شاپا چاپی: ۱۸۴۱-۲۷۸۳
شاپای الکترونیکی: ۱۹۲۲-۲۷۸۳

فصلنامه تمدن حقوقی

تمدن حقوقی

دوره ۸ - شماره ۲۶ - زمستان ۱۴۰۴

تحلیل مسئولیت بانک گشاینده در حقوق اعتبارات اسنادی
همایون مافی، محسن رئیسی
نقش هوش مصنوعی در بهبود فرآیندهای تحقیق کیفری و تحلیل شواهد دیجیتال در نظام حقوقی ایران
امیررضا محمودی، زهرا رهنما
بازخوانی تعهدات قراردادی در شرایط تورم شدید؛ تحلیلی از ظرفیت‌های تعدیل در حقوق ایران
شیما شکوری بلقور، قاسم نبی زاده کبریا
آسیب شناسی سیاست کیفری ایران در قبال جرائم بغی، محاربه و افساد فی‌الارض در پرتو مفهوم امنیت ملی و ثبات سیاسی کشور
روح الله شیخی، محمد محمودی
چهارچوب مسئولیت مدنی ناشی از فعالیت‌های تفریحی پرخطر؛ مطالعه اتاق‌های فرار
رحیم مختاری، غلامحسین کشاورز
دعاوی ناشی از مالکیت فکری در نظام حقوقی ایران
سیدمحمدباقر حقایقی، محمدرضا نصیری، امیرحسن ابوالحسنی
تحلیل جرم‌شناختی جرایم حوزه رمزارزها: مطالعه کلاهبرداری‌های رایج در ایران
حسین محمودی تکانلو، رویا آسیایی
راهبردهای پیشگیرانه از جرم رانت خواری در سیاست کیفری ایران با تاکید بر چالش ها و خلاءهای جرم شناختی
فاضل موحدی، حمیدرضا کناری زاده، داود سلمانپور
واکاوی اصل تناسب میان جرم و مجازات در ساختار دیوان کیفری بین‌المللی
حسن پیرفلک لسکوکلایه، طیبه قدرتی سیاهمزگی
توافق طرفین قرارداد در تعیین ادله اثبات دعوا
حبیب اله عبداله پور، مهدی شجاعی
عملکرد دادگاه‌های کیفری در پیشگیری از جرم: با نگاهی به جرم‌شناسی انتقادی و تمرکز بر نظام قضایی ایران
ایرج مروتی، نغمه فرهود
مسئولیت دولت‌ها در قبال تروریسم بین‌المللی و دیپلماسی ضدتروریسم
مسعود سرفرازی صالح، مهدی قره داغی
پایان حکمرانی متمرکز: تحلیل ظهور حکمرانی غیرمتمرکز در عصر بلاکچین و قراردادهای هوشمند
هادی زارع، مجید وزیری
تحلیل تطبیقی حمایت‌های جبرانی تأمین اجتماعی در قبال خسارت بدنی و دامنه شمول زیان‌دیدگان در ایران و انگلستان
زینب تاری
انتقال دعاوی در نظام حقوقی ایران با تأکید بر مقررات و ماده‌های منتخب قانون ثبت اسناد و املاک
امیررضا علی تبار
جایگاه هوش مصنوعی در پهنه سیاستگذاری جنایی
محبوبه طالبی رستمی
تعهد به ایمن‌سازی داده‌ها به‌عنوان تعهد به نتیجه یا تعهد به وسیله در حقوق خصوصی
سیدامیرحسن مصطفوی
مسئولیت کیفری شرکت‌های فناوری در قبال جرائم ارتکابی کاربران
وحید کیومرثی
مسئولیت مدنی ناشی از پردازش خودکار داده های شخصی توسط هوش مصنوعی در حقوق ایران و افغانستان (با نگاهی به اسناد بین المللی)
راضیه جعفرزاده، وحید حمیدی، محمدرضا رشید
بررسی تأثیر آگاهی حقوقی و شفافیت در پیشگیری و کاهش فساد اداری و مالی
سیده مهشید میری بالاجورشری
مالکیت داده های شخصی در حقوق خصوصی؛ از حق شخصیت تا مال غیرمادی
سینا یوسفی
مسئولیت مدنی پزشک و سازنده ربات در جراحی‌های رباتیک نظام های حقوقی ایران و انگلستان
ابراهیم شیروانی
تحلیلی بر مسئله أخذ خسارت تأخیر تادیه از محکوم به دولتی
محمدمهدی رضوانی فر، زهرا سلیمی
آثار حقوقی و اداری تملک بر وضعیت ثبتی املاک در نظام حقوقی ایران
احسانه وثوقی منفرد، محمد وارسته بازقلعه
دیپلماسی اقتصادی و حقوق قراردادهای بین‌المللی خصوصی؛ تعامل سیاست و حقوق در تأمین منافع ملی
رادمهر رحمانی گل افشان
پذیرش تشخیص تقلب مبتنی بر هوش مصنوعی در بانکداری: نقش اعتماد، شفافیت و ادراک انصاف در موسسات مالی در ایران، امارات متحده عربی و قطر
عبدالمجید یوسفی
جرم‌شناسی جنگ در واقعیت‌های کنونی و لزوم توسعه آن در اوکراین
یاسر شاکری

Legal Civilization
Vol. 8, No. 26, Winter 2026
Pages: 413-444
Article Type: Original Research
https://www.pzhfars.ir/article_238747.html
doi: 10.22034/lc.2026.560935.1715

تمدن حقوقی
دوره ۸، شماره ۲۶، زمستان ۱۴۰۴
صفحات: ۴۴۴-۴۱۳
نوع مقاله: پژوهشی

Criminal Liability of Technology Companies for Crimes Committed by Users

Vahid Kioumarsi
PhD researcher in criminal law and criminology, Faculty of Humanities, lecturer at Islamic Azad University, Central Tehran Branch, Tehran, Iran

Abstract

Criminal liability of technology companies for crimes committed by users is one of the complex and emerging issues in criminal law that has gained increasing importance with the expansion of the digital space and the increase in the use of online platforms. These companies, as service providers, can play an effective role in facilitating or preventing the commission of crimes. The main question of the research is under what conditions and to what extent can technology companies be held criminally liable. This research was conducted with a descriptive-analytical approach and based on the study of scientific and library resources, and by examining existing legal theories and legal frameworks, an attempt has been made to extract the criteria for realizing the criminal liability of technology companies. The findings show that the realization of the criminal liability of technology companies depends on the existence of a causal relationship between the company's performance and the crime, the company's awareness or fault, and the possibility of preventing or controlling the crime by it. Also, the role of companies in committing user crimes can range from indirect cooperation to direct participation. The results of the study indicate that in order to ensure criminal justice and effectively prevent cybercrime, it is essential to update and clarify legal frameworks and judicial procedures so that the criminal liability of technology companies can be determined more accurately, fairly, and efficiently.

Keywords: Criminal Liability, Technology Companies, Cybercrime, User Crimes, Digital Space.

Received: 2025/12/29 - Review: 2026/02/12 - Accepted: 2026/03/14

مسئولیت کیفری شرکت‌های فناوری در قبال جرائم ارتکابی کاربران

وحید کیومرثی
پژوهشگر دکتری حقوق جزا و جرم‌شناسی، دانشکده علوم انسانی، مدرس دانشگاه آزاد اسلامی، واحد تهران مرکزی، تهران، ایران
vahidkiomarsi@yahoo.com
http://orcid.org/0009-0006-7951-2990

چکیده

مسئولیت کیفری شرکت‌های فناوری در قبال جرایم ارتکابی کاربران یکی از مسائل پیچیده و نوظهور در حقوق کیفری است که با گسترش فضای دیجیتال و افزایش استفاده از پلتفرم‌های آنلاین، اهمیت فزاینده‌ای یافته است. این شرکت‌ها به‌عنوان بسترهای ارائه‌دهنده خدمات، می‌توانند نقش مؤثری در تسهیل یا جلوگیری از ارتکاب جرایم ایفاء کنند. پرسش اصلی پژوهش این است که تحت چه شرایطی و تا چه میزان می‌توان شرکت‌های فناوری را از منظر کیفری مسئول دانست؟ این پژوهش با رویکردی توصیفی-تحلیلی و بر پایه مطالعه منابع علمی و کتابخانه‌ای انجام شده و با بررسی نظریه‌های حقوقی و چهارچوب‌های قانونی موجود، تلاش شده است معیارهای تحقق مسئولیت کیفری شرکت‌های فناوری استخراج گردد. یافته‌ها نشان می‌دهند تحقق مسئولیت کیفری شرکت‌های فناوری منوط به وجود رابطه علیت میان عملکرد شرکت و جرم، احراز آگاهی یا تقصیر شرکت و امکان پیشگیری یا کنترل جرم توسط آن است. همچنین، نقش شرکت‌ها در ارتکاب جرایم کاربران می‌تواند طیفی از همکاری غیرمستقیم تا مشارکت مستقیم را شامل شود. نتایج پژوهش بیانگر آن است که برای تضمین عدالت کیفری و پیشگیری مؤثر از جرایم فضای مجازی، ضروری است چهارچوب‌های قانونی و رویه‌های قضایی به‌روز و شفاف شوند تا احراز مسئولیت کیفری شرکت‌های فناوری با دقت، انصاف و کارآمدی بیشتری صورت گیرد.

واژگان کلیدی: مسئولیت کیفری، شرکت‌های فناوری، جرایم فضای مجازی، جرایم کاربران، فضای دیجیتال.

دریافت مقاله: ۱۴۰۴/۱۰/۰۸ – بازنگری مقاله: ۱۴۰۴/۱۱/۲۳ – پذیرش مقاله: ۱۴۰۴/۱۲/۲۳

ارجاع:
کیومرثی، وحید؛ (۱۴۰۴)، مسئولیت کیفری شرکت‌های فناوری در قبال جرائم ارتکابی کاربران، تمدن حقوقی، شماره ۲۶.

مقدمه

با پیشرفت روزافزون فناوری اطلاعات و ارتباطات، شرکت‌های فناوری به عوامل کلیدی در فضای دیجیتال تبدیل شده‌اند که خدمات متنوعی از جمله پلتفرم‌های ارتباطی، تجارت الکترونیک، شبکه‌های اجتماعی و فضای ذخیره‌سازی داده‌ها را به کاربران ارائه می‌دهند. این گسترش سریع و فراگیر، در کنار مزایای بی‌شمار، مسائل و چالش‌های حقوقی جدیدی را نیز به وجود آورده است که یکی از مهم‌ترین آن‌ها مسئله مسئولیت کیفری شرکت‌های فناوری در قبال جرایم ارتکابی کاربران است. شرکت‌ها به‌عنوان بستری برای فعالیت‌های کاربران، ممکن است نقش‌های متفاوتی در ارتکاب جرم ایفاء کنند؛ از مشارکت مستقیم گرفته تا همکاری غیرمستقیم یا حتی بی‌توجهی به وقوع جرایم. این امر موجب پیچیدگی در تعیین حدود مسئولیت کیفری آن‌ها شده و ضرورت بررسی دقیق حقوقی آن را دوچندان کرده است.

در این راستا، پرسش‌های کلیدی این پژوهش عبارت‌اند از: مسئولیت کیفری شرکت‌های فناوری تحت چه شرایطی محقق می‌شود؟ چه ارکانی برای احراز این مسئولیت لازم است؟ انواع نقش‌هایی که شرکت‌ها ممکن است در جرایم کاربران داشته باشند کدام‌اند؟ و معیارهای قانونی و عملی برای تعیین و اثبات مسئولیت کیفری این شرکت‌ها چیست؟ پاسخ به این پرسش‌ها به فهم بهتر جایگاه

حقوقی شرکت‌های فناوری در نظام کیفری و ارائه راهکارهای قانونی برای پیشگیری و مقابله با جرایم سایبری کمک خواهد کرد. هدف این پژوهش، تحلیل و بررسی ارکان تحقق مسئولیت کیفری شرکت‌های فناوری، تبیین انواع نقش‌های ممکن این شرکت‌ها در جرایم کاربران وشناسایی حدود و معیارهای احراز مسئولیت کیفری آنان است. با توجه به اهمیت موضوع و کمبود پژوهش‌های جامع در این حوزه، این مطالعه سعی دارد چهارچوبی نظری و کاربردی ارائه دهد که هم برای قانون‌گذاران و مراجع قضایی مفید باشد و هم راهنمایی برای شرکت‌های فناوری در جهت مسئولیت‌پذیری و رعایت قوانین باشد.

مسئولیت کیفری شرکت‌های فناوری در قبال جرایم کاربران، موضوعی چندوجهی و پیچیده است که نیازمند تعادل میان حمایت از حقوق کاربران، آزادی فعالیت‌های فناوری و جلوگیری از سوءاستفاده‌های احتمالی است. بنابراین، به‌روزرسانی قوانین و تقویت همکاری میان نهادهای قضایی، انتظامی و فناوری از جمله ضرورت‌های اساسی برای تحقق عدالت کیفری در این حوزه به شمار می‌آید.

۱- مبانی نظری و مفهومی

مبانی نظری و مفهومی به‌عنوان زیربنای هر پژوهش علمی، نقش مهمی در درک صحیح و عمیق موضوع تحقیق ایفاء می‌کند. در این مبحث با ارائه تعاریف دقیق مفاهیم کلیدی و بررسی نظریه‌ها و چهارچوب‌های علمی مرتبط، زمینه لازم برای تحلیل‌های بعدی را فراهم می‌آوریم. بررسی مبانی نظری و مفهومی، امکان شناخت دقیق‌تر موضوع وشناسایی ابعاد مختلف آن را میسر می‌سازد.

۱-۱- مفهوم مسئولیت کیفری

مسئولیت کیفری یکی از بنیادی‌ترین مفاهیم در نظام حقوق کیفری است که به معنای الزام قانونی فرد یا شخصیت حقوقی به پاسخ گویی و تحمل مجازات به‌خاطر ارتکاب فعل مجرمانه است. به عبارت دیگر، مسئولیت کیفری عبارت است از التزام و تعهد شخص به تحمل نتایج زیانبار ناشی

از ارتکاب جرم، به‌گونه‌ای که قانون برای آن مجازات یا اقدامات تأمینی و تربیتی پیش‌بینی کرده است (اردبیلی، ۱۴۰۴، ۲۸۵).

این مفهوم بر مبنای اصول اساسی حقوق کیفری مانند اصل قانونی بودن جرم و مجازات، اصل شخصی بودن مسئولیت و اصل تساوی افراد در برابر قانون شکل گرفته است. در حقوق ایران، مسئولیت کیفریبه‌طور مشخص در قانون مجازات اسلامی مصوب ۱۳۹۲ و قوانین خاص دیگر تعریف و مقررات مربوط به آن تنظیم شده است. بر اساس ماده ۱۴۰ قانون مجازات اسلامی مصوب ۱۳۹۲، مسئولیت کیفری تنها شامل افرادی می‌شود که عاقل، بالغ و مختار باشد؛ به این معنی که افراد زیر سن بلوغ یا کسانی که فاقد توانایی درک و قصد هستند، مسئولیت کیفری ندارند یا مسئولیت آن‌ها متفاوت است. همچنین، در حقوق ایران مسئولیت کیفری شخصی است و هیچ فرد یا شخصیت حقوقی بدون ارتکاب فعل مجرمانه و رعایت شرایط قانونی مسئول شناخته نمی‌شود.

ارکان مسئولیت کیفری در حقوق ایران شامل سه عنصر اصلی است: فعل مجرمانه[۱]؛ ۲) تقصیر[۲]؛ و ارتباط سببیتی میان فعل و نتیجه جرم. بدون وجود هریک از این ارکان، مسئولیت کیفری قابل احراز نیست. همچنین، وجود برخی شرایط مانند فورس ماژور یا اضطرار می‌تواند مسئولیت کیفری را از بین ببرد یا تخفیف دهد (اردبیلی، ۱۴۰۴، ۹۹). مسئولیت کیفری در ایران محدود به اشخاص حقیقی نیست و در موارد خاصی، شخصیت‌های حقوقی از جمله شرکت‌ها نیز می‌توانند تحت شرایط مشخصی مسئول شناخته شوند، هرچند این مسئله هنوز در نظام حقوقی ایرانبه‌طور کامل جا نیفتاده و در حال تحول است. در نهایت، مسئولیت کیفری در حقوق ایران همواره با رعایت اصول حقوق بشر، تضمین حق دفاع متهم و وجود دادرسی عادلانه همراه است تا عدالت کیفری به درستی برقرار شود.

۱- که می‌تواند فعل یا ترک فعل باشد

۲- اعم از عمد یا شبه‌عمد

۱-۲- شرکت‌های فناوری و جایگاه حقوقی آن‌ها

شرکت‌های فناوری، به‌عنوان عوامل محوری در عرصه اقتصاد دیجیتال و جامعه اطلاعاتی، جایگاهی بی‌بدیل در تحولات نوین ارتباطی، اقتصادی، اجتماعی و حقوقی یافته‌اند. این شرکت‌ها با تکیه بر نوآوری، داده‌محوری و ارائه خدمات فناورانه چون پلتفرم‌های شبکه‌های اجتماعی، سامانه‌های خدمات‌رسانی دیجیتال، ذخیره‌سازی ابری، هوش مصنوعی و بلاکچین نقش فزاینده‌ای در مدیریت داده‌ها، تبادل اطلاعات و حتی شکل‌دهی به رفتار کاربران ایفاء می‌کنند. ازاین رو تأمل در جایگاه حقوقی آن‌ها، ضرورتی اجتناب‌ناپذیر در دنیای معاصر تلقی می‌شود.

اقسام شرکت‌های فناوری معمولاً به چند دسته کلی تقسیم می‌شوند که بر اساس مرحله رشد، نوع فعالیت و میزان بلوغ فناوری تأیید می‌شوند. طبق آیین‌نامه‌ها و دسته بندی‌های رایج در ایران، شرکت‌های فناوری به سه دسته اصلی زیر تقسیم می‌شوند: اول- شرکت‌های فناوری نوپا[3]: در مراحل ابتدایی فعالیت هستند، معمولاً ایده محورند و هنوز به بلوغ کامل نرسیده‌اند، نیازمند حمایت مالی بیشتر هستند. فروش سالانه معمولاً کمتر از پنج میلیارد تومان است. سهم نیروی انسانی در تحقیق و توسعه حداقل بیست درصد است. دوم- شرکت‌های فناوری نوآور: از مرحله نوپایی عبور کرده و به دنبال توسعه و گسترش فعالیت‌ها هستند. فروش سالانه بین پنج تا پنجاه میلیارد تومان دارد و حداقل سی درصد از فروش باید محصول یا خدمت دانش‌بنیان باشد. سوم- شرکت‌های فناوری فناور: شرکت‌های بالغ و پیشرو در بازار فناوری، فروش سالانه بیش از پنجاه میلیارد تومان و حداقل پنجاه درصد از فروش محصولات دانش‌بنیان است (ذبیحی‌جامخانه و همکاران، ۱۳۹۷، ۱۲۰).

شخصیت حقوقی نهادهای اقتصادی همچون شرکت‌ها، به‌عنوان موجودیتی مستقل از اعضای حقیقی تلقی می‌شود که دارای حق و تکلیف مستقل بوده و می‌تواند طرف قرارداد یا دعوا قرار گیرد. شرکت‌های فناوری نیز از این قاعده مستثنی نبوده و به‌موجب قوانین بازرگانی و ثبتی دارای شخصیت حقوقی مستقل‌اند. بااین‌حال، ویژگی‌های منحصربه‌فرد این شرکت‌ها در حوزه فضای سایبری، سبب

3- Startup

ایجاد چالش‌های نوین درشناسایی حدود مسئولیت، نحوه اعمال صلاحیت قضایی و تنظیم رابطه آن‌ها با دولت‌ها، کاربران و سایر بازیگران شده است. یکی از برجسته‌ترین ابعاد جایگاه حقوقی شرکت‌های فناوری، مسئولیت آن‌ها در قبال محتوای تولید یا تبادل شده توسط کاربران است. برخلاف شرکت‌های سنتی که عمدتاً در محدوده فعالیت‌های قراردادی یا فیزیکی پاسخگو هستند، شرکت‌های فناوری به‌واسطه میزبانی، ذخیره‌سازی یا انتشار اطلاعات دیجیتال، گاه به‌عنوان تسهیل‌گر، واسطه یا حتی شریک در رفتارهای ناقض قانون تلقی می‌شوند. این موضوع در جرایمی چون نشر محتوای غیرقانونی، افشای اطلاعات خصوصی، اخاذی دیجیتال و سوءاستفاده از داده‌ها نمود بیشتری می‌یابد و سبب می‌شود ضرورت تعیین دقیق حدود مسئولیت آن‌ها، از منظر تقنینی و قضایی برجسته گردد (السان، ۱۴۰۲، ۱۴).

در نظام‌های حقوقی مختلف، رویکردها نسبت به تنظیم جایگاه حقوقی شرکت‌های فناوری متنوع است. برخی نظام‌ها مانند اتحادیه اروپا، با مقرراتی چون «مقررات عمومی حفاظت از داده‌ها»[۴]، الزاماتی دقیق درباره نحوه پردازش داده‌ها، رضایت کاربران و پاسخگویی شرکت‌ها پیش‌بینی کرده‌اند. در مقابل، برخی نظام‌ها هنوز در حال گذار و تطبیق با الزامات حقوقی عصر دیجیتال هستند و چهارچوب‌های حقوقی موجود، پاسخگوی پیچیدگی‌های عملکردی این شرکت‌ها نیست (Solove,2010,62).

در حقوق ایران نیز، شرکت‌های فناوری از منظر حقوق شرکت‌ها، تابع قواعد کلی تجارت‌اند، اما در زمینه مسئولیت‌های ویژه ناشی از فعالیت در بستر دیجیتال، خلأهای قانون‌گذاری مشهود است.

4- General Data Protection Regulation (GDPR)

مقررات عمومی حفاظت از داده‌ها یا مقررات عمومی حفاظت از داده‌های شخصی گفته می‌شود. این مقررات در سال ۲۰۱۶ میلادی توسط اتحادیه اروپا تصویب شد و از بیست و پنجم مه ۲۰۱۸ میلادی به اجرا درآمد. هدف اصلی محافظت از داده‌های شخصی افراد داخل اتحادیه اروپا است و همچنین به افراد این حق را می‌دهد که درباره چگونگی جمع‌آوری، ذخیره و پردازش اطلاعات‌شان تصمیم‌گیری کنند. این قانون تأثیر گسترده‌ای بر شرکت‌های فناوری، به‌ویژه در زمینه مسئولیت‌ها و پاسخگویی آن‌ها در قبال کاربران، داشته است

اگرچه قوانینی چون قانون تجارت الکترونیکی مصوب ۱۳۸۲، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و آیین‌نامه‌های مرتبط به‌نوعی درصدد تنظیم رفتارهای این نهادها برآمده‌اند، اما گستردگی فعالیت و نقش‌آفرینی فناوری‌های نوظهور، فراتر از ظرفیت‌های فعلی نظام حقوقی کشور است. این امر لزوم تدوین مقررات خاص، ایجاد نهادهای نظارتی فناورمحور و تبیین اصول شفاف مسئولیت کیفری، مدنی و اداری برای شرکت‌های فناوری را بیش از پیش آشکار می‌سازد (میری، ۱۳۹۴، ۱۲۱).

شرکت‌های فناوری در دوران معاصر، از جایگاه حقوقی خاص و پیچیده‌ای برخوردارند که نیازمند بازتعریف مستمر با توجه به تحولات فناورانه، الزامات حقوق بشر دیجیتال، حاکمیت داده و صیانت از حقوق کاربران است. این شرکت‌ها نه‌تنها به‌عنوان بنگاه‌های اقتصادی، بلکه به‌عنوان نهادهای تأثیرگذار اجتماعی و فرهنگی، مسئولیتی فراتر از منطق صرفاً تجاری بر عهده دارند و این مسئولیت، مستلزم توسعه تدریجی و هوشمندانه‌ی نظام‌های حقوقی ملی و فراملی است.

۱-۳- جرایم کاربران در بستر فناوری

جرایم کاربران در بستر فناوری جلوه‌ای نوین از رفتارهای مجرمانه است که در ساختارهای سنتی حقوق کیفری جای نمی‌گیرند و ماهیتی فراملی، پیچیده و گاه ناشناس دارند. این دسته از جرایم در فضای دیجیتال و از طریق ابزارها و بسترهای فناورانه، نظیر اینترنت، شبکه‌های اجتماعی، پلتفرم‌های ارتباطی و زیرساخت‌های ابری واقع می‌شوند و با توجه به ظرفیت گسترش‌پذیر این فضا، امکان ارتکاب آن‌ها در هر زمان و مکان، بدون نیاز به حضور فیزیکی مرتکب در محل جرم، فراهم است. جرایم یادشده از حیث ماهوی دارای طیف وسیعی‌اند؛ از جرایم علیه داده و سامانه‌های اطلاعاتی نظیر دسترسی غیرمجاز، شنود غیرقانونی، اخلال در داده یا سامانه، تا جرایم مبتنی‌بر محتوا مانند نشر اکاذیب، توهین، تهدید، اشاعه محتوای مستهجن، یا تحریک به خشونت. این دسته از جرایم می‌توانند همچنین اشکال سنتی جرم مانند کلاهبرداری، اخاذی یا جعل را با استفاده از فناوری‌های نو بازتولید کرده و موجب بروز تهدیدات نوظهور شوند.

عنصر اساسی در این جرایم، بهره‌گیری از فناوری اطلاعات و ارتباطات به‌عنوان ابزار یا بستر وقوع رفتار مجرمانه است. تمایز این جرایم از سایر جرایم سنتی، نه صرفاً در شیوه ارتکاب بلکه در چالش‌هایی است که در فرآیندشناسایی، اثبات، انتساب و تعقیب کیفری آن‌ها مطرح می‌شود. برای نمونه، استفاده از رمزنگاری، بسترهای ناشناس‌ساز و زیرساخت‌های توزیع‌شده می‌تواند موجب اختلال در مسیر ردیابی فنی مجرم شود. افزون بر این، پلتفرم‌های دیجیتال نقش واسطه‌ای ایفاء می‌کنند که می‌تواند درعین‌حال بستر وقوع جرم بوده یا در تحقق آن سهیم باشند، بی‌آن که مستقیماً فاعل جرم شناخته شوند. چنین جرایمی در نظام حقوق کیفری ایران ذیل عنوان کلی «جرایم رایانه‌ای» یا «جرایم سایبری»شناسایی شده‌اند و قانون‌گذار در قانون جرایم رایانه‌ای مصوب ۱۳۸۸، انواعی از این جرایم را به تفکیک تبیین نموده است. بااین‌حال، تحول سریع فناوری و پیدایش شکل‌های جدیدی از بزهکاری دیجیتال ایجاب می‌کند که سیاست جنایی کشور در راستای چابکی، همسویی با تحولات بین‌المللی و ارتقای توان پاسخ‌دهی نهادهای کیفری بازنگری و روزآمد گردد (عزیزی، ۱۳۹۸، ۹۰).

۲- ارکان، انواع نقش‌ها و معیارهای احراز مسئولیت شرکت

احراز مسئولیت شرکت در قبال جرایم ارتکابی کاربران، از جمله مباحث کلیدی و نوپدید در حقوق کیفری فناوری اطلاعات است که به بررسی حدود و شرایطی می‌پردازد که در آن شرکت‌های ارائه‌دهنده خدمات فناورانه[۵] ممکن است مسئولیت کیفری پیدا کنند. این مبحث با تکیه بر مفاهیم کلاسیک مسئولیت کیفری و تطبیق آن‌ها با ساختارهای نوین شرکتی، به دنبال تبیین مبانی و ارکان قانونی و فنی انتساب جرم به اشخاص حقوقی است و می‌کوشد نقش‌هایی چون مباشرت، معاونت، یا تسهیلگری شرکت‌ها در ارتکاب بزه از سوی کاربران را تحلیل کند. همچنین، معیارهایی مانند آگاهی، نظارت، سیاست‌های کنترلی و اقدامات پیشگیرانه شرکت‌ها در تعیین حدود مسئولیت آن‌ها اهمیت اساسی دارند. پرداختن به این مبحث، گامی ضروری برای فهم بهتر نظام مسئولیت کیفری در

۵- نظیر پلتفرم‌های دیجیتال، شبکه‌های اجتماعی و شرکت‌های میزبان داده

دوران دیجیتال و تدوین سیاست جنایی کارآمد و پاسخگو در مواجهه با بزهکاری فناورانه است.

۲-۱- ارکان تحقق مسئولیت کیفری شرکت‌ها

برای تحقق مسئولیت کیفری شرکت‌های فناوری در قبال جرایم ارتکابی کاربران، باید ارکان سه‌گانه‌ای که اساس مسئولیت کیفری را تشکیل می‌دهند،به‌طور دقیق در بستر حقوق کیفری اشخاص حقوقی و با لحاظ ویژگی‌های خاص شرکت‌های فناوری مورد تحلیل قرار گیرد. این ارکان شامل عنصر قانونی، عنصر مادی و عنصر روانی[۶] هستند. هریک از این ارکان باید با توجه به ساختار خاص فعالیت‌های فناورانه و نقش واسطه‌ای یا فعال شرکت‌های فناوری در وقوع جرم کاربران بررسی شوند.

عنصر قانونی در مسئولیت کیفری شرکت‌های فناوری، به معنای وجود یک حکم صریح قانونی است که ارتکاب یک رفتار خاص را جرم‌انگاری کرده و دایره مسئولیت را نیز نسبت به اشخاص حقوقی[۷] تسری داده باشد. در نظام حقوقی ایران، این امر در ماده ۱۴۳ قانون مجازات اسلامی مصوب ۱۳۹۲ تصریح شده که مقرر می‌دارد «در جرایم عمدی، شخص حقوقی زمانی مسئول است که جرم به نام، یا در راستای منافع آن ارتکاب یابد و دارای شرایط مقرر در قانون باشد». بنابراین، وجود یک قاعده قانونی که جرم‌انگاری مشخصی انجام داده باشد و تصریح کند که این جرم در صورت ارتکاب توسط اشخاص حقوقی یا در بستر فعالیت‌های آن‌ها نیز قابل انتساب است، شرط اول تحقق مسئولیت است. بدون چنین حکم صریحی، استناد به مسئولیت کیفری شرکت نه‌تنها از نظر اصول قانونی‌بودن جرم و مجازات مردود است، بلکه خلاف اصول دادرسی کیفری نیز خواهد بود (عالی پور، ۱۴۰۰، ۲۱۱).

عنصر مادی مسئولیت کیفری شرکت‌های فناوری، پیچیده‌تر از عنصر مادی در جرایم سنتی است. در این جا رفتار مجرمانه مستقیماً توسط شرکت انجام نمی‌شود، بلکه شرکت بستر، ابزار یا محیطی را

۶- معنوی

۷- از جمله شرکت‌های فناوری

در اختیار کاربران قرار می‌دهد که در آن بستر، رفتار مجرمانه از سوی کاربر واقع می‌شود. بنابراین، باید بررسی شود که آیا شرکت در فراهم‌کردن ابزار یا بستری که منجر به وقوع جرم شده، نقش مؤثری ایفاء کرده و آیا این نقش به گونه‌ای بوده که عرفاً یا قانوناً به‌عنوان مشارکت، معاونت یا تقصیر قابل انتساب به شرکت باشد؟ برای مثال، اگر پلتفرمی مانند شبکه اجتماعی یا سایت اشتراک فایل، به‌رغم دریافت گزارش‌های مکرر از انتشار محتوای مجرمانه، بدون اتخاذ تدابیر مؤثر مانند حذف محتوا، اخطار به کاربر یا انسداد دسترسی وی، به فعالیت خود ادامه دهد، عنصر مادی در قالب ترک فعل معنادار و مؤثر تحقق می‌یابد. این نقش ممکن است به‌صورت فعل مثبت[۸] یا ترک فعل[۹] ظاهر شود. در برخی موارد نیز نقش شرکت در سطح بالاتری از «آمادگی بستر وقوع جرم» قرار می‌گیرد، مانند وقتی که الگوریتم‌های توصیه‌گر شرکت عامدانه یا با غفلت شدید، محتوای مجرمانه یا تحریک‌آمیز را در اولویت قرار می‌دهند که این می‌تواند مصداق رفتار مادی فعال تلقی شود.

عنصر روانی که به قصد، علم و سوءنیت شرکت مربوط است، در مورد اشخاص حقوقی مسئله‌برانگیزتر است، زیرا شخص حقوقی فاقد ذهن، اراده و شعور انسانی به معنای سنتی آن است. بنابراین، باید دید چگونه می‌توان قصد یا علم را به شرکت نسبت داد (شریفی، ۱۳۹۶، ۱۴۱).

رویه‌های حقوقی بین‌المللی و همچنین تفاسیر فقهی و دکترین حقوقی داخلی معمولاً عنصر روانی شرکت را از طریق اراده مدیران، نمایندگان، یا افراد صاحب اختیار آن احراز می‌کنند. چنان چه تصمیمات مدیریتی، سیاست‌های داخلی یا عملکرد سازمانی شرکت به نحوی باشد که آگاهانه یا بر اثر سهل‌انگاری سنگین، امکان وقوع جرم را برای کاربران فراهم کند، می‌توان علم و سوءنیت را منتسب دانست. همچنین، تکرار رویه‌های بی‌مبالات در مدیریت محتوای کاربر یا بی‌تفاوتی آشکار نسبت به مخاطرات، قرینه‌ای قوی بر وجود سوءنیت سازمانی است. برای مثال، اگر شرکتی عمداً سیاستی اتخاذ کند که در آن، گزارش‌های مربوط به محتوای غیرقانونی نادیده گرفته شود تا آمار

۸- تسهیل بارگذاری محتوای مجرمانه با آگاهی قبلی

۹- عدم حذف یا هشدار پس از اطلاع از جرم

کاربران فعال کاهش نیابد، این تصمیم مدیریتی، عنصر روانی سازمان را شکل می‌دهد. در مقابل، اگر شرکت دارای پروتکل‌ها و سامانه‌های پیشگیری و نظارت باشد، ولی با وجود این تلاش‌ها، کاربر مرتکب جرم شود، عنصر روانی به دشواری قابل اثبات است.

تحقق مسئولیت کیفری شرکت‌های فناوری مستلزم آن است که رفتار کاربر نهبه‌طور کامل مستقل، بلکه با نوعی نقش فعال یا منفعل اما معنادار شرکت همراه باشد؛ این نقش باید بر پایه قانونی جرم‌انگاری شده باشد و همچنین قابل استناد به اراده، علم یا تقصیر قابل انتساب به بدنه مدیریتی شرکت باشد. در غیاب هریک از این عناصر، انتساب کیفری با اصل شخصی بودن مسئولیت کیفری در تعارض خواهد بود (شریفی، ۱۳۹۴، ۱۵۰).

۲-۲- انواع نقش‌های ممکن شرکت در جرم کاربران

نقش شرکت‌های فناوری در ارتکاب جرایم توسط کاربران، بر اساس اصول دقیق حقوق کیفری، به اشکال متعددی قابل تحلیل است. این نقش‌ها باید به گونه‌ای باشند که بتوان آن‌ها را در قالب یکی از صور مشارکت یا معاونت در جرم، یا در برخی موارد نادر، ارتکاب مستقیم جرم توسط شخص حقوقی، تحلیل کرد. آن چه اهمیت دارد، کیفیت ارتباط میان شرکت و رفتار مجرمانه کاربر است؛ این ارتباط باید از حد تصادف و بی‌ربطی فراتر رود و به درجه‌ای از دخالت، آگاهی، یا غفلت برسد که مسئولیت کیفری را توجیه کند.

یکی از صورت‌های بارز نقش شرکت در جرم کاربر، فراهم‌سازی ابزار یا بستر فنی وقوع جرم است. در این حالت، شرکت با طراحی پلتفرم یا سامانه‌ای که به لحاظ ساختاری یا تنظیمات پیش‌فرض، امکان ارتکاب جرم را برای کاربران تسهیل می‌کند، نقشی مؤثر در بروز جرم ایفاء می‌نماید. نمونه‌ی رایج آن، شبکه‌های اجتماعی یا سرویس‌های اشتراک فایل هستند که فاقد سیستم‌های فیلترینگ، احراز هویت یا مدیریت محتوا هستند و این فقدان به نحوی است که وقوع جرایم خاصی مانند انتشار محتوای مستهجن، افتراء، یا تحریک به خشونت را تسهیل می‌کند. در این

جا، شرکت از لحاظ حقوقی در موقعیتی قرار می‌گیرد که دست‌کم می‌توان از آن به‌عنوان معاونت در جرم از طریق تسهیلگری فنی یاد کرد، مشروط بر آن که آگاهی یا احتمال آگاهی شرکت از این کارکرد مخرب سامانه قابل اثبات باشد (شریفی، ۱۳۹۴، ۱۳۲).

در برخی موارد، نقش شرکت از صرف تسهیلگری فراتر رفته و به تشویق یا تحریک غیرمستقیم کاربران به ارتکاب جرم منجر می‌شود. این وضعیت زمانی رخ می‌دهد که الگوریتم‌ها یا سیاست‌های داخلی شرکت به گونه‌ای طراحی شده‌اند که آگاهانه محتوای مجرمانه، نفرت‌افکن یا تحریک‌آمیز را ترویج می‌دهند، چرا که چنین محتواهایی معمولاً باعث افزایش تعامل کاربران و سود اقتصادی شرکت می‌شوند. در این حالت، شرکت با علم به نتایج احتمالی اقدامات خود، ساختاری ایجاد کرده است که گرایش کاربران به سمت رفتار مجرمانه را تقویت می‌کند. اگر بتوان رابطه مستقیمی میان عملکرد الگوریتم و گسترش جرم اثبات کرد، می‌توان گفت شرکت در چهارچوب نظریه «علت مقدم» یا حتی در سطح معاونت تحریک‌آمیز، مسئولیت کیفری دارد.

در وضعیتی دیگر، شرکت ممکن است نقش منفعل اما مقصرانه در قالب ترک فعل مؤثر ایفاء کند. این حالت به‌ویژه زمانی صادق است که شرکت از وقوع یا احتمال قریب‌الوقوع وقوع جرم توسط کاربران آگاه بوده، اما با وجود قدرت و اختیار، از انجام اقدامات پیشگیرانه مانند مسدودسازی محتوا، گزارش به مراجع ذیصلاح، یا تعلیق حساب کاربری خودداری می‌کند. در حقوق کیفری، ترک فعل تنها در صورتی منجر به مسئولیت کیفری می‌شود که مرتکب دارای «وظیفه قانونی یا قراردادی» برای اقدام باشد. در مورد شرکت‌های فناوری، این وظیفه ممکن است ناشی از مقررات ناظر بر پلتفرم‌های برخط، شرایط استفاده کاربران، یا استانداردهای حرفه‌ای صنعت باشد. در صورت اثبات این وظیفه و همچنین توانایی شرکت در جلوگیری از جرم، ترک فعل می‌تواند مصداق مسئولیت کیفری باشد.

شکل دیگر نقش شرکت، تولید یا توزیع فناوری‌هایی است که به‌طور خاص برای ارتکاب جرم طراحی یا بهینه‌سازی شده‌اند. در این حالت، شرکت ممکن است نرم‌افزارهایی را ارائه دهد که هدف

یا کارکرد اصلی آن‌ها انجام یا پنهان‌سازی فعالیت‌های مجرمانه باشد، مانند ابزارهای رمزگذاری مخفیانه، شبکه‌های غیرقابل ردیابی[۱۰]، یا بدافزارهای قابل استفاده برای نفوذ و جاسوسی. چنان چه ثابت شود که شرکت علم داشته است که کاربران عمدتاً از این فناوری در جهت فعالیت مجرمانه استفاده می‌کنند و به‌رغم این علم به توسعه یا توزیع آن ادامه داده، مسئولیت کیفری شرکت در حد مشارکت عمدی یا حتی مباشرت غیرمستقیم در جرم قابل طرح است. این تحلیل مبتنی‌بر اصل «ارائه آگاهانه ابزار برای ارتکاب جرم» در فقه کیفری و رویه‌های بین‌المللی است.

در مواردی نادر، ممکن است شرکت نه‌تنها زمینه را برای ارتکاب جرم فراهم کند، بلکه سیاست‌ها و دستورات داخلی صریحی صادر کند که کارمندان یا کاربران را به ارتکاب جرم هدایت یا مجبور سازد. این حالت در چهارچوب «سازمان‌یافتگی مجرمانه» شرکت قرار می‌گیرد و می‌توان آن را مصداق ارتکاب مستقیم جرم توسط شخص حقوقی دانست، حتی اگر اعمال مادی جرم توسط افراد انسانی انجام شده باشد. در این فرض، شرکت در مقام یک واحد تصمیم‌گیر و برنامه‌ریز، شخصاً در جرم مداخله کرده و مسئولیت کیفری مستقیم آن قابل طرح است. برخی شرکت‌ها ممکن است «در فرآیند پنهان‌سازی جرم یا جلوگیری از کشف آن» مشارکت داشته باشند. این امر ممکن است از طریق پاک‌سازی شواهد دیجیتال، تغییر در داده‌های سرور، یا عدم همکاری با مراجع قضایی و انتظامی در ارائه اطلاعات صورت گیرد. چنین رفتارهایی در حوزه «ممانعت از اجرای عدالت» یا «تبانی پس از وقوع جرم» قرار می‌گیرند و بسته به کیفیت همکاری یا کارشکنی شرکت، مسئولیت کیفری مستقل برای آن قابل تحقق است.

در تمامی این موارد، تحلیل دقیق نقش شرکت نیازمند بررسی هم‌زمان رفتارهای مثبت یا منفی، میزان علم و آگاهی، قدرت مداخله و پیوند علی میان اقدامات شرکت و نتیجه مجرمانه است. در غیاب این عناصر، هرچند ممکن است نقد اخلاقی یا مدنی متوجه شرکت باشد، اما استناد به مسئولیت

۱۰- مانند برخی نسخه‌های خاص از شبکه‌های تور

کیفری بدون پشتوانه روشن حقوقی امکان‌پذیر نخواهد بود (Buell,2018,86).

۲-۳- حدود و معیارهای احراز مسئولیت

احراز مسئولیت کیفری شرکت‌های فناوری در قبال جرایم ارتکابی توسط کاربران، مستلزم تعیین حدود و معیارهایی است که از یک سو مبتنی‌بر اصول بنیادین حقوق کیفری همچون اصل فردی بودن مسئولیت و اصل قانونی بودن جرم و مجازات است و از سوی دیگر، باید با پیچیدگی‌های ساختارهای فناورانه، غیرمتمرکز و چندلایه این شرکت‌ها انطباق یابد. تعیین این حدود نیازمندشناسایی رابطه علی بین رفتار یا ساختار شرکت و جرم ارتکابی است، به گونه‌ای که نه صرفاً ارتباط فنی یا زمانی، بلکه پیوند حقوقی و تقصیرآمیز بین آن دو اثبات شود.

نخستین معیار اساسی، اثبات وجود «رفتار مؤثر منتسب به شرکت» است. در نظام‌های حقوقی که مسئولیت کیفری اشخاص حقوقی را به رسمیت می‌شناسند، صرف عضویت در فضای وقوع جرم یا ارائه خدمات بی‌طرفانه برای تحقق مسئولیت کفایت نمی‌کند. باید نشان داده شود که شرکت در قالب فعل یا ترک فعل، نقشی معنادار در فرایند ارتکاب جرم ایفاء کرده است. این نقش می‌تواند در قالب طراحی سازوکارهای تسهیلگر، الگوریتم‌های محرک محتواهای مجرمانه، یا عدم انجام تکالیف پیشگیرانه محقق شود. در این حالت، فعل یا ترک فعل باید قابل انتساب به اراده و ساختار شرکت به‌عنوان یک واحد حقوقی مستقل باشد، نه صرفاً نتیجه عملکرد غیرقابل پیش‌بینی کاربران.

عنصر دوم، «عنصر ذهنی یا تقصیر کیفری شرکت» است که تحقق آن در حوزه اشخاص حقوقی با چالش خاصی مواجه است، زیرا این اشخاص فاقد شعور یا اراده انسانی مستقیم هستند. حقوق کیفری برای عبور از این مانع، دو رویکرد را به‌کار گرفته است: یکی «انتساب اراده افراد تصمیم‌گیر در شرکت به خود شرکت» و دیگری «پذیرش خطای ساختاری یا سوءمدیریت به‌عنوان جانشین عنصر روانی». در رویکرد نخست، باید اثبات شود که مدیران یا مسئولان رده‌بالای شرکت با علم به نتایج مجرمانه ساختار فنی یا سیاست داخلی، تصمیماتی اتخاذ کرده‌اند که زمینه ارتکاب جرم را فراهم

آورده است. در رویکرد دوم، لازم است نشان داده شود که شرکت با وجود آگاهی از خطرات موجود، اقدامات لازم برای جلوگیری از وقوع جرم را اتخاذ نکرده یا سازوکارهای کنترل درونی و نظارتی مؤثری نداشته است. در هر دو صورت، عنصر روانی از طریق ساختار تصمیم‌گیری و نظام داخلی شرکت ارزیابی می‌شود و نه از طریق اثبات نیت مجرمانه مستقیم (شریفی، ۱۳۹۴، ۲۱۲).

معیار مهم بعدی، «وجود رابطه علیت کیفری میان رفتار شرکت و جرم ارتکابی توسط کاربر» است. این رابطه باید بیش از یک رابطه فنی یا غیرشخصی باشد. در واقع، باید نشان داده شود که بدون رفتار خاص شرکت، جرم یا به وقوع نمی‌پیوست یا به این شکل و شدت رخ نمی‌داد. در علم حقوق، این نوع رابطه علیت نه صرفاً رابطه مادی، بلکه رابطه‌ای حقوقی و تقصیرآمیز است که از طریق ارزیابی نقش تعیین‌کننده یا تسهیلگر رفتار شرکت در زنجیره علیت محقق می‌شود. این تحلیل مخصوصاً در جرایم سایبری که چندین عامل هم‌زمان و متداخل وجود دارد، از اهمیت بیشتری برخوردار است، زیرا احراز سهم دقیق شرکت در وقوع جرم دشوار است و باید با معیار «اهمیت نقش» یا «سبب اقوی» ارزیابی شود (ترخان، ۱۳۹۵، ۳۸).

از دیگر معیارهای مهم، «داشتن توانایی پیش‌بینی و قدرت مداخله» است. مسئولیت کیفری فقط در صورتی قابل انتساب است که شرکت یا مدیران آن امکان پیش‌بینی رفتار مجرمانه کاربران را داشته و بااین‌حال، از اتخاذ اقدامات پیشگیرانه یا کنترلی خودداری کرده باشند. این معیار بر پایه مفهوم «تقصیر در عدم پیش‌بینی یا پیشگیری» بنا شده است که در حقوق کیفری نوین پذیرفته شده و در قالب دکترین «وظیفه مراقبت سازمانی» قابل تبیین است. برای مثال، اگر شرکت به دلیل سابقه قبلی کاربران یا هشدارهای فنی مستمر از خطر ارتکاب جرم آگاه بوده اما هیچ سازوکار شفاف، سریع و مؤثری برای محدودسازی کاربران یا گزارش به مقامات تعبیه نکرده باشد، آن گاه تقصیر در چهارچوب عدم ایفای وظیفه مراقبت سازمانی تحقق یافته و مسئولیت کیفری شرکت قابل استناد است.

در کنار این عناصر، باید توجه داشت که احراز مسئولیت کیفری شرکت مشروط به نبود مانع قانونی یا اصل «قانونی بودن جرم و مجازات» است. به عبارت دیگر، مسئولیت کیفری تنها زمانی قابل

اعمال است که قانون صریحاً ارتکاب جرم توسط شخص حقوقی را در موضوع موردنظر پیش‌بینی کرده باشد یا بر اساس اصول کلی قابل توسعه باشد. در غیاب این شرط، هرچند ممکن است مسئولیت مدنی یا انتظامی برای شرکت مطرح باشد، اما ورود به حوزه کیفری نیازمند پیش‌بینی صریح قانونی است (Diamantis,2015,249).

به‌ویژه در حقوق کیفری ایران که رویکرد مضیق و تفسیری در قبال جرم‌انگاری دارد. احراز مسئولیت کیفری شرکت‌های فناوری منوط به ارزیابی هم‌زمان چهار بعد بنیادین است: رفتار قابل انتساب به شرکت، وجود عنصر روانی سازمان‌یافته، رابطه علیت تقصیرآمیز و امکان پیش‌بینی و مداخله مؤثر. تنها در صورت اجتماع این ابعاد، مسئولیت کیفری شرکت در قبال جرایم کاربران قابل استناد خواهد بود و در غیر این صورت، اصل بر برائت است.

۳- تحلیل تطبیقی و رویه‌های حقوقی

تحلیل تطبیقی و بررسی رویه‌های حقوقی در زمینه مسئولیت کیفری شرکت‌های فناوری در قبال جرایم کاربران، به منظور درک دقیق‌تر نحوه مواجهه نظام‌های حقوقی مختلف با چالش‌های نوین ناشی از فعالیت‌های پلتفرم‌های دیجیتال، ضرورتی علمی و عملی دارد. در نظام‌های حقوقی پیشرفته مانند ایالات متحده امریکا، بریتانیا و اتحادیه اروپا تلاش شده است تا با بهره‌گیری از مفاهیمی چون «سوءمدیریت سازمانی»، «قصور در نظارت» و «ساختارهای تسهیلگر جرم»، شرکت‌های فناوری در قبال جرایم کاربران، در موارد خاص، تحت مسئولیت کیفری قرار گیرند. در مقابل، نظام‌های حقوقی با ساختار سنتی‌تر، مانند ایران، با تردید بیشتری به این موضوع می‌نگرند و چهارچوب‌های مسئولیت کیفری اشخاص حقوقی را به‌صورت مضیق و محدود اعمال می‌کنند. بررسی تطبیقی این رویکردها، ضمن روشن ساختن نقاط قوت و ضعف هر نظام، می‌تواند راهگشای اصلاح و توسعه قوانین داخلی متناسب با واقعیت‌های پیچیده‌ی فضای سایبری باشد.

۳-۱- نظام حقوقی ایران

در نظام حقوقی ایران، مسئولیت کیفری اشخاص حقوقی، از جمله شرکت‌های فناوری، مفهومی نوپدید و تا حدودی محدودشده تلقی می‌شود که مبنای آن عمدتاً در اصلاحات قانونی اخیر و برخی تفسیرهای حقوقی جای دارد، نه در یک نظام منسجم و ساختاریافته همچون آن چه در کشورهای دارای سنت حقوقی نهادینه‌شده در حوزه مسئولیت کیفری شرکت‌ها مشاهده می‌شود. تا پیش از قانون مجازات اسلامی مصوب ۱۳۹۲، اصولاً مسئولیت کیفری اشخاص حقوقی در حقوق کیفری ایران به رسمیت شناخته نمی‌شد و تنها از طریق مجازات‌های مدنی یا اداری به عملکرد نهادهای حقوقی رسیدگی می‌شد. اما ماده ۱۴۳ قانون مجازات اسلامی مصوب ۱۳۹۲ با پذیرش اصل مسئولیت کیفری اشخاص حقوقی، مشروط بر این که جرم در راستای اهداف شخص حقوقی و توسط نماینده قانونی آن ارتکاب یافته باشد، گامی مقدماتی در جهت پذیرش این مفهوم برداشت.

بااین‌حال، این ماده چهارچوبی مضیق و محدود را ترسیم می‌کند که انعطاف لازم برای تطبیق با تحولات پیچیده فضای دیجیتال را ندارد. قانون‌گذار ایران در ماده مذکور وقوع جرم را منوط به اثبات رابطه بین فعل مجرمانه و اهداف و منافع شخص حقوقی کرده است، بدون آن که معیارهای دقیق احراز عنصر روانی در بستر سازمانی یا ساختارهای درونی شرکت‌های فناوری را مشخص سازد. چنین محدودیتی در حقوق فناوری اطلاعات که روابط پیچیده، غیرمتمرکز و غالباً ناشناس بین کاربران و پلتفرم‌ها برقرار است، به‌روشنی ناکارآمد جلوه می‌کند. همچنین، از آن جا که بسیاری از جرایم کاربران در بستر خدماتی صورت می‌گیرد که شرکت‌های فناوری تنها زیرساخت فنی آن را فراهم کرده‌اند، تفسیر مضیق از «ارتکاب توسط نماینده قانونی» مانع از توسعه مسئولیت کیفری در قبال این نوع نقش‌های غیرمستقیم یا ساختاری می‌شود (مصدق، ۱۴۰۲، ۱۶۴).

از سوی دیگر، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ نیز با آن که پاره‌ای از تکالیف را متوجه ارائه‌دهندگان خدمات اینترنتی کرده است، اما فاقد نظام مسئولیت کیفری ناظر بر رفتار کاربران در بسترهای پلتفرمی است. رویکرد قانون‌گذار در این قانون بیش از آن که به سراغ مدل‌های نوین

مسئولیت مبتنی‌بر «نقض الزامات ایمنی»، «سهل‌انگاری در نظارت»، یا «ایجاد بستر جرم‌زا» برود، به سمت تعیین مصادیق فنی جرم‌انگاری سوق یافته است. این در حالی است که در دیگر نظام‌های حقوقی، مفهوم «خطای سازمانی» یا «فقدان سازوکارهای کنترل داخلی» به‌عنوان معیارهای سنجش مسئولیت کیفری نهادها به کار گرفته می‌شود. در نتیجه، حقوق کیفری ایران در این زمینه بیشتر به سمت مسئولیت فردی گرایش دارد و به سختی می‌توان در آن جایگاهی برای مسئولیت ساختاری شرکت‌های فناوری در قبال رفتار کاربران یافت (عزیزی، ۱۳۹۸، ۵۷).

باید اذعان کرد که دادگاه‌های کیفری ایران نیز غالباً در مواجهه با جرایم ناشی از پلتفرم‌های دیجیتال، تمرکز خود را بر عامل انسانی مستقیم یعنی کاربر خاطی می‌گذارند و کمتر به بررسی نقش نهاد میزبان یا تسهیلگر می‌پردازند. در موارد نادری که شرکت به‌عنوان طرف دعوی وارد شده، مبنا بیشتر مسئولیت مدنی یا نقض مقررات بوده تا احراز مسئولیت کیفری ساختاریافته. مجموع این عوامل نشان می‌دهد که نظام حقوقی ایران هنوز به مرحله‌ای نرسیده است که بتواند به‌طور اثربخش و علمی، شرکت‌های فناوری را در قبال ارتکاب جرایم کاربران شان پاسخگو سازد، مگر در موارد بسیار محدود و خاص. این موضوع نیازمند بازنگری اساسی در مفهوم مسئولیت کیفری اشخاص حقوقی، توسعه معیارهای احراز عنصر روانی در ساختارهای حقوقی و اقتباس سنجیده از تجارب تطبیقی در زمینه مفاهیمی چون تقصیر سازمانی، نظام‌های پیشگیرانه نظارتی و تحلیل ریسک‌های دیجیتال است (رضایی، ۱۳۹۸، ۲۸۷-۳۰۳).

۳-۲- نظام‌های فرانسه و ایالات متحده امریکا

در نظام حقوقی فرانسه، مسئولیت کیفری اشخاص حقوقی از جمله شرکت‌های فناوری اطلاعات، جایگاهی تثبیت‌شده و منسجم دارد و از دیرباز در متن قوانین کیفری این کشور به رسمیت شناخته شده است. ماده ۱۲۱-۲ قانون جزای فرانسه[11] مقرر می‌دارد که اشخاص حقوقی، به‌جز دولت،

11- Code pénal

می‌توانند در قبال ارتکاب جرایم توسط اعضاء یا نمایندگان خود، مشروط بر این که در چهارچوب وظایف محوله و به نفع شرکت صورت گرفته باشد، مسئولیت کیفری داشته باشند. این قاعده عام، در نظام حقوقی فرانسه منجر به پذیرش اصل استقلال مسئولیت کیفری اشخاص حقوقی از مرتکبین حقیقی شده و نیازی به اثبات تقصیر یا سوءنیت مدیرعامل خاصی وجود ندارد، بلکه کافی است اثبات شود که جرم در قالب فعالیت حرفه‌ای یا ساختار سازمانی شرکت و در مسیر منافع آن انجام شده است (Dreyer,2016,744).

در مورد شرکت‌های فناوری، رویه قضایی و تفاسیر دکترین حقوقی فرانسه، بر مدل‌هایی مانند «نقض تعهدات ایمنی»، «سهل‌انگاری در مدیریت داده‌ها» و «عدم جلوگیری از تحقق نتیجه مجرمانه» تأکید دارند. در این راستا، شرکت‌های پلتفرمی مانند شبکه‌های اجتماعی یا میزبانان خدمات دیجیتال، در صورتی که نتوانند نشان دهند اقدامات پیشگیرانه مناسب برای کنترل فعالیت‌های کاربران داشته‌اند یا از هشدارهای قبلی چشم‌پوشی کرده‌اند، می‌توانند تحت عنوان «قصور سازمانی» مسئول شناخته شوند. در پرونده‌های مطرح‌شده علیه شرکت‌هایی نظیر گوگل فرانسه[۱۲] یا فیسبوک[۱۳]، دادگاه‌ها به بررسی دقیق سازوکارهای کنترلی داخلی، وجود سیستم‌های گزارش‌دهی[۱۴] و توان فنی و اداری شرکت در پیشگیری از گسترش محتوای مجرمانه پرداختند. در این مدل، توجه به جایگاه سازمانی جرم[۱۵] بر عنصر فردی ارجح دانسته می‌شود و شرکت نه به‌عنوان بدیلی برای فرد، بلکه به‌عنوان فاعل مستقل جرم شناخته می‌شود (Boccon-Gibod,2014,923).

از سوی دیگر، در نظام حقوقی ایالات متحده امریکا، مسئولیت کیفری شرکت‌های فناوری در قبال جرایم کاربران، بر پایه نظریه‌های پیشرفته‌تری مانند پاسخگویی به نیابت از کارمند[۱۶]، شکست در

12- Google France
13- Facebook
14- reporting
15- contextual criminality
16- respondeat superior

نظارت و رعایت الزامات قانونی[۱۷] و نادیده‌انگاری عمدی[۱۸] بنا شده است. حقوق کیفری فدرال ایالات متحده امریکا به موجب رویه دادگاه‌های عالی، مانند «امریکا علیه هیلتون هتل»[۱۹] و «امریکا علیه بانک نیو انگلند»[۲۰] اشخاص حقوقی را حتی در غیاب قصد مجرمانه مدیر ارشد، مسئول می‌داند، اگر رفتار یکی از کارکنان در چهارچوب وظایف محوله صورت گرفته باشد و شرکت از نظر ساختاری یا فرهنگی زمینه ارتکاب جرم را فراهم کرده باشد.

دادگاه‌های ایالات متحده امریکا مدل مسئولیت را بر مبنای تحلیل ریسک سازمانی[۲۱] قرار داده‌اند. مثلاً اگر شرکتی پلتفرمی را فراهم کند که قابلیت انتشار گسترده محتوا توسط کاربران را دارد، اما به‌صورت عامدانه از طراحی یا پیاده‌سازی فیلترهای محتوایی یا سیستم‌های هشداردهنده امتناع کند، این امر می‌تواند مصداق «بی‌مبالاتی مجرمانه»[۲۲] یا حتی «سهل‌انگاری عمدی» تلقی شود. در پرونده معروف «داو علیه مای اسپک»[۲۳] دادگاه بررسی کرد که آیا پلتفرم می‌تواند در برابر سوءاستفاده‌های جنسی که کاربران از طریق آن مرتکب شدند، مسئول شناخته شود. هرچند بر مبنای «بند ۲۳۰ قانون ارتباطات محترمانه»[۲۴] بسیاری از دعاوی مدنی رد شدند، اما در موارد کیفری، شرکت‌هایی که در برابر هشدارهای مکرر مراجع قضایی یا کاربران هیچ‌گونه اقدام اصلاحی نکردند، در معرض پیگرد فدرال قرار گرفته‌اند (De Maglie,2005,547).

در این نظام، مسئولیت کیفری با عناصر ساختاری همچون عدم تدوین برنامه‌های «مقرراتی»[۲۵] ضعف در سیاست‌های حفظ داده، یا فقدان واحدهای گزارشگری داخلی مرتبط است. سازمان‌هایی که سیستم‌های «کنترل داخلی» ندارند یا در برابر نشانه‌های خطر و فعالیت‌های مشکوک، منفعل عمل

17- corporate compliance failure
18- willful blindness
19- United States v. Hilton Hotels
20- United States v. Bank of New England
21- Organizational Risk Analysis
22- criminal negligence
23- Doe v. MySpace
24- Section 230 of the Communications Decency Act
25- compliance

می‌کنند، حتی اگر مدیران ارشد مستقیماً مطلع نباشند، مسئول شناخته می‌شوند. این رویکرد که در سیاستگذاری نهادهایی مانند وزارت دادگستری ایالات متحده امریکا و اف بی‌آی[۲۶] نیز به چشم می‌خورد، به شرکت‌های فناوری این پیام را می‌دهد که صرف فراهم‌آوردن پلتفرم، کفایت نمی‌کند و باید سازوکارهای فعال برای جلوگیری از بروز جرم در بستر خدمات خود فراهم کنند (Podgor,2003,167).

اگرچه هر دو نظام فرانسه و ایالات متحده امریکا اصل مسئولیت کیفری شرکت‌های فناوری را در قبال اعمال کاربران پذیرفته‌اند، فرانسه بیشتر به نقش ساختاری جرم و فقدان نظارت مؤثر تأکید دارد، درحالی‌که ایالات متحده امریکا علاوه بر این عوامل، به تحلیل اراده سازمانی، سازوکارهای پیشگیری و مسئولیت ناشی از عدم رعایت مقررات ایالتی و فدرال می‌پردازد. این دو نظام با آن که در جزئیات با یکدیگر تفاوت دارند، اما به‌روشنی از مدل سنتی مسئولیت فردی فاصله گرفته و به سمت مدل‌های سیستمی، ساختاری و مدیریتی در قبال مسئولیت کیفری اشخاص حقوقی حرکت کرده‌اند.

۳-۳- نهادهای تنظیم‌گر و نقش آن‌ها

نهادهای تنظیم‌گر در حوزه فناوری اطلاعات، به‌ویژه در زمینه مسئولیت شرکت‌ها در قبال جرایم کاربران، دارای جایگاه ویژه‌ای هستند و نقش آن‌ها از سطح سیاستگذاری کلان تا اعمال نظارت و اجرای مقررات گسترده است. تحلیل عملکرد این نهادها مستلزم درک پیوسته‌ای از رابطه میان ساختار حقوقی، سیاست عمومی و تحولات فناوری است. در نظام‌های مختلف حقوقی، این نهادها به‌عنوان بازوی اجرایی و نظارتی دولت‌ها در قبال فعالیت‌های شرکت‌های فناوری عمل می‌کنند، با این هدف که توازن میان نوآوری‌های تکنولوژیک و حفظ منافع عمومی، حریم خصوصی، نظم عمومی و امنیت ملی برقرار گردد.

در سطح نخست، نهادهای تنظیم‌گر با تدوین مقررات و دستورالعمل‌های اجرایی،

26- FBI

چهارچوب‌هایی را تعیین می‌کنند که شرکت‌های فناوری در ارائه خدمات به کاربران ملزم به رعایت آن‌ها هستند. این مقررات می‌توانند حوزه‌هایی چون جمع‌آوری و پردازش داده‌ها، اقدامات پیشگیرانه در قبال محتوای مجرمانه، رعایت حقوق مالکیت فکری و مقابله با نفرت‌پراکنی یا تحریک به خشونت را شامل شوند. در این سطح، تنظیم‌گران نه‌فقط نقش قانون‌گذار مکمل، بلکه نقشی هدایت‌گر برای تبیین حدود مسئولیت شرکت‌ها ایفاء می‌کنند.

در سطح دوم، این نهادها با ایجاد نظام‌های پایش و ارزیابی عملکرد، به نظارت بر اجرای صحیح مقررات توسط شرکت‌ها می‌پردازند. نظارت‌هایی از نوع ممیزی‌های امنیت سایبری، ارزیابی تبعیت از دستورالعمل‌های حفاظت از داده‌ها یا بررسی سازوکارهای کنترل محتوای مجرمانه، به تنظیم‌گر این امکان را می‌دهد که به‌موقع با موارد تخلف برخورد کند. ازاین رو این نهادها صرفاً تنظیم‌گر نیستند، بلکه به‌عنوان مرجع مسئولیت‌سنجی و پاسخ‌خواهی نیز عمل می‌کنند. از سوی دیگر، نهادهای تنظیم‌گر اغلب نقش میانجی میان نهادهای قضایی و شرکت‌های فناوری را نیز ایفاء می‌کنند. آن‌ها در مواردی که فعالیت کاربران در پلتفرم‌های دیجیتال منجر به ارتکاب جرم شده، از شرکت‌ها می‌خواهند که اطلاعات مربوط به کاربران یا داده‌های لازم برای تحقیقات کیفری را در اختیار نهادهای ذیصلاح قرار دهند. این نقش که به نوعی میان نظارت اداری و کمک به فرآیند کیفری قرار دارد، نشان می‌دهد که تنظیم‌گران در حوزه فناوری، نقشی فراتر از قواعد کلاسیک ایفاء می‌کنند (برزگرکهنمویی، ۱۴۰۳، ۶۲).

یکی دیگر از ابعاد مهم عملکرد نهادهای تنظیم‌گر، هدایت و الزام شرکت‌ها به طراحی سازوکارهای خودتنظیم‌گر در درون ساختارشان است. به عبارت دیگر، تنظیم‌گرها تلاش می‌کنند با تشویق شرکت‌ها به ایجاد نهادهای داخلی رعایت مقررات[۲۷]، فرآیند مسئولیت‌پذیری را نهادینه کنند. این اقدامات می‌تواند شامل ایجاد الگوریتم‌های فیلتر محتوا، گزارش‌دهی تخلفات کاربران، و تدوین سیاست‌های محرمانگی و امنیت اطلاعات باشد. تنظیم‌گر در این حالت، به‌جای تحمیل مستقیم قواعد، چهارچوبی را ترسیم می‌کند که شرکت بر اساس آن، خود فرآیندشناسایی و پیشگیری از جرایم را

27- compliance units

مدیریت کند. در کنار این نقش‌های اجرایی و نظارتی، نهادهای تنظیم‌گر گاه وارد عرصه تفسیر و توسعه هنجارهای حقوقی نیز می‌شوند. به‌ویژه در کشورهایی که قواعد حقوقی سنتی ظرفیت پاسخگویی به پیچیدگی جرایم فضای مجازی را ندارند، تنظیم‌گران با صدور راهنماها، تفاسیر اجرایی و مشاوره‌های تخصصی به شکلی شبه‌قضایی در توسعه رویه‌های قابل اتکاء برای‌شناسایی مسئولیت شرکت‌ها مشارکت می‌کنند. این موضوع، رابطه میان حقوق نرم[۲۸] و حقوق الزام‌آور[۲۹] را در بستر فناوری برجسته می‌سازد (Shleifer,2005,35).

نهادهای تنظیم‌گر با ایفای نقش چندلایه شامل مقرره‌گذاری، نظارت، هماهنگی میان‌بخشی و تسهیلگر اجرای عدالت ستون اصلی در شکل‌دهی و اجرای مسئولیت کیفری شرکت‌های فناوری در قبال جرایم کاربران به‌شمار می‌روند. این نهادها، ضمن حفظ بی‌طرفی نهادی، قادرند هم منافع عمومی و هم الزامات نوآوری را در یک سازوکار پویا و متوازن تأمین کنند. بدون حضور مؤثر و شفاف آن‌ها، تحقق عملی مسئولیت شرکت‌ها در محیط متغیر دیجیتال امکان‌پذیر نخواهد بود.

۴- چالش‌ها و راهکارها

در دوران معاصر، گسترش پلتفرم‌های دیجیتال و نفوذ گسترده فناوری‌های نوین در تمامی عرصه‌های زندگی، چالش‌های بی‌سابقه‌ای را در عرصه حقوق کیفری به‌ویژه در حوزه مسئولیت شرکت‌های فناوری در قبال اعمال کاربران پدید آورده است. پرسش از حدود، معیارها و سازوکارهای پاسخگویی این شرکت‌ها به جرایم ارتکابی در بستر خدمات‌شان، نقطه تمرکز اصلی چالش‌ها است؛ چالش‌هایی که نه‌تنها در سطح نظری بلکه در عمل نیز نظام‌های حقوقی را با دشواری‌های پیچیده مواجه ساخته است. در این میان، ارائه راهکارهای متناسب با تحول فناوری و درعین‌حال مبتنی‌بر اصول بنیادین حقوق کیفری از ضرورت‌های انکارناپذیر به شمار می‌رود. از این‌رو، در ادامه با تمرکز بر چالش‌های اساسی و راهکارهای ممکن، تلاش می‌شود به

28- soft law
29- hard law

تحلیل نظام‌مند این مبحث از مسئولیت کیفری در فضای فناوری پرداخته شود.

۴-۱- چالش‌های اثبات مسئولیت کیفری

یکی از اساسی‌ترین موانع در مسیر اعمال مسئولیت کیفری بر شرکت‌های فناوری، دشواری‌ها و پیچیدگی‌های مربوط به اثبات عناصر مسئولیت کیفری است که با توجه به ماهیت غیرمادی، پراکندگی جغرافیایی و سازوکارهای پیچیده فناوری‌های نوین، ابعاد خاص و منحصر به فردی یافته‌اند. این دشواری‌ها، هم در بعدشناسایی نقش شرکت در وقوع جرم و هم در تشخیص رابطه علیت میان فعل یا ترک فعل شرکت و تحقق نتیجه مجرمانه، نمود پیدا می‌کنند.

نخستین چالش بنیادین در این راستا، فقدان عنصر مادی قابل رؤیت به شیوه سنتی در جرایم رخ‌داده در بستر فناوری است. در موارد بسیاری، بستر ارتکاب جرم نه یک کنش مشهود بلکه ساختار یا خدماتی است که توسط شرکت فناوری فراهم شده و به‌ظاهر بی‌طرفانه در اختیار کاربران قرار گرفته است. همین ویژگی سبب می‌شود تمایز میان فعل مجرمانه و بستر بی‌طرف تسهیل‌کننده به‌سادگی ممکن نباشد. در مواردی که شرکت صرفاً بستری فنی برای تبادل داده یا انتشار محتوا فراهم کرده، احراز این که این اقدام مصداق فعل مجرمانه یا معاونت در جرم باشد، نیازمند تحلیل پیچیده فنی–حقوقی است و صرف وجود محتوای مجرمانه در پلتفرم، برای اثبات مسئولیت کیفری شرکت کفایت نمی‌کند.

چالش دوم، ناظر بر احراز عنصر روانی یا سوءنیت است. برخلاف اشخاص حقیقی که در رویه‌های سنتی کیفری، علم و اراده آن‌ها به‌عنوان مبنای مسئولیت در نظر گرفته می‌شود، در مورد شرکت‌های فناوری، سوءنیت باید در قالب سازوکارهای درونی سازمان، خط‌مشی‌های رسمی، یا تصمیمات مدیران عالی‌رتبه بازسازی و اثبات شود. با توجه به سلسله‌مراتب پیچیده مدیریتی، تفویض اختیارات و فقدان اراده واحد قابل احراز، اثبات این که شرکت از بروز جرم مطلع بوده و به‌طور آگاهانه از مداخله خودداری کرده یا حتی زمینه‌ساز ارتکاب آن شده، با دشواری جدی مواجه است.

این امر به‌ویژه در شرکت‌هایی که به‌صورت الگوریتمی و خودکار محتوا را مدیریت می‌کنند، موجب می‌شود ارزیابی سوءنیت، امری انتزاعی و محل تردید باشد.

از دیگر موانع مهم، اثبات رابطه علیت بین رفتار یا ساختار شرکت و وقوع جرم است. در نظام حقوق کیفری، مسئولیت کیفری تنها در صورتی قابل اعمال است که میان رفتار متهم و نتیجه زیان‌بار جرم، رابطه علیت وجود داشته باشد. در فضای دیجیتال، وقوع جرم ممکن است از طریق زنجیره‌ای از عوامل و بازیگران صورت گیرد و شرکت فناوری تنها یکی از حلقه‌های این زنجیره باشد. تمایز میان علت مستقیم و غیرمستقیم و تبیین این که نقش شرکت، شرط لازم برای وقوع جرم بوده یا صرفاً تسهیلگر آن یک چالش اثباتی پیچیده ایجاد می‌کند. در این موارد، شرکت‌ها غالباً با استناد به اصل عدم مسئولیت در قبال اعمال غیرقابل پیش‌بینی کاربران، خود را از شمول عنصر علیت خارج می‌سازند (Watney,2017,78).

علاوه بر موارد یاد شده، مشکلات فنی و محدودیت‌های دسترسی به داده‌ها نیز مانعی جدی در اثبات مسئولیت کیفری هستند. در بسیاری از موارد، داده‌های مربوط به فعالیت کاربران در اختیار خود شرکت‌ها است و امکان ارزیابی نقش واقعی شرکت‌ها بدون همکاری آن‌ها، برای مراجع قضایی وجود ندارد. این وابستگی موجب نوعی عدم تقارن اطلاعاتی میان نهادهای تعقیب و شرکت‌های فناوری می‌شود که فرایند اثبات را به‌شدت تضعیف می‌کند. همچنین، در مواردی که شرکت‌ها در خارج از حوزه قضایی صلاحیتی قرار دارند یا داده‌ها در سرورهای برون‌مرزی نگهداری می‌شود، اجرای دستورات قضایی و دسترسی به شواهد لازم برای اثبات مسئولیت تقریباً غیرممکن می‌گردد.

پیچیدگی ساختارهای فناورانه و تغییرات سریع الگوریتم‌های پردازش اطلاعات، امکان ارزیابی حقوقی دقیق از فعل یا ترک فعل شرکت را دشوار می‌سازد. الگوریتم‌هایی که به‌صورت پویا و با یادگیری ماشین توسعه می‌یابند، مسئولیت را از سطح تصمیم‌گیری انسانی به حوزه‌های نیمه‌خودکار منتقل می‌کنند. چنین وضعیتی سبب می‌شود تا هم در مقام کشف حقیقت و هم در مقام انتساب مسئولیت، دقت و شفافیت لازم برای اثبات جرم در قالب‌های سنتی حقوق کیفری حاصل نشود.

ساختار پیچیده، عدم شفافیت، تعدد واسطه‌ها، فناوری‌های متغیر و نبود استانداردهای جهانی روشن برای ارزیابی تقصیر یا علم شرکت‌ها، چالش‌هایی را در مسیر اثبات مسئولیت کیفری ایجاد کرده‌اند که مستلزم بازنگری‌های عمیق در ابزارها و معیارهای اثبات جرم در حوزه شرکت‌های فناوری است (رئیسی و قاسم‌زاده‌لیاسی، ۱۳۹۹، ۱۲۰).

۴-۲- موازنه بین آزادی بیان و کنترل محتوا

موازنه میان آزادی بیان و کنترل محتوا در بسترهای فناوری و پلتفرم‌های دیجیتال یکی از بنیادی‌ترین مسائل حقوقی در دوران معاصر است که با توسعه فناوری اطلاعات و شبکه‌های اجتماعی اهمیت مضاعفی یافته است. این موازنه در واقع میان دو ارزش اساسی قرار دارد: از یک سو، آزادی بیان که به‌عنوان یکی از حقوق بنیادین بشر شناخته می‌شود و در اسناد بین‌المللی از جمله ماده ۱۹ اعلامیه جهانی حقوق بشر و میثاق بین‌المللی حقوق مدنی و سیاسی به رسمیت شناخته شده است و از سوی دیگر، نیاز به حفاظت از منافع عمومی نظیر امنیت ملی، نظم عمومی، اخلاق عمومی و حقوق دیگران که اقتضاء می‌کند گاه محدودیت‌هایی نسبت به محتوای منتشر شده در فضای مجازی اعمال شود.[۳۰]

در عمل، مسئله از آن جا آغاز می‌شود که شرکت‌های فناوری، به‌ویژه پلتفرم‌های بزرگ مانند شبکه‌های اجتماعی میزبان حجم عظیمی از محتوا هستند که توسط کاربران تولید می‌شود. این محتوا می‌تواند شامل اظهارنظرهای سیاسی، فرهنگی، دینی یا حتی نفرت‌پراکنی، تهدید، نشر اکاذیب، تحریک به خشونت یا تروریسم یا محتوای ناقض حقوق مالکیت فکری و حریم خصوصی باشد. از آن جا که این شرکت‌ها نقش واسطه‌گری بین کاربران و فضای عمومی را ایفاء می‌کنند، ازیک‌سو باید امکان اظهار آزادانه نظرات را فراهم آورند و از سوی دیگر، باید مانع انتشار محتوای زیان‌بار یا غیرقانونی شوند. این جا است که ضرورت موازنه میان این دو ضرورت قانونی و اخلاقی مطرح می‌شود.

30- UN Human Rights Council. Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, David Kaye, A/HRC/38/35, June 2018

نظام‌های حقوقی مختلف برای ایجاد این موازنه، معیارهایی را وضع کرده‌اند که اغلب بر سه پایه استوارند: ضرورت، تناسب و مشروعیت هدف. اصل ضرورت اقتضاء دارد که محدودیت‌های اعمال‌شده بر آزادی بیان فقط در مواقعی اعمال شود که واقعاً نیاز غیرقابل اجتنابی وجود دارد. تناسب به معنای آن است که محدودیت باید به نحوی طراحی شود که آسیب آن به آزادی بیان کمتر از ضرری باشد که از طریق انتشار محتوا متوجه جامعه می‌شود. مشروعیت هدف نیز به این معنا است که هدف از محدودیت باید در چهارچوب اهدافی باشد که قوانین بین‌المللی آن را مجاز دانسته‌اند، نظیر پیشگیری از نفرت‌پراکنی، تروریسم یا حفاظت از کودکان (کازرونی، ۱۳۹۵، ۱۹۸). از سوی دیگر، ساختار تصمیم‌گیری در شرکت‌های فناوری اغلب شفاف نیست. الگوریتم‌های هوش مصنوعی یا کمیته‌های داخلی که تصمیم می‌گیرند چه محتوایی حذف شود، معمولاً پاسخگو نیستند و معیارهای اعمال‌شده توسط آن‌ها مبهم و تغییرپذیر است. این وضعیت می‌تواند منجر به خودسانسوری کاربران یا حذف اشتباه محتوا شود، به‌ویژه زمانی که زبان، زمینه فرهنگی یا نیت گوینده به‌درستی درک نشود. به همین دلیل، برخی اسناد بین‌المللی بر لزوم شفافیت، سازوکارهای بازنگری و امکان اعتراض کاربران تأکید کرده‌اند.

در پاسخ به این چالش‌ها، رویکردهای مختلفی مطرح شده‌اند. برخی کشورها مانند آلمان با وضع قوانینی[۳۱]، شرکت‌های فناوری را ملزم کرده‌اند که در صورت دریافت گزارش درباره محتوای غیرقانونی ظرف مدت مشخصی آن را بررسی و در صورت لزوم حذف کنند، در غیر این صورت با جریمه‌های سنگین مواجه خواهند شد. این رویکرد باعث نوعی «نظارت خصوصی اجباری» شده که انتقادات زیادی را به همراه داشته است، چرا که شرکت‌ها ممکن است برای پرهیز از مسئولیت، محتوا را بیش از حد حذف کنند. در مقابل، برخی کشورها از جمله ایالات متحده امریکا با استناد به اصل حمایت از آزادی بیان در متمم اول قانون اساسی، هرگونه اجبار مستقیم دولت درباره سانسور محتوا

۳۱- مانند NetzDG

توسط پلتفرم‌ها را محدود کرده‌اند، هرچند در عمل، شرکت‌ها بر اساس سیاست‌های داخلی خود محتوا را حذف یا محدود می‌کنند (Barendt,2005,8).

نکته مهم دیگر، نقش رویه‌های قضایی است. دادگاه‌های داخلی و بین‌المللی در سال‌های اخیر به شکل‌گیری معیارهای دقیق‌تری برای سنجش مشروعیت محدودیت‌ها کمک کرده‌اند. برای مثال، دادگاه اروپایی حقوق بشر در چندین پرونده از جمله پرونده دلفی علیه استونیا[۳۲]، اصولی را برای تعیین مسئولیت واسطه‌ها و میزان مداخله در آزادی بیان کاربران ترسیم کرده است. موازنه میان آزادی بیان و کنترل محتوا نه‌تنها یک مسئله حقوقی، بلکه امری سیاسی، اخلاقی و فناورانه است که نیازمند تحلیل چندبعدی، تدوین سیاست‌های شفاف و سازوکارهای قابل نظارت و بازنگری است. فقدان این موازنه یا غلبه یکجانبه یکی از این ارزش‌ها بر دیگری می‌تواند یا به سرکوب آزادی‌ها منجر شود یا به تضعیف امنیت و اخلاق عمومی (Mowbray,2009,201).

نتیجه

بررسی موضوع مسئولیت کیفری شرکت‌های فناوری در قبال جرایم ارتکابی کاربران نشان می‌دهد که تحقق این مسئولیت صرفاً در شرایطی خاص امکان‌پذیر است. بر اساس مقررات حقوق کیفری ایران و به‌ویژه ماده ۱۴۳ قانون مجازات اسلامی مصوب ۱۳۹۲ که مسئولیت اشخاص حقوقی را به رسمیت شناخته است، انتساب جرم به شرکت‌ها زمانی قابل تصور است که تمامی ارکان قانونی، مادی و روانی موجود باشد. وجود نص قانونی صریح نخستین شرط است، چرا که بدون پذیرش مسئولیت کیفری اشخاص حقوقی در قانون، امکان تعقیب آن‌ها وجود ندارد. از منظر رکن مادی، باید رابطه سببیت میان اقدامات یا ترک فعل شرکت و جرم ارتکابی کاربر اثبات شود؛ این امر ممکن است ناشی از طراحی بستر فنی ناقص، تسهیل ارتکاب جرم، قصور در اعمال نظارت یا عدم رعایت الزامات قانونی باشد.

در بعد روانی نیز احراز سوءنیت سازمانی یا دست‌کم آگاهی و قابلیت پیش‌بینی وقوع جرم

32- Delfi AS v. Estonia

ضرورت دارد و بی‌احتیاطی یا بی‌مبالاتی مدیریتی می‌تواند برای تحقق این شرط کفایت کند. شرکت‌های فناوری ممکن است در جرایم کاربران به‌صورت مستقیم به‌عنوان فاعل اصلی، یا به‌صورت غیرمستقیم به‌عنوان شریک، معاون یا حتی مقصر ناشی از ترک فعل‌شناسایی شوند. این نقش‌ها بسته به میزان کنترل شرکت بر بستر ارائه‌شده و چگونگی ارتباط اقدامات آن با جرم ارتکابی قابل تفکیک خواهد بود. معیارهای عملی و قضایی برای احراز چنین مسئولیتی نیز بر پایه میزان نظارت و کنترل شرکت، رعایت استانداردهای قانونی و فنی، اتخاذ تدابیر پیشگیرانه و واکنشی مناسب و نیز وجود سیاست‌های داخلی کارآمد در زمینه مقابله با جرایم سایبری استوار است.

در نهایت می‌توان گفت مسئولیت کیفری شرکت‌های فناوری مطلق و بی‌قید نیست، بلکه محدود به مواردی است که میان اقدامات یا ترک فعل شرکت و وقوع جرم کاربران ارتباط روشن و اثبات‌شده برقرار باشد. چنین تفسیر و رویکردی هم به تأمین اهداف عدالت کیفری و حمایت از بزه‌دیدگان کمک می‌کند و هم مانع از تحمیل تکالیف غیرمنطقی و بازدارنده بر فعالان حوزه فناوری و نوآوری خواهد شد.

پیشنهاد

در ادامه چند پیشنهاد عملی و راهبردی برای بهبود وضعیت مسئولیت کیفری شرکت‌های فناوری در قبال جرایم ارتکابی کاربران ارائه می‌شود: اول- تدوین و تصویب قوانین خاص و به‌روز که مختص فضای فناوری اطلاعات و شرکت‌های فعال در این حوزه باشد وبه‌طور دقیق ارکان و حدود مسئولیت کیفری آن‌ها را تعیین کند تا ابهامات موجود برطرف شود. دوم- ایجاد سازوکارهای شفاف و قابل نظارت برای مدیریت محتوا در شرکت‌های فناوری، شامل الزام به گزارش‌دهی منظم، راهکارهای بازنگری تصمیمات حذف یا محدودسازی محتوا و تضمین حق اعتراض کاربران. سوم- توسعه استانداردهای فنی و اخلاقی برای الگوریتم‌ها و سیستم‌های خودکار مدیریت محتوا به منظور کاهش خطا و تبعیض در اعمال محدودیت‌ها و افزایش دقت در تشخیص محتوای مجرمانه. چهارم- گسترش

آموزش و آگاهی‌بخشی به مدیران، کارکنان شرکت‌های فناوری و همچنین کاربران درباره حقوق و مسئولیت‌ها به‌ویژه در زمینه جرایم سایبری و محدودیت‌های قانونی. پنجم- استفاده از تجارب بین‌المللی و تطبیق آن‌ها با شرایط داخلی به منظور بهره‌مندی از مدل‌های موفق و جلوگیری از بروز مشکلات ناشی از تقلید ناقص یا نامناسب.

این پیشنهادها می‌توانند زمینه‌ساز تقویت نظام مسئولیت کیفری شرکت‌های فناوری و ارتقاء امنیت و عدالت در فضای دیجیتال باشند.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانتداری در استناد به متون و ارجاعات مقاله تماماً رعایت گردیده است.

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی نگارش یافته است.

منابع

فارسی

- اردبیلی، محمدعلی، ۱۴۰۴، **حقوق جزای عمومی**، جلد اول، چاپ هفتادوهفتم، تهران، انتشارات میزان.
- اردبیلی، محمدعلی، ۱۴۰۴، **حقوق جزای عمومی**، جلد دوم، چاپ شصت و پنجم، تهران، انتشارات میزان.
- السان، مصطفی، ۱۴۰۲، **حقوق تجارت الکترونیکی**، چاپ دهم، تهران، انتشارات سمت.
- برزگرکهنمویی، مسعود، ۱۴۰۳، مسئولیت کیفری مدیران کانال‌ها در شبکه‌های پیام رسان داخلی در برابر نشر محتواهای منافی عفت، **کنفرانس بین‌المللی و ملی مطالعات مدیریت، حسابداری و حقوق**.
- ترخان، علیرضا، ۱۳۹۵، **مقدمات احراز رابطه علیت در حقوق کیفری**، چاپ اول، تهران، انتشارات گیوا.
- ذبیحی‌جامخانه، محسن؛ مهدیار، مجید؛ مشعلی، بهزاد، ۱۳۹۷، **مدیریت شرکت‌ها و سازمان‌های دانش‌بنیان**، چاپ اول، تهران، انتشارات رصد علم.

- رضایی، حسن، ۱۳۹۸، نسبت توسعه فضای سایبر با تحولات در فهم‌های فقهی–حقوقی در ایران امروز، **فصلنامه تحقیق و توسعه در حقوق تطبیقی**، شماره ۴.

- رئیسی، لیلا و قاسم‌زاده‌لیاسی، فلور، ۱۳۹۹، چالش‌های نظام حقوقی ایران در نقض داده‌های شخصی و حریم خصوصی در فضای سایبر، **مجله حقوقی دادگستری**، شماره ۱۱۰.

- شریفی، محسن، ۱۳۹۴، **مسئولیت کیفری اشخاص حقوقی در حقوق ایران و انگلستان**، چاپ اول، تهران، انتشارات میزان.

- شریفی، محسن، ۱۳۹۶، مسئولیت کیفری شرکت‌های تجاری در وضعیت‌های خاص (قبل از ثبت، پس از ادغام و در حال تصفیه)، **فصلنامه پژوهش حقوق کیفری**، شماره ۲۰.

- عالی پور، حسن، ۱۴۰۰، **حقوق کیفری فناوری اطلاعات**، چاپ چهارم، تهران، انتشارات خرسندی.

- عزیزی، امیرمهدی، ۱۳۹۸، **حقوق کیفری جرایم رایانه‌ای**، چاپ سوم، تهران، انتشارات مجد.

- کازرونی، سیدمصطفی، ۱۳۹۵، چالش تطبیق حق آزادی بیان با منع استفاده تروریسم از فضای مجازی، **فصلنامه مطالعات بین‌المللی**، شماره ۴۸.

- مصدق، محمد، ۱۴۰۲، **شرح قانون مجازات اسلامی مصوب ۱۳۹۲ با رویکرد کاربردی**، چاپ پانزدهم، تهران، انتشارات جنگل.

- میری، حمید، ۱۳۹۴، **مسئولیت مدنی ارائه کنندگان خدمات اینترنتی**، چاپ اول، تهران، انتشارات شهر دانش.

لاتین

- Barendt, Eric M., 2005, Freedom of speech. Oxford University Press, 2 Nd Edition.

- Boccon-Gibod, Didier, 2014, Sur la responsabilité pénale des personnes morales, Droit Social 11.

- Buell, Samuel W., 2018, Criminally bad management, Research Handbook on Corporate

Crime and Financial Misdealing. Edward Elgar Publishing.

- De Maglie, Cristina, 2005, Models of corporate criminal liability in comparative law, Wash. U. Global Stud. L. Rev. 4.

- Dreyer, Emmanuel, 2016, Droit pénal spécial.

- Diamantis, Mihailis E., 2015, Corporate criminal minds, Notre Dame L. Rev. 91.

- Mowbray, Alastair, 2009, An examination of the European court of human rights' approach to overruling its previous case law, Human Rights Law Review 9.2.

- Podgor, Ellen S., 2003, Department of Justice guidelines: Balancing discretionary justice, Cornell JL & Pub. Pol'y 13.

- Shleifer, Andrei, 2005, Understanding regulation, European Financial Management 11.4.

- Solove, Daniel J., 2010. Understanding privacy, Harvard university press.

- Watney, Murdoch, 2017, Evaluating Internet Intermediary Responsibility and Liability for Criminal Law and National Security Enforcement, European Conference on Cyber Warfare and Security. Academic Conferences International Limited.

Legal Civilization

ISSN: 2873-1841
ISSN: 2873-1922

No.26- Winter 2026

Analysis of the Issuing Bank's Liability under the Law of Documentary Credits
Homayoun Mafi, Mohsen Raeisi
The Role of Artificial Intelligence in Improving Criminal Investigation Processes and Digital Evidence Analysis in the Iranian Legal System
Amirreza Mahmoudi, Zahra Rahnama
Revisiting Contractual Obligations in Conditions of High Inflation: an Analysis of Adjustment Capacities in Iranian Law
Shima Shakouri, Ghasem Nabizadeh Kebrya
Iranian Criminal Policy Ppathology Regarding the Crimes of Rebellion, Moharebeh and Corruption on Earth in Light of the Concept of National Security and Political Stability of the Country
Ruhollah Sheikhi, Mohammad Momahmoodi
The Framework of Civil Liability Arising from High-Risk Recreational Activities: A Study of Escape Rooms
Rahim Mokhtari, Gholamhossein Keshavarz
Handling Intellectual Property Claims in the Iranian Legal System
Sayyed Mohammadbagher Haghayeghi, Mohammadreza Nasiri, Amirhasan Abolhasani
Criminological Analysis of Crimes in the Field of Cryptocurrencies: A Study of Common Frauds in Iran
Hossein Mahmoudi Tekanloo, Roya Asiaei
Preventive Strategies for the Crime of Rent-Taking in Iran's Criminal Policy with an Emphasis on Criminological Challenges and Gaps
Fazal Movahedi, Hamidreza Konari Zhadeh, Davoud Salmanpour
An Analysis of the Principle of Proportionality Between Crime and Punishment in the Structure of the International Criminal Court
Hasan Pirfalak, Tayebe Ghodrati Siyahmazgi
Agreement Between the Parties to the Contract in Determining the Evidence to Prove the Claim
Habibolah Abdolah Poor, Mahdi Shojayi
Performance of Criminal Courts in Crime Prevention: A Critical Criminology Perspective with Focus on Iran's Judicial System
Iraj Morvati, Naghmeh Farhood
The Responsibility of States for Human Rights Violations by Private Security Companies on Foreign Missions
Mahdi Gharedaqi, Masoud Sarfarazi Saleh
The End of Centralized Governance: an Analysis of the Emergence of Decentralized Governance in the Era of Block chain and Smart Contracts
Hadi Zare, Majid Vaziri
Comparative Analysis of Social Security Compensatory Protection for Bodily Injuries and the Scope of Eligible Victims in Iran and England
Zeinab Tari
Transfer of Lawsuits in the Iranian Legal System with Emphasis on Selected Provisions of the Deeds and Real Estate Registration Law
Amirreza Alitabar
The Position of Artificial Intelligence in the Field of Criminal Policymaking
Mahbobeh Talebi Rostami
Commitment to Data Security as a Commitment to Result or a Commitment to Means in Private Law
Sayyed Amirhasan Mostafavi
Criminal Liability of Technology Companies for Crimes Committed by Users
Vahid Kioumarsi
Civil Liability Arising from Automated Processing of Personal Data by Artificial Intelligence in Iranian and Afghan Law (With a Look at International Documents)
Raziyeh Jafarzade, Vahid Hamidi, Mohammadreza Rashid
The Impact of Legal Awareness and Transparency on the Prevention and Reduction of Administrative and Financial Corruption
Sayyedeh Mahshid Miri Balajorshari
Ownership of Personal Data in Private Rights; from Personality Right to Intangible Property
Sina Youseffi
Civil Liability of the Physician and Robot Manufacturer in Robotic Surgeries: Iranian and English Legal Systems
Ebrahim Shiravanian
an Analysis of the Issue of Receiving Compensation for Delayed Payment from the Convict to the Government
Mohammadmahdi Rezvanifar, Zahra Salimi
Legal and Administrative Effects of Acquisition on the Registered Status of Real Estate in the Iranian Legal System
Ehsaneh Vosoughi Monfared, Mohammad Varaste Bazghale
Economic Diplomacy and the Law of Private International Contracts; The Interaction of Politics and Law in Securing National Interests
Radmehr Rahmani Golafshan
Adoption of Artificial Intelligence-Driven Fraud Detection in Banking: The Role of Trust, Transparency, and Fairness Perception in Financial Institutions in Iran, the United Arab Emirates and Qatar
Abdolmajid Yousefi
Criminology of War in the Current Realities and the Need for its Development in Ukraine
Yasser Shakeri