



فصلنامه علمی تخصصی حقوق وکیل دعاوی

وابسته به مرکز وکلای قوه قضاییه خراسان رضوی

دوره ۱، شماره ۴، زمستان ۱۴۰۴، صص: ۳۹-۱۹

چالش‌های حقوقی و اخلاقی هوش مصنوعی
در حفاظت از حریم خصوصی کودکان در فضای

مجازی

نویسنده:

نبی غلامی



URL: <https://www.vakildaavirazavi.ir/>

DOI: <https://doi.org/10.22034/vd.2026.2092801.1014>

COPYRIGHTS

© 2026 by the authors. Licensee Khorasan Razavi Center of Attorneys – Judiciary. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution 4.0 International (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/>)

چالش‌های حقوقی و اخلاقی هوش مصنوعی در حفاظت از حریم خصوصی کودکان در فضای مجازی

نبی غلامی

Email: n.gholami@tabaran.ac.ir

استادیار مؤسسه آموزش عالی تابران، مشهد، ایران

چکیده

پیشرفت شتابان فناوری‌های هوش مصنوعی و افزایش روزافزون حضور کودکان در فضای مجازی، ضرورت بهره‌مندی از این فناوری برای حفاظت از حریم خصوصی آنان را به یک مسئله حیاتی تبدیل کرده است. هوش مصنوعی با قابلیت‌های منحصربه‌فرد خود در تحلیل داده‌های حجیم، تشخیص الگوها و ارائه راه‌حل‌های هوشمندانه، می‌تواند نقش مؤثری در شناسایی و مقابله با تهدیدات حریم خصوصی کودکان ایفا کند. با این حال، کاربرد این فناوری در حوزه حساس حریم خصوصی کودکان، با چالش‌های حقوقی و اخلاقی متعددی مواجه است که از جمله می‌توان به جمع‌آوری و پردازش گسترده داده‌های شخصی، پروفایل‌سازی و تبلیغات هدفمند، نشت و سوءاستفاده از اطلاعات، عدم شفافیت الگوریتم‌ها، دشواری پاسخگویی حقوقی، خلأهای قانونی در نظام حقوقی ایران، مشکل صلاحیت قضائی فرامرزی و نبود مقررات صریح برای هوش مصنوعی اشاره کرد. این مقاله با رویکردی توصیفی-تحلیلی و با استفاده از منابع کتابخانه‌ای و اسنادی، ضمن تبیین مفاهیم بنیادین، به شناسایی و تحلیل جامع این چالش‌ها در پرتو قوانین داخلی ایران و اسناد بین‌المللی پرداخته است. یافته‌های پژوهش نشان می‌دهد که علی‌رغم وجود برخی قوانین پراکنده، خلأهای قانونی عمیقی در نظام حقوقی ایران وجود دارد و هماهنگی لازم با استانداردهای بین‌المللی صورت نگرفته است. مقاله در پایان، راهکارهایی نظیر تصویب قانون جامع حفاظت از داده‌های کودکان، افزایش شفافیت الگوریتم‌ها، تقویت همکاری‌های بین‌المللی، ایجاد نهادهای نظارتی مستقل و توانمندسازی والدین و کودکان ارائه می‌دهد.

واژگان کلیدی: هوش مصنوعی، حریم خصوصی کودکان، فضای مجازی، چالش‌های حقوقی، چالش‌های اخلاقی، قانون جرایم رایانه‌ای، کنوانسیون حقوق کودک، GDPR، COPPA.

بیان مسئله و ضرورت تحقیق

در عصر دیجیتال کنونی، افزایش بی‌سابقه استفاده از اینترنت و فضای مجازی توسط کودکان، به یکی از مهم‌ترین مسائل اجتماعی، فرهنگی و حقوقی تبدیل شده است. کودکان به عنوان یکی از آسیب‌پذیرترین اقشار جامعه، با ورود به فضای مجازی با انبوهی از فرصت‌ها و تهدیدات روبرو می‌شوند. از یک سو، فضای مجازی امکان دسترسی به منابع آموزشی گسترده، ارتباط با همسالان و شکوفایی خلاقیت را فراهم می‌کند و از سوی دیگر، تهدیدات جدی مانند دسترسی به محتوای نامناسب، به اشتراک‌گذاری اطلاعات شخصی، سوءاستفاده از داده‌ها، آزار و اذیت آنلاین و نقض حریم خصوصی را به همراه دارد.

هوش مصنوعی به عنوان یکی از پیشرفته‌ترین فناوری‌های عصر حاضر، توانسته است تحولات شگرفی در حوزه‌های مختلف از جمله پزشکی، حمل و نقل، آموزش و امنیت ایجاد کند. این فناوری با قابلیت‌های چشمگیر خود در تحلیل داده‌های حجیم، شناسایی الگوهای پیچیده و ارائه راه‌حل‌های هوشمندانه، پتانسیل بالایی برای حفاظت از حریم خصوصی کودکان در فضای مجازی دارد. سیستم‌های مبتنی بر هوش مصنوعی می‌توانند به طور خودکار محتوای نامناسب را شناسایی و فیلتر کنند، رفتارهای مشکوک و تهدیدآمیز را تشخیص دهند و هشدارهای لازم را به والدین و مسئولان امنیتی ارسال نمایند. علاوه بر این، این فناوری می‌تواند در مدیریت رضایت والدین، شناسایی و جلوگیری از جمع‌آوری غیرمجاز داده‌ها و آموزش کودکان در مورد تهدیدات آنلاین نقش مؤثری ایفا کند. با این وجود، استفاده از هوش مصنوعی در حوزه حساس حریم خصوصی کودکان با چالش‌ها و مخاطرات جدی همراه است. یکی از مهم‌ترین نگرانی‌ها، حفظ حریم خصوصی خود داده‌های کودکان است. جمع‌آوری و پردازش داده‌های حساس کودکان، اگر با رعایت اصول اخلاقی و قانونی انجام نشود، می‌تواند به نقض حریم خصوصی و سوءاستفاده از اطلاعات منجر شود. از سوی دیگر، پیچیدگی و عدم شفافیت الگوریتم‌های هوش مصنوعی، پاسخگویی حقوقی در قبال تصمیمات و اقدامات این سیستم‌ها را با دشواری مواجه ساخته است. همچنین، خلأهای قانونی موجود در نظام حقوقی ایران، نبود مقررات صریح برای هوش مصنوعی، مشکل صلاحیت قضائی فرامرزی و دشواری شناسایی متخلفان در محیط دیجیتال، از دیگر چالش‌های اساسی در این حوزه به شمار می‌روند.

با توجه به پیچیدگی‌های روزافزون فضای مجازی و سرعت رشد فناوری‌های اطلاعاتی، استفاده از روش‌های سنتی برای حفاظت از حریم خصوصی کودکان کافی نیست و بهره‌مندی هوشمندانه از قابلیت‌های هوش مصنوعی، همراه با تدوین چارچوب‌های حقوقی و اخلاقی کارآمد، اجتناب‌ناپذیر است. این مقاله در صدد است تا با رویکردی جامع و دقیق، به شناسایی و تحلیل چالش‌های حقوقی و اخلاقی فراروی استفاده از هوش مصنوعی در حفاظت از حریم خصوصی کودکان در فضای مجازی بپردازد و راهکارهای عملی برای برون‌رفت از این چالش‌ها ارائه نماید.

پرسش اصلی پژوهش این است که مهم‌ترین چالش‌های حقوقی و اخلاقی هوش مصنوعی در حفاظت از حریم خصوصی کودکان کدامند و چه راهکارهایی برای مقابله با این چالش‌ها وجود دارد؟

پیشینه تحقیق

موضوع حریم خصوصی کودکان در فضای مجازی و نقش هوش مصنوعی در آن، در سال‌های اخیر مورد توجه پژوهشگران و نهادهای بین‌المللی قرار گرفته است. از جمله مهم‌ترین پژوهش‌های انجام شده در این زمینه می‌توان به موارد زیر اشاره کرد:

طلائی زواره در مقاله‌ای با عنوان «حریم خصوصی در عصر هوش مصنوعی» به تحلیل تعادل بین بهره‌برداری از فناوری‌های هوش مصنوعی و حفاظت از حقوق حریم خصوصی افراد پرداخته و پیشنهاداتی برای سیاستگذاران ارائه داده است. هیئت تحریریه فصلنامه ره‌آورد نور در مقاله‌ای با عنوان «چالش‌های امنیتی و حریم خصوصی در هوش مصنوعی»، با ارائه مثال‌ها و نمونه‌های متعدد، به تبیین چالش‌های موجود در حوزه امنیتی و حریم خصوصی هوش مصنوعی پرداخته است. قربانی‌فر و محسن‌پور در مقاله‌ای با عنوان «حریم خصوصی کودکان در فضای مجازی»، به بررسی جایگاه حفظ حریم خصوصی کودکان در حقوق داخلی و اسناد بین‌المللی و حدود و ثغور حق نظارت والدین پرداخته‌اند.

پورمسجدیان و ابراهیمی در مقاله‌ای با عنوان «واکاوی حقوقی حمایت از حریم خصوصی کودک در فضای مجازی با نگاهی به قوانین ایران و معاهدات بین‌المللی»، به بررسی قوانین و مقررات موجود در ایران، به ویژه قانون حمایت از اطفال و نوجوانان، و کنوانسیون‌ها و معاهدات بین‌المللی در این زمینه پرداخته‌اند. فرامرزیانی، سلطانی‌فر و مظفری در مقاله‌ای با عنوان «طراحی الگوی راهکارهای حمایت از حریم خصوصی کودکان در فضای مجازی»، به تدوین راهکارهای موجود در شاخه‌های مختلف اجتماعی، فرهنگی، حقوقی و آموزشی پرداخته‌اند. علی‌احمدی جشفقانی و شوق‌نیا در مقاله‌ای با عنوان «رعایت حریم خصوصی در فضای مجازی: مورد مطالعه حقوق ایران»، به بررسی قوانین و مقررات مربوط به حریم خصوصی در حقوق ایران پرداخته‌اند.

با وجود این پژوهش‌ها، همچنان خلأ تحقیقی جامع و منسجمی در زمینه شناسایی و تحلیل همه‌جانبه چالش‌های حقوقی و اخلاقی هوش مصنوعی در حفاظت از حریم خصوصی کودکان در فضای مجازی، به ویژه با رویکرد تطبیقی و با تأکید بر قوانین ایران، احساس می‌شود که این مقاله در صدد پر کردن این خلأ است.

اهداف و روش تحقیق

هدف اصلی این مقاله، بررسی و تحلیل جامع چالش‌های حقوقی و اخلاقی فراروی استفاده از هوش مصنوعی در حفاظت از حریم خصوصی کودکان در فضای مجازی و ارائه راهکارهای عملی برای رفع این چالش‌هاست. اهداف

فرعی شامل تبیین مفاهیم بنیادین، شناسایی انواع چالش‌ها و تحلیل قوانین داخلی و بین‌المللی مرتبط است. روش تحقیق در این مقاله، توصیفی-تحلیلی و با استفاده از منابع کتابخانه‌ای و اسنادی است. داده‌های مورد نیاز از طریق مطالعه قوانین، مقررات، کنوانسیون‌ها، مقالات علمی و کتب مرتبط گردآوری و با رویکردی تحلیلی و انتقادی مورد بررسی قرار گرفته‌اند.

مبانی نظری و مفاهیم بنیادین

چیستی و کارکردهای هوش مصنوعی

تعریف هوش مصنوعی

هوش مصنوعی یکی از شاخه‌های مهم و پویای علوم کامپیوتر است که به طراحی و توسعه سیستم‌هایی اشاره دارد که قادر به انجام وظایفی هستند که به طور معمول نیازمند هوش انسانی می‌باشند. این وظایف شامل یادگیری، استدلال، درک زبان طبیعی، تصمیم‌گیری و حل مسائل پیچیده است. به عبارت دیگر، هوش مصنوعی به دنبال شبیه‌سازی توانایی‌های شناختی انسان در ماشین‌ها است تا بتوانند وظایف را به صورت خودکار و هوشمندانه انجام دهند.

هدف اصلی از هوش مصنوعی، ایجاد ماشین‌هایی است که بتوانند از داده‌ها و تجربیات گذشته خود یاد بگیرند، الگوها را شناسایی کنند و با تحلیل و پردازش اطلاعات، به تصمیمات بهینه دست یابند. این سیستم‌ها می‌توانند از داده‌های متنوعی مانند تصاویر، متون، صداها و اطلاعات حسگرهای مختلف استفاده کنند تا پیش‌بینی‌های دقیقی ارائه دهند. برای مثال، یک سیستم تشخیص تصویر می‌تواند با مشاهده تعداد زیادی از تصاویر برچسب‌گذاری شده، ویژگی‌هایی مانند شکل‌ها، رنگ‌ها و بافت‌ها را شناسایی کرده و از آن برای شناسایی تصاویر جدید استفاده نماید. این توانایی یادگیری از تجربه، به هوش مصنوعی اجازه می‌دهد که در طول زمان و با استفاده مداوم، عملکرد خود را بهبود بخشد.

انواع هوش مصنوعی

هوش مصنوعی به طور کلی به دسته‌بندی‌های مختلفی تقسیم می‌شود که هر یک توانایی‌ها و کاربردهای خاص خود را دارند:

الف) هوش مصنوعی ضعیف یا محدود: به سیستم‌هایی اطلاق می‌شود که تنها برای انجام یک وظیفه خاص طراحی شده‌اند و نمی‌توانند فراتر از آن عمل کنند. این نوع هوش مصنوعی به دنبال ایجاد سیستم‌هایی است که قادر به حل مسائل خاص هستند، اما توانایی انجام وظایف گسترده مشابه انسان‌ها را ندارند. نمونه‌های بارز هوش مصنوعی ضعیف عبارتند از دستیارهای صوتی مانند سیری و الکسا که تنها می‌توانند در حوزه‌هایی مانند

پاسخ به سوالات ساده، انجام فرمان‌های صوتی و تنظیم یادآوری‌ها عمل کنند.

ب) هوش مصنوعی قوی یا عمومی: به سیستمی اطلاق می‌شود که قادر است همانند انسان‌ها، وظایف مختلف را در زمینه‌های گوناگون انجام دهد. هوش مصنوعی عمومی در واقع مدلی مشابه هوش انسانی است که می‌تواند در تمامی حوزه‌ها به تفکر، تصمیم‌گیری و یادگیری بپردازد. هوش مصنوعی عمومی هنوز به طور کامل تحقق نیافته است و عمدتاً در مرحله تحقیقات و توسعه قرار دارد.

ج) هوش مصنوعی رباتیک: به سیستم‌های هوش مصنوعی اطلاق می‌شود که در ربات‌ها به کار گرفته می‌شوند. این ربات‌ها می‌توانند محیط اطراف خود را حس کنند و با آن تعامل داشته باشند. ربات‌های جراحی که در عملیات پزشکی کمک می‌کنند، نمونه‌ای از هوش مصنوعی رباتیک هستند.

فناوری‌های مرتبط با هوش مصنوعی

هوش مصنوعی به عنوان یک حوزه گسترده، شامل فناوری‌ها و زیرشاخه‌های متعددی است:

یادگیری ماشین: یکی از زیرمجموعه‌های اصلی هوش مصنوعی است که به سیستم‌ها این امکان را می‌دهد تا از داده‌ها یاد بگیرند و الگوهای پنهان را شناسایی کنند، بدون اینکه برای هر وظیفه خاص نیاز به کدنویسی دقیق داشته باشند.

یادگیری عمیق: نوعی پیشرفته‌تر از یادگیری ماشین است که در آن از شبکه‌های عصبی مصنوعی چندلایه برای پردازش داده‌ها استفاده می‌شود.

پردازش زبان طبیعی: یکی از شاخه‌های هوش مصنوعی است که به درک زبان انسان توسط ماشین‌ها اشاره دارد.

بینایی کامپیوتری: شاخه‌ای از هوش مصنوعی است که به ماشین‌ها امکان می‌دهد تا تصاویر و ویدئوها را درک و تفسیر کنند.

مفهوم و ابعاد حریم خصوصی

تعریف حریم خصوصی

حریم خصوصی به مفهوم حفاظت از اطلاعات و داده‌های شخصی فرد است که شامل هرگونه جزئیاتی از زندگی شخصی، رفتار، افکار و ارتباطات افراد می‌شود. به عبارت ساده‌تر، حریم خصوصی به حق هر فرد برای کنترل اطلاعات و جزئیات زندگی شخصی خود و تصمیم‌گیری در مورد اینکه کدام اطلاعات باید به اشتراک گذاشته شوند و کدام باید محفوظ بمانند، اشاره دارد. این مفهوم یکی از اصول اساسی حقوق بشر است که در بسیاری از کشورهای جهان به رسمیت شناخته شده است.

ابعاد حریم خصوصی

حریم خصوصی ابعاد مختلفی دارد که می‌توان آن را به چند دسته تقسیم کرد:

حریم خصوصی اطلاعاتی: این بعد از حریم خصوصی به داده‌ها و اطلاعات شخصی فرد مربوط می‌شود، نظیر اطلاعات مالی، وضعیت سلامتی، شماره‌های تماس، آدرس‌ها، تاریخ تولد و دیگر جزئیات شناسایی.

حریم خصوصی ارتباطات: این بعد شامل حفاظت از مکالمات، پیام‌ها، ایمیل‌ها، تماس‌های تلفنی و سایر روش‌های ارتباطی است.

حریم خصوصی فیزیکی: این بعد به محافظت از فضای فیزیکی و جسمی فرد مربوط می‌شود.

حریم خصوصی در فضای مجازی: با گسترش فضای دیجیتال و اینترنت، حریم خصوصی آنلاین به موضوعی مهم تبدیل شده است.

اهمیت و جایگاه حریم خصوصی کودکان

حریم خصوصی کودکان به دلیل آسیب‌پذیری خاص این گروه سنی، از اهمیت دوچندانی برخوردار است. کودکان به دلیل کمبود تجربه، عدم بلوغ عقلانی و جسمی، توانایی درک کامل خطرات فضای مجازی و عواقب استفاده نادرست از داده‌های شخصی خود را ندارند. بنابراین، حمایت از حریم خصوصی کودکان نه تنها یک الزام اخلاقی، بلکه یک وظیفه قانونی برای دولت‌ها، نهادهای بین‌المللی، پلتفرم‌های آنلاین و والدین است. در بسیاری از کشورها، قوانین خاصی برای محافظت از حریم خصوصی کودکان در فضای دیجیتال وضع شده است که از جمله می‌توان به قانون COPPA در ایالات متحده و مقررات GDPR در اتحادیه اروپا اشاره کرد.

چیستی و ویژگی‌های فضای مجازی

تعریف فضای مجازی

فضای مجازی محیطی دیجیتال و آنلاین است که افراد می‌توانند در آن از طریق شبکه‌های اینترنتی، ارتباط برقرار کنند، اطلاعات به اشتراک بگذارند و به منابع مختلف دسترسی پیدا کنند. این فضا به نوعی یک دنیای مجازی است که در آن تعاملات انسانی، فعالیت‌های تجاری، آموزشی، اجتماعی و سرگرمی از طریق ابزارها و پلتفرم‌های دیجیتال انجام می‌شود.

ویژگی‌های فضای مجازی

فضای مجازی دارای ویژگی‌های خاصی است که آن را از فضای فیزیکی متمایز می‌کند: ناشناسی که در آن افراد می‌توانند به صورت ناشناس فعالیت کنند، دسترسی پذیری جهانی که امکان دسترسی از هر نقطه‌ای از جهان را

فراهم می‌کند. استقلال از زمان و مکان که به افراد اجازه می‌دهد در هر زمان و مکانی به فضای مجازی دسترسی داشته باشند. گستردگی و تنوع که حاوی انواع اطلاعات و محتوای متنوع است. تعاملات غیرمستقیم که تعاملات معمولاً به صورت غیرمستقیم و از طریق واسطه‌های دیجیتال انجام می‌شود.

تهدیدات فضای مجازی برای کودکان

فضای مجازی علی‌رغم مزایای فراوان، تهدیدات جدی برای کودکان به همراه دارد که از جمله مهم‌ترین آنها می‌توان به موارد زیر اشاره کرد: دسترسی به محتوای نامناسب مانند محتوای خشونت‌آمیز، پورنوگرافی و محتوای توهین‌آمیز. به اشتراک‌گذاری اطلاعات شخصی بدون آگاهی از عواقب. آزار و اذیت آنلاین که می‌تواند آسیب‌های روانی جدی به کودکان وارد کند. سوءاستفاده جنسی آنلاین از طریق تولید و توزیع محتوای پورنوگرافی کودکان. نقض حریم خصوصی از طریق جمع‌آوری و استفاده غیرمجاز از داده‌های شخصی کودکان.

چالش‌های حقوقی و اخلاقی هوش مصنوعی در حفاظت از حریم خصوصی کودکان

جمع‌آوری و پردازش گسترده داده‌های شخصی کودکان

هوش مصنوعی برای عملکرد بهینه و ارائه خدمات دقیق و شخصی‌سازی شده، نیازمند داده‌های حجیم و متنوع است. این داده‌ها ممکن است شامل اطلاعات شخصی کودکان از جمله نام، سن، آدرس، شماره تلفن، آدرس ایمیل، موقعیت جغرافیایی، تاریخچه جستجو، رفتار آنلاین، تصاویر، ویدئوها و حتی اطلاعات بیومتریک مانند اثر انگشت یا تشخیص چهره باشد. جمع‌آوری و پردازش گسترده این داده‌ها، اگر با رعایت اصول اخلاقی و قانونی همراه نباشد، یکی از بزرگ‌ترین چالش‌های حقوقی و اخلاقی در حوزه هوش مصنوعی و حریم خصوصی کودکان محسوب می‌شود.

داده‌هایی که از کودکان جمع‌آوری می‌شود، ممکن است به صورت مستقیم (مانند ثبت نام در یک بازی آنلاین یا یک پلتفرم اجتماعی) یا غیرمستقیم (از طریق ردیابی فعالیت‌های آنلاین یا استفاده از کوکی‌ها) جمع‌آوری شوند. این اطلاعات می‌تواند برای تبلیغات هدفمند، پروفایل‌سازی کاربران، تحلیل داده‌ها و حتی برای کسب‌وکارهای تجاری استفاده شود. یکی از چالش‌های اصلی در پردازش داده‌های شخصی کودکان، خطر نقض حریم خصوصی و سوءاستفاده از داده‌ها است. به عنوان مثال، بسیاری از پلتفرم‌ها و شرکت‌ها ممکن است از داده‌های کودکان برای تبلیغات هدفمند استفاده کنند که می‌تواند بر انتخاب‌های خرید، تصمیمات مصرفی و حتی سلامت روانی کودکان تأثیر بگذارد.

پروفایل‌سازی کودکان یکی دیگر از تهدیدات جدی است. با استفاده از داده‌های شخصی، شرکت‌ها می‌توانند پروفایل‌های دیجیتالی از کودکان ایجاد کنند که شامل علایق، رفتارها و ویژگی‌های شخصیتی آن‌ها باشد.

این پروفایل‌ها می‌توانند برای ایجاد محتوای شخصی‌سازی شده یا تبلیغات هدفمند استفاده شوند، که ممکن است منجر به نفوذ به زندگی خصوصی کودکان و سوءاستفاده‌های تجاری شود. یکی دیگر از خطرات، دسترسی غیرمجاز به داده‌ها است. در صورت نقص امنیتی یا نفوذ هکرها، داده‌های شخصی کودکان ممکن است در معرض خطر قرار گیرد و توسط مجرمان سایبری برای سوءاستفاده‌های مالی یا آزار و اذیت آنلاین استفاده شوند. از دیدگاه حقوقی، این چالش با اصول بنیادین حقوق حریم خصوصی مانند اصل حداقل‌سازی داده‌ها و اصل هدف‌مندی در تعارض است. اصل حداقل‌سازی داده‌ها ایجاب می‌کند که فقط داده‌های ضروری برای هدف معین جمع‌آوری شوند و اصل هدف‌مندی نیز تصریح می‌کند که داده‌ها نباید برای اهدافی غیر از آنچه که در زمان جمع‌آوری اعلام شده است، استفاده شوند. متأسفانه، در بسیاری از موارد، پلتفرم‌های آنلاین این اصول را نادیده می‌گیرند.

پروفایل‌سازی و تبلیغات هدفمند علیه کودکان

پروفایل‌سازی و تبلیغات هدفمند علیه کودکان یکی از تهدیدات جدی برای حریم خصوصی و امنیت آنلاین کودکان در دنیای دیجیتال است. با گسترش استفاده از اینترنت و شبکه‌های اجتماعی، پروفایل‌سازی و جمع‌آوری داده‌های شخصی کودکان به یک نگرانی بزرگ تبدیل شده است. پروفایل‌سازی به معنای ایجاد پروفایل‌های دیجیتال از کودکان است که بر اساس اطلاعات شخصی، ترجیحات، رفتار آنلاین و عادات خرید آن‌ها ساخته می‌شود. این پروفایل‌ها می‌توانند به طور مستقیم بر تبلیغات هدفمند تأثیر بگذارند و کودک را در معرض تبلیغاتی قرار دهند که ممکن است بر تصمیمات خرید، علاقه‌ها و رفتارهای آن‌ها تأثیر بگذارد.

پروفایل‌سازی برای کودکان می‌تواند به روش‌های مختلفی انجام شود. این داده‌ها می‌توانند شامل اطلاعات شخصی مانند نام، سن، آدرس ایمیل، شماره تلفن، اطلاعات جغرافیایی و حتی تصاویر یا ویدئوهای آپلود شده باشند. علاوه بر این، رفتار آنلاین کودکان شامل جستجوهای اینترنتی، فعالیت در شبکه‌های اجتماعی و تعاملات آنلاین نیز می‌تواند به جمع‌آوری داده‌ها کمک کند. الگوریتم‌های هوش مصنوعی و یادگیری ماشین می‌توانند با تحلیل داده‌های جمع‌آوری شده، پروفایل‌های دقیق و شخصی‌سازی شده برای کودکان ایجاد کنند.

یکی از بزرگ‌ترین تهدیدات ناشی از پروفایل‌سازی کودکان، استثمار تجاری و آسیب به حریم خصوصی آن‌ها است. پروفایل‌های دیجیتال کودکان می‌توانند به طور مداوم به روزرسانی شوند و از این داده‌ها برای تبلیغات هدفمند و شخصی‌سازی محتوای آنلاین استفاده شود. در حالی که این تبلیغات ممکن است به ظاهر مفید به نظر برسند، اما می‌توانند بر تصمیمات کودکان تأثیر بگذارند و باعث فشارهای مالی و روانی بر آنان شوند. تبلیغات هدفمند می‌تواند باعث ایجاد وابستگی به مصرف و تقویت رفتارهای نادرست در کودکان شود. به عنوان مثال، تبلیغات برای محصولات غیرضروری مانند بازی‌ها، خوراکی‌های ناسالم و کالاهای گران‌قیمت می‌تواند کودکان را به

خرید محصولات نامناسب یا پرهزینه ترغیب کند.

از منظر حقوقی و اخلاقی، پروفایل سازی و تبلیغات هدفمند علیه کودکان با اصولی مانند حق بر حریم خصوصی، حق بر انتخاب آگاهانه و اصل منع بهره‌کشی از کودکان در تعارض است. کودکان به دلیل عدم بلوغ فکری و تجربه کافی، توانایی تشخیص ماهیت فریبنده و تأثیرگذار تبلیغات هدفمند را ندارند و به راحتی می‌توانند تحت تأثیر این تبلیغات قرار گیرند.

جمع‌آوری خودکار و هوشمند داده‌ها

جمع‌آوری خودکار و هوشمند داده‌ها یکی از ویژگی‌های بارز فناوری‌های مدرن است که به ویژه با استفاده از هوش مصنوعی و الگوریتم‌های یادگیری ماشین در دنیای دیجیتال امروز در حال رشد است. این فرآیند به جمع‌آوری داده‌ها به صورت اتوماتیک و بدون نیاز به دخالت مستقیم انسان اشاره دارد. داده‌های شخصی، رفتاری، موقعیت جغرافیایی و تصاویر از جمله انواع داده‌هایی هستند که ممکن است از کاربران جمع‌آوری شوند. با استفاده از الگوریتم‌های پیشرفته، پلتفرم‌ها و اپلیکیشن‌ها می‌توانند اطلاعات وسیعی از کاربران خود به طور خودکار و بدون اطلاع کامل یا رضایت فرد جمع‌آوری کنند.

جمع‌آوری خودکار داده‌ها به این معنا است که سیستم‌ها قادرند به طور مستقل و بدون نیاز به اقدام انسان، داده‌ها را از منابع مختلف جمع‌آوری کنند. این ویژگی می‌تواند شامل داده‌های مرورگر اینترنتی، داده‌های خرید آنلاین، موقعیت مکانی و رفتار آنلاین کاربران باشد. به عنوان مثال، گوگل با استفاده از داده‌های جستجو، محل زندگی و ترجیحات جغرافیایی می‌تواند محتوای مرتبط با علایق فرد را به صورت خودکار نمایش دهد. از مزایای این نوع جمع‌آوری داده‌ها می‌توان به دقت بیشتر در ارائه خدمات، شخصی سازی تجربه کاربری و پیش بینی رفتار اشاره کرد.

در عین حال، جمع‌آوری خودکار و هوشمند داده‌ها تهدیدات زیادی به همراه دارد که می‌تواند بر حریم خصوصی افراد تأثیر منفی بگذارد. یکی از بزرگترین نگرانی‌ها، نشت اطلاعات شخصی است. هنگامی که داده‌های شخصی از کاربران به طور خودکار جمع‌آوری می‌شوند، این اطلاعات ممکن است به طور غیرمجاز در اختیار افراد یا نهادهای غیرمجاز قرار گیرد. همچنین، عدم آگاهی کاربران از نحوه جمع‌آوری و استفاده از داده‌هایشان، خطراتی را در خصوص استفاده غیرمجاز از اطلاعات ایجاد می‌کند. یکی دیگر از تهدیدات، پروفایل سازی است. در جمع‌آوری خودکار داده‌ها، سیستم‌ها ممکن است پروفایل‌های دقیق از کاربران بسازند که این پروفایل‌ها شامل اطلاعات حساس مانند ترجیحات شخصی، سلیقه‌ها و اطلاعات مالی باشد.

مشکل شفافیت الگوریتم‌ها

شفافیت الگوریتم‌ها یکی از چالش‌های اساسی در دنیای دیجیتال امروز است، به ویژه در زمینه حریم خصوصی و امنیت داده‌ها. با گسترش استفاده از هوش مصنوعی و الگوریتم‌ها در سیستم‌های مختلف مانند شبکه‌های اجتماعی، پلتفرم‌های آنلاین و خدمات دیجیتال، نیاز به شفافیت در نحوه عملکرد این الگوریتم‌ها بیشتر از هر زمان دیگری احساس می‌شود. الگوریتم‌ها به طور فزاینده‌ای در فرآیندهای تصمیم‌گیری در دنیای دیجیتال مورد استفاده قرار می‌گیرند. این الگوریتم‌ها می‌توانند در زمینه‌های مختلفی مانند تبلیغات هدفمند، مدیریت محتوا، تعیین رتبه‌بندی نتایج جستجو، تصمیم‌گیری‌های مالی و حتی تعیین تصمیمات قضائی کاربرد داشته باشند. با این حال، یکی از بزرگ‌ترین نگرانی‌ها، عدم شفافیت در عملکرد این الگوریتم‌ها است. بسیاری از کاربران از چگونگی عملکرد یا دلیل تصمیمات اتخاذ شده توسط این الگوریتم‌ها بی‌خبر هستند. شفافیت الگوریتم‌ها به معنای این است که کاربران و ذی‌نفعان باید بتوانند درک کنند که الگوریتم‌ها چگونه کار می‌کنند، داده‌هایی که مورد استفاده قرار می‌گیرند و چگونگی اتخاذ تصمیمات توسط این سیستم‌ها. این شفافیت باعث می‌شود که تصمیمات الگوریتمی به طور شفاف و قابل فهم برای همه افراد باشد، به ویژه در مواردی که این تصمیمات تأثیرات بزرگی بر زندگی افراد دارند، مانند اعتباردهی مالی یا آزادی بیان.

در عمل، بسیاری از الگوریتم‌ها به ویژه آن‌هایی که بر مبنای یادگیری ماشین و هوش مصنوعی هستند، به طور پیچیده و در بسته عمل می‌کنند. این پیچیدگی‌ها باعث می‌شود که درک نحوه عملکرد آن‌ها دشوار باشد و برخی از کاربران احساس کنند که در معرض بی‌عدالتی یا سوءاستفاده قرار دارند. برای مثال، یک الگوریتم تبلیغاتی ممکن است به طور هدفمند محتوای خاصی را به کاربران نمایش دهد، بدون اینکه آن‌ها از اصول دقیق شخصی‌سازی و انتخاب‌های پشت پرده آن آگاه باشند. این عدم شفافیت، به ویژه در مورد کودکان که توانایی درک پیچیدگی‌های فنی را ندارند، می‌تواند به نقض حقوق آن‌ها و تصمیمات ناعادلانه منجر شود.

پاسخگویی حقوقی و دشواری تعیین مسئولیت

یکی از مسائل مهمی که با استفاده از الگوریتم‌ها در فرآیندهای مختلف به وجود می‌آید، پاسخگویی حقوقی نسبت به تصمیمات اتخاذ شده توسط این سیستم‌ها است. اگر یک الگوریتم به اشتباه تصمیمی بگیرد که به ضرر فرد یا گروهی خاص باشد، سوال اساسی این است که چه کسی مسئول است؟ آیا شرکت توسعه‌دهنده الگوریتم باید پاسخگو باشد یا الگوریتم به طور خودکار باید مسئولیت تصمیمات خود را بپذیرد؟ پاسخگویی حقوقی الگوریتم‌ها باید شامل سازوکاری باشد که به کاربران امکان دهد اعتراض کنند و درخواست تجدید نظر در مورد تصمیمات الگوریتمی داشته باشند. در صورتی که الگوریتم‌ها به اشتباه منجر به تبعیض، نقض حقوق افراد یا تصمیمات نادرست شوند، لازم است که مسئولیت‌ها به طور شفاف مشخص شوند و حقوق افراد مورد حمایت قرار گیرد.

در این راستا، قوانینی مانند GDPR و COPPA به ویژه در زمینه حفاظت از داده‌های شخصی و حق اطلاع‌رسانی کاربران، تأکید دارند که افراد باید از نحوه جمع‌آوری و پردازش داده‌های خود آگاه باشند و همچنین می‌توانند در صورت وجود خطا یا سوءاستفاده، اعتراض کنند. با این حال، چالش اصلی این است که سیستم‌های هوش مصنوعی اغلب بسیار پیچیده و غیرشفاف هستند و تشخیص اینکه آیا یک تصمیم خاص نادرست یا تبعیض‌آمیز بوده است، نیازمند تخصص فنی بالاست که معمولاً برای کاربران عادی و حتی برای بسیاری از متخصصان حقوقی در دسترس نیست.

در زمینه حریم خصوصی کودکان، این چالش به مراتب پیچیده‌تر می‌شود. کودکان به دلیل سن کم و عدم درک کافی از مفاهیم حقوقی و فنی، توانایی اعتراض به تصمیمات الگوریتمی یا پیگیری حقوقی نقض حریم خصوصی خود را ندارند. بنابراین، پاسخگویی حقوقی در این حوزه باید با حمایت ویژه والدین، سرپرستان قانونی و نهادهای نظارتی همراه باشد. همچنین، ضروری است که توسعه‌دهندگان و پلتفرم‌ها، سیستم‌هایی را طراحی کنند که قابلیت توضیح‌دهی داشته باشند و بتوانند به زبان ساده و قابل فهم، دلایل تصمیمات خود را برای والدین و حتی کودکان توضیح دهند.

خلأهای قانونی در نظام حقوقی ایران

با وجود تصویب قوانین مختلف در ایران برای حمایت از حقوق کودکان در فضای مجازی و حفاظت از حریم خصوصی آن‌ها، هنوز خلأهای قانونی مهمی در این زمینه وجود دارد که نیازمند توجه و اصلاح است. این خلأها مانع از اجرای مؤثر برخی از این قوانین و محافظت کامل از کودکان در فضای دیجیتال می‌شوند. یکی از مهم‌ترین خلأهای قانونی در ایران، عدم وجود قانون جامع و مستقل برای حمایت از حقوق کودکان در فضای مجازی است. قوانین موجود مانند قانون جرایم رایانه‌ای، هرچند به جنبه‌هایی از این موضوع پرداخته‌اند، اما هیچ‌کدام به طور خاص و جامع به مشکلات و چالش‌های فضای دیجیتال و حریم خصوصی کودکان نپرداخته‌اند.

اگرچه قوانین موجود مانند قانون جرایم رایانه‌ای و قانون حمایت از کودکان به طور کلی محتوای مضر و غیراخلاقی را جرم‌انگاری کرده‌اند، اما در بسیاری از موارد این قوانین به اندازه کافی شفاف و مستقل در خصوص محتوای مضر برای کودکان نیستند. در عمل، تشخیص و فیلتر کردن محتوای مناسب برای کودکان می‌تواند چالش‌برانگیز باشد و قوانین موجود به طور مشخص الزامات لازم را برای فیلتر کردن دقیق محتوای مناسب در پلتفرم‌ها و سرویس‌های آنلاین ارائه نمی‌دهند.

در ایران، شبکه‌های اجتماعی بین‌المللی همچنان از محبوبیت بالایی برخوردارند، اما عدم وجود قوانین دقیق و شفاف برای نظارت بر استفاده کودکان از این پلتفرم‌ها یکی از چالش‌ها است. قوانین موجود نمی‌توانند به طور مؤثر کنترل‌های ویژه‌ای را بر نظارت و دسترسی کودکان به این پلتفرم‌ها اعمال کنند. بسیاری از این پلتفرم‌ها به

طور پیش فرض شرایطی را فراهم می‌کنند که ممکن است منجر به دسترسی کودکان به محتوای مضر یا آسیب‌های روانی شود.

نبود استانداردهای مشخص برای حفاظت از داده‌های شخصی کودکان یکی دیگر از خلأهای مهم است. با وجود اینکه قانون حمایت از داده‌های شخصی در کشورهایی مانند اتحادیه اروپا وجود دارد که به طور خاص از حفاظت از داده‌های کودکان حمایت می‌کند، در ایران هنوز قانون مشخص و مستقلی برای حفاظت از داده‌های شخصی کودکان به طور ویژه وجود ندارد. این خلأ باعث می‌شود که داده‌های شخصی کودکان در بسیاری از مواقع به طور ناخواسته یا بدون رضایت والدین جمع‌آوری شده و برای اهداف تجاری استفاده شود. حتی اگر قوانینی برای حفاظت از حقوق کودکان در فضای مجازی وجود داشته باشد، عدم نظارت و اجرای مؤثر این قوانین می‌تواند باعث شکست آن‌ها شود. در بسیاری از موارد، حتی زمانی که تخلفاتی مانند انتشار محتوای مضر یا دستکاری داده‌های شخصی صورت می‌گیرد، پیگیری‌های قانونی کافی برای مجازات مجرمان وجود ندارد. این ضعف در اجرای قوانین می‌تواند منجر به نقض مستمر حقوق کودکان در فضای دیجیتال شود.

نبود مقررات صریح برای هوش مصنوعی

نبود مقررات صریح برای هوش مصنوعی یکی از چالش‌های مهم در حوزه فناوری‌های نوین است که به ویژه در زمینه حفاظت از حقوق کودکان و حریم خصوصی افراد در فضای دیجیتال اهمیت بیشتری پیدا می‌کند. هوش مصنوعی با سرعت بسیار بالایی در حال پیشرفت است و در بسیاری از زمینه‌ها، از جمله جمع‌آوری داده‌ها، پردازش اطلاعات و اتخاذ تصمیمات خودکار در حال استفاده است. با این حال، قوانین و مقررات موجود هنوز به طور کامل این فناوری را پوشش نداده و مشکلاتی در زمینه‌های حقوقی، اخلاقی و اجتماعی ایجاد کرده است. هوش مصنوعی توانایی پردازش داده‌ها، یادگیری از اطلاعات گذشته و حتی اتخاذ تصمیمات را دارد. در نتیجه، این فناوری می‌تواند به طور مستقیم یا غیرمستقیم بر زندگی افراد و به ویژه حقوق کودکان تأثیر بگذارد. اما بسیاری از کشورها هنوز مقررات صریح و جامعی برای نظارت بر هوش مصنوعی و حفاظت از داده‌های شخصی در مقابل سوءاستفاده از این فناوری‌ها ندارند. یکی از مشکلات اصلی در این زمینه این است که هوش مصنوعی به طور روزافزون به ابزاری برای جمع‌آوری و تحلیل داده‌ها تبدیل شده است. به عنوان مثال، الگوریتم‌های یادگیری ماشین و تحلیل‌های داده‌های بزرگ می‌توانند رفتارهای آنلاین افراد را ردیابی کنند و اطلاعات شخصی حساس از جمله علاقه‌ها، عادات خرید، رفتارهای آنلاین و حتی اطلاعات بیومتریک را پردازش کنند.

در بسیاری از کشورها، حفاظت از داده‌ها از طریق قوانین مانند GDPR در اتحادیه اروپا و COPPA در ایالات متحده صورت می‌گیرد، اما این قوانین به طور کامل نمی‌توانند از هوش مصنوعی به عنوان ابزاری برای پردازش و تحلیل داده‌ها محافظت کنند. در حالی که این قوانین برای جمع‌آوری داده‌های شخصی از افراد و به ویژه کودکان

محدودیت‌هایی اعمال می‌کنند، هوش مصنوعی می‌تواند این داده‌ها را در مقیاس وسیعی تجزیه و تحلیل کند و به طور غیرمستقیم به نقض حریم خصوصی منجر شود.

مشکل صلاحیت قضائی فرامرزی

مشکل صلاحیت قضائی فرامرزی یکی از بزرگ‌ترین چالش‌ها در زمینه حفاظت از حقوق کودکان در فضای مجازی و مقابله با تهدیدات آنلاین است. فضای دیجیتال و اینترنت به طور کلی مرزهای جغرافیایی را از بین برده و باعث شده که تهدیدات سایبری از هر نقطه‌ای از جهان به کشورها وارد شوند. در این شرایط، تعیین صلاحیت قضائی فرامرزی برای پیگیری و مجازات جرایم سایبری به مسئله‌ای پیچیده تبدیل شده است.

صلاحیت قضائی فرامرزی به این معناست که دادگاه‌ها و مقامات قضائی باید بتوانند تصمیمات خود را در خصوص جرایم و مسائل قانونی که در خارج از مرزهای کشور رخ داده، اعمال کنند. در دنیای دیجیتال، بسیاری از جرایم و تهدیدات آنلاین ممکن است از یک کشور به کشور دیگر انتقال یابد یا از یک مکان مجازی انجام شود که هیچ ارتباط مستقیمی با مرزهای جغرافیایی ندارد.

یکی از مهم‌ترین چالش‌های صلاحیت قضائی فرامرزی در فضای مجازی این است که ممکن است جرایم مرتبط با حریم خصوصی کودکان، سوءاستفاده‌های آنلاین یا پخش محتوای مضر در کشورهایی انجام شود که قوانین مربوطه را رعایت نمی‌کنند یا قوانین آن‌ها در این زمینه ضعیف است. به عنوان مثال، ممکن است یک فرد که در یک کشور دیگر فعالیت می‌کند، محتوای غیرمجاز یا سوءاستفاده‌کننده از داده‌های شخصی کودکان را منتشر کند و از آن‌جا که این فعالیت در کشور خود او قانونی است یا هیچ نظارتی بر آن وجود ندارد، پیگیری آن در سطح بین‌المللی بسیار دشوار می‌شود.

دشواری شناسایی متخلفان در محیط دیجیتال

دشواری شناسایی متخلفان در محیط دیجیتال یکی از بزرگ‌ترین چالش‌های حوزه حقوقی، به ویژه در زمینه حفاظت از حقوق کودکان و حریم خصوصی افراد است. فضای دیجیتال، به ویژه اینترنت و شبکه‌های اجتماعی، به دلیل ویژگی‌های خاص خود، شناسایی متخلفان را بسیار پیچیده کرده است. متخلفان در فضای مجازی می‌توانند از روش‌های مختلف برای پنهان کردن هویت خود استفاده کنند و این موضوع، مشکلات فراوانی برای شناسایی و پیگیری آنان ایجاد کرده است.

یکی از دلایل اصلی که باعث دشواری شناسایی متخلفان در محیط دیجیتال می‌شود، ناشناس بودن کاربران است. برخلاف محیط‌های فیزیکی که هویت افراد به راحتی قابل شناسایی است، در فضای مجازی افراد می‌توانند از نام‌های مستعار، آدرس‌های IP جعلی، VPN‌ها و شبکه‌های پراکنده استفاده کنند تا هویت واقعی خود را پنهان

کنند. این روش‌ها باعث می‌شود که تشخیص متخلفان و ردیابی فعالیت‌های آن‌ها به ویژه در صورتی که این فعالیت‌ها در فضاها بین‌المللی انجام شوند، بسیار دشوار گردد.

با توجه به اینکه هوش مصنوعی، یادگیری ماشین و الگوریتم‌های پیچیده در فضای دیجیتال به طور گسترده استفاده می‌شوند، متخلفان می‌توانند به راحتی از این فناوری‌ها برای پنهان‌سازی ردپاهای دیجیتال خود بهره‌برداری کنند. به عنوان مثال، در صورتی که فردی از سیستم‌های یادگیری ماشین برای تحلیل داده‌ها یا پردازش اطلاعات شخصی استفاده کند، امکان ردیابی و شناسایی هویت واقعی او بسیار محدود می‌شود.

چارچوب‌های حقوقی حمایت از کودکان در برابر تهدیدات هوش مصنوعی

حقوق داخلی ایران

قانون اساسی جمهوری اسلامی ایران

قانون اساسی جمهوری اسلامی ایران به طور کلی به حقوق و آزادی‌های فردی، از جمله حق حریم خصوصی اشاره دارد. بر اساس اصول مختلف قانون اساسی، هر فردی در ایران از حقوقی نظیر حریم خصوصی برخوردار است که به طور خاص در اصل ۲۵ قانون اساسی آمده است. این اصل بر ممنوعیت شنود غیرقانونی مکالمات و نامه‌ها تأکید دارد و محافظت از اطلاعات شخصی افراد را یکی از اصول اساسی در حفاظت از حقوق شهروندی معرفی می‌کند. اصل ۲۵ قانون اساسی مقرر می‌دارد: «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها، استراق سمع و هر گونه تجسس ممنوع است، مگر به حکم قانون.» این اصل، هرچند به طور خاص به فضای مجازی اشاره نکرده است، اما می‌تواند به عنوان یک مبنا و چارچوب کلی برای حفاظت از حریم خصوصی در فضای دیجیتال نیز مورد استناد قرار گیرد.

قانون حمایت از کودکان و نوجوانان

یکی از مهم‌ترین قوانین در زمینه حقوق کودکان، قانون حمایت از کودکان و نوجوانان است که در سال ۱۳۹۹ به تصویب رسید. این قانون به حفاظت از حقوق کودکان در تمامی جنبه‌های زندگی، از جمله استفاده از فضای مجازی، پرداخته است. در این قانون به محافظت از کودکان در برابر خطرات احتمالی در فضای مجازی و ارتقای آگاهی‌های آن‌ها درباره تهدیدات دیجیتال تأکید شده است. همچنین، این قانون مسئولیت‌هایی را بر دوش والدین، نهادهای آموزشی و نهادهای حکومتی برای نظارت بر رفتارهای آنلاین کودکان و محافظت از آن‌ها در برابر محتوای مضر قرار داده است.

قانون جرایم رایانه‌ای

قانون جرایم رایانه‌ای ایران که در سال ۱۳۸۸ به تصویب رسید، به عنوان یک چارچوب قانونی برای مقابله با تهدیدات دیجیتال و حفاظت از اطلاعات و داده‌های شخصی در فضای مجازی طراحی شده است. این قانون با هدف مقابله با جرایم سایبری از جمله هک، کلاهبرداری‌های اینترنتی، دسترسی غیرمجاز به داده‌ها و انتشار محتوای غیراخلاقی و تهدیدآمیز در فضای مجازی تصویب شده است.

ماده ۱ این قانون، تعاریف اساسی مرتبط با جرایم رایانه‌ای را ارائه می‌دهد. ماده ۲ به طور خاص به جرایم رایانه‌ای اشاره دارد و برخی از جرایم مربوط به فضای مجازی مانند دسترسی غیرمجاز به سیستم‌های رایانه‌ای، سرقت داده‌ها، انتشار محتوای توهین‌آمیز و تهدیدآمیز و خودداری از اعلام وقوع جرم سایبری را تحت پوشش قرار می‌دهد. ماده ۴ به انتشار محتوای غیرمجاز در فضای مجازی می‌پردازد و بر اساس آن، انتشار محتوای توهین‌آمیز، ضد اخلاقی یا مضر برای اخلاق عمومی مانند محتوای پورنوگرافی و خشونت‌آمیز در فضای دیجیتال جرم است. ماده ۲۱ به مجازات‌های مربوط به هک و دسترسی غیرمجاز به سیستم‌ها و شبکه‌ها اشاره دارد و ماده ۲۲ به مجازات‌هایی مانند حبس‌های طولانی‌مدت و جریمه‌های سنگین برای مجرمانی که اقدام به انتشار محتواهای غیراخلاقی یا تهدیدآمیز در فضای دیجیتال می‌کنند، پرداخته است.

با وجود این که قانون جرایم رایانه‌ای ایران به طور جامع به تهدیدات سایبری پرداخته، اما همچنان با چالش‌هایی مواجه است. یکی از این چالش‌ها عدم هماهنگی با استانداردهای جهانی است. بسیاری از تهدیدات جدید که در فضای دیجیتال به وجود می‌آید، ممکن است در این قانون به طور دقیق پیش‌بینی نشده باشد. به همین دلیل، برای جلوگیری از مجرمان سایبری و تهدیدات نوین، باید این قانون به طور مرتب به‌روزرسانی شود.

حقوق بین‌الملل

کنوانسیون حقوق کودک

کنوانسیون حقوق کودک سازمان ملل متحد که در سال ۱۹۸۹ تصویب شد و بیش از ۱۹۰ کشور از جمله ایران آن را پذیرفته‌اند، یکی از مهم‌ترین و جامع‌ترین اسناد حقوقی بین‌المللی در زمینه حقوق کودکان است. این کنوانسیون به حقوق و آزادی‌های کودکان در تمامی ابعاد زندگی می‌پردازد و شامل حق حریم خصوصی، حق آموزش و حق محافظت از تهدیدات و آزار آنلاین است.

ماده ۱۶ این کنوانسیون به طور مستقیم به حق حریم خصوصی کودکان اشاره دارد و مقرر می‌دارد: «۱- هیچ کودکی نباید مورد دخالت خودسرانه یا غیرقانونی در امور خصوصی، خانواده، خانه یا مکاتبات خود قرار گیرد و همچنین نباید حیثیت و اعتبار او مورد تعرض غیرقانونی واقع شود. ۲- کودک حق دارد که قانون از او در برابر چنین تعرضات و دخالت‌ها حمایت کند.» این ماده، یک چارچوب حقوقی مستحکم برای حمایت از حریم خصوصی

کودکان در همه زمینه‌ها، از جمله فضای مجازی، فراهم می‌کند.

مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR)

مقررات عمومی حفاظت از داده‌ها که در تاریخ ۲۵ مه ۲۰۱۸ به طور رسمی اجرایی شد، یکی از جامع‌ترین و سخت‌گیرانه‌ترین مقررات در زمینه حفاظت از داده‌های شخصی در سطح جهانی است. این مقررات، که به ویژه به حریم خصوصی افراد و امنیت داده‌ها در فضای دیجیتال پرداخته، به طور خاص از اطلاعات شخصی افراد محافظت می‌کند.

از منظر حفاظت از داده‌های کودکان، GDPR دارای مقررات خاص و سخت‌گیرانه‌ای است. بر اساس این مقررات، پردازش داده‌های شخصی کودکان زیر ۱۶ سال، مستلزم کسب رضایت والدین یا سرپرست قانونی آن‌ها است. کشورهای عضو اتحادیه اروپا می‌توانند این سن را تا ۱۳ سال کاهش دهند، اما نمی‌توانند آن را از ۱۶ سال بیشتر کنند. همچنین، شرکت‌ها موظفند اطلاعات مربوط به پردازش داده‌ها را به زبان ساده و قابل فهم برای کودکان ارائه دهند.

قانون حفاظت از حریم خصوصی آنلاین کودکان ایالات متحده (COPPA)

قانون حفاظت از حریم خصوصی آنلاین کودکان یکی از مهم‌ترین قوانین ایالات متحده است که به طور خاص به حفاظت از داده‌های شخصی کودکان در فضای اینترنت پرداخته است. این قانون برای اولین بار در سال ۱۹۹۸ به تصویب رسید و هدف اصلی آن محافظت از کودکان زیر ۱۳ سال در برابر جمع‌آوری داده‌های شخصی توسط وبسایت‌ها و اپلیکیشن‌های آنلاین است.

طبق این قانون، وبسایت‌ها و سرویس‌های آنلاین باید از جمع‌آوری هرگونه اطلاعات شخصی از کودکان زیر ۱۳ سال بدون رضایت والدین جلوگیری کنند. این اطلاعات شامل نام، آدرس، ایمیل، شماره تلفن و هر نوع داده شخصی دیگری است که می‌تواند به شناسایی کودک کمک کند. وبسایت‌ها و اپلیکیشن‌ها موظفند که به والدین اطلاع دهند که چه داده‌هایی جمع‌آوری می‌کنند و چگونه از این داده‌ها استفاده خواهند کرد.

نتیجه‌گیری

در دنیای دیجیتال امروزی که کودکان به طور فزاینده‌ای در فضای آنلاین حضور دارند و از خدمات مختلف اینترنتی استفاده می‌کنند، مسأله حمایت از حقوق کودکان و حریم خصوصی آنان به موضوعی اساسی و غیرقابل انکار تبدیل شده است. هوش مصنوعی به عنوان یک فناوری قدرتمند و دوگانه، هم می‌تواند به حفاظت از حریم خصوصی کودکان کمک کند و هم تهدیدات جدید و پیچیده‌ای برای آن ایجاد نماید. از یک سو، الگوریتم‌های

تحلیل قوانین داخلی ایران نشان می‌دهد که علی‌رغم وجود برخی قوانین پراکنده مانند قانون اساسی، قانون حمایت از کودکان و نوجوانان و قانون جرایم رایانه‌ای، خلأهای قانونی عمیقی در زمینه حفاظت از حریم خصوصی کودکان در برابر تهدیدات هوش مصنوعی وجود دارد. نبود قانون جامع حفاظت از داده‌های شخصی، فقدان مقررات خاص برای هوش مصنوعی، ضعف در اجرای قوانین موجود و عدم هماهنگی با استانداردهای بین‌المللی، از جمله مهم‌ترین این خلأها هستند.

در سطح بین‌المللی، اسناد مهمی مانند کنوانسیون حقوق کودک، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) و قانون حفاظت از حریم خصوصی آنلاین کودکان ایالات متحده (COPPA)، چارچوب‌های حقوقی مستحکمی برای حمایت از حریم خصوصی کودکان در فضای دیجیتال فراهم کرده‌اند. این اسناد بر اصولی مانند رضایت آگاهانه والدین، شفافیت، حداقل‌سازی داده‌ها، حق دسترسی و حق فراموشی تأکید دارند و می‌توانند به عنوان الگویی برای اصلاح و تدوین قوانین در ایران مورد استفاده قرار گیرند.

پیشنهادهای

بر اساس یافته‌های این پژوهش، راهکارهای عملی زیر برای بهبود وضعیت موجود و رفع چالش‌های حقوقی و اخلاقی هوش مصنوعی در حفاظت از حریم خصوصی کودکان پیشنهاد می‌شود:

۱. **تدوین و تصویب قانون جامع حفاظت از داده‌های شخصی کودکان:** قانون‌گذاران ایران باید هرچه سریع‌تر نسبت به تدوین و تصویب قانونی جامع و مستقل برای حفاظت از داده‌های شخصی کودکان در فضای مجازی اقدام نمایند. این قانون باید با الهام از استانداردهای بین‌المللی مانند GDPR و COPPA، اصولی مانند رضایت آگاهانه والدین، شفافیت، حداقل‌سازی داده‌ها، حق دسترسی، اصلاح و حذف داده‌ها و مسئولیت‌پذیری پلتفرم‌ها را به طور صریح و روشن مورد تأکید قرار دهد.

۲. **تصویب مقررات خاص برای هوش مصنوعی:** با توجه به رشد سریع و تأثیرات گسترده هوش مصنوعی، ضروری است که مقررات خاصی برای تنظیم و نظارت بر توسعه و استفاده از این فناوری، به ویژه در حوزه‌های حساس مانند حریم خصوصی کودکان، تدوین و به تصویب برسد. این مقررات باید بر شفافیت الگوریتم‌ها، قابلیت توضیح‌دهی، عدالت و عدم تبعیض، مسئولیت‌پذیری و پاسخگویی حقوقی تأکید داشته باشند.

۳. **ایجاد نهادهای نظارتی مستقل و کارآمد:** برای نظارت بر اجرای مؤثر قوانین و مقررات مربوط به حریم خصوصی کودکان و هوش مصنوعی، ایجاد نهادهای نظارتی مستقل، تخصصی و کارآمد ضروری است. این نهادها باید دارای اختیارات کافی برای بازرسی، تحقیق، صدور دستور و اعمال جریمه در موارد نقض قوانین باشند.

۴. **افزایش شفافیت الگوریتم‌های هوش مصنوعی:** پلتفرم‌ها و توسعه‌دهندگان باید ملزم به شفاف‌سازی در مورد نحوه عملکرد الگوریتم‌های هوش مصنوعی، داده‌های مورد استفاده و فرآیندهای تصمیم‌گیری شوند. این شفافیت

باید به گونه‌ای باشد که برای والدین و حتی کودکان (به زبان ساده) قابل درک باشد و امکان نظارت و اعتراض را فراهم کند.

۵. **تقویت همکاری‌های بین‌المللی:** با توجه به ماهیت فرامرزی فضای مجازی، تقویت همکاری‌های بین‌المللی و انعقاد معاهدات دوجانبه و چندجانبه برای حل مشکل صلاحیت قضائی فرامرزی، تبادل اطلاعات و همکاری در پیگیری جرایم سایبری علیه کودکان، از اهمیت ویژه‌ای برخوردار است.

۶. **توانمندسازی والدین و کودکان از طریق آموزش و آگاهی‌بخشی:** آموزش و آگاهی‌بخشی به والدین و کودکان در مورد تهدیدات فضای مجازی، حقوق حریم خصوصی، نحوه استفاده ایمن از اینترنت و چگونگی مدیریت داده‌های شخصی، یکی از مؤثرترین راهکارهای پیشگیرانه است.

۷- **تشویق به توسعه فناوری‌های هوش مصنوعی با رویکرد حفظ حریم خصوصی:** پژوهشگران، توسعه‌دهندگان و شرکت‌های فعال در حوزه هوش مصنوعی باید تشویق شوند تا سیستم‌هایی را طراحی و پیاده‌سازی کنند که از ابتدا با رعایت اصول حفظ حریم خصوصی و امنیت داده‌ها طراحی شده‌اند.

فهرست منابع

- انصاری، باقر. (۱۳۸۳). حریم خصوصی و حمایت از آن در حقوق اسلام، تطبیقی و ایران. دانشکده حقوق و علوم سیاسی (دانشگاه تهران)، شماره ۶۶.
- پورمسجدیان، فاطمه، و ابراهیمی، سید نصرالله. (۱۴۰۱). واکاوی حقوقی حمایت از حریم خصوصی کودک در فضای مجازی با نگاهی به قوانین ایران و معاهدات بین‌المللی. مطالعات حقوقی فضای مجازی، شماره ۴.
- خلیلی، مهسا، و سیدهاشمی، زهراسادات. (زمستان ۱۴۰۳). امکان‌سنجی مسئولیت کیفری هوش مصنوعی با تأکید بر شخصیت مستقل حقوقی. عدلیه، شماره ۱۱.
- خواجه، احمد، و انبارکی، لیل. (بهار ۱۳۹۲). ضرورت سواد رسانه‌ای در فضای مجازی و تأثیر آن بر حفظ حریم خصوصی. امنیت انتظامی دریایی، شماره ۱۲.
- خوان، یاشار. (۱۴۰۳). تأثیر هوش مصنوعی بر حریم خصوصی اشخاص حقیقی و حقوقی از منظر نظام حقوقی ایران (پیشنهاد کارشناسی ارشد). دانشگاه پیام نور استان تهران، مرکز تهران جنوب.
- ستوده، زهرا. (۱۴۰۱). رویکرد حقوق بین‌الملل به قاعده‌مندسازی در حوزه هوش مصنوعی با تأکید بر حفظ حریم خصوصی کاربران شبکه‌های اجتماعی (پیشنهاد کارشناسی ارشد). دانشگاه شیراز، دانشکده حقوق و علوم سیاسی.
- سیدسعادت، فهیمه. (پاییز ۱۳۹۲). صیانت از حریم خصوصی در فضای مجازی بر اساس هنجارهای اسلامی. راهبرد فرهنگ، شماره ۶.
- طباطبایی‌پور، فاطمه‌السادات. (۱۴۰۱). حفاظت از حق بر حریم خصوصی در کاربرد سیستم‌های هوش مصنوعی (پیشنهاد کارشناسی ارشد). دانشگاه شهید بهشتی، دانشکده حقوق.
- طلائی زواره، سید محمد صالح. (۱۴۰۳). حریم خصوصی در عصر هوش مصنوعی. مطالعات حقوقی فضای مجازی، شماره ۸.
- ظفریان، طیب، اسلامی، رحیم، و صادقی، مرتضی. (۱۴۰۴). حفظ حریم خصوصی در تکنولوژی‌های مبتنی بر هوش مصنوعی. مطالعات حقوقی فضای مجازی، شماره ۱۳.
- عبدی‌پور، ابراهیم. (بهار ۱۳۹۴). رویکرد نظام‌های حقوقی نسبت به نقض حریم خصوصی اطلاعاتی در شبکه‌های اجتماعی مجازی. پژوهش تطبیقی حقوق اسلام و غرب، شماره ۳.
- علی‌احمدی جشفقانی، حسین، و شوق‌نیا، آر. (زمستان ۱۳۹۲). رعایت حریم خصوصی در فضای مجازی: مورد مطالعه حقوق ایران. مدیریت فرد، شماره ۵۲.
- علیمرادی، مصطفی. (پاییز ۱۴۰۱). نظارت بر فضای مجازی و حریم خصوصی کاربران. ره‌آورد نور، شماره ۸۱.
- فرامرزیانی، پروانه، سلطانی‌فر، محمد، و مظفری، افسانه. (تابستان ۱۴۰۱). طراحی الگوی راهکارهای حمایت از حریم خصوصی کودکان در فضای مجازی. پژوهش‌های ارتباطی، شماره ۱۱۶.
- فرشته بنافی. (۱۴۰۲). حفاظت از حق حریم خصوصی اطلاعاتی در مقابل تهدیدات ناشی از هوش مصنوعی نظامی. پژوهش حقوق خصوصی، شماره ۴۵.

- قربانی فر، مریم، و محسن پور، سمیرا. (۱۴۰۲). حریم خصوصی کودکان در فضای مجازی. *مطالعات حقوقی فضای مجازی*، شماره ۶.
- قوامی پور سرشکه، محدثه، و محمودی، امیررضا. (۱۴۰۴). درآمدی بر چهارچوب های حقوقی مسئولیت کیفری برای سیستم های هوش مصنوعی. *حقوق فناوری های نوین*، شماره ۱۱.
- گرامی، رضا، و جاویدپور، مریم. (بهار ۱۴۰۴). بررسی چالش های حقوقی هوش مصنوعی در نظام حقوقی ایران. *مطالعات حقوقی*، شماره ۴۵.
- محمدی، علی. (۱۴۰۳). بررسی حریم خصوصی خانواده و چالش های نقض آن در فضای مجازی از منظر حقوق ایران و اسناد بین المللی (پایان نامه کارشناسی ارشد). دانشگاه پیام نور استان خوزستان، مرکز دزفول.
- ملایری، محمدرضا، جباری تکانته، سیدهادی، و خزائی، امیر. (پاییز ۱۴۰۳). تحلیل فقهی و حقوقی مسئولیت کیفری افراد در جرائم مرتبط با فناوری های نوظهور مانند هوش مصنوعی و بلاک چین. *حقوق اشراق*، شماره ۱۱.
- میرشکاری، عباس، ثابت قدم، فاطمه، و اصغرینیا، مرتضی. (۱۴۰۳). درآمدی بر چالش های فناوری هوش مصنوعی در حوزه حریم خصوصی. *مطالعات حقوقی فضای مجازی*، شماره ۱۲.
- نجیب زاده، فاطمه، و وامق آبادی، فاطمه. (۱۴۰۲). مسئولیت هوش مصنوعی و اینترنت اشیا. تهران: انتشارات جاودانه.