



The Legal Responsibility of Social Media Platforms for Automated Decisions Made by AI Algorithms: A Comparative Study of the Legal Systems in the United States, Europe, and Iran

Emad Molla Ebrahimi (Corresponding Author)

PhD., Department of Private Law, Faculty of Law, Central Tehran Branch, Islamic Azad University, Tehran, Iran. E-mail: em.ebrahimi63@gmail.com

Abstract

Objective

The rapid integration of artificial intelligence (AI) into social media platforms has transformed the digital ecosystem, reshaping how content is produced, disseminated, moderated, and consumed. Algorithms now determine what billions of users see, whom they interact with, and which narratives are amplified or suppressed. These systems perform tasks such as content curation, ranking posts, detecting illicit behavior, and removing harmful material with unprecedented speed and scale. Despite the immense societal benefits, AI-driven automated decisions have raised complex legal and ethical questions concerning transparency, accountability, fairness, and the protection of fundamental rights. This article aims to examine the extent to which social media platforms may be held legally responsible for automated decisions produced by machine-learning systems, especially when these decisions affect users' rights, opportunities, or access to information.

The primary goal of this study is to analyze the legal responsibility of social media companies for the outcomes of automated decision-making systems powered by AI. While previous literature has explored challenges such as algorithmic bias and data governance, the legal dimensions—particularly the allocation of responsibility when automated decisions cause harm—remain insufficiently addressed. By examining these issues, the article contributes to an emerging and critically important debate regarding platform liability in the age of algorithmic governance. Specifically, the study investigates whether current legal frameworks are adequate for governing autonomous AI decisions, what gaps exist in user protection, and how regulatory systems might evolve to ensure that automated decision-making remains lawful, ethical, and accountable.

Citation: Molla Ebrahimi, Emad (2025). The Legal Responsibility of Social Media Platforms for Automated Decisions Made by AI Algorithms: A Comparative Study of the Legal Systems in the United States, Europe, and Iran. *Media Management Review*, 4(3), 415-437. (in Persian)

Research Methodology

This research employs a descriptive–analytical methodology grounded in comparative legal analysis. It draws on statutory materials, international legal instruments, regulatory proposals, case law, industry guidelines, academic publications, and electronic sources. The comparative dimension examines regulatory trends in multiple jurisdictions—particularly the European Union, the United States, and selected Asia-Pacific countries—to assess whether existing frameworks such as the EU Digital Services Act, the EU AI Act, or Section 230 of the U.S. Communications Decency Act adequately address challenges posed by AI-generated decisions. The study synthesizes doctrinal legal analysis with theoretical perspectives from technology governance, human rights law, and information law. Findings are categorized, systematized, and analyzed to develop a structured conceptual understanding of platform liability within AI-driven environments.

Findings

The analysis reveals that AI algorithms deployed by social media platforms exercise significant power over users' digital experiences. These systems collect and process large volumes of user-generated data, generating predictive insights that shape decisions related to content visibility, moderation, and user segmentation. However, automated decisions raise at least three major legal concerns:

1. Lack of Transparency:

Many AI systems operate as “black boxes,” particularly those based on deep learning. Users often have no understanding of why content is removed, accounts are suspended, or certain posts are prioritized. The opacity of these decisions makes it difficult for users to challenge or appeal outcomes and hinders regulators from assessing compliance with legal standards. This lack of transparency undermines procedural fairness and violates principles found in emerging regulatory frameworks that emphasize explainability and documentation of algorithmic processes.

2. Accountability Gaps:

A central challenge is determining who is legally responsible when an algorithm makes a harmful or incorrect decision. Platforms frequently assert that automated decisions are neutral outputs of technical systems, not intentional human actions. Yet algorithms are designed, trained, fine-tuned, and supervised by human teams. When an automated system erroneously removes lawful content, discriminates against certain users, or disproportionately affects minority groups, identifying the responsible party becomes legally complex. In many jurisdictions, existing laws either do not explicitly cover algorithmic harms or provide platforms with broad immunity from liability.

3. Algorithmic Bias and Discrimination:

AI systems may inadvertently reproduce or amplify biases present in training datasets. For example, automated moderation tools often misclassify content from linguistic minorities, political dissidents, or marginalized communities. Biased algorithms can restrict freedom of expression, distort political discourse, and perpetuate digital inequality. The absence of robust oversight mechanisms allows such discriminatory outcomes to persist without adequate safeguards or remedies.

The study further finds that although social media platforms generate enormous societal value, the lack of effective regulation surrounding AI-driven content governance creates structural vulnerabilities. These vulnerabilities can result in wrongful account suspensions, uneven enforcement of community standards, suppression of legitimate speech, and wrongful reporting to law-enforcement authorities. On the regulatory side, while some jurisdictions (such as the EU) are developing stringent obligations for transparency, auditing, and human oversight, others (such as the U.S.) maintain broad immunity protections for platforms, creating global inconsistencies.

Opportunities and Recommendations:

The research identifies several opportunities for strengthening legal and regulatory frameworks:

Independent Supervisory Bodies: Establishing specialized regulatory authorities capable of auditing algorithms, investigating platform practices, and imposing sanctions where necessary.

Transparency Obligations: Requiring platforms to disclose key information about how algorithms function, including criteria for content removal, ranking, and risk assessment.

User Rights and Redress Mechanisms: Ensuring users have meaningful avenues to challenge automated decisions, including the right to request human review and access to explanations.

Mandatory Bias Audits: Implementing regular third-party audits to detect discriminatory outcomes and ensure compliance with equality and human rights standards.

Harmonization of Global Standards: Developing coordinated international frameworks to avoid fragmentation and ensure consistent levels of user protection

Discussion & Conclusion

As AI continues to become a foundational component of social media ecosystems, the legal implications of automated decision-making cannot be overlooked. The study concludes that existing regulatory frameworks are insufficient to address the unique risks posed by autonomous algorithmic systems. More precise, transparent, and enforceable rules are required to govern the deployment of AI in digital platforms, safeguard user rights, and promote accountability. Strengthening regulatory mechanisms will enhance trust, improve platform governance, and ensure healthier interactions between platforms and their users. Ultimately, the establishment of coherent legal frameworks that address transparency, accountability, and fairness will provide a more resilient foundation for digital ecosystems increasingly driven by algorithmic intelligence.

Keywords: Platform; Social media; AI algorithms; Automated decisions; Legal challenges.



مسئولیت حقوقی پلتفرم‌های رسانه‌های اجتماعی در قبال تصمیم‌های خودکار

الگوریتم‌های هوش مصنوعی: مطالعه تطبیقی در نظام حقوقی امریکا، اروپا و ایران

عماد ملاابراهیمی

دکتری، گروه حقوق خصوصی، دانشکده حقوق، واحد تهران مرکز، دانشگاه آزاد اسلامی، تهران، ایران. رایانامه: em.ebrahimi63@gmail.com

چکیده

هدف: این مقاله به بررسی مسئولیت حقوقی پلتفرم‌های رسانه‌های اجتماعی در قبال تصمیم‌های خودکار الگوریتم‌های هوش مصنوعی می‌پردازد. در این راستا، ابتدا نقش و تأثیر این الگوریتم‌ها در مدیریت محتوا و رفتار کاربران به بحث گذاشته می‌شود؛ سپس چالش‌های حقوقی مرتبط با این تصمیم‌ها، از جمله کمبود شفافیت، مسئولیت‌پذیری و تعصب‌های احتمالی بررسی خواهد شد.

روش: پژوهش حاضر، پژوهشی توصیفی - تحلیلی است که با بهره‌گیری از روش‌های مطالعه تطبیقی و با استفاده از منابع مکتوب، شفاهی، اسناد الکترونیکی و مطالعات قانونی، به تشریح مباحث پرداخته است؛ سپس با گردآوری، انسجام و دسته‌بندی یافته‌ها، مباحث پرسش شده در پژوهش را تحلیل و سرانجام به استنتاج می‌پردازد.

یافته‌ها: الگوریتم‌های هوش مصنوعی، با تحلیل داده‌های گسترده کاربران، وظایف مختلفی مانند نمایش محتوا، رتبه‌بندی پست‌ها، حذف مطالب نامناسب و تشخیص رفتارهای غیرقانونی را برعهده دارند. با این حال، تصمیم‌های خودکار این الگوریتم‌ها، می‌تواند برای پلتفرم‌ها چالش‌های حقوقی جدی ایجاد کند؛ زیرا ممکن است به نقض حقوق کاربران، تبعیض ناعادلانه یا اشتباه‌های شایان توجهی منجر شود. این مقاله، فرصت‌های موجود برای بهبود و توسعه قوانین و مقررات در این زمینه، از جمله ایجاد نهادهای نظارتی مستقل، افزایش شفافیت و امکان اعتراض کاربران به تصمیم‌های خودکار را بررسی می‌کند.

نتیجه‌گیری: با توجه به نقش گسترده هوش مصنوعی در رسانه‌های اجتماعی، تدوین مقررات دقیق‌تر و شفاف‌تر، می‌تواند به حل چالش‌های حقوقی کمک کند و فرصتی برای بهبود عملکرد و تعامل میان پلتفرم‌ها و کاربران فراهم کند.

کلیدواژه‌ها: پلتفرم، رسانه‌های اجتماعی، الگوریتم‌های هوش مصنوعی، تصمیم‌های خودکار، چالش‌های حقوقی.

استناد: ملاابراهیمی، عماد (۱۴۰۴). مسئولیت حقوقی پلتفرم‌های رسانه‌های اجتماعی در قبال تصمیم‌های خودکار الگوریتم‌های هوش مصنوعی: مطالعه تطبیقی در نظام حقوقی امریکا، اروپا و ایران. *بررسی‌های مدیریت رسانه*، ۴(۳)، ۴۱۵-۴۳۷.

تاریخ دریافت: ۱۴۰۳/۰۶/۱۰

تاریخ ویرایش: ۱۴۰۴/۰۴/۲۰

تاریخ پذیرش: ۱۴۰۴/۰۵/۱۵

تاریخ انتشار: ۱۴۰۴/۰۷/۰۱

doi: <https://doi.org/10.22059/MMR.2025.381742.1108>

بررسی‌های مدیریت رسانه، ۱۴۰۴، دوره ۴، شماره ۳، صص. ۴۱۵-۴۳۷

ناشر: دانشکده مدیریت دانشگاه تهران

نوع مقاله: علمی - پژوهشی

© نویسندگان

مقدمه

در دهه‌های اخیر، گسترش فناوری و رشد بی‌سابقه هوش مصنوعی (AI) و الگوریتم‌های خودکار، به تحولی اساسی در مدیریت داده‌ها و محتوا در پلتفرم‌های رسانه‌های اجتماعی منجر شده است. این پلتفرم‌ها با استفاده از الگوریتم‌های پیچیده هوش مصنوعی، می‌توانند حجم عظیمی از داده‌ها و اطلاعات کاربران را پردازش کنند و بر اساس تحلیل داده‌ها، تصمیم‌های خودکار متعددی اتخاذ کنند. برخی از این تصمیم‌های خودکار عبارت‌اند از: نمایش یا پنهان‌سازی محتوا، مدیریت تبلیغات هدفمند، حذف یا تعدیل پُست‌ها و حتی مسدود کردن کاربران بر اساس فعالیت‌های آن‌ها. چنین تصمیم‌هایی، بر تجربه کاربران از پلتفرم‌های اجتماعی تأثیر بسزایی دارند و هم‌زمان می‌توانند مسائلی همچون نقض حقوق فردی، تبعیض یا محدودیت آزادی بیان را به همراه داشته باشند.

یکی از چالش‌های بسیار مهم پیش روی پلتفرم‌های رسانه‌های اجتماعی در این زمینه، مسئولیت حقوقی آن‌ها در قبال تصمیم‌های خودکار الگوریتم‌های هوش مصنوعی است. این پرسش اساسی مطرح می‌شود که تا چه حد پلتفرم‌ها باید در قبال تصمیم‌هایی که از سوی الگوریتم‌های خودکار اتخاذ می‌شود، مسئول شناخته شوند؟ آیا پلتفرم‌ها می‌توانند مسئولیت خود را در قبال خطاهای احتمالی این سیستم‌ها، به دلیل اتکا به فناوری از خود سلب کنند یا باید به‌عنوان نهادهای تصمیم‌گیرنده، پاسخ‌گوی پیامدهای اجتماعی و حقوقی این تصمیم‌ها باشند؟ از سوی دیگر، چالش‌های حقوقی مرتبط با این موضوع، به دلیل عدم شفافیت و پیچیدگی عملکرد الگوریتم‌های هوش مصنوعی نیز برجسته می‌شود. کاربران اغلب از نحوه کارکرد این الگوریتم‌ها بی‌اطلاع هستند و در بسیاری موارد نمی‌دانند که تصمیم‌های پلتفرم‌ها بر اساس چه معیارهایی اتخاذ شده است. این عدم شفافیت، می‌تواند به نارضایتی عمومی، کاهش اعتماد به پلتفرم‌ها و حتی طرح دعوی حقوقی علیه آن‌ها منجر شود.

افزون‌براین، مسئله تبعیض و تعصب‌های الگوریتمی نیز یکی از نگرانی‌های جدی است؛ زیرا الگوریتم‌ها ممکن است بر اساس داده‌های ناقص یا ناعادلانه، تصمیم‌هایی بگیرند که به نابرابری‌های اجتماعی یا تبعیض علیه برخی گروه‌ها منجر شود. در مقابل این چالش‌ها، فرصت‌هایی نیز برای پلتفرم‌ها و جامعه حقوقی وجود دارد. یکی از این فرصت‌ها، بهبود قوانین و مقررات مربوط به مسئولیت حقوقی پلتفرم‌هاست. در بسیاری از نظام‌های حقوقی، پلتفرم‌های رسانه‌های اجتماعی، به‌عنوان واسطه‌های دیجیتال، در قبال محتوای تولید شده توسط کاربران مسئولیت محدودی دارند؛ اما این قوانین هنوز به‌طور کامل به تصمیم‌های خودکار الگوریتم‌های هوش مصنوعی تسری نیافته است. تدوین مقررات جدید، می‌تواند به وضوح بیشتر در این زمینه منجر شود و چارچوبی قانونی برای مسئولیت‌پذیری و شفافیت پلتفرم‌ها فراهم کند. از سوی دیگر، پلتفرم‌های رسانه‌های اجتماعی می‌توانند از فرصت‌های فناوری بهره‌مند شوند تا از طریق بهبود الگوریتم‌ها، دقت تصمیم‌گیری‌های خودکار را افزایش دهند و از وقوع اشتباه‌ها و سوگیری‌های ناعادلانه جلوگیری کنند. به‌علاوه، توسعه نهادهای نظارتی مستقل و افزایش شفافیت فرایندهای خودکار، به افزایش اعتماد کاربران و کاهش مشکلات حقوقی منجر می‌شود. در مجموع، موضوع مسئولیت حقوقی پلتفرم‌های رسانه‌های اجتماعی در قبال تصمیم‌های خودکار الگوریتم‌های هوش مصنوعی، یکی از مباحث مهم و چالش‌برانگیز در عصر دیجیتال است که بررسی دقیق آن از منظر حقوقی، اجتماعی و فناورانه ضروری است که در این مقاله به بررسی و ارائه راهکارهای مدنظر خواهیم پرداخت.

الف. تعریف و جایگاه هوش مصنوعی در پلتفرم‌های رسانه‌های اجتماعی

رسانه‌های اجتماعی به پلتفرم‌های آنلاین و دیجیتالی اشاره دارند که به کاربران امکان می‌دهند محتوای چندرسانه‌ای خود را به اشتراک بگذارند، تعامل داشته باشند و شبکه‌های اجتماعی گسترده‌ای ایجاد کنند. پلتفرم‌هایی نظیر فیسبوک^۱، اینستاگرام^۲، توییتر^۳، یوتیوب^۴ و تیک‌تاک^۵، از محبوب‌ترین نمونه‌های رسانه‌های اجتماعی هستند که میلیون‌ها کاربر را از سراسر جهان جذب کرده‌اند. این پلتفرم‌ها نه تنها محلی برای انتشار محتوا و تعامل کاربران هستند، بلکه به‌عنوان ابزارهای قدرتمند تبلیغاتی، بازاریابی و ارتباطات عمومی عمل می‌کنند. با رشد سریع رسانه‌های اجتماعی، چالش‌های جدیدی مانند انتشار اطلاعات نادرست، ترویج نفرت و خشونت و تجاوز به حریم خصوصی کاربران نیز ظهور یافته است. این موضوعات موجب شده است تا پلتفرم‌ها به دنبال استفاده از فناوری‌های پیشرفته‌ای همچون هوش مصنوعی باشند تا این چالش‌ها را به‌شکلی مؤثرتر مدیریت کنند (راسل، نوروینگ و اینتلیجنس^۶، ۲۰۲۰).

• رسانه‌های اجتماعی

بسترهای مجازی به‌عنوان رسانه‌های اجتماعی برای تعاملات اجتماعی و اشتراک‌گذاری محتوا، در زندگی روزمره افراد و جامعه نقش مهمی ایفا می‌کنند. پلتفرم‌هایی مانند فیسبوک، اینستاگرام، توییتر و یوتیوب، فضای گسترده‌ای برای تولید و انتشار محتوای متنی، تصویری و ویدئویی فراهم کرده‌اند که توسط میلیون‌ها کاربر مورد استفاده قرار می‌گیرند. این پلتفرم‌ها با بهره‌گیری از شبکه‌های اجتماعی به کاربران امکان می‌دهند که ارتباطات فردی خود را گسترش دهند، محتوای دلخواه خود را منتشر کنند و در جامعه‌ای گسترده‌تر مشارکت کنند. رسانه‌های اجتماعی به شکل چشمگیری در بازاریابی، تبلیغات، ارتباطات اجتماعی و حتی، سیاست‌گذاری‌ها تأثیرگذارند (کاپلان و هانلین^۷، ۲۰۱۰). یکی از ویژگی‌های منحصربه‌فرد این پلتفرم‌ها، تولید محتوا توسط کاربران است؛ به این معنا که کاربران نه تنها مصرف‌کنندگان محتوا هستند، بلکه تولیدکنندگان آن نیز به‌شمار می‌آیند. این موضوع باعث شده است که رسانه‌های اجتماعی، به یکی از ابزارهای مهم ارتباطی در عصر دیجیتال تبدیل شوند. با این حال، رسانه‌های اجتماعی با چالش‌های متعددی روبه‌رو هستند؛ انتشار اطلاعات نادرست، ترویج خشونت یا نفرت‌پراکنی، حریم خصوصی کاربران و امنیت داده‌ها، از جمله مسائل مهمی هستند که باید مدیریت شوند. مدیریت حجم وسیع داده‌ها و محتوای تولید شده توسط کاربران، به ابزارهای پیشرفته‌ای مانند هوش مصنوعی نیاز دارد (گانینگ و همکاران^۸، ۲۰۱۹).

• هوش مصنوعی و الگوریتم‌های خودکار

هوش مصنوعی و الگوریتم‌های خودکار هوش مصنوعی (AI) به مجموعه‌ای از فناوری‌ها اشاره دارد که قابلیت یادگیری

1. Facebook
2. Instagram
3. Twitter
4. YouTube
5. TikTok
6. Russell, Norvig & Intelligence
7. Kaplan & Haenlein
8. Gunning et al.

و تصمیم‌گیری شبیه به انسان را دارند. این فناوری، به‌ویژه در پلتفرم‌های رسانه‌های اجتماعی، نقش کلیدی در مدیریت و تحلیل حجم بالای داده‌ها، نقش کلیدی ایفا می‌کند. استفاده از الگوریتم‌های خودکار در این پلتفرم‌ها، به این منظور است که تصمیم‌گیری‌هایی نظیر رتبه‌بندی محتوا، فیلتر کردن پُست‌های نامناسب، تشخیص رفتارهای غیرقانونی و شخصی‌سازی تبلیغات با دقت و سرعت بیشتری انجام شود. الگوریتم‌های هوش مصنوعی، به‌طور پیوسته داده‌های کاربران را تحلیل می‌کنند و بر اساس آن‌ها تصمیم می‌گیرند که به‌طور مستقیم تجربه کاربری افراد را تحت تأثیر قرار می‌دهد. برای مثال، در اینستاگرام و فیسبوک، الگوریتم‌های هوش مصنوعی تصمیم می‌گیرند که چه محتوایی به کاربران نشان داده شود و چه مطالبی در اولویت نمایش قرار گیرند. این الگوریتم‌ها بر اساس تاریخچه جست‌وجو، رفتار کلیک کردن، تعاملات اجتماعی و حتی موقعیت مکانی کاربران، محتوای پیشنهادی را تعیین می‌کنند. کاربردهای اصلی هوش مصنوعی در رسانه‌های اجتماعی عبارت‌اند از:

۱. فیلتر کردن و مدیریت محتوا: پلتفرم‌ها از هوش مصنوعی برای شناسایی و حذف محتواهای نامناسب، نظیر پُست‌های توهین‌آمیز یا محتوای مرتبط با تروریسم و خشونت استفاده می‌کنند. برای مثال، یوتیوب از الگوریتم‌های خودکار برای شناسایی و حذف ویدئوهای مخرب استفاده می‌کند.^۱

۲. تجزیه و تحلیل داده‌ها و تبلیغات هدفمند: یکی از اصلی‌ترین کاربردهای هوش مصنوعی در رسانه‌های اجتماعی، ارائه تبلیغات هدفمند به کاربران است. الگوریتم‌های پیشرفته با تحلیل رفتار کاربران، می‌توانند تبلیغات شخصی‌سازی شده‌ای ارائه دهند که احتمالاً با علایق و نیازهای کاربران هم‌خوانی دارد. برای مثال شرکت فیسبوک از هوش مصنوعی برای تجزیه و تحلیل داده‌های کاربران و ارائه تبلیغات هدفمند استفاده می‌کند. این سیستم‌ها با تحلیل رفتار کاربران و تاریخچه تعاملات آن‌ها، تبلیغاتی را که با علایق و نیازهای آن‌ها تطابق دارد، نمایش می‌دهند؛ همچنین شرکت توییتر از هوش مصنوعی برای ارائه تبلیغات متناسب با علایق کاربران استفاده می‌کند. تبلیغات بر اساس رفتار کاربران در پلتفرم، توییت‌هایی که لایک کرده‌اند، اکانت‌هایی که دنبال می‌کنند و هشتگ‌هایی که استفاده می‌کنند، هدف‌گذاری می‌شوند. یوتیوب نیز از هوش مصنوعی برای نمایش تبلیغات هدفمند در ویدئوها استفاده می‌کند. سیستم‌های یوتیوب بر اساس محتوای ویدئوها و رفتار مشاهده‌کنندگان، تبلیغاتی را که احتمال کلیک بیشتری دارند، در ویدئوها قرار می‌دهند.

۳. تشخیص رفتارهای غیرقانونی یا مشکوک: الگوریتم‌های هوش مصنوعی قادرند فعالیت‌های مشکوک مانند تلاش برای هک کردن حساب‌های کاربری یا انتشار اطلاعات نادرست را شناسایی کنند و به‌سرعت اقداماتی برای مقابله با آن‌ها انجام دهند.

۴. تحلیل احساسات و داده‌های کاربران: هوش مصنوعی می‌تواند از تحلیل داده‌های کاربران برای تشخیص

1. **YouTube:** YouTube relies heavily on artificial intelligence to recommend videos to users. YouTube's algorithms analyze video content, viewing history, and user interests to place videos that are more likely to be viewed by the user on the home page and in suggested sections.

Facebook: Artificial intelligence algorithms are used on Facebook to analyze user behavior and create content recommendations. Based on user activity, posted content, likes, comments, and shares, these algorithms suggest content to users that they are likely to be interested in.

Twitter: Twitter uses artificial intelligence to manage the content of timelines and suggest topics and hash tags. Twitter's machine learning algorithms analyze user interactions and suggest tweets and accounts that may be of interest to the user.

احساسات و نظرهای آنان در خصوص موضوعات مختلف استفاده کند. این تحلیل‌ها به شرکت‌ها و سازمان‌ها کمک می‌کند تا بازاریابی و تعاملات خود را بهبود بخشند. با وجود کاربردهای گسترده هوش مصنوعی در رسانه‌های اجتماعی، چالش‌های متعددی نیز در این زمینه وجود دارد. الگوریتم‌های خودکار ممکن است دچار سوگیری شوند و به اشتباه محتوای مهم را حذف کنند یا به دلیل نبود شفافیت، کاربران درک دقیقی از نحوه عملکرد این الگوریتم‌ها نداشته باشند. همچنین، حفاظت از حریم خصوصی کاربران، یکی از مسائل حساس در این زمینه است؛ زیرا هوش مصنوعی از داده‌های کاربران برای تحلیل رفتارها و ارائه محتوای هدفمند استفاده می‌کند. در نهایت، رسانه‌های اجتماعی و هوش مصنوعی، به شکلی تنگاتنگ به یکدیگر وابسته‌اند. در حالی که هوش مصنوعی به پلتفرم‌ها کمک می‌کند تا با چالش‌های موجود مقابله کنند و تجربه کاربری را بهبود بخشند، نیاز به مقررات و سیاست‌های نظارتی جدید نیز برای مدیریت درست این فناوری‌ها احساس می‌شود (بانتین و گلبک،^۱ ۲۰۱۷).

ب. جایگاه قانونی پلتفرم‌های رسانه‌های اجتماعی در قبال تصمیم‌های خودکار

در دهه‌های اخیر، حجم بالای داده‌ها و محتوای تولید شده توسط کاربران، باعث شده است که این پلتفرم‌ها به‌طور فزاینده‌ای از هوش مصنوعی و الگوریتم‌های خودکار برای مدیریت و کنترل این محتوا استفاده کنند. این استفاده گسترده از هوش مصنوعی، چالش‌های متعددی را در زمینه مسئولیت‌های حقوقی و تنظیم مقررات ایجاد کرده است. در این بخش، به بررسی وضعیت حقوقی پلتفرم‌های رسانه‌های اجتماعی در قبال تصمیم‌های خودکار و مسئولیت‌های حقوقی آن‌ها در استفاده از هوش مصنوعی می‌پردازیم.

• وضعیت حقوقی پلتفرم‌ها

پلتفرم‌های رسانه‌های اجتماعی نظیر فیسبوک، توییتر، یوتیوب و اینستاگرام، معمولاً به‌عنوان واسطه‌های ارتباطی فعالیت می‌کنند. این واسطه‌ها، برای کاربران فضای مجازی فراهم می‌کنند تا محتواهای خود را منتشر کنند، بدون اینکه خودشان به‌طور مستقیم تولیدکننده یا کنترل‌کننده این محتوا باشند. این نقش واسطه‌گری باعث می‌شود که پلتفرم‌ها تا حدی، از مسئولیت مستقیم در قبال محتوای منتشرشده توسط کاربران معاف شوند. در بسیاری از نظام‌های حقوقی، از جمله در اروپا و آمریکا، مقرراتی وجود دارد که اگر واسطه‌های ارتباطی در ایجاد محتوا نقشی نداشته باشند، از مسئولیت مستقیم در قبال محتواهای غیرقانونی یا مضر معاف می‌شوند (بالکین^۲، ۲۰۱۸). یکی از مهم‌ترین قوانین در این زمینه، مقررات مربوط به «مسئولیت واسطه‌ها» است. برای مثال، در ایالات متحده، تحت بخش ۲۳۰ قانون نزاکت ارتباطات^۳، پلتفرم‌ها از مسئولیت مستقیم در قبال محتوای تولیدشده توسط کاربران معاف هستند. این قانون به پلتفرم‌ها اجازه می‌دهد

1. Buntain & Golbeck

2. Balkin

3. Communications Decency Act: Section 230 has two primary parts both listed under §230(c) as the "Good Samaritan" portion of the law. Under section 230(c) (1), as identified above, an information service provider shall not be treated as a "publisher or speaker" of information from another provider. Section 230(c) (2) provides immunity from civil liabilities for information service providers that remove or restrict content from their services they deem "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected", as long as they act "in good faith" in this action.

تا بدون نگرانی از مسئولیت قانونی، به کاربران امکان انتشار محتوا را بدهند، مگر در مواردی که خود پلتفرم به‌طور مستقیم، در تولید محتوا دخالت داشته باشد. در اتحادیه اروپا، «دستورالعمل تجارت الکترونیک» (DSA)^۱ که از سال ۲۰۲۰ تصویب شد، به پلتفرم‌ها معافیت مشابهی اعطا کرده است و بیان می‌کند که واسطه‌های اینترنتی، تنها در صورتی مسئول محتوای غیرقانونی خواهند بود که به‌طور فعال در ایجاد یا مدیریت آن مشارکت داشته باشند (گیلسپی^۲، ۲۰۱۸).

• مسئولیت حقوقی در قبال هوش مصنوعی

یکی از چالش‌های بسیار مهم پیش‌روی پلتفرم‌های دیجیتال، تعیین محدوده و مبنای مسئولیت حقوقی آن‌ها در استفاده از الگوریتم‌های خودکار و سامانه‌های هوش مصنوعی است. این فناوری‌ها وظایف حساسی مانند شناسایی و حذف محتوای غیرقانونی، مدیریت تبلیغات هدفمند و ارائه توصیه‌های شخصی‌سازی شده را برعهده دارند. در نتیجه، تصمیم‌های اتخاذشده توسط این الگوریتم‌ها، بر حقوق و منافع کاربران تأثیر مستقیم و گسترده‌ای دارد. با این حال، این الگوریتم‌ها می‌توانند دچار خطا یا سوگیری‌های ناخواسته شوند که پیامدهای منفی حقوقی و اجتماعی به‌دنبال دارد. برای نمونه، حذف اشتباه محتوای قانونی یا عدم شناسایی به‌موقع محتوای غیرقانونی، ممکن است به نقض آزادی بیان، تضییع حقوق کاربران یا حتی تسهیل انتشار محتوای آسیب‌زا بینجامد. در این وضعیت، دعاوی مسئولیت مدنی علیه پلتفرم‌ها قابل طرح خواهد بود. مبنای حقوقی این مسئولیت در نظام‌های مختلف می‌تواند متفاوت باشد؛ اما در اغلب موارد سه مبنای مطرح است:

نخست، مسئولیت مبتنی بر تقصیر است که بر اساس آن، اگر پلتفرم نتواند اثبات کند که تدابیر احتیاطی کافی برای جلوگیری از خطا یا سوگیری اتخاذ کرده است، مسئول شناخته می‌شود.

دوم، در برخی حوزه‌ها، مسئولیت بدون تقصیر یا مسئولیت مبتنی بر خطر اعمال می‌شود، به‌ویژه اگر استفاده از فناوری مخاطره‌آمیز تلقی شود و اثبات تقصیر عملی نباشد. در این چارچوب، اصل «احتیاط و پیشگیری»^۳ اهمیت زیادی دارد و پلتفرم باید ثابت کند که با رعایت استانداردهای فنی و مدیریتی معقول، خطرهای پیش‌بینی‌پذیر را کنترل کرده است (ویل و بورخسیوس^۴، ۲۰۲۱).

سوگیری‌های الگوریتمی از مصادیق مهم مسئولیت مدنی پلتفرم‌ها محسوب می‌شود. این سوگیری‌ها می‌توانند تصمیم‌های ناعادلانه‌ای را رقم بزنند که موجب تبعیض علیه گروه‌های خاص شود؛ برای مثال، الگوریتم‌های تبلیغات هدفمند یا پالایش محتوا ممکن است ناخواسته رفتار تبعیض‌آمیز داشته باشند. اگر ثابت شود طراحی یا مدیریت این الگوریتم‌ها با بی‌احتیاطی یا قصور همراه بوده یا استانداردهای ضد تبعیض رعایت نشده است، مبنای مسئولیت مدنی فراهم می‌شود.

در سطح حقوق تطبیقی، اتحادیه اروپا، در راستای تنظیم مسئولیت پلتفرم‌ها در قبال هوش مصنوعی گام‌های مهمی

1. Digital Services Act

2. Gillespie

3. Precautionary Principle

4. Veale & Borgesius

برداشته است. «قانون خدمات دیجیتال»^۱، مصوب ۲۰۲۲، الزامات جدیدی را برای شفافیت عملکرد الگوریتم‌ها، ارزیابی منظم ریسک و گزارش‌دهی دربارهٔ پیامدهای احتمالی فناوری‌های خودکار پیش‌بینی کرده است (کمیسیون اروپا^۲، ۲۰۲۲). به موجب این مقررات، عدم رعایت تدابیر پیشگیرانه و شفاف‌سازی، می‌تواند به مسئولیت حقوقی و جریمه‌های سنگین منجر شود. بنابراین، چارچوب نظارتی و تدابیر کنترلی‌ای که پلتفرم‌ها برای مدیریت سیستم‌های هوش مصنوعی به کار می‌گیرند، در تشخیص و میزان مسئولیت حقوقی آن‌ها نقش تعیین‌کننده‌ای دارد. اتخاذ استانداردهای قوی در طراحی، نظارت و پاسخ‌گویی، می‌تواند در مواردی موجب معافیت یا کاهش مسئولیت مدنی شود.

ج. تحلیل تطبیقی مبانی حقوقی حاکم در مسئولیت‌پذیری پلتفرم‌ها

برای پلتفرم‌های آنلاین حمایت‌ها و مصونیت‌های خاصی پیش‌بینی شده است که همگی به تفکیک در نظام‌های حقوقی اروپا، آمریکا و ایران مورد بحث و بررسی قرار خواهد گرفت.

اروپا

در اروپا، برای پلتفرم‌های آنلاین حمایت‌ها و مصونیت‌های خاصی پیش‌بینی شده است که این حمایت و مصونیت، در سال ۲۰۱۸، تحت دستورالعمل عمومی حمایت از داده‌ها (GDPR)^۳، دستورالعمل تجارت الکترونیک و اصل آزادی بیان را تبیین کرده است.

• دستورالعمل عمومی حمایت از داده‌ها (۲۰۱۸)

دستورالعمل عمومی حمایت از داده اروپا، عموماً در صورت برقرار بودن چهار شرط اجرا می‌شود: شخصی بودن، اطلاعات پردازش از سوی یک کنترل‌کننده و اصل سرزمینی بودن. پلتفرم‌های آنلاین، همواره کنترل‌کننده‌های اطلاعات خصوصی افرادند و بر این مبنا با حصول شرط دیگر، یعنی رعایت اصل سرزمینی بودن، مشمول مقررات دستورالعمل مزبور واقع می‌شوند. بر اساس دستورالعمل گروه کاری کمیسیون اروپایی در ارتباط با حفظ حریم خصوصی در اینترنت، کاربران پلتفرم‌های آنلاین دو حالت دارند: یا شخص ثالث محسوب می‌شوند یا آنکه در کنار پلتفرم‌ها، کنترل‌کننده قلمداد می‌شوند.

شبکه‌های اجتماعی و پلتفرم‌های آنلاین، از مصادیق بارز کنترل‌کننده‌های داده خصوصی منطبق با مقررات دستورالعمل عمومی حمایت از داده به حساب می‌آیند؛ زیرا اهداف و ابزار پردازش اطلاعات مزبور را مشخص می‌کنند^۴. چنانچه کاربر مشمول مقررات کنترل‌کنندگی باشد، به‌طور مشترک با پلتفرم آنلاین واجد مسئولیت خواهد بود. اگر فعالیت کاربر مصداق استفادهٔ شخصی و خانگی باشد، این مقررات فقط در خصوص پلتفرم آنلاین به اجرا گذاشته می‌شود، فرض اخیر مصداق بارز مسئولیت ناشی از فعل کاربر تلقی می‌شود.

1. Digital Services Act

2. European Commission

3. General Data Protection Regulation (GDPR)

۴. مطابق بند ۷ ماده ۴ دستورالعمل مزبور، کنترل‌کننده عبارت است از شخص حقیقی یا حقوقی... که اهداف و ابزار پردازش اطلاعات را مشخص می‌سازد.

نقض داده‌های خصوصی زمانی محقق می‌شود که عدم مقابله مقتضی و به‌موقع به آن، به خسارت فیزیکی، مادی یا غیرمادی به اشخاص حقیقی (از قبیل از دست دادن کنترل روی داده‌های خطی یا تحدید حقوق تبعیض سرقت هویت یا کلاهبرداری)، زیان مالی آسیب به شهرت یا محرمانگی اطلاعاتی که به‌شکل حرفه‌ای محافظت شده‌اند یا هرگونه زیان مالی یا اجتماعی منتهی شود؛ بنابراین به محض اطلاع پلتفرم آنلاین از وقوع نقض این امر، باید به‌سرعت به آگاهی مقامات مربوط برسد تا تدابیر مقتضی اتخاذ شود؛ جز در حالتی که وفق مقررات دستورالعمل مزبور، پلتفرم دارای عذر موجه است، نباید در مسئولیت مدنی پلتفرم تردید به خود راه داد (حسام، مدیو جونی، میری و یمرلی، ۱۴۰۰: ۷۶-۷۵).

• شرایط مسئولیت

پردازش اطلاعات شخصی کاربران از طریق پلتفرم‌های آنلاین، در صورت حصول برخی شرایط می‌تواند به مسئولیت پلتفرم‌ها منجر شود؛ برخلاف دستورالعمل تجارت الکترونیک اروپا که به موجب آن، آن پلتفرم‌های آنلاین از نوعی مصونیت ابتدایی برخوردارند بر اساس دستورالعمل حمایت از داده، پلتفرم‌های آنلاین واجد برخی تکالیف هستند. در صورت انجام ندادن این تکالیف، مشمول مسئولیت ناشی از نقض حریم اطلاعاتی از سوی کاربران خواهند شد. مستفاد از ماده ۱۷ این دستورالعمل، پلتفرم آنلاین باید تدابیر فنی و سازمانی مناسب را برای حمایت از اطلاعات خصوصی در برابر تخریب اتفاقی یا غیرقانونی خسارت اتفاقی، تغییر، افشا یا دسترسی بدون مجوز به‌ویژه در جایی که پردازش شامل ارسال اطلاعات در شبکه بوده، اتخاذ کند. به موجب ماده ۲۳ همان دستورالعمل نیز، هر فعل یا ترک فعل مغایر با این دستورالعمل‌ها این دستورالعمل که به بروز زیان منتهی شود، موجبات مسئولیت پلتفرم‌های آنلاین را فراهم می‌سازد. در این فرض، رفتار کاربر به همراه رفتار پلتفرم، به نقض حریم اطلاعاتی منتهی می‌شود؛ بنابراین کاربر ناقض و پلتفرم آنلاین، به‌طور مشترک در برابر صاحب حق واجد مسئولیت مدنی هستند (اسمیت^۱، ۲۰۲۰؛ ون در اسلوت^۲، ۲۰۱۵).

• دستورالعمل تجارت الکترونیک

مستفاد از اصل مصونیت عمومی مقرر در ماده ۱۲ دستورالعمل تجارت الکترونیک، هرگاه سه شرط حاصل شود، پلتفرم آنلاین از مسئولیت ناشی از افعال کاربران مصون خواهد بود: ۱. پلتفرم ارسال اطلاعات را آغاز نکرده باشد؛ ۲. دریافت‌کننده اطلاعات ارسالی را تعیین نکرده باشد؛ ۳. پلتفرم اطلاعات را گزینش یا اصلاح نکرده باشد. علاوه‌براین، مستنبط از ماده ۱۴ این دستورالعمل، پلتفرم آنلاین در صورت احراز شرایط زیر فاقد مسئولیت در قبال اطلاعات ذخیره شده از سوی کاربران خود نخواهد بود: ۱. پلتفرم علم حقیقی یا نوعی به ماهیت غیرقانونی فعالیت کاربر یا اطلاعات مزبور نداشته باشد و ۲. با فرض وجود چنین علمی، به‌سرعت به حذف اطلاعات مرقوم یا قطع دسترسی به چنین اطلاعاتی اقدام کرده باشد (اسمیت، ۲۰۲۰: ۲۱۳).

ممکن است اطلاعاتی که از سوی کاربر در پلتفرم ارسال یا ذخیره شده، متضمن نقض حریم خصوصی دیگری باشد. در این صورت، مسئله مسئولیت پلتفرم در قبال چنین امری مطرح می‌شود. بدیهی است هرگاه پلتفرم آنلاین، مشمول قواعد یاد شده باشد، فاقد مسئولیت خواهد بود. این استدلال به‌ویژه از آن جهت قابل تأیید است که به موجب

1. Smith

2. Van der Sloot

ماده ۱۵ از همان دستورالعمل، عرضه‌کنندگان خدمات اینترنتی، فاقد تکلیف ایجابی بررسی اطلاعات ارسالی یا ذخیره شده از سوی کاربران خود هستند. دیوان دادگستری اروپا نیز، در یکی از آرای خود، این امر را تأیید کرده است. این دادگاه در پرونده‌ای بی، اعلام کرد که صرف ذخیره اطلاعات کلی از سوی پلتفرم آنلاین ای بی که البته متضمن داده‌های غیرقانونی است، نمی‌تواند دستاویزی برای تحمیل مسئولیت برای ای بی باشد (حسام و همکاران، ۱۴۰۰: ۷۷).

• اصل آزادی

اشخاص حقوقی مانند پلتفرم‌های آنلاین نیز می‌توانند به این اصل استناد کنند. به موجب ماده ۱۰ کنوانسیون حقوق بشر اروپا، هر شخصی، بدون دخالت مراجع عمومی و بدون هیچ مرزی از حق آزادی بیان برخوردار است. این حق شامل آزادی ابراز عقیده و دریافت و فهم اطلاعات و ایده‌هاست. البته این ماده مانع از آن نمی‌شود که دولت‌ها الزاماتی را برای صدور مجوز پخش رادیو تلویزیونی یا مؤسسه‌های سینمایی مقرر کنند. به موجب رأی دیوان دادگستری و حقوق بشر اروپا، این اصل علاوه بر ایده‌ها و اطلاعات مشروع اطلاعات نامشروع را نیز دربرمی‌گیرد؛ بنابراین اگر کاربری با استفاده از امکان استوری در پلتفرم اینستاگرام موجب هتک حریم خصوصی دیگری شود، اینستاگرام می‌تواند با استناد به اصل آزادی بیان از مسئولیت احتمالی مبرا شود (اسمیت، ۲۰۲۰: ۲۲۱).

با این حال، اصل آزادی بیان رسانه‌ها و کاربران آن‌ها با اصل رعایت حریم خصوصی دیگران، ممکن است در تراحم باشد. در چنین وضعیتی، یافتن معیارهایی برای برقراری موازنه میان این دو حق، از اهمیت بسزایی برخوردار است. دیوان دادگستری اروپا، در پرونده دلفی، معیارهایی را به همین منظور مقرر کرده است که عبارت‌اند از: منافع عمومی شهرت شخص موضوع پرونده هدف، گزارش رفتار قبلی شخص موضوع پرونده، روش دستیابی به اطلاعات و صحت آن‌ها، محتوا، شکل و تبعات ناشی از نشر و شدت ضمانت اجرای تحمیلی بر شخص (دلفی / استونیا، پارا ۸۳). بنابراین هرگاه کاربری با استفاده از پلتفرم‌های آنلاین، به هتک حریم خصوصی افراد مبادرت کند، پلتفرم با استناد به اصل آزادی بیان مقرر در ماده کنوانسیون حقوق بشر اروپا، از مسئولیت مدنی معاف می‌شود. با وجود اینکه مطابق دستورالعمل مورد بحث در اروپا، به ظاهر پلتفرم‌های آنلاین واجد مسئولیت اولیه در نظارت بر عملکرد کاربران خود هستند، به موجب بند ۲۱ از مقدمه همان دستورالعمل، اعمال آن قاعده نمی‌تواند به تخطی از مقررات مسئولیت مندرج در مواد ۱۲ تا ۱۵ دستورالعمل تجارت الکترونیک پلتفرم‌ها یا صرفاً نقش کانال عبور ۲۰۰۰ اروپا منجر شود. در برخی موارد، پلتفرم‌ها یا صرفاً نقش کانال عبور را دارند و اطلاعات را ذخیره می‌کنند یا میزبانی شبکه را برعهده می‌گیرند. در این موارد پلتفرم فاقد مسئولیت است.

امریکا

برخلاف اروپا که مقررات جامع و منسجمی برای مسئولیت پلتفرم‌ها در خصوص نقض حریم خصوصی اطلاعات وجود دارد، مقررات مشابهی در آمریکا وجود ندارد. اصول و قواعد حاکم بر مسئولیت مدنی ناشی از نقض حریم خصوصی اطلاعات در قوانین، مقررات و دستورالعمل‌های پراکنده فدرال و ایالتی گنجانده شده است.

• اصل

در حقوق آمریکا، اصل کلی این است که پلتفرم‌ها در قبال محتوای زیان‌بار کاربران مسئولیتی ندارند. این اصل عمومی در ماده ۲۳۰ قانون نزاکت^۱ در ارتباطات ۱۹۹۶ آمریکا، به‌صراحت بیان شده است؛ به موجب این ماده «هیچ عرضه‌کننده ... خدمات کامپیوتری ارتباط متقابل به‌عنوان ناشر یا گوینده اطلاعات تهیه شده توسط تهیه‌کننده محتوای اطلاعاتی دیگری محسوب نمی‌شود». بر این مبنا، پلتفرم‌های آنلاین از مصونیتی کلی نسبت به اعمال زیان‌بار کاربران خود برخوردارند. این مصونیت منوط به آن است که پلتفرم فقط عرضه‌کننده خدمات ارتباطات متقابل باشد و چنانچه علاوه‌براین، در تهیه محتوای اطلاعاتی نیز ایفای نقش کند، واجد مسئولیت خواهد بود؛ البته در فرض اخیر، مسئولیت پلتفرم ناشی از فعل شخصی خود است، نه رفتار کاربران. مادامی که پلتفرم فقط نقش واسطه را ایفا می‌کند، در قبال محتوای زیان‌بار کاربران خود مسئولیتی ندارد (حسام و همکاران، ۱۴۰۰: ۷۹-۷۷).

اما وقتی خود پلتفرم در تولید محتوای غیرقانونی فعالیت می‌کند، مشمول عنوان ناشر و گوینده و واجد مسئولیت شخصی خواهد بود. پلتفرم‌ها به‌دلیل نقش واسطه‌ای خود و ارائه تسهیلات به کاربران، مشمول قاعده حقوقی «نیکوکار خوب»^۲ تلقی می‌شوند (سوانیان^۳، ۲۰۱۴: ۱۳۱) و به همین سبب تا زمانی که حسن نیتشان محرز باشد یا خلاف آن به هر طریقی اثبات نشود، مصون از مسئولیت در قبال اعمال زیان‌بار کاربران هستند. مصونیت پلتفرم‌ها، مبتنی بر ماده ۲۳۰ قانون فوق، به حدی است که حتی، اگر پلتفرم بعد از دریافت اخطاریه حذف پُست، از آن قصور کند، بازهم دادگاه پلتفرم را مصون از مسئولیت می‌داند.

در پرونده‌های آمریکا آنلاین^۴ مارک زاکربرگ و فیسبوک^۵، دادگاه به‌رغم احراز قصور پلتفرم آنلاین در حذف پُست توهین‌آمیز کاربرش، با استناد به نص ماده مزبور، ادعای خواهان مبنی بر مسئولیت پلتفرم را رد کرد. در دعوا علیه پلتفرم‌های اسپیس نیز با این استدلال که این پلتفرم در تأیید سن کاربر دچار تقصیر شده و در نتیجه کاربر ۱۳ ساله، خود را ۱۸ ساله جا زده، دادگاه با استناد به ماده ۲۳۰ قانون مرقوم، مای اسپیس را از مسئولیت مبرا دانست.^۶ همچنین مطابق این قانون، سایت‌های «قرار عاشقانه» نیز از مسئولیت ناشی از اعمال زیان‌بار کاربران مصون هستند. در پرونده مترواسپلش^۷، دادگاه به استناد به همان ماده، درخواست حکم به مسئولیت سایت قرار عاشقانه‌ای را که کاربری با ایجاد پروفایل جعلی در آن، به زیان یکی از افراد مشهور عمل کرده بود، مردود اعلام کرد.^۸

• استثنا

با وجود ماده ۲۳۰ قانون نزاکت در ارتباطات، در صورت احراز برخی شروط، ممکن است پلتفرم‌ها مسئول اعمال زیان‌بار کاربران خود شناخته شوند. مطابق بند ۴ قسمتی از همان ماده، «هیچ چیزی در این ماده نباید به‌گونه‌ای تفسیر شود که

1. Communications Decency Act

2. Good samaritan

3. Sevanian

4. Zeran v. America online, Inc...129 F.3d 327-courts of appeals, 4th circuit 1997.

5. Klayman v. Zuckerberg, 753 F.3d 1354 - courts of appeals, Dist. Of Columbia circuit 2014.

6. Doe v. MySpace, Inc., 528 F3d 413, 416 (5th Cir.2008).

7. Metrosplash

8. Carafano v.Metrosplash.com, Inc., 339 F.3d 1119, 1121, 1125 (9th cir.2003).

اعمال قانون محرمانگی ارتباطات ۱۹۸۶ یا اصلاحات راجع به آن یا مقررات ایالتی مشابه را محدود کند». در نظام حقوقی امریکا، بر مبنای نظریه مسئولیت مشارکتی و نیابتی، ممکن است مسئولیت بر کسی غیر از مباشر اصلی خطا تحمیل شود. گاه پلتفرم قطع نظر از وجه واسطه‌ای در نشر محتوا، مرتکب تقصیری می‌شود که ضرر حاصل از محتوای نامشروع قابل انتساب به او نیز می‌گردد. مسئولیت مشارکتی در این مورد مسئولیت، پلتفرم مبتنی بر تقصیر است (بویل و جنکینز^۱، ۲۰۱۸: ۵۱۹).

هرگاه به هر دلیلی، حسن نیت پلتفرم مخدوش شود یا عمل زیان‌بار به طریقی به پلتفرم نسبت داده شود یا به عبارت دیگر، عملکرد پلتفرم از حالت واسطه به ناشر یا گوینده تغییر یابد، مسئله شرکت در مسئولیت محقق می‌شود. اثبات چنین مسئولیتی در عمل بسیار دشوار است؛ زیرا مسئولیت مشارکتی منوط به احراز تقصیر عمدی یا علم پلتفرم آنلاین به وقوع نقض حریم خصوصی است. با این همه، دست کم یک دادگاه در این زمینه حکم به مسئولیت مدنی واسطه‌ها داده است. دادگاه در این پرونده روزنامه‌ای را که به واسطه انتشار یک آگهی موجب تجاوز به حریم خصوصی دیگری شده بود، واجد مسئولیت مدنی تشخیص داد.

در میان قوانین فدرال، قانون حمایت از حریم خصوصی کودکان در محیط آنلاین، نمونه مناسبی است که ممکن است به موجب آن، مشارکت در مسئولیت علیه پلتفرم آنلاین قابل استنباط باشد. در نظام حقوقی آمریکا، قانون مزبور به همراه آیین‌نامه اجرایی کمیسیون تجارت فدرال، مجموعه مقررات حاکم بر دریافت و استفاده از اطلاعات کودکان است. به موجب این قانون و آیین‌نامه، اپراتورهای آنلاین نیز مانند پلتفرم‌های آنلاین، از دریافت و استفاده از اطلاعات شخصی کودکان زیر ۱۳ سال بدون رضایت والدینشان منع شده‌اند. علاوه بر این، پلتفرم‌ها مکلف‌اند والدین کودکان را از سیاست‌های حریم خصوصی خود آگاه سازند.

همچنین پلتفرم‌های آنلاین تکلیف دارند در مواردی که به گردآوری اطلاعات شخصی کودکان اقدام می‌کنند، به شکل بارزی سیاست‌های حریم خصوصی خود را نمایش دهند و در صورت گردآوری اطلاعات از سوی پلتفرم‌ها نیز آن‌ها ملزم شده‌اند که تدابیر متعارف را به منظور حفظ محرمانگی، امنیت و تمامیت این اطلاعات اتخاذ کنند. هرگاه پلتفرم آنلاین در خصوص الزامات خود دچار تقصیر شود، این سؤال مطرح می‌شود که آیا در صورت نقض حریم خصوصی داده‌های کودکان، می‌توان حکم به مسئولیت مشارکتی پلتفرم داد؟ مطابق قاعده عمومی احراز مسئولیت مشارکتی، چنانچه پلتفرم مقصر شناخته شود و این تقصیر نقشی اساسی در وقوع نقض داشته باشد، امکان تحمیل مسئولیت مشارکتی بر پلتفرم دور از ذهن نخواهد بود.

• بررسی موضع حقوق ایران

قواعد مسئولیت مدنی در نظام حقوقی ایران، مبتنی بر فقه امامیه به اتلاف و تسبیب قابل تقسیم است؛ در اتلاف تقصیر شرط نیست و صرف احراز رابطه سببیت برای اثبات مسئولیت کافی است. در مقابل، اصولاً مسئولیت ناشی از سببیت در ورود ضرر، منوط به احراز تقصیر شده است. ماهیت ضررهای ناشی از اعمال کاربران پلتفرم‌های آنلاین به گونه‌ای است

که شمول قواعد تسبیب بر پلتفرم‌ها را به ذهن متبادر می‌سازد؛ زیرا برای مثال، در جایی که شخصی به‌واسطه پلتفرم دیوار، اسنپ یا دیجی‌کالا، از سوی کاربر دیگری مورد سوءاستفاده قرار می‌گیرد، کاربری که سوءاستفاده کرده است، مباشر ورود ضرر و پلتفرم دیوار، اسنپ یا دیجی‌کالا سبب ورود ضرر تلقی می‌شوند؛ بنابراین جز در فرضی که مرتکب تقصیر نشوند، فاقد مسئولیت خواهند بود.

البته این استدلال، ناظر بر فرض تحقق سببیت محض در ورود ضرر است؛ وگرنه، وقتی کاربری به‌واسطه پلتفرم دیوار به کسی زیان می‌زند، اجتماع مباشر و سبب حاصل قاعده مسئولیت در فرض اجتماع مباشر و سبب حاکم است. حکم کلی مسئولیت در این زمینه، مقتبس از نظر مشهور و اجماعی در فقه امامیه، جز در صورت اقوی بودن سبب اصل مسئولیت مباشر است. به همین سبب است که مسئولیت طرح شده در این آیین‌نامه‌ها بازتابی از قواعد عمومی مسئولیت مدنی در حقوق ایران است و مطالعه برخی مواد آن‌ها به‌خوبی از این امر حکایت دارد. در مقدمه مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای مصوب ۱۳۸۰ شورای عالی انقلاب فرهنگی، آمده است که این مقررات با تأکید بر برخی نکات اساسی، از جمله مسئولیت حقوقی و مدنی افراد در قبال فعالیت‌های خود تنظیم می‌شوند. تأکید بر اینکه مسئولیت مدنی افراد در فضای اینترنتی، صرفاً در قبال فعالیت خود آنان خواهد بود، از همان ابتدا نشان می‌دهد که شورای عالی انقلاب فرهنگی، ضمن پایبندی به اصول کلی مسئولیت مدنی در ایران از جمله اصل شخصی بودن مسئولیت، به تصویب چنین ضوابطی همت گمارده است (نجفی و مدنی، ۱۳۹۹: ۴۷۴-۴۷۵).

علاوه‌براین، در مواد مختلف آیین‌نامه موصوف به عدم مسئولیت رساها^۱، به سبب تخلف کاربران اشاره شده است. به موجب ماده ۱-۳-۵ این آیین‌نامه، رسانه‌ها و کاربران، در قبال محتوایی که خود روی شبکه عرضه می‌کنند، مسئولیت دارند. همچنین به موجب ماده ۳-۵-۴ آیین‌نامه واحدهای ارائه‌کننده خدمات اطلاع‌رسانی و اینترنت رسا ISP، مسئولیت رسا ISP در مورد دسترسی به اطلاعات عرضه شده از سوی دیگران، به ایجاد امکان و اعمال برقراری پالایه در شبکه محدود خواهد بود. حال چنانچه رسا در انجام چنین تکلیفی قصور ورزد و در نتیجه این قصور، حریم خصوصی کاربران نقض شود، آیا می‌توان با استناد به آن، رسا را در قبال رفتار ناقض حریم خصوصی واجد مسئولیت مدنی تلقی کرد؟

در این مورد ناقض حریم خصوصی مباشر نقض و رسا، سبب نقض عمومی به حساب می‌آید و فرض اجتماع مباشر و سبب محقق می‌شود. قاعده عمومی در نظام حقوقی ایران، در چنین فرضی مسئولیت را با مباشر می‌داند، مگر سبب اقوی باشد، به نظر می‌رسد که به‌رغم قصور رسا در پالایه، وقتی کاربری با اراده مرتکب نقض حریم خصوصی دیگری می‌شود، در هر حال اقوی تلقی می‌شود و حکم به مسئولیت وی از وجه منطقی بیشتری برخوردار است. با این حال، ممکن است ادعا شود که در این موارد، از آنجا که اگر فضای فراهم آمده از طریق رسا وجود نداشت، نقض حریم خصوصی منتفی می‌شد. دست‌کم حکم به مسئولیت رسا در کنار مسئولیت مباشر، مطلوب به نظر می‌رسد. این استدلال را می‌توان بر مبنای ملاک مقرر در ماده ۵۲۶ قانون مجازات اسلامی ۱۳۹۲، قابل قبول دانست. بر اساس این ماده «هرگاه دو یا چند عامل، برخی به مباشرت و بعضی به تسبیب در وقوع جنایتی تأثیر داشته باشند، عاملی که جنایت مستند به اوست، ضامن است و چنانچه جنایت مستند به تمام عوامل باشد، به‌طور مساوی ضامن می‌باشند، مگر تأثیر رفتار مرتکبان

۱. رساننده خدمات اینترنتی یا رسا که از آن باواژه ISP

متفاوت باشد که در این صورت، هر یک به میزان تأثیر رفتارشان مسئول هستند. در صورتی که مباشر در جنایت بی‌اختیار، جاهل صغیر غیر ممیز یا مجنون و مانند آن‌ها باشد، فقط سبب ضامن است». در موردی که به سبب قصور رسا، کاربری مبادرت به نقض حریم خصوصی دیگری می‌کند، عرف می‌تواند ورود ضرر را به کاربر ناقض و رسا نسبت دهد و در نتیجه حکم به مسئولیت مساوی آنان کند.

با این همه، از آنجایی که حکم مندرج در این ماده قانونی، مخالف نظر مشهور در فقه امامیه و حقوق ایران است، باید آن را به شکل مضیق تفسیر کنیم و صرفاً ناظر بر اجتماع عرضی اسباب بدانیم. مورد بحث، از مصادیق اجتماع طولی اسباب است و در نتیجه مشمول قاعده مشهور مسئولیت در این زمینه که همان مسئولیت مباشر است تلقی می‌شود. پایبندی به اصول و قواعد مسئولیت مدنی در برخی لوایح ارائه شده به مجلس نیز قابل مشاهده است. به همین دلیل است که در لایحه جامع رسانه‌های همگانی در تبصره ۳ ماده ۱۱ آمده است: تبصره ۳- مطالب اختصاصی رسانه‌ها - اگر نام پدیدآورنده اثر، به نام اصلی یا مستعار منتشر شود، به نام او و در غیر این صورت به نام رسانه مشمول قوانین و مقررات مربوط می‌باشد». به موجب این ماده، اصل شخصی بودن مسئولیت در فضای رسانه‌های همگانی نیز مراعی است و چنانچه شخصی با استفاده از این رسانه‌ها که طبق تعریف شامل پلتفرم‌های آنلاین هم می‌شود (برای مثال، پلتفرم آنلاینی که به عنوان یک رسانه خبری فعالیت می‌کند) اقدام به نقل به نقض حریم خصوصی دیگری کند، خود شخص مسئول است.

طرح قانون حمایت از حقوق کاربران و خدمات پایه کاربردی فضای مجازی که ذیل اصل ۸۵ قانون اساسی قرار گرفته، متضمن مقرراتی است که در صورت تصویب نهایی در کمیسیون‌های مربوطه، شائبه امکان تحمیل مسئولیت بر پلتفرم‌های آنلاین را فراهم می‌سازد.

با این همه مذاقه، در مفاد این طرح نشان می‌دهد که واضعان آن نیز ضمن پایبندی به اصول کلی مسئولیت مدنی، اقدام به تدوین چنین طرحی کرده‌اند. در این طرح، تکالیف مشخصی بر عهده پلتفرم‌های آنلاین نهاده شده است. به موجب تبصره ۵ ماده ۲ این طرح، کلیه پیام‌رسان‌های اجتماعی داخلی و همچنین نمایندگی پیام‌رسان‌های خارجی اثرگذار (حسب توافقات انجام شده در مذاکرات رسمی) ملزم به رعایت مصوبات کارگروه تعیین مصادیق مجرمانه و موارد ابلاغی دبیرخانه کارگروه در راستای پالایش مصادیق مجرمانه می‌باشند». مسئولیت پیام‌رسان‌های اجتماعی در این تبصره، به پالایش مصادیق مجرمانه محدود شده است. مطابق تبصره ۶ همان ماده نیز، کلیه پیام‌رسان‌های اجتماعی موضوع این قانون مشمول تکالیف و مسئولیت‌های ناظر بر فعالیت ارائه‌دهندگان خدمات دسترسی و میزبانی مندرج در فصل جرایم رایانه‌ای قانون مجازات اسلامی و بخش دهم قانون آیین دادرسی کیفری می‌باشند». بررسی مقررات قانون جرایم رایانه‌ای و بخش دهم آیین دادرسی کیفری، از مسئولیت مدنی پیام‌رسان‌های اجتماعی حکایت ندارد؛ زیرا بر اساس مفاد مواد ۲۱ تا ۲۳ قانون جرایم رایانه‌ای، تکالیف ارائه‌دهندگان خدمات دسترسی محدود به پالایش و قطع ادامه دسترسی و نقض این تکالیف، حسب مورد ممکن است صرفاً به انحلال، جزای نقدی یا تعطیلی موقت منجر شود. فصل هفتم این طرح ذیل عنوان مسئولیت در پیام‌رسان‌های اجتماعی، به نحو کلی مسئولیت در پیام‌رسان‌های اجتماعی را مطرح کرده است. به موجب بند ۱ ماده ۷ این طرح، مدیران پیام‌رسان‌های اجتماعی و ارائه‌دهندگان و میزبانی، حسب مورد مکلف به صیانت از داده‌های خصوصی خدمات دسترسی و اشخاص اعم از حقیقی و حقوقی بوده و...».

جمع بین این مواد و مقررات با مفاد مواد ۱۵ تا ۲۰ طرح مزبور که به ضمانت اجراهای نقض مقررات این طرح پرداخته نشان می‌دهد که مفاد هم‌سو با قواعد عمومی مسئولیت مدنی است و نمی‌توان بر اساس آن، مسئولیت مدنی پلتفرم‌ها یا مدیران و مسئولان نشان ناشی از نقض حریم خصوصی افراد را استنباط کرد. آنچه به‌عنوان ضمانت اجرای این قانون آمده، چیزی جز حبس، جزای نقدی یا ... نیست و با عنایت به سکوت در خصوص مسئولیت مدنی تردیدی در شمول قواعد عمومی مسئولیت مدنی، آن گونه که پیشتر توضیح داده شد، باقی نمی‌ماند (حسام و دیگران، ۱۴۰۰: ۸۴-۸۱).

د. چالش‌های حقوقی و اجتماعی در مسئولیت‌پذیری پلتفرم‌ها

پلتفرم‌های رسانه‌های اجتماعی به‌عنوان بازیگران اصلی در دنیای دیجیتال امروز، در قبال کاربران و جامعه مسئولیت‌های مهمی دارند. با توسعه سریع فناوری هوش مصنوعی و استفاده گسترده از الگوریتم‌های خودکار در تصمیم‌گیری‌های این پلتفرم‌ها، چالش‌های جدیدی در زمینه حقوقی و اجتماعی ظهور کرده‌اند. سه محور اصلی در این چالش‌ها، شامل شفافیت و پاسخ‌گویی، تبعیض و تعصبات الگوریتمی و حقوق کاربران و حفاظت از داده‌ها هستند که در ادامه به بررسی آن‌ها پرداخته خواهد شد.

• شفافیت و پاسخ‌گویی

ضرورت شفافیت در تصمیم‌گیری‌های الگوریتمی پلتفرم‌های رسانه‌های اجتماعی، به‌طور گسترده از الگوریتم‌های هوش مصنوعی برای مدیریت محتوا، تبلیغات و تعاملات کاربران استفاده می‌کنند. این الگوریتم‌ها می‌توانند به‌طور خودکار تصمیم‌هایی مانند حذف یا سانسور محتوا، پیشنهاد دوستان جدید یا نمایش تبلیغات را بگیرند. با این حال، کاربران اغلب نمی‌دانند که چگونه این تصمیمات اتخاذ می‌شوند و چه معیارهایی در آن‌ها دخیل است. عدم شفافیت در تصمیم‌گیری‌های الگوریتمی، می‌تواند به کاهش اعتماد کاربران به این پلتفرم‌ها منجر شود. شفافیت به‌معنای ارائه اطلاعات دقیق درباره نحوه عملکرد الگوریتم‌ها و تأثیرات آن‌ها بر کاربران است. برای مثال، اتحادیه اروپا با تصویب قانون خدمات دیجیتال^۱ در سال ۲۰۲۲، پلتفرم‌ها را ملزم کرده است که اطلاعات بیشتری درباره نحوه کارکرد الگوریتم‌ها و فرایندهای تصمیم‌گیری خود ارائه دهند (کمیسیون اروپا، ۲۰۲۲). پلتفرم‌ها باید در قبال تصمیم‌های خودکار الگوریتمی که به‌طور مستقیم یا غیرمستقیم بر کاربران تأثیر می‌گذارد، پاسخ‌گو باشند. در صورتی که این تصمیم‌ها به حذف اشتباه محتوای کاربران یا تضعیف حقوق آزادی بیان آنان منجر شود، کاربران باید امکان اعتراض و درخواست بازنگری داشته باشند. پاسخ‌گویی به‌معنای فراهم کردن سازوکارهای مناسب، برای رسیدگی به شکایت‌های کاربران و اصلاح تصمیم‌های اشتباه است. برای نمونه، قانون عمومی حفاظت از داده‌ها در اتحادیه اروپا، حق کاربران را در خصوص اعتراض به تصمیم‌های خودکار توسط الگوریتم‌ها به رسمیت شناخته و پلتفرم‌ها را موظف به ارائه توضیحات در خصوص این تصمیم‌ها کرده است (پاسکوئال^۲، ۲۰۱۵).

• تبعیض و تعصب‌های الگوریتمی

بروز سوگیری‌های ناخواسته در الگوریتم‌ها، یکی از چالش‌های بسیار مهم حقوقی و اجتماعی، در استفاده از هوش مصنوعی در پلتفرم‌های رسانه‌های اجتماعی، تبعیض و تعصب‌های الگوریتمی است. الگوریتم‌ها ممکن است به دلیل نوع داده‌هایی که بر اساس آن‌ها آموزش داده شده‌اند یا نحوه طراحی آن‌ها، تصمیم‌های ناعادلانه‌ای بگیرند. به طور مثال، مطالعات نشان داده است که برخی الگوریتم‌ها ممکن است به طور ناعادلانه تبلیغات یا محتواهای خاصی را به گروه‌های اقلیت نرسانند یا در مدیریت محتوای کاربران دچار تبعیض شوند. مسئولیت پلتفرم‌ها در مقابله با تبعیض الگوریتمی پلتفرم‌ها، باید به طور فعال تلاش کنند تا سوگیری‌های ناخواسته در الگوریتم‌های خود را شناسایی و اصلاح کنند. این شامل بازبینی دقیق فرایندهای تصمیم‌گیری الگوریتمی و ارزیابی منظم الگوریتم‌ها برای جلوگیری از بروز تبعیض می‌شود. به طور مثال، برخی شرکت‌ها با اجرای روش‌های نظارت بر عملکرد الگوریتم‌ها و استفاده از داده‌های متنوع‌تر، سعی در کاهش سوگیری‌های ناعادلانه دارند. علاوه بر این، قوانین مختلف نیز به این مسئله پرداخته‌اند. برای مثال، قانون هوش مصنوعی اتحادیه اروپا (که هنوز در مراحل اولیه تدوین است) پلتفرم‌ها را موظف می‌کند تا از ایجاد سوگیری‌ها و تبعیض‌های ناعادلانه توسط الگوریتم‌های هوش مصنوعی جلوگیری کنند و در صورت بروز چنین مشکلاتی، پاسخ‌گو باشند.

• حقوق کاربران و حفاظت از داده‌ها

حفاظت از حریم خصوصی کاربران یکی دیگر از چالش‌های مهم حقوقی در زمینه مسئولیت‌پذیری پلتفرم‌های رسانه‌های اجتماعی، حفاظت از داده‌های شخصی کاربران است. پلتفرم‌های رسانه‌های اجتماعی به طور گسترده‌ای از داده‌های کاربران برای بهبود الگوریتم‌ها و ارائه تبلیغات هدفمند استفاده می‌کنند. این امر نگرانی‌های جدی‌ای را در مورد نقض حریم خصوصی و سوءاستفاده از داده‌های کاربران ایجاد کرده است. در اتحادیه اروپا، قانون عمومی حفاظت از داده‌ها به عنوان یکی از سخت‌گیرانه‌ترین قوانین حفاظت از داده‌ها، پلتفرم‌ها را ملزم به رعایت حقوق کاربران در زمینه جمع‌آوری، پردازش و استفاده از داده‌های شخصی آن‌ها کرده است. بر اساس این قانون، کاربران حق دارند بدانند چه داده‌هایی از آن‌ها جمع‌آوری می‌شود و چگونه مورد استفاده قرار می‌گیرد. همچنین، آن‌ها می‌توانند درخواست کنند داده‌های آن‌ها حذف یا اصلاح شود. حق کاربران به اطلاعات و کنترل بر داده‌های خود یکی از حقوق اصلی کاربران در زمینه حفاظت از داده‌ها، حق دسترسی به اطلاعات و کنترل بر داده‌های شخصی آن‌ها است. کاربران باید قادر باشند تا اطلاعات دقیقی در مورد نحوه استفاده پلتفرم‌ها از داده‌هایشان دریافت کنند و در صورت لزوم بتوانند از ادامه پردازش داده‌ها توسط پلتفرم جلوگیری کنند. این موضوع، به ویژه در زمینه استفاده از داده‌ها برای تصمیم‌های خودکار هوش مصنوعی اهمیت دارد. پلتفرم‌ها باید به کاربران توضیح دهند که چگونه داده‌های آن‌ها در تصمیمات الگوریتمی دخالت دارد و چه تأثیراتی بر زندگی آن‌ها خواهد داشت (پاسکونال، ۲۰۱۵). علی‌رغم وجود قوانینی مانند مقررات عمومی حفاظت از داده‌ها، چالش‌های متعددی در زمینه حفاظت از داده‌های کاربران وجود دارد. یکی از این چالش‌ها، تأثیر فرامرزی پلتفرم‌هاست. پلتفرم‌های جهانی مانند فیسبوک و توییتر، به دلیل فعالیت در کشورهای مختلف با قوانین متنوعی مواجهند که رعایت هم‌زمان آن‌ها، می‌تواند پیچیده باشد. این مسئله نیاز به همکاری بین‌المللی برای هماهنگ‌سازی قوانین و

تنظیم مقررات فرامرزی را مطرح کرده است. پلتفرم‌های رسانه‌های اجتماعی، به نحو بسیار فزاینده‌ای به داده‌های بزرگ^۱ برای بهینه‌سازی خدمات خود و ایجاد تجربیات شخصی‌سازی شده برای کاربران تکیه می‌کنند. این امر به این معناست که حجم عظیمی از داده‌های شخصی کاربران به‌طور مداوم جمع‌آوری، تحلیل و استفاده می‌شود. استفاده گسترده از داده‌های بزرگ، علاوه بر فرصت‌های اقتصادی و فنی، خطرهای جدی حقوقی را نیز به همراه دارد، به‌ویژه در زمینه حریم خصوصی و کنترل بر داده‌ها.

۱. فرصت‌های پیش روی پلتفرم‌ها و جوامع حقوقی

گسترش روزافزون فناوری‌های دیجیتال در بستر هوش مصنوعی و الگوریتم‌های خودکار در پلتفرم‌های رسانه‌های اجتماعی، چالش‌ها و فرصت‌های متعددی را برای جوامع حقوقی و پلتفرم‌ها ایجاد کرده است. اگرچه مشکلاتی نظیر تبعیض‌های الگوریتمی، نقض حقوق کاربران و عدم شفافیت در تصمیم‌گیری‌های خودکار وجود دارد، از سوی دیگر، این فناوری‌ها می‌توانند به‌طور قابل‌توجهی به بهبود کارکرد پلتفرم‌ها، کاهش اشتباه‌ها و ایجاد ساختارهای مسئولیت‌پذیری مؤثر کمک کنند. این مقاله به بررسی سه محور کلیدی از فرصت‌های پیش روی پلتفرم‌ها و جوامع حقوقی پرداخته و به بررسی بهبود الگوریتم‌ها و کاهش اشتباه‌ها، مسئولیت‌پذیری مشترک پلتفرم‌ها و دولت‌ها و فراهم کردن زیرساخت‌های حقوقی برای هماهنگی میان فناوری و حقوق می‌پردازد.

• بهبود الگوریتم‌ها و کاهش اشتباه‌ها

از اصلی‌ترین فرصت‌هایی که پلتفرم‌های رسانه‌های اجتماعی در اختیار دارند، بهبود الگوریتم‌ها از طریق استفاده از فناوری‌های پیشرفته هوش مصنوعی و یادگیری ماشین است. این فناوری‌ها می‌توانند به‌طور مؤثری دقت و صحت تصمیم‌گیری‌های خودکار را افزایش دهند و به کاهش اشتباه در زمینه‌هایی مانند شناسایی محتوای نامناسب یا تبلیغات هدفمند کمک کنند. به‌طور مثال، در زمینه فیلترینگ محتوای غیرقانونی یا نامناسب، الگوریتم‌های هوش مصنوعی با بهره‌گیری از داده‌های بزرگ و یادگیری ماشین، می‌توانند دقت خود را در تشخیص محتوای مضر بهبود بخشند و احتمال حذف محتوای قانونی به اشتباه را کاهش دهند. از دیگر فرصت‌های مهم در این زمینه، خودآموزی و بهبود مستمر الگوریتم‌هاست. الگوریتم‌های هوش مصنوعی با استفاده از داده‌های جدید و بازخورد کاربران، می‌توانند به مرور زمان عملکرد خود را بهبود بخشند. این امکان باعث می‌شود که اشتباه‌های سیستماتیک در الگوریتم‌ها کاهش یابد و کیفیت خدمات ارائه‌شده به کاربران به‌طور مداوم ارتقا یابد. برای مثال، الگوریتم‌های فیلترینگ محتوا در یوتیوب و فیس‌بوک با تحلیل مداوم داده‌های جدید و بازخورد کاربران، می‌توانند دقت بیشتری در شناسایی محتوای مضر پیدا کنند و از اشتباهات مکرر جلوگیری کنند (پاسکوئال، ۲۰۱۵). نظارت مستمر بر عملکرد الگوریتم‌ها نیز فرصتی دیگر برای بهبود آن‌هاست. پلتفرم‌ها می‌توانند از طریق ایجاد سازوکارهای نظارتی و تحلیل دقیق نتایج عملکرد الگوریتم‌های خود، نقاط ضعف و خطاهای موجود در آن‌ها را شناسایی کنند. این رویکرد به پلتفرم‌ها اجازه می‌دهد تا فرایندهای خودکار را بهینه‌سازی کنند و از تأثیرهای منفی احتمالی بر حقوق کاربران جلوگیری کنند.

• مسئولیت پذیری مشترک پلتفرم‌ها و دولت‌ها

یکی از فرصت‌های مهم پیش روی پلتفرم‌های رسانه‌های اجتماعی و جوامع حقوقی، مسئولیت‌پذیری مشترک پلتفرم‌ها و دولت‌ها در تنظیم و نظارت بر استفاده از هوش مصنوعی است. این همکاری می‌تواند به تدوین مقررات مؤثر و کاربردی‌تر کمک کند و چالش‌های حقوقی ناشی از استفاده از فناوری‌های جدید را کاهش دهد. برای مثال، در اتحادیه اروپا با تصویب قانون خدمات دیجیتال^۱، نقش دولت‌ها در نظارت بر عملکرد پلتفرم‌ها و تضمین حقوق کاربران افزایش یافته است. این قانون پلتفرم‌ها را ملزم می‌کند که درباره نحوه عملکرد الگوریتم‌های خود شفافیت بیشتری داشته باشند و در موارد بروز خطا پاسخ‌گو باشند. در دنیای دیجیتال امروز، حمایت از حقوق کاربران یکی از مهم‌ترین اولویت‌ها برای پلتفرم‌ها و دولت‌ها به شمار می‌رود. پلتفرم‌ها باید نه تنها از نظر فنی، بلکه از نظر حقوقی نیز مسئولیت‌پذیر باشند و در قبال تصمیم‌های خودکار و عملکرد الگوریتم‌های هوش مصنوعی خود پاسخ‌گو باشند. دولت‌ها می‌توانند با تدوین قوانین و مقررات مؤثر، به ایجاد چارچوب‌های حقوقی‌ای که تضمین‌کننده حقوق کاربران و جلوگیری از سوءاستفاده از داده‌های آن‌ها باشد، کمک کنند. مسئولیت‌پذیری مشترک به این معناست که پلتفرم‌ها و دولت‌ها با همکاری یکدیگر بتوانند ساختارهای پاسخ‌گویی مناسبی ایجاد کنند. این ساختارها می‌توانند شامل سازوکارهای بررسی و بازنگری تصمیم‌های الگوریتمی، فرایندهای بازگشت به تصمیم‌های نادرست و شفافیت در عملکرد سیستم‌های هوش مصنوعی باشند.

• فراهم نمودن زیرساخت‌های حقوقی برای هماهنگی میان فناوری و حقوق

توسعه سریع هوش مصنوعی نیازمند تدوین قوانین و مقررات نوینی است که بتواند چالش‌های پیچیده و چندبُعدی مرتبط با این فناوری‌ها را مدیریت کند. دولت‌ها و جوامع حقوقی باید با همکاری پلتفرم‌ها، چارچوب‌های حقوقی منسجم و مؤثری طراحی کنند که نه تنها از حقوق اساسی کاربران حفاظت کند، بلکه زمینه‌ساز نوآوری، رقابت‌پذیری و رشد فناوری نیز باشد. در این راستا، برخی کشورها و نهادهای بین‌المللی مانند اتحادیه اروپا پیشگام بوده‌اند و با تدوین مقرراتی مانند «قانون هوش مصنوعی اتحادیه اروپا»، تلاش کرده‌اند تا توازن میان حفاظت از حقوق شهروندان و پیشرفت فناوری را برقرار کنند. یکی از چالش‌های کلیدی در این مسیر، ایجاد تعادل میان حریم خصوصی کاربران و بهره‌وری الگوریتم‌های مبتنی بر داده‌های کلان است. پلتفرم‌های رسانه‌های اجتماعی، به‌طور گسترده‌ای از داده‌های کاربران برای آموزش مدل‌های هوش مصنوعی و بهینه‌سازی خدمات استفاده می‌کنند؛ در حالی که حفاظت از حریم خصوصی و داده‌های شخصی، حق بنیادین کاربران است و باید در هر نظام حقوقی مورد توجه ویژه قرار گیرد. در این راستا، تدوین قوانین جامع حفاظت از داده‌ها و الزامات شفافیت در عملکرد الگوریتم‌ها، یکی از ضرورت‌های حیاتی است.

در سطح ملی، «سند ملی توسعه هوش مصنوعی جمهوری اسلامی ایران» که در سال‌های اخیر توسط معاونت علمی و فناوری ریاست‌جمهوری تدوین و ابلاغ شده است، به‌عنوان نقشه راه سیاست‌گذاری در حوزه هوش مصنوعی عمل می‌کند. این سند اهداف کلانی همچون توسعه زیرساخت‌های فناوری، ارتقای توان رقابتی کشور در سطح منطقه‌ای و جهانی و حمایت از نوآوری را دنبال می‌کند. در عین حال، «سند ملی هوش مصنوعی» بر ضرورت تدوین مقررات

شفاف برای مدیریت ابعاد حقوقی و اخلاقی هوش مصنوعی از جمله صیانت از داده‌های شخصی، تضمین عدالت الگوریتمی و ایجاد نهادهای نظارتی تأکید دارد. این سند می‌تواند مبنای طراحی قوانین مکمل و آیین‌نامه‌های اجرایی در حوزه‌های تخصصی مانند رسانه‌های اجتماعی باشد. علاوه بر تصویب قوانین جدید، تقویت زیرساخت‌های حقوقی و فنی برای تضمین اجرای مؤثر این مقررات نیز ضروری است. دولت‌ها و پلتفرم‌ها باید با همکاری مشترک، سازوکارهای لازم برای نظارت بر عملکرد الگوریتم‌ها، رسیدگی به شکایات کاربران و ارزیابی‌های دوره‌ای سامانه‌های هوش مصنوعی را فراهم کنند. این زیرساخت‌ها می‌تواند شامل ایجاد سازمان‌های مستقل نظارت بر هوش مصنوعی، طراحی سامانه‌های بازخورد و بازبینی و بهره‌گیری از فناوری‌های نوین برای رصد مستمر عملکرد پلتفرم‌ها باشد.

نتیجه‌گیری

پلتفرم‌های رسانه‌های اجتماعی، الگوریتم‌های خودکار هوش مصنوعی را اتخاذ می‌کنند؛ آن‌ها علی‌رغم مزایای بسیار، دارای چالش‌های حقوقی و اجتماعی پیچیده‌اند. در مقابل، فرصت‌هایی نیز برای بهبود و توسعه عملکرد این پلتفرم‌ها و ایجاد ساختارهای حقوقی مناسب وجود دارد. قوانین و قواعد موجود در ایالات متحده، مصونیتی برای پلتفرم‌ها فراهم کرده است که حتی در صورت اطلاع از محتوای ناقض حریم خصوصی، از مسئولیت معاف می‌شوند. اما این مصونیت که به حُسن نیت پلتفرم‌ها متکی است، در مواردی که پلتفرم‌ها از حذف محتوا خودداری می‌کنند، مورد انتقاد قرار گرفته است و در اروپا، رویکرد «خطا و حذف» به‌طور بهتری بین مصالح مختلف تعادل برقرار می‌کند. دستورالعمل جدید ۲۰۱۹ در اروپا، مسئولیت بیشتری برای مدیریت محتوای ناقض بر پلتفرم‌ها قرار داده است، اما این رویکرد نیز چالش‌های خود را دارد. در ایران نیز، مسئولیت مدنی پلتفرم‌ها در قبال اعمال زیان‌بار کاربران با اصول فقهی منطبق نیست و تنها در موارد خاص می‌توان پلتفرم را مسئول دانست. در مجموع، نظام حقوقی ایران، در مقایسه با آمریکا و اروپا، در حمایت از حریم خصوصی کاربران در پلتفرم‌های آنلاین ضعیف‌تر عمل می‌کند.

در نتیجه دولت‌ها نیز باید قوانین و مقرراتی وضع کنند که شفافیت و پاسخ‌گویی پلتفرم‌ها را تضمین کند؛ به‌عنوان مثال، قوانین جدیدی مانند قانون خدمات دیجیتال (DSA) در اتحادیه اروپا، پلتفرم‌ها را ملزم به افزایش شفافیت در عملکرد الگوریتم‌های خود کرده است. برای مقابله با تبعیض و تعصب‌های الگوریتمی، پلتفرم‌ها باید به‌طور مداوم الگوریتم‌های خود را بازبینی کرده و از داده‌های متنوع‌تر و غیرمغرضانه استفاده کنند. در کنار چالش‌ها، فرصت‌های مهمی نیز برای پلتفرم‌ها و جوامع حقوقی وجود دارد. بهبود الگوریتم‌ها از طریق فناوری‌های پیشرفته هوش مصنوعی، می‌تواند به کاهش اشتباه‌ها و افزایش دقت تصمیم‌گیری‌های خودکار منجر شود. همچنین، مسئولیت‌پذیری مشترک میان پلتفرم‌ها و دولت‌ها می‌تواند به ایجاد چارچوب‌های حقوقی کارآمدتر و هماهنگ‌تر کمک کند. در نهایت، موفقیت در ایجاد تعادل میان استفاده از فناوری‌های نوین و رعایت حقوق کاربران به همکاری مؤثر میان پلتفرم‌ها، دولت‌ها و جوامع حقوقی وابسته است. ایجاد شفافیت، رفع تبعیض‌های الگوریتمی، و حفاظت از داده‌های کاربران، سه رکن اساسی در مسئولیت‌پذیری حقوقی پلتفرم‌ها هستند.

منابع

حسام، ابوالفضل؛ مدیو جونی، محمد؛ میری حسین؛ یمرلی صالح (۱۴۰۰). مسئولیت مدنی پلتفرم‌های آنلاین ناشی از نقض حریم خصوصی اطلاعاتی از سوی کاربران؛ مطالعه تطبیقی در ایران، آمریکا و اتحادیه اروپا. *مجله پژوهش‌های ارتباطی*، ۲۸(۱۰۷)، ۶۹-۹۱.

نجفی، حامد و مدنی، مهسا (۱۳۹۹). *مشارکت در نقض اموال فکری در حقوق ایران و آمریکا*. تهران: نشر میزان.

References

- Balkin, J. M. (2017). Free speech in the algorithmic society: Big data, private governance, and new school speech regulation. *UC Davis Law Review*, 51(3), 1149.
- Hesam, A., Madibo Jooni, M., Miri, H. & Yamerli, S. (2021). Civil liability of online platforms arising from users' violation of informational privacy: A comparative study of Iran, the United States, and the European Union. *Communication Research Journal*, 28(107), 69-91. (in Persian)
- Najafi, H. & Madani, M. (2020). Participation in the infringement of intellectual property rights in Iranian and U.S. law. Tehran: Mizan Publishing. (in Persian)
- Boyle, J. & Jenkins, J. (2024). *Intellectual Property: Law & the Information Society: Cases & Materials*. Center for the Study of the Public Domain.
- Buntain, C. & Golbeck, J. (2017, November). Automatically identifying fake news in popular twitter threads. In *2017 IEEE international conference on smart cloud (smart Cloud)* (pp. 208-215). IEEE.
- European Commission (2022). *Digital services act*. Retrieved from [European Commission website].
- European Commission. (2021). *Proposal for a regulation laying down harmonised rules on Artificial Intelligence* (Artificial Intelligence Act).
- European Commission. (2022). *Digital services act package*. Retrieved from [European Commission website].
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Gunning, D., Stefik, M., Choi, J., Miller, T., Stumpf, S. & Yang, G. Z. (2019). XAI—Explainable Artificial Intelligence. *Science Robotics*, 4(37), eaay7120.
- Kaplan, A. M. & Haenlein, M. (2010). Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, 53(1), 59-68.
- Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Harvard University Press.

- Russell, S., Norvig, P. & Intelligence, A. (2020). *Artificial intelligence: A modern approach*. (4th ed.). Pearson.
- Sevanian, A. M. (2014). Section 230 of the communications decency act: A "good samaritan" law without the requirement of acting as a "good samaritan". *UCLA Ent. L. Rev.*, 21, 121.
- Van der Sloot, B. (2015). Welcome to the jungle: The liability of internet intermediaries for privacy violations in Europe. *J. Intell. Prop. Info. Tech. & Elec. Com. L.*, 6, 211.
- Veale, M. & Borgesius, F. Z. (2021). Demystifying the draft EU artificial intelligence act. *Computer Law Review International*, 22(4), 97-112.