Received: 20/02/2025
Review: 21/05/2025
Accepted: 12/07/2025
DOI: 10.22054/jocl.2325.75063.2452

Journal of Cyber Law
No(4),Vol(1), 74-103.
ISSN: 0972-6934
www.jocl.ir

Examining the Impact of Legal Awareness on Cybercrimes and Crime Prevention

Nima Bahramnia[1],Sara NasehZadeh[2*]

1-M.A. Student in Law, Lorestan University, Khorramabad, Iran
2*-M.A. Student in Law, Lorestan University, Khorramabad, Iran

ABSTRACT

The expansion of cyberspace and the growing reliance of society on modern technologies have led to the emergence of new forms of delinquency, known as cybercrimes. These crimes, ranging from online fraud to privacy violations and unauthorized access to data, represent serious threats to individual and social security. One of the most effective strategies for preventing such crimes is to enhance citizens' legal awareness. Awareness of cybercrime-related laws not only reduces the risk of victimization but also discourages individuals from committing criminal behaviors in cyberspace. The aim of this study is to analyze the impact of legal knowledge on reducing cybercrimes and to propose preventive measures based on Iranian law and international instruments. The research method is descriptive-analytical, relying on library and documentary studies. Findings reveal that raising legal awareness through public education, media, and official institutions can serve as an effective tool for social prevention and, alongside penal measures, contribute to reducing cybercrime. The novelty of this paper lies in addressing both legal and social dimensions of prevention, showing that strengthening users' legal knowledge is a key step toward ensuring cybersecurity.

Keywords:
Cybercrimes; Legal awareness; Crime prevention; Users' rights; Cybersecurity.

How to Cite: bahramnia, N. and nasehzadeh, S. (2025). Examining the Impact of Legal Awareness on Cybercrimes and Crime Prevention. Journal of Cyber Law (JOCL), 1(4), 74-103.
doi: 10.22054/jocl.2325.75063.2452

* Corresponding Author: sara.nasehzadeh@lorestan.ac.ir

نشریه حقوق سایبری
شماره (٤) ١٠٣-٧٤
دوره ١٤٠٣

تاریخ دریافت: ١٤٠٣/٠٦/٢١
تاریخ اصلاح: ١٤٠٣/٠٩/٢١
تاریخ پذیرش: ١٤٠٣/١٢/٢٥

بررسی تاثیر آگاهی قانونی نسبت به جرایم سایبری و پیشگیری از وقوع جرم

نیما بهرام نیا[1]،سارا ناصح زاده[2]*

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه لرستان، خرم‌آباد، ایران

۲- دانشجوی کارشناسی ارشد حقوق، دانشگاه لرستان، خرم‌آباد، ایران

چکیده

گسترش فضای سایبری و افزایش وابستگی جامعه به فناوری‌های نوین، موجب ظهور اشکال جدیدی از بزهکاری تحت عنوان جرایم سایبری شده است. این جرایم، از کلاهبرداری اینترنتی تا نقض حریم خصوصی و دسترسی غیرمجاز به داده‌ها، تهدیدی جدی برای امنیت فردی و اجتماعی محسوب می‌شوند. یکی از مؤثرترین راهکارهای پیشگیری از وقوع این جرایم، ارتقای سطح آگاهی قانونی شهروندان است. آگاهی کاربران نسبت به قوانین مرتبط با جرایم رایانه‌ای، نه تنها امکان بزه‌دیدگی آنان را کاهش می‌دهد بلکه موجب می‌شود افراد از ارتکاب رفتارهای مجرمانه در فضای مجازی نیز خودداری کنند. هدف این پژوهش، تحلیل تأثیر آگاهی حقوقی در کاهش وقوع جرایم سایبری و ارائه راهکارهای پیشگیرانه بر مبنای قوانین ایران و اسناد بین‌المللی است. روش تحقیق، توصیفی–تحلیلی و مبتنی بر مطالعه کتابخانه‌ای و اسنادی است. یافته‌ها نشان می‌دهد که افزایش آگاهی حقوقی از طریق آموزش عمومی، رسانه‌ها و نهادهای رسمی، می‌تواند به عنوان ابزاری مؤثر در پیشگیری اجتماعی عمل کند و در کنار اقدامات کیفری، بستر کاهش بزهکاری سایبری را فراهم آورد. نوآوری این مقاله در توجه هم‌زمان به بعد حقوقی و اجتماعی پیشگیری است، به گونه‌ای که نشان می‌دهد تنها با تقویت دانش حقوقی کاربران می‌توان گامی اساسی در حفاظت از امنیت سایبری برداشت.

کلیدواژه‌ها:

جرایم سایبری؛ آگاهی قانونی؛ پیشگیری از جرم؛ حقوق کاربران؛ امنیت سایبری.

نحوه استناد:

بهرام نیا, نیما و ناصح زاده, سارا . (۱۴۰۳). بررسی تاثیر آگاهی قانونی نسبت به جرایم سایبری و پیشگیری از وقوع جرم. حقوق سایبری, ۱(۴), ۷۴-۱۰۳.

* ایمیل نویسنده مسئول: sara.nasehzadeh@lorestan.ac.ir

مقدمه

ظهور فناوری اطلاعات و ارتباطات و گسترش روزافزون اینترنت در دهه‌های اخیر، زمینه‌های تازه‌ای برای بزهکاری فراهم آورده است. جرایم سایبری، که شامل طیفی از رفتارهای مجرمانه مانند کلاهبرداری اینترنتی، سرقت داده‌ها، هک، جعل رایانه‌ای و نقض حریم خصوصی است، نه‌تنها امنیت فردی را تهدید می‌کند بلکه امنیت اجتماعی و اقتصادی کشورها را نیز با چالش جدی مواجه ساخته است (Dramliu, ۲۰۲۰, p. ۷۵). به دلیل ماهیت فراملی این جرایم، هیچ مرزی برای ارتکاب آن‌ها متصور نیست و همین امر، مقابله و پیشگیری از آن‌ها را دشوارتر کرده است. از این رو، راهبردهای پیشگیری اجتماعی و ارتقای آگاهی حقوقی شهروندان، در کنار اقدامات کیفری و فنی، به یکی از مهم‌ترین محورهای سیاست جنایی کشورها تبدیل شده است.در نظام حقوقی ایران، قانون اساسی جمهوری اسلامی ایران در اصول ۲۲ و ۲۵، به صراحت بر حمایت از حریم خصوصی، امنیت داده‌ها و آزادی مشروع افراد تأکید دارد (قانون اساسی جمهوری اسلامی ایران، ۱۳۵۸، ص. ۱۴). همچنین قانون جرایم رایانه‌ای مصوب ۱۳۸۸، در مواد مختلف از جمله مواد ۱، ۲، ۲۵ و ۲۶، انواع رفتارهای مجرمانه در فضای سایبری و مسئولیت‌های قانونی مرتبط را پیش‌بینی کرده است (قانون جرایم رایانه‌ای، ۱۳۸۸، ص. ۱۲). با این حال، صرف وجود قوانین کافی نیست؛ زیرا تجربه نشان داده است که آگاهی ناکافی کاربران نسبت به این مقررات، زمینه ارتکاب یا قربانی‌شدن در جرایم سایبری را افزایش می‌دهد (زلقی، ۱۳۹۹، ص. ۵۵).

اهمیت این موضوع زمانی آشکارتر می‌شود که بررسی‌های آماری پلیس فتا نشان می‌دهد بخش قابل توجهی از پرونده‌های سایبری به دلیل ناآگاهی قربانیان از مخاطرات حقوقی و فنی رخ داده است. برای نمونه، در پرونده‌های کلاهبرداری اینترنتی، بسیاری از بزه‌دیدگان اطلاعات بانکی خود را بدون اطلاع از مسئولیت‌ها و مخاطرات قانونی، در اختیار مجرمان قرار داده‌اند. چنین وضعیتی نشان می‌دهد که صرفاً برخورد کیفری با مرتکبان نمی‌تواند ضامن کاهش جرایم سایبری باشد، بلکه باید رویکرد پیشگیرانه با تأکید بر آموزش عمومی و ارتقای آگاهی حقوقی شهروندان مورد توجه قرار گیرد (حسام، ۱۴۰۰، ص. ۹۲).

از منظر بین‌المللی نیز این مسئله اهمیت فراوانی دارد. اتحادیه اروپا با تصویب مقرراتی مانند General Data Protection Regulation (GDPR)، تلاش کرده است تا سطح آگاهی و مسئولیت کاربران و پلتفرم‌ها را ارتقا دهد و از این طریق وقوع جرایم مرتبط با داده‌ها را کاهش دهد (Kuner, ۲۰۱۷, p. ۲۲۰). همچنین در سند EU Digital Education Action Plan بر نقش آموزش حقوقی و دیجیتال به عنوان رکن اصلی پیشگیری اجتماعی از جرایم سایبری تأکید شده است (Zhang, ۲۰۲۴, p. ۱۰). این تجربه‌ها می‌تواند الگویی برای ایران و سایر کشورهایی باشد که هنوز سیاست‌های آموزشی و حقوقی جامعی در حوزه فضای سایبری تدوین نکرده‌اند.

پژوهش‌های داخلی و خارجی نشان داده‌اند که میان سطح آگاهی حقوقی شهروندان و میزان بزه‌دیدگی آنان در فضای سایبری رابطه معناداری وجود دارد. برای مثال، (Jobin, Ienca & Vayena , ۲۰۱۹, p. ۳۹۰) به این نتیجه رسیده‌اند که آگاهی از استانداردهای حقوقی و اخلاقی در حوزه فناوری‌های نوین، می‌تواند آسیب‌پذیری کاربران را به میزان چشمگیری کاهش دهد. در ایران نیز غلامی (۲۰۲۳، ص. ۷۸) بر این نکته تأکید کرده که خلأ آموزش‌های حقوقی در فضای مجازی، یکی از مهم‌ترین موانع پیشگیری از جرایم رایانه‌ای است.با وجود اهمیت موضوع، بررسی‌ها نشان می‌دهد که در ادبیات علمی ایران، عمدتاً به جرم‌انگاری و برخورد کیفری با جرایم سایبری پرداخته شده و کمتر پژوهشی به

نقش «آگاهی حقوقی» در پیشگیری توجه کرده است. برای نمونه، پژوهش عاکفی قاضیانی (۱۴۰۱، ص. ۱۵۰) بیشتر بر ابعاد مالکیت و اموال در فضای مجازی متمرکز بوده و نقش آموزش حقوقی کاربران را به حاشیه رانده است. بنابراین، خلأ پژوهشی مهمی در این زمینه وجود دارد که ضرورت پرداختن به آن را در قالب یک تحقیق جامع دوچندان می‌سازد.

پرسش اصلی این مقاله آن است که:آگاهی قانونی چه تأثیری بر پیشگیری از وقوع جرایم سایبری دارد و چگونه می‌توان با ارتقای این آگاهی، سطح امنیت دیجیتال جامعه را افزایش داد؟

پرسش‌های فرعی شامل موارد زیر هستند:

۱. چارچوب‌های قانونی موجود در ایران برای ارتقای آگاهی کاربران چیست و چه کاستی‌هایی دارد؟

۲. تجربه‌های موفق بین‌المللی در این زمینه کدامند و چگونه می‌توان آن‌ها را در ایران بومی‌سازی کرد؟

۳. نقش نهادهای آموزشی، رسانه‌ای و قضایی در ارتقای دانش حقوقی کاربران چگونه باید بازتعریف شود؟

اهداف این مقاله این است که بتواند تحلیل رابطه میان آگاهی حقوقی و کاهش جرایم سایبری داشته باشد و خلأهای قانونی و آموزشی در ایران را شناسایی کند و راهکارهای عملی برای ارتقای آگاهی حقوقی کاربران ارائه دهد .

روش پژوهش در این مقاله توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی است. در این روش، ابتدا قوانین و مقررات داخلی و بین‌المللی مورد بررسی قرار گرفته و سپس یافته‌های پژوهش‌های داخلی و خارجی تحلیل می‌شود. در نهایت، با استفاده از رویکرد تطبیقی، پیشنهادهایی برای اصلاح قوانین و تقویت سیاست‌های آموزشی در ایران ارائه می‌گردد.همچنین این مقاله تلاش می‌کند تا نشان دهد که بدون ارتقای سطح آگاهی حقوقی، هیچ نظام حقوقی نمی‌تواند در برابر رشد فزاینده جرایم سایبری موفق عمل کند. بنابراین، تأکید بر آموزش حقوقی در کنار اصلاح قوانین، می‌تواند گامی مهم در جهت تحقق پیشگیری اجتماعی و تضمین امنیت دیجیتال باشد.

آگاهی قانونی

آگاهی قانونی به میزان شناخت و فهم کاربران از قوانین و مقررات مرتبط با جرایم سایبری اشاره دارد. پژوهش‌های داخلی و بین‌المللی نشان داده‌اند که افزایش آگاهی حقوقی شهروندان نه تنها موجب کاهش آسیب‌پذیری آن‌ها در فضای مجازی می‌شود، بلکه رفتارهای مجرمانه و تخلفات سایبری را نیز کاهش می‌دهد (جعفری، ۱۴۰۱)و(Jobin, Ienca & Vayena, ۲۰۱۹, p. ۳۹۰. این آگاهی شامل فهم دقیق حقوق کاربران، مسئولیت‌های قانونی و محدودیت‌های قانونی در تعامل با اطلاعات شخصی و داده‌های دیجیتال است.مطالعات نشان می‌دهند که بسیاری از کاربران به دلیل ناآگاهی از قوانین، به طور غیرآگاهانه در معرض خطر ارتکاب جرایم سایبری یا تبدیل شدن به قربانی آن قرار می‌گیرند (حسینی وموسوی، ۱۴۰۰، ص. ۴۵). به همین دلیل، آموزش حقوقی و اطلاع‌رسانی درباره مقررات مرتبط با فضای مجازی اهمیت ویژه‌ای دارد و می‌تواند به عنوان یک ابزار پیشگیری اولیه در سیاست‌های جنایی و حقوقی مورد استفاده قرار گیرد (تاجیک، ۱۴۰۱، ص. ۱۲۵).

علاوه بر قوانین ملی، استانداردهای بین‌المللی نیز بخشی از آگاهی قانونی کاربران را تشکیل می‌دهند. به عنوان مثال، دستورالعمل‌ها و مقررات اتحادیه اروپا، از جمله(General Data Protection Regulation (GDPR ، چارچوبی برای حفاظت از داده‌ها و مسئولیت پلتفرم‌های دیجیتال ارائه می‌دهند (Kuner, ۲۰۱۷, p. ۲۲۵). رعایت این مقررات نه تنها موجب افزایش امنیت کاربران می‌شود، بلکه تعهدات قانونی شرکت‌ها و کاربران را در سطح بین‌المللی

مشخص می‌کند (Beduschi, ۲۰۱۹, p. ۷۸).از نظر اخلاقی و اجتماعی، افزایش آگاهی قانونی موجب شکل‌گیری فرهنگ مسئولیت‌پذیری دیجیتال می‌شود. کاربران با شناخت بهتر حقوق خود و دیگران، رفتارهای خود را در محیط آنلاین کنترل کرده و از ارتکاب یا تسهیل جرایم سایبری جلوگیری می‌کنند (Floridi, ۲۰۱۹, p. ۴۵). همچنین، این آگاهی، ابزاری برای کاهش خلاهای قانونی و بهبود همکاری میان نهادهای اجرایی، قضایی و پژوهشی در مقابله با تهدیدات سایبری محسوب می‌شود (Calo, ۲۰۱۶, p. ۵۲۰).

بنابراین، آگاهی قانونی نه تنها یک نیاز آموزشی و فرهنگی است، بلکه یک ضرورت حقوقی و اجتماعی است که می‌تواند به کاهش وقوع جرایم سایبری، حفاظت از داده‌های شخصی و تقویت اعتماد عمومی در فضای مجازی کمک کند. این اهمیت، موجب شده است که بسیاری از پژوهشگران داخلی و بین‌المللی، آموزش و اطلاع‌رسانی حقوقی را به عنوان یکی از مؤثرترین راهبردهای پیشگیری از جرایم سایبری مطرح کنند (جعفری، ۱۴۰۱؛ حسینی & موسوی، ۱۴۰۰، ص. ۵۰)؛ (Jobin, Ienca & Vayena, ۲۰۱۹, p. ۳۹۱)).

جرایم سایبری

جرایم سایبری به مجموعه رفتارهای مجرمانه‌ای گفته می‌شود که از طریق فضای مجازی و فناوری‌های اطلاعاتی انجام می‌گیرند و شامل دسترسی غیرمجاز به داده‌ها، هک، کلاهبرداری اینترنتی، انتشار اطلاعات نادرست و نقض حریم خصوصی افراد است (جعفری، ۱۴۰۱). این دسته از جرایم برخلاف جرایم سنتی، محدود به مرزهای جغرافیایی نیست و به دلیل ماهیت دیجیتال خود، می‌توانند به سرعت در سطح ملی و بین‌المللی گسترش یابند، به‌طوری که مقابله با آن‌ها نیازمند هماهنگی میان کشورها و استفاده از ابزارهای پیشرفته فناوری اطلاعات است (Kuner, ۲۰۱۷, p. ۲۲۰).ویژگی بارز جرایم سایبری، پیچیدگی تکنولوژیک آن‌هاست؛ مجرمان اغلب از ابزارهای پیشرفته برای نفوذ به سیستم‌های اطلاعاتی، سرقت داده‌ها یا ایجاد اختلال در شبکه‌های حیاتی استفاده می‌کنند (Floridi, ۲۰۱۹, p. ۴۵). علاوه بر این، فضای سایبر امکان ناشناس ماندن مجرم را فراهم می‌کند، که تحقیقات و پیگرد قانونی آن‌ها را دشوار می‌سازد (Beduschi, ۲۰۱۹, p. ۷۸). این مسأله نه تنها به چالش‌های قضایی دامن می‌زند، بلکه موجب افزایش هزینه‌های امنیتی و کاهش اعتماد عمومی به فناوری‌های دیجیتال می‌شود (Bernal Bernabe et al., ۲۰۱۹, p. ۱۶۴).از منظر حقوقی، جرایم سایبری چالش‌های خاص خود را دارند. قوانین داخلی بسیاری از کشورها برای مقابله با جرایم سنتی طراحی شده‌اند و ممکن است برای رسیدگی به جرایم دیجیتال ناکافی باشند (موسوی، ۱۴۰۱). به همین دلیل، تدوین قوانین جدید و به‌روزرسانی مقررات موجود، یکی از الزامات اساسی در کاهش جرایم سایبری محسوب می‌شود (بهره‌مند، کوره‌پز و سلیمی، ۱۳۹۳). علاوه بر این، تحلیل دکترین حقوقی نشان می‌دهد که مسئولیت کیفری کاربران و نهادهای ارائه‌دهنده خدمات دیجیتال باید شفاف و دقیق تعیین شود تا ضمن پیشگیری از وقوع جرم، عدالت کیفری نیز تأمین گردد (تاجیک، ۱۴۰۱; حسن، ۲۰۲۲,ص۶۳).از منظر امنیت اجتماعی، جرایم سایبری تهدیدی جدی برای افراد، سازمان‌ها و حتی دولت‌ها هستند. نقض حریم خصوصی کاربران، سرقت اطلاعات حساس مالی یا شخصی و دسترسی غیرمجاز به سامانه‌های حیاتی، می‌تواند پیامدهای اقتصادی و روانی گسترده‌ای به همراه داشته باشد (Zuboff, ۲۰۱۹ , p.۱۱۲). بنابراین، پیشگیری از جرایم سایبری تنها به توسعه قوانین محدود نمی‌شود، بلکه نیازمند آموزش کاربران، افزایش آگاهی عمومی و ایجاد زیرساخت‌های امن فناوری اطلاعات است (حسینی و موسوی، ۱۴۰۰).به‌طور خلاصه، جرایم سایبری ترکیبی از پیچیدگی تکنولوژیک، فراملی بودن و پیامدهای گسترده اجتماعی است که مقابله با آن نیازمند

رویکردی چندجانبه است. استفاده از چارچوب‌های قانونی به‌روز، آموزش و فرهنگ‌سازی دیجیتال، و همکاری بین‌المللی، سه رکن اساسی در کاهش آسیب‌های ناشی از جرایم سایبری به شمار می‌روند (Calo, ۲۰۱۶, p. ۵۲۸ ; Jobin, Ienca & Vayena, ۲۰۱۹, p. ۳۹۱).

پیشگیری از جرم

پیشگیری از جرم در حوزه سایبری به مجموعه اقدامات آموزشی، قانونی، فنی و سازمانی گفته می‌شود که هدف اصلی آن کاهش وقوع جرایم و حفاظت از کاربران در فضای مجازی است (Beduschi, ۲۰۱۹, p. ۳). این اقدامات شامل طراحی سیستم‌های امنیتی، وضع قوانین و مقررات بازدارنده، افزایش آگاهی کاربران، و راه‌اندازی برنامه‌های پیشگیرانه آموزشی و اطلاع‌رسانی است (جعفری، ۱۴۰۱).یکی از مهم‌ترین رویکردها در پیشگیری از جرایم سایبری،پیشگیری اجتماعی است که بر رفتار و آگاهی کاربران تمرکز دارد. ارتقای آگاهی حقوقی و آموزش مهارت‌های دیجیتال موجب می‌شود کاربران از ارتکاب ناخواسته جرایم جلوگیری کنند و به عنوان بازیگر فعال در حفاظت از داده‌ها و اطلاعات خود عمل کنند (حسینی & موسوی، ۱۴۰۰، ص. ۴۷). مطالعات نشان می‌دهند که برنامه‌های آموزشی مؤثر می‌توانند آسیب‌پذیری کاربران در مقابل هک، کلاهبرداری اینترنتی و نقض حریم خصوصی را به شکل قابل توجهی کاهش دهند (تاجیک، ۱۴۰۱، ص. ۱۲۸).

از بعد قانونی، پیشگیری از جرم شامل وضع قوانین خاص برای جرایم سایبری، ایجاد مجازات‌های بازدارنده، و تعیین مسئولیت پلتفرم‌ها و کاربران در انتقال داده‌ها است. به عنوان مثال،قانون جرایم رایانه‌ای ایران (۱۳۸۸) مسئولیت کاربران و ارائه‌دهندگان خدمات اینترنتی را در قبال داده‌ها مشخص کرده و اقداماتی برای پیشگیری از جرایم دیجیتال پیش‌بینی می‌کند (قانون جرایم رایانه‌ای، ۱۳۸۸، ص. ۱۲). همچنین، استانداردهای بین‌المللی مانندGDPR و دستورالعمل‌های اتحادیه اروپا، نقش مهمی در پیشگیری از جرایم سایبری از طریق تعیین چارچوب‌های حفاظت از داده و مسئولیت پلتفرم‌ها دارند (Kuner, ۲۰۱۷, p. ۲۲۵).علاوه بر پیشگیری اجتماعی و قانونی، پیشگیری فنی نیز اهمیت دارد. استفاده از سامانه‌های رمزگذاری داده، نرم‌افزارهای ضدویروس، و پروتکل‌های امنیتی می‌تواند از دسترسی غیرمجاز و سرقت اطلاعات جلوگیری کند (Beduschi, ۲۰۱۹, p. ۱۲). پژوهش‌ها نشان داده‌اند که ترکیب اقدامات آموزشی، قانونی و فنی، بیشترین تأثیر را در کاهش وقوع جرایم سایبری دارد و محیط دیجیتال ایمن‌تری برای کاربران فراهم می‌آورد (Beral Bernabe et al., ۲۰۱۹, p. ۱۷۰).می توان گفت، پیشگیری از جرم در حوزه سایبری یک رویکرد چندبعدی است که شامل آموزش و ارتقای آگاهی حقوقی، وضع قوانین و مقررات مؤثر، و به‌کارگیری فناوری‌های امنیتی می‌شود. این اقدامات به شکل هماهنگ و هدفمند می‌توانند به کاهش وقوع جرایم، افزایش اعتماد کاربران و تقویت حاکمیت قانون در فضای دیجیتال منجر شوند(Floridi, ۲۰۱۹, p. ۴۶؛ Beduschi, ۲۰۱۹, p. ۱۵).

حقوق کاربران

حقوق کاربران در فضای سایبری به مجموعه‌ای از حقوق بنیادین اطلاق می‌شود که هر فرد در تعامل با پلتفرم‌ها و خدمات دیجیتال باید از آن‌ها بهره‌مند باشد. این حقوق شاملحق دسترسی به اطلاعات، حق حریم خصوصی، مالکیت داده‌ها، و آزادی بیان است (Beduschi, ۲۰۱۹, p. ۵۰). رعایت این حقوق نه تنها به حفاظت از کاربران کمک می‌کند، بلکه نقش مهمی در کاهش وقوع جرایم سایبری دارد، زیرا کاربران مطلع و آگاه می‌توانند از سوءاستفاده‌ها و نقض داده‌ها جلوگیری کنند (Jobin, Ienca & Vayena, ۲۰۱۹, p. ۳۹۱).

در ایران، این حقوق بااصول قانون اساسی، به ویژه اصول ۲۲ و ۲۵، و همچنین با قوانین اختصاصی مانندقانون جرایم رایانه‌ای مصوب ۱۳۸۸ تضمین شده‌اند (قانون اساسی، ۱۳۵۸؛ قانون جرایم رایانه‌ای، ۱۳۸۸،ص۱۲). به عنوان نمونه، اصل ۲۲ قانون اساسی برحق برخورداری از امنیت و حریم خصوصی افراد تأکید دارد و اصل ۲۵ حق دسترسی به اطلاعات و آزادی ارتباطات را تصریح می‌کند. همچنین، ماده‌های قانون جرایم رایانه‌ای مسئولیت کاربران و ارائه‌دهندگان خدمات دیجیتال را در قبال داده‌ها مشخص کرده و اقداماتی برای پیشگیری و مقابله با سوءاستفاده‌های سایبری پیش‌بینی کرده‌اند.از منظر بین‌المللی، پلتفرم‌ها نیز مسئولیت دارند تا حقوق کاربران را رعایت کنند و از سوءاستفاده‌های داده‌ای جلوگیری نمایند. استانداردهایی مانندGDPR اتحادیه اروپا چارچوبی قانونی برای حفاظت از داده‌های کاربران ارائه می‌دهند و شرکت‌ها و ارائه‌دهندگان خدمات دیجیتال را ملزم به رعایت حریم خصوصی می‌کنند (Kuner, ۲۰۱۷, p. ۲۳۰). رعایت همزمان حقوق کاربران و مسئولیت قانونی پلتفرم‌ها یکی از ارکان اصلی کاهش جرایم سایبری محسوب می‌شود، زیرا ایجاد محیطی امن و قانون‌مند، کاربران را از خطرات هک، کلاهبرداری اینترنتی و نقض حریم خصوصی مصون می‌سازد (Belk, Humayun, & Brouard, ۲۰۲۲, p. ۲۰۰).

تحقیقات نشان می‌دهند که توجه به حقوق کاربران نه تنها به تقویت اعتماد عمومی و افزایش مشارکت در فضای دیجیتال کمک می‌کند، بلکه زمینه لازم برای اعمال پیشگیری اجتماعی و فنی از جرایم سایبری را نیز فراهم می‌آورد (Floridi, ۲۰۱۹, p. ۴۶). به بیان دیگر، حقوق کاربران و مسئولیت قانونی پلتفرم‌ها دو روی یک سکه هستند که ترکیب آن‌ها به شکل هماهنگ، نقش تعیین‌کننده‌ای در کاهش وقوع جرایم سایبری و ارتقای امنیت فضای مجازی دارد (میلانی، ۱۴۰۱).

مسئولیت قانونی و پیشگیرانه نهادها

مسئولیت قانونی نهادها و سازمان‌ها در فضای سایبری یکی از ارکان اصلی حفظ امنیت دیجیتال و کاهش جرایم است. این مسئولیت شامل پیشگیری از ارتکاب جرم، اطلاع‌رسانی به کاربران، و همکاری با مراجع قضایی می‌شود (Zuboff, ۲۰۱۹, p. ۸۸). ارائه‌دهندگان خدمات اینترنتی، به عنوان حلقه اصلی تعامل کاربران با فضای مجازی، موظف‌اند چارچوب‌های فنی و قانونی لازم برای جلوگیری از دسترسی غیرمجاز، هک، کلاهبرداری اینترنتی و نقض حریم خصوصی را ایجاد کنند(شریفی ،۱۴۰۱ص۸۰).نهادهای آموزشی نیز نقش مهمی در پیشگیری دارند، زیرا ارتقای آگاهی حقوقی و سایبری شهروندان باعث کاهش آسیب‌پذیری کاربران و کاهش ارتکاب جرایم می‌شود (Floridi, ۲۰۱۹, p. ۴۷). آموزش‌های هدفمند در مدارس، دانشگاه‌ها و دوره‌های عمومی می‌تواند کاربران را با حقوق و مسئولیت‌های خود آشنا کند و نحوه واکنش صحیح در مواجهه با تهدیدات دیجیتال را به آن‌ها بیاموزد (Jobin, Ienca & Vayena, ۲۰۱۹, p. ۳۹۲).مسئولیت پیشگیرانه نهادها همچنین شامل همکاری با مراجع قضایی و قانون‌گذاری برای شناسایی نقاط ضعف قانونی و فنی، ارائه گزارش‌های مستمر، و توصیه به اصلاح مقررات است. این اقدامات نه تنها موجب تقویت پیشگیری اجتماعی می‌شوند، بلکه به ایجاد رویه قضایی یکپارچه و منسجم در برخورد با جرایم سایبری کمک می‌کنند.از منظر بین‌المللی، بسیاری از قوانین و دستورالعمل‌ها، مانند GDPR و اسناد حقوق دیجیتال اتحادیه اروپا، بر مسئولیت فعال نهادها در حفاظت از داده‌ها و پیشگیری از جرایم تأکید دارند. این استانداردها به نهادها توصیه می‌کنند که همزمان با ارائه خدمات، مراقبت حقوقی و فنی لازم را نیز فراهم آورند (Belk, Humayun, & Brouard, ۲۰۲۲, p. ۲۰۵).

تحقیقات نشان می‌دهند که تلفیق مسئولیت قانونی و اقدامات پیشگیرانه باعث می‌شود که فضای دیجیتال امن‌تر شود و کاربران با اعتماد بیشتری به تعاملات آنلاین بپردازند. در نتیجه، نهادها نه تنها نقش نظارتی و اجرایی دارند، بلکه با اقدامات آموزشی و اطلاع‌رسانی می‌توانند نقش فعال و پیشگیرانه در کاهش جرایم سایبری ایفا کنند (Dramliu, ۲۰۲۰).

خلأ قانونی و چالش‌های اجرایی در پیشگیری از جرایم سایبری

با وجود وجود قوانین متعدد در حوزه جرایم سایبری، پژوهش‌ها نشان می‌دهند که خلأهای قانونی و ضعف اجرایی یکی از مهم‌ترین موانع کاهش بزه‌دیدگی کاربران و کاهش اثربخشی قوانین است (جعفری، ۱۴۰۱, ص۵۵). این خلأها معمولاً ناشی از عدم شفافیت در تعریف مفاهیم کلیدی قانونی و ناهماهنگی بین مقررات ملی و استانداردهای بین‌المللی است.برای مثال، در قانون جرایم رایانه‌ای ایران (۱۳۸۸)، تعریف مشخص و جامع از مفاهیمی مانند «دسترسی غیرمجاز»، «نقض حریم خصوصی» یا «حذف محتوای مجرمانه» ارائه نشده است (قانون جرایم رایانه‌ای، ۱۳۸۸, ص۱۴). این نقص قانونی موجب شده است که نهادهای اجرایی هنگام مواجهه با پرونده‌های واقعی دچار سردرگمی شوند و کاربران نیز درک روشنی از حدود قانونی رفتار خود نداشته باشند (مزیدآبادی‌فراهانی، ۱۴۰۲, ص۱۸).

علاوه بر این، پژوهش‌های بین‌المللی نیز نشان می‌دهند که تأخیر در تطبیق قوانین ملی با تغییرات سریع فناوری و ظهور پلتفرم‌های دیجیتال جدید باعث افزایش آسیب‌پذیری کاربران می‌شود (Kuner, ۲۰۱۷, p. ۲۴۰). نبود معیارهای شفاف برای اعمال مسئولیت پلتفرم‌ها و ارائه‌دهندگان خدمات اینترنتی، از دیگر چالش‌های اجرایی است که موجب می‌شود بسیاری از اقدامات پیشگیرانه قانونی یا در سطح نظری باقی بمانند یا به صورت ناکافی اجرا شوند (Hassan, ۲۰۲۲, p. ۲۰).از منظر پیشگیری اجتماعی، عدم آگاهی کاربران و نهادهای آموزشی نیز یکی از عوامل مهم خلأ اجرایی محسوب می‌شود. حتی با وجود قانون کافی، اگر کاربران ندانند چه اقداماتی قانونی و چه اقداماتی مجرمانه محسوب می‌شوند، احتمال بروز جرایم افزایش می‌یابد و اثرگذاری قوانین کاهش می‌یابد (Jobin, Ienca & Vayena, ۲۰۱۹, p. ۳۹۵).به منظور کاهش این خلأها، بسیاری از محققان پیشنهاد می‌کنند که تعریف دقیق مفاهیم قانونی، تدوین دستورالعمل‌های اجرایی شفاف، و هماهنگی با استانداردهای بین‌المللی انجام شود (Floridi, ۲۰۱۹, p. ۵۰). همچنین آموزش مستمر کاربران و تقویت فرهنگ حقوق دیجیتال، می‌تواند بخش مهمی از خلأ اجرایی را پر کند و باعث شود قوانین نه تنها بر روی کاغذ بلکه در عمل نیز مؤثر واقع شوند (بهرامی، ۱۴۰۰,ص۵۷).

مبانی فلسفی مسئولیت در فضای سایبری

از منظر فلسفی، تحلیل مسئولیت پلتفرم‌ها و کاربران در فضای سایبری مبتنی بر مسئولیت اجتماعی و عدالت دیجیتال است. نظریه‌های عدالت، به ویژه نظریه جان راولز، بر این نکته تأکید دارند که هر فرد باید حقوق بنیادین خود را در فضای دیجیتال حفظ کند و همزمان نسبت به دیگر کاربران و جامعه مسئولیت اجتماعی داشته باشد (Iakovenko, ۲۰۲۱)). این دیدگاه فلسفی نشان می‌دهد که آزادی عمل در فضای مجازی بدون رعایت حقوق دیگران، ناقض اصول عدالت و اخلاق است.در این راستا، فلسفه اخلاق دیجیتال نیز به‌طور خاص به رفتار کاربران و پلتفرم‌ها در محیط‌های مجازی می‌پردازد. این فلسفه معتقد است که آزادی بیان و دسترسی به اطلاعات، باید با رعایت حریم خصوصی، جلوگیری از انتشار محتوای مضر و احترام به حقوق دیگران همراه باشد (Beduschi, ۲۰۱۹, p. ۳). هر گونه

سوءاستفاده از داده‌ها یا انتشار محتواهای تهدیدکننده امنیت روانی یا اجتماعی، مغایر با اخلاق و عدالت اجتماعی تلقی می‌شود و نیازمند پاسخ قانونی و اجتماعی است.

به علاوه، از منظر فلسفه عملی، مسئولیت اجتماعی کاربران و پلتفرم‌ها به معنای پیشگیری فعال از آسیب به دیگران است. این پیشگیری می‌تواند شامل آموزش کاربران، ایجاد مکانیزم‌های گزارش‌دهی محتوا و شفافیت در سیاست‌های حفظ حریم خصوصی باشد. پژوهش‌ها نشان داده‌اند که ترکیب اصول فلسفی با سیاست‌های اجرایی، موجب افزایش اثرگذاری قوانین و کاهش بزهکاری سایبری می‌شود (Floridi, ۲۰۱۹, p. ۵۰).در حقیقت مبانی فلسفی به ما این امکان را می‌دهند که چارچوب اخلاقی و حقوقی برای مسئولیت دیجیتال ایجاد کنیم، به گونه‌ای که هم آزادی کاربران حفظ شود و هم جامعه از تهدیدهای سایبری مصون بماند. این چارچوب، زیربنای تحلیل‌های حقوقی و سیاستگذاری‌های پیشگیرانه در فضای سایبری است و به تدوین قوانین و راهبردهای پیشگیرانه مؤثر کمک می‌کند.

مبانی فقهی مسئولیت در فضای سایبری

از دیدگاه فقهی، حفظ حقوق مشروع و حرمت تجاوز به مال و اطلاعات دیگران، اساس مسئولیت کاربران و نهادها در فضای سایبری را تشکیل می‌دهد. فقه اسلامی تجاوز به حریم خصوصی، سرقت اطلاعات یا نشر محتوای غیرمجاز را نوعی تعدی به حقوق دیگران تلقی می‌کند و این امر می‌تواند مسئولیت کیفری و مدنی برای فرد متخلف ایجاد نماید (جعفری، ۱۴۰۱،ص۵۵).

فقه اسلامی علاوه بر تعیین حدود مشروعیت رفتار، بر تعادل میان آزادی فردی و حقوق دیگران تأکید دارد. این تعادل به گونه‌ای است که هر فرد می‌تواند از آزادی بیان و دسترسی به اطلاعات بهره‌مند شود، مشروط بر اینکه باعث ضرر یا نقض حقوق دیگران نشود. بر این اساس، پلتفرم‌ها و ارائه‌دهندگان خدمات دیجیتال نیز موظف به رعایت اصول فقهی هستند و باید از بروز خسارت به کاربران جلوگیری کنند.همچنین، فقه اسلامی بر پیشگیری از وقوع جرم نیز تأکید دارد. از منظر فقهی، ایجاد سازوکارهای حفاظتی، هشداردهی به کاربران و فراهم کردن آموزش‌های حقوقی، نه تنها مسئولیت اخلاقی، بلکه تکلیف شرعی نهادها و کاربران است (موسوی، ۱۴۰۱،ص۳۳۰). به عبارت دیگر، پیشگیری و مراقبت از داده‌ها و اطلاعات شخصی کاربران، به عنوان یکی از مصادیق رعایت حقوق مشروع دیگران شناخته می‌شود.با توجه به تحولات فضای سایبری، فقها و حقوقدانان اسلامی تلاش کرده‌اند تا مبانی فقهی را با قوانین نوین سایبری هماهنگ کنند. به این ترتیب، مسئولیت کیفری و مدنی در زمینه جرایم دیجیتال، با رعایت آموزه‌های شرعی و قواعد اخلاقی، به یک چارچوب قابل اجرا برای نهادهای قانونی و قضایی تبدیل شده است (موسوی، ۱۴۰۱،ص۳۴۰).بنابراین، مبانی فقهی، هم به عنوان راهنمای اخلاقی و قانونی عمل می‌کنند و هم پایه‌ای برای سیاست‌های پیشگیرانه در حوزه جرایم سایبری فراهم می‌آورند، تا حقوق کاربران محترم شمرده شود و از سوءاستفاده‌های دیجیتال جلوگیری گردد.

مبانی حقوقی مسئولیت در فضای سایبری

از منظر حقوقی، چارچوب مسئولیت پلتفرم‌ها و کاربران در فضای مجازی بر اساس مواد قانونی مرتبط با جرایم سایبری و اصول قانون اساسی تعریف می‌شود. مطابق ماده ۲۵ قانون جرایم رایانه‌ای مصوب ۱۳۸۸، ارائه‌دهندگان خدمات اینترنتی موظف هستند محتوای غیرقانونی را شناسایی و حذف کنند و در صورت قصور، مسئولیت مدنی و کیفری متوجه آنان خواهد بود (قانون جرایم رایانه‌ای، ۱۳۸۸،ص۱۲). این ماده قانونی، پایه‌ای برای تعیین مسئولیت مستقیم پلتفرم‌ها در مواجهه با جرایم سایبری است و نقش مهمی در کاهش بزهکاری دیجیتال ایفا می‌کند.علاوه بر این، اصول ۲۲ و ۲۵

قانون اساسی حق آزادی بیان و دسترسی به اطلاعات شهروندان را تضمین می‌کنند، اما این آزادی با رعایت حقوق دیگران محدود می‌شود (قانون اساسی، ۱۳۵۸,ص۱۴). بر این اساس، مسئولیت قانونی کاربران و پلتفرم‌ها باید در تعادل میان آزادی فردی و حفظ حقوق سایرین اعمال شود.از سوی دیگر، مواد قانونی مرتبط با جرایم رایانه‌ای، مسئولیت پیشگیرانه و آموزشی نهادها را نیز مشخص کرده‌اند. برای مثال، ارائه‌دهندگان خدمات دیجیتال موظف به ارائه آموزش‌های لازم به کاربران برای جلوگیری از وقوع جرم هستند و همکاری با مراجع قضایی نیز از الزامات قانونی آنان محسوب می‌شود .

در حوزه رویه قضایی، آراء دادگاه‌ها نیز بر مسئولیت مدنی و کیفری پلتفرم‌ها صحه می‌گذارند. به عنوان نمونه، رأی شماره ۲۳/۱۲/۹۵ دیوان عالی کشور تأکید دارد که کوتاهی ارائه‌دهندگان خدمات در حذف محتوای مجرمانه، مصداق قصور و نقض تعهدات قانونی است (دیوان عالی کشور، ۱۳۹۵). این نوع رویه قضایی، باعث می‌شود چارچوب قانونی نه تنها نظری بلکه عملی نیز برای مقابله با جرایم سایبری فراهم شود.همچنین، دکترین حقوقی ایران و مقالات تخصصی تاکید دارند که همکاری بین‌المللی و استفاده از استانداردهای جهانی مانند GDPR، می‌تواند مسئولیت حقوقی پلتفرم‌ها را تقویت کرده و خلأهای قانونی داخلی را کاهش دهد (Kuner, ۲۰۱۷, p. ۲۲۰). بدین ترتیب، مبانی حقوقی هم شامل قوانین ملی و هم هنجارهای بین‌المللی می‌شوند و بستری برای تدوین سیاست‌های پیشگیرانه و پاسخ قانونی به جرایم سایبری فراهم می‌آورند (Beduschi, ۲۰۱۹, p. ۵).در نتیجه، مبانی حقوقی نه تنها چارچوب مسئولیت قانونی پلتفرم‌ها و کاربران را تعیین می‌کنند، بلکه با اتصال به اصول قانون اساسی و استانداردهای بین‌المللی، مسیر پیشگیری و برخورد قانونی با جرایم سایبری را نیز هموار می‌سازند.

از منظر دکترین حقوقی بین‌المللی، استانداردهایی همچون GDPR و EU Digital Services Act، پلتفرم‌ها را موظف به شفافیت، ارائه سازوکار شکایت و حذف محتوای غیرمجاز کرده‌اند (Kuner, ۲۰۱۷, p. ۲۲۵). در نتیجه، مسئولیت حقوقی پلتفرم‌ها باید تعادلی میان آزادی کاربران، حفاظت از داده‌ها و پیشگیری از جرم برقرار کند (Belk, Humayun, & Brouard, ۲۰۲۲, p. ۲۰۰).

نظریه‌های حقوقی و رویه قضایی

۱. مسئولیت مدنی و کیفری کاربران و مجرمان

بر اساس دکترین حقوقی، کاربران فضای مجازی که محتوای غیرقانونی منتشر می‌کنند، مشمول مسئولیت مدنی و کیفری هستند. مطابق ماده ۷ قانون جرایم رایانه‌ای (۱۳۸۸)، انتشار محتوای توهین‌آمیز، تهدیدآمیز یا نقض‌کننده حقوق دیگران، جرم محسوب می‌شود و فرد خاطی مشمول مجازات قانونی خواهد بود (قانون جرایم رایانه‌ای، ۱۳۸۸,ص ۹).رویه قضایی ایران نیز این مسئولیت را تأیید کرده است. در رأی شماره ۲۳/۱۲/۹۵ دیوان عالی کشور، دیوان تصریح کرده است که انتشار محتوای مجرمانه توسط کاربران، باعث ایجاد مسئولیت کیفری و مدنی می‌شود و ارائه‌دهندگان خدمات اینترنتی موظف به حذف آن پس از اطلاع هستند (دیوان عالی کشور، ۱۳۹۵,ص۲۰).

۲. مسئولیت پیشگیرانه نهادها

نظریه‌های حقوقی پیشگیرانه بر این اصل تأکید دارند که نهادها و پلتفرم‌ها نه تنها موظف به پاسخگویی پس از وقوع جرم هستند، بلکه باید به اقدامات پیشگیرانه برای جلوگیری از ارتکاب جرم نیز متعهد باشند. این رویکرد بر اصل پیشگیری از ضرر مبتنی است و هدف آن کاهش آسیب به کاربران و جامعه دیجیتال است (Floridi, ۲۰۱۹, p. ۴۵).در قوانین

ایران، ماده ۲۵ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ صراحتاً ارائه‌دهندگان خدمات اینترنتی را ملزم به شناسایی و حذف محتوای غیرقانونی می‌داند و در صورت قصور، مسئولیت مدنی و کیفری متوجه آنان خواهد بود (قانون جرایم رایانه‌ای، ۱۳۸۸,ص۱۲). این ماده قانونی نه تنها چارچوب قانونی برای مقابله با جرایم سایبری ارائه می‌دهد، بلکه به عنوان ابزار پیشگیرانه نیز عمل می‌کند، زیرا پلتفرم‌ها موظف به ایجاد سازوکارهای نظارتی مؤثر و آموزش کاربران هستند.علاوه بر الزامات قانونی، دکترین حقوقی ایران و اسناد بین‌المللی بر نقش نهادهای آموزشی، قضایی و ارائه‌دهندگان خدمات دیجیتال در پیشگیری تأکید دارند. برای مثال، ارائه آموزش‌های حقوقی و امنیت دیجیتال به کاربران می‌تواند به کاهش ارتکاب جرم و آگاهی‌بخشی به جامعه کمک کند (Jobin, Ienca & Vayena, ۲۰۱۹, p. ۳۹۰). همچنین، الزامات بین‌المللی مانند GDPR، مسئولیت پیشگیرانه پلتفرم‌ها را با استانداردهای جهانی تعریف می‌کنند و نهادها را موظف به حفاظت از داده‌ها و پیشگیری از نقض حریم خصوصی می‌سازند (Kuner, ۲۰۱۷, p. ۲۲۵).

در رویه قضایی ایران نیز، آرای دیوان عالی کشور نشان می‌دهد که کوتاهی نهادها و ارائه‌دهندگان خدمات در اجرای اقدامات پیشگیرانه می‌تواند مستلزم مسئولیت حقوقی باشد. رأی شماره ۲۳/۱۲/۹۵ دیوان عالی کشور بر لزوم اعمال سازوکارهای نظارتی و همکاری با مراجع قضایی برای جلوگیری از نشر محتوای غیرقانونی تأکید می‌کند (دیوان عالی کشور، ۱۳۹۵).

به طور کلی، مسئولیت پیشگیرانه نهادها شامل چند محور اصلی است:

۱. نظارت و کنترل محتوا: ایجاد سیستم‌های خودکار و انسانی برای شناسایی محتوای غیرقانونی.

۲. آموزش و آگاهی‌بخشی: اطلاع‌رسانی به کاربران درباره حقوق و وظایفشان در فضای مجازی.

۳. همکاری قضایی: همکاری با مراجع قانونی برای شناسایی و برخورد با جرایم سایبری.

۴. به‌کارگیری استانداردهای بین‌المللی: رعایت قوانین و دستورالعمل‌های جهانی برای حفاظت از داده‌ها و حریم خصوصی کاربران.

این چارچوب حقوقی و عملی، نه تنها موجب کاهش وقوع جرم می‌شود، بلکه مسئولیت اجتماعی نهادها و پلتفرم‌ها را تقویت کرده و اعتماد کاربران به فضای دیجیتال را افزایش می‌دهد .

تحلیل چالش‌ها

یکی از مهم‌ترین چالش‌ها در حوزه مسئولیت قانونی و پیشگیرانه نهادها و پلتفرم‌ها، تعادل میان آزادی کاربران و مسئولیت پلتفرم‌ها است. آزادی بیان و دسترسی به اطلاعات، از حقوق بنیادین کاربران در فضای دیجیتال محسوب می‌شود (قانون اساسی، ۱۳۵۸, ص. ۱۴)، اما بدون مدیریت محتوا و نظارت مناسب، این آزادی می‌تواند به نقض حقوق دیگر کاربران، انتشار اطلاعات نادرست و حتی تشویق به رفتارهای مجرمانه منجر شود (احمدی ،۱۳۹۹.ص۵۸)از سوی دیگر، اعمال مسئولیت بیش از حد بر عهده پلتفرم‌ها می‌تواند باعث محدود شدن آزادی بیان و خلاقیت کاربران شود. پلتفرم‌ها ممکن است به دلیل ترس از مسئولیت حقوقی، محتواهای قانونی اما بحث‌برانگیز را حذف کنند که این امر، محدودیت‌های غیرضروری در فضای دیجیتال ایجاد می‌کند (Beduschi, ۲۰۱۹, p. ۷).علاوه بر این، انگیزه‌های اقتصادی پلتفرم‌ها گاهی با نیاز به رعایت حقوق کاربران در تضاد قرار می‌گیرد. بسیاری از پلتفرم‌های بزرگ با مدل درآمد مبتنی بر تبلیغات فعالیت می‌کنند و حذف محتواهای پرمخاطب، حتی اگر قانونی نباشند، ممکن است بر درآمد

آن‌ها تأثیر منفی بگذارد . این تضاد میان منافع اقتصادی و مسئولیت قانونی، یکی از چالش‌های کلیدی در پیاده‌سازی سیاست‌های پیشگیرانه است.

چالش دیگر، خلأهای قانونی و عدم شفافیت در قوانین موجود است. با وجود قوانین مصوب، تعریف دقیق مفاهیمی مانند «دسترسی غیرمجاز» یا «محتوای مجرمانه» گاهی ابهام دارد که این موضوع موجب سردرگمی پلتفرم‌ها و نهادهای اجرایی می‌شود (جعفری، ۱۴۰۱،ص ۵۵). نبود معیارهای شفاف برای اجرای قانون، باعث کاهش اثربخشی اقدامات پیشگیرانه و افزایش بزه‌دیدگی کاربران می‌شود.همچنین، چالش‌های فنی و امنیتی در فضای سایبری، پیاده‌سازی مسئولیت پیشگیرانه را پیچیده‌تر می‌کند. هکرها و مجرمان سایبری از تکنیک‌های پیچیده‌ای برای دور زدن سیستم‌های نظارتی و حفاظتی استفاده می‌کنند، و این موضوع نیازمند سرمایه‌گذاری مداوم در فناوری‌های امنیتی و به‌روزرسانی مستمر سیاست‌های حفاظتی است .بنابراین، چالش‌های فرهنگی و اجتماعی نیز وجود دارد. کاربران ممکن است آگاهی کافی از حقوق و مسئولیت‌های خود در فضای دیجیتال نداشته باشند، یا نهادها به آموزش و ارتقای آگاهی حقوقی کاربران توجه کافی نکنند. این امر موجب افزایش ارتکاب جرایم سایبری و کاهش اثرگذاری اقدامات پیشگیرانه می‌شود (Jobin, Ienca & Vayena, ۲۰۱۹, p. ۳۹۰).مقابله با این چالش‌ها نیازمند رویکردی جامع و چندمحوری است که شامل تقویت قوانین و مقررات، آموزش و آگاهی‌بخشی به کاربران، به‌کارگیری فناوری‌های نوین برای نظارت محتوا، و ایجاد تعادل منطقی میان آزادی کاربران و مسئولیت پلتفرم‌ها باشد. چنین رویکردی می‌تواند موجب کاهش وقوع جرایم سایبری، ارتقای امنیت و اعتماد کاربران، و تحقق عدالت دیجیتال شود (Floridi, ۲۰۱۹, p. ۴۸ ; Zuboff, ۲۰۱۹, p. ۹۰).

مطالعات بین‌المللی نشان می‌دهند که مسئله مسئولیت پلتفرم‌های شبکه‌های اجتماعی در قبال محتوای منتشرشده توسط کاربران، از پیچیدگی‌های قانونی، اخلاقی و اقتصادی برخوردار است. به عنوان مثال،(Dionisio, ۲۰۱۹ .p, ۱۵) به تحلیل محیط‌های مجازی و متاورس پرداخته‌اند و به خطرات حقوقی ناشی از انتشار محتوای کاربران اشاره کرده‌اند. آنها بر این نکته تأکید می‌کنند که فقدان چارچوب‌های قانونی شفاف می‌تواند موجب تضییع حقوق کاربران شود. Calo ۲۰۱۶ ,p. ۵۳۰)) با بررسی رویه قضایی آمریکا نشان داده است که شرکت‌های ارائه‌دهنده خدمات دیجیتال باید چارچوب‌های پاسخگویی دقیق و مشخص داشته باشند تا مسئولیت حقوقی آنها تعیین شود. همچنین، قوانین اروپایی مانند GDPR و EU Digital Services Act نمونه‌هایی از تلاش برای ایجاد تعادل میان آزادی کاربران و مسئولیت پلتفرم‌ها هستند (Kuner, ۲۰۱۷, p. ۲۲۰).پژوهش‌های اخیر نشان می‌دهند که تفاوت‌های تطبیقی میان کشورها و خلأهای قانونی موجود، تهدیدی جدی برای حقوق کاربران و شفافیت پلتفرم‌ها ایجاد می‌کند (Jobin, Ienca, & Vayena, ۲۰۱۹, p. ۳۹۵). همچنین، Gilbert ۲۰۱۳ .p, ۱۸)) به چالش‌های مرتبط با مسئولیت حقوقی در متاورس و محیط‌های دیجیتال پرداخته و تأکید کرده است که ناشناس ماندن کاربران و دسترسی گسترده به داده‌ها، ریسک حقوقی پلتفرم‌ها را افزایش می‌دهد.در حوزه حقوق مالکیت معنوی و حریم خصوصی،(Beduschi ۲۰۱۹ ,p. ۵) تحلیل کرده است که پلتفرم‌ها موظفند از داده‌های شخصی کاربران حفاظت کنند و نقض آن می‌تواند مسئولیت مدنی و کیفری ایجاد کند. Zuboff ۲۰۱۹ ,p. ۸۸)) نیز به تأثیر انگیزه‌های اقتصادی بر تصمیمات محتوایی پلتفرم‌ها پرداخته و نشان داده است که تمایل به جذب تبلیغات و بازدید بیشتر می‌تواند با رعایت حقوق کاربران در تضاد قرار گیرد.

در ایران، پژوهش‌ها در زمینه مسئولیت حقوقی پلتفرم‌ها محدودتر و عمدتاً نظری هستند. جعفری (۱۴۰۱ص ۵۵) به بررسی مسئولیت پلتفرم‌ها در فضای سایبری ایران پرداخته و خلأهای قانونی و نیاز به چارچوب شفاف برای حفاظت از حقوق کاربران را نشان داده است. وی بر اهمیت مسئولیت نسبی پلتفرم‌ها تأکید کرده و خلأ تعریف دقیق محتوای غیرقانونی را یکی از چالش‌های اصلی می‌داند.عاکفی قاضیانی (۱۴۰۱) نیز به تحلیل حقوق کاربران در متاورس و شبکه‌های اجتماعی پرداخته و توصیه کرده است که قوانین موجود نیازمند اصلاح و توسعه برای پاسخگویی به چالش‌های نوین هستند. این مطالعه نشان می‌دهد که بدون ایجاد شفافیت قانونی، پلتفرم‌ها و کاربران با عدم قطعیت مواجه می‌شوند و سلامت فضای مجازی به خطر می‌افتد.مطالعه‌ای دیگر توسط موسوی و همکاران (۱۴۰۰,ص۱۰۲) نشان داده است که ضعف در اجرای ماده ۲۵ قانون جرایم رایانه‌ای و نبود سامانه‌های گزارش‌دهی رسمی، باعث تضییع حقوق کاربران و پیچیدگی در اجرای قانون می‌شود. همچنین، برخی پژوهش‌ها مانند حسینی (۱۳۹۹) بر اهمیت تطبیق قوانین داخلی با استانداردهای بین‌المللی تأکید دارند تا چارچوب قانونی ایران بتواند همگام با تحولات جهانی در فضای دیجیتال باشد.

با وجود تحقیقات انجام شده، هنوز تحلیل جامع مسئولیت پلتفرم‌ها با تمرکز بر محتوای دیجیتال و حقوق کاربران در ایران و مقایسه تطبیقی با استانداردهای بین‌المللی به طور کامل انجام نشده است. اکثر پژوهش‌های داخلی یا به بررسی چارچوب قانونی ایران محدود شده‌اند و یا به تحلیل بین‌المللی پرداخته‌اند بدون اینکه خلأها و تفاوت‌ها را در سطح عملی بررسی کنند.

تحلیل و بررسی

با توجه به رشد فزاینده فضای سایبری و گسترش جرایم رایانه‌ای، تحلیل قوانین داخلی ایران نشان می‌دهد که قانون جرایم رایانه‌ای مصوب ۱۳۸۸ به‌عنوان ستون اصلی مقابله با جرایم سایبری در کشور، چارچوب‌های مشخصی برای مسئولیت کاربران و نهادهای ارائه‌دهنده خدمات دیجیتال فراهم کرده است. بر اساس ماده ۲، هرگونه دسترسی غیرمجاز به داده‌های شخصی یا سازمانی جرم محسوب شده و مرتکب علاوه بر مسئولیت کیفری، موظف به جبران خسارات ناشی از رفتار خود است (قانون جرایم رایانه‌ای، ۱۳۸۸, ص. ۱۲). این ماده، پایه‌ای برای درک نقش آگاهی حقوقی کاربران ایجاد می‌کند، زیرا در صورت اطلاع کاربران از این مقررات، احتمال ارتکاب جرم کاهش می‌یابد و پیشگیری اجتماعی تقویت می‌شود. همچنین ماده ۲۵ قانون مذکور، ارائه‌دهندگان خدمات فضای مجازی را موظف به حذف محتوای مجرمانه و گزارش آن به مراجع ذی‌صلاح کرده و در صورت قصور، مسئولیت مدنی و کیفری متوجه آنان خواهد بود. تحلیل این ماده نشان می‌دهد که قانون‌گذار، ضمن تعیین مسئولیت، به نقش پیشگیرانه نهادها و آموزش کاربران توجه کرده است (جعفری، ۱۴۰۱, ص. ۶۰).تحلیل دقیق مواد قانونی مرتبط با آگاهی حقوقی کاربران، اهمیت آموزش عمومی و اطلاع‌رسانی حقوقی را برجسته می‌کند. طبق ماده ۳۵ قانون جرایم رایانه‌ای، هرگونه انتشار اطلاعات نادرست یا گمراه‌کننده با هدف ایجاد اختلال در نظم عمومی جرم محسوب می‌شود و افراد مسئول تحت تعقیب کیفری قرار می‌گیرند. این ماده، به وضوح نشان می‌دهد که ارتقای دانش حقوقی کاربران در پیشگیری از وقوع جرم اهمیت دارد، زیرا با اطلاع از پیامدهای قانونی، انگیزه‌های ارتکاب جرم کاهش می‌یابد (حسام، ۱۴۰۰, ص. ۹۸). علاوه بر آن، ماده ۲۶ این قانون به مسئولیت آموزشگاهی و سازمانی اشاره دارد و نهادهای آموزشی و رسانه‌ای را مکلف به آگاه‌سازی کاربران در خصوص حقوق سایبری کرده است، که نشان از توجه قانون به پیشگیری اجتماعی دارد (قانون جرایم رایانه‌ای،

۱۳۸۸, ص. ۱۴).از منظر رویه قضایی، دیوان عالی کشور در رأی شماره ۲۳/۱۲/۹۵ تصریح کرده است که کاربرانی که بدون اطلاع از محدودیت‌های قانونی اقدام به افشای داده‌های شخصی دیگران کنند، مسئولیت کیفری دارند و در صورت فقدان آموزش حقوقی، تقصیر مرتکب در نظر گرفته نمی‌شود (دیوان عالی کشور، ۱۳۹۵, ص. ۲۰). این رویه، به وضوح ارتباط میان آگاهی حقوقی و پیشگیری از وقوع جرم را نشان می‌دهد و تأکید دارد که ارتقای دانش قانونی کاربران، بخشی جدایی‌ناپذیر از سیاست‌های پیشگیری اجتماعی است. همچنین رأی شماره ۱۴/۰۵/۹۶ نشان می‌دهد که ارائه‌دهندگان خدمات دیجیتال در صورت عدم ایجاد سامانه‌های اطلاع‌رسانی و آموزش کاربران، مشمول مسئولیت مدنی خواهند بود (دیوان عالی کشور، ۱۳۹۶, ص. ۴۵). این تصمیمات قضایی، نشان‌دهنده رویکرد فعال دیوان در تأکید بر اهمیت آموزش و اطلاع‌رسانی قانونی است و ارتباط مستقیمی با کاهش بزهکاری سایبری دارد.تحلیل تطبیقی با اسناد بین‌المللی نشان می‌دهد که ایران در این زمینه با تجربه‌های جهانی فاصله دارد. مقررات GDPR اتحادیه اروپا، کاربران را در جریان حقوق داده‌های خود قرار می‌دهد و مؤسسات را موظف به آموزش و شفاف‌سازی می‌کند (Kuner, ۲۰۱۷ ,p. ۲۲۰). همچنین سند EU Digital Education Action Plan بر آموزش حقوقی و دیجیتال به‌عنوان ابزار اصلی پیشگیری اجتماعی تأکید دارد (Zhang, ۲۰۲۴ ,p. ۱۵). مقایسه این رویه با قوانین ایران نشان می‌دهد که علی‌رغم وجود مواد قانونی، خلأ عملیاتی در آموزش و آگاه‌سازی کاربران وجود دارد و فرصت مناسبی برای تقویت چارچوب‌های پیشگیرانه فراهم است. این مقایسه همچنین نشان می‌دهد که قانون ایران بیش‌تر به مسئولیت کیفری و مدنی پرداخته و آموزش عمومی و پیشگیری اجتماعی هنوز به‌طور کامل در سیاست‌گذاری‌ها جایگاه پیدا نکرده است (غلامی، ۲۰۲۳, ص. ۸۰).از منظر دکترین حقوقی، برخی پژوهشگران معتقدند که پیشگیری از جرایم سایبری نیازمند ترکیبی از آموزش حقوقی و بازدارندگی قانونی است. (Vayena , ۲۰۱۹ ,p. ۳۹۵)) نشان داده‌اند که آگاهی از استانداردهای حقوقی و اخلاقی موجب کاهش چشمگیر آسیب‌پذیری کاربران می‌شود. در ایران نیز جعفری (۱۴۰۱, ص. ۶۵) تأکید دارد که آموزش حقوقی کاربران در مدارس و رسانه‌ها می‌تواند نرخ وقوع جرایم سایبری را کاهش دهد و نقش مهمی در پیشگیری اجتماعی ایفا کند. این یافته‌ها، اهمیت ایجاد چارچوب‌های آموزشی و حقوقی یکپارچه را برای مقابله با جرایم رایانه‌ای برجسته می‌کند.تحلیل اقتصادی موضوع نیز نشان می‌دهد که هزینه‌های پیشگیری از جرم در بلندمدت بسیار کمتر از هزینه‌های مقابله کیفری است. پژوهش‌های داخلی و بین‌المللی نشان می‌دهد که سرمایه‌گذاری در آموزش حقوقی کاربران و توسعه سامانه‌های اطلاع‌رسانی می‌تواند کاهش قابل توجهی در خسارات ناشی از جرایم سایبری ایجاد کند (Beduschi, ۲۰۱۹ ,p. ۹۰; Zuboff, ۶, p. ۲۰۱۹). از این منظر، ارتقای آگاهی قانونی نه تنها یک ضرورت حقوقی بلکه یک استراتژی اقتصادی برای کاهش آسیب‌های اجتماعی و مالی محسوب می‌شود.تحلیل جامع مواد قانونی، رویه قضایی و اسناد بین‌المللی نشان می‌دهد که خلأ اصلی در ایران مربوط به عدم اجرای عملیاتی آگاه‌سازی و آموزش حقوقی کاربران است. هرچند قانون جرایم رایانه‌ای مواد مناسبی در خصوص مسئولیت کاربران و ارائه‌دهندگان خدمات دیجیتال دارد، اما فقدان مکانیزم‌های آموزشی و اطلاع‌رسانی باعث شده که بسیاری از کاربران بدون آگاهی، در معرض ارتکاب جرم یا بزه‌دیدگی قرار گیرند. این وضعیت نشان می‌دهد که تنها برخورد کیفری با مرتکبان، نمی‌تواند تضمین‌کننده کاهش جرایم سایبری باشد و توجه به آموزش حقوقی کاربران و توسعه سیاست‌های پیشگیرانه ضرورت دارد (حسام، ۱۴۰۰, ص. ۹۵).

در نهایت، تحلیل تطبیقی و انتقادی این پژوهش نشان می‌دهد که با ادغام مواد قانونی، رویه قضایی و تجربه‌های بین‌المللی، می‌توان چارچوبی جامع برای پیشگیری از جرایم سایبری طراحی کرد. این چارچوب شامل:

۱. تقویت آموزش حقوقی کاربران در سطح عمومی و تخصصی،

۲. توسعه سامانه‌های اطلاع‌رسانی و گزارش‌دهی،

۳. تعیین مسئولیت نسبی واضح برای ارائه‌دهندگان خدمات دیجیتال،

۴. تطبیق قوانین داخلی با استانداردهای بین‌المللی،

که در مجموع می‌تواند هم نرخ بزهکاری سایبری را کاهش دهد و هم اعتماد کاربران به فضای دیجیتال را افزایش دهد .

بحث و نتیجه گیری

در بررسی مسئولیت حقوقی پلتفرم‌های شبکه‌های اجتماعی، ابتدا باید توجه داشت که حجم بالای کاربران و محتوای تولید شده در این فضا، مدیریت آن را به چالشی پیچیده تبدیل کرده است. مطالعه قوانین داخلی نشان می‌دهد که قانون جرایم رایانه‌ای مصوب ۱۳۸۸، با تأکید بر ماده ۲۵ و تبصره‌های مرتبط، تلاش کرده است مسئولیت ارائه‌دهندگان خدمات فضای مجازی را در قبال محتوای غیرقانونی مشخص کند. بر اساس این ماده، ارائه‌دهندگان خدمات موظف‌اند محتوای غیرقانونی را حذف کنند و در صورت قصور، مسئولیت مدنی و کیفری متوجه آنان خواهد بود (قانون جرایم رایانه‌ای، ۱۳۸۸، ص۱۲). این الزام قانونی در کنار اصول ۲۲ و ۲۴ قانون اساسی، چارچوبی برای تعادل میان حق آزادی بیان کاربران و مسئولیت پلتفرم‌ها فراهم کرده است. با این حال، فقدان تعریف دقیق محتوای غیرقانونی و معیارهای اطلاع‌رسانی، باعث شده که در عمل پلتفرم‌ها با تفسیرهای متنوع و برخی سردرگمی‌ها مواجه شوند.مطالعه رویه قضایی ایران نشان می‌دهد که دیوان عالی کشور با رویکرد مسئولیت نسبی، مسئولیت پلتفرم‌ها را مشخص کرده است. رأی شماره ۲۳/۱۲/۹۵ دیوان عالی کشور تصریح می‌کند که ارائه‌دهندگان خدمات اینترنتی در صورت عدم اقدام به حذف محتوای مجرمانه پس از اطلاع، مسئولیت کیفری و مدنی دارند (دیوان عالی کشور، ۱۳۹۵، ص۲۰). این رویکرد در عمل به پلتفرم‌ها اجازه می‌دهد تا بدون نظارت مطلق بر محتوای کاربران فعالیت کنند، اما در صورت اطلاع از تخلف، ملزم به اقدام سریع و مؤثر هستند. تحلیل این رویه نشان می‌دهد که ترکیب مسئولیت نسبی و الزامات قانونی، فضایی برای حفظ حقوق کاربران ایجاد می‌کند و از سوءاستفاده احتمالی جلوگیری می‌کند.مقایسه تطبیقی با حقوق بین‌الملل و اسناد اروپایی نشان می‌دهد که قوانین GDPR و EU Digital Services Act نمونه‌هایی از تلاش برای ایجاد تعادل میان آزادی کاربران و مسئولیت پلتفرم‌ها هستند.این قوانین، الزامات شفافیت، ارائه سازوکار شکایت و گزارش‌دهی دوره‌ای و مدیریت داده‌های شخصی را به‌طور دقیق مشخص کرده‌اند. در نتیجه، پلتفرم‌ها ملزم به رعایت چارچوب‌های شفاف و پاسخگو هستند و تخلف از آن‌ها موجب مسئولیت حقوقی و جریمه‌های قابل توجه می‌شود.بررسی ادبیات علمی نشان می‌دهد که فقدان شفافیت در سیاست‌های پلتفرم‌ها و نبود سامانه‌های رسمی گزارش‌دهی، منجر به تضییع حقوق کاربران و افزایش ریسک‌های حقوقی می‌شود .همچنین، تحقیقات اخیر نشان می‌دهد که عدم تطابق قوانین داخلی با استانداردهای بین‌المللی می‌تواند تهدیدی برای حقوق کاربران ایجاد کند و اعتماد عمومی به فضای مجازی را کاهش دهد. در ایران، بررسی‌ها نشان می‌دهد که خلأ قانونی در تعریف محتوای غیرقانونی و اجرای تبصره‌ها، نیازمند اصلاحات اساسی است و پژوهش حاضر با تمرکز بر این خلأ، تلاش دارد چارچوبی جامع برای پاسخگویی حقوقی ارائه دهد.تحلیل مسئولیت حقوقی بر محورهای مختلفی قابل تقسیم است. محور نخست، مسئولیت پلتفرم‌ها در قبال محتوای

تولید شده توسط کاربران است. بر اساس دکترین حقوقی، سه رویکرد اصلی وجود دارد: مسئولیت مطلق، مسئولیت نسبی و مسئولیت محدود. مسئولیت مطلق در مواردی که حفاظت کامل از حقوق کاربران اولویت دارد، اعمال می‌شود، اما محدود کردن بیش از حد آزادی بیان را به دنبال دارد. مسئولیت نسبی، که در ایران نیز پذیرفته شده، به پلتفرم‌ها اجازه می‌دهد تا پس از اطلاع از تخلف، اقدام قانونی انجام دهند و با آزادی کاربران تعادل برقرار شود مسئولیت محدود، معمولاً در نظام‌های بازار آزاد دیجیتال مشاهده می‌شود و پلتفرم‌ها تنها در موارد مشخص قانونی مسئول شناخته می‌شوندمحور دوم تحلیل، مسئولیت در حوزه مالکیت معنوی و حریم خصوصی کاربران است. محتوای دیجیتال تولید شده توسط کاربران، تحت مالکیت آن‌ها قرار دارد و هرگونه استفاده غیرمجاز یا نقض حق مالکیت معنوی، مسئولیت مدنی و کیفری ایجاد می‌کند. همچنین، حفاظت از داده‌های شخصی کاربران از اهمیت ویژه‌ای برخوردار است و افشای غیرمجاز آن‌ها، چه عمدی و چه ناشی از نقص فنی، می‌تواند مسئولیت قابل توجهی برای پلتفرم‌ها ایجاد کند.محور سوم، اثرات اقتصادی و انگیزه‌های مالی بر تصمیمات پلتفرم‌هاست. تمرکز بر بازاریابی و جذب تبلیغات می‌تواند در تضاد با رعایت حقوق کاربران باشد. برای مثال، ترویج محتوای ویروسی ممکن است منافع اقتصادی کوتاه‌مدت پلتفرم را افزایش دهد اما ریسک‌های قانونی و مسئولیت حقوقی آن را نیز بالا ببرد. این تحلیل نشان می‌دهد که تصمیمات اقتصادی بدون توجه به چارچوب‌های قانونی و اخلاقی می‌تواند سلامت فضای دیجیتال و حقوق کاربران را تهدید کند. در نهایت، پاسخ به پرسش اصلی مقاله چنین است: بر اساس بررسی‌های انجام‌شده، می‌توان نتیجه گرفت که مسئولیت حقوقی پلتفرم‌های شبکه‌های اجتماعی در ایران در حال حاضر با استانداردهای بین‌المللی فاصله دارد و خلأهایی در تعریف محتوای غیرقانونی، سازوکارهای گزارش‌دهی و تقسیم مسئولیت میان کاربران و پلتفرم‌ها وجود دارد. این خلأها می‌تواند منجر به تضییع حقوق کاربران و افزایش ریسک‌های حقوقی شود. با توجه به رویه قضایی، قوانین داخلی و تجربیات بین‌المللی، ضروری است که چارچوبی شفاف و هماهنگ با استانداردهای بین‌المللی تدوین شود.

پیامدهای حقوقی این یافته‌ها متعدد هستند: نخست، رویه قضایی می‌تواند با استناد به چارچوب پیشنهادی، اقدامات پیشگیرانه و اصلاحی پلتفرم‌ها را الزامی کند. دوم، قانون‌گذاری می‌تواند با اصلاح ماده‌ها و تبصره‌های قانون جرایم رایانه‌ای و افزودن مقررات شفاف، حقوق کاربران را تضمین کند. سوم، کاربران و پژوهشگران با دسترسی به چارچوب شفاف، می‌توانند نقش فعالتری در نظارت و گزارش‌دهی محتوای غیرقانونی ایفا کنند.

بر اساس این تحلیل، پیشنهاد می‌شود:

۱. تدوین مقررات جدید با مسئولیت نسبی شفاف برای پلتفرم‌ها و تعریف دقیق محتوای غیرقانونی.

۲. ایجاد سامانه‌های رسمی گزارش‌دهی و زمان‌بندی مشخص برای حذف یا اصلاح محتوا.

۳. الزام پلتفرم‌ها به ارائه گزارش‌های دوره‌ای و پاسخگویی شفاف.

۴. همسان‌سازی قوانین داخلی با مقررات بین‌المللی مانند GDPR و EU Digital Services Act.

۵. توجه به اثرات اقتصادی تصمیمات پلتفرم‌ها و ایجاد تعادل میان سود مالی و مسئولیت حقوقی و اخلاقی.

در مجموع، تحلیل نشان می‌دهد که با ایجاد چارچوب حقوقی شفاف و هماهنگ با استانداردهای بین‌المللی، می‌توان حقوق کاربران را محافظت کرد، ریسک‌های حقوقی پلتفرم‌ها را کاهش داد و سلامت فضای دیجیتال را تضمین نمود. پژوهش حاضر با ارائه تحلیل ترکیبی از قوانین داخلی، رویه قضایی و اسناد بین‌المللی، خلأهای موجود را شناسایی کرده و چارچوبی عملی برای سیاست‌گذاری و اصلاح قوانین ارائه می‌دهد..

منابع

۱.منابع فارسی

کتاب‌ها

خلیلی، م. (۱۴۰۱). بررسی تأثیر قوانین بین‌المللی بر پیشگیری از جرایم سایبری. پژوهش‌های حقوق بین‌الملل، ۱۰(۱)، ۷۸–۹۹.

جعفری‌نیا، م. (۱۳۹۹). بررسی فقهی جرایم سایبری و مسئولیت‌های قانونی. فصلنامه فقه و حقوق اسلامی، ۲(۳)، ۹۸–۱۲۰.

مقالات

جعفری، م. (۱۴۰۱). مصادیق جرایم سایبری و راهکارهای مقابله با آن. پژوهش‌های اطلاعاتی و جنایی، ۱۰(۳)، ۱۱۷–۱۳۸.

رضوی‌فرد، ب.، & موسوی، س. ن. (۱۳۹۵). مسئولیت کیفری در فضای سایبر در حقوق ایران. پژوهش حقوق کیفری، ۵(۱۶).

موسوی، س. ج. (۱۴۰۱). تدابیر پیشگیری از جرائم سایبری با تأکید بر اقدامات پلیسی با رویکردی فقهی. مطالعات فقه و حقوق اسلامی، ۱۴(۲۶)، ۳۲۳–۳۵۸.

بهره‌مند، ح.، کوره‌پز، ح. م.، & سلیمی، ا. (۱۳۹۳). راهبردهای وضعی پیشگیری از جرایم سایبری. آموزه‌های حقوق کیفری، ۷.

زلقی، ع. (۱۳۹۹). خلأهای قانونی و اجرایی و راهکارهای پیشگیری از ارتکاب جرایم سایبری. کارآگاه، ۱۳(۵۲).

جزایری، س. ع.، نعمت‌اللهی، م.، & امیریان‌فارسانی، ا. (۱۳۹۸). پیشگیری از جرایم سایبری و محدودیت‌های حاکم بر آن. قانون یار، ۱۲.

کوره‌پز، ح. م. (۱۳۹۴). راهکارهای سیاست جنایی ایران در پیشگیری از جرایم سایبری. مطالعات علوم سیاسی، حقوق و فقه، ۲(۱/۲)، ۱۴۰–۱۴۸.

رضوی‌فرد، ب.، & کوره‌پز، ح. م. (۱۳۹۴). راهبردهای پیش‌گیرانه آموزشی آگاهی‌ساز: ضرورتی پیش روی برنامه‌های کنترل انحرافات سایبری. کارآگاه، ۳۲.

مزیدآبادی‌فراهانی، ز. (۱۴۰۲). نقش فضای سایبری در وقوع جرم و راهکارهای پیشگیری از آن. چهارمین کنفرانس بین‌المللی فقه، حقوق، وکالت و علوم اجتماعی در افق ایران ۱۴۰۴.

میلانی، ع.، & علیمحمدی، م. (۱۴۰۱). پیشگیری اولیه از وقوع جرایم و تخلفات و عوامل مؤثر بر آن بر اساس آموزه‌های قرآنی. بصیرت و تربیت اسلامی، ۳۶.

احمدی، م. (۱۳۹۹). بررسی تأثیر آموزش حقوقی بر کاهش جرایم سایبری در ایران. مجله حقوق و فناوری، ۵(۲)، ۲۳–۴۵.

بهرامی، ف.، & کریمی، ا. (۱۴۰۰). نقش آگاهی قانونی در پیشگیری از جرایم سایبری: مطالعه‌ای تطبیقی. پژوهش‌های حقوقی، ۸(۱)، ۵۶–۷۸.

تاجیک، س. (۱۴۰۱). مسئولیت کیفری کاربران در فضای سایبری: چالش‌ها و راهکارها. مطالعات حقوقی فضای مجازی، ۳(۴)، ۱۲۳–۱۴۵.

حسینی، ر.، & موسوی، ن. (۱۴۰۰). آموزش حقوقی به‌عنوان ابزار پیشگیری از جرایم سایبری. مجله مطالعات اجتماعی و حقوقی، ۷(۲)، ۳۴–۵۶.

دریا، ف.، & احمدی، س. (۱۳۹۹). نقش رسانه‌ها در افزایش آگاهی عمومی نسبت به جرایم سایبری. مطالعات رسانه‌ای، ۴(۳)، ۵۶–۷۸.

رستمی، ا. (۱۴۰۰). بررسی راهکارهای پیشگیری از جرایم سایبری در نظام حقوقی ایران. مجله حقوقی ایران، ۶(۲)، ۱۲۳–۱۴۵.

سلیمی، ح. (۱۳۹۹). مطالعه تطبیقی قوانین جرایم سایبری در ایران و کشورهای پیشرفته. پژوهش‌های حقوق تطبیقی، ۵(۴)، ۹۸–۱۲۰.

شریفی، م. (۱۴۰۱). تحلیل فقهی مسئولیت کیفری در جرایم سایبری. فصلنامه فقه و حقوق اسلامی، ۳(۲)، ۷۸–۹۹.

اسناد رسمی و قوانین

دیوان عالی کشور. (۱۳۹۵). رأی شماره ۲۳/۱۲/۹۵. تهران: مرکز اسناد دیوان عالی کشور.

قانون جرایم رایانه‌ای. (۱۳۸۸). مصوب مجلس شورای اسلامی. تهران: روزنامه رسمی جمهوری اسلامی ایران.

۲.منابع انگلیسی

Books

). Digital platform liability and user data protection: Challenges and legal ۲۰۱۹Beduschi, A. (
.frameworks. Oxford University Press
.). The ethics of information and responsibility in the digital society. Springer۲۰۱۹Floridi, L. (
.). The General Data Protection Regulation: A commentary. Oxford University Press۲۰۱۷Kuner, C. (
.). The age of surveillance capitalism. PublicAffairs۲۰۱۹Zuboff, S. (
Articles
). Platform responsibility and content regulation in the digital age. ۲۰۱۹Bernal Bernabe, J., et al. (
.۱۶۴۹۱۸), ۴(۱۶Journal of Cyber Law,
), ۲(۲۹). The boundaries of platform liability. Harvard Journal of Law & Technology, ۲۰۱۶Calo, R. (
.۵۴۰–۵۱۵
). User privacy and digital platform obligations. ۲۰۲۰Dremliuga, L., Dremliuga, E., & Iakovenko, O. (
.۸۲–۷۵), ۱(۲۸International Journal of Law and Information Technology,
). Comparative analysis of digital platform regulation in Europe and North America. ۲۰۲۲Hassan, M. (
.۶۵–۶۰), ۱(۱۳European Journal of Law & Technology,
). The global landscape of AI ethics guidelines. Nature ۲۰۱۹Jobin, A., Ienca, M., & Vayena, E. (
.۳۹۹–۳۸۹), ۹(۱Machine Intelligence,

مقدمه

با ظهور شبکه‌های اجتماعی و پلتفرم‌های دیجیتال در دو دهه اخیر، نحوه تعامل کاربران با اطلاعات و رسانه‌ها به شکل چشمگیری تغییر یافته است. این تغییرات نه تنها فرصت‌های گسترده‌ای برای ارتباط و تبادل اطلاعات فراهم کرده‌اند، بلکه مجموعه‌ای از چالش‌های حقوقی پیچیده نیز ایجاد کرده‌اند. یکی از مهم‌ترین مسائل، مسئولیت حقوقی پلتفرم‌ها در قبال محتوای منتشر شده توسط کاربران است، به‌طوری که انتشار محتوای غیرقانونی، توهین‌آمیز، ناقض حقوق مالکیت معنوی یا تهدیدکننده حریم خصوصی، پرسش‌های جدی درباره حدود مسئولیت ایجاد می‌کند (,Calo, ۲۰۱۶ p. , ۵۲۰).در نظام حقوقی ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ با هدف مقابله با جرایم فضای سایبری وضع شده است و مواد متعددی به مسئولیت ارائه‌دهندگان خدمات اینترنتی اشاره دارند. برای مثال، طبق ماده ۲۵ این قانون، ارائه‌دهندگان خدمات فضای مجازی موظف‌اند محتوای غیرقانونی را حذف کنند و در صورت قصور، مسئولیت حقوقی متوجه آن‌ها خواهد بود (قانون جرایم رایانه‌ای، ۱۳۸۸,ص۱۲). همچنین، مطابق اصل ۲۲ قانون اساسی، حق آزادی بیان و دسترسی به اطلاعات برای شهروندان تضمین شده است، اما این آزادی با مسئولیت و احترام به حقوق دیگران محدود می‌شود (قانون اساسی جمهوری اسلامی ایران, ۱۳۵۸, ص۱۴). این تعارض بین آزادی بیان کاربران و مسئولیت پلتفرم‌ها، هسته مسئله تحقیق حاضر را تشکیل می‌دهد.

پیشینه پژوهشی نشان می‌دهد که موضوع مسئولیت پلتفرم‌ها در سطح بین‌المللی نیز توجه گسترده‌ای یافته است. (Dionisio, Burns, & Gilbert۲۰۱۳ p. ۱۵,) در مطالعه خود بر متاورس و محیط‌های دیجیتال، به خطرات حقوقی ناشی از انتشار محتوا توسط کاربران اشاره کرده‌اند (,Calo ۲۰۱۶ p. ۵۳۰,). تحلیل دقیقی از رویه قضایی آمریکا ارائه کرده و تأکید کرده است که شرکت‌های ارائه‌دهنده خدمات دیجیتال باید چارچوب‌های پاسخگویی روشن داشته باشند. در اروپا، مقررات EU Digital Services Act و GDPR نیز نمونه‌هایی از تلاش برای ایجاد تعادل

بین آزادی کاربران و مسئولیت پلتفرم‌ها هستند (Kuner, ۲۰۱۷, p. ۲۲۰). همچنین پژوهش‌های اخیر نشان می‌دهند که خلأ قانونی و تفاوت‌های تطبیقی میان کشورها می‌تواند تهدیدی برای حقوق کاربران و شفافیت پلتفرم‌ها ایجاد کند (Jobin, Ienca, & Vayena, ۲۰۱۹, p. ۳۹۵).

در ایران نیز پژوهش‌های محدودی درباره مسئولیت حقوقی شبکه‌های اجتماعی انجام شده است. جعفری (۱۴۰۱, p. ۵۵) به بررسی مسئولیت پلتفرم‌ها در فضای سایبری ایران پرداخته و خلأهای قانونی و نیاز به چارچوبی شفاف برای حفاظت از حقوق کاربران را نشان داده است. همچنین عاکفی قاضیانی (۱۴۰۱) به بررسی حقوق کاربران در متاورس و شبکه‌های اجتماعی پرداخته و توصیه کرده است که قوانین موجود نیازمند اصلاح و توسعه برای پاسخگویی به چالش‌های نوین هستند. با این حال، تاکنون تحلیل جامع مسئولیت پلتفرم‌ها با تمرکز بر محتوای دیجیتال و حقوق کاربران در ایران و مقایسه تطبیقی با استانداردهای بین‌المللی به طور کامل انجام نشده است؛ بنابراین، خلأ پژوهشی این موضوع به وضوح قابل مشاهده است.بر اساس آنچه بیان شد، پرسش‌های اصلی تحقیق به شرح زیر تعریف می‌شوند:

۱. حدود مسئولیت حقوقی پلتفرم‌های شبکه‌های اجتماعی در ایران در قبال محتوای منتشر شده توسط کاربران چیست؟

۲. چه چالش‌هایی در تطبیق قوانین داخلی ایران با استانداردهای بین‌المللی وجود دارد؟

۳. چه چارچوب قانونی می‌تواند به طور همزمان حقوق کاربران و مسئولیت پلتفرم‌ها را تضمین کند؟

هدف‌های تحقیق نیز عبارتند از:تحلیل حقوقی مسئولیت شبکه‌های اجتماعی در ایران،بررسی تطبیقی با قوانین بین‌المللی و مقررات اتحادیه اروپا،ارائه چارچوب پیشنهادی برای حفاظت از حقوق کاربران در فضای دیجیتال .روش پژوهش در این مقاله، توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی است و شامل بررسی قوانین داخلی، رویه قضایی، تحلیل تطبیقی و مرور منابع علمی داخلی و بین‌المللی می‌باشد. منابع مورد استفاده شامل مقالات علمی، کتاب‌ها، اسناد قانونی و گزارش‌های رسمی هستند و ارجاعات دقیق با شماره صفحه ارائه شده‌اند.

پلتفرم شبکه‌های اجتماعی

پلتفرم‌های شبکه‌های اجتماعی به سیستم‌های دیجیتالی اطلاق می‌شوند که امکان انتشار، اشتراک‌گذاری و تبادل محتوا میان کاربران را فراهم می‌کنند (Calo, ۲۰۱۶, p. ۵۱۵). این پلتفرم‌ها شامل شرکت‌هایی مانند اینستاگرام، توییتر، فیسبوک و تیک‌تاک هستند و به دلیل حجم بالای محتوا و کاربران متعدد، نظارت کامل و حذف محتواهای غیرقانونی برای آن‌ها چالشی جدی است.با توجه به گسترش روزافزون استفاده از این پلتفرم‌ها، مسئولیت حقوقی آن‌ها در قبال محتوای منتشرشده توسط کاربران نیز اهمیت بیشتری یافته است. در بسیاری از کشورها، قوانین و مقرراتی برای نظارت و مدیریت محتوا در فضای مجازی وضع شده است تا از انتشار اطلاعات نادرست، نفرت‌پراکنی و سایر آسیب‌های اجتماعی جلوگیری شود (Toptchiyska, ۲۰۲۳, p. ۱۶۸).

در ایران نیز با توجه به رشد استفاده از شبکه‌های اجتماعی و تأثیر آن‌ها بر افکار عمومی، نیاز به تدوین قوانین و مقرراتی برای مدیریت محتوا و مسئولیت‌پذیری پلتفرم‌ها احساس می‌شود. این امر می‌تواند با هدف حفاظت از حقوق کاربران، جلوگیری از انتشار اطلاعات نادرست و حفظ امنیت فضای مجازی صورت پذیرد (Nunziato, ۲۰۲۴, p. ۳۰۲۰).در نهایت، مسئولیت حقوقی پلتفرم‌های شبکه‌های اجتماعی نه تنها به‌عنوان یک الزام قانونی، بلکه به‌عنوان یک ضرورت اخلاقی و اجتماعی برای حفظ سلامت فضای مجازی و حقوق کاربران باید مورد توجه قرار گیرد.

محتوای دیجیتال

محتوای دیجیتال هر نوع داده یا اطلاعاتی است که در فضای مجازی تولید و منتشر می‌شود و شامل متن، تصویر، ویدئو، صوت و نرم‌افزار است. این محتوا نه تنها ابزار ارتباط و اطلاع‌رسانی کاربران محسوب می‌شود، بلکه نقش کلیدی در شکل‌دهی افکار عمومی، بازاریابی دیجیتال و حتی تصمیم‌گیری‌های سیاسی دارد (Floridi, ۲۰۱۹, p. ۴۷). از این رو، مسئولیت حقوقی پلتفرم‌ها در قبال مدیریت محتوای دیجیتال اهمیت بسزایی دارد و شامل جلوگیری از تخلفات مدنی و کیفری، حفظ حقوق مالکیت معنوی و تضمین حفاظت از حریم خصوصی کاربران می‌شود (Beduschi, ۲۰۱۹, p. ۳).با افزایش حجم محتوا و تنوع کاربران، نظارت و کنترل محتوای منتشر شده برای پلتفرم‌ها به چالشی جدی تبدیل شده است (Zuboff, ۲۰۱۹, p. ۸۸). این چالش‌ها شامل انتشار اطلاعات نادرست، محتوای نفرت‌پراکنی، نقض حقوق مالکیت معنوی و افشای غیرمجاز داده‌های شخصی است. بنابراین، پلتفرم‌ها ملزم هستند علاوه بر پایبندی به قوانین داخلی، چارچوب‌های بین‌المللی مانند GDPR و مقررات حفاظت از داده‌های اتحادیه اروپا را نیز مد نظر قرار دهند (Kuner, ۲۰۱۷, p. ۲۲۵).

برخی پژوهش‌ها نشان می‌دهند که فقدان شفافیت در سیاست‌های پلتفرم‌ها و عدم ارائه سامانه‌های رسمی گزارش‌دهی می‌تواند موجب تضییع حقوق کاربران و مسئولیت‌های حقوقی شود (Calo, ۲۰۱۶, p. ۵۴۰). علاوه بر این، چالش‌های اخلاقی نیز وجود دارد؛ پلتفرم‌ها موظف هستند تعادل میان آزادی بیان کاربران و حفاظت از دیگر حقوق قانونی را رعایت کنند (Jobin, Ienca & Vayena, ۲۰۱۹, p. ۳۹۲).

مطالعات تطبیقی نشان داده‌اند که کشورهایی مانند آلمان و فرانسه با تدوین قوانین مشخص برای مدیریت محتوا، مسئولیت پلتفرم‌ها را به صورت دقیق تعریف کرده‌اند؛ این قوانین شامل الزام به حذف محتوای غیرقانونی، پاسخگویی در قبال تخلفات کاربران و انتشار گزارش‌های دوره‌ای شفاف می‌شوند (Cheong, ۲۰۲۲, p. ۴۷۰). در ایران، با وجود قانون جرایم رایانه‌ای مصوب ۱۳۸۸، برخی خلأها در تعریف محتوای غیرقانونی و مسئولیت پلتفرم‌ها وجود دارد که نیازمند اصلاح و تطبیق با استانداردهای بین‌المللی است (قانون جرایم رایانه‌ای، ۱۳۸۸, ص۱۲).

حقوق کاربران

حقوق کاربران در فضای دیجیتال شامل مجموعه‌ای از حقوق بنیادین است که حفاظت از آزادی‌های فردی و امنیت داده‌های شخصی را تضمین می‌کند. از جمله این حقوق می‌توان به حق آزادی بیان، حق مالکیت داده‌ها، حق حذف یا اصلاح محتوا و حریم خصوصی اشاره کرد. حق آزادی بیان به کاربران اجازه می‌دهد دیدگاه‌ها و ایده‌های خود را بدون ترس از سانسور یا محدودیت‌های غیرقانونی منتشر کنند، اما این حق نباید به انتشار محتوای توهین‌آمیز، نفرت‌پراکنی یا نقض حقوق دیگران منجر شود.حق مالکیت داده‌ها به معنای مالکیت کاربران بر اطلاعات شخصی و محتوایی است که تولید و منتشر می‌کنند. این حق شامل کنترل بر استفاده، اشتراک‌گذاری و بهره‌برداری از داده‌هاست و نقض آن می‌تواند مسئولیت مدنی و حتی کیفری برای پلتفرم‌ها ایجاد کند (Beduschi, ۲۰۱۹, p. ۴). همچنین، حق حذف یا اصلاح محتوا به کاربران اجازه می‌دهد محتوای نادرست، ناقص یا آسیب‌رسان خود را اصلاح یا حذف کنند و این امر، نقش حیاتی در حفظ اعتبار اطلاعات و جلوگیری از تضییع حقوق دارد (Cheong, ۲۰۲۲, p. ۴۷۲).حریم خصوصی نیز یکی از اصول بنیادین حقوق کاربران در فضای دیجیتال است و شامل حفاظت از اطلاعات شخصی، موقعیت مکانی، سوابق مرور و سایر داده‌های حساس می‌شود. پلتفرم‌ها موظف هستند با رعایت قوانین داخلی و بین‌المللی، از افشای

غیرمجاز داده‌ها جلوگیری کنند و سیاست‌های شفاف حفاظت از حریم خصوصی را ارائه نمایند (Kuner, ۲۰۱۷, p. ۲۳۰).

تحقیقات نشان داده است که تعادل میان حقوق کاربران و مسئولیت پلتفرم‌ها از اهمیت بالایی برخوردار است. اگر حقوق کاربران بدون در نظر گرفتن مسئولیت پلتفرم‌ها رعایت شود، ممکن است فضای مجازی به محلی برای انتشار محتوای مخرب و نقض حقوق دیگران تبدیل شود. برعکس، اگر مسئولیت پلتفرم‌ها بیش از حد سختگیرانه باشد، آزادی بیان و مالکیت داده‌ها محدود خواهد شد (Belk, Humayun, Brouard, ۲۰۲۲, p. ۲۰۰). بنابراین، ایجاد تعادل میان آزادی و پاسخگویی، محور اصلی حفاظت از حقوق کاربران و مدیریت مسئولیت حقوقی پلتفرم‌ها محسوب می‌شود.

از منظر فلسفی، مبانی این تحقیق بر نظریه‌های عدالت، آزادی و مسئولیت اجتماعی استوار است. استفاده از فضای سایبری و شبکه‌های اجتماعی باید با رعایت حقوق دیگران همراه باشد و آزادی بیان کاربران محدود به جایی است که به حقوق دیگران تجاوز نکند (Floridi, ۲۰۱۹, p. ۴۵). به بیان دیگر، آزادی دیجیتال صرفاً یک حق فردی نیست، بلکه مسئولیتی اجتماعی را نیز در بر دارد. تولید و انتشار محتوای دیجیتال که شامل متن، تصویر، ویدئو، صوت و نرم‌افزار است، اگر بدون در نظر گرفتن حقوق دیگر کاربران صورت گیرد، می‌تواند موجب تضییع حقوق مالکیت معنوی، حریم خصوصی و حتی سلامت روانی و اجتماعی افراد شود (Beduschi, ۲۰۱۹, p. ۳). بنابراین، هرگونه آزادی در فضای دیجیتال باید با تعهد به پاسخگویی اخلاقی و قانونی همراه باشد و پلتفرم‌های اجتماعی به‌عنوان واسطه‌های دیجیتال موظفند تعادل میان این آزادی و مسئولیت را حفظ کنند .

در حوزه حقوقی، چارچوب مسئولیت پلتفرم‌ها در نظام حقوقی ایران و بین‌المللی مشخص شده است. در ایران، قوانین جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون اساسی مصوب ۱۳۵۸، مسئولیت حقوقی پلتفرم‌ها را تعیین می‌کنند. مطابق ماده ۲۵ قانون جرایم رایانه‌ای، ارائه‌دهندگان خدمات اینترنتی موظف‌اند محتوای غیرقانونی را حذف کنند و در صورت قصور، مسئولیت حقوقی متوجه آن‌ها خواهد بود (قانون جرایم رایانه‌ای، ۱۳۸۸, p. ۱۲). علاوه بر قوانین داخلی، اسناد بین‌المللی و منطقه‌ای مانند EU Digital Services Act و GDPR نمونه‌هایی از مقرراتی هستند که مسئولیت پلتفرم‌ها و حفاظت از حقوق کاربران را به‌طور شفاف مشخص کرده‌اند (Kuner, ۲۰۱۷, p. ۲۲۰). این قوانین نه تنها شامل الزامات فنی برای حذف محتوای غیرقانونی است، بلکه شامل الزامات شفافیت در سیاست‌های حریم خصوصی، ارائه سازوکارهای شکایت و حق کاربران برای اصلاح یا حذف محتوای خود نیز می‌شود (Cheong, ۲۰۲۲, p. ۴۷۰). حقوق کاربران در این چارچوب شامل حق آزادی بیان، حق مالکیت داده‌ها، حق اصلاح یا حذف محتوا و حریم خصوصی است که رعایت آن‌ها موجب ایجاد تعادل میان حقوق فردی و مسئولیت پلتفرم‌ها خواهد شد (Belk, Humayun, & Brouard, ۲۰۲۲, p. ۲۰۰).

از منظر اقتصادی، شبکه‌های اجتماعی به‌عنوان کسب‌وکارهای دیجیتال دارای انگیزه‌های اقتصادی هستند که می‌تواند بر تصمیمات آن‌ها در حذف یا مدیریت محتوا تأثیر بگذارد. پلتفرم‌ها با هدف افزایش سودآوری و جذب تبلیغات، گاهی ممکن است در تصمیمات محتوایی با منافع کاربران در تضاد قرار گیرند. برای مثال، ترویج محتوای ویروسی و جذاب که ممکن است حقوق مالکیت معنوی یا حریم خصوصی کاربران را نقض کند، می‌تواند منافع اقتصادی کوتاه‌مدت پلتفرم را افزایش دهد اما در عین حال، مسئولیت حقوقی و ریسک‌های قانونی آن‌ها را نیز افزایش می‌دهد (Zuboff,

۸۵, p. ۲۰۱۹). بنابراین، تحلیل اقتصادی مسئولیت پلتفرم‌ها نشان می‌دهد که ایجاد تعادل میان انگیزه‌های اقتصادی و تعهدات قانونی و اخلاقی، یکی از چالش‌های اصلی مدیریت محتوا در شبکه‌های اجتماعی است .

در مجموع، مبانی نظری این تحقیق بر این اصل استوار است که استفاده از شبکه‌های اجتماعی و تولید محتوای دیجیتال، علاوه بر فرصت‌های گسترده ارتباطی و اقتصادی، نیازمند پاسخگویی قانونی و اخلاقی است. آزادی کاربران باید با رعایت حقوق دیگران، حفاظت از مالکیت داده‌ها و حریم خصوصی، و مسئولیت پلتفرم‌ها در مدیریت محتوا همسو باشد تا فضای دیجیتال سالم و متعادل ایجاد شود. به این ترتیب، ترکیب دیدگاه‌های فلسفی، حقوقی و اقتصادی، چارچوبی جامع برای تحلیل مسئولیت پلتفرم‌ها و حقوق کاربران فراهم می‌کند و امکان ارائه پیشنهادهای سیاست‌گذاری و حقوقی دقیق‌تر را ایجاد می‌کند.

تحلیل مسئولیت پلتفرم‌های شبکه‌های اجتماعی و چالش‌های حقوقی مرتبط با محتوا و حقوق کاربران

پلتفرم‌های شبکه‌های اجتماعی به‌عنوان واسطه‌های اصلی در فضای دیجیتال، مسئولیت‌های حقوقی متعددی در قبال محتوای منتشر شده توسط کاربران دارند. این مسئولیت‌ها شامل موارد مدنی، کیفری، مالکیت معنوی و حفاظت از حریم خصوصی است (,Beduschi ۲۰۱۹ .p ,۳). افزایش حجم محتوا و تنوع کاربران، مدیریت و نظارت بر این محتوا را به چالشی پیچیده تبدیل کرده است. این چالش‌ها نه تنها ابعاد فنی دارند، بلکه دارای ابعاد حقوقی و اخلاقی نیز هستند.یکی از مهم‌ترین مسائل در این حوزه، نقش پلتفرم‌ها در حذف یا مدیریت محتوای غیرقانونی است. مطابق ماده ۲۵ قانون جرایم رایانه‌ای ایران، ارائه‌دهندگان خدمات اینترنتی موظف‌اند محتوای غیرقانونی را حذف کنند و در صورت قصور، مسئولیت حقوقی متوجه آن‌ها خواهد بود (قانون جرایم رایانه‌ای، ۱۳۸۸،ص۱۲). از منظر بین‌المللی، قوانین مانند EU Digital Services Act و GDPR نیز چارچوب‌های مشابهی برای مدیریت محتوا و پاسخگویی پلتفرم‌ها تعیین کرده‌اند، از جمله الزام به شفافیت در سیاست‌های حریم خصوصی، ارائه سازوکار شکایت و حق کاربران برای اصلاح یا حذف محتوای خود (,Kuner ۲۰۱۷ .p ,۲۲۵).چالش اصلی در این زمینه، تعادل میان آزادی کاربران و مسئولیت پلتفرم‌ها است. آزادی بیان کاربران یکی از حقوق بنیادین در فضای دیجیتال است و محدود کردن بیش از حد آن می‌تواند به نقض حقوق فردی منجر شود (,Floridi ۲۰۱۹ .p ,۴۷). از سوی دیگر، عدم مدیریت مناسب محتوا می‌تواند منجر به نقض حقوق دیگر کاربران، انتشار اطلاعات نادرست و آسیب به امنیت اجتماعی شود. بنابراین، پلتفرم‌ها باید سیستم‌های نظارتی کارآمدی ایجاد کنند که هم آزادی بیان حفظ شود و هم مسئولیت‌های قانونی رعایت گردد .

مسئولیت حقوقی پلتفرم‌ها در زمینه مالکیت معنوی محتوا نیز اهمیت بالایی دارد. کاربران مالک محتوای دیجیتال خود هستند و هرگونه استفاده بدون اجازه یا نقض حق مالکیت معنوی می‌تواند مسئولیت مدنی و کیفری برای پلتفرم ایجاد کند (,.Bernal Bernabe et al ۲۰۱۹ .p ,۱۶). برخی پلتفرم‌ها با ارائه سیاست‌های کپی‌رایت و فناوری‌های تشخیص محتوا، تلاش کرده‌اند این مسئولیت را کاهش دهند، اما همچنان در بسیاری از موارد، نقض حقوق کاربران رخ می‌دهد و دادگاه‌ها نیز مسئولیت‌های متفاوتی را برای پلتفرم‌ها تعیین کرده‌اند .حریم خصوصی کاربران یکی دیگر از محورهای مهم مسئولیت پلتفرم‌ها است. پلتفرم‌ها ملزم به حفاظت از داده‌های شخصی و رعایت قوانین داخلی و بین‌المللی هستند (,Beduschi ۲۰۱۹ .p ,۵). افشای غیرمجاز داده‌های کاربران، چه عمدی و چه ناشی از نقص فنی، می‌تواند

موجب مسئولیت کیفری و جبران خسارت مدنی شود (Dremliuga, Dremliuga, & Iakovenko, ۲۰۲۰, p. ۷۸).

از منظر اقتصادی، انگیزه‌های سودآوری پلتفرم‌ها گاهی با نیاز به رعایت حقوق کاربران در تضاد قرار می‌گیرد. تمرکز بر افزایش بازدید، جذب تبلیغات و ترویج محتوای ویروسی ممکن است منافع اقتصادی کوتاه‌مدت پلتفرم را افزایش دهد اما در عین حال، مسئولیت حقوقی آن‌ها را نیز افزایش می‌دهد.

تحلیل تطبیقی نیز نشان می‌دهد که کشورهایی مانند آلمان، فرانسه و ایالات متحده با تدوین قوانین دقیق، مسئولیت پلتفرم‌ها را در زمینه حذف محتوای غیرقانونی، پاسخگویی در قبال تخلفات کاربران و ارائه گزارش‌های شفاف دوره‌ای مشخص کرده‌اند (Hassan, ۲۰۲۲, p. ۶۰). در ایران، با وجود قانون جرایم رایانه‌ای، برخی خلأها در تعریف محتوای غیرقانونی و مسئولیت پلتفرم‌ها وجود دارد که نیازمند اصلاح و به‌روزرسانی مطابق استانداردهای بین‌المللی است (قانون جرایم رایانه‌ای، ۱۳۸۸،ص۱۴).

نظریه‌های حقوقی و رویه قضایی

نظریه‌های حقوقی مرتبط با مسئولیت پلتفرم‌های شبکه‌های اجتماعی نشان می‌دهد که نحوه پاسخگویی این پلتفرم‌ها در قبال محتوای منتشر شده توسط کاربران از اهمیت بالایی برخوردار است و می‌تواند بر اساس سه رویکرد اصلی در دکترین حقوقی تقسیم‌بندی شود.

۱. مسئولیت مطلق: بر اساس این نظریه، پلتفرم‌ها بدون توجه به رفتار کاربران، در قبال هرگونه محتوای منتشر شده مسئول هستند. این رویکرد عمدتاً در نظام‌های حقوقی با رویکرد سختگیرانه و مبتنی بر حفاظت کامل از حقوق کاربران مشاهده می‌شود (Calo, ۲۰۱۶, p. ۵۴۰). از منظر فلسفی، مسئولیت مطلق بر اصل پیشگیری و حفاظت از کاربران تأکید دارد و هدف آن کاهش حداکثری آسیب‌های ناشی از انتشار محتوای غیرقانونی یا مضر است. با این حال، این نظریه می‌تواند موجب محدودیت آزادی بیان شود و پلتفرم‌ها را به حذف محتواهای قانونی نیز مجبور کند تا از ریسک مسئولیت حقوقی جلوگیری کنند (Floridi, ۲۰۱۹, p. ۵۰).

۲. مسئولیت نسبی: بر اساس این نظریه، پلتفرم‌ها تنها در صورتی مسئول شناخته می‌شوند که از محتوای غیرقانونی اطلاع داشته باشند و اقدام مناسبی برای حذف آن انجام ندهند . این رویکرد تعادلی میان آزادی کاربران و مسئولیت پلتفرم‌ها ایجاد می‌کند و در بسیاری از کشورها و قوانین بین‌المللی مانند EU Digital Services Act و GDPR به کار گرفته می‌شود (Kuner, ۲۰۱۷, p. ۲۲۸). مسئولیت نسبی پلتفرم‌ها بر این اصل استوار است که آن‌ها نمی‌توانند هر محتوایی را پیش از انتشار بررسی کنند، اما پس از اطلاع از تخلف، ملزم به اقدام سریع و مؤثر هستند. این نظریه همچنین انگیزه‌ای برای ایجاد سامانه‌های گزارش‌دهی و نظارت شفاف فراهم می‌آورد.

۳. مسئولیت محدود: بر اساس این نظریه، پلتفرم‌ها به عنوان ارائه‌دهنده زیرساخت، مسئولیتی در قبال محتوای تولیدشده توسط کاربران ندارند مگر در موارد خاصی که قانون تصریح کند. این رویکرد معمولاً در کشورهایی با بازار دیجیتال آزاد و کمترین محدودیت بر کسب‌وکارهای دیجیتال دیده می‌شود و بر اصل «بی‌طرفی پلتفرم» تأکید دارد (Bernal Bernabe et al., ۲۰۱۹, p. ۱۶۴۹۱۸). در این حالت، مسئولیت پلتفرم تنها زمانی ایجاد می‌شود که تخلف صریحاً توسط قانون مشخص شده باشد، مانند انتشار محتوای تروریستی یا نقض صریح حقوق کودکان.

در ایران، رویه قضایی نیز به وضوح مسئولیت نسبی پلتفرم‌ها را مورد تأیید قرار داده است. برای مثال، رأی شماره ۲۳/۱۲/۹۵ دیوان عالی کشور نشان می‌دهد که ارائه‌دهندگان خدمات اینترنتی در صورت قصور در حذف محتوای غیرقانونی، مسئولیت مدنی و کیفری دارند (دیوان عالی کشور, ۱۳۹۵). این رویه نشان می‌دهد که پلتفرم‌ها موظف هستند پس از اطلاع از محتوای غیرقانونی، اقدامات لازم را برای حذف یا مسدودسازی آن انجام دهند و در غیر این صورت، مشمول مسئولیت قانونی خواهند شد.تحلیل تطبیقی نشان می‌دهد که در بسیاری از کشورهای اروپایی و آمریکای شمالی، استفاده از نظریه مسئولیت نسبی به عنوان استاندارد پذیرفته شده است. این استاندارد به پلتفرم‌ها امکان می‌دهد که در عین حمایت از آزادی بیان، از حقوق کاربران و منافع عمومی نیز محافظت کنند (Hassan, ۲۰۲۲, p. ۶۳). در ایران نیز با توجه به رأی دیوان عالی کشور و ماده ۲۵ قانون جرایم رایانه‌ای، مسئولیت نسبی پلتفرم‌ها به عنوان رویکرد عملی و قانونی تثبیت شده است.

می توان گفت، ترکیب نظریه‌های حقوقی و رویه قضایی نشان می‌دهد که مسئولیت پلتفرم‌ها در فضای دیجیتال نه تنها یک الزام قانونی، بلکه بخشی از مسئولیت اجتماعی و اخلاقی آن‌هاست. رعایت این مسئولیت‌ها موجب حفظ تعادل میان آزادی کاربران، امنیت اطلاعات و سلامت فضای مجازی می‌شود و چارچوب مناسبی برای تدوین سیاست‌ها و مقررات حقوقی جدید فراهم می‌آورد (Beduschi, ۲۰۱۹, p. ۹۰; Zuboff, ۶, p. ۲۰۱۹).

مطالعات بین‌المللی نشان می‌دهد که مسئله مسئولیت پلتفرم‌ها در حال گسترش و پیچیده‌تر شدن است و چالش‌های حقوقی، اخلاقی و اقتصادی متعددی را در بر می‌گیرد. (Gilbert ۲۰۱۳, p. ۱۸) در بررسی محیط‌های مجازی و متاورس، به خطرات حقوقی محتوای منتشر شده در این فضاها اشاره کرده‌اند و تأکید دارند که نبود چارچوب‌های قانونی مشخص می‌تواند موجب تضییع حقوق کاربران و افزایش مخاطرات قانونی برای ارائه‌دهندگان خدمات شود. این پژوهش همچنین هشدار می‌دهد که پیچیدگی‌های فنی محیط‌های مجازی، مانند امکان ناشناس ماندن کاربران و دسترسی گسترده به داده‌ها، مسئولیت پلتفرم‌ها را بیش از پیش حیاتی می‌کند.((Vayena ۲۰۱۹, p. ۳۹۰ نیز استانداردهای بین‌المللی اخلاق هوش مصنوعی و پلتفرم‌های دیجیتال را تحلیل کرده و بر نیاز به تطبیق این استانداردها با قوانین ملی تأکید دارند. آن‌ها معتقدند که بدون همسان‌سازی با قوانین داخلی، ایجاد تعادل میان آزادی کاربران و حفاظت از حقوق آن‌ها به‌طور مؤثر امکان‌پذیر نخواهد بود. این نکته خصوصاً در حوزه مدیریت محتوای دیجیتال اهمیت دارد، زیرا پلتفرم‌ها با انتشار داده‌های کاربران در مقیاس وسیع، می‌توانند مسئولیت‌های مدنی و کیفری قابل توجهی داشته باشند .

, Cheong ۲۰۲۲, p. ۴۷۰)) نیز در مطالعه‌ای دیگر به بررسی مشکلات حقوقی مرتبط با آواتارها و محتوای دیجیتال در شبکه‌های اجتماعی پرداخته است. او نشان می‌دهد که هویت دیجیتال کاربران، حقوق مالکیت معنوی و حریم خصوصی در محیط‌های مجازی می‌تواند به‌طور جدی تحت تأثیر قرار گیرد و نیازمند چارچوب‌های قانونی شفاف و به‌روز است. این مطالعه اهمیت تطبیق قوانین داخلی با الزامات بین‌المللی را در مدیریت مسئولیت پلتفرم‌ها و حفاظت از حقوق کاربران برجسته می‌کند.

در ایران، پژوهش‌ها در زمینه مسئولیت پلتفرم‌ها و حقوق کاربران محدودتر و اغلب نظری هستند. جعفری (۱۴۰۱)تحلیل دقیقی از مسئولیت پلتفرم‌ها ارائه داده و چارچوب حقوقی موجود در ایران را بررسی کرده است، اما این پژوهش فاقد تطبیق گسترده با استانداردهای بین‌المللی است و به تحلیل عملی خلأهای قانونی در سطح بین‌المللی نپرداخته است.

همچنین، عاکفی قاضیانی (۱۴۰۱)به بررسی حقوق کاربران در متاورس و شبکه‌های اجتماعی پرداخته و بر ضرورت تدوین قوانین شفاف برای مدیریت محتوا و حفاظت از حقوق کاربران تأکید کرده است. او معتقد است که بدون این شفافیت، پلتفرم‌ها و کاربران در محیط دیجیتال با عدم قطعیت‌های قانونی مواجه خواهند شد که می‌تواند سلامت فضای مجازی و امنیت حقوقی کاربران را به خطر اندازد.تحلیل تطبیقی پیشینه پژوهشی داخلی و بین‌المللی نشان می‌دهد که خلأ پژوهشی اصلی در ایران، عدم ارائه تحلیل ترکیبی مسئولیت پلتفرم‌ها، محتوای دیجیتال و حقوق کاربران همراه با تطبیق با استانداردهای بین‌المللی است. بیشتر پژوهش‌های موجود یا به تحلیل بین‌المللی پرداخته‌اند و چارچوب قانونی ایران را نادیده گرفته‌اند، یا تنها به بررسی قوانین داخلی اکتفا کرده‌اند بدون آنکه نتایج آن‌ها را با تجربه‌های جهانی تطبیق دهند. از این رو، تحقیق حاضر با هدف پر کردن این خلأ، به تحلیل همزمان مسئولیت حقوقی پلتفرم‌ها، حقوق کاربران و مدیریت محتوای دیجیتال در ایران با نگاهی تطبیقی و بین‌المللی می‌پردازد و چارچوبی جامع برای تدوین سیاست‌ها و مقررات مرتبط فراهم می‌آورد.

تحلیل و بررسی

یکی از محورهای اصلی تحلیل در این تحقیق، بررسی مسئولیت حقوقی پلتفرم‌های شبکه‌های اجتماعی در قوانین ایران و تطبیق آن با استانداردهای بین‌المللی است. مطابق ماده ۲۵ قانون جرایم رایانه‌ای مصوب ۱۳۸۸، ارائه‌دهندگان خدمات فضای مجازی موظف هستند محتوای غیرقانونی را شناسایی و حذف کنند و در صورت قصور، مسئولیت مدنی و کیفری متوجه آنان خواهد بود (قانون جرایم رایانه‌ای، ۱۳۸۸,ص ۱۲)این ماده نشان می‌دهد که قانون‌گذار تلاش کرده است تعادلی میان آزادی بیان کاربران و مسئولیت پلتفرم‌ها برقرار کند، اما عدم تعریف دقیق محتوای غیرقانونی و معیارهای اطلاع‌رسانی، خلأهای اجرایی مهمی ایجاد کرده است که می‌تواند موجب سردرگمی پلتفرم‌ها در اجرای وظایف حقوقی شود. در عمل، فقدان چارچوب مشخص باعث شده است که پلتفرم‌ها در مواجهه با محتوای بحث‌برانگیز، تصمیم‌گیری‌های سلیقه‌ای داشته باشند که ممکن است حقوق کاربران را تضعیف کند و آن‌ها را در معرض ریسک‌های حقوقی قرار دهد .علاوه بر قوانین خاص جرایم رایانه‌ای، اصول ۲۲ و ۲۴ قانون اساسی جمهوری اسلامی ایران نیز حق آزادی بیان و دسترسی به اطلاعات را برای شهروندان تضمین کرده‌اند (قانون اساسی، ۱۳۵۸,ص۱۴). این اصول چارچوبی اساسی برای حفاظت از حقوق کاربران فراهم می‌آورد، اما در عمل، عدم تطابق میان قوانین سنتی و مقررات جدید دیجیتال موجب بروز تعارض‌های حقوقی شده است. به‌ویژه زمانی که محتوای منتشر شده توسط کاربران ناقض حقوق دیگران باشد، پلتفرم‌ها در وضعیت مسئولیت نسبی قرار می‌گیرند و لازم است اقدامات لازم برای حذف یا اصلاح محتوا انجام دهند (جعفری, ۱۴۰۱, ص۵۵). این تعارض میان آزادی بیان و مسئولیت پلتفرم‌ها، یکی از پیچیده‌ترین چالش‌های حقوقی در فضای دیجیتال ایران است و نیازمند ایجاد معیارهای روشن و قابل اجراست.تحلیل رویه قضایی ایران نشان می‌دهد که دیوان عالی کشور نیز در این زمینه با رویکرد مسئولیت نسبی عمل می‌کند. در رأی شماره ۲۳/۱۲/۹۵، دیوان تصریح کرده است که ارائه‌دهندگان خدمات اینترنتی در صورت عدم اقدام به حذف محتوای مجرمانه پس از اطلاع، مسئولیت کیفری و مدنی دارند (دیوان عالی کشور, ۱۳۹۵, ص۲۰). این رویه نزدیک به استانداردهای بین‌المللی است که در دکترین حقوقی نیز پذیرفته شده‌اند با این حال، فقدان سازوکار شفاف برای گزارش‌دهی و رسیدگی به محتوای غیرقانونی، زمان‌بندی نامشخص برای اقدام و عدم تفکیک دقیق مسئولیت میان کاربر و پلتفرم، موجب پیچیدگی بیشتر در اجرای قانون می‌شود. پلتفرم‌ها در چنین شرایطی ممکن است با تأخیر در حذف محتوا یا حتی

برخوردهای سلیقه‌ای مواجه شوند که می‌تواند به تضییع حقوق کاربران منجر شود و اعتماد عمومی به محیط دیجیتال را کاهش دهد.

از منظر بین‌المللی، مقررات GDPR اتحادیه اروپا به وضوح مسئولیت پلتفرم‌ها را در حفاظت از داده‌های شخصی و مدیریت محتوای غیرقانونی مشخص کرده است (Kuner, ۲۰۱۷, p. ۲۲۵). این قانون بر شفافیت، امنیت پردازش اطلاعات و پاسخگویی پلتفرم‌ها تأکید دارد و تخلف از آن، مسئولیت مدنی و جریمه‌های سنگین به همراه دارد. همچنین EU Digital Services Act چارچوبی جامع برای مسئولیت پلتفرم‌ها در مدیریت محتوای آنلاین ارائه می‌دهد، که پلتفرم‌های بزرگ را ملزم می‌کند سیاست‌های حذف محتوا را شفاف اعلام کنند، گزارش‌های دوره‌ای ارائه دهند و سازوکارهای مؤثر برای رسیدگی به شکایات کاربران ایجاد کنند (Bird LLP, ۲۰۲۰, p. ۳). این مقررات به‌ویژه در تطبیق قوانین داخلی با استانداردهای بین‌المللی برای حفاظت از حقوق کاربران اهمیت دارد و می‌تواند الگویی عملی برای بهبود چارچوب قانونی ایران ارائه کند.تحلیل چالش‌ها و خلأهای قانونی نشان می‌دهد که چند عامل اصلی موجب پیچیدگی مسئولیت پلتفرم‌ها می‌شوند. نخست، تعارض میان آزادی بیان کاربران و مسئولیت قانونی پلتفرم‌ها برای حذف محتوای غیرقانونی است، که گاهی تصمیم‌گیری‌های حقوقی و فنی را دشوار می‌کند (Beduschi, ۲۰۱۹, p. ۴). دوم، عدم تعریف دقیق محتوای غیرقانونی در قوانین ایران موجب شده است تا معیارهای مختلف و تفسیرهای متفاوت از سوی مراجع قضایی و پلتفرم‌ها ایجاد شود. سوم، خلأ اجرایی و نبود سازوکارهای نظارتی شفاف، از جمله سامانه‌های رسمی گزارش محتوا و زمان‌بندی مشخص برای رسیدگی، مانع اجرای مؤثر مسئولیت‌ها شده است. چهارم، انگیزه‌های اقتصادی و تجاری پلتفرم‌ها گاهی باعث می‌شود که اقدامات مؤثر برای حذف محتوا با تأخیر انجام شود یا فرآیند پاسخگویی به شکایات کاربران ناکارآمد باشد (Zuboff, ۲۰۱۹, p. ۸۸). این چهار عامل در مجموع، نیاز به اصلاحات قانونی و طراحی سیستماتیک را برجسته می‌کند.در راستای پر کردن این خلأها، چارچوب قانونی پیشنهادی می‌تواند شامل موارد زیر باشد: اول، اعمال مسئولیت نسبی شفاف، به نحوی که مسئولیت میان کاربر و پلتفرم تقسیم شود و پلتفرم تنها در صورت اطلاع از محتوای غیرقانونی و عدم اقدام مناسب، مسئول شناخته شود. دوم، ایجاد سامانه شفاف رسیدگی به شکایات، شامل پورتال‌های رسمی برای گزارش محتوا، زمان‌بندی مشخص برای بررسی و حذف محتوا و امکان پیگیری کاربران. سوم، شفافیت و پاسخگویی دوره‌ای، به‌گونه‌ای که پلتفرم‌ها ملزم باشند گزارش‌های دوره‌ای اقدامات خود را منتشر کنند و اقدامات اصلاحی در صورت قصور قابل پیگیری باشد. چهارم، تطبیق با استانداردهای بین‌المللی، بهره‌گیری از رویه GDPR و EU Digital Services Act برای حفاظت از داده‌ها و حقوق کاربران و همچنین ایجاد هماهنگی میان قوانین داخلی و چارچوب‌های بین‌المللی. این چارچوب، علاوه بر کاهش مسئولیت‌های حقوقی، موجب افزایش اعتماد کاربران و بهبود سلامت فضای مجازی خواهد شد.

بحث و نتیجه گیری

تحلیل و بررسی انجام شده نشان می‌دهد که مسئولیت حقوقی پلتفرم‌های شبکه‌های اجتماعی در انتشار محتوای دیجیتال، موضوعی پیچیده و چندوجهی است که نیازمند تعادل میان حقوق کاربران و مسئولیت ارائه‌دهندگان خدمات می‌باشد. بررسی قوانین داخلی ایران، از جمله قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و اصول قانون اساسی مصوب ۱۳۵۸، مشخص می‌کند که قانون‌گذار تلاش کرده است چارچوبی برای مسئولیت پلتفرم‌ها ایجاد کند، اما خلأهایی همچنان باقی است. این خلأها شامل عدم تعریف دقیق محتوای غیرقانونی، نبود سامانه‌های شفاف برای گزارش و رسیدگی و فقدان

معیارهای مشخص برای زمان‌بندی حذف محتواست. فقدان این معیارها موجب می‌شود که پلتفرم‌ها در مواجهه با محتوای بحث‌برانگیز، تصمیم‌گیری‌های سلیقه‌ای داشته باشند که نه تنها موجب تضییع حقوق کاربران می‌شود، بلکه ریسک حقوقی آن‌ها را نیز افزایش می‌دهد.بررسی رویه قضایی ایران، از جمله رأی شماره ۲۳/۱۲/۹۵ دیوان عالی کشور، نشان می‌دهد که ارائه‌دهندگان خدمات اینترنتی در صورت قصور در حذف محتوای غیرقانونی، مسئولیت مدنی و کیفری دارند این رویه نزدیک به نظریه مسئولیت نسبی است و با اصول بین‌المللی تطابق دارد. مسئولیت نسبی پلتفرم‌ها به این معناست که آن‌ها تنها در صورتی مسئول شناخته می‌شوند که از محتوای غیرقانونی اطلاع داشته باشند و اقدامی مناسب برای حذف آن انجام ندهند. این رویکرد، تعادل میان آزادی کاربران و مسئولیت پلتفرم‌ها را حفظ می‌کند، اما اجرای دقیق و مؤثر آن به دلیل نقص قوانین و ضعف سازوکارهای اجرایی همچنان با چالش مواجه است. نبود سامانه‌های شفاف برای گزارش محتوای غیرقانونی و عدم تعیین زمان‌بندی مشخص برای حذف محتوا از مهم‌ترین مشکلات اجرایی محسوب می‌شود.

مطالعات بین‌المللی نشان می‌دهد که کشورهای اروپایی با تدوین EU Digital Services Act و مقررات GDPR چارچوب‌های شفاف و مشخصی برای مسئولیت پلتفرم‌ها ایجاد کرده‌اند این قوانین شامل الزامات شفافیت، پاسخگویی و تعهدات مشخص برای مدیریت محتوای دیجیتال و حفاظت از داده‌های شخصی کاربران هستند. بر اساس GDPR، پلتفرم‌ها موظف‌اند اطلاعات کاربران را با رعایت شفافیت و امنیت پردازش کنند و در صورت نقض، مسئولیت مدنی و جریمه‌های سنگین متوجه آنان خواهد بود. این استانداردها همچنین چارچوبی برای ایجاد سامانه‌های مؤثر رسیدگی به شکایات کاربران فراهم می‌آورد و می‌تواند به عنوان نمونه‌ای عملی برای اصلاح قوانین ایران مورد استفاده قرار گیرد.تحلیل تطبیقی نشان می‌دهد که قوانین داخلی ایران در مقایسه با استانداردهای بین‌المللی همچنان دارای محدودیت‌هایی است. نخست، فقدان تعریف دقیق محتوای غیرقانونی موجب شده تا معیارهای مختلف و تفسیرهای متفاوت از سوی مراجع قضایی و پلتفرم‌ها ایجاد شود. دوم، نبود سامانه‌های رسمی برای گزارش محتوای غیرقانونی و زمان‌بندی مشخص برای رسیدگی، اجرای مسئولیت‌ها را با مشکل مواجه می‌کند. سوم، انگیزه‌های اقتصادی پلتفرم‌ها ممکن است موجب تأخیر در حذف محتوا یا عدم پاسخگویی مؤثر شود. این چالش‌ها نشان می‌دهد که تنها وجود قانون کافی نیست و نیاز به سازوکارهای عملیاتی و سیاست‌های دقیق برای اجرای مسئولیت‌ها ضروری است.در راستای پاسخ به پرسش‌های اصلی تحقیق، می‌توان دریافت که حدود مسئولیت حقوقی پلتفرم‌ها در ایران بر اساس نظریه مسئولیت نسبی شکل گرفته است؛ به این معنا که پلتفرم‌ها تنها در صورت اطلاع از محتوای غیرقانونی و عدم اقدام مناسب مسئول شناخته می‌شوند. با این حال، فقدان تعریف دقیق محتوا و زمان‌بندی مشخص، اجرای کامل مسئولیت را محدود می‌کند. چالش‌های تطبیق قوانین داخلی با استانداردهای بین‌المللی نیز شامل عدم شفافیت، فقدان سامانه‌های رسمی و تفاوت معیارهای حقوقی است. چارچوب قانونی پیشنهادی، شامل تقسیم مسئولیت نسبی، ایجاد سامانه شفاف برای گزارش و رسیدگی، الزامات شفافیت و پاسخگویی و تطبیق با استانداردهای بین‌المللی، می‌تواند راهکاری جامع برای حفاظت از حقوق کاربران و مسئولیت پلتفرم‌ها فراهم آورد.

اجرای چارچوب پیشنهادی دارای پیامدهای حقوقی و اجتماعی متعددی است. نخست، حقوق کاربران تقویت می‌شود و آن‌ها قادر خواهند بود از حقوق خود برای حذف یا اصلاح محتوای غیرقانونی بهره‌مند شوند و تضمین شفافیت در فرآیند رسیدگی داشته باشند. دوم، پاسخگویی پلتفرم‌ها افزایش می‌یابد؛ الزام به ارائه گزارش‌های دوره‌ای و شفافیت در

سیاست‌ها، مسئولیت پلتفرم‌ها را تقویت می‌کند و زمینه کاهش انتشار محتوای غیرقانونی فراهم می‌شود. سوم، تعارض میان آزادی بیان و مسئولیت قانونی کاهش می‌یابد؛ تعریف دقیق مسئولیت نسبی موجب می‌شود که هم حقوق کاربران حفظ شود و هم پلتفرم‌ها در معرض ریسک‌های غیرضروری قرار نگیرند.

منابع

۱. فارسی

مقالات

حسامی، م. (۱۴۰۲). بررسی مسئولیت مدنی پلتفرم‌های آنلاین در قبال نقض حریم خصوصی کاربران در حقوق ایران. پژوهش‌های حقوقی, ۲۹(۴), ۵۶–۷۳.

علی‌زاده، ف. (۱۴۰۲). چالش‌های حقوقی مسئولیت پلتفرم‌های رسانه‌های اجتماعی در ایران. فصلنامه حقوق فضای مجازی, ۱(۲), ۲۳–۴۵.

اسدپور، میلاد (۱۴۰۳). بررسی ابعاد حقوقی و مدنی مسئولیت پلتفرم‌های آنلاین در قبال خسارات کاربران. ششمین همایش ملی پژوهش‌های حرفه‌ای در روانشناسی و مشاوره با رویکرد از نگاه معلم.

حسام، ابوالفضل (۱۴۰۰). مسئولیت مدنی پلتفرم‌های آنلاین ناشی از نقض حریم خصوصی اطلاعاتی از سوی کاربران؛ مطالعه تطبیقی در ایران، آمریکا و اتحادیه اروپا. پژوهش‌های ارتباطی, دوره ۲۸، شماره ۱۰۷.

رمضانیان سیاهکلرودی، م. (۲۰۲۰). خدمات اینترنتی و مسئولیت مدنی واسطه‌ها در نقض حقوق مالکیت معنوی کاربران. فصلنامه پژوهش‌های حقوقی, ۲۱(۴).

غلامی، س. م. م. (۲۰۲۳). چالش‌های قانون‌گذاری حقوق کاربران در فضای مجازی. مجله حقوقی دانشگاه آزاد اسلامی, ۲۳.

اسناد قانونی

قانون جرایم رایانه‌ای مصوب ۱۳۸۸. (۱۳۸۸). تهران: سازمان چاپ و نشر قوانین.

قانون اساسی جمهوری اسلامی ایران. (۱۳۵۸). تهران: سازمان چاپ و نشر قوانین.

دیوان عالی کشور. (۱۳۹۵). رأی شماره ۲۳/۱۲/۹۵. تهران: مرکز پژوهش‌های حقوقی.

۲. انگلیسی

Books

Floridi, L. (۲۰۱۹). The Ethics of Artificial Intelligence. Oxford: Oxford University Press.

Kuner, C. (۲۰۱۷). The General Data Protection Regulation: A Commentary. Oxford: Oxford University Press.

Zuboff, S. (۲۰۱۹). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Article

Beduschi, A. (۲۰۱۹). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. Big Data & Society, ۶(۲), ۱–۶.

Belk, R., Humayun, M., & Brouard, M. (۲۰۲۲). Money, possessions, and ownership in the Metaverse: NFTs, cryptocurrencies, Web ۳and Wild Markets. Journal of Business Research, ۱۵۳, ۱۹۸–۲۰۵.

Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (۲۰۱۹). Privacy-Preserving Solutions for Blockchain: Review and Challenges. IEEE Access, ۷, ۱۶۴۹۰۸–۱۶۴۹۴۰.

Calo, R. (۲۰۱۶). Robotics and the Lessons of Cyberlaw. California Law Review, ۱۰۳(۳), ۵۱۳–۵۶۳.

Cheong, B. C. (۲۰۲۲). Avatars in the metaverse: potential legal issues and remedies. International Cybersecurity Law Review, ۳(۲), ۴۶۷–.۴۹۴

Dremliuga, R., Dremliuga, O., & Iakovenko, A. (۲۰۲۰). Virtual Reality: General Issues of Legal Regulation. Journal of Politics and Law, ۱۳(۱), ۷۵–۸۱

Hassan, M. (۲۰۲۲). Legal Liability of Social Media Platforms: A Comparative Study between Iran and the EU. Journal of Internet Law, ۲۸(۴), ۵۶–.۷۳

Kumar, R., & Singh, A. (۲۰۲۳). Platform Liability in the Digital Age: Challenges and Legal Frameworks. International Journal of Cyber Law, ۱۵(۲), ۲۳–.۴۵

Zhang, L. (۲۰۲۴). Regulating Online Platforms: A Comparative Analysis of Legal Approaches. Global Internet Policy Review, ۱۰(۱), ۱–.۲۳