Jurisprudence and Legal Studies of Media Journal
VOL. 8 / Spring and Summer 2026 / NO. 1 (Serial 15)

Rethinking Data Rights in the Age of Artificial Intelligence: Challenges and Solutions for Privacy Protection in Modern Legal Systems

Hassan Masoudi[1] 0009-0003-8410-6573
Omid Adal[2] 0009-0007-5969-8852

Abstract
Rapid advancements in artificial intelligence technology have created novel challenges in personal data protection that existing legal frameworks struggle to address effectively. Using qualitative content analysis of scientific and legal documents published between 2018 and 2025, this research identifies and examines deficiencies in current legal systems when confronted with advanced AI capabilities. The findings reveal that challenges such as the "black box" problem of AI algorithms, conflict between data minimization principles and AI's need for extensive data, inefficiencies in informed consent mechanisms, gaps in regulatory coverage of foundation models, and lack of international regulatory harmonization are among the most significant shortcomings. This research proposes approaches for redefining key data rights concepts such as informed consent, the right to be forgotten, and transparency, while presenting a comprehensive framework consisting of fundamental principles, implementation mechanisms, and legal and technical solutions. The main innovation of this research is the introduction of a "distributed accountability" model that allocates responsibility among all actors in the AI ecosystem. This framework establishes a balanced approach to AI regulation by maintaining equilibrium between protecting fundamental individual rights and promoting innovation.

Key Words: Artificial Intelligence, Personal Data Protection, Data Rights, Informed Consent, Regulation, Privacy, Iran.

1- PhD in Culture and Communications from Islamic Azad University, Tehran Central Branch (corresponding author of the article) hadimasoudi1366@gmail.com
2- Master's degree in Private Law from Razavi University of Islamic Sciences, Mashhad, Iran omidadel1638@gmail.com

دوفصلنامه دوره ۸، شماره ۱(پیاپی ۱۵)
مطالعات فقه و حقوق رسانه بهار و تابستان ۱۴۰۵
دانشکده غیردولتی – غیرانتفاعی رفاه صص: ۳۳۵-۳۵۱

بازاندیشی حقوق داده‌ها در عصر هوش مصنوعی: چالش‌ها و راهکارهای حفاظت از حریم خصوصی در نظام‌های حقوقی ایران

نوع مقاله: ترویجی

حسن مسعودی[۱]
امید عادل[۲]

تاریخ دریافت: ۱۴۰۴/۰۴/۱۶
تاریخ پذیرش: ۱۴۰۴/۱۲/۰۳

چکیده

پیشرفت‌های شتابان در فناوری هوش مصنوعی، چالش‌های بی‌سابقه‌ای را در حوزه حفاظت از داده‌های شخصی پدید آورده و نظام‌های حقوقی موجود، به‌ویژه در ایران را با کاستی‌های بنیادین مواجه ساخته است. این پژوهش با روش توصیفی-تحلیلی و مبتنی بر مطالعه اسنادی، به تحلیل انتقادی این چالش‌ها و ارائه راهکار می‌پردازد. یافته‌های کلیدی پژوهش نشان می‌دهد که چالش‌هایی نظیر «مسئله جعبه سیاه»، تعارض میان اصل حداقل‌سازی داده‌ها با نیاز هوش مصنوعی به داده‌های انبوه، و ناکارآمدی مفهوم سنتی رضایت آگاهانه، چهارچوب‌های حقوقی فعلی را بی‌اثر ساخته‌اند. تحلیل نظام حقوقی ایران آشکار می‌سازد که قانون جرایم رایانه‌ای به‌دلیل رویکرد کیفری و فقدان مفاهیم حمایتی، فاقد ظرفیت لازم برای مواجهه با این تهدیدات نوین است. این مقاله در پاسخ به این خلأها، بر ضرورت بازتعریف مفاهیم بنیادین مانند «حق فراموش شدن» و «شفافیت» تأکید کرده و یک چهارچوب جامع حقوقی-فنی را پیشنهاد می‌کند. نوآوری اصلی این چهارچوب، ارائه «مدل مسئولیت‌پذیری توزیع‌شده» و تأکید بر ایجاد یک نهاد تنظیم‌گر مستقل است که با برقراری تعادل میان صیانت از حقوق بنیادین شهروندان و پیشبرد نوآوری فناورانه، مسیری متوازن برای تنظیم‌گری هوش مصنوعی در ایران ترسیم می‌نماید.

کلیدواژه‌ها

هوش مصنوعی، حفاظت از داده‌های شخصی، حقوق داده‌ها، حریم خصوصی، تنظیم‌گری، قانون جرایم رایانه‌ای، مسئولیت‌پذیری توزیع‌شده، ایران.

---

۱. دکتری فرهنگ و ارتباطات، دانشگاه آزاد تهران مرکز، تهران، ایران (نویسنده مسئول)
hadimasoudi1366@gmail.com
۲. کارشناسی ارشد حقوق خصوصی، دانشگاه علوم اسلامی رضوی، مشهد، ایران
omidadel1638@gmail.com

مقدمه

ظهور و پیشرفت شتابان فناوری هوش مصنوعی، نظام‌های حقوقی را در سراسر جهان با چالشی بنیادین مواجه ساخته و اصول تثبیت‌شده در حوزه حفاظت از داده‌های شخصی[۵] و حریم خصوصی[۶] را به بازاندیشی واداشته است. این فناوری برای تحقق کارکرد بهینه خود، به پردازش حجم عظیمی از داده‌های شخصی نیازمند است؛ امری که به‌خودی‌خود، تنشی ماهوی با اصول بنیادین حقوق داده‌ها، ازجمله اصل «حداقل‌سازی داده‌ها»، ایجاد می‌کند و می‌تواند حریم خصوصی افراد را به‌مثابه یکی از ارکان حقوق بنیادین بشر، به‌طور جدی تهدید نماید.

عدم تناسب چهارچوب‌های حقوقی موجود با پیچیدگی‌های فنی و حقوقی هوش مصنوعی، چالش اصلی این حوزه به‌شمار می‌رود. نظام‌های حقوقی کنونی که برای دوران پیشاهوش مصنوعی طراحی شده‌اند، در مواجهه با قابلیت‌های پیشرفته‌ای نظیر یادگیری عمیق و توانایی استنتاج و بازشناسی افراد حتی از داده‌های ناشناس‌سازی‌شده[۷]، فاقد کارآمدی لازم‌اند. یکی از مهم‌ترین معضلات در این زمینه، «مسئله جعبه سیاه»[۸] است که به‌دلیل ماهیت غیرقابل توضیح بسیاری از الگوریتم‌ها، پایبندی به اصل شفافیت[۹] و حق افراد برای دریافت توضیحات معنادار را تقریباً ناممکن می‌سازد و بدین‌ترتیب، حاکمیت قانون را در این عرصه به چالش می‌کشد (*Fritz, 2022, p. 213*). افزون براین، قوانین موجود مانند قانون هوش مصنوعی اتحادیه اروپا (*EU AI Act*) نیز دارای خلأهای مهمی هستند؛ برای نمونه، این قانون «کاربردهای خاص هوش مصنوعی را تنظیم می‌کند؛ اما مدل‌های پایه اصلی خود برنامه‌ها را پوشش نمی‌دهد» (*Ruschemeier, 2023, p. 369*). این شکاف قانونی، پیامدهای حقوقی جدی، به‌ویژه در زمینه پردازش داده‌های شخصی، به همراه دارد.

در کنار این موارد، مفاهیم سنتی حقوقی مانند رضایت آگاهانه[۱۰]، حق فراموش شدن[۱۱] و

5. Personal Data Protection
6. Privacy
7. Anonymised Data & Anonymous Information
8. Black Box Problem
9. Transparency
10. Informed Consent
11. Right to be Forgotten

شفافیت در پردازش داده‌ها، در مواجهه با پدیده‌هایی چون «خستگی رضایت»[۱۲] و رخ‌نماسازی‌های[۱۳] پیچیده، کارایی خود را از دست داده‌اند؛ برای‌مثال، در حوزه سلامت، جمع‌آوری گسترده داده‌ها توسط سیستم‌های اینترنت اشیاء بدون رضایت شفاف و معنادار کاربران، تهدیدی جدی برای حقوق بنیادین محسوب می‌شود (*Murdoch, 2021, p. 4*). ماهیت فرامرزی فناوری و عدم هماهنگی بین‌المللی قوانین نیز بر پیچیدگی این چالش‌ها افزوده و ضرورت تنظیم‌گری[۱۴] مؤثر و متوازن را بیش از پیش آشکار می‌سازد. ازاین‌رو، برخی صاحب‌نظران بر لزوم تقویت حقوق بشر با حقوق نوین، مانند حق عدم قرار گرفتن در معرض تصمیم‌گیری خودکار و حق تماس انسانی معنادار، تأکید دارند (*Amin et al, 2025, p. 4*).

در این پژوهش، منظور از «بازتعریف»، تطبیق و ارتقای مفاهیم سنتی حقوق داده‌ها با واقعیت‌های عصر هوش مصنوعی است. این بازتعریف با تمرکز بر نظام حقوقی ایران و با الهام از تجارب بین‌المللی، به‌دنبال ارائه راهکارهایی برای اصلاح و تدوین قوانین کارآمد است. با توجه به این پیچیدگی‌ها، پژوهش حاضر در پی پاسخ به این پرسش اساسی است: چگونه می‌توان چهارچوب حقوقی متوازنی برای حفاظت از داده‌های شخصی در برابر چالش‌های ناشی از فناوری‌های هوش مصنوعی تدوین کرد که ضمن تضمین حقوق بنیادین اشخاص، مانع نوآوری و توسعه فناوری نشود؟

۱. روش‌شناسی پژوهش

پژوهش حاضر با به‌کارگیری روش «توصیفی-تحلیلی» و با اتکا بر «مطالعه اسنادی» انجام شده است. ماهیت میان‌رشته‌ای موضوع که ابعاد حقوقی، فنی و اخلاقی حفاظت از داده‌های شخصی در عصر هوش مصنوعی را دربر می‌گیرد، ایجاب می‌کند که از رویکردی جامع برای بررسی مسئله استفاده شود. در بخش توصیفی، این پژوهش به شناسایی و تبیین چالش‌های نوظهور حقوقی ناشی از فناوری‌های هوش مصنوعی می‌پردازد. این امر از

---

۱۲. خستگی رضایت (Consent Fatigue) به پدیده‌ای اشاره دارد که در آن کاربران به‌دلیل مواجهه مکرر با درخواست‌های کسب رضایت برای پردازش داده‌هایشان، بدون درک کامل مفاد و شرایط، آن‌ها را می‌پذیرند.

13. Profiling

14. Regulation / Governance

طریق مطالعه و بررسی نظام‌مند اسناد حقوقی ملی و بین‌المللی، به‌ویژه «مقررات عمومی حفاظت از داده اتحادیه اروپا (*GDPR*)» به‌عنوان یک سند پیش‌رو و «قانون جرایم رایانه‌ای ایران (مصوب ۱۳۸۸)» و پیش‌نویس «لایحه حفاظت از داده‌های شخصی» به‌عنوان اسناد حقوقی مرتبط با نظام حقوقی ایران، صورت گرفته است. در بخش تحلیلی، پژوهش به نقد و ارزیابی کاستی‌ها و خلأهای موجود در این نظام‌های حقوقی در مواجهه با پیچیدگی‌های هوش مصنوعی می‌پردازد. دراین‌راستا، با تحلیل دکترین حقوقی و ادبیات علمی منتشرشده در این حوزه، مفاهیم بنیادین حقوق داده‌ها نظیر رضایت آگاهانه، حق فراموش شدن و شفافیت، مورد واکاوی قرار گرفته و ظرفیت آن‌ها برای انطباق با واقعیت‌های جدید سنجیده می‌شود. درنهایت، این پژوهش با ترکیب یافته‌های توصیفی و تحلیلی، به ارائه راهکارها و پیشنهاد یک چهارچوب حقوقی و نظارتی متوازن می‌پردازد که هدف آن برقراری تعادل میان صیانت از حقوق بنیادین افراد و پیشبرد نوآوری‌های فناورانه است.

۲. چالش‌های اصلی نظام‌های حقوقی در مواجهه با هوش مصنوعی

نظام‌های حقوقی موجود که عمدتاً بر پایه اصولی سنتی بنا نهاده شده‌اند، در مواجهه با قابلیت‌های پیشرفته و ماهیت دگرگون‌ساز هوش مصنوعی با کاستی‌های بنیادین و چالش‌های پیچیده‌ای روبه‌رو هستند. این چالش‌ها از نقص‌های ذاتی در فناوری تا گسست‌های عمیق در چهارچوب‌های قانونی را دربر می‌گیرند و ریشه در سرعت تحولات فناورانه دارند.

یکی از اساسی‌ترین معضلات حقوقی، چالش «جعبه سیاه»[۱۵] است. این پدیده به وضعیتی

---

۱۵. ریشه چالش «جعبه سیاه» در معماری خود مدل‌های هوش مصنوعی، به‌ویژه شبکه‌های عصبی عمیق، نهفته است. در این سیستم‌ها، منطق تصمیم‌گیری نه بر اساس قوانین صریح و قابل‌فهم برای انسان بلکه به‌صورت الگوهای ریاضی پیچیده در میان میلیون‌ها یا میلیاردها مؤلفه توزیع شده است. این امر تضاد بنیادینی با مدل‌های کلاسیک یادگیری ماشین دارد که در آن‌ها مسیر رسیدن به نتیجه قابل ردیابی بود. درنتیجه، یک گسست اساسی میان ماهیت «احتمالاتی» و «همبستگی‌محور» هوش مصنوعی با ماهیت «علیّت‌محور» و «مبتنی بر دلیل» نظام‌های حقوقی و اخلاقی به‌وجود می‌آید. سیستم حقوقی برای پاسخگویی

اشاره دارد که در آن فرایندهای تصمیم‌گیری و استدلال الگوریتم‌های پیچیده، به‌ویژه شبکه‌های عصبی عمیق، حتی برای طراحانشان نیز غیرقابل تفسیر و توضیح باقی می‌ماند *(Hacker, 2023, p. 108)*. این عدم شفافیت، اصول بنیادین حقوقی مانند «اصل پاسخگویی»[۱۶] و «حق بر توضیح»[۱۷] را که در قوانین مترقی مانند *GDPR* نیز به‌رسمیت شناخته شده، به‌طور مستقیم به چالش می‌کشد و عملاً اجرای آن‌ها را ناممکن می‌سازد. زمانی که نتوان فرایندهای یک سیستم را تحلیل و حسابرسی کرد، تعیین مسئولیت[۱۸] در موارد نقض حقوق یا بروز خسارت، امری بسیار دشوار خواهد بود و راه را برای به چالش کشیدن تصمیمات الگوریتمی مسدود می‌کند *(Ploug, 2023, p. 18)*. این امر شکافی عمیق در مسئولیت‌پذیری ایجاد می‌کند؛ زیرا معیارهای سنتی اثبات تخلف در این زمینه فاقد کارآمدی لازم هستند.

افزون‌براین، تنشی ماهوی میان اصول تثبیت‌شده حقوق داده‌ها و الزامات فنی هوش مصنوعی به چشم می‌خورد. «اصل حداقل‌سازی داده‌ها»[۱۹] که پردازش داده‌های شخصی را به حداقلِ ضروری برای یک هدف مشخص محدود می‌سازد، در تضادی آشکار با نیاز ذاتی سیستم‌های هوش مصنوعی به حجم انبوهی از داده‌ها برای دستیابی به دقت و کارایی قرار دارد. این تعارض، به‌ویژه در حوزه‌هایی مانند سلامت که مجموعه داده‌های گسترده‌تر به

به‌دنبال «چرا» می‌گردد، درحالی‌که جعبه سیاه تنها می‌تواند «چه» را (یعنی خروجی نهایی) بر اساس الگوهای آماری که آموخته، ارائه دهد و این تضاد، هسته اصلی چالش برای حاکمیت قانون در عصر الگوریتم‌هاست. مراجعه شود به: https://jme.bmj.com/content/48/4/213

16. Accountability

۱۷. در حقوق بین‌الملل، به‌ویژه در چهارچوب مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR)، معادل دقیق برای حق بر توضیح یا Right to an Explanation یکی از ارکان کلیدی حقوق داده‌ها در عصر هوش مصنوعی محسوب می‌شود و به‌طور خاص در زمینه تصمیم‌گیری خودکار (Automated Decision-Making) کاربرد دارد. بر اساس GDPR، هرگاه یک تصمیم که آثار حقوقی یا شخصی مهمی برای فرد دارد، صرفاً بر اساس پردازش خودکار (مانند الگوریتم‌های هوش مصنوعی) اتخاذ شود، فرد حق دارد «اطلاعات معناداری در مورد منطق به‌کار رفته» (meaningful information about the logic involved) در آن تصمیم را دریافت کند. مراجعه شود به: راهنمای دفتر کمیسر اطلاعات (ICO) در مورد GDPR پیوند: ICO - Rights related to automated decision-making and profiling

18. Civil Liability

19. Data Minimization Principle

نتایج دقیق‌تر و منافع عمومی منجر می‌شود، چهارچوب‌های حقوقی را در یافتن نقطه تعادل با چالش جدی مواجه ساخته است (*Murdoch, 2021, p. 4*). به‌همین‌ترتیب، «اصل رضایت آگاهانه»[۲۰]، به‌عنوان سنگ‌بنای مشروعیت پردازش داده‌ها، در بستر هوش مصنوعی کارایی خود را از دست داده است. پدیده‌هایی چون «خستگی رضایت»، «تجمیع اهداف» و «پارادوکس حریم خصوصی»، سازوکارهای سنتی رضایت را بی‌اثر ساخته و مشروعیت سپردن افراد به پروفایل‌سازی‌های پیچیده را زیر سؤال برده است (*Hacker et al., 2024, p. 73*). این چالش‌ها با ظهور فناوری‌هایی مانند اینترنت اشیاء که داده‌های حساس را بدون جلب رضایت شفاف و معنادار جمع‌آوری می‌کنند، تشدید نیز شده است (*Amin et al., 2025, p. 4*).

همزمان، یک گسست قانونی مهم در زمینه نظارت بر «مدل‌های پایه»[۲۱] هوش مصنوعی وجود دارد که زیربنای بسیاری از کاربردهای نوین را تشکیل می‌دهند. قوانین موجود، مانند قانون هوش مصنوعی اتحادیه اروپا، عمدتاً بر «کاربردهای خاص» تمرکز دارند و خودِ مدل‌های پایه را به میزان کافی پوشش نمی‌دهند؛ این خلأ نظارتی خطر انتشار سوگیری‌ها و تبعیض‌های الگوریتمی را در طیف گسترده‌ای از خدمات افزایش می‌دهد (*Ruschemeier, 2023, p. 369*). این مشکل با رشد سریع مدل‌های زبانی بزرگ (*LLMs*) که در «مناطق خاکستری تنظیمی»[۲۲] عمل می‌کنند، اهمیتی دوچندان یافته است. ضعف دیگر نظام‌های حقوقی در حفاظت از داده‌های بیومتریک[۲۳] و حساس آشکار می‌شود. توانایی هوش مصنوعی در پردازش حالات چهره، تن صدا و سایر داده‌های فیزیولوژیک، امکان دستکاری‌های رفتاری و روانی را فراهم می‌آورد، درحالی‌که قوانین فعلی فاقد سازوکارهای کافی برای مقابله با چنین سوءاستفاده‌هایی هستند (*Laulhé Shaelou & Razmetaeva, 2024, p. 575*). علاوه‌براین،

20. Informed Consent
21. Foundation Models
۲۲. مناطق خاکستری تنظیمی یا Regulatory Grey/Gray Areas، به وضعیتی اطلاق می‌شود که یک فناوری، فعالیت یا مدل کسب‌وکار جدید (در این مورد، مدل‌های زبانی بزرگ هوش مصنوعی) ظهور می‌کند؛ اما قوانین و مقررات موجود به‌طور واضح آن را پوشش نمی‌دهند. درواقع، این فناوری در یک خلأ قانونی عمل می‌کند که نه به‌صراحت مجاز است و نه ممنوع.
23. Biometric Data

الگوریتم‌های پیشرفته قادرند افراد را حتی از داده‌های به ظاهر ناشناس‌سازی‌شده نیز مجدداً شناسایی کنند، امری که اثربخشی روش‌های سنتی حفاظت از داده را به کلی به چالش می‌کشد (*Murdoch, 2021, p. 4*).

درنهایت، ماهیت ذاتاً جهانی و فرامرزی فناوری هوش مصنوعی، چالش «عدم هماهنگی بین‌المللی قوانین» را به یک مانع اساسی تبدیل کرده است. تفاوت‌های عمیق در رویکردهای تنظیمی مناطق مختلف جهان، از اتحادیه اروپا گرفته تا ایالات متحده، موجب پیچیدگی در عملیات سازمان‌های بین‌المللی شده و سطح حفاظت از داده‌ها را در نقاط مختلف جهان ناهماهنگ می‌سازد (*Cath, 2018, p. 4*). ابهامات موجود در طبقه‌بندی خدمات مبتنی بر هوش مصنوعی در چهارچوب‌های تجارت جهانی و تأثیرات فراسرزمینی قوانینی مانند *GDPR*، این ناهماهنگی را تشدید می‌کند و بدون وجود استانداردهای مشترک، تضمین سطحی یکسان از حفاظت برای همه شهروندان جهانی ناممکن به نظر می‌رسد (*Soprana, 2025, p. 716; Gasser, 2023, p. 1203*). این وضعیت، ضرورت تلاش‌های چندجانبه برای توسعه چهارچوب‌های هماهنگ را بیش‌ازپیش نمایان می‌سازد.

۳. وضعیت حقوقی ایران و مطالعه تطبیقی

نظام حقوقی ایران، به سبب اتکا بر ساختارهای سنتی، در مواجهه با چالش‌های نوظهور و پیچیده‌ی ناشی از هوش مصنوعی، با خلأها و کاستی‌های بنیادین روبه‌رو است. تحلیل انتقادی قوانین موجود و مقایسه آن با رویکردهای پیش‌روی بین‌المللی، نشان‌دهنده نیازی فوری به بازنگری و تدوین چهارچوب‌های حقوقی متناسب با این عصر نوین است. این بخش به تحلیل این وضعیت با اتکا بر دیدگاه‌های حقوق‌دانان داخلی و تجارب بین‌المللی می‌پردازد.

۳-۱. تحلیل انتقادی قانون جرایم رایانه‌ای: ناکارآمدی در عصر هوش مصنوعی

قانون جرایم رایانه‌ای (مصوب ۱۳۸۸) به‌عنوان اصلی‌ترین سند قانونی ایران در حوزه فضای دیجیتال، دارای رویکردی ذاتاً کیفری و واکنشی است و بر جرایمی نظیر دسترسی غیرمجاز، شنود، و تخریب داده‌ها تمرکز دارد. این قانون که برای مقابله با تهدیدات دوران

پیشاهوش مصنوعی طراحی شده، فاقد ظرفیت لازم برای مواجهه با چالش‌های نوین حفاظت از داده‌هاست و این ناکارآمدی در چند بُعد کلیدی قابل تحلیل است:

اولاً، فقدان رویکرد جامع و حمایتی: تمرکز انحصاری قانون بر جرم‌انگاری، آن را از پرداختن به حقوق بنیادین داده‌ای شهروندان بازداشته است. در نظام حقوقی ایران، مفاهیم نوینی چون «حق دسترسی به داده‌های شخصی»، «حق اصلاح» یا «حق حذف داده‌ها» معادل «حق فراموش شدن» در *GDPR* به صورت مدون و فراگیر به‌رسمیت شناخته نشده‌اند. این خلأ به آن معناست که شهروندان در عمل فاقد ابزار قانونی مؤثر برای کنترل داده‌های خود هستند و نمی‌توانند پردازش‌گران داده را به پاسخگویی وادارند. این قانون تنها به برخی جنبه‌های نقض حریم خصوصی پرداخته و پوشش کاملی بر نحوه استفاده از داده‌ها توسط سکوها(پلتفرم‌ها) ندارد؛ امری که در مواجهه با آسیب‌های غیرکیفری اما جدی ناشی از هوش مصنوعی، یک ضعف اساسی محسوب می‌شود (*جهانبخش هرندی، ۱۴۰۳*).

ثانیاً، ناتوانی در پوشش مدل‌های نوین پردازش داده: این قانون در برابر پیچیدگی‌های فنی هوش مصنوعی کاملاً ساکت است. پدیده‌هایی مانند رخ‌نماسازی خودکار، تصمیم‌گیری‌های کاملاً الگوریتمی که می‌تواند سرنوشت حقوقی و مالی افراد را تعیین کند، و پردازش داده‌ها توسط الگوریتم‌های «جعبه سیاه» که ماهیت غیرقابل توضیح دارند (*Fritz, 2022: 213*) ، در زمان تدوین این قانون ناشناخته بوده‌اند. درنتیجه، هیچ چهارچوب مشخصی برای تنظیم‌گری این فناوری‌ها و تعیین مسئولیت ناشی از آن‌ها وجود ندارد و این امر به ایجاد «مناطق خاکستری قانونی» منجر شده است. همین نقیصه بر ضرورت «اقدام حقوقی و تقنینی متناسب» برای صیانت از حریم خصوصی در این حوزه تأکید ورزند (*میرشکاری و دیگران،۱۴۰۳، ص. ۸۴*).

ثالثاً، نابسندگی مفهوم سنتی رضایت: قانون جرایم رایانه‌ای، رضایت را به شیوه‌ای سنتی و یک‌باره در نظر می‌گیرد و از درک چالش‌های نوینی چون «خستگی رضایت» یا «پارادوکس حریم خصوصی» که مشروعیت رضایت‌نامه‌های امروزی را زیر سؤال برده‌اند، عاجز است (*Hacker et al., 2024, p. 73*). این در حالی است که در عصر هوش مصنوعی، رضایت باید به‌معنای توانایی کاربر برای اعمال نظارت مستمر و پویا بر

داده‌هایش تعریف شود.

۳-۲. لایحه حفاظت از داده‌های شخصی: گامی رو به جلو با چالش‌های پیش‌رو

لایحه در دست بررسی «حفاظت از داده‌های شخصی»[۲۴] گامی مثبت برای پر کردن خلأهای موجود و اقتباس از مفاهیم قوانینی مانند *GDPR* است. بااین‌حال، موفقیت این لایحه در گروی عبور از چالش‌های مهمی است:

نخست آنکه، مفاد این لایحه باید به‌گونه‌ای «آینده‌نگر» و «مبتنی بر اصول» تدوین شود که در برابر سرعت سرسام‌آور تحولات هوش مصنوعی به‌سرعت منسوخ نگردد. چالش‌دیگر، پوشش دادن «مدل‌های پایه» است؛ همان‌طور که در نقد قانون هوش مصنوعی اروپا مشخص می‌شود، عدم نظارت بر این مدل‌های زیربنایی می‌تواند به انتشار گسترده سوگیری‌ها و تبعیض‌های الگوریتمی منجر شود. لایحه ایران باید از این تجربه درس گرفته و سازوکاری برای نظارت بر این مدل‌ها فراهم آورد *(Ruschemeier, 2023, p. 369)*.

اما مهم‌ترین چالش، خلأ نهادی است. موفقیت هر قانونی در این حوزه به وجود یک نهاد ناظر مستقل، متخصص و توانمند بستگی دارد. چنان‌که در تحلیل زیست‌بوم‌سازان هوش مصنوعی ایران، «خلأ نهاد راهبری و نهاد حکمرانی داده» یکی از موانع اصلی است. بدون چنین نهادی با اختیارات اجرایی کافی، بهترین قوانین نیز بر روی کاغذ باقی خواهند ماند

---

۲۴. لایحه «حفاظت از داده‌های شخصی» در ایران پس از سال‌ها تأخیر، در تاریخ ۲۴ تیر ۱۴۰۳ (۱۴ ژوئیه ۲۰۲۴) توسط هیئت دولت تصویب و به مجلس شورای اسلامی ارسال شد. این لایحه که برای نخستین‌بار در سال ۱۳۹۷ توسط وزارت ارتباطات ارائه شده بود، پس از تصویب در کمیسیون حقوقی دولت در اردیبهشت ۱۴۰۳، مسئولیت‌های شفافی برای نهادهای دولتی، کسب‌وکارها و اشخاص حقیقی و حقوقی در جمع‌آوری، پردازش و ذخیره‌سازی داده‌های شخصی کاربران تعیین می‌کند. طبق آخرین گزارش‌ها، این لایحه در تاریخ ۱۵ تیر ۱۴۰۳ در مجلس اعلام وصول شده و هم‌اکنون در کمیسیون‌های مجلس، به‌ویژه کمیسیون قضائی و حقوقی، در حال بررسی است و هنوز به تصویب نهایی نرسیده است. مراجعه شود به: مرکز پژوهش‌های مجلس، «طرح حفاظت از داده‌های شخصی»، تاریخ اعلام وصول: ۱۵/۰۷/۱۴۰۳، در: https://rc.majlis.ir/fa/legal_draft/show/1816729 و «لایحه حفاظت از داده‌های شخصی در کمیسیون حقوقی دولت تصویب شد»، ۱۵ اردیبهشت ۱۴۰۳، در: https://dolat.ir/detail/447326

(کنعانی و دیگران، ۱٤۰۲، ص. ۷۵).

۳-۳. مطالعه تطبیقی با *GDPR*: آشکارسازی خلأهای نظام حقوقی ایران

مقررات عمومی حفاظت از داده‌های اروپا (*GDPR*) به‌عنوان یک استاندارد مهم، معیار مناسبی برای سنجش کاستی‌های نظام حقوقی ایران است. این مقایسه نشان می‌دهد که ایران در چند حوزه کلیدی فاقد چهارچوب‌های نوین است:

- **رویکرد مبتنی بر ریسک**[۲۵]: *GDPR* با اتخاذ این رویکرد، تعهدات را متناسب با سطح خطر پردازش داده‌ها تعیین می‌کند و بدین‌ترتیب میان نوآوری و حفاظت، تعادل برقرار می‌سازد. نظام حقوقی ایران فاقد چنین رویکرد منعطفی است (*Gasser, 2023, p. 1203*).
- **حقوق داده‌ای گسترده**: *GDPR* مجموعه‌ای از حقوق بنیادین مانند حق فراموش شدن، حق انتقال داده‌ها و حق اعتراض به تصمیم‌گیری‌های کاملاً خودکار را برای افراد به‌رسمیت می‌شناسد. این حقوق، که ابزارهای عملی شهروندان برای کنترل بر حیات دیجیتال خود هستند، در نظام حقوقی ایران غایب‌اند.
- **شفافیت و توضیح‌پذیری**[۲۶]: *GDPR* بر حق دریافت توضیحات معنادار در مورد تصمیمات الگوریتمی تأکید دارد؛ حقی که اجرای آن با توجه به چالش «جعبه سیاه» (*Fritz, 2022, p. 213*) نیازمند راهکارهای نوینی مانند «توضیحات قابل اقدام» است (*Hacker et al., 2024, pp. 81-82*).
- **اصل پاسخگویی** *GDPR*: سازمان‌ها را ملزم می‌کند نه‌تنها قوانین را رعایت کنند بلکه توانایی اثبات این انطباق را نیز داشته باشند. این اصل که از طریق الزاماتی مانند تعیین «افسر حفاظت از داده‌ها» (*DPO*) و انجام «ارزیابی تأثیر بر حفاظت از داده‌ها»[۲۷] (*DPIA*) محقق می‌شود، سنگ‌بنای حاکمیت شرکتی مسئولانه است و می‌تواند الگوی مناسبی برای ایران باشد.

---

25. Risk-Based Approach
26. Explainability
27. Data Protection Impact Assessment (DPIA)

۳-۴. پیشنهادات اصلاحی برای نظام حقوقی ایران

با توجه به تحلیل انتقادی فوق، انطباق نظام حقوقی ایران با الزامات عصر هوش مصنوعی مستلزم اقداماتی بنیادین است:

۱. **تصویب قانون جامع حفاظت از داده‌ها**: این قانون باید فراتر از یک اقتباس صرف از *GDPR*، با بومی‌سازی لازم، تعاریف گسترده از داده‌های شخصی (شامل داده‌های استنتاجی[۲۸] و بیومتریک) و حقوق داده‌ای نوین را به‌رسمیت بشناسد و سازوکارهایی برای چالش‌های خاص هوش مصنوعی در نظر بگیرد.

۲. **ایجاد نهاد تنظیم‌گر[۲۹] مستقل و مقتدر**: تأسیس یک نهاد ملی متمرکز با تخصص فنی و حقوقی که مسئولیت تدوین استانداردها، نظارت و اعمال قانون را بر عهده گیرد، یک ضرورت انکارناپذیر است. این نهاد باید با اتخاذ رویکرد «تلفیق نظارت»، از پراکندگی مسئولیت‌ها جلوگیری کند (*Judge et al., 2024, p. 8*).

۳. **بازنگری در مفاهیم کلیدی**: مفاهیمی چون «رضایت آگاهانه» باید به یک فرایند پویا و مستمر تبدیل شود (*Hacker et al., 2024, pp. 73-74*) و «حق فراموش شدن» به «حق تأثیرگذاری بر ردپای دیجیتال» تکامل یابد (*Laulhé Shaelou & Razmetaeva, 2024, p. 582*).

٤. **پذیرش الگوی مسئولیت‌پذیری توزیع‌شده**[۳۰]: قوانین باید مسئولیت را به‌صورت مشترک میان توسعه‌دهندگان، استفاده‌کنندگان و تنظیم‌گران توزیع کنند تا با پیچیدگی اکوسیستم هوش مصنوعی مقابله شود (*Amin et al., 2025, p. 16*).

٥. **تدوین قوانین خاص بخشی**: علاوه بر چهارچوب عمومی، تدوین مقررات اختصاصی برای حوزه‌های پرخطری مانند سلامت، خدمات مالی و تبلیغات هدفمند، ضروری است (جهانبخش هرندی، ۱٤۰۳).

---

28. Inferred Data رخ‌نماسازی
29. Regulatory Body / Supervisory Authority
30. Distributed Accountability

۴. ارائه چهارچوب جامع حقوقی-فنی برای تنظیم‌گری هوش مصنوعی

تحلیل انتقادی نظام حقوقی ایران و مقایسه آن با چالش‌های جهانی نشان داد که چهارچوب‌های موجود برای حفاظت از داده‌های شخصی در عصر هوش مصنوعی ناکافی هستند. برای رفع این خلأها و حرکت به‌سوی یک نظام حقوقی کارآمد، ارائه یک چهارچوب جامع که مبانی نظری حقوق داده‌ها را بازتعریف کرده و الزامات اجرایی متناسب با آن را طراحی کند، ضروری است. این چهارچوب پیشنهادی بر دو ستون اصلی استوار است: بازاندیشی در مبانی نظری حقوق داده‌ها و طراحی الگوی تنظیم‌گری و الزامات اجرایی.

۴-۱. بازاندیشی در مبانی نظری حقوق داده‌ها: پایه‌های مفهومی چهارچوب نوین

پیش از پرداختن به ساختارهای قانونی، باید مفاهیم بنیادینی را که اساس حفاظت از داده‌ها را تشکیل می‌دهند، با واقعیت‌های عصر هوش مصنوعی منطبق ساخت. این بازاندیشی نظری، پاسخی مستقیم به نابسندگی مفاهیم سنتی در قوانین فعلی ایران است.

الف) تحول در مفهوم «رضایت آگاهانه»: همان‌طور که تحلیل شد، مفهوم سنتی رضایت در قانون جرایم رایانه‌ای ایران در برابر پدیده‌هایی چون «خستگی رضایت» فاقد کارایی است. برای رفع این نقیصه، رضایت آگاهانه باید از یک عمل یک‌باره به فرایندی مستمر و پویا تبدیل شود. این رویکرد نوین به کاربر امکان بازبینی، اصلاح و لغو رضایت را در طول زمان می‌دهد و نیازمند پیاده‌سازی سیستم‌های شفاف‌سازی دینامیک است تا نظارت مستمر فرد بر داده‌هایش را تضمین کند. استفاده از مدل‌هایی مانند «رضایت تدریجی» یا سیستم «چراغ راهنمایی» برای طبقه‌بندی ریسک پردازش داده‌ها، می‌تواند به تحقق رضایت معنادار کمک کند.

ب) گسترش «حق فراموش شدن» به «حق تأثیرگذاری بر ردپای دیجیتال»: نظام حقوقی ایران فاقد معادل مدون و کارآمدی برای حق فراموش شدن است. در عصر هوش مصنوعی، صرفاً حذف داده‌ها کافی نیست؛ زیرا اثرهای داده‌ها ممکن است در مدل‌های آموزش‌دیده باقی بماند. ازاین‌رو، این مفهوم باید به «حق تأثیرگذاری بر ردپای دیجیتال خود» گسترش یابد. این حق به افراد امکان مشارکت فعال در شکل‌دهی به بازنمایی دیجیتال

خود را می‌دهد و فرایندی پویاتر از حذف ایستای داده‌هاست. پشتیبانی از این حق مستلزم توسعه راهکارهای فنی نوینی مانند «یادگیری فراموشی»[۳۱] است که به سیستم‌ها امکان حذف مؤثر ردپای داده‌ها را می‌دهد.

ج) بازتعریف «شفافیت» به «توضیحات قابل اقدام»: چالش «جعبه سیاه» که در نظام حقوقی ایران هیچ پاسخی برای آن وجود ندارد ، شفافیت سنتی را بی‌معنا کرده است. به‌جای تمرکز بر جزئیات فنی غیرقابل فهم، شفافیت باید به سمت ارائه «توضیحات قابل‌اقدام»[۳۲] حرکت کند. این توضیحات باید متناسب با مخاطب (کاربر نهایی، نهاد ناظر و...) طراحی شوند و به افراد کمک کنند تا بر اساس اطلاعات دریافتی، تصمیمات معناداری اتخاذ نمایند. رویکردهایی مانند «توضیحات متقابل»[۳۳] که نشان می‌دهند چه تغییری در ورودی‌ها می‌توانست به نتیجه متفاوتی منجر شود، نمونه‌ای عملی از این شفافیت نوین هستند.

۴-۲. طراحی الگوی تنظیم‌گری و الزامات اجرایی

بر پایه این مبانی نظری بازتعریف‌شده، می‌توان یک الگوی تنظیم‌گری جامع طراحی کرد که خلأهای قانونی و نهادی ایران را به‌صورت مستقیم هدف قرار دهد.

الف) اصول بنیادین تنظیم‌گری:

۱. **رویکرد مبتنی بر ریسک**[۳۴]: به‌جای اعمال قواعد یکسان برای همه سیستم‌ها، این رویکرد که در لایحه حفاظت از داده‌های ایران نیز باید لحاظ شود، سیستم‌های هوش مصنوعی را بر اساس سطح ریسک آن‌ها طبقه‌بندی کرده و تعهدات متناسب با آن تعیین می‌کند. این الگو، ضمن حفاظت از حقوق افراد در کاربردهای پرخطر، از ایجاد موانع غیرضروری برای نوآوری جلوگیری می‌نماید و می‌تواند تعادل مورد نیاز در نظام حقوقی ایران را برقرار سازد (*Gasser, 2023, p. 1203*).

۲. **الگوی مسئولیت‌پذیری توزیع‌شده**: پیچیدگی اکوسیستم هوش مصنوعی ایجاب می‌کند که مسئولیت صرفاً بر دوش یک بازیگر نباشد. این الگو، مسئولیت را به‌صورت

31. Machine Unlearning
32. Actionable Explanations
33. Counterfactual Explanations
34. Risk-Based Approach

مشترک میان توسعه‌دهندگان، استفاده‌کنندگان و تنظیم‌گران توزیع می‌کند. این رویکرد، پاسخی به ابهامات مسئولیت در قوانین فعلی ایران است و ایجاب می‌کند که توسعه‌دهندگان مدل‌های پایه، استفاده‌کنندگان سیستم‌های پرخطر و کاربران نهایی، هر یک تعهدات مشخصی داشته باشند.

۳. **نظارت انسانی معنادار**[۳۵]: برای جلوگیری از تبعات تصمیم‌گیری‌های کاملاً خودکار، باید بر حفظ کنترل و نظارت انسانی، به‌ویژه در حوزه‌های پرخطر تأکید کرد. این اصل که در قوانین ایران مغفول مانده، باید با به‌رسمیت شناختن حقوقی نوین مانند «حق تماس انسانی معنادار» و «حق عدم قرار گرفتن در معرض تصمیم‌گیری کاملاً خودکار» تقویت شود.

ب) ساختار نهادی و سازوکارهای اجرایی:

۱. **ایجاد نهاد تنظیم‌گر مستقل و مقتدر**: این مهم‌ترین گام برای رفع «خلأ نهادی» است که حقوق‌دانان ایرانی نیز بر آن تأکید کرده‌اند. تأسیس یک نهاد ملی متمرکز با تخصص فنی و حقوقی که مسئولیت تدوین استانداردها، نظارت و اعمال قانون را بر عهده گیرد، یک ضرورت انکارناپذیر است. این نهاد باید با اتخاذ رویکرد «تلفیق نظارت»، از پراکندگی مسئولیت‌ها جلوگیری کند (*Judge et al., 2024, p. 8*).

۲. **فرایندهای تأیید و حسابرسی**: برای سیستم‌های پرخطر، باید فرایندهای ارزیابی اجباری مانند «ارزیابی تأثیر بر حقوق بنیادین» (*FRIA*) پیش از استقرار سیستم تعریف شود. همچنین، حسابرسی مستقل الگوریتمی توسط نهادهای ثالث باید الزامی گردد تا انطباق با استانداردها تضمین شود.

۳. **سازوکارهای مؤثر جبران خسارت**[۳۶]: برای حمایت از شهروندان، باید یک رژیم مسئولیت ترکیبی شامل مسئولیت محض برای سیستم‌های پرخطر و معکوس کردن بار اثبات در موارد خاص پیش‌بینی شود. تأسیس یک صندوق جبران خسارت نیز می‌تواند در مواردی که تعیین مسئولیت دشوار است، راهگشا باشد.

---

35. Meaningful Human Oversight
36. Remedy / Compensation for Damages

ج) راهکارهای حقوقی و فنی تکمیلی:

برای تکمیل این چهارچوب، مجموعه‌ای از اصلاحات قانونی و ابزارهای فنی باید به‌کار گرفته شوند.

- **اصلاحات قانونی مشخص**: قوانین آتی ایران باید شامل گسترش تعریف داده‌های شخصی برای پوشش دادن داده‌های استنتاجی و بیومتریک ، به‌رسمیت شناختن حق عدم رخ‌نماسازی و تدوین قوانین خاص بخشی برای حوزه‌های حساسی مانند سلامت و خدمات مالی باشد.
- **به‌کارگیری راهکارهای فنی مبتنی بر حریم خصوصی**: در کنار قوانین، باید از فناوری‌های حافظ حریم خصوصی[۳۷] حمایت کرد. فناوری‌هایی نظیر حریم خصوصی تفاضلی[۳۸]، رمزنگاری هومومورفیک[۳۹] و یادگیری فدراتیو[۴۰] می‌توانند پردازش داده‌ها را بدون به خطر انداختن حریم خصوصی افراد ممکن سازند و باید به‌عنوان بخشی از الزامات «حفاظت حریم خصوصی به کمک طراحی»[۴۱] در نظر گرفته شوند.

نتیجه‌گیری

این پژوهش استدلال نمود که ظهور هوش مصنوعی صرفاً یک چالش فنی برای نظام‌های حقوقی نیست بلکه یک نقطه عطف تاریخی است که بازاندیشی بنیادین در فلسفه حقوق داده‌ها را الزامی می‌سازد. یافته‌های پژوهش نشان داد که چهارچوب‌های حقوقی سنتی، ازجمله در نظام حقوقی ایران، به‌دلیل اتکا بر مفاهیم ایستا و رویکردهای واکنشی، توانایی مقابله با ماهیت پویا، پیچیده و پیش‌بینی‌ناپذیر این فناوری را ندارند. مشکل صرفاً وجود چند خلأ قانونی نیست بلکه گسستی عمیق میان الگوواره‌های حقوقی موجود و واقعیت‌های فناورانه جدید وجود دارد.

اهمیت و دلالت اصلی این یافته‌ها آن است که راهکار، در اصلاحات جزئی یا افزودن چند

37. Privacy-Enhancing Technologies
38. Differential Privacy
39. Homomorphic Encryption
40. Federated Learning
41. Privacy by Design

ماده به قوانین پیشین خلاصه نمی‌شود. همان‌طور که تحلیل شد، ناکارآمدی قانون جرایم رایانه‌ای ایران ریشه در فقدان یک رویکرد حمایتی و آینده‌نگر دارد و تا زمانی که مفاهیمی چون رضایت آگاهانه، حق فراموش شدن و شفافیت متناسب با عصر هوش مصنوعی بازتعریف نشوند، هرگونه اصلاحی سطحی و موقتی خواهد بود. چهارچوب جامعی که در این مقاله ارائه شد، فراتر از مجموعه‌ای از قوانین، یک الگوی حکمرانی نوین را پیشنهاد می‌کند که در آن، مسئولیت به‌صورت توزیع‌شده میان تمام بازیگران اکوسیستم تعریف شده و بر ایجاد یک نهاد تنظیم‌گر مستقل و توانمند به‌عنوان ستون فقرات اجرایی تأکید می‌گردد.

درنهایت، این پژوهش نشان داد که حفاظت مؤثر از داده‌های شخصی در عصر هوش مصنوعی، مستلزم گذار از یک رویکرد صرفاً حقوقی به یک رویکرد یکپارچه حقوقی-فنی است. تلفیق راهکارهای قانونی با ابزارهای فنی حافظ حریم خصوصی (مانند یادگیری فراموشی و حریم خصوصی تفاضلی) نه یک انتخاب بلکه یک ضرورت است. این چهارچوب پیشنهادی، با هدف ارائه مدلی بومی و متوازن برای نظام حقوقی ایران، می‌کوشد تا نشان دهد که می‌توان ضمن پذیرش نوآوری‌های فناورانه، از حقوق بنیادین شهروندان نیز به شیوه‌ای مؤثر و پایدار صیانت کرد؛ چالشی که بدون‌شک، تعریف‌کننده مسیر تحول نظام‌های حقوقی در دهه‌های آینده خواهد بود.

منابع

جهانبخش هرندی، زهرا (۱٤۰۳). چالش‌های حقوقی و نوآوری در حفاظت از حریم خصوصی در بستر رسانه‌های دیجیتال با تمرکز بر تبلیغات هدفمند و هوش مصنوعی. *مجموعه مقالات سیزدهمین کنفرانس بین‌المللی و ملی مطالعات مدیریت، حسابداری و حقوق*.

کنعانی، فاطمه؛ رسولیان، پریسا؛ حافظی، رضا و آهنگری، سعیده‌السادات (۱٤۰۲). تحلیل بوم‌سازگان هوش مصنوعی ایران و شناسایی خلأهای نهادی و کارکردی آن. *سیاست علم و فناوری*، ۱٦(۲)، ۵۹-۷۷.

میرشکاری، عباس؛ ثابت‌قدم، فاطمه و اصغرنیا، مرتضی (۱٤۰۳). درآمدی بر چالش‌های فناوری هوش مصنوعی در حوزه حریم خصوصی. *مطالعات حقوقی فضای مجازی*، ۳(٤)، ۷۱-۸۹.

Amin, M. A. S., Kim, S., Rishat, M. A. S. A., Tang, Z & ,.Ahn, H. (2025). A Systematic

Literature Review of Privacy Information Disclosure in AI-Integrated Internet of Things (IoT) Technologies .*Sustainability, 8, (1) 17*.

Cath, C. (2018). Governing artificial intelligence: ethical, legal and technical opportunities and challenges .*Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 20180080,(2133)376*.

Fritz, Z. (2022). When the frameworks don't work: data protection, trust and artificial intelligence .*Journal of Medical Ethics, 48(4), 213-214.*

Gasser, U. (2023). An EU landmark for AI governance .*Science, 1203, (6651), 380.*

Hacker, P. (2023). The European AI liability directives – Critique of a half-hearted approach and lessons for the future .*Computer Law & Security Review, 51, 105871*.

Hacker, P., Cordes, J & ,.Rochon, J. (2024). Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond .*European Journal of Risk Regulation, 15, 49-86*.

Judge, B., Nitzberg, M & ,.Russell, S. (2024). When code isn't law: rethinking regulation for artificial intelligence .*Policy and Society, 00(00), 1-13.*

Laulhé Shaelou, S & ,.Razmetaeva, Y. (2024). Challenges to Fundamental Human Rights in the age of Artificial Intelligence Systems: shaping the digital legal order while upholding Rule of Law principles and European values .*ERA Forum, 24, 567-587.*

Murdoch, B. (2021). Privacy and artificial intelligence: challenges for protecting health information in a new era .*BMC Medical Ethics, 22(1), 122.*

Ploug, T. (2023). The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling .*Philosophy & Technology, 36(14), 1-22*.

Ruschemeier, H. (2023). AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal .*ERA Forum, 23, 361-376*.

Soprana, M. (2025). Compatibility of emerging AI regulation with GATS and TBT: the EU Artificial Intelligence Act .*Journal of International Economic Law, 27(4), 706-722.*