Jurisprudence and Legal Studies of Media Journal
VOL. 8 / Autumn 2026 and Winter 2027 / NO. 2 (Serial 16)

Children and Artificial Intelligence: Regulating Recommender Algorithms with a Comparative Approach

Mohammad Hajali[1] 0000-0003-0917-9249
Zahra Hoseinpour [2] 0009-0002-2211-6613

Abstract

Digital transformation has shifted the nature of risks facing children from content-related harm to algorithmic harm, challenging traditional legal frameworks. Focusing on "Recommender Algorithms" within digital platforms, this research demonstrates how these systems, driven by the attention economy and behavioral engineering, target children's mental health and endanger the fundamental objective of Sharia, namely the "protection of the intellect" (Hifz al-Aql). The paper argues that the Iranian legal system possesses dynamic jurisprudential capacities to confront this phenomenon. Drawing on the views of Imami jurists regarding the maxim of "Tasbib" (causation), the platform is identified as the "stronger cause" due to cognitive manipulation and structural deception (Ghurur). Furthermore, applying the preventive function of the "La Darar" (no harm) maxim imposes a positive duty on platforms. Ultimately, through a comparative study of pioneering legislation (notably the EU Digital Services Act and the UK Online Safety Act), this research proposes a forward-looking framework for Iran centered on the "Algorithmic Duty of Care" and the procedural mandate of "Algorithmic Impact Assessment for Children," shifting the supervisory paradigm from reactive responses to proactive prevention.

Keywords: Children's Rights, Artificial intelligence, Recommender Algorithms, Attention Economy, Algorithmic Duty of Care, Algorithmic Impact Assessment.

1- PhD Graduate in Technology Management, University of Tehran, Tehran, Iran
(corresponding author of the article) m.hajali@ut.ac.ir
2- Master's Graduate in Family Law, Refah Non-Profit College, Tehran, Iran
sh_hoseinpour@outlook.com

دوفصلنامه
مطالعات فقه و حقوق رسانه
دانشکده غیردولتی – غیرانتفاعی رفاه

دوره ۸، شماره ۲ (پیاپی ۱۶)
پاییز و زمستان ۱۴۰۵
صص: ۲۷۳-۳۰۰

کودکان و هوش مصنوعی: تنظیم‌گری «الگوریتم‌های توصیه‌گر» با رویکرد تطبیقی

DOI: 10.22034/jlsm.2026.2072599.1052

نوع مقاله: پژوهشی

تاریخ دریافت: ۱۴۰۴/۰۷/۰۳ **تاریخ بازنگری:** ۱۴۰۵/۰۲/۱۷ **تاریخ پذیرش:** ۱۴۰۵/۰۵/۰۴

محمد حاجعلی[۱] زهرا حسین‌پور[۲]

چکیده

تحول دیجیتال، ماهیت مخاطرات پیش‌روی کودکان را از آسیب‌های محتوایی به آسیب‌های الگوریتمی تغییر داده است؛ الگووارهای که چهارچوب‌های حقوقی سنتی را به چالش می‌کشد. این پژوهش با تمرکز بر «الگوریتم‌های توصیه‌گر» در سکو(پلتفرم)های دیجیتال، نشان می‌دهد که چگونه این سیستم‌ها با اتکا به اقتصاد توجه و مهندسی رفتار، سلامت روان کودکان را هدف قرار داده و مقصد بنیادین شریعت یعنی «حفظ العقل» را به مخاطره می‌اندازند. مقاله استدلال می‌کند که نظام حقوقی ایران با اتکا به ظرفیت‌های پویای فقهی توان مواجهه با این پدیده را دارد. با ارجاع به آرای فقهای امامیه در قاعده «تسبیب»، سکو به دلیل دستکاری شناختی و فریب ساختاری (غرور)، «سبب اقوی از مباشر» شناخته می‌شود. همچنین، با کاربست کارکرد حکومتی و پیشگیرانه قاعده «لاضرر»، تکلیفی ایجابی بر سکوها بار می‌گردد. درنهایت، این پژوهش با مطالعه تطبیقی قوانین پیشرو (به‌ویژه قانون خدمات دیجیتال اروپا و قانون ایمنی برخط بریتانیا)، یک چهارچوب آینده‌نگر برای ایران پیشنهاد می‌دهد که بر مفهوم «وظیفه مراقبت الگوریتمی» و الزام رویه‌ای به «ارزیابی تأثیر الگوریتمی بر کودک» استوار است تا نظارت از واکنشی پسینی به پیشگیری فعالانه ارتقا یابد.

واژگان کلیدی

حقوق کودک، هوش مصنوعی، الگوریتم توصیه‌گر، اقتصاد توجه، وظیفه مراقبت الگوریتمی، ارزیابی تأثیر الگوریتمی.

---

۱. دانش‌آموخته دکتری تخصصی مدیریت تکنولوژی، دانشگاه تهران، تهران، ایران (نویسنده مسئول)
m.hajali@ut.ac.ir

۲. دانش‌آموخته کارشناسی ارشد حقوق خانواده، دانشکده غیرانتفاعی رفاه، تهران، ایران
sh_hoseinpour@outlook.com

۱- مقدمه: گذار الگوواره‌ای از مخاطرات محتوا به مخاطرات الگوریتمی

بر اساس آخرین آمارها، نوجوانان به‌طور متوسط روزانه نزدیک به پنج ساعت از وقت خود را در شبکه‌های اجتماعی سپری می‌کنند و قریب به نیمی از آنها گزارش می‌دهند که تقریباً به‌طور مداوم برخط هستند (*Gallup, 2023*). این آمار نه‌تنها نشان‌دهنده یک تحول در سبک زندگی، بلکه بیانگر یک دگرگونی بنیادین در معماری شناختی و اجتماعی دوران رشد است. درحالی‌که نسل‌های پیشین سیاست‌گذاری حقوقی بر حفاظت از کودکان در برابر مخاطراتی ملموس و قابل شناسایی متمرکز بودند، ظهور هوش مصنوعی ماهیت، مقیاس و سازوکار آسیب را به‌طور بنیادین دگرگون کرده است. این تحول، چالشی عمیق برای چهارچوب‌های حقوقی سنتی و به‌ویژه اهداف بنیادین شریعت (مقاصد الشریعه) ایجاد کرده است؛ اهدافی که غایت نهایی نظام حقوقی اسلام یعنی حفظ دین، نفس، عقل، نسل، مال و عرض (آبرو) را تشکیل می‌دهند *(عودة، ۱٤۳۲ق)*. آسیب‌های نوظهور الگوریتمی، این مقاصد ضروری را به شیوه‌هایی بی‌سابقه هدف قرار می‌دهند؛ به‌ویژه الگوریتم‌های توصیه‌گر که با مهندسی رفتار، دستکاری شناختی و ترویج اعتیاد دیجیتال، مقصد کلیدی «حفظ العقل» را تضعیف می‌کنند *(غلامی، ۱٤۰۱؛ Habib, 2025)*.

این گذار صرفاً یک تغییر فناورانه نیست بلکه همان‌طور که نظریه‌پردازانی چون گیلسپی اشاره کرده‌اند، نوعی بازتوزیع قدرت از تولیدکنندگان محتوا به معماران سیستم است (*Gillespie, 2014*). در الگوواره قدیم (عصر رسانه‌های جمعی)، قدرت دروازه‌بانی در دست کسی بود که محتوا را تولید یا منتشر می‌کرد؛ اما در الگوواره جدید (عصر سکوها)، این قدرت به لایه زیرساختی منتقل شده و در دست کسی است که «الگوریتم‌های توزیع و اولویت‌بندی» را طراحی می‌کند. پدیده‌ای که ناپولی از آن به‌عنوان گذار به «دروازه‌بانی الگوریتمی» یاد می‌کند (*Napoli, 2015*). این تغییر بنیادین، کانون مسئولیت حقوقی را نیز از ناشر به طراح سیستم منتقل می‌سازد و نیازمند ابزارهای حقوقی متناسب با این معماری نوین قدرت است. قوانین موجود که عمدتاً «قاعده‌محور»[5] هستند و بر ممنوعیت مصادیق مشخصی از محتوا تمرکز دارند، در برابر فناوری‌های نوظهور که به‌سرعت تکامل می‌یابند، کارایی خود را از دست می‌دهند (*Carter*

5. Rules–based

& Marchant, 2011). ازاین‌رو، مواجهه مؤثر با این چالش‌ها مستلزم گذار به یک رویکرد «اصل‌محور»[6] است؛ رویکردی که با تعریف اصول و اهداف سطح بالا، قادر به انطباق با تحولات آینده بوده و به اصطلاح «آینده‌پژوهانه»[7] است (*Carter & Marchant, 2011; Ojanen, 2025*). این پژوهش استدلال می‌کند که تعریف یک «وظیفه مراقبت الگوریتمی» به‌عنوان یک اصل حقوقی، هسته اصلی چنین رویکردی را تشکیل می‌دهد.

برای درک عمق این تحول، می‌توان مخاطرات برخط برای کودکان را در سه نسل متوالی طبقه‌بندی کرد. نسل اول که الگوواره حاکم بر دهه‌های گذشته بود، بر مخاطرات محتوایی تمرکز داشت. در این نگاه، خطر اصلی، مواجهه منفعلانه کودک با محتوای مضر، مستهجن یا خشونت‌آمیز بود. پاسخ حقوقی نیز متناسب با این تعریف، بر ابزارهایی مانند فیلترینگ، رده‌بندی سنی و جرم‌انگاری تولید و انتشار محتوای غیرقانونی استوار بود (*Kids Online Health and Safety Task Force, 2024*).

نسل دوم مخاطرات با تعاملی شدن وب ظهور کرد و کانون توجه را به مخاطرات معماری‌محور منتقل ساخت. در این الگوواره، آسیب صرفاً از محتوای منفرد نشئت نمی‌گرفت بلکه از خودِ طراحی سکوها، مانند ویژگی‌های اعتیادآور[8]، الگوهای تاریک[9] و سازوکارهای تقویت‌کننده تعاملات مضر (مانند قلدری سایبری) ناشی می‌شد. در پاسخ، نظام‌های حقوقی پیشرو به سمت الگوواره «مسئولیت‌پذیری سکو» و تحمیل «وظیفه مراقبت» برای طراحی‌های ایمن حرکت کردند.

اکنون، ما در آستانه نسل سوم مخاطرات قرار داریم: آسیب‌های الگوریتمی. این نسل جدید از تهدیدات که توسط سیستم‌های هوش مصنوعی هدایت می‌شود، دارای سه ویژگی متمایز است: فعالانه، شخصی‌سازی‌شده و غیرشفاف. برخلاف نسل‌های پیشین، در اینجا آسیب دیگر یک محصول جانبی یا یک انتخاب کاربر نیست بلکه محصول مستقیم عملکرد یک سیستم خودکار است که برای بهینه‌سازی اهداف تجاری (مانند حداکثرسازی تعامل) طراحی شده و در این فرایند، به‌طور نظام‌مند آسیب‌های روانی و رشدی تولید می‌کند (*Campbell,*

6. Principles–based
7. Future–proof
8. infinite scroll
9. dark patterns

2025). الگوریتم‌های توصیه‌گر، با شناسایی نقاط ضعف شناختی، محتوای افراطی و اعتیادآور را به نوجوانی آسیب‌پذیر پیشنهاد می‌دهند و چرخه‌ای از وابستگی ایجاد می‌کنند.

۲- طرح مسئله و پرسش اصلی پژوهش

مسئله اصلی این است که چهارچوب‌های حقوقی موجود که برای مقابله با مخاطرات نسل اول و دوم طراحی شده‌اند، در برابر این نسل سوم از تهدیدات الگوریتمی دچار نارسایی و عدم کفایت هستند. ناکارآمدی رویکردهای نسل اول (مانند فیلترینگ کلیدواژه‌ای) در برابر هوش مصنوعی ناشی از ماهیت «ایستا»ی قوانین در برابر ماهیت «پویا»ی الگوریتم است. فیلترینگ سنتی بر مسدودسازی «مصادیق مشخص» (مانند یک *URL* یا کلمه خاص) استوار است؛ درحالی‌که سیستم‌های هوش مصنوعی مولد و توصیه‌گر، محتوا را به‌صورت لحظه‌ای و شخصی‌سازی‌شده تولید یا بازآرایی می‌کنند. یک الگوریتم می‌تواند هزاران نسخه متفاوت از یک محتوای مضر را در ثانیه تولید کند که با هیچ فهرست سیاهی قابل تطبیق نیست؛ بنابراین، نظارت باید از «کنترل خروجی» به «نظارت بر فرایند» تغییر یابد *(غمامی، ۱۴۰۳)*. همچنین، مفاهیم سنتی مسئولیت مدنی مانند «تقصیر» و «رابطه سببیت» در مواجهه با الگوریتم‌های «جعبه-سیاه» که فرایندهای تصمیم‌گیری آن‌ها برای انسان قابل درک نیست، با چالش‌های اثباتی جدی روبه‌رو می‌شوند.

علاوه‌براین، ماهیت آسیب‌های الگوریتمی، سازوکارهای سنتی جبران خسارت پسینی را نیز به چالش می‌کشد. این آسیب‌ها اغلب ماهیتی جمعی، گسترده و پراکنده دارند؛ به این معنا که آسیب‌های روانی یا مالی کوچک به میلیون‌ها نفر وارد می‌شود که پیگیری انفرادی آن‌ها از طریق نظام دادرسی سنتی، به دلیل دشواری اثبات سببیت و غیرمقرون‌به‌صرفه بودن، عملاً غیرممکن است (*Ausloos et al., 2022*). این وضعیت، ضرورت طراحی سازوکارهای «جبران خسارت جمعی» یا «دعوای گروهی» را آشکار می‌سازد (*Lu, 2024*). ناکارآمدی نظام جبرانی فعلی در ارائه راه‌حل مؤثر برای این نوع آسیب‌های نوظهور، خود یکی از قوی‌ترین استدلال‌ها به نفع تغییر الگوواره به سمت تنظیم‌گری پیشگیرانه و سیستمی است که این مقاله از آن دفاع می‌کند.

نظام حقوقی ایران نیز از این قاعده مستثنی نیست. تمرکز غالب قوانین بر کنترل محتوا و جرم‌انگاری‌های پسینی، سپر حمایتی مؤثری در برابر آسیب‌های پیشگیرانه و ساختاری هوش مصنوعی فراهم نمی‌آورد. این وضعیت، این پرسش بنیادین را مطرح می‌سازد: چهارچوب‌های حقوقی چگونه می‌توانند بدون سرکوب نوآوری، از کودکان در برابر آسیب‌های ناشی از الگوریتم‌های غیرشفاف، محتوای تولیدشده توسط هوش مصنوعی و رخ‌نما(پروفایل)سازی رفتاری محافظت کنند؟

اگرچه مخاطرات هوش مصنوعی دامن‌گیر بزرگسالان نیز می‌شود؛ اما تمرکز این پژوهش بر کودکان به دلیل وجود یک «عدم تقارن رشدی و حقوقی» است. از منظر عصب‌شناختی، مغز کودکان و نوجوانان هنوز در حال توسعه است؛ سیستم لیمبیک (مرکز پاداش و هیجان) فعال است؛ اما قشر پیش‌پیشانی (مرکز کنترل تکانه و تصمیم‌گیری منطقی) تا اواسط دهه سوم زندگی کامل نمی‌شود (*Arain et al., 2013*). این ویژگی زیستی، کودکان را در برابر سازوکارهای «اقتصاد توجه» و الگوریتم‌های اعتیادآور، به‌مراتب آسیب‌پذیرتر از بزرگسالان می‌سازد. از منظر حقوقی نیز، کودکان به دلیل عدم اهلیت کامل (محجوریت)، توانایی «رضایت آگاهانه» واقعی در برابر پردازش داده‌های پیچیده را ندارند *(رضایی و همکاران، ۱۴۰۳)*؛ بنابراین، استانداردهای «انسان متعارف» که در حقوق مسئولیت مدنی برای بزرگسالان به کار می‌رود، برای حفاظت از این گروه کافی نیست و نیازمند یک رژیم حمایتی سخت‌گیرانه‌تر است.

این پژوهش برای ارائه الگوی تنظیم‌گری بومی، از روش مطالعه تطبیقی با رویکرد «مسئله‌محور» بهره برده است. انتخاب حوزه‌های قضائی مورد مطالعه (اتحادیه اروپا، بریتانیا و ایالات متحده) بر اساس معیار «تنوع در مدل‌های تنظیم‌گری» صورت گرفته است تا طیف کاملی از راه‌حل‌ها بررسی شود. اتحادیه اروپا به‌عنوان نماینده مدل «قانون‌گذاری جامع و ریسک‌محور» که تلاش دارد با تصویب «قانون هوش مصنوعی» یک استاندارد جهانی ایجاد کند، انتخاب شده است (*European Union, 2024*). درمقابل، بریتانیا به‌عنوان نماینده مدل «مسئولیت‌پذیری پلتفرمی» و «وظیفه مراقبت» که تمرکز آن بر ایمنی در طراحی است (*UK Parliament, 2023*) و ایالات متحده آمریکا به‌عنوان نماینده مدل «مبتنی بر بازار و

پاسخگویی» که بر شفافیت و ارزیابی تأثیر تمرکز دارد، مورد بررسی قرار گرفته است. مقایسه این سه رویکرد متفاوت با ظرفیت‌های فقهی و حقوقی ایران (به‌ویژه قواعد مسئولیت مدنی)، امکان ارائه یک مدل ترکیبی و بومی را فراهم می‌آورد. همچنین در تحلیل چالش‌های حقوقی، از منابع جدید داخلی در حوزه حکمرانی داده‌محور و مسئولیت سکوها *(زوالقدر، ۱۴۰۳؛ کرمدار، ۱۴۰۳)* بهره گرفته شده است تا انطباق‌پذیری مدل پیشنهادی با نظام حقوقی ایران تضمین گردد.

در ادامه مقاله، سازوکار فنی و چالش‌های حقوقی الگوریتم‌های توصیه‌گر کالبدشکافی می‌شود. سپس مقاله به بررسی پاسخ‌های تنظیم‌گرانه در نظام‌های حقوقی پیشرو، به‌ویژه اتحادیه اروپا، بریتانیا و ایالات متحده آمریکا، می‌پردازد. پس از آن با نگاهی به درون، ظرفیت‌های نظام حقوقی ایران، به‌ویژه قانون مدنی، را برای بومی‌سازی یک چهارچوب حمایتی ارزیابی می‌کند. درنهایت نیز، با تلفیق یافته‌های تحلیلی و تطبیقی، یک مدل تنظیم‌گرانه آینده‌نگر برای ایران پیشنهاد می‌دهد که بر مفهوم «وظیفه مراقبت الگوریتمی» و یک سازوکار رویه‌ای مشخص استوار است.

۳- کالبدشکافی مخاطرات نوظهور: سازوکار فنی و حقوقی «الگوریتم‌های توصیه‌گر»

برای طراحی یک چهارچوب حقوقی مؤثر، ابتدا باید ماهیت فنی و حقوقی تهدیدات جدید را به دقت درک کرد. این بخش به تحلیل سازوکار الگوریتم‌های توصیه‌گر می‌پردازد که کودکان را به شیوه‌هایی نوین و پیچیده هدف قرار می‌دهند.

ضروری است تمایز دقیق میان مفاهیم کلیدی این پژوهش شامل سکو، الگوریتم و هوش مصنوعی پیش از ورود به تحلیل مخاطرات، تبیین گردد تا از خلط مباحث جلوگیری شود. «سکوی برخط»[10] بستری دیجیتال است که تعامل میان کاربران و محتوا را تسهیل می‌کند و نقش واسطه‌گری دارد. «الگوریتم»[11] مجموعه‌ای از دستورالعمل‌های ریاضی است که برای حل یک مسئله یا انجام یک وظیفه خاص (مانند رتبه‌بندی محتوا) در دل سکو تعبیه

10. Online Platform
11. Algorithm

می‌شود. اما «هوش مصنوعی»[۱۲] به سیستم‌هایی اطلاق می‌شود که قادرند با تحلیل داده‌ها، یادگیری و استنتاج، اهدافی را محقق کنند که پیش‌تر نیازمند هوش انسانی بود. در این پژوهش، تمرکز بر آن دسته از سیستم‌های هوش مصنوعی (مانند الگوریتم‌های توصیه‌گر پیشرفته) است که به‌صورت خودمختار بر تجربه و امنیت کودکان تأثیر می‌گذارند.

الگوریتم‌های توصیه‌گر، موتور محرک سکوهای نوین هستند. این سیستم‌ها با تحلیل رفتار گذشته کاربر، محتوایی را که احتمالاً برای او جذاب است، پیش‌بینی و پیشنهاد می‌کنند. هرچند این فناوری می‌تواند به کشف محتوای مفید کمک کند؛ اما مدل کسب‌وکار مبتنی بر «اقتصاد توجه» آن را به یک ابزار قدرتمند برای مهندسی رفتار و بهره‌کشی از آسیب‌پذیری‌های روانی، به‌ویژه در کودکان و نوجوانان، تبدیل کرده است (*Kohl, 2024*).

این آسیب‌پذیری روانی، ریشه‌ای عصب‌شناختی دارد. مغز نوجوان با یک عدم تقارن رشدی مشخص می‌شود: سیستم لیمبیک که مسئول پردازش هیجانات و پاداش است، به بلوغ کامل رسیده و به محرک‌های اجتماعی (مانند تأیید همسالان) بسیار حساس است؛ درحالی‌که قشر پیش‌پیشانی که مسئول کنترل تکانه، تفکر بلندمدت و تصمیم‌گیری منطقی است، هنوز در حال توسعه بوده و تا اواسط دهه سوم زندگی به بلوغ کامل نمی‌رسد (*Arain et al., 2013*). عملکرد الگوریتم‌های توصیه‌گر فراتر از بازتاب ساده علایق کاربر است. این سیستم‌ها بر مبنای توابع هدف طراحی شده‌اند که اولویت اصلی آن‌ها «حداکثرسازی زمان حضور کاربر» و «نرخ تعامل» است. از منظر فنی، الگوریتم با ایجاد «حلقه‌های بازخورد»، نه‌تنها علایق فعلی کودک را شناسایی می‌کند بلکه با پیشنهاد محتوای هیجانی‌تر، ذائقه او را به سمت موضوعاتی سوق می‌دهد که بیشترین واکنش عصبی را ایجاد کنند (کرمدار، ۱۴۰۳). تفاوت این فرایند با انتخاب آزادانه در این است که سیستم با بهره‌گیری از ضعف سیستم پاداش مغزی در نوجوانان (دوپامین‌محور بودن)، قدرت انتخاب ارادی را کاهش می‌دهد *(Galván, 2010)* و چرخه‌ای از وابستگی رفتاری ایجاد می‌کنند که می‌تواند به اضطراب، افسردگی و کاهش کیفیت زندگی منجر شود *(جوادی و همکاران، ۱۴۰۳)*؛ بنابراین، چالش اصلی نه در «نمایش علایق» بلکه در «تقویت افراطی» است که می‌تواند یک علاقه

12. Artificial Intelligence

ساده را به یک وسواس رفتاری یا اعتیاد دیجیتال تبدیل کند.

سازوکار اصلی این سیستم‌ها، تقویت الگوریتمی[۱۳] است؛ فرایندی که در آن محتوای هیجان‌انگیز، تفرقه‌افکنانه یا افراطی به دلیل توانایی بالاتر در جلب «تعامل» (لایک، اشتراک‌گذاری، کامنت)، به‌طور نامتناسبی ترویج می‌شود (*Noble, 2018*). این امر می‌تواند کاربر را به یک «چاله خرگوش»[۱۴] خطرناک سوق دهد که در آن به‌تدریج به سمت محتوای مضرتر کشیده می‌شود (*Ofcom, 2024*). تحقیقات متعدد نشان داده‌اند که این سازوکار می‌تواند به‌طور فعال محتوای مرتبط با اختلالات خوردن، خودآزاری و ایده‌پردازی خودکشی را به نوجوانان آسیب‌پذیر پیشنهاد دهد (*Office of the Surgeon General (OSG), 2023*).

اگرچه الگوریتم‌های توصیه‌گر که توسط سکوها به کار گرفته می‌شوند، از منظر فنی با هدف شناسایی و تطبیق «علایق کاربر» طراحی شده‌اند و می‌توانند محتوای مفید را نیز پیشنهاد دهند؛ اما کارکرد آن‌ها در بستر «اقتصاد توجه» دو چالش بنیادین ایجاد می‌کند: نخست، چالش عمومی «اعتیاد به محتوا» برای حداکثرسازی زمان حضور کاربر، و دوم، چالش اختصاصی «تشدید ناهنجاری‌ها» در گروه‌های آسیب‌پذیر. در خصوص کودکان، الگوریتم در جستجوی علایق، ممکن است کنجکاوی‌های گذرا یا حالات روحی منفی آن‌ها را به‌عنوان «علاقه پایدار» تفسیر کرده و با ارائه انبوه محتوای مشابه، آن‌ها را در یک چرخه آسیب‌زا یا «نفوذ ناروا» گرفتار کند (*Milano et al., 2020*). این وضعیت، مفهوم رضایت کاربر را از منظر فقهی به چالش می‌کشد. حتی اگر سکوها به‌صراحت اعلام کنند که از الگوریتم‌های مبتنی بر علاقه استفاده می‌کنند، آنچه معمولاً مسکوت می‌ماند، «سازوکار مهندسی رفتار» و «تأثیرات عصب‌شناختی» این الگوریتم‌ها بر مغز نابالغ کودک است. این عدم شفافیت در بیان «ماهیت اثر» (و نه اصل وجود ابزار)، مصداق بارز قاعده فقهی «غرور» (فریب) است. قاعده غرور مقرر می‌دارد هرکس دیگری را فریب دهد و از این طریق ضرری به او وارد آورد، ضامن است *(امیدی‌فرد، ۱۳۸۵)*. در اینجا نیز سکو با معرفی سرویس خود به‌عنوان یک «بستر سرگرمی» و پنهان‌سازی «معماری اعتیادآور» آن، ولی یا کودک را نسبت به ایمنی محیط فریفته است. این فریب ساختاری، مبنای محکمی برای بی‌اعتباری

13. algorithmic amplification
14. rabbit hole

رضایت اخذ شده و مسئولیت مدنی سکو فراهم می‌آورد *(مکارم شیرازی، ۱٤۱۰)*.

علاوه‌براین، این شکل از مداخله روان‌شناختی هدفمند، گفتمان نوظهور «حقوق عصب‌شناختی»[۱۵] را به میان می‌آورد که بر لزوم حفاظت از حریم خصوصی ذهنی، آزادی شناختی و تمامیت روانی در برابر فناوری‌های نوین تأکید دارد *(واثقی، ۱٤۰۲)*. این حقوق، ترجمان مدرنی از مقصد بنیادین «حفظ العقل» در شریعت اسلامی هستند (*Habib, 2025*). اهمیت این مقصد از آن‌روست که در اندیشه اسلامی، عقل صرفاً یک ابزار شناختی نیست بلکه زیربنای تکلیف، مسئولیت اخلاقی و وجه تمایز انسان است *(غلامی، ۱٤۰۱)*؛ بنابراین، فناوری‌هایی که عامدانه این قوه بنیادین را هدف قرار داده و آن را تضعیف می‌کنند، نه‌تنها به سلامت روان آسیب می‌زنند بلکه شالوده مسئولیت‌پذیری انسان را به چالش می‌کشند و از این‌منظر، یک تهدید وجودی برای اهداف عالیه شریعت محسوب می‌شوند.

٤- پاسخ‌های تنظیم‌گرانه تطبیقی: از رویکرد مبتنی بر ریسک تا وظیفه مراقبت الگوریتمی

در مواجهه با این نسل جدید از مخاطرات، نظام‌های حقوقی پیشرو در حال تدوین چهارچوب‌های نوآورانه‌ای هستند که از الگوواره سنتی کنترل محتوا فراتر می‌روند. تحلیل سه الگوی متمایز، یعنی رویکرد «ریسک‌محور» اتحادیه اروپا، مدل «وظیفه مراقبت» بریتانیا و رویکرد «پاسخگویی الگوریتمی» ایالات متحده آمریکا، می‌تواند طیف وسیعی از گزینه‌های تنظیم‌گری را برای ایران روشن سازد.

٤-۱- اتحادیه اروپا: قانون خدمات دیجیتال و قانون هوش مصنوعی

اتحادیه اروپا پیشگام تنظیم‌گری معماری سکوها و حفاظت از کودکان است. این اتحادیه رویکرد خود را در دو لایه مکمل تدوین کرده است. لایه نخست و مهم‌تر، «قانون خدمات

15. Neurorights

دیجیتال»[16] مصوب ۲۰۲۲ است که مستقیماً الگوریتم‌های توصیه‌گر را هدف قرار می‌دهد. ماده ۲۷ این قانون، سکوها را موظف می‌کند مؤلفه‌های اصلی الگوریتم‌های توصیه‌گر خود را شفاف سازند. مهم‌تر از آن، ماده ۲۸ قانون *DSA* به‌صراحت سکوها را ملزم می‌کند که سطح بالایی از حریم خصوصی و ایمنی خردسالان را در طراحی رابط کاربری و الگوریتم‌های خود تضمین کنند. همچنین بر اساس ماده ۳۸، سکوهای بسیار بزرگ مکلف‌اند حداقل یک گزینه در الگوریتم توصیه‌گر خود ارائه دهند که مبتنی بر رخ‌نماسازی رفتاری نباشد *(European Parliament, 2022)*.

لایه دوم، «قانون هوش مصنوعی»[17] مصوب ۲۰۲٤ است که با اتخاذ رویکردی ریسک‌محور، استفاده از سیستم‌هایی را که با بهره‌برداری از آسیب‌پذیری‌های ناشی از سن (کودکان)، رفتار آن‌ها را به‌گونه‌ای تحریف می‌کنند که منجر به آسیب جسمی یا روانی شود، در ماده ٥ صراحتاً ممنوع اعلام کرده است (*European Union, 2024*).

٤-۲- بریتانیا و وظیفه مراقبت

بریتانیا با تصویب «قانون ایمنی برخط»[18] مصوب ۲۰۲۳ الگوواره نظارتی را از محتوا به سمت ارزیابی ریسک‌های سیستمی تغییر داده است. بخش ۱۱ این قانون، سکوها را به انجام مستمر «ارزیابی ریسک کودکان» ملزم می‌کند. همچنین بخش ۱۲ به‌صراحت «وظیفه مراقبت»[19] را در طراحی سیستم‌ها اعمال کرده و سکوها را مکلف می‌سازد تا از طریق طراحی الگوریتم‌های خود، مانع از مواجهه کودکان با محتوای مضر (مانند ترویج خودآزاری و اختلالات خوردن) شوند (*UK Parliament, 2023*). این قانون، بار اثبات را به مرحله پیش از وقوع آسیب منتقل کرده است.

این وظیفه مراقبت با آیین‌نامه طراحی مناسب سن[20] تکمیل می‌شود که اصول کلی حفاظت از داده را به ۱۵ استاندارد عملیاتی برای «ایمنی در طراحی»[21] ترجمه می‌کند (*ICO,*

16. DSA
17. AI Act
18. Online Safety Act 2023
19. duty of care
20. Age-Appropriate Design Code - AADC
21. Safety by Design

2020). این استانداردها سکوها را ملزم می‌کنند که:

- منافع عالیه کودک را به‌عنوان یک ملاحظه اولیه در تمام مراحل طراحی در نظر بگیرند؛
- تنظیمات حریم خصوصی را به‌طور پیش‌فرض روی بالاترین سطح حفاظت قرار دهند؛
- از روش‌های اغواگرانه[۲۲] که کودکان را به تضعیف تنظیمات حفاظتی یا اشتراک‌گذاری داده‌های غیرضروری تشویق می‌کند، استفاده نکنند.

مدل بریتانیا یک گذار مفهومی مهم را به نمایش می‌گذارد: تغییر کانون توجه از «محتوای غیرقانونی» به «سیستم‌های مولد خطر». این رویکرد، بار مسئولیت را از اثبات آسیب پس از وقوع، به الزام سکو برای اثبات ایمنی پیش از عرضه محصول منتقل می‌کند. این الگووار، مبنای قدرتمندی برای مقابله با آسیب‌های الگوریتمی فراهم می‌آورد؛ زیرا به‌جای تمرکز بر خروجی‌های منفرد یک الگوریتم، خودِ فرایند طراحی و مدیریت ریسک آن را هدف قرار می‌دهد.

٤-۳- ایالات متحده و تأکید بر شفافیت از طریق قانون پاسخگویی الگوریتمی

برخلاف اتحادیه اروپا که مسیر قانون‌گذاری جامع را برگزیده، رویکرد ایالات متحده به‌طور سنتی بر تنظیم‌گری بخشی و نظارت پسینی استوار بوده است. بااین‌حال، در واکنش به مخاطرات نوین، الگوواره جدیدی تحت عنوان «پاسخگویی الگوریتمی»[۲۳] (*U.S. Congress, 2023*) در حال شکل‌گیری است که برای موضوع این پژوهش بسیار الهام‌بخش است.

الف) قانون پاسخگویی الگوریتمی (طرح پیشنهادی): این طرح قانونی، شرکت‌های بزرگ فناوری را ملزم می‌کند که برای سیستم‌های تصمیم‌گیر خودکار، به‌طور مرتب «ارزیابی تأثیر» انجام دهند. تمرکز این ارزیابی‌ها بر شناسایی خطراتی چون تبعیض، نقض حریم خصوصی و آسیب به گروه‌های آسیب‌پذیر (مانند کودکان) است. اهمیت این مدل برای ایران در این است که به جای ممنوعیت فناوری، بر «شفافیت فرایند» تأکید دارد.

ب) چهارچوب مدیریت ریسک هوش مصنوعی[۲۴]: این سند که توسط مؤسسه ملی استاندارد

22. nudge techniques
23. Algorithmic Accountability Act
24. NIST AI RMF

و فناوری آمریکا تدوین شده، اگرچه داوطلبانه است؛ اما به استاندارد طلایی صنعت تبدیل شده است. این چهارچوب بر مفهوم «ایمنی اجتماعی–فنی» تأکید دارد؛ یعنی ایمنی هوش مصنوعی را نمی‌توان فقط در کدنویسی جستجو کرد بلکه باید تأثیر آن بر بستر اجتماعی (مثلاً رشد کودک) سنجیده شود (*NIST, 2023*).

ج) نقش کمیسیون تجارت فدرال: این نهاد ناظر با تفسیر موسع از قوانین «منع رویه‌های فریبکارانه»، اعلام کرده است که استفاده پنهانی از الگوریتم‌های اعتیادآور یا تبعیض‌آمیز علیه کودکان، مصداق رویه تجاری ناعادلانه است. این رویکرد عملیاتی نشان می‌دهد که حتی بدون قانون جدید، می‌توان با تفسیر پویای قوانین موجود (مشابه ظرفیت‌های قانون مدنی ایران)، سکوها را مسئول شناخت.

۵- ظرفیت‌سنجی نظام حقوقی ایران: بومی‌سازی چهارچوب حمایتی در برابر هوش مصنوعی

هرچند نظام حقوقی ایران فاقد قوانین خاص و مدون برای تنظیم‌گری هوش مصنوعی است؛ اما این به‌معنای وجود یک خلأ حقوقی مطلق نیست. مبانی و اصول کلی حقوق مدنی ایران که ریشه در فقه امامیه دارند، ظرفیت‌های قابل توجهی برای بومی‌سازی یک چهارچوب حمایتی و تحمیل مسئولیت بر سکوهای هوش مصنوعی فراهم می‌آورند.

۵-۱- بازخوانی قواعد مسئولیت مدنی

قواعد عمومی ضمان قهری در قانون مدنی، ابزارهای قدرتمندی برای مسئول شناختن سکوها در قبال آسیب‌های الگوریتمی ارائه می‌دهند.

قاعده تسبیب و معیار «سبب اقوی از مباشر» در عصر الگوریتمی: در نظام حقوقی ایران، با استناد به اصل شخصی بودن مسئولیت و قواعد عمومی حاکم بر اجتماع سبب و مباشر، اصل بر عدم مسئولیت سکوهای برخط در قبال اعمال کاربرانشان استوار است. *(حسام و غلامعلی‌زاده، ۱۴۰۲)*. براین‌اساس، در نگاه اول، کاربر به‌عنوان مباشر (کسی که محتوای مضر را مشاهده یا تولید می‌کند) مسئول اصلی شناخته می‌شود و سکو صرفاً یک سبب معد (فراهم‌کننده بستر) تلقی می‌گردد که مسئولیتی متوجه او نیست. بااین‌حال،

چنین تحلیلی ماهیت فعالانه، جهت‌دهنده و مهندسی‌شده الگوریتم‌های نوین را نادیده می‌گیرد و نیازمند بازخوانی و توسعه مفهومی قاعده «سبب اقوی از مباشر» متناسب با واقعیت‌های عصر فناوری است. در ادامه استدلال خواهد شد که چگونه ویژگی‌های منحصربه‌فرد سیستم‌های هوش مصنوعی، این اصل اولیه را به چالش کشیده و مسئولیت را به سمت سکو به‌عنوان سبب اقوی منتقل می‌سازد.

در کاربست قاعده تسبیب (ماده ۳۳۱ و ۳۳۲ قانون مدنی) بر فضای مجازی، تفکیک دقیق نقش‌ها در ساختار سکوها ضروری است. در حالت سنتی، «کاربرِ تولیدکننده محتوا» به‌عنوان مباشر (ایجادکننده مستقیم زیان) و سکو صرفاً به‌عنوان سبب مُعِد (فراهم‌کننده بستر) شناخته می‌شود. طبق قواعد عمومی، اصل بر مسئولیت مباشر است. اما این تحلیل صرفاً در مورد «سکوهای غیرفعال»[۲۵] صادق است.

مسئله این پژوهش، نسل جدیدی از واسطه‌ها یعنی «سکوهای الگوریتم‌محور» است. در اینجا، رابطه میان سکو و الگوریتم، رابطه «ابزار و کاربر» است؛ الگوریتم ابزاری است که سکو از طریق آن بر توزیع محتوا اعمال حاکمیت می‌کند. در این فرض، سکو از نقش خنثی خارج شده و با استفاده از الگوریتم‌های توصیه‌گر، محتوای تولید شده توسط کاربر (مباشر) را «انتخاب»، «اولویت‌بندی» و «توزیع هدفمند» می‌کند.

استدلال حقوقی این است که وقتی الگوریتم با شناسایی ضعف‌های شناختی کودک، محتوای آسیب‌زایی را که ممکن بود هرگز توسط کودک دیده نشود، به‌صورت فعالانه به او پیشنهاد می‌دهد و ضریب نفوذ آن را هزاران برابر می‌کند، نقش سکو در وقوع خسارت از نقش تولیدکننده اولیه فراتر می‌رود. اینجا «سبب» (سکو) به دلیل «اقوی بودن در تأثیر» و «کنترل بر معماری توزیع»، بر «مباشر» (تولیدکننده) غلبه کرده و طبق بخش دوم ماده ۳۳۲ قانون مدنی، مسئول جبران خسارت شناخته می‌شود.

در فقه امامیه، معیار اقوی بودن سبب از مباشر، صرفاً غلبه مادی و فیزیکی نیست بلکه شدت تأثیر عرفی و میزان دخالت در اراده مباشر ملاک است. فقیهانی چون محقق بجنوردی در «القواعد الفقهیهٔ» در بحث اجتماع سبب و مباشر تصریح می‌کنند که هرگاه مباشر به

25. Passive

دلیل «غرور» (فریب) یا جهل، اراده‌اش تحت تأثیر مسبب قرار گیرد و مسبب منشأ ایجاد انگیزه در او باشد، سبب اقوی محسوب شده و ضامن است *(بجنوردی، ۱٤۱۹ق، ص. ۳٦)*. در بستر شبکه‌های اجتماعی، سکو با در اختیار داشتن داده‌های عظیم و دانش روان‌سنجی، از طریق الگوریتم‌های توصیه‌گر دست به یک «دستکاری شناختی هدفمند» می‌زند. این عدم تقارن شدید اطلاعاتی و طراحی اعتیادآور، مصداق بارز «غرور» است که اراده و ادراک کودک را مخدوش می‌سازد. در این حالت، فریبِ ساختاریِ سکو، معادلِ کارکردیِ سلب اراده است.

علاوه‌براین، طراحی اعتیادآور و مهندسی رفتار که پیشتر بحث شد، مصداق بارز «غرور» (فریب) است که اراده کاربر را مخدوش می‌سازد. در فقه نیز تصریح شده است که اگر مباشر به دلیل جهل یا فریب خوردن مرتکب خسارت شود، سبب ایجادکننده جهل یا فریب، اقوی و ضامن است؛ بنابراین، اقوی بودن سکو نه از منظر تأثیر فیزیکی، بلکه از منظر «تأثیر معرفتی و ارادی» است. این دستکاری شناختی، اگرچه اکراه مادی نیست؛ اما با بهره‌کشی نظام‌مند از آسیب‌پذیری‌های ناخودآگاه، اراده مؤثر را از کاربر سلب کرده و از نظر کارکردی، معادل حقوقی فریب یا ایجاد جهل نسبت به خطر است. این تسلط معرفتی و روان‌شناختی، تأثیرگذاری سکو را از نظر عرفی به مراتب قوی‌تر از اراده محدود کاربر ساخته و استناد ضرر به آن را کاملاً موجه می‌سازد.

هنگامی که یک الگوریتم به‌طور هدفمند محتوایی را به سمت یک کودک آسیب‌پذیر سوق می‌دهد، این دیگر یک «فراهم کردن زمینه» ساده نیست، بلکه «جهت‌دهی اراده» و «ایجاد سبب اصلی» ضرر است. در این فرض، سکو به دلیل داشتن دانش برتر، کنترل بر معماری سیستم و بهره‌برداری عامدانه از آسیب‌پذیری‌های رشدی کودک برای حداکثرسازی تعامل، به‌مراتب تأثیرگذارتر از کاربر با اراده محدود و اطلاعات ناقص است *(حسام و غلامعلی‌زاده، ۱٤۰۲)*. درنتیجه، عرفاً اتلاف به او مستند شده و مصداق بارز «سبب اقوی از مباشر» محسوب می‌شود و می‌توان مسئولیت جبران خسارت را مستقیماً متوجه سکو دانست *(محمدرضایی و ریاحی، ۱٤۰۲)*. این رویکرد، اصل شخصی بودن مسئولیت را نقض نمی‌کند بلکه آن را به جایی منتقل می‌کند که قدرت واقعی برای کنترل ریسک وجود دارد.

کاربست قاعده «لاضرر» به مثابه تکلیف پیشگیرانه: بر اساس مبانی مستحکم اصولی در فقه امامیه، قاعده «لا ضرر و لا ضرار»، صرفاً یک حکم وضعی برای جبران خسارت پس از وقوع نیست. فقیهانی نظیر امام خمینی در رساله «بدائع الدرر فی قاعدهٔ نفی الضرر» استدلال می‌کنند که نهی در «لا ضرار»، یک نهی تکلیفی، تحریمی و دارای شأن حکومتی است که دولت و مکلفان را به پیشگیری از ایجاد بستر ضرری ملزم می‌سازد *(خمینی، ۱٤۱۵ق، ص. ۱۰٦)*. در عصر فناوری، کاربست این تفسیر پیشگیرانه بدین‌معناست که رها کردن یک الگوریتم قدرتمند و دوپامین‌محور که مستقیماً روان و سلامت ذهنی کودکان را هدف قرار می‌دهد، بدون ارزیابی ریسک پیشینی، مصداق بارز «اضرار» به جامعه است. ازاین‌رو، قاعده لاضرر تکلیفی ایجابی بر دوش نهادهای تنظیم‌گر و سکوها می‌گذارد تا از طریق تعبیه سازوکارهای ایمنی (مانند ارزیابی تأثیر الگوریتمی)، منافذ ورود ضرر را مسدود نمایند *(محقق داماد، ۱۳۹۵؛ موسوی بجنوردی، ۱۳۷۹، ص. ۲۱۲)*.

مسئولیت ناشی از عیب محصول: یکی از کارآمدترین مبانی حقوقی، تلقی کردن سرویس‌های هوش مصنوعی به‌عنوان «محصول» و اعمال دکترین مسئولیت ناشی از عیب محصول است. هرچند در دکترین حقوقی ایران در خصوص ماهیت نرم‌افزار به‌عنوان کالا یا خدمت اختلاف‌نظر وجود دارد و قوانین موجود مانند قانون حمایت از حقوق مصرف‌کنندگان *(مجلس شورای اسلامی، ۱۳۸۸)* تعریف روشنی در این زمینه ارائه نداده‌اند *(غریبه و همکاران، ۱۳۹۹)*؛ اما با تفسیری هدف‌محور و با توجه به ماهیت عملکردی سکوهای دیجیتال که به‌صورت انبوه و استاندارد عرضه می‌شوند، می‌توان آن‌ها را مشمول قواعد حاکم بر محصولات دانست *(رجبی، ۱٤۰۳)*. در این چهارچوب، «عیب» نه یک نقص فنی در کدنویسی، بلکه یک «عیب در طراحی»[۲٦] است؛ یعنی محصول ذاتاً فاقد ایمنی متعارف و مورد انتظار برای گروه آسیب‌پذیری از مصرف‌کنندگان (کودکان) است. معیار «ایمنی متعارف» باید با در نظر گرفتن آسیب‌پذیرترین گروهی که به‌طور قابل پیش‌بینی از محصول استفاده می‌کنند، تعریف شود؛ بنابراین، سکویی که برای یک کاربر بزرگسال ایمن تلقی می‌شود، ممکن است به‌دلیل فقدان سازوکارهای حفاظتی متناسب با ویژگی‌های رشدی

26. design defect

کودکان، برای این گروه سنی «معیوب» محسوب شود. این رویکرد که در حقوق ایران نیز به سمت آن گرایش وجود دارد *(هیئت وزیران، ۱۳۸۳)*، به مسئولیت محض[۲۷] تولیدکننده منتهی می‌شود *(عربیان و موسی نتاج، ۱۴۰۱)*. بر اساس این دکترین که در روح قانون حمایت از حقوق مصرف‌کنندگان نیز رگه‌هایی از آن دیده می‌شود، بار اثبات تقصیر از دوش زیان‌دیده برداشته شده و صرف اثبات وجود عیب در طراحی و رابطه سببیت برای تحقق مسئولیت کافی است. این تفسیر، ابزار قدرتمندی برای مقابله با آسیب‌های ساختاری ناشی از مدل‌های کسب‌وکار مبتنی بر بهره‌کشی از توجه کاربران فراهم می‌آورد *(حسینی مقدم و همکاران، ۱۴۰۲)*.

۵-۲- اصل احتیاط فقهی به‌مثابه مبنای تنظیم‌گری پیشگیرانه

علاوه بر قواعد ضمان‌آور، اصول فقهی نیز ظرفیت قابل توجهی برای تنظیم‌گری پیشگیرانه هوش مصنوعی دارند. «اصل احتیاط» یا «اشتغال»، به‌عنوان یکی از اصول عملیه، مکلف را در هنگام شک در تکلیف و در جایی که احتمال ضرر مهمی وجود دارد، ملزم به رعایت جوانب امر می‌کند تا یقین به برائت ذمه حاصل شود. این اصل، به‌ویژه در مواردی که با خطرات جدی و جبران‌ناپذیر برای امور خطیری چون جان، ناموس و اموال مواجه هستیم، کاربرد می‌یابد. آسیب‌های الگوریتمی به سلامت روان و آینده کودکان، به‌دلیل گستردگی، پیچیدگی و برگشت‌ناپذیر بودن بالقوه، مصداق بارز چنین خطراتی هستند. در شرایطی که رابطه سببیت میان یک طراحی الگوریتمی خاص و آسیب روانی یک کودک به‌صورت قطعی قابل اثبات نیست (ریسک نامعلوم)، اصل احتیاط ایجاب می‌کند که قانون‌گذار رویکردی پیشگیرانه اتخاذ کرده و بار مسئولیت را بر دوش توسعه‌دهنده فناوری قرار دهد تا ایمنی محصول خود را پیش از عرضه به جامعه اثبات کند *(خوبیاری، ۱۳۹۷)*. این اصل فقهی، مبنای نظری محکمی برای الزام شرکت‌ها به انجام «ارزیابی تأثیر الگوریتمی» و اتخاذ رویکرد «ایمنی در طراحی» فراهم می‌آورد.

27. Strict Liability

۵-۳- تحلیل قوانین و اسناد بالادستی نوین

نظام حقوقی ایران در سال‌های اخیر با تصویب اسناد مهمی، گام‌هایی در جهت حمایت از کودکان در فضای دیجیتال برداشته است. «قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹» با ارائه تعاریف گسترده از مفاهیمی چون «سوءرفتار» و «وضعیت مخاطره‌آمیز»، ظرفیت بالایی برای انطباق با آسیب‌های الگوریتمی دارد. طبق بند «ت» ماده ۱ این قانون، هر فعل یا ترک فعلی که «سلامت روانی، اخلاقی یا اجتماعی طفل و نوجوان را در معرض خطر و آسیب قرار دهد» سوءرفتار محسوب می‌شود. طراحی الگوریتم‌هایی که عامدانه کودکان را به سمت محتوای مضر یا اعتیادآور سوق می‌دهند، به‌وضوح ذیل این تعریف قرار می‌گیرد. همچنین، قرار گرفتن کودک در معرض محتوای مستهجن یا مبتذل که توسط هوش مصنوعی تولید یا توصیه می‌شود، طبق ماده ۱۰ این قانون جرم‌انگاری شده است *(مجلس شورای اسلامی، ۱۳۹۹)*.

علاوه‌براین، «سند صیانت از کودکان و نوجوانان در فضای مجازی مصوب ۱۴۰۰» شورای عالی فضای مجازی، یک سند بالادستی راهبردی است که تکالیف مشخصی را برای دستگاه‌های مختلف جهت ایجاد «محیط صیانت‌شده» بر بستر شبکه ملی اطلاعات تعیین کرده است. این سند بر سیاست‌هایی چون «رده‌بندی کلیه محتوا و خدمات متناسب با سن»، «تشویق و ساماندهی بخش غیردولتی فعال در ارائه محتوا و خدمات سالم، مفید و ایمن» و «ارتقای سواد فضای مجازی» تأکید دارد *(شورای عالی فضای مجازی، ۱۴۰۰)*. چهارچوب پیشنهادی این مقاله، مبنی بر الزام به ارزیابی تأثیر الگوریتمی، می‌تواند به‌عنوان یک سازوکار اجرایی مؤثر برای تحقق اهداف این سند بالادستی تلقی شود و نشان می‌دهد که حرکت به سمت مسئولیت‌پذیری سیستمی سکوها، همسو با سیاست‌های کلان کشور است.

۶- طراحی چهارچوب تنظیم‌گری آینده‌نگر: به‌سوی یک «وظیفه مراقبت الگوریتمی»

با تلفیق تحلیل‌های فنی، تطبیقی و دکترینال، می‌توان یک چهارچوب تنظیم‌گرانه بومی و آینده‌نگر برای ایران طراحی کرد که از رویکردهای پیشین فراتر می‌رود. درحالی‌که «نسل دوم تنظیم‌گری» بر مفهوم کلی «طراحی ایمن» و «وظیفه مراقبت» متمرکز بود، مدل

پیشنهادی این پژوهش با گذر به «نسل سوم»، بر «حسابرسی الگوریتمی»[۲۸] و «ارزیابی تأثیر پیشینی» تأکید دارد. تفاوت بنیادین در این است که در رویکرد جدید، صرفِ ادعای رعایت ایمنی کافی نیست بلکه سکو مکلف است از طریق سازوکار شفاف «ارزیابی تأثیر الگوریتمی بر حقوق کودک» (*DPIA-C*)، بی‌خطر بودن معماری خود را پیش از عرضه اثبات کند. هسته اصلی این چهارچوب، تبدیل تکلیف اخلاقیِ مراقبت به یک تکلیف حقوقیِ رویه‌ای و قابل‌سنجش است که بر مبانی فقهی «نفی ضرر محتمل» استوار شده است.

۶-۱- تعریف «وظیفه مراقبت الگوریتمی» در حقوق ایران

پیشنهاد می‌شود یک مفهوم حقوقی جدید تحت عنوان «وظیفه مراقبت الگوریتمی»[۲۹] در نظام حقوقی ایران تعریف و تدوین شود *(انصاری، ۱۴۰۱)*. این وظیفه، یک تکلیف قانونی بر عهده طراحان، توسعه‌دهندگان و ارائه‌دهندگان سیستم‌های هوش مصنوعی (که احتمالاً توسط کودکان مورد استفاده قرار می‌گیرند) قرار می‌دهد تا اقدامات متعارف و متناسبی را برای شناسایی، ارزیابی و کاهش ریسک‌های قابل پیش‌بینی ناشی از طراحی و عملکرد الگوریتم‌های خود به عمل آورند.

این وظیفه باید بر مبانی حقوقی داخلی استوار باشد:

- **ریشه در قاعده لاضرر**: این وظیفه، جنبه پیشگیرانه و حکومتی قاعده لاضرر را عملیاتی می‌کند و از یک تکلیف صرفاً جبرانی به یک الزام پیشگیرانه ارتقا می‌یابد.
- **مبتنی بر قواعد تسبیب و مسئولیت عیب محصول**: نقض این وظیفه، «تقصیر» سکو را در چهارچوب قاعده تسبیب محرز می‌سازد و محصولی که با نقض این وظیفه طراحی شده، «کالای معیوب» تلقی می‌شود.

این وظیفه، بار اثبات را از دوش زیان‌دیده برمی‌دارد و معکوس می‌کند؛ اما این جابجایی صرفاً یک تغییر شکلی در دادرسی نیست بلکه از طریق سازوکار عینی «ارزیابی تأثیر» عملیاتی می‌شود. در مقام اجرا، سکو برای اثبات عدم تقصیر، نمی‌تواند به صرف ادعا اکتفا کند بلکه مکلف است «مستندات فنی» و «گواهی‌های حسابرسی الگوریتمی» را که پیش از

28. Algorithmic Auditability
29. Algorithmic Duty of Care

عرضه محصول توسط نهادهای ناظر یا ممیزان مستقل تأیید شده است، به دادگاه ارائه دهد. بدین‌ترتیب، اطمینان از طراحی مناسب، نه بر اساس ادعای سکو، بلکه بر مبنای «استانداردهای قابل‌سنجش» و اسناد مثبته‌ای حاصل می‌شود که رعایت ایمنی را در مرحله طراحی گواهی می‌کنند.

جدول ۱: ماتریس تحلیلی انطباق آسیب‌های الگوریتمی با دکترین‌های مسئولیت در حقوق ایران

قاعده تسبیب (سبب اقوی)	قاعده لاضرر (تکلیف پیشگیرانه)	مسئولیت ناشی از عیب محصول
سکو به دلیل دستکاری شناختی و دانش نامتقارن، سبب اقوی است (نیازمند بازخوانی مفهوم «اقوی بودن»).	طراحی اعتیادآور، مصداق «اضرار» به سلامت روان جامعه است و تکلیف به پیشگیری را ایجاب می‌کند.	طراحی فاقد ایمنی متعارف برای گروه سنی کودک، مصداق «عیب در طراحی» است.

۶-۲- سازوکار اجرایی: عدالت رویه‌ای و الزام به ارزیابی تأثیر الگوریتمی بر کودک

برای آنکه «وظیفه مراقبت الگوریتمی» از یک مفهوم انتزاعی به یک تکلیف عملی تبدیل شود، نیازمند یک سازوکار اجرایی قدرتمند است. در مواجهه با سیستم‌های پیچیده هوش مصنوعی که اثبات سببیت مستقیم در آن‌ها دشوار است، نظریه «عدالت رویه‌ای» راهگشاست. این نظریه که بیان می‌دارد منصفانه بودن فرایندها به نتایج مشروعیت می‌بخشد (*Tyler, 2000*)، ریشه‌های عمیقی در فلسفه قضائی اسلام دارد. اصولی چون «حق دفاع متهم»، لزوم شفافیت فرایند دادرسی و منع صدور حکم بدون استماع دفاعیات، همگی بر اهمیت رویه منصفانه تأکید دارند *(نجفیان رضوی و همکاران، ۱۴۰۱)*. براین‌اساس، می‌توان پیشنهاد این مقاله را نه یک واردات نظری، بلکه تجلی مدرن این اصول بنیادین دانست؛ سازوکاری برای تضمین «انصاف رویه‌ای»، نه در دادگاه قضائی، بلکه در «دادگاه الگوریتم» که در آن تصمیماتی حیاتی برای آینده کودک گرفته می‌شود.

بنابراین، با الهام از رویه‌های بین‌المللی و با اتکا به مبانی داخلی، پیشنهاد می‌شود انجام

«ارزیابی تأثیر الگوریتمی بر کودک»[۳۰] به‌عنوان یک الزام قانونی و مصداق بارز یک تکلیف رویه‌ای، برای تمام سیستم‌های هوش مصنوعی که احتمالاً توسط کودکان مورد استفاده قرار می‌گیرند، پیش‌بینی شود (*Aitken et al., 2023*). این ارزیابی، یک فرایند مستندسازی‌شده و پیشگیرانه است که توسعه‌دهندگان را ملزم می‌کند پیش از عرضه محصول، به‌طور نظام‌مند به تحلیل و کاهش ریسک‌های آن برای کودکان بپردازند. جدول زیر، چهارچوب پیشنهادی برای این ارزیابی را با اتکا به مبانی فقهی و حقوقی داخلی ارائه می‌دهد.

جدول ۲: چهارچوب پیشنهادی برای ارزیابی تأثیر الگوریتمی بر کودک (*CAIA*) در نظام حقوقی ایران

حوزه ارزیابی	پرسش‌های کلیدی برای ارزیابی	مبنای حقوقی داخلی	مبنای فقهی
ایمنی و سلامت روان	آیا سیستم می‌تواند کودک را به سمت محتوای مضر (اختلالات خوردن، خودآزاری) سوق دهد؟ آیا از سازوکارهای طراحی اعتیادآور (اسکرول بی‌نهایت) استفاده شده است؟	ماده ۱ (بند ت) و ماده ۳ (بند ژ) قانون حمایت از اطفال و نوجوانان ۱۳۹۹ (تعریف سوءرفتار و وضعیت مخاطره‌آمیز)	قاعده لاضرر، حفظ النفس، حفظ العقل
حریم خصوصی و حفاظت از داده‌ها	چه داده‌های رفتاری از کودک جمع‌آوری می‌شود؟ آیا الگوریتم توصیه‌گر بر اساس رخ‌نماسازی رفتاری و داده‌های حساس کودک عمل می‌کند؟	مواد ۳۷ و ٤٠ قانون تجارت الکترونیکی (الزام به شفافیت در پردازش داده‌ها)، بند پ ماده ۳ قانون حمایت از اطفال و نوجوانان	حفظ العرض (آبرو)، نهی از تجسس، شرطیت مصلحت در ولایت
انصاف و عدم تبعیض	آیا داده‌های آموزشی بازتاب‌دهنده سوگیری‌های اجتماعی (جنسیتی، قومی) است؟ آیا خروجی الگوریتم فرصت‌های یک گروه را محدود می‌کند؟	اصول ۱۹ و ۲۰ قانون اساسی (برابری)، ماده ۳ قانون حمایت از اطفال (منع تبعیض)	اصل عدالت، قاعده انصاف
شفافیت و	آیا برای کاربر مشخص است که با	قانون حمایت از حقوق	نهی از غرر

30. Child–centric Algorithmic Impact Assessment (CAIA)

حوزه ارزیابی	پرسش‌های کلیدی برای ارزیابی	مبنای حقوقی داخلی	مبنای فقهی
توضیح‌پذیری	یک سیستم هوش مصنوعی در تعامل است؟ آیا منطق کلی عملکرد الگوریتم (چرا این محتوا پیشنهاد شده؟) قابل توضیح است؟	مصرف‌کنندگان (حق بر اطلاعات)، قانون تجارت الکترونیکی	(فریب)، لزوم شفافیت در معاملات
توسعه و شکوفایی کودک	آیا سیستم خلاقیت و تفکر انتقادی را تقویت می‌کند یا کودک را به مصرف‌کننده منفعل تبدیل می‌سازد؟ آیا به «حق بر بازی» و «حق بر آینده‌ای گشوده» احترام می‌گذارد؟	ماده ۱۱۸٤ قانون مدنی (مصلحت)، اهداف سند تحول بنیادین آموزش و پرورش	حفظ العقل، مصلحت در تربیت

۶-۳- نهاد ناظر: یک ساختار دو لایه و عمل‌گرایانه

برای تضمین اجرای مؤثر این چهارچوب، تعیین یک نهاد ناظر متخصص ضروری است. با توجه به ساختار حکمرانی فضای مجازی در ایران و با اذعان به مباحث حقوقی پیرامون جایگاه شورای عالی فضای مجازی، یک رویکرد دو لایه و عمل‌گرایانه پیشنهاد می‌شود:

سطح سیاست‌گذاری کلان: شورای عالی فضای مجازی، به‌عنوان نهاد فرادستی و هماهنگ‌کننده، تکلیف قانونی کلان یعنی «وظیفه مراقبت الگوریتمی» و الزام به انجام *CAIA* را به‌عنوان یک «سیاست ملی» تصویب و ابلاغ می‌کند.

سطح نظارت عملیاتی: جنبه‌های اجرایی، شامل تدوین استانداردهای فنی *CAIA*، دریافت و بررسی گزارش‌های ارزیابی و اعمال ضمانت اجراهای لازم، به یک نهاد تخصصی تحت نظر آن، مانند «کمیسیون عالی حفاظت از کودکان در برابر آسیب‌های الگوریتمی» ذیل مرکز ملی فضای مجازی، تفویض می‌شود.

این رویکرد، ضمن استفاده از ظرفیت‌های نهادی موجود و نشان دادن درک عمیق از واقعیت‌های حکمرانی در ایران، پیشنهاد را عملیاتی‌تر و در برابر نقدها مقاوم‌تر می‌سازد. عدم انجام *CAIA* یا انجام یک ارزیابی ناقص و صوری، به‌خودی‌خود یک فعل زیان‌بار و مصداق بارز نقض وظیفه مراقبت تلقی شده و مبنای محکمی برای مسئولیت مدنی سکو

فراهم می‌آورد.

٦-٤- چالش‌های اجرایی و مدل‌های پیاده‌سازی CAIA: موازنه میان شفافیت و اسرار تجاری

الزام به افشای جزئیات عملکرد الگوریتم‌ها در فرایند *CAIA*، با یکی از بزرگترین موانع عملیاتی یعنی تعارض با «اسرار تجاری» مواجه است. الگوریتم‌ها، داده‌های آموزشی و معماری سیستم، دارایی‌های اصلی و محرمانه شرکت‌های فناوری هستند و تحت حمایت نظام حقوقی قرار دارند. الزام به افشای کامل این اطلاعات می‌تواند با مقاومت شدید صنعت مواجه شده و پیشنهاد مقاله را غیرعملی جلوه دهد. برای حل این تعارض و ایجاد موازنه میان شفافیت برای حمایت از کودک و منفعت مشروع شرکت، می‌توان از مدل‌های اجرایی زیر که در تجربیات بین‌المللی نیز به کار رفته‌اند، الهام گرفت:

دسترسی طبقه‌بندی شده: در این مدل، خلاصه‌ای از نتایج ارزیابی و اقدامات کاهشی به‌صورت عمومی منتشر می‌شود؛ اما جزئیات فنی کامل، کد منبع و داده‌های آموزشی، صرفاً در اختیار نهاد ناظر متخصص و تحت توافق‌نامه‌های سخت‌گیرانه عدم افشا قرار می‌گیرد تا امکان راستی‌آزمایی فراهم شود (*Suarez & Haie, 2025*).

حسابرسی توسط شخص ثالث معتمد: شرکت‌ها به جای افشای مستقیم اطلاعات به نهاد دولتی، الگوریتم خود را در اختیار حسابرسان فنی–حقوقی مستقل و مورد تأیید نهاد ناظر قرار می‌دهند. این حسابرسان انطباق سیستم با استانداردها را بررسی کرده و گزارش تأیید یا عدم تأیید را به نهاد ناظر ارائه می‌دهند.

استثنای منافع عمومی: باید چهارچوب حقوقی مشخصی تدوین شود که بر اساس آن، در شرایطی که ریسک آسیب به حقوق بنیادین کودکان بسیار بالا و جدی باشد (مانند ترویج نظام‌مند محتوای خودآزاری)، منافع عمومی جامعه بر حفظ اسرار تجاری اولویت یافته و الزام به شفافیت کامل موجه گردد (*Hattingh, 2025*).

نتیجه‌گیری

ظهور هوش مصنوعی، حقوق کودک را با چالشی بی‌سابقه و الگوواره‌ای نوین مواجه کرده

است. آسیب‌های الگوریتمی که به‌صورت فعالانه، شخصی‌سازی‌شده و غیرشفاف عمل می‌کنند، چهارچوب‌های حقوقی سنتی را که بر کنترل محتوا و مسئولیت‌های پسینی استوارند، ناکارآمد ساخته‌اند. این پژوهش نشان داد که الگوریتم‌های توصیه‌گر با بهره‌گیری از ضعف‌های تکاملی مغز کودک در بستر اقتصاد توجه، تهدیداتی عمیق برای سلامت روان و اراده آزاد کودکان ایجاد می‌کنند که مستقیماً با مقاصد بنیادین شریعت در تعارض است.

درحالی‌که نظام حقوقی ایران فاقد قوانین خاص برای این حوزه است، تحلیل دکترینال نشان داد که مبانی استوار فقه امامیه و اصول حقوقی داخلی، ظرفیت بالایی برای بومی‌سازی یک چهارچوب حمایتی نوین دارند. با تفسیری پویا و متناسب با پیچیدگی‌های عصر دیجیتال، می‌توان از قواعدی چون «تسبیب» (با اقوی دانستن پلتفرم)، «لاضرر» (به‌عنوان تکلیف پیشگیرانه)، «مسئولیت ناشی از عیب محصول» و به‌ویژه «اصل احتیاط» برای تحمیل مسئولیت بر سکوها و گذار به یک نظام پیشگیرانه بهره برد.

بااین‌حال، اتکای صرف به تفسیر قضائی کافی نیست. این پژوهش با الهام از مدل‌های تطبیقی (به‌ویژه مدل «وظیفه مراقبت» بریتانیا و «ارزیابی تأثیر» آمریکا) و با اتکا به نظریه عدالت رویه‌ای، پیشنهاد می‌کند که ایران به‌جای تمرکز بر کنترل «خروجی‌های» الگوریتم، «فرایند» طراحی و توسعه آن را از طریق تعریف قانونی «وظیفه مراقبت الگوریتمی» و الزام به «ارزیابی تأثیر الگوریتمی بر کودک» تنظیم کند. این رویکرد، مسئولیت را به جایی منتقل می‌کند که قدرت و دانش برای پیشگیری از آسیب وجود دارد.

درنهایت، این پژوهش گامی در مسیر تدوین «فقه فناوری» و «فقه حکمرانی» است؛ حوزه‌ای که می‌کوشد با استفاده از اصول پایدار فقهی، برای پیچیده‌ترین مسائل فناورانه معاصر، راه‌حل‌های عادلانه، کارآمد و آینده‌نگر ارائه دهد. تطبیق هوشمندانه اصول حقوقی سنتی با واقعیت‌های فناورانه جدید می‌تواند راه را برای نوآوری مسئولانه هموار کرده و تضمین نماید که هوش مصنوعی در خدمت شکوفایی کودکان قرار گیرد، نه بهره‌کشی از آنها. پژوهش‌های آتی باید به ابعاد دیگری از این چالش، ازجمله سازوکارهای جبران خسارت جمعی و نقش نهادهای تنظیم‌گر بخشی بپردازند. حرکت به‌سوی یک نظام حقوقی

کارآمد برای هوش مصنوعی نیازمند گفتگویی مستمر میان فقها، حقوق‌دانان، فناوران و سیاست‌گذاران است. این پژوهش نشان داد که روش‌شناسی «نوآوری در حقوق اسلامی» از طریق بازخوانی و انطباق‌پذیری اصول بنیادین فقهی با واقعیت‌های نوظهور، ظرفیتی عظیم برای تولید دانش حقوقی کارآمد و بومی فراهم می‌آورد *(جلالی، ۱٤۰۰)*. امید است این مقاله، ضمن کمک به شکل‌گیری این گفتگوی ضروری، الهام‌بخش پژوهش‌های آتی در مسیر تکامل «فقه حکمرانی فناوری» باشد.

منابع

امیدی‌فرد، عبدالله (۱۳۸۵). سیری در پیشینه قاعده غرر. *مجله پژوهشهای فقهی دانشگاه تهران*، ۲(٤ شماره پیاپی ۱٦۷۹).

انصاری، باقر (۱٤۰۱). مطالعه حقوقی تبعیض الگوریتمی. *دانش حقوق عمومی*، ۱۱(۳۸)، ۱٤۷–۱۷۸.

جلالی، حسین (۱٤۰۰). تبارشناسی و راهبردهای گفتمان نوآوری در حقوق اسلامی. *تحقیقات حقوق خصوصی و کیفری (دانشنامه حقوق و سیاست)*، *۱۷*(۵۰)، ۲۹–۵٦.

جوادی، علی؛ شجاعی، ستاره و ده‌بزرگی، سارا (۱٤۰۳). نقش سبک‌های فرزندپروری در پیش‌بینی اعتیاد به اینترنت در کودکان با اختلال نارسایی توجه/بیش‌فعالی. *فصلنامه اختلال‌های هیجانی و رفتاری، دانشگاه شیراز*، ۱(شماره ۱ پیاپی ۱).

حسام، ابوالفضل و غلامعلی‌زاده، محمد (۱٤۰۲). مسئولیت مدنی بسترهای مجازی آنلاین در قبال اَعمال کاربران. *فصلنامه حقوق اسلامی، پژوهشگاه فرهنگ و اندیشه اسلامی*، ۲۰(۷۹)، ۱۲۷–۱٤۵.

حسینی مقدم، سیدحسن؛ ایوبی، ستاره و طالقان غفاری، مهدی (۱٤۰۲). مسئولیت مدنیِ فروشگاه‌های اینترنتی در حقوق ایران و مطالعۀ تطبیقی موردی در اتحادیۀ اروپا. *پژوهش حقوق خصوصی*، ۱۲(٤٤)، ۲۵۵–۲۸٤.

خوبیاری، حامد (۱۳۹۷). بررسی احتیاط در معنای فقهی به‌مثابه اصل زیست‌محیطی احتیاط. *فصلنامه پژوهش‌های حقوق تطبیقی عدل و انصاف*، ۱(۳)، ۲۴–۴۱.

ذوالقدر، هدایت‌الله (۱۴۰۳). بررسی تطبیقی مسئولیت مدنی دسترسی‌دهندگان اینترنتی، میزبانان اینترنتی و تولیدکنندگان محتوا: مطالعه قوانین ایران و آلمان در فضای مجازی. *حقوق و مطالعات نوین*، ۵(۳ (پیاپی ۱۷))، ۲۲-۱.

رجبی، عبداله (۱۴۰۳). نرم‌افزار متن‌باز؛ حقوق مالکیت فکری یا حقوق قراردادها. *مجله حقوقی دادگستری*، ۸۸(۱۲۶)، ۹۱–۱۱۴.

رضایی، فاطمه؛ زرینی، لیلا و راعی، مسعود (۱۴۰۳). حقوق سلامت کودک و فضای مجازی. در *سومین همایش ملی تحکیم و تعالی بنیان خانواده*.

شورای عالی فضای مجازی (۱۴۰۰). صیانت از کودکان و نوجوانان در فضای مجازی.

عربیان، اصغر و موسی نتاج، عبدالرزاق (۱۴۰۱). مفاهیم اصلی و مبنای مسئولیت عرضه‌کنندگان کالا براساس قانون حمایت از مصرف‌کنندگان مصوب ۱۳۸۸ و مقایسه آن با دستورالعمل اتحادیه اروپا. *فصلنامه تحقیق و توسعه در حقوق تطبیقی*، ۵(۱۴)، ۱۳۲–۱۵۸.

غریبه، علی؛ پناهی، هادی و پاشازاده، حسن (۱۳۹۹). واکاوی ماهیت نرم‌افزار الکترونیکی هوشمند نمایندگی الکترونیکی) در انعقاد قرارداد و پیامدهای اجتماعی آن. *فصلنامه جامعه‌شناسی سیاسی ایران*، ۳(شماره ٤ پیاپی ۱۲)، ۶۶۲–۶۸۱.

غلامی، رضا (۱۴۰۱، ۲۱ تیر). مواجهه عقلانیت اسلامی با فناوری هوش مصنوعی. https://r-gholami.ir/?p=2790

غمامی، سیدمحمدمهدی (۱۴۰۳). تنظیم هوش مصنوعی به‌منظور تأمین و تضمین حقوق عامه. *درگاه‌های حقوق قضایی*، (۱۰۸)، ۱۲۹-۱۰۱.

کرمدار، کیوان (۱۴۰۳). *مسئولیت مدنی پلتفرم‌های آنلاین در قبال محتوای منتشر شده توسط کاربران*. مقاله ارائه‌شده در اولین همایش بین‌المللی ایده‌های تحول‌آفرین.

مجلس شورای اسلامی (۱۳۸۸). قانون حمایت از حقوق مصرف کنندگان. ش. ۱۳/۳۶۹۶۵.

مجلس شورای اسلامی (۱۳۹۹). قانون حمایت از اطفال و نوجوانان.

محقق داماد، سیدمصطفی (۱۳۹۵). *قواعد فقه: بخش مدنی (مالکیت - مسئولیت)* (ویرایش

۲، ص ۳۰۱). مرکز نشر علوم اسلامی. (نشر اثر اصلی ۱۳٦۳)

محمدرضایی، معصومه و ریاحی، ناهید (۱٤۰۲). *بررسی فقهی اقوی بودن سبب از مباشر در قانون مجازات اسلامی* مصوب ۱۳۹۲. مقاله ارائه‌شده در اولین کنفرانس بین‌المللی پژوهش در حقوق و علوم اجتماعی.

موسوی بجنوردی، محمد (۱۳۷۹). *قواعد فقهیه* (ج۱). مؤسسه تنظیم و نشر آثار امام خمینی (ره)، مؤسسه چاپ و نشر عروج.

نجفیان رضوی، مهدی؛ شیخ الاسلامی، عباس و هژبر ساداتی، هانیه (۱٤۰۱). حقوق دفاعی متهم در پرتو موازین فقهی و بخشنامه‌های قضایی. *فصلنامه فقه جزای تطبیقی*، ۲(۳)، ۱–۹.

هیئت وزیران (۱۳۸۳). آیین‌نامه اجرایی مواد (۲) و (۱۷) قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای. ج. ۲۱۱۸۵ت۲٦۰۸۹ه.

واثقی، محسن (۱٤۰۲). علوم اعصاب و فناوری‌های عصبی در ترازوی حقوق بشر. *دانشگاه تهران-مطالعات حقوق تطبیقی*، ۱٤(۲)، ۱۰٦۹–۱۰۸۸.

بجنوردی، حسن (۱٤۱۹ق). *القواعد الفقهیة*. (مهدی مهریزی و محمدحسین درایتی، محققان) قم: نشر الهادی.

خمینی، روح‌الله (۱٤۱۵ق). *بدائع الدرر فی قاعدة نفی الضرر*. مؤسسه تنظیم و نشر آثار امام خمینی (ره).

عودة، جاسر (۱٤۳۲ق). *مقاصد الشرعیة کفلسفة للتشریع الإسلامی: رؤیة منظومیة*. المعهد العالمی للفکر الاسلامی.

مکارم شیرازی، ناصر (۱٤۱۰ق). *القواعد الفقهیة*. *بی‌جا:* مدرسه الامام امیرالمومنین (ع).

Aitken, Mhairi; Mahomed, Sabeehah; Briggs, Morgan; & Atabey, Ayça. (2023). How should children's rights be integrated into AI governance? Retrieved from https://www.unesco.org/en/articles/how-should-childrens-rights-be-integrated-ai-governance

Arain, Mariam; Haque, Maliha; Johal, Lina; Mathur, Puja; Nel, Wynand; Rais, Afsha; Sandhu, Ranbir; & Sharma, Sushil. (2013). Maturation of the adolescent brain. *Neuropsychiatric Disease and Treatment*, *9*, 449–461. https://doi.org/10.2147/NDT.S39776

Ausloos, Jef; Toh, Jill; & Giannopoulou, Alexandra. (2022, November 23). The case for collective action against the harms of data-driven technologies: To what extent are the GDPR's data rights an effective tool for enabling collective action?

Campbell, Jeff. (2025). AI Guardrails and Ethics: A Needed Paradigm Shift.

Carter, Ruth B.; & Marchant, Gary E. (2011). Principles-Based Regulation and Emerging Technology. In B. R. Allenby & J. R. Herkert (Eds.), (B. R. Allenby & J. R. Herkert, Eds.), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (pp. 157–166). Springer Netherlands. https://doi.org/10.1007/978-94-007-1356-7_10

European Parliament. 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) (2022).

European Union. Artificial Intelligence Act (2024).

Gallup. (2023, October 13). Teens Spend Average of 4.8 Hours on Social Media Per Day. Retrieved undefined 13, 1404, from https://news.gallup.com/poll/512576/teens-spend-average-hours-social-media-per-day.aspx

Galván, Adriana. (2010). Adolescent development of the reward system. *Frontiers in Human Neuroscience*, *4*. https://doi.org/10.3389/neuro.09.006.2010

Gillespie, Tarleton. (2014). The Relevance of Algorithms. In P. J. Boczkowski, K. A. Foot, & T. Gillespie (Eds.), (P. J. Boczkowski, K. A. Foot, & T. Gillespie, Eds.), *Media Technologies: Essays on Communication, Materiality, and Society* (pp. 185–193). The MIT Press. https://doi.org/10.7551/mitpress/9780262525374.001.0001

Habib, Zainal. (2025). Ethics of Artificial Intelligence in Maqāṣid Al-Sharīa's Perspective. *KARSA Journal of Social and Islamic Culture*, *33*(1), 105–134.

Hattingh, Julius. (2025). New AI Transparency Rules Have a Trade Secrets Problem. Retrieved from https://www.lawfaremedia.org/article/new-ai-transparency-rules-have-a-trade-secrets-problem

ICO. (2020). Introduction to the Children's Code. Retrieved from https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/

Kids Online Health and Safety Task Force. (2024). *Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry*. U.S. Department of Health and Human Services.

Kohl, Uta. (2024). Toxic recommender algorithms: immunities, liabilities and the regulated self-regulation of the Digital Services Act and the Online Safety Act. *Journal of Media Law*, *16*(2), 301–335. https://doi.org/10.1080/17577632.2024.2408912

Lu, Sylvia. (2024). Regulating Algorithmic Harms. *Law & Economics Working Papers* , 277.

Milano, Silvia; Taddeo, Mariarosaria; & Floridi, Luciano. (2020). Recommender systems and their ethical challenges. *AI & SOCIETY*, *35*(4), 957–967. https://doi.org/10.1007/s00146-020-00950-y

Napoli, Philip M. (2015). Social media and the public interest: Governance of news platforms in the realm of individual and algorithmic gatekeepers. *Telecommunications Policy*, *39*(9), 751–760.

NIST. Artificial Intelligence Risk Management Framework (AI RMF 1.0) (2023). https://doi.org/10.6028/NIST.AI.100-1

Noble, Safiya Umoja. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. NYU Press.

Ofcom. (2024). *The Causes and Impacts of Online Harm (Volume 2) – Ofcom Consultation Document*. Ofcom.

Office of the Surgeon General (OSG). (2023). *Social Media and Youth Mental Health: The U.S. Surgeon General's Advisory*. US Department of Health and Human Services.

Ojanen, Atte. (2025). Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act. *European Journal of Risk Regulation*, 1–16. https://doi.org/10.1017/err.2025.10024

Suarez, Christopher; & Haie, Anne-Gabrielle. (2025). How to Keep Trade Secrets Secret When Regulators Demand AI Transparency. Retrieved from https://www.corporatecomplianceinsights.com/how-to-keep-trade-secrets-secret-ai-transparency/

Tyler, Tom R. (2000). Social Justice: Outcome and Procedure. *International Journal of Psychology*, *35*(2), 117–125. https://doi.org/10.1080/002075900399411

UK Parliament. Online Safety Act 2023 (2023). Statute Law Database.

U.S. Congress. Algorithmic Accountability Act of 2023 (2023).