های صنعتی یا توسعه فنون سودمند در یک هدف صنعتی خاص موردنیاز هستند. در حقوق اتحادیه اروپا در راستای موافقت‌نامه تریپس[1]، برای اسرار تجاری سه ویژگی اساسی در نظر گرفته است: نخست، اطلاعات در کلیت یا در ترکیب‌بندی اجزای تشکیل‌دهنده خود سری و ناشناخته بوده و به‌آسانی قابل دسترسی نباشد؛ دوم، به دلیل سری بودن دارای ارزش تجاری باشد؛ و سوم، دارنده قانونی آن اقدامات معقول و منطقی را برای حفظ محرمانگی انجام داده باشد. اسرار تجاری برخلاف سایر شاخه‌های مالکیت فکری، مانند حق اختراع، نیازی به ثبت ندارند. حمایت از آن‌ها نیز به معنای ایجاد انحصار در تولید یا ساخت نیست. *(World Intellectual Property Organization, n.d European Innovation Council and SMEs Executive Agency, 2024.)*

تعهد به حفظ محرمانگی داده‌ها نیز ناظر بر مجموعه‌ای از قواعد حقوقی، فنی و سازمانی است که هدف آن محدودسازی دسترسی به اطلاعات حساس و تضمین حمایت از آن‌ها در برابر دسترسی‌های غیرمجاز است. در محیط‌های مبتنی بر هوش مصنوعی، این تدابیر اهمیت مضاعفی پیدا می‌کنند؛ زیرا ورود اطلاعات به یک سامانه هوشمند ممکن است افزون بر ایجاد امکان پردازش فوری، زمینه ذخیره‌سازی، بازآموزی، ترکیب یا بازتولید بعدی آن اطلاعات را نیز فراهم سازد. در فضای دیجیتال، نشت اطلاعات و داده‌های محرمانه به سامانه‌های هوش مصنوعی می‌تواند به‌منزله اتخاذ تدابیر حفاظتی غیرمعقول تلقی شده و حمایت از راز تجاری را از بین ببرد. همچنین این خطر جدی برای سازمان‌ها وجود دارد که اطلاعات محرمانه سهواً توسط کارکنان در اختیار هوش مصنوعی قرار گیرد و از این طریق افشا یا نشت پیدا کند (قناد و شریف، ۱۴۰۰. لطیف‌زاده و دیگران، ۱۴۰۲). اهمیت این مسئله از آن جهت است که افشا در محیط هوش مصنوعی لزوماً به معنای انتشار مستقیم و عمومی اطلاعات نیست، بلکه ممکن است از طریق ورود داده به یک مدل عمومی، ذخیره‌سازی احتمالی، استفاده در فرایند آموزش، بازیابی در پاسخ‌های بعدی یا بازتولید غیرمستقیم محتوا تحقق یابد. ازاین‌رو، تمرکز قوانین موجود بر مفهوم سنتی افشا، به معنای انتشار عمومی یا انتقال مستقیم اطلاعات به دیگری، نمی‌تواند تمام اشکال نشت و بهره‌برداری الگوریتمی از داده‌ها را پوشش دهد یکی از مهم‌ترین ابعاد این موضوع، مسئله مالکیت داده‌های ورودی و خروجی در مدل‌های زبانی بزرگ است. در اروپا،

[1] Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement)

قانون هوش مصنوعی و در آمریکا، قوانین حق نشر به‌طور جدی با این پرسش مواجه‌اند که آیا استفاده از داده‌ها برای آموزش سامانه‌های هوش مصنوعی، استفاده منصفانه محسوب می‌شود یا نقض حقوق مالکیت فکری است. داده‌کاوی و استثنائات حقوقی مربوط به آن نیز از موضوعات پرطرفدار در میان پژوهشگران علم اطلاعات به شمار می‌رود؛ زیرا پژوهشگران برای انجام تحلیل‌های علمی نیازمند پردازش میلیون‌ها مقاله و مجموعه داده هستند، بدون آنکه امکان مطالعه انفرادی تمام آن‌ها وجود داشته باشد. اتحادیه اروپا با پذیرش استثنا، این امکان را فراهم کرده است*(Alzoubi & Mishra, 2025)* .

اتحادیه اروپا و ایالات متحده با رویکردی متفاوت، اما مکمل، چارچوب‌های متعددی برای حمایت از محرمانگی اطلاعات در هوش مصنوعی ایجاد کرده‌اند. در اتحادیه اروپا، قانون هوش مصنوعی [1]با اتخاذ رویکرد مبتنی بر ریسک، ضمن الزام به شفافیت در سامانه‌های هوش مصنوعی، در ماده ۷۸ از اسرار تجاری، اطلاعات محرمانه و حقوق مالکیت فکری حمایت کرده و افشای آن‌ها را تنها در موارد استثنایی مجاز می‌داند؛ مقررات عمومی حفاظت از داده‌ها [2]نیز با تأکید بر اصول تمامیت و محرمانگی، کنترل‌کنندگان داده را به اتخاذ تدابیر فنی و قراردادی مناسب ملزم ساخته است. دستورالعمل حمایت از اسرار تجاری [3]نیز ضمن تعریف شرایط حمایت از اسرار تجاری، امکان رسیدگی محرمانه دادگاه‌ها به اطلاعات حساس را پیش‌بینی کرده است؛ همچنین قانون داده ها [4]با ایجاد سازوکارهای قراردادی برای اشتراک داده، میان الزام به اشتراک‌گذاری داده و حفاظت از اسرار تجاری تعادل برقرار می‌کند و مقرراتی همچون دستورالعمل حریم خصوصی و ارتباطات الکترونیکی [5]، دستورالعمل حق مؤلف در بازار واحد دیجیتال [6]و دستورالعمل امنیت شبکه و اطلاعات [7]نیز این نظام حمایتی را تکمیل می‌کنند. در ایالات متحده نیز کمیسیون تجارت فدرال [8]از طریق نظارت، شرکت‌های هوش مصنوعی را به رعایت تعهدات محرمانگی و منع استفاده غیرمجاز از داده‌های کاربران ملزم می‌سازد؛ قانون حریم خصوصی مصرف‌کنندگان کالیفرنیا [9]و قانون حقوق حریم خصوصی کالیفرنیا [10]حقوق گسترده‌ای در زمینه دسترسی، حذف و شفافیت داده‌های شخصی ایجاد کرده‌اند؛ قانون افشای داده‌های آموزشی هوش مصنوعی کالیفرنیا [11]نیز توسعه‌دهندگان هوش مصنوعی مولد را به انتشار اطلاعات کلی درباره داده‌های آموزشی ملزم می‌کند؛ افزون بر این، قانون فدرال

[1] AI Act – Regulation (EU) 2024/1689با
[2] General Data Protection Regulation – GDPR, Regulation (EU) 2016/679
[3] Trade Secrets Directive – Directive (EU) 2016/943
[4] Data Act – Regulation (EU) 2023/2854
[5] ePrivacy Directive
[6] Copyright Directive Directive (EU) 2019/790
[7] NIS2 Directive – Directive (EU) 2022/2555
[8] Federal Trade Commission Act – FTC Act
[9] California Consumer Privacy Act – CCPA
[10] California Privacy Rights Act – CPRA
[11] California Assembly Bill 2013

حمایت از اسرار تجاری [1]و قوانین ایالتی مبتنی بر قانون یکنواخت اسرار تجاری [2]حمایت از اطلاعات محرمانه را مشروط به ارزش اقتصادی و اتخاذ تدابیر معقول حفاظتی دانسته و ضمانت اجراهای مؤثری برای مقابله با افشا یا سوءاستفاده از اسرار تجاری پیش‌بینی کرده‌اند. در این میان، پدیده «نوع‌دوستی داده‌ها[3]» که در قانون داده اتحادیه اروپا [4]معرفی شده است، رویکردی نوین در حکمرانی داده به شمار می‌رود. این قانون نهادهای حقوقی جدیدی با عنوان واسط‌های داده نیز ایجاد کرده است که وظیفه دارند داده‌های شهروندان را برای اهداف عام‌المنفعه، مانند تحقیقات پزشکی یا مدیریت ترافیک، به کار گیرند، بدون آنکه منفعت تجاری مستقیمی داشته باشند. شکل‌گیری چنین نهادهایی نشان می‌دهد که نظام‌های نوین حکمرانی داده، میان مالکیت، محرمانگی، دسترسی کنترل‌شده، استفاده عمومی و بهره‌برداری تجاری تمایز قائل می‌شوند و تلاش دارند به‌جای منع مطلق گردش داده، سازوکارهای حقوقی و نهادی لازم را برای استفاده مشروع، ایمن و مسئولانه از آن فراهم آورند .بااین‌حال، نظام حقوقی ایران از قانون جامع و مستقلی برای حمایت از محرمانگی داده‌ها و اسرار تجاری برخوردار نیست و حمایت‌های موجود عمدتاً در مقررات پراکنده کیفری، قانون تجارت الکترونیکی، شروط قراردادی و قواعد عمومی مسئولیت مدنی مشاهده می‌شوند.

از سوی دیگر، در بحث حفاظت از اطلاعات و اسرار تجاری که می‌تواند شامل الگوریتم‌ها و داده‌های نهان هوش مصنوعی نیز باشد، نظام حقوقی ایران با چالش فقدان قانون جامع مواجه است و حمایت‌های موجود عمدتاً به مواد ۶۴ و ۷۵ قانون تجارت الکترونیکی و قواعد عمومی مسئولیت مدنی محدود می‌شود. بااین‌حال، ویژگی ناملموس بودن اطلاعات در عصر دیجیتال سبب شده است قواعد سنتی قراردادها، نظیر خیار عیب و استرداد مورد معامله در صورت فسخ، کارایی پیشین خود را از دست بدهند؛ زیرا استرداد اطلاعات افشاشده یا معیوب عملاً ناممکن است. به همین دلیل، در صورت نقض تعهدات یا معیوب‌بودن داده‌ها، به‌جای فسخ و استرداد باید از سازوکارهایی مانند پرداخت مابه‌التفاوت استفاده شود تا از داراشدن ناعادلانه جلوگیری شود (قبولی درافشان، دانش ناری، و ساعتچی، ۱۳۹۲؛ ساعتچی و تیموری مقدم، ۱۴۰۴). براین‌اساس، خلأ اصلی در نظام حقوقی ایران آن است که مقررات موجود، به سبب پراکندگی در بسترهای کیفری و تجارت الکترونیکی و تمرکز بر

---

[1] Defend Trade Secrets Act – DTSA 2016

[2] Uniform Trade Secrets Act – UTSA

[3] فصل چهارم (Chapter IV) به نوع‌دوستی داده‌ها (Data Altruism) اختصاص یافته است و درماده ۲ بند ۱۶ نیز تعریف «نوع‌دوستی داده‌ها» را ارائه می‌دهد؛ یعنی رضایت اشخاص یا اجازه دارندگان داده برای استفاده از داده‌ها بدون دریافت پاداش و صرفاً برای اهداف دارای منفعت عمومی، مانند پژوهش‌های علمی، بهداشت عمومی، مقابله با تغییرات اقلیمی، بهبود خدمات عمومی و سایر اهداف عام‌المنفعه .همچنین این قانون نهادهای واسطه خدمات داده (Data Intermediation Services) را نیز در فصل سوم (مواد ۱۰ تا ۱۵) پیش‌بینی کرده است که به‌عنوان واسطه‌ای بی‌طرف، اشتراک‌گذاری داده‌ها را تسهیل می‌کنند و نباید از داده‌ها برای منافع تجاری خود بهره‌برداری کنند.

[4] Data Governance Act – Regulation (EU) 2022/868

مفهوم سنتی افشا، پاسخگوی ماهیت سیال، تکثیرپذیر و پردازش‌محور داده‌ها در سامانه‌های هوش مصنوعی نیستند. قواعد سنتی نیز عموماً برای اموال مادی یا روابط قراردادی‌ای طراحی شده‌اند که در آن‌ها امکان استرداد، رفع تصرف یا توقف بهره‌برداری وجود دارد؛ حال‌آنکه اطلاعات پس از افشا یا ورود به یک مدل هوش مصنوعی، ممکن است بدون زوال در اختیار دارنده اصلی، تکثیر، پردازش و بازتولید شود. در نتیجه، مفاهیمی مانند مالکیت، تصرف، افشا، اتلاف، استرداد و جبران خسارت باید متناسب با ویژگی‌های فنی و اقتصادی داده‌ها بازخوانی شوند.

این پژوهش، در پی پاسخ به این پرسش است که چگونه می‌توان مفاهیم سنتی حقوق ایران را با دکترین‌های نوین، مانند استرداد الگوریتمی[1] و تعهد مراقبت دیجیتال، هماهنگ و بازتفسیر کرد تا حمایت مؤثر از دارایی‌های فکری و اطلاعات محرمانه در برابر خطرات ناشی از هوش مصنوعی فراهم شود. هدف پژوهش آن است که با تبیین ماهیت حقوقی داده‌های ورودی و خروجی، بررسی مفهوم اقدامات معقول حفاظتی، تحلیل مسئولیت ناشی از ورود اطلاعات محرمانه به سامانه‌های هوش مصنوعی و ارزیابی ظرفیت قواعد قراردادی، کیفری و مسئولیت مدنی ایران، چارچوبی منسجم برای پیشگیری از نشت اطلاعات، تعیین مسئولیت و جبران خسارت در محیط‌های هوشمند ارائه کند.

۲. پیشینه پژوهش

با ظهور فناوری‌های نوین، مباحث مربوط به مدیریت اطلاعات و حفاظت از اسرار تجاری دگرگون شده است. در این راستا، اگرچه در منابع فارسی آثار ارزشمندی در حوزه کلی اسرار تجاری و داده‌های شخصی وجود دارد، اما بررسی تخصصی تعامل این مفاهیم با هوش مصنوعی مولد کمتر

---

[1] دکترین استرداد الگوریتمی (Algorithmic Disgorgement) یکی از نوآورانه‌ترین ضمانت‌اجراهای حقوقی در حوزه هوش مصنوعی و حفاظت از داده‌ها است که بر این مبنا استوار است که هرگاه یک مدل هوش مصنوعی یا الگوریتم با استفاده از داده‌هایی که به‌صورت غیرقانونی، فریبکارانه یا بدون رضایت معتبر گردآوری شده‌اند آموزش ببیند، حذف داده‌های اولیه به‌تنهایی برای جبران نقض کافی نیست؛ زیرا آثار آن داده‌ها در پارامترها، وزن‌ها و کارکرد مدل باقی می‌ماند. ازاین‌رو، مرجع رسیدگی می‌تواند علاوه بر حذف داده‌های نامشروع، امحا یا توقف بهره‌برداری از مدل‌ها، الگوریتم‌ها و سایر محصولات مشتق از آن داده‌ها را نیز الزام کند تا منفعت حاصل از رفتار غیرقانونی از بین برود. این دکترین نخستین‌بار در پرونده In the Matter of Everalbum, Inc. (FTC, 2021)به‌صورت عملی اجرا شد؛ جایی که کمیسیون تجارت فدرال آمریکا (FTC) پس از احراز استفاده غیرمجاز از تصاویر کاربران برای توسعه فناوری تشخیص چهره، شرکت را مکلف کرد علاوه بر حذف تصاویر و داده‌های زیستی، تمامی مدل‌ها و الگوریتم‌های تشخیص چهره آموزش‌دیده با آن داده‌ها را نیز نابود کند. این رویکرد در پرونده FTC v. Kurbo (WW International) (2022)نیز استمرار یافت؛ به‌گونه‌ای که شرکت، علاوه بر حذف اطلاعات کودکان که برخلاف قانون COPPA جمع‌آوری شده بود، ملزم شد هرگونه الگوریتم یا محصول مبتنی بر آن داده‌ها را نیز از چرخه بهره‌برداری خارج کند. همچنین در پرونده(2023) FTC v. Ring LLC ، هرچند دستور مستقلی مبنی بر امحای مدل هوش مصنوعی صادر نشد، اما کمیسیون تجارت فدرال با ممنوعیت استفاده از داده‌های به‌دست‌آمده برخلاف قانون برای توسعه یا بهبود محصولات الگوریتمی، همین رویکرد بازدارنده را تقویت کرد. مجموعه این تصمیمات نشان می‌دهد که در حقوق آمریکا، ضمانت‌اجرای نقض قواعد حریم خصوصی و محرمانگی به‌تدریج از حذف صرف داده‌های غیرقانونی فراتر رفته و به حذف یا توقف بهره‌برداری از خود محصولات هوش مصنوعی که بر پایه آن داده‌ها شکل گرفته‌اند، توسعه یافته است؛ رویکردی که در ادبیات حقوقی از آن با عنوان استرداد یا امحای الگوریتمی یاد می‌شود(Roberts. 2025).

موردتوجه قرار گرفته است .در میان منابع داخلی، شاکری (۱۳۹۴) در پژوهشی با عنوان «خوانشی بر تحدید قلمرو حقوق اسرار تجاری» به بررسی دفاعیات در دعاوی نقض پرداخته است. همچنین انصاری (۱۴۰۱) در مقاله «حمایت از اسرار تجاری در برابر افشای غیرمجاز» مبانی مسئولیت در این حوزه را تحلیل کرده است. لطیف‌زاده و همکاران (۱۴۰۲) نیز در پژوهش خود چگونگی پردازش داده‌های شخصی خاص را با نگاهی به حقوق اتحادیه اروپا مورد واکاوی قرار داده‌اند که از حیث توجه به داده‌های حساس حائز اهمیت است. بااین‌حال، پژوهش‌های مذکور عمدتاً بر پارادایم‌های سنتی یا صرفاً بر داده‌های شخصی متمرکز بوده و چالش‌های نوین ناشی از نشت الگوریتمی و تغذیه مدل‌های زبانی بزرگ را که منجر به انصراف عملی از محرمانگی می‌شود، به طور جامع پوشش نداده‌اند .در منابع لاتین، ادبیات حقوقی گسترده‌تری یافت می‌شود که می‌تواند به‌عنوان پشتوانه علمی این پژوهش مورد استفاده قرار گیرد. به‌عنوان نمونه، *Mylly (2023)* در پژوهشی به تضاد میان شفافیت هوش مصنوعی و قواعد اسرار تجاری پرداخته و لزوم ارزیابی پویای خطر محرمانگی را مطرح کرده است. همچنین، *Levine (2023)* در مقاله «هوش مصنوعی مولد و اسرار تجاری» به چالش‌های استفاده از داده‌های دارای حق نشر در آموزش مدل‌های هوش مصنوعی اشاره دارد. افزون بر آن، *Hrdy and Seaman (2024)* در بررسی تحولات قراردادهای عدم افشا، کارکرد این توافقات را پس از محدودیت‌های اعمال‌شده بر قراردادهای عدم رقابت در ایالات متحده آمریکا تحلیل کرده‌اند. همچنین، *Kesavan (2024)* چالش‌های اخلاقی و حقوقی هوش مصنوعی، به‌ویژه در زمینه حریم خصوصی داده‌ها، را بررسی کرده و بر ضرورت تدوین قوانین به‌روز، شفافیت الگوریتمی و حمایت مؤثر از داده‌های شخصی تأکید می‌کند. باوجود غنای منابع لاتین، پژوهش حاضر وجوه تمایزی با آثار پیشین دارد. نخست آنکه این پژوهش با رویکردی تطبیقی، خلأهای نظام حقوقی ایران را در مواجهه با پدیده‌هایی مذکور بررسی می‌کند. دوم اینکه، برخلاف پژوهش‌های پیشین که عمدتاً بر یکی از ابعاد مسئولیت (مدنی یا کیفری) تمرکز داشته‌اند، این مطالعه به دنبال بازتعریف ماهیت تعهد محرمانگی از یک تعهد منفی به تعهد مراقبتی مشدد ، حرفه ای و ویژه در عصر هوش مصنوعی است.

۳. روش پژوهش

پژوهش حاضر از حیث هدف، بنیادی و از نظر ماهیت، توصیفی ـ تحلیلی است و با رویکرد تطبیقی انجام شده است. هدف پژوهش، تبیین دامنه و آثار تعهد محرمانگی در حمایت از اسرار تجاری در عصر هوش مصنوعی، شناسایی چالش‌های ناشی از پردازش الگوریتمی اطلاعات و ارزیابی ظرفیت قواعد حقوق ایران با بهره‌گیری از تجارب حقوقی اتحادیه اروپا و ایالات متحده آمریکا است. گردآوری داده‌ها به شیوه کتابخانه‌ای و اسنادی صورت گرفته و منابع مورد استفاده شامل قوانین و مقررات، اسناد رسمی، آرای قضایی، تصمیم‌های نهادهای تنظیم‌گر، گزارش‌های سازمان‌های معتبر

بین‌المللی و آثار علمی مرتبط با موضوع بوده است.انتخاب منابع بر اساس چهار معیار اعتبار حقوقی، ارتباط مستقیم با پرسش پژوهش، روزآمدی و قابلیت دسترسی و ارزیابی انجام شده است. در هر نظام حقوقی، به ترتیب منابع اولیه از جمله قوانین، مقررات، آرای قضایی و تصمیم‌های رسمی نهادهای تنظیم‌گر بر منابع تفسیری و دکترین حقوقی مقدم دانسته شده‌اند و منابع ثانویه صرفاً برای تبیین، نقد و تکمیل تحلیل منابع اولیه به کار رفته‌اند. برای انجام مطالعه تطبیقی، داده‌های گردآوری‌شده بر اساس محورهای از پیش تعیین‌شده شامل مفهوم و شرایط شناسایی اطلاعات محرمانه و اسرار تجاری، معیار اقدامات معقول حفاظتی، قلمرو افشا و پردازش غیرمجاز، ماهیت تعهد محرمانگی، مبانی مسئولیت، بار اثبات، شیوه جبران خسارت و ضمانت‌اجراهای حذف یا منع استفاده از داده‌ها و الگوریتم ها دسته‌بندی شده‌اند. سپس، مقررات و رویه‌های سه نظام حقوقی در هر محور به‌صورت جداگانه توصیف و تحلیل و در مرحله بعد، وجوه اشتراک، افتراق و قابلیت بهره‌برداری از راهکارهای تطبیقی در حقوق ایران ارزیابی شده است..به طور خاص، در حقوق ایالات متحده تمرکز بر رویه قضایی و اقدامات کمیسیون تجارت فدرال [1]و تحولات سال ۲۰۲۴ در خصوص قراردادهای عدم رقابت بوده است. در حقوق اتحادیه اروپا، اسنادی نظیر دستورالعمل ۹۴۳/۲۰۱۶ مقررات عمومی حفاظت از داده [2]و قانون هوش مصنوعی [3]محور تحلیل بوده‌اند [4]. در نظام حقوقی ایران نیز قوانین تجارت الکترونیکی، مسئولیت مدنی و قواعد فقهی مرتبط مورد واکاوی قرار گرفته‌اند .داده‌های گردآوری شده به شرح پردازش شده‌اند تا نقاط اشتراک و افتراق رویکردها و نکات قابل اعمال در حقوق ایران ستخراج گردد.

۴. یافته‌های پژوهش

در اتحادیه اروپا، بنا بر ماده ۵(۱) (*f*) مقررات عمومی حفاظت از داده[5]، پردازش داده‌های شخصی باید با رعایت اصل تمامیت و محرمانگی انجام شود و در ماده ۳۲ نیز اتخاذ تدابیر فنی و سازمانی مناسب برای جلوگیری از دسترسی یا پردازش غیرمجاز الزام شده است. افزون بر این، ماده ۲۸ مقرر می‌کند پردازش‌کننده باید تضمین کند تمامی افرادی که به داده‌ها دسترسی دارند، متعهد به حفظ محرمانگی هستند یا تحت الزام قانونی مشابه قرار دارند. در کنار این مقررات، دستورالعمل اسرار تجاری نیز حفاظت از اطلاعات محرمانه تجاری را تقویت می‌کند. همچنین در ماده ۷۸ قانون هوش

---

[1] FTC (Federal Trade Commission)

[2] GDPR (General Data Protection Regulation)

[3] AI Act

[4] مباحث مربوط به محرمانگی در فرایند اجرای قانون و نظارت، موضوع ماده ۷۸؛ الزامات فنی و سازمانی حفاظت از داده شخصی، موضوعGDPR ؛ حمایت از اسرار تجاری، موضوعDirective 2016/943 و تکالیف ارائه‌دهنده مدل یا سامانه، موضوع مقررات اختصاصیAI Act ؛

[5] Article 5(1)(f) of Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)

مصنوعی اتحادیه اروپا [1]، به طور ویژه بر محرمانگی اطلاعات تأکید شده است؛ مطابق بند نخست این ماده، تمام اشخاص حقیقی یا حقوقی ذی‌مدخل در اجرای قانون مکلف‌اند داده‌های به‌دست‌آمده را محرمانه دانسته و از افشای اسرار تجاری و مالکیت فکری خودداری کنند. بند دوم همان ماده نیز مراجع نظارتی را ملزم می‌کند صرفاً داده‌های لازم را برای ارزیابی سیستم‌های پرخطر مطالبه کرده، تدابیر امنیت سایبری و محرمانگی را رعایت نموده و پس از اتمام ضرورت، داده‌ها را حذف کنند. دیوان دادگستری اروپا نیز اعلام کرده است هرگاه دو طرف در تعیین اهداف و شیوه پردازش داده نقش داشته باشند، کنترل‌کننده مشترک محسوب می‌شوند. (*ICO,2025.Gikay,*۲۰۲۵)

٤-١ دگردیسی مفهوم محرمانگی در عصر هوش مصنوعی

امروزه محرمانگی دیگر یک وضعیت ثابت و مطلق نیست، بلکه ماهیتی پویا، سیال و زمان‌مند دارد. داده‌ها در محیط دیجیتال به‌سرعت بازتولید، تغییر، پردازش و بازترکیب می‌شوند؛ بنابراین کنترل محرمانگی نیازمند نگرشی نوین است. در این رویکرد، محرمانگی باید متناسب با میزان گردش داده، تعاملات سیستمی، درجه استنباط‌پذیری توسط هوش مصنوعی و احتمال نشت الگوریتمی تنظیم شود. *(Mylly, 2023)*در اتحادیه اروپا، مقررات شرکت‌ها را موظف می‌سازد تا از افشای ناخواسته داده‌های آموزشی جلوگیری کنند و در صورت وقوع چنین رخدادی، مسئولیت مستقیم بر عهده آن‌ها خواهد بود.

کمیسیون تجارت فدرال آمریکا نیز احکامی صادر کرده که بر اساس آن، اگر داده‌ای به طور غیرقانونی جمع‌آوری شده باشد، تنها حذف داده کافی نیست؛ بلکه هر مدل هوش مصنوعی یا الگوریتمی که با آن داده آموزش‌دیده نیز باید به وضعیت سابق بازگردد. این رویکرد به‌نوعی مجازات مرگ برای داده‌ها و محصولات اطلاعاتی محسوب می‌شود. در اروپا، تمرکز بیشتر بر جریمه‌های مالی است، اما آمریکا با تأکید بر امحای کامل محصول اطلاعاتی، مسیر رادیکال‌تری را در پیش گرفته است. این موضوع به مرحله امحا در چرخه مدیریت اطلاعات مربوط می‌شود؛ مرحله‌ای که معمولاً در سیاست‌های اطلاعاتی نادیده گرفته می‌شود .ازبین‌رفتن کنترل انسانی بر داده پس از ورود به مدل می‌تواند نقض محرمانگی باشد. اروپا بر ضرورت کنترل انسانی تأکید دارد و توسعه‌دهندگان باید امکان نظارت و بازنگری انسانی را تضمین کنند.*(Brkan, 2023)* افزون بر این موارد، توانایی مدل‌های زبانی بزرگ در بازتولید داده‌های پژوهشی یکی از مسائل نوظهور در حوزه حقوق داده و مالکیت فکری است. در اتحادیه اروپا اگر بازتولید داده‌ها شامل اطلاعات شخصی یا محتوای دارای حق مؤلف باشد، شرکت‌ها موظف‌اند سازوکارهای جلوگیری از افشای غیرمجاز را پیاده‌سازی کنند. در آمریکا اگر خروجی مدل به طور مستقیم داده‌های پژوهشی را بازتولید کند، ناشران یا صاحبان حق می‌توانند

[1] Data Governance Act – Regulation (EU) 2022/868

دعوی نقض حق نشر یا محرمانگی مطرح کنند در ایران، بازتولید داده‌های پژوهشی توسط هنوز در قوانین خاص پیش‌بینی نشده است، اما می‌تواند ذیل قواعد کلی مسئولیت مدنی، نقض محرمانگی و حقوق مؤلف قرار گیرد. چالش اصلی در هر سه‌نظام حقوقی، تعیین مرز میان الهام‌گیری مشروع و بازتولید غیرمجاز است. به طور اگر پژوهشگری از هوش مصنوعی برای تحلیل داده یا نگارش بخش‌هایی از مقاله استفاده کند، پرسش اصلی این است که کدام بخش‌ها مشمول حمایت حقوقی خواهند بود. در آمریکا، راهنماهای اخیر بر ضرورت افشای نقش هوش مصنوعی تأکید دارند و بخش‌هایی که مستقیماً توسط ماشین تولید شده‌اند از دایره حمایت خارج می‌شوند. (*Kuner* & ۲۰۲۵ *Bäcker*,)

الگوی سنتی حمایت از اطلاعات محرمانه که نقض تعهد را عمدتاً در افشای مستقیم اطلاعات به شخص ثالث جست‌وجو می‌کند، دیگر برای تنظیم روابط مبتنی بر داده کفایت ندارد. در معماری سامانه‌های هوش مصنوعی، اطلاعات ممکن است بدون انتشار عمومی، در فرایندهای ذخیره‌سازی، آموزش، تنظیم مدل، استنتاج، بازترکیب، تولید خروجی یا استفاده ثانویه قرار گیرد و دارنده، امکان نظارت، حذف، محدودسازی یا جلوگیری از بازتولید آن را از دست بدهد؛ بنابراین، نقطه ثقل حمایت حقوقی باید از تحقق افشای بالفعل به حفظ کنترل مؤثر بر چرخه حیات اطلاعات انتقال یابد. محرمانگی در عصر هوش مصنوعی، وصفی ایستا و صرفاً وابسته به مخفی بودن مادی اطلاعات نیست، بلکه وضعیتی پویا، تدریجی و وابسته به میزان کنترل حقوقی، فنی و سازمانی دارنده بر اطلاعات است. ممکن است اطلاعات هنوز در دسترس عموم قرار نگرفته باشد، اما به دلیل ورود به یک سامانه عمومی، فقدان تضمین قراردادی درباره عدم استفاده آموزشی، انتقال به زیرپردازشگران ناشناخته، نبود امکان حذف یا احتمال بازیابی از طریق خروجی‌های بعدی، کنترل مؤثر دارنده بر آن عملاً زایل شده باشد. در چنین وضعی، اصرار بر اثبات مشاهده یا دریافت بالفعل اطلاعات توسط شخص ثالث، حمایت حقوقی را به مرحله‌ای موکول می‌کند که زیان غالباً غیر قابل بازگشت شده است بر این مبنا، مفهوم افشا باید در حقوق ایران به‌صورت کارکردی و فناورانه تفسیر شود. افشا تنها انتشار، تسلیم یا انتقال مستقیم اطلاعات نیست، بلکه هر اقدامی است که اطلاعات را خارج از قلمرو کنترل متعارف دارنده قرار دهد و احتمال دسترسی، استنتاج، استفاده ثانویه، بازتولید یا ادغام آن در یک سامانه دیگر را به نحو قابل توجه افزایش دهد. ازاین‌رو، ورود اطلاعات محرمانه به مدل عمومی یا سامانه‌ای که درباره محل ذخیره‌سازی، مدت نگهداری، استفاده آموزشی، زیرپردازشگران، امکان حذف و حدود بازتولید آن تضمین قابل اتکایی ارائه نمی‌کند، حسب اوضاع و احوال می‌تواند افشا یا دست‌کم نقض مستقل تعهد مراقبت از اطلاعات محسوب شود؛ هرچند هنوز انتشار عمومی یا زیان نهایی اثبات نشده باشد.

٤-١-١ توهم زایی هوش مصنوعی

توهم‌زایی هوش مصنوعی از مهم‌ترین و درعین‌حال خطرناک‌ترین چالش استفاده از هوش مصنوعی مولد در پژوهش‌های علمی است. برخلاف پایگاه‌های دانش، هوش مصنوعی مولد بر مبنای الگوهای زبانی پاسخ تولید می‌کند، نه بر اساس حقیقت‌سنجی داده‌ها. در نتیجه، این سامانه‌ها ممکن است با اعتمادبه‌نفس کامل اقدام به تولید ارجاعات جعلی، تغییر نامحسوس داده‌های عددی یا بازآرایی اطلاعات کنند تا خروجی با ساختار زبانی سازگار شود. این خطر به‌ویژه زمانی تشدید می‌شود که داده‌های خام پژوهشی برای پاک‌سازی، طبقه‌بندی یا تحلیل اولیه به هوش مصنوعی سپرده می‌شود؛ زیرا حتی تغییرات جزئی و غیرقابل‌تشخیص در داده‌ها می‌تواند کل نتایج پژوهش و قابلیت بازتولید آن را مخدوش کند .از منظر حقوقی، پدیده‌هایی نظیر دستوردادن [1]و داده‌کاوی انبوه[2]صرفاً به‌عنوان چالش‌های فنی تلقی نمی‌شوند، بلکه در بسیاری از نظام‌های حقوقی، به‌مثابه وسایل نامشروع برای تحصیل اطلاعات محرمانه مورد ارزیابی قرار می‌گیرند. معیار محوری در دعاوی مربوط به اسرار تجاری، نقض اقدامات معقول برای حفظ محرمانگی است. براین‌اساس، اگر پژوهشگر یا شرکت، داده‌های پژوهشی حساس را در پلتفرم‌های عمومی هوش مصنوعی وارد کند که صراحتاً استفاده آموزشی از داده‌ها را مجاز دانسته‌اند، ممکن است حمایت حقوقی از آن داده‌ها به طور کامل زایل شود. این وضعیت نوعی انصراف عملی از محرمانگی را مفروض می‌گیرد و بار مسئولیت حقوقی را به طور سنگینی بر دوش استفاده‌کننده از هوش مصنوعی قرار می‌دهد *(Magesh et al., 2025. Mylly, 2023.)*

٤-١-٢ توضیح‌ناپذیری هوش مصنوعی

مطابق چالش جعبه سیاه و مسئله توضیح‌پذیری در پژوهش‌های علمی[3]، صرف دستیابی به نتیجه کافی نیست، بلکه فرایند رسیدن به نتیجه باید شفاف، قابل‌توضیح و قابل‌تکرار باشد. بسیاری از مدل‌های پیشرفته هوش مصنوعی، ماهیتی جعبه سیاه دارند؛ به این معنا که داده وارد می‌شود و پاسخ خارج می‌شود، بدون آنکه منطق درونی تصمیم‌گیری به‌صورت دقیق قابل‌ردیابی باشد. این ویژگی، چالشی بنیادین برای اعتبار علمی پژوهش‌هایی ایجاد می‌کند. مقررات عمومی حفاظت از داده مفهومی تحت عنوان حق دریافت توضیح را مطرح کرده است که بر اساس آن، در صورت اتخاذ تصمیم‌های مؤثر بر اشخاص توسط الگوریتم‌ها، باید امکان توضیح منطق تصمیم‌گیری وجود داشته باشد؛ بنابراین، اگر پژوهشی مبتنی بر خروجی هوش مصنوعی باشد و پژوهشگر نتواند چرایی نتایج را تبیین کند، آن پژوهش از منظر استانداردهای حقوقی و علمی اروپا فاقد قابلیت حسابرسی تلقی می‌شود و مسئولیت

[1] Prompt Injection
[2] Scraping
[3] The Black Box Problem

خطا مستقیماً متوجه پژوهشگر خواهد بود، نه سامانه هوش مصنوعی .

اگر پژوهشگر داده‌های اختصاصی خود را به یک سامانه هوش مصنوعی بسپارد و این سامانه به کشف یک فرمول دارویی، روش فنی یا الگوریتم نوین منجر شود، این پرسش اساسی مطرح می‌شود که مخترع واقعی چه کسی است. در ایالات متحده، اداره ثبت اختراعات و علائم تجاری [1] و دادگاه‌های فدرال، به‌صراحت اعلام کرده‌اند [2] که «هوش مصنوعی نمی‌تواند مخترع باشد» و مخترع الزاماً باید یک شخص حقیقی باشد. پیامد عملی این رویکرد آن است که اگر سهم خلاقانه هوش مصنوعی بر نقش انسان غلبه داشته باشد، ممکن است اختراع اساساً فاقد قابلیت ثبت پتنت شود و در قلمرو مالکیت عمومی قرار گیرد .در اتحادیه اروپا نیز اداره ثبت اختراعات اروپا [3] موضع مشابهی اتخاذ کرده است، هرچند بحث‌هایی درباره ایجاد حقوق خاص برای پایگاه‌های داده و خروجی‌های ماشینی در حال شکل‌گیری است. بااین‌حال، در وضعیت فعلی، استفاده گسترده و غیر کنترل‌شده از هوش مصنوعی در فرایند پژوهش می‌تواند ادعای مالکیت فکری پژوهشگر را تضعیف کرده و ریسک ازدست‌رفتن انحصار حقوقی را به همراه داشته باشد*(Gryz & Rojszczak, 2021)* .

٤-١-٣ مبانی و مسئولیت در تعهدات محرمانگی

بر اساس ماده ۱۰ و ۲۲۱ قانون مدنی، توافق بر عدم افشای اطلاعات از مصادیق تعهدات قراردادی معتبر است، اما در هوش مصنوعی، موضوع تعهد دیگر صرفاً افشای مستقیم داده نیست، بلکه شامل آموزش مدل، ذخیره داده‌های مشتق‌شده و حتی تولید الگوهای آماری قابل‌بازسازی می‌شود. این تحول، تعهد محرمانگی را از یک تعهد رفتاری ساده (عدم افشا) به یک تعهد به نتیجه نسبی نزدیک می‌کند؛ به این معنا که متعهد باید نشان دهد تدابیر فنی و سازمانی متعارف برای جلوگیری از نشت داده اتخاذ کرده است. به نظر می‌رسد با ورود هوش مصنوعی، تفسیر این تعهد به سمت معیارهای سخت‌گیرانه‌تری حرکت نماید؛ به‌گونه‌ای که استفاده از داده‌های محرمانه برای آموزش یا دستور به مدل‌های هوش مصنوعی، حتی در صورت عدم افشای بیرونی، می‌تواند مصداق تعدی و تفریط در امانت یا نقض تعهد قراردادی تلقی شود. در این چارچوب، معیار تقصیر بیشتر ماهیتی عینی می‌یابد و اثبات سوءنیت شرط تحقق مسئولیت نیست؛ بلکه صرف خروج از حدود متعارف استفاده مجاز از داده، برای تحقق زمان کافی خواهد بود. همچنین ورود داده محرمانه به سامانه‌ای که عرفاً فاقد کنترل مؤثر است، می‌تواند مصداق تفریط مستقل تلقی شود، حتی اگر افشای بالفعل و قابل‌اثبات رخ نداده باشد.

---

[1] United States Patent and Trademark Office (USPTO)
[2] Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022).
[3] European Patent Office (EPO)

از منظر مسئولیت مدنی، چه در چارچوب هشدارهای کمیسیون تجارت فدرال آمریکا [1] و چه ذیل الزامات سیستم‌های پرخطر در قانون هوش مصنوعی اروپا، این اصل تثبیت شده است که مسئولیت خطا، تبعیض یا اطلاعات نادرست تولیدشده، متوجه کاربر یا بهره‌بردار سیستم است، نه الگوریتم؛ بنابراین، اتکای صرف به خروجی‌های هوش مصنوعی، بدون سازوکارهای راستی‌آزمایی انسانی، نه‌تنها از منظر علمی، بلکه از حیث حقوقی نیز غیرقابل‌دفاع خواهد بود. لکن موضع مشترک نظام‌های حقوقی آمریکا و اروپا، مبنی بر ضرورت انسان بودن مخترع، این خطر را ایجاد می‌کند که دستاوردهای حاصل از استفاده حرفه‌ای کاربر از هوش مصنوعی، از شمول حمایت خارج و عملاً وارد قلمرو مالکیت عمومی شوند. این وضعیت، پژوهشگران را با یک نتیجه مواجه می‌سازد: هرچه نقش هوش مصنوعی در تولید دانش پررنگ‌تر شود، امکان بهره‌برداری انحصاری حقوقی از نتایج آن کاهش می‌یابد.

در نظام حقوقی آمریکا، تعهد محرمانگی ماهیتی دوگانه دارد و در مرز میان مسئولیت قراردادی و مسئولیت غیرقراردادی قرار می‌گیرد. قوانین [2] سه معیار «عدم عمومیت»، «ارزش اقتصادی مستقل» و «اتخاذ اقدامات معقول حفاظتی» را برای شناسایی اسرار تجاری مقرر کرده‌اند و رویه‌های اخیر دادگاه‌های فدرال [3] ورود اطلاعات محرمانه به سامانه‌های غیرقابل‌کنترل را مخدوش‌کننده شرط سوم دانسته‌اند. بدین ترتیب، نقض تعهد محرمانگی نه‌تنها موجب ازبین‌رفتن حمایت قانونی از اطلاعات می‌شود، بلکه دعوای «سوءاستفاده از اسرار تجاری» را نیز غیرقابل‌طرح می‌سازد *(Greenberg Traurig LLP, 2024)*.

دستورالعمل و مقررات اتحادیه اروپا [4] با ترکیب رویکردهای حمایتی الگویی متفاوت ارائه کرده است. این نظام از یک‌سو بر حمایت از اسرار تجاری تأکید دارد و از سوی دیگر، با تمایز میان «اسرار تجاری» و «دانش و تجربه حرفه‌ای» کارمندان، آزادی شغلی و جابه‌جایی نیروی کار را تضمین می‌کند. در مواردی که اطلاعات محرمانه حاوی داده شخصی باشد، انتقال آن به مدل‌های هوش مصنوعی بیرون از منطقه اقتصادی اروپا بدون ابزارهای انتقالی معتبر [5] نقض مستقیم مقررات عمومی حفاظت از داده تلقی می‌شود. *(Gauci, 2025. Mylly, 2023. Chamikara et al., 2020; Pina et al., 2022; ENISA, 2014)* قانون حریم خصوصی مصرف کنندگان کالیفرنیا [6] حقوقی مانند انصراف از فروش داده، درخواست اصلاح، و محدودسازی استفاده از اطلاعات حساس را برای کاربران پیش‌بینی می‌کند.

---

[1] Federal Trade Commission (FTC)
[2] DTSA و UTSA
[3] *Beijing Neu Cloud v. IBM Corp.*, No. 22-3132 (2d Cir. 2024).
[4] GDPR و قواعد 2016/943 (EU) دستورالعمل
[5] BCR یا SCC مانند
[6] California Consumer Privacy Act

بااین‌حال، اقامه دعوی در سطح فدرال با مانع عدم امکان اثبات ذی نفعی روبه‌رو است .در واقع در نظام قضایی آمریکا، تحلیل دعاوی نقض داده مبتنی بر معیار «صدمه عینی» برای احراز ذی نفعی است. دادگاه‌ها معمولاً ادعاهای مبنی بر ترس از سوءاستفاده یا احتمال ضرر آینده را کافی نمی‌دانند *(Coffey,. 2023)*

برای اثبات نقض محرمانگی سه عنصر اساسی باید محقق شود: نخست، وجود یک داده معتبر که دارای ارزش اقتصادی بالفعل یا بالقوه بوده، ناشناخته برای عموم باشد و تحت اقدامات حفاظتی معقول قرار گرفته باشد. دوم، وقوع سوءاستفاده از طریق تصاحب، افشا یا استفاده غیرمجاز که معمولاً ناشی از خیانت، نقض اعتماد یا دسترسی نامشروع است. سوم، تحقق ضرر یا تهدید به ضرر که باید توسط شاکی اثبات گردد. در عصر هوش مصنوعی این معیار پیچیده‌تر شده، زیرا مدل‌های یادگیری می‌توانند دانش داخلی شرکت‌ها را استخراج کنند یا داده‌های محرمانه به‌طور غیرمستقیم وارد فرآیند آموزش شوند. حتی بازسازی داده‌ها تهدیدی نوین محسوب می‌شود. مهم‌ترین اقدامات معقول در آمریکا شامل کنترل دسترسی مبتنی بر نقش، محدودسازی مدل‌های زبانی داخلی، رمزنگاری داده‌های پژوهشی و ممنوعیت استفاده از مدل‌های خارجی در داده‌های محرمانه است. (*Mayer Brown, 2025*)

یکی از تفاوت‌های بنیادین میان آمریکا و اتحادیه اروپا، ضرورت اثبات ضرر مشخص در دعاوی محرمانگی است. دیوان عالی آمریکا نیز تصریح کرده است[1] که احتمال ضرر کافی نیست و شاکی باید وقوع ضرر واقعی و ملموس را نشان دهد. یکی از چالش‌های عملی دعاوی نقض محرمانگی در حقوق ایران، سنگینی بار اثبات بر دوش زیان‌دیده است؛ به‌ویژه در محیط‌های دیجیتال که اثبات مسیر نشت داده یا رابطه سببیت فنی بسیار دشوار است. بااین‌حال، با تفسیر پویا از قواعد مسئولیت مدنی، می‌توان به‌سوی جابه‌جایی محدود بار اثبات حرکت کرد. هرگاه متعهد مدیریت داده را بر عهده گرفته و داده محرمانه در حوزه تصرف و کنترل او قرار داشته باشد، اصل باید بر مسئولیت وی استوار شود، مگر آنکه اثبات کند کلیه تدابیر متعارف و متناسب با ریسک را اتخاذ کرده است.

در ایران، قانون جرایم رایانه‌ای نیز افشای غیرمجاز یا دسترسی بدون مجوز به داده‌ها و سامانه‌های حفاظت‌شده را واجد وصف کیفری دانسته است. در ایالات متحده نیز چارچوب ایالتی و متغیر حریم خصوصی مصرف‌کننده حقوقی همچون حق انصراف از فروش داده، حق تصحیح و حق محدودسازی استفاده از داده‌های حساس ایجاد کرده است.*(Nautsch et al., 2019)* ابعاد مسئولیت و جبران خسارت ناشی از نقض محرمانگی در ماده ۸۲ نیز و تفاسیر دیوان دادگستری اتحادیه اروپا [2]روشن شده است. این دیوان با پذیرش نظام مسئولیت مبتنی بر تقصیر، بار اثبات را بر دوش کنترل‌کننده قرار داده است؛

---

[1] TransUnion LLC v. Ramirez
ممکن است برای دستور موقت، تهدید به سوءاستفاده کافی باشد، حتی اگر خسارت نهایی هنوز محقق نشده باشد

[2] CJEU

به‌گونه‌ای که وی باید نشان دهد هیچ نقشی در وقوع حادثه نداشته است. این استاندارد در حوزه هوش مصنوعی، با توجه به پیچیدگی و آسیب‌پذیری سیستم‌ها در برابر حملات سایبری، چالش‌های عملیاتی مضاعفی ایجاد می‌کند و کنترل‌کننده ناچار است ثابت کند اقدامات اتخاذشده مطابق استانداردهای ماده ۲۴ و ۳۲ بوده و متناسب با ریسک عمل کرده است (*Timelex, 2024;; Inside Privacy, 2024.European Parliamentary Research Service, 2025*) .

قوانین ایالتی آمریکا [1] نیز بعد دیگری به این چارچوب افزوده‌اند. مقررات جدید فناوری تصمیم‌گیری خودکار شرکت‌ها را ملزم می‌کند هنگام استفاده از ابزارهای هوش مصنوعی برای تصمیمات مهم، اطلاع‌رسانی شفاف ارائه دهند و امکان دسترسی و اعتراض کاربران را فراهم سازند؛ سازوکاری که معادل ایالتی تضمین‌های ماده ۲۲ حفاظت از داده تلقی می‌شود. دادگاه‌ها حتی داده‌های محرمانه خروجی را برای اثبات دعاوی مالکیت فکری قابل افشا دانسته‌اند[2]. همچنین پرونده دیگری [3] نشان داد که استفاده تحول‌آفرین از داده‌های دارای حق نشر در آموزش مدل، اگر با روش غیرقانونی به‌دست آمده باشد، خارج از حمایت استفاده منصفانه قرار می‌گیرد؛ بدین معنا که مشروعیت روش دستیابی به داده‌ها نیز شرط اساسی حمایت است(*Levine, 2023* .) تفاوت اصلی میان نظام‌ها در تعادل میان شفافیت الگوریتمی و حفاظت از راز تجاری نهفته است. اتحادیه اروپا با اولویت حقوق فردی، در ماده ۲۲ حفاظت از داده حق افراد برای عدم پذیرش تصمیمات صرفاً خودکار، حق مداخله انسانی و حق توضیح‌پذیری را تضمین کرده است. رأی دیوان دادگستری اتحادیه اروپا [4] نیز تصریح کرد که اعضا نمی‌توانند به‌طور مطلق با استناد به راز تجاری مانع دسترسی افراد به داده‌های شخصی شوند و باید میان حقوق رقابتی توازن برقرار کنند(*Stibbe, 2025*) .

٤-١-٤ جایگاه قرارداد عدم افشا و عدم رقابت در خدمات مبتنی بر هوش مصنوعی

هم‌زمان، با گسترش فناوری‌های دیجیتال و هوش مصنوعی، دکترین‌های سنتی حقوق اسرار تجاری با تأکید بیشتری بر استثنائاتی مانند کشف مستقل، مهندسی معکوس و اطلاعات در دسترس عموم تفسیر می‌شوند و صرف شباهت نتیجه، بدون اثبات دسترسی غیرمجاز یا سوءاستفاده واقعی از اطلاعات محرمانه، برای مسئولیت قراردادی یا مدنی کافی تلقی نمی‌شود. در مجموع، نظام حقوقی آمریکا به‌سوی مدلی حرکت کرده است که در آن حفاظت از اطلاعات محرمانه صرفاً تا جایی معتبر است که به انحصار دانشی، قفل‌شدن نیروی انسانی یا اختلال ناموجه در رقابت منجر نشود. در ایالات

---

[1] مانند CCPA/CPRA
[2] OpenAI ، مانند پرونده نیویورک تایمز علیه
[3] Anthropic
[4] پرونده C-203/22

متحده افزون بر سازوکارهای جبرانی متعارف، این قانون امکان صدور دستور توقیف قضایی فوری را در موارد خطر قریب‌الوقوع نابودی یا انتقال غیرقانونی اسرار تجاری پیش‌بینی کرده است. (Chambers and Partners, n.d.; Legal Information Institute, ۲۰۲۴; World Intellectual Property Organization, ۲۰۲۵) توسعه بیش‌ازحد شروط محرمانگی می‌تواند عملاً اثر یک موافقت‌نامه عدم رقابت را ایجاد کند. (Pelletier, 2019) دکترین افشای اجتناب ناپذیر به محاکم اجازه می‌دهد تا با استناد به این امر که کارمند سابق با توجه به دانش فنی کسب شده در موقعیت قبلی، نمی‌تواند از آن در شغل جدید خودداری کند، استخدام او توسط رقیب را ممنوع سازند. این دکترین به‌عنوان معادل قرارداد عدم رقابت عمل می‌کند و به همین دلیل، در برخی ایالت‌ها مانند کالیفرنیا که از پویایی نیروی کار حمایت می‌کنند، پذیرفته نشده است. بااین‌حال، در حقوق ایران، با وجود عدم تصریح به این دکترین، می‌توان با استناد به اصل عدم سلب حقوق مدنی شرط نامعقولی که منجر به سلب حق اشتغال شود، را اجرا نکرد یا آن را محدود ساخت (انصاری، ۱۴۰۱. بخت‌جو و دیگران، ۱۳۹۸.). رخداد افشای اطلاعات محرمانه سامسونگ در ۲۰۲۳ [1]نشان داد که ورود سهوی کدها به مدل‌های عمومی می‌تواند وضعیت حقوقی شرکت را به‌شدت تضعیف کند، و در بسیاری از حوزه‌های قضایی چنین رفتاری معادل زوال وصف محرمانگی تلقی می‌شود. ازاین‌رو، شرکت‌ها ناگزیر شده‌اند بند ممنوعیت تغذیه هوش مصنوعی [2]را در قراردادهای کار و عدم افشا درج کنند و ضمانت‌اجراهایی را برای نقض احتمالی پیش‌بینی نمایند. این ضرورت با تعارض هایی در عمل همراه است بدین شرح که کارکنان برای ارتقای بهره‌وری، ناخواسته داده‌های حساس را در پرامپت مدل‌های خارجی وارد می‌کنند، رفتاری که با توجه به پردازش خارجی و غیرقابل‌کنترل، مصداق افشا به شخص ثالث تلقی شده و تفسیر سنتی افشا و محرمانگی را در سطح بین‌المللی دگرگون کرده است.(Hacker et al., 2023; Kwakye, 2022) . باید توجه داشت که تعهد به محرمانگی تنها زمانی مشروعیت دارد که محدود به اطلاعات مشخص، دارای ارزش اقتصادی مستقل و مستند باشد و نه یک ممنوعیت کلی و نامحدود زمانی-مکانی. در حقوق ایران، محرمانگی ضمنی می‌تواند تعادل مناسبی ایجاد کند. درج یک ممنوعیت کلی نسبت به هرگونه استفاده از هوش مصنوعی، راهکاری واقع‌بینانه نیست و می‌تواند بهره‌وری مشروع را مختل کند. راه‌حل مناسب، تنظیم نظام استفاده مجاز و طبقه‌بندی‌شده است. قرارداد یا سیاست سازمانی باید مشخص کند چه اطلاعاتی، در چه سامانه‌هایی، برای چه هدفی، با چه سطحی از ناشناس‌سازی، تحت چه تضمین‌های قراردادی و با تأیید کدام مقام سازمانی قابل پردازش است. همچنین باید استفاده از داده برای آموزش مدل، نگهداری پرامپت‌ها، استفاده ثانویه، انتقال به زیرپردازشگر، تولید خروجی

[1] Samsung’s confidential data leak to ChatGPT.
[2] Clause Prohibiting AI Training

مشتق‌شده و نگهداری سوابق پردازش به‌طور مستقل تعیین تکلیف شود.

٤-١-٤ -١ تعهد به عدم رقابت پس از خاتمه قرارداد

قراردادهای عدم افشا و عدم رقابت بر پیش‌فرض‌های انسان‌محور استوارند؛ یعنی فرض می‌شود متعهد قادر به تشخیص رقیب، درک معنای رازداری و کنترل آگاهانه انتقال یا عدم انتقال اطلاعات است، حال آن‌که هوش مصنوعی فاقد چنین ادراک هنجاری و قصد حقوقی است و اطلاعات را نه بر اساس تعهد قراردادی بلکه صرفاً بر مبنای الگوهای آماری و پرسش‌های ورودی پردازش و بازتولید می‌کند. افزون بر این، در معماری رایج سامانه‌های هوش مصنوعی، داده‌های محرمانه غالباً به زیرساخت‌های شرکت‌های ثالث منتقل می‌شوند؛ امری که عملاً دایره روابط قراردادی را از دو طرف اصلی فراتر برده و شخص یا اشخاص ثالثی را وارد زنجیره پردازش داده می‌کند که الزاماً تابع تعهدات عدم رقابت اولیه نیستند؛ بنابراین، اتکای صرف به سازوکارهای قراردادی سنتی در مواجهه با هوش مصنوعی ناکافی بوده و بدون پیش‌بینی تعهدات ویژه، کنترل‌های فنی و رژیم‌های مسئولیت متناسب با چرخه یادگیری و بازتولید داده، کارکرد حمایتی این قراردادها به‌طور جدی تضعیف می‌شود (Veale & Borgesius, 2021). تعهد به عدم رقابت و تعهد به محرمانگی در دهه‌های گذشته اغلب به‌صورت توأمان به کار می‌رفتند تا کارفرما پس از خروج کارمند، هم از انتقال مستقیم اطلاعات و هم از بهره‌برداری غیرمستقیم آن در شرکت رقیب جلوگیری کند. با ممنوعیت تقریباً کامل توافق‌نامه‌های عدم رقابت در آمریکا و محدودیت شدید آن در اتحادیه اروپا (اصل تناسب و حفظ پویایی بازار کار طبق دستورالعمل ۹۴۳/۲۰۱۶)، این تحولات، مرز میان استفاده از اطلاعات محرمانه شرکت و بهره‌گیری از تجربه شخصی کارمند را بیش از پیش حساس کرده و دادگاه‌ها را وادار می‌سازد تا با دقت بررسی کنند که آیا رفتار کارمند سابق واقعاً نقض اطلاعات مشخص و قابل شناسایی است یا صرفاً کاربرد مهارت عمومی(Hrdy & Seaman, 2024) . مدت زمان تعهد به محرمانگی معمولاً مستقل از قرارداد اصلی بوده و تا زمانی ادامه دارد که اطلاعات وصف محرمانه خود را حفظ کرده باشند؛ بنابراین پایان قرارداد، خاتمه سمت یا استعفا تأثیری در بقای آن ندارد و مدیر یا کارمند سابق همچنان مکلف به رعایت محرمانگی است .در نظام‌های حقوقی آمریکا این مدت غالباً حدود پنج سال و در اروپا تا ده سال نیز قابل تمدید است، اما در مورد اطلاعاتی با ارزش اقتصادی نامعلوم مانند دانش فنی غیر قابل ثبت یا فهرست مشتریان، تعهد محرمانگی ممکن است بدون قید زمان و به‌صورت نامحدود برقرار بماند(Aplin et al. .2023) .

٤-١-٥ دامنه تعهد

ایالات متحده تعریف گسترده‌ای از اطلاعات محرمانه ارائه می‌دهد و حتی اطلاعات منفی [۱] را نیز تحت پوشش قرار می‌دهد. اروپا با وجود حمایت گسترده، دایره اطلاعات را با ملاحظات رقابتی و حقوق بنیادین محدود کرده و میان اسرار تجاری و دانش و مهارت عمومی کارکنان تفکیک قائل شده است. در ایران، معیار تشخیص اطلاعات محرمانه عمدتاً مبتنی بر «ماهیت ذاتی محرمانگی» است و قانون تجارت الکترونیک امکان تفسیر موسع را فراهم می‌کند، اما نبود تمایز میان اسرار تجاری و داده‌های فاقد ارزش اقتصادی موجب ابهام شده است. در تعریف اسرار تجاری الکترونیکی در ایران (ماده ۶۵ قانون تجارت الکترونیکی)، مجموعه‌ای از اطلاعات (شامل فرمول‌ها، الگوها، نرم‌افزارها، طرح‌های تجاری و...) به‌عنوان اسرار تجاری ذکر شده که به طور مستقل دارای ارزش اقتصادی بوده و در دسترس عموم قرار ندارند الگوی دسترس پذیری مشروع میتواند در تفسیر ماده به کار رود.

قرارداد محرمانگی در شرکت‌ها، به‌ویژه در سازمان‌های بزرگ، باید دامنه شمول اشخاصی را که اطلاعات محرمانه را دریافت می‌کنند به‌طور دقیق برای تمام طرفین از جمله مدیران، کارکنان سطح بالا، سرمایه‌گذاران، مشاوران و حتی شرکت‌های فرعی و وابسته مشخص کند (Zuiderveen Borgesius & Steenbruggen, 2023; Pina et al., 2022).

٤-١-٥-١ استثنائات تعهد محرمانگی

در حقوق آمریکا و اتحادیه اروپا، برای جلوگیری از شکل‌گیری انحصار مطلق بر اطلاعات محرمانه، مجموعه‌ای از استثنائات بنیادین بر تعهد به محرمانگی شناسایی شده است. مهم‌ترین این استثنائات کشف مستقل و مهندسی معکوس هستند؛ بدین معنا که اگر شخص بدون اتکا به اطلاعات دیگری و از طریق تحقیق یا سرمایه‌گذاری مستقل به همان داده دست یابد، یا محصولی را با ابزارهای مشروع تحلیل کند، نقض محرمانگی محسوب نمی‌شود. همچنین اطلاعاتی که بدون تقصیر دریافت‌کننده وارد حوزه عمومی شده یا به‌طور قانونی از شخص ثالثی بدون تعهد محرمانگی به دست آمده باشد، از شمول حمایت خارج است. افزون بر این، دستورالعمل ۲۰۱۶ اتحادیه اروپا و رویه آمریکا در مواردی استثنایی افشای اسرار برای منافع عمومی مانند سلامت، امنیت یا رقابت را مشروع می‌دانند (European Union, 2016; GDPR.2016 ; Hrdy & Seaman, 2024; De Noyette, Stähler, & Margoni, 2025). در آمریکا، تمایز میان نحوه اعلام رضایت [۲] ضروری است و صرفاً رضایت صریح به‌عنوان اقدام معقول پذیرفته می‌شود. در اتحادیه اروپا، رضایت باید صریح و آگاهانه باشد و

---

[۱] منظور از اطلاعات منفی Negative Information یا Negative Know-how در حقوق اسرار تجاری، اطلاعاتی نیست که ارزش منفی داشته باشند؛ بلکه به دانش حاصل از شکست‌ها، آزمون‌های ناموفق، مسیرهای اشتباه و نتایجی که نشان می‌دهد چه کاری نباید انجام شود اشاره دارد.

[۲] در قراردادهای Clickwrap کاربر با اقدام صریح مانند کلیک بر دکمه «I Agree» رضایت خود را اعلام می‌کند و همین امر آن را معتبرتر می‌سازد. در مقابل، Browsewrapصرفاً با استفاده یا مرور سایت رضایت ضمنی کاربر را فرض می‌گیرد که معمولاً از نظر دادگاه‌ها کمتر الزام‌آور است.

توافق‌های ضمنی یا چک‌باکس‌های از پیش فعال بی‌اعتبارند .(Drexl, J. 2019)

در حقوق ایران، تعهد محرمانگی نمی‌تواند به‌گونه‌ای تفسیر یا اجرا شود که به‌طور غیرمستقیم موجب محدودیت ناموجه آزادی شغلی یا رقابت مشروع گردد و اگر شخص بدون دسترسی غیرمجاز و بدون نقض تعهد قراردادی، از طریق تحقیق مستقل یا منابع آزاد به همان اطلاعات دست یابد، وصف محرمانگی نسبت به او قابل تسری نیست. همچنین اطلاعاتی که بدون تقصیر متعهد وارد حوزه عمومی شده‌اند، موضوع تعهد محرمانگی باقی نمی‌مانند. افزون بر این، افشای اطلاعات در موارد استثنایی برای دفع ضرر شدید، حفظ منافع عمومی، یا اجرای تکالیف قانونی می‌تواند با اتکاء به قواعدی چون اضطرار، لاضرر و نظم عمومی، موجه تلقی شود. در نهایت، در حقوق ایران نیز، مرز میان عدم افشا و عدم رقابت باید مضیق تفسیر شود و هرگونه شرط محرمانگی که عملاً کارکرد منع رقابت پیدا کند، در معرض بی‌اعتباری یا تفسیر محدودکننده قرار می‌گیرد.

٤-١-٦ قابلیت انتقال و مدیریت داده های پژوهشی

در ایالات متحده، شرکت‌های فناوری و پژوهشگران با اتکا به دکترین استفاده منصفانه استدلال می‌کنند که بهره‌گیری از آثار دارای حق مؤلف برای آموزش مدل‌های هوش مصنوعی، ماهیتی تغییریافته دارد و جایگزین اثر اصلی نمی‌شود. طبق دستورالعمل کپی رایت اتحادیه اروپا[1]، پژوهشگران دانشگاهی از استثنای خاصی برای متن‌کاوی و داده‌کاوی برخوردارند، اما شرکت‌های تجاری تنها در صورتی مجاز به استفاده هستند که صاحبان حق صراحتاً آن را منع نکرده باشند.

در آمریکا، مقررات حریم خصوصی با اعطای یک استثناء پژوهشی در قوانین ایالتی انعطاف‌پذیری خاصی را برای داده‌های علمی و عمومی فراهم کرده‌اند. با این وجود، استفاده از این استثناء مشروط به رعایت معیارهای سخت‌گیرانه‌ای از جمله ضرورت حفظ داده برای تحقق هدف پژوهش، اخذ رضایت آگاهانه پیشینی و رعایت الزامات اخلاقی و حریم خصوصی است. این چارچوب یک توازن دشوار میان منافع عمومی پژوهش و حق کنترل داده‌های شخصی ایجاد می‌کند. در اتحادیه اروپا، پروژه‌های تحقیقاتی که داده‌های شخصی را پردازش می‌کنند، به‌طور کامل تحت الزامات محافظت از داده قرار دارند. رعایت تدابیر فنی و سازمانی مناسب برای جلوگیری از دسترسی غیرمجاز یا ازدست‌رفتن داده‌ها الزامی است و شبه‌گمنام‌سازی به‌عنوان یک ابزار کلیدی به‌کار می‌رود.

---

[1] در اتحادیه اروپا، مواد ۳ و ۴ دستورالعمل کپی‌رایت در بازار دیجیتال واحد (Directive 2019/790) استثنای خاصی را برای متن‌کاوی و داده‌کاوی جهت اهداف پژوهشی و علمی پیش‌بینی کرده‌اند. بر اساس این استثنا، مؤسسات تحقیقاتی و دانشگاه‌ها مجازند داده‌ها و مقالات را برای آموزش مدل‌ها و تحلیل‌های الگوریتمی پردازش کنند، مشروط بر آنکه دسترسی اولیه قانونی باشد. اما برای مصارف تجاری، دارندگان حقوق می‌توانند با استفاده از سازوکار خروج اختیاری(Opt-out) ، مانع داده‌کاوی شوند. در مقابل، در ایالات متحده آمریکا، شرکت‌های فناوری عمدتاً با اتکا به دکترین استفاده منصفانه (Fair Use) ذیل ماده ۱۰۷ قانون کپی‌رایت استدلال می‌کنند که آموزش مدل‌های زبانی از داده‌های عمومی، ماهیتی دگرگون‌کننده (Transformative)داشته و نقض مالکیت فکری یا محرمانگی محسوب نمی‌شود؛ موضعی که هم‌اکنون موضوع دعاوی متعدد قضایی است.

بااین‌حال، محافظت از داده تأکید می‌کند که داده‌های شبه‌گمنام همچنان داده شخصی محسوب می‌شوند مادامی که امکان بازشناسایی از طریق اطلاعات تکمیلی وجود داشته باشد؛ بنابراین مؤسسات پژوهشی موظف‌اند داده‌های هویتی و کلیدهای بازشناسایی را به‌طور مستقل و در محیط کاملاً امن نگهداری کنند تا ریسک انتساب داده‌ها به افراد کاهش یابد .(*Crescioni & Sklar, 2020*) مسئولیت مدنی و قراردادی دراحتمال نقض اسرار تجاری شامل جبران خسارت کامل و مؤثر است؛ در اتحادیه اروپا حتی جریمه باید بیش از سود متخلف باشد .قراردادهای عدم افشا می‌توانند با وجه التزام قراردادی از دشواری اثبات خسارت جلوگیری کنند و دارنده حق دارد دستور توقف افشا یا استفاده غیرمجاز را از دادگاه بخواهد .همچنین گیرنده اطلاعات موظف است پس از پایان قرارداد، تمامی داده‌های محرمانه را بازگرداند یا نابود کند.

الزام به مستندسازی داده‌های آموزشی و الزامات شفافیت می‌تواند تهدیدی برای اسرار تجاری شرکت‌ها باشد، زیرا افشاگری بیش از حد می‌تواند به افشای معماری مدل یا منابع داده منجر شود. همچنین تحت قانون بازارهای دیجیتال[1]،تکالیفی درخصوص تضمین بی‌طرفی، جلوگیری از سوءاستفاده داده و حفاظت از اسرار تجاری کسب‌وکارها دارند و هرگونه استخراج الگوریتمی داده از طریق مدل‌های هوش مصنوعی می‌تواند نقض تکلیف استفاده مشروع از داده تلقی شود. علاوه بر این، حق دسترسی پژوهشگران به داده‌های آموزشی ممکن است به‌طور ناخواسته امکان نفوذ به اطلاعات محرمانه یا مالکیت فکری شرکت‌ها را فراهم آورد. *(Busuioc et al., 2023)*

برای هر مقاله یا مجموعه‌داده پژوهشی، باید از ابتدای فرایند تحقیق، نوع داده‌های گردآوری‌شده، میزان حساسیت آن‌ها و شیوه یا حدود اشتراک‌گذاری مشخص شود و اطلاعات مربوط به استفاده ثانویه و انتشار احتمالی داده‌ها نیز به‌صورت شفاف در فرم رضایت آگاهانه شرکت‌کنندگان درج گردد. پیش از هرگونه اشتراک‌گذاری، لازم است خطر بازشناسایی هویت اشخاص، هم از نظر کمی و هم از نظر کیفی، ارزیابی شود؛ زیرا حذف نام و مشخصات مستقیم، به‌تنهایی مانع شناسایی مجدد افراد نمی‌شود و ممکن است ترکیب متغیرها، داده‌های زمینه‌ای یا فراداده‌ها امکان پیوند دادن اطلاعات به اشخاص معین را فراهم سازد. بر همین اساس، باید متناسب با ماهیت داده‌ها و سطح خطر، روش مناسبی برای ناشناس‌سازی یا مستعارسازی انتخاب شود و فراداده‌ها نیز تنها در حد ضروری و به‌گونه‌ای ثبت و منتشر شوند که احتمال ردیابی و بازشناسایی شرکت‌کنندگان کاهش یابد. در مواردی که انتشار عمومی داده‌ها می‌تواند حقوق و حریم خصوصی اشخاص را به خطر اندازد، استفاده از محیط‌های پژوهشی امن، دسترسی کنترل‌شده، قراردادهای استفاده از داده و مستندسازی دقیق شرایط دسترسی، بر انتشار آزاد و کامل داده‌ها ترجیح دارد.

[1] Digital Markets Act (DMA)

همچنین در مقالات بالینی، مطابق دستورالعمل‌های کمیته بین‌المللی سردبیران نشریات پزشکی، باید بیانیه‌ای روشن درباره اشتراک‌گذاری داده‌ها منتشر شود که در آن نوع داده‌های قابل دسترس، اشخاص یا گروه‌های مجاز به استفاده، شرایط دسترسی و تدابیر حفاظتی پیش‌بینی‌شده مشخص شده باشد. از آنجا که فناوری‌ها و روش‌های بازشناسایی داده‌ها به‌طور مستمر در حال تحول‌اند، سیاست‌های مربوط به ناشناس‌سازی، دسترسی و اشتراک‌گذاری داده‌های شخصی نیز باید به‌صورت مستمر ارزیابی و در دوره‌های زمانی معین بازنگری و به‌روزرسانی شوند.(Sandeen & Mylly, 2020)

۵. نتیجه‌گیری و پیشنهاد ها

یافته‌های پژوهش حاضر نشان می‌دهد که الگوی سنتی حمایت از محرمانگی برای مواجهه با مخاطرات ناشی از هوش مصنوعی نیازمند بازنگری است. در حالی که شاکری (۱۳۹۴) و انصاری (۱۴۰۱) نقض محرمانگی را عمدتاً در قالب افشای غیرمجاز یا استفاده بدون مجوز از اطلاعات تحلیل کرده‌اند، یافته‌های این پژوهش بیانگر آن است که در محیط‌های مبتنی بر هوش مصنوعی، صرف ورود اطلاعات محرمانه به مدل‌های عمومی یا فاقد کنترل کافی، حتی بدون افشای مستقیم، می‌تواند از طریق ذخیره، استنتاج، بازترکیب یا بازتولید داده‌ها موجب ازدست‌رفتن کنترل مؤثر دارنده بر اطلاعات شود و ازاین‌رو، خود از مصادیق نقض تعهد محرمانگی محسوب گردد. همچنین، یافته‌ها با نتایج لطیف‌زاده و همکاران (۱۴۰۲) در خصوص لزوم اتخاذ تدابیر متناسب حفاظتی و با دیدگاه ***Mylly (2023)*** درباره ارزیابی مستمر خطر محرمانگی و ***Levine (2023)*** پیرامون مخاطرات آموزش مدل‌های هوش مصنوعی با داده‌های محرمانه همسو است؛ با این تفاوت که پژوهش حاضر افزون بر داده‌های شخصی، اسرار تجاری، داده‌های پژوهشی، مجموعه‌داده‌های آموزشی، الگوریتم‌ها و پارامترهای مدل را نیز در بر می‌گیرد و با استناد به قواعد مسئولیت قراردادی و مدنی در حقوق ایران، از جمله امانت، تعدی و تفریط و تسبیب، مبنای حقوقی تعهد مراقبتی ویژه را تبیین می‌کند. افزون بر این، اگرچه مطابق دیدگاه ***Seaman*** و ***Hrdy (2024)***، قراردادهای عدم افشا همچنان نقش بنیادینی در حمایت از اطلاعات محرمانه دارند، یافته‌های این پژوهش نشان می‌دهد که تحقق معیار اقدامات معقول حفاظتی مستلزم تلفیق تعهدات قراردادی با تدابیر فنی و سازمانی نظیر کنترل دسترسی، رمزنگاری، ثبت وقایع، محدودیت استفاده ثانویه، حذف ایمن داده‌ها و ارزیابی مستمر مخاطرات است.

در حقوق ایران، با وجود فقدان قانون جامع اسرار تجاری و حکمرانی داده، نمی‌توان از فقدان کامل مبنای حمایت سخن گفت. مواد ۱۰، ۲۱۹، ۲۲۰، ۲۲۱ و ۲۳۰ قانون مدنی، قواعد مربوط به امانت، تعدی و تفریط، تسبیب، اتلاف، لاضرر، منع سوءاستفاده از حق، قانون مسئولیت مدنی و مقررات قانون تجارت الکترونیکی ظرفیت آن را دارند که تعهد محرمانگی را در روابط قراردادی و حرفه‌ای پوشش دهند. بااین‌حال، پراکندگی مقررات، تمرکز آنها بر اشکال سنتی افشا، فقدان تعریف روشن از پردازش

مجاز و غیرمجاز، دشواری اثبات رابطه سببیت فنی و نبود ضمانت‌اجراهای متناسب با ماهیت تکثیرپذیر داده، مانع شکل‌گیری حمایت منسجم و قابل پیش‌بینی شده است.

مهم‌ترین بازسازی نظری لازم در حقوق ایران آن است که تعهد محرمانگی از یک تعهد صرفاً سلبی مبنی بر خودداری از افشا به یک تعهد مراقبت دیجیتال تحول یابد. بر اساس این تعهد، متعهد نه‌تنها باید از افشای عمدی اطلاعات خودداری کند، بلکه موظف است متناسب با ماهیت اطلاعات، ارزش اقتصادی آن، شدت خسارت احتمالی، قابلیت بازشناسایی، نوع سامانه مورد استفاده و هزینه معقول پیشگیری، اقدامات قراردادی، فنی و سازمانی لازم را اتخاذ کند.

این تعهد را نباید مطلقاً تعهد به نتیجه دانست؛ زیرا تضمین عدم وقوع هرگونه نشت در محیط پیچیده دیجیتال، حتی با رعایت بالاترین استانداردها، همواره ممکن نیست. از سوی دیگر، تقلیل آن به یک تعهد ساده به وسیله نیز حمایت کافی ایجاد نمی‌کند. در الگو پیشنهادی، زیان‌دیده باید وجود رابطه محرمانگی، سپردن یا دسترسی متعهد به اطلاعات و وقوع یک حادثه خارج از روند مجاز پردازش را اثبات کند؛ پس از آن، متعهد باید نشان دهد که تمام تدابیر فنی، قراردادی و سازمانی متناسب با خطر را رعایت کرده است. چنین جابه‌جایی محدودی در بار اثبات، نه مسئولیت محض ایجاد می‌کند و نه زیان‌دیده را مکلف می‌سازد واقعیت‌هایی را اثبات کند که منحصراً در اختیار کنترل‌کننده سامانه قرار دارند. معیار ارزیابی رفتار متعهد نیز باید تناسب اقدامات حفاظتی با سطح خطر باشد. بدین معنا که یک استاندارد واحد برای تمام اطلاعات و سازمان‌ها قابل اعمال نیست. سطح مراقبت مورد انتظار درباره فرمول صنعتی، کد منبع، داده پزشکی، اطلاعات مشتریان، طرح تجاری و داده پژوهشی حساس با اطلاعات عادی اداری یکسان نیست. ارزش اقتصادی اطلاعات، تعداد اشخاص دارای دسترسی، قابلیت تکثیر، امکان بازشناسایی، حساسیت داده، محل پردازش، نوع مدل و احتمال استفاده آموزشی باید در تعیین میزان مراقبت مؤثر باشد. اقدامات لازم برای تحقق این تعهد، حسب مورد، شامل طبقه‌بندی اطلاعات، تعیین مالکان و متولیان داده، اعمال اصل حداقل دسترسی، احراز هویت چندمرحله‌ای، رمزنگاری، ثبت وقایع، محدودسازی انتقال، ناشناس‌سازی یا مستعارسازی، ارزیابی تأمین‌کنندگان فناوری، ممنوعیت استفاده از مدل‌های عمومی برای اطلاعات طبقه‌بندی‌شده، ایجاد مدل‌های داخلی یا محیط‌های سازمانی کنترل‌شده، ممیزی امنیتی دوره‌ای، آموزش کارکنان، مدیریت رخداد، تعیین دوره نگهداری و حذف ایمن اطلاعات است. وجود قرارداد عدم افشا بدون اجرای این تدابیر، به‌تنهایی دلیل اتخاذ اقدامات معقول حفاظتی محسوب نمی‌شود.

از حیث مسئولیت، باید میان اشخاص مختلف زنجیره پردازش تفکیک صورت گیرد. مسئولیت کارمند یا کاربر نهایی، مدیر سازمان، مالک اطلاعات، کنترل‌کننده داده، پیمانکار فنی، پردازشگر و ارائه‌دهنده مدل لزوماً یکسان نیست. کارمند هنگامی مسئول است که برخلاف آموزش، سیاست روشن

یا حدود دسترسی عمل کرده باشد. مدیر یا سازمان زمانی مسئول خواهد بود که از تدوین سیاست، آموزش کارکنان، انتخاب سامانه ایمن یا نظارت بر دسترسی‌ها خودداری کرده باشد. ارائه‌دهنده سامانه نیز در صورتی باید مسئول شناخته شود که برخلاف تعهدات اعلامی، اطلاعات را ذخیره، برای آموزش استفاده یا به اشخاص ثالث منتقل کرده، یا خطرات اساسی و قابل پیش‌بینی محصول خود را پنهان کرده باشد .در این زمینه، پذیرش مسئولیت مشترک یا تضامنی باید محدود به مواردی باشد که رفتار چند عامل در ایجاد زیان نقش مؤثر داشته و تفکیک سهم آنها برای زیان‌دیده ناممکن یا به نحو نامتعارفی دشوار باشد. در روابط داخلی، هر عامل باید متناسب با درجه تقصیر، میزان کنترل، انتفاع اقتصادی و قابلیت پیشگیری، حق رجوع یا مسئولیت نهایی داشته باشد. این الگو از تحمیل تمام خسارت به ضعیف‌ترین حلقه زنجیره، مانند کارمند، جلوگیری می‌کند.

در حوزه اثبات، داده‌های فنی مانند گزارش دسترسی، سوابق پرامپت، لاگ‌های سامانه، نسخه سیاست‌های امنیتی، گزارش ممیزی، قرارداد ارائه‌دهنده مدل، سوابق حذف و مستندات ارزیابی ریسک ادله اصلی دعاوی محرمانگی بوده که هرگاه نگهداری این ادله در اختیار متعهد یا ارائه‌دهنده سامانه باشد و وی بدون توجیه از ارائه یا حفظ آنها خودداری کند، دادگاه میتواند اماره‌ای به زیان او استنباط کند. همچنین دستور حفظ فوری ادله دیجیتال باید پیش از طرح یا در ابتدای دعوا قابل صدور باشد؛ زیرا حذف یا تغییر لاگ‌ها می‌تواند امکان اثبات را به‌کلی از بین ببرد.

در خصوص خسارت، اتکا به کاهش مستقیم سود یا اثبات فروش اطلاعات کافی نیست. نقض محرمانگی ممکن است موجب ازدست‌رفتن مزیت رقابتی، کاهش ارزش انحصاری اطلاعات، هزینه مهار حادثه، هزینه تحقیق فنی، هزینه بازآموزی مدل، کاهش اعتبار تجاری، محرومیت از فرصت قراردادی یا تحصیل منفعت نامشروع توسط ناقض شود؛ بنابراین، دادگاه باید بتواند خسارت را بر پایه مجموعه‌ای از معیارها، از جمله کاهش ارزش اطلاعات، هزینه ایجاد مجدد، منفعت تحصیل‌شده، حق امتیاز فرضی و هزینه‌های معقول پیشگیری و بازیابی تعیین کند. وجه التزام قراردادی نیز باید پذیرفته شود، مشروط بر آنکه به‌گونه‌ای تنظیم نشده باشد که ماهیت کیفری نامتناسب پیدا کند یا وسیله‌ای برای محدود کردن ناموجه آزادی شغلی باشد .ضمانت‌اجراها نیز نباید منحصر به پرداخت خسارت باشند. در بسیاری از موارد، توقف استفاده، منع انتقال، حذف نسخه‌های قابل شناسایی، بازگرداندن اسناد، محدودسازی دسترسی، اصلاح تنظیمات مدل، جداسازی مجموعه‌داده، تعلیق پردازش و نظارت مستقل، مؤثرتر از جبران مالی صرف‌اند. بااین‌حال، حذف یا از بین بردن کامل مدل نباید به‌صورت خودکار و در همه موارد اعمال شود. چنین اقدامی باید تابع امکان فنی، سهم داده نامشروع در مدل، شدت نقض، قابلیت جداسازی، آثار آن بر اشخاص ثالث، هزینه اجرا و اصل تناسب باشد.

اگر داده محرمانه نقش اساسی و غیر قابل تفکیکی در ایجاد مدل داشته و ادامه بهره‌برداری

موجب استمرار انتفاع نامشروع باشد، دادگاه باید بتواند حذف مجموعه‌داده، بازآموزی مدل، غیر قابل استفاده کردن نسخه آلوده یا توقف بهره‌برداری را مقرر کند. اما هرگاه داده مورد اختلاف سهم محدود و قابل حذف داشته باشد، نابودی کامل مدل ممکن است نامتناسب باشد. در این حالت، حذف هدفمند، بازآموزی، محدودسازی خروجی، حسابرسی مستقل یا پرداخت عوض منصفانه می‌تواند راه‌حل مناسب‌تری باشد .همچنین، تبدیل داده محرمانه به وزن‌ها یا پارامترهای مدل، به‌خودی‌خود نباید موجب ایجاد سهم مالکیت برای صاحب هر داده در کل مدل شود. چنین راه‌حلی از حیث اثبات میزان تأثیر، تعدد صاحبان داده و قابلیت تفکیک، با دشواری جدی روبه‌روست و ممکن است توسعه مدل‌ها را عملاً ناممکن سازد. راه‌حل متناسب‌تر آن است که در صورت استفاده غیرمجاز و مؤثر از اطلاعات محرمانه، حسب مورد حق توقف استفاده، حذف یا بازآموزی، مطالبه خسارت، استرداد منافع یا حق امتیاز فرضی برای دارنده اطلاعات شناسایی شود. ایجاد حق مالکیت مشترک تنها در مواردی قابل تصور است که مشارکت در تولید مدل یا خروجی بر پایه قرارداد، سرمایه‌گذاری مشترک یا آورده فنی قابل اندازه‌گیری اثبات شود.

در نهایت، حمایت مؤثر از محرمانگی در عصر هوش مصنوعی نه با منع مطلق گردش داده و نه با آزادی کامل پردازش آن محقق می‌شود. منع مطلق، پژوهش، نوآوری و بهره‌برداری مشروع از داده را مختل می‌کند و آزادی نامحدود نیز کنترل اشخاص بر سرمایه‌های اطلاعاتی را از میان می‌برد. راه‌حل مطلوب، استقرار نظامی مبتنی بر «استفاده مشروع، کنترل‌شده، متناسب و پاسخ‌گو» است؛ نظامی که در آن ارزش اقتصادی و محرمانه اطلاعات حمایت شود، اما این حمایت به پوششی برای انحصار ناموجه، محدودیت دائمی اشتغال، جلوگیری از گزارش تخلف، اخلال در رقابت یا ممانعت از پژوهش مشروع تبدیل نشود .براین‌اساس، پاسخ نهایی به پرسش پژوهش آن است که ظرفیت‌های موجود حقوق ایران برای حمایت اولیه از اطلاعات محرمانه قابل استفاده‌اند، اما برای مواجهه مؤثر با هوش مصنوعی کافی نیستند. کارآمدی این ظرفیت‌ها منوط به بازتعریف افشا بر مبنای ازدست‌رفتن کنترل مؤثر، شناسایی تعهد مراقبت دیجیتال مشدد، توزیع متناسب مسئولیت در زنجیره پردازش، تعدیل بار اثبات، توسعه ادله فنی، تنوع‌بخشی به ضمانت‌اجراها و تدوین قواعد اختصاصی برای استفاده از اطلاعات در سامانه‌های هوش مصنوعی است. تنها با تحقق هم‌زمان این اصلاحات می‌توان میان حمایت از اسرار تجاری، توسعه فناوری، آزادی شغلی، رقابت مشروع و منافع عمومی توازن پایدار و قابل اجرا برقرار کرد.

پیشنهادها

۱. پذیرش معیار «ازدست‌رفتن کنترل مؤثر» در کنار افشای بالفعل و شناسایی ورود اطلاعات به سامانه غیر قابل کنترل به‌عنوان قرینه نقض تعهد.

۲. شناسایی تعهد محرمانگی به‌عنوان تعهد مراقبت ویژه همراه با فرض تقصیر، نه مسئولیت

مطلق و نه تعهد ساده به وسیله.

۳. تنظیم الگوی ملی قرارداد محرمانگی و استفاده از هوش مصنوعی با تعیین دقیق اطلاعات، اهداف مجاز، سامانه‌های مجاز، دوره نگهداری، حذف، ممیزی، استفاده ثانویه و استثنائات قانونی.

۴. پیش‌بینی مسئولیت مستقل مدیران و سازمان‌ها در صورت فقدان سیاست استفاده از هوش مصنوعی، آموزش کارکنان یا نظارت بر انتقال داده به همراه شناسایی مسئولیت ارائه‌دهندگان مدل در صورت استفاده برخلاف توافق از داده‌ها، پنهان‌سازی خطرات، نگهداری غیرمجاز یا انتقال به اشخاص ثالث.

۵. پذیرش جابه‌جایی محدود بار اثبات در مواردی که اطلاعات فنی و ادله اصلی منحصراً در اختیار متعهد، پردازشگر یا ارائه‌دهنده سامانه است.

۶. بازنگری دوره‌ای سیاست‌های محرمانگی؛ زیرا معقول‌بودن اقدامات حفاظتی مفهومی ثابت نیست و باید متناسب با تحول فناوری و روش‌های بازشناسایی ارزیابی شود.

موضوع	راهکار
ماهیت حقوقی محرمانگی و مبنای حمایت	قانون‌گذار با شناسایی تعهد مراقبت ویژه و تعریف قلمرو پردازش مجاز و غیرمجاز، مبنای مستقلی برای حمایت از اطلاعات محرمانه در محیط‌های هوشمند ایجاد کند.
معیار شناسایی سر تجاری و اقدامات معقول	معیار قانونی «اقدامات معقول» بر پایه سطح خطر، ارزش اطلاعات، نوع سامانه هوش مصنوعی و هزینه متعارف پیشگیری تدوین شود.
معیار مسئولیت و تعهد مراقبت	تعهد مراقبتی مشدد به‌عنوان معیار ارزیابی تقصیر و مبنای مسئولیت قراردادی و مدنی در روابط مبتنی بر هوش مصنوعی پذیرفته شود.
جایگاه مفاهیم افشا و نشت الگوریتمی تصاحب و بازتولید غیرمجاز	مفهوم افشا به تصاحب، استفاده، استنتاج و بازتولید غیرمجاز داده‌ها توسعه یابد.
بار اثبات	اثبات نقض محرمانگی بدون دسترسی به ادله فنی برای زیان‌دیده دشوار است. در چنین مواردی با جابه‌جایی محدود بار اثبات و پذیرش امارات قضایی، تعادل اثبات برقرار شود.

اقدامات حفاظتی	در هر قراردادی ابتدا الزام به اجرای تدابیر فنی، سازمانی و قراردادی متناسب با سطح خطر پیش‌بینی شود.
ضمانت‌اجراها و استرداد الگوریتمی	خسارت مالی به‌تنهایی جبران‌کننده آثار نقض محرمانگی نیست. دادگاه اختیار صدور دستور حذف داده، بازآموزی مدل، توقف بهره‌برداری و استرداد الگوریتمی متناسب را دارد.
توازن میان عدم افشا و عدم رقابت	حمایت از محرمانگی نباید به ابزار محدودسازی رقابت یا اشتغال تبدیل شود.

فهرست منابع

۱. Allard, T., Béziaud, L., & Gambs, S. (2020). Online publication of court records: Circumventing the privacy–transparency trade-off.

۲. Alzoubi, Y. I., & Mishra, A. (2025). Differential privacy and artificial intelligence: Potentials, challenges, and future avenues. EURASIP Journal on Information Security, 2025, Article 18.

۳. Anderson, D. Q. (2019). Piercing the veil of confidentiality in mediation to ensure good faith participation: An untenable position? South African Law Journal, 136(4), 713–735.

۴. Ansari, B. (2023). Protection of trade secrets against unauthorized disclosure. Private Law Research, 11(41), 41–82. [In Persian]

۵. Arcidiacono, D. (2016). The Trade Secrets Directive in the international legal framework. European Parliamentary Research Service.

۶. Bakhtjoo, R., Karimi, A., Sadeghi, M., & Sarvaei, P. (2020). An analytical and practical examination of confidentiality agreements (non-disclosure agreements), with emphasis on the International Chamber of Commerce model contract. Journal of Commerce Research, 91, 168–188. [In Persian]

۷. Barzi, V., Gharibe, A., Saghiri, E., & Masoudi, N. (2023). Disclosure of electronic trade secrets under the competition laws of Iran and the European Union. Journal of New Technologies Law Studies, 1(2), 65–82. [In Persian]

۸. Bharati, R. K. (2024). AI and intellectual property: Legal frameworks and future directions. International Journal of Law, Justice and Jurisprudence, 4(2), 31–193.

۹. Brkan, M. (2023). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. International Data Privacy Law, 13(1), 1–17.

۱۰. Busuioc, M., Curtin, D., & Almada, M. (2023). Reclaiming transparency: Contesting the logics of secrecy within the AI Act. European Law Open, 2(1), 79–105.

۱۱. Chaisse, J. (2024). Arbitration in cross-border data protection disputes. Journal of International Dispute Settlement, 15, 534–551.

۱۲. Chamikara, M. A. P., Bertok, P., Liu, D., Camtepe, S., & Khalil, I. (2020). Efficient privacy preservation of big data for accurate data mining. Information Sciences, 527, 420–443.

۱۳. Coffey, K. (2023). Standing up to hackers: Article III standing for victims of data breaches. University of Miami Law Review, 77(2), 295–340.

۱۴. Crescioni, M., & Sklar, T. (2020). The research exemption carve out: Understanding research participants' rights under GDPR and U.S. data privacy laws. Jurimetrics Journal, 60(2), 125–138.

۱۵. Defend Trade Secrets Act of 2016, 18 U.S.C. §§ 1836–1839.

۱۶. De Noyette, E., Stähler, L., & Margoni, T. (2025). Data secrets: The Data Act's new trade secrets framework. International Review of Intellectual Property and Competition Law, 56, 984–1014.

۱۷. Desai, S. (2018). SHHH! It's a secret: A comparison of the United States Defend Trade Secrets Act and European Union Trade Secrets Directive.

۱۸. European Union Agency for Network and Information Security. (2014). Privacy and data protection by design: From policy to engineering.

۱۹. European Union. (2016). Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets). Official Journal of the European Union, L 157, 1–18.

۲۰. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88.

۲۱. European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). Official Journal of the European Union, L 277, 1–102.

۲۲. European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

۲۳. European Union Agency for Network and Information Security. (2014). Privacy and data protection by design: From policy to engineering. ENISA.

۲۴. Flowers, M. C. (2019). Facing the inevitable: The inevitable disclosure doctrine and the Defend Trade Secrets Act of 2016. Washington and Lee Law Review, 75(4), 2207–2250.

۲۵. Fox, B. (2020). Tripping over the EU Trade Secrets Directive: "Reasonable steps" to get back on track. Chicago-Kent Journal of Intellectual Property, 19(1).

۲۶. Garrison, M. J., Swink, D. R., & Wendt, J. T. (2024). A proposed framework for a federal inevitable disclosure doctrine under the Defend Trade Secrets Act. Buffalo Law Review, 72(1), 271–320.

۲۷. Ghaed, F., & Sharif, E. (2022). A brief study of personal data protection in the Iranian legal system and the European Union General Data Protection Regulation. Biannual Journal of New Technologies Law, 2(4), 21–61. [In Persian]

۲۸. Ghobooli Derafshan, S. M. M., Danesh Nari, H. R., & Saatchi, A. (2014). A comparative study of civil and criminal protection of trade secret rights in the legal systems of Iran and the United States. Encyclopedia of Economic Law, 20(4). [In Persian]

۲۹. Gikay, A. A. (2025). Trade secrecy in automated decisions: Against the myth of irreconcilability and the imposition of patents. Journal of Intellectual Property Law & Practice, 20(8), 552–561.

۳۰. Gryz, J., & Rojszczak, M. (2021). Black box algorithms and the rights of individuals: No easy solution to the "explainability" problem. Internet Policy Review, 10(2).

۳۱. Hacker, P., Cordes, J., & Rochon, J. (2023). Regulating gatekeeper AI and data: Transparency, access, and fairness under the DMA, the GDPR, and beyond.

۳۲. Heilig, L., Buyya, R., & Voß, S. (2017). Location-aware brokering for consumers in multi-cloud computing environments. Journal of Network and Computer Applications, 95, 79–93.

۳۳. Hrdy, C. A., & Seaman, C. B. (2024). Beyond trade secrecy: Confidentiality agreements that act like noncompetes. Yale Law Journal, 133(1), 45–110.

۳۴. Information Commissioner's Office. (2025). A guide to the data protection principles: UK GDPR guidance.

۳۵. International Chamber of Commerce. (2019). Protecting trade secrets: Recent EU and US reforms—Guidance for businesses; Recommendations for policymakers worldwide. ICC Publishing.

۳۶. Kesavan, E. (2024). A review on ethical and legal issues in artificial intelligence and data privacy. International Journal of Innovations in Science Engineering and Management, 3(4), 94–99.

۳۷. Ke, T. T., & Sudhir, K. (2022). Privacy rights and data security: GDPR and personal data markets. Yale School of Management Working Paper.

۳۸. Khatamifar, F., Ghanavati, J., & Azarbayjani, A. (2023). The principle of disclosure in the contractual process: A comparative study of European and Iranian legal instruments. Legal Studies in Digital Age, 4(1), 1–24. [In Persian]

۳۹. Krook, J., Winter, P., Downer, J., & Blockx, J. (2025). A systematic literature review of AI transparency laws in the EU and UK. AI and Ethics, 5(4), 4069–4090.

۴۰. Kwakye, M. (2022). Privacy-preserving data management using blockchains.

۴۱. Latifzadeh, M., Ghobooli Derafshan, S. M. M., Mohseni, S., & Abedi, M. (2023). Processing special categories of personal data under European Union law and its examination in the Iranian legal system. Information Processing and Management Research, 39(1), 157–199. [In Persian]

۴۲. Levine, D. S. (2023). Generative artificial intelligence and trade secrecy. Journal of Free Speech Law, 2(1), 45–78.

۴۳. Lucchi, N. (2025). Generative AI and copyright: Training, creation, regulation (PE 774.095). Policy Department for Justice, Civil Liberties and Institutional Affairs, European Parliament.

۴۴. Magesh, V., Surani, F., Dahl, M., Suzgun, M., Manning, C. D., & Ho, D. E. (2025). Hallucination-free? Assessing the reliability of leading AI legal research tools. Journal of Empirical Legal Studies.

۴۵. Majedi, M. (2016). The privacy policy permission diagram: Toward a unified view of privacy (Doctoral dissertation, University of Calgary).

۴۶. Michailidou, A.-V., Gounaris, A., Symeonides, M., & Trihinas, D. (2022). EQUALITY: Quality-

aware intensive analytics on the edge. Information Systems, 105, Article 101953.

۴۷. Mic, V., & Zezula, P. (2022). Data-dependent metric filtering. Information Systems, 108, Article 101980.

۴۸. Mishova, A. (2025, July 3). GDPR for machine learning: Data protection in AI development. GDPR Local Blog.

۴۹. Morek, R. (2013). Nihil silentio utilius: Confidentiality in mediation and its legal safeguards in the EU Member States. ERA Forum, 14, 421–435.

۵۰. Mylly, U.-M. (2023). Transparent AI? Navigating between rules on trade secrets and access to information. International Review of Intellectual Property and Competition Law, 54, 1013–1043.

۵۱. Nautsch, A., Jasserand, C., Kindt, E., Todisco, M., Trancoso, I., & Evans, N. (2019). The GDPR and speech data: Reflections of legal and technology communities, first steps towards a common understanding.

۵۲. Pelletier, D. (2019). New ICC report: Protecting trade secrets—Recent EU and US reforms. International Chamber of Commerce.

۵۳. Pina, E., Ramos, J., Jorge, H., Váz, P., Silva, J., Wanzeller, C., Abbasi, M., & Martins, P. (2022). Data privacy and ethical considerations in database management. Journal of Cybersecurity and Privacy, 2(4), 672–689.

۵۴. Rahmani, S., & Rezamim, M. (2024). Examination of criminal guarantees against the infringement of trade secrets and trademarks from the perspectives of Islamic jurisprudence, Iranian law, and French law. Journal of Jurisprudence, Law and Judicial Studies, 3(4), 26–46. [In Persian]

۵۵. Saatchi, A., & Teimouri Moghadam, F. (2025). An analysis of the legal status of the subject matter in information-based contracts. Journal of Legal Research, 28(3), 215–232. [In Persian]

۵۶. Sandeen, S. K., & Mylly, U.-M. (2020). Trade secrets and the right to information: A comparative analysis of EU and U.S. approaches to freedom of expression and whistleblowing. North Carolina Journal of Law & Technology, 21(3), 607–668.

۵۷. Shakeri, Z. (2016). A reconsideration of the limitations on the scope of trade secret rights: With an examination of defenses available to defendants in infringement proceedings. Private Law Research Quarterly, 15(1), 1–26. [In Persian]

۵۸. Shojaifar, A., & Fricker, S. A. (2020). SMEs' confidentiality concerns for security information sharing.

۵۹. Roberts, C. L. (2025). Algorithmic erasure in the shadow of statutes. Louisiana Law Review, 85(3), 955–980.

۶۰. Federal Trade Commission. (2021). In the Matter of Everalbum, Inc., FTC Matter No. 1923172. Federal Trade Commission.

۶۱. Federal Trade Commission. (2022). United States of America v. Kurbo, Inc., and WW International, Inc., FTC Matter No. 2023138. Federal Trade Commission.

۶۲. Federal Trade Commission. (2023). In the Matter of Ring LLC, FTC File No. 2023082. Federal Trade Commission.

۶۳. Thaler v. Vidal, 43 F.4th 1207 (Fed. Cir. 2022).

۶۴. TransUnion LLC v. Ramirez, 594 U.S. 413 (2021).

۶۵. Beijing Neu Cloud Oracle Science & Technology Co., Ltd. v. International Business Machines Corp., No. 22-3132 (2d Cir. 2024).

۶۶. Case C-203/22. (2025). Court of Justice of the European Union (Grand Chamber).

۶۷. The New York Times Company v. Microsoft Corp., No. 23-cv-11195 (S.D.N.Y. Apr. 4, 2025).

۶۸. Bartz v. Anthropic PBC, No. 3:24-cv-05417 (N.D. Cal. 2025).

۶۹. Veale, M., & Zuiderveen Borgesius, F. J. (2021). Demystifying the draft EU Artificial Intelligence Act. Computer Law & Security Review International, 22(4), 97–112.

۷۰. Zuiderveen Borgesius, F. J., & Steenbruggen, W. (2023). The right to communications confidentiality in Europe: Protecting privacy, freedom of expression, and trust.

پژوهش‌نامهٔ پردازش و مدیریت اطلاعات
x ۱۳ | دورهٔ xx | شمارهٔ x

The Scope and Effects of Confidentiality Obligations in the Protection of Trade Secrets in the Age of Artificial Intelligence: A Comparative Study of the Legal Systems of Iran, the European Union, and the United States

Author Information

Ali Saatchi
Ph.D. in Private Law
Assistant Professor, Faculty of Law and Political Science, Ferdowsi University of Mashhad, Mashhad,Iran.
Email: alisaatchi@um.ac.ir

Javad Fahimi Tabar
Ph.D. Candidate in Private Law, Ferdowsi University of Mashhad, Mashhad, Iran.
Email: fahimitabar.javad@gmail.com

Abstract:

Today, data have become the most valuable assets of businesses, and the obligation to preserve confidentiality plays a fundamental role in protecting these strategic resources. The emergence of generative artificial intelligence has created unprecedented challenges, including the input of sensitive information into large language models and the potential reproduction of confidential research data, thereby raising novel legal questions concerning the scope and nature of confidentiality obligations. This study aims to examine the scope and legal effects of the duty of confidentiality in protecting trade secrets in the age of artificial intelligence and to evaluate the capacity of the Iranian legal system through a comparative analysis with the legal frameworks of the European Union and the United States. The necessity of this research stems from the fact that the traditional doctrine, centered on the prohibition of direct disclosure, appears inadequate to address the risks posed by algorithmic data processing and the loss of effective control over confidential information. The study adopts a descriptive-analytical methodology with a comparative approach. Data were collected through library-based research from legislation and legal scholarship relating to the three legal systems and were analyzed using qualitative content analysis.The findings indicate that, under United States law, the continuation of trade secret protection is contingent upon demonstrating reasonable measures to preserve secrecy, and the submission of confidential information to uncontrollable AI platforms may result in the loss of legal protection. In contrast, the European Union regulates trade secret protection alongside data

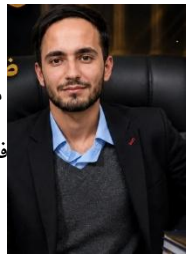
protection requirements, transparency, fundamental rights, competition policy, and the public interest. In Iran, despite the absence of a comprehensive legal framework, significant capacities exist through the principle of freedom of contract, the rules of civil liability, and Islamic jurisprudential concepts such as trust (amanah), negligence (tafrit), and wrongful destruction (itlaf). Nevertheless, the continued emphasis on the traditional notion of disclosure and the difficulties associated with proving unauthorized disclosure have undermined the effectiveness of legal protection. The study concludes that, in the era of artificial intelligence, the duty of confidentiality should be reconceptualized as a special duty of care, encompassing the adoption of appropriate technical and organizational safeguards. Furthermore, recognizing the loss of effective control over confidential information as a form of disclosure, adopting a limited shift in the burden of proof in favor of the injured party, and introducing concepts such as a digital duty of care would enhance the adaptability of the Iranian legal system to technological developments.

Keywords:

Commitment, confidentiality, non-disclosure, data, Trade Secrets, artificial intelligence

علی ساعتچی:

متولد سال ۱۳۶۸، دارای مدرک تحصیلی دکتری در رشته حقوق خصوصی از دانشگاه شهید بهشتی است. ایشان هم‌اکنون استادیار گروه حقوق خصوصی دانشگاه فردوسی مشهد است. حقوق مالکیت فکری، قراردادها و فناوری های نوین از جمله علایق پژوهشی وی است.



جواد فهیمی تبار:

متولد سال ۱۳۸۱؛ دانشجوی دکتری حقوق خصوصی دانشگاه فردوسی است حوزه های مختلف مرتبط با فناوری های نوین از قبیل هوش مصنوعی،ارزهای دیجیتال از جمله علایق پژوهشی وی است.