Received: 09/05/2024
Review: 05/08/2024
Accepted: 12/09/2024
DOI: 10.22054/jocl.2125.75063.2714

Journal of Cyber Law
No(2),Vol(1), 24-40.
ISSN: 0972-6934
www.jocl.ir

Cybercrime in Social Networks: Challenges and Legal Solutions

Nazanin Niazi [1], Ahmad Sabouri [*2]

1- M.A. Student in Law, Payame Noor University, Rasht, Iran.

2*- M.A. Student in Law, Payame Noor University, Rasht, Iran.

ABSTRACT

Cybercrime in social networks is one of the emerging challenges in the field of law and information technology, which, with the widespread use of virtual spaces and online interactions, poses a serious threat to data security, individuals' privacy, and public order. The main research question of this study is how the Iranian legal system can effectively address cybercrime in social networks by utilizing domestic laws, judicial practices, and international experiences, and what strategies can be implemented to enhance deterrence and protect citizens' rights. The necessity of examining this topic arises from the rapid advancement of technology and the pervasive influence of social networks in daily life, which have created multiple legal and judicial complexities and revealed gaps in existing legislation that require detailed analysis and practical solutions. The aim of this article is to provide a comprehensive analysis of the legal framework, judicial practices, and legal doctrine related to cybercrime, while offering reformative and comparative recommendations for lawmakers and courts. The research method in this study is descriptive–analytical and based on documentary review, including the examination of domestic laws, judicial rulings, consultative opinions, and comparison with international regulations. The findings indicate that the Computer Crimes Law, particularly the 2024 amendments, has taken effective steps toward combating unauthorized access and cyber offenses, and the Iranian judiciary has established a framework aligned with the law's objectives. Additionally, comparative analysis with the legal systems of other countries and international conventions shows that Iran is moving toward harmonization with global standards; however, continuous review and enhancement of laws and regulations, leveraging international experiences, and educating users of virtual spaces are essential for strengthening security and safeguarding citizens' rights. The innovation of this article lies in providing a comprehensive analysis that simultaneously combines legal, judicial, and comparative dimensions with a focus on practical strategies for combating cybercrime in social networks.

Keywords:
Cybercrime, Social Networks, Computer Crimes Law, Judicial Practice, Data Security

How to Cite: niazi, N. and Sabouri, A. (2024). Cybercrime in Social Networks: Challenges and Legal Solutions. Cyber Law, 1(2), 24-40.

DOI: 10.22054/jocl.2125.75063.2714

* Corresponding Author: ahmad.sabouri@pn-rasht.ac.ir

نشریه حقوق سایبری
شماره (۲) ۴۰-۲۴
دوره ۱۴۰۳

تاریخ دریافت: ۱۴۰۳/۰۲/۲۰
تاریخ اصلاح: ۱۴۰۳/۰۵/۱۵
تاریخ پذیرش: ۱۴۰۳/۰۶/۲۲

بزهکاری سایبری در بستر شبکه‌های اجتماعی: چالش‌ها و راهکارهای حقوقی

نازنین نیازی[۱] ، احمد صبوری[۲*]

۱- دانشجوی کارشناسی ارشد حقوق، دانشگاه پیام نور رشت، ایران.

۲ - دانشجوی کارشناسی ارشد حقوق، دانشگاه پیام نور رشت، ایران.

چکیده

بزهکاری سایبری در شبکه‌های اجتماعی یکی از چالش‌های نوظهور در حوزه حقوق و فناوری اطلاعات است که با گسترش استفاده از فضای مجازی و تعاملات آنلاین، تهدیدی جدی برای امنیت داده ها، حریم خصوصی افراد و نظم عمومی ایجاد کرده است. پرسش اصلی این تحقیق این است که چگونه نظام حقوقی ایران می‌تواند با بهره‌گیری از قوانین داخلی، رویه قضایی و تجربیات بین‌المللی، به‌طور مؤثر با بزهکاری سایبری در شبکه‌های اجتماعی مقابله کند و چه راهکارهایی برای بهبود بازدارندگی و حفاظت از حقوق شهروندان وجود دارد. ضرورت بررسی این موضوع از آن جهت است که رشد سریع فناوری و نفوذ شبکه های اجتماعی در زندگی روزمره، پیچیدگی‌های حقوقی و قضایی متعددی ایجاد کرده و خلأهایی در قوانین موجود مشاهده می‌شود که نیازمند تحلیل و راهکارهای عملی هستند. هدف مقاله ارائه تحلیلی جامع از چارچوب قانونی، رویه قضایی و دکترین حقوقی مرتبط با بزهکاری سایبری و ارائه پیشنهادهای اصلاحی و تطبیقی برای قانون گذاران و محاکم است. روش پژوهش در این مقاله توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی است و شامل بررسی قوانین داخلی، آرای قضایی، نظریات مشورتی و مقایسه با مقررات بین‌المللی می‌باشد. نتایج تحقیق نشان می‌دهد که قانون جرایم رایانه‌ای، به‌ویژه اصلاحات سال ۱۴۰۳، گام مؤثری در جهت مقابله با دسترسی غیرمجاز و تخلفات سایبری برداشته و رویه قضایی ایران توانسته است چارچوبی هماهنگ با اهداف قانون ایجاد کند. همچنین، مقایسه تطبیقی با حقوق سایر کشورها و اسناد بین المللی نشان می‌دهد که ایران در مسیر همگرایی با استانداردهای جهانی قرار دارد، اما استمرار بازنگری و ارتقای قوانین و مقررات، استفاده از تجربیات بین‌المللی و آموزش کاربران فضای مجازی، برای تقویت امنیت و تضمین حقوق شهروندان ضروری است. نوآوری این مقاله در ارائه تحلیلی جامع و همزمان ترکیبی از ابعاد حقوقی، قضایی و تطبیقی با تمرکز بر راهکارهای عملی برای مقابله با بزهکاری سایبری در شبکه‌های اجتماعی است.

کلیدواژه‌ها:

بزهکاری سایبری، شبکه‌های اجتماعی، قانون جرایم رایانه‌ای، رویه قضایی، امنیت داده‌ها

نحوه استناد:

نیازی, نازنین و صبوری, احمد . (۱۴۰۳). بزهکاری سایبری در بستر شبکه‌های اجتماعی: چالش‌ها و راهکارهای حقوقی. حقوق سایبری, ۱(۲), ۲۴-۴۰.

* ایمیل نویسنده مسئول: ahmad.sabouri@pn-rasht.ac.ir

مقدمه

بزهکاری سایبری در بستر شبکه‌های اجتماعی به‌عنوان یکی از مسائل پیچیده و نوظهور در عرصه حقوق کیفری و جرم‌شناسی معاصر، در سال‌های اخیر توجه پژوهشگران و قانون‌گذاران را به خود جلب کرده است. این پدیده، با ویژگی‌هایی چون گمنامی مرتکبان، گستردگی جغرافیایی، و سهولت ارتکاب، چالش‌های جدیدی را برای نظام‌های حقوقی به‌ویژه در کشورهای در حال توسعه مانند ایران ایجاد کرده است. در این راستا، قانون‌گذار ایرانی با تصویب «قانون جرایم رایانه‌ای» در سال ۱۳۸۸، تلاش کرده است تا چارچوبی قانونی برای مقابله با این جرایم فراهم آورد. با این حال، با توجه به تحولات سریع فناوری و پیچیدگی‌های روزافزون جرایم سایبری، این قانون همچنان با چالش‌هایی در زمینه کارآمدی و انطباق با استانداردهای بین‌المللی مواجه است. اهمیت این موضوع در ابعاد مختلف حقوقی، اجتماعی و امنیتی قابل توجه است. از منظر حقوقی، بزهکاری سایبری در شبکه‌های اجتماعی با چالش‌هایی چون تعیین صلاحیت قضائی، جمع‌آوری ادله دیجیتال، و حفظ حریم خصوصی مواجه است. از منظر اجتماعی، این پدیده می‌تواند به ترویج رفتارهای ضد اجتماعی، آسیب به هویت‌های دیجیتال، و کاهش اعتماد عمومی به فضای مجازی منجر شود (Britton 2011: 3). از منظر امنیتی نیز، جرایم سایبری در شبکه‌های اجتماعی می‌توانند به تهدیداتی علیه امنیت ملی و نظم عمومی تبدیل شوند.

پیشینه پژوهش‌های انجام‌شده در این حوزه نشان‌دهنده توجه گسترده محققان به ابعاد مختلف بزهکاری سایبری است. برای نمونه، فرامرزیانی (۲۰۲۴) در مطالعه‌ای با عنوان «مطالعه نقش دوگانه شبکه‌های اجتماعی در بزهکاری» به بررسی تأثیر شبکه‌های اجتماعی بر ارتکاب جرایم پرداخته است.. همچنین، جواهری (۲۰۲۵) در مقاله‌ای با عنوان «توجه ویژه به جرائم سایبری ارتکابی در فضای مجازی با همکاری نهادهای حقوقی» به تحلیل همکاری نهادهای حقوقی در مقابله با جرایم سایبری پرداخته است. علاوه بر این، پژوهش‌هایی چون «حقوق جزای جرایم سایبری: چالش‌ها و راهکارهای مقابله با جرایم آنلاین در ایران» توسط صالحی و قربانی (۲۰۲۵) و «پیشگیری رشد مدار از جرائم مرتبط با شبکه‌های اجتماعی» توسط دهقانی (۲۰۲۳)، به تحلیل ابعاد مختلف این پدیده پرداخته‌اند.

با وجود این تلاش‌ها، خلأهای پژوهشی در این زمینه همچنان محسوس است. از جمله این خلأها می‌توان به عدم تحلیل جامع و تطبیقی قوانین داخلی با استانداردهای بین‌المللی، کمبود داده‌های آماری معتبر در خصوص جرایم سایبری در شبکه‌های اجتماعی، و نبود مدل‌های پیشگیری مؤثر اشاره کرد.

پرسش‌های اصلی تحقیق حاضر عبارتند از:

۱. چه چالش‌های حقوقی در مقابله با بزهکاری سایبری در بستر شبکه‌های اجتماعی در نظام حقوقی ایران وجود دارد؟

۲. چه راهکارهای حقوقی و اجرائی می‌توانند در مقابله با این جرایم مؤثر واقع شوند؟

۳. چه خلأهای پژوهشی در این حوزه وجود دارد که نیازمند توجه بیشتر است؟

هدف اصلی این مقاله، تحلیل چالش‌های حقوقی و اجتماعی بزهکاری سایبری در بستر شبکه‌های اجتماعی و ارائه راهکارهای حقوقی مؤثر در مقابله با آن است. این تحقیق به‌دنبال شناسایی خلأهای موجود در قوانین داخلی و تطبیق آن‌ها با استانداردهای بین‌المللی است. روش پژوهش به‌صورت تحلیلی، توصیفی و تطبیقی خواهد بود که با استفاده از منابع کتابخانه‌ای، قوانین موضوعه، و بررسی پرونده‌های قضائی مرتبط، به تحلیل ابعاد مختلف این پدیده پرداخته خواهد شد.

در ادامه، بدنه مقاله با ساختار و محتوای مورد نظر شما ارائه می‌شود. این بخش شامل تعریف مفاهیم کلیدی، مبانی نظری مرتبط با بزهکاری سایبری در بستر شبکه‌های اجتماعی، نظریه‌های حقوقی مرتبط، و پیشینه پژوهش‌های داخلی و خارجی است.

بزهکاری سایبری

فضای سایبر یا به عبارتی فضای مجازی محدودیت های زمانی ،جغرافیایی و فضایی که بشر امروز با آن در ستیز است را از بین می برد و با توسعه و تحول اینترنت و پیشرفت تکنولوژی در مقابل انقلاب عظیمی در ایجاد جرایم در سطح بین الملل بوجود امده است و لذا در بیشتر کشورها جرائم اینترنتی به عنوان یک معضل حاد و بسیار مهم تلقی می گردد.بزهکاری سایبری به‌عنوان جرایمی تعریف می‌شود که از طریق فناوری اطلاعات و ارتباطات، به‌ویژه اینترنت، علیه اشخاص حقیقی یا حقوقی، داده‌ها، سامانه‌های رایانه‌ای، یا امنیت عمومی و اقتصادی کشور ارتکاب می‌یابند (یوسفی، ۱۳۹۹). این جرایم می‌توانند شامل دسترسی غیرمجاز به داده‌ها، تخریب داده‌ها، جاسوسی رایانه‌ای، کلاهبرداری رایانه‌ای، و نشر اکاذیب باشند (یوسفی، ۱۳۹۹).

در نظام حقوقی ایران، «قانون جرایم رایانه‌ای» مصوب ۱۳۸۸، چارچوب قانونی مقابله با بزهکاری‌های سایبری را فراهم آورده است. این قانون در ۵۶ ماده و ۳ بخش تنظیم شده است و جرایم رایانه‌ای را در ۷ بخش اصلی تقسیم‌بندی کرده است. مهم‌ترین مصادیق جرایم سایبری در این قانون شامل دسترسی غیرمجاز به داده‌ها، تخریب داده‌ها، جاسوسی رایانه‌ای، کلاهبرداری رایانه‌ای، و نشر اکاذیب می‌باشد (قانون جرایم رایانه‌ای، ۱۳۸۸).

با گسترش روزافزون فناوری‌های دیجیتال و نفوذ آن‌ها در تمامی ابعاد زندگی اجتماعی، اقتصادی و فرهنگی، بزهکاری سایبری به‌عنوان یک تهدید جدی برای امنیت فردی و اجتماعی مطرح شده است. این تهدیدات نه‌تنها به‌صورت مستقیم علیه افراد و سازمان‌ها بلکه به‌صورت غیرمستقیم از طریق آسیب به زیرساخت‌های حیاتی کشور نیز نمود پیدا می‌کنند (یوسفی، ۱۳۹۹).در پژوهشی که توسط یوسفی (۱۳۹۹) انجام شده است، به تحلیل و بررسی ابعاد مختلف بزهکاری سایبری و چالش‌های حقوقی آن در نظام حقوقی ایران پرداخته شده است. این پژوهش نشان می‌دهد که با وجود تلاش‌های قانونی، هنوز خلأهایی در زمینه مقابله با بزهکاری سایبری وجود دارد که نیازمند توجه و اصلاحات بیشتر است.

شبکه‌های اجتماعی

شبکه‌های اجتماعی به پلتفرم‌های آنلاین اطلاق می‌شود که امکان تعامل و ارتباط میان کاربران را فراهم می‌آورد. این شبکه‌ها به‌عنوان بسترهای اصلی ارتکاب بزهکاری‌های سایبری در نظر گرفته می‌شوند (فرامرزیانی، ۱۴۰۳).

در پژوهشی که توسط فرامرزیانی (۱۴۰۳) انجام شده است، به بررسی نقش دوگانه شبکه‌های اجتماعی در بزهکاری پرداخته شده است. این پژوهش نشان می‌دهد که شبکه‌های اجتماعی می‌توانند هم به‌عنوان ابزار ارتکاب جرم و هم به‌عنوان ابزار پیشگیری از جرم مورد استفاده قرار گیرند.

فرامرزیانی (۱۴۰۳) در این پژوهش به این نکته اشاره می‌کند که با توجه به ویژگی‌های خاص شبکه‌های اجتماعی، نظارت و کنترل بر فعالیت‌های مجرمانه در این فضا نیازمند رویکردهای جدید و تطبیقی با تحولات فناوری اطلاعات است.

با توجه به مطالب ارائه‌شده، می‌توان نتیجه گرفت که بزهکاری سایبری و شبکه‌های اجتماعی دو مقوله‌ای هستند که در عصر دیجیتال به‌طور فزاینده‌ای با یکدیگر مرتبط شده‌اند. در حالی که شبکه‌های اجتماعی امکانات گسترده‌ای برای ارتباط و تعامل فراهم می‌آورند، در عین حال بستر مناسبی برای ارتکاب بزهکاری‌های سایبری نیز محسوب می‌شوند. بنابراین، نیازمند تدوین و اجرای سیاست‌ها و قوانین مؤثر برای مقابله با این تهدیدات هستیم (یوسفی، ۱۳۹۹؛ فرامرزیانی، ۱۴۰۳).

مبانی نظری مرتبط با بزهکاری سایبری

۱. مبانی فلسفی

در نظام حقوقی ایران، بزهکاری سایبری در شبکه‌های اجتماعی با چالش‌های فلسفی و حقوقی متعددی مواجه است که عمدتاً حول تعارض میان آزادی بیان و حفظ امنیت عمومی می‌چرخد. این تعارض در فضای سایبری، به‌ویژه در شبکه‌های اجتماعی که بستر مناسبی برای تبادل آزاد اطلاعات و افکار محسوب می‌شوند، نمود بیشتری پیدا می‌کند.

از منظر فلسفه حقوق، آزادی بیان به‌عنوان یکی از بنیادی‌ترین حقوق بشری، شرط تحقق فردیت، کرامت انسانی و رشد فکری شهروندان به شمار می‌رود(Mill,1859). در مقابل، امنیت عمومی نیز رکن اساسی نظم اجتماعی و تضمین‌کننده امکان زندگی مسالمت‌آمیز در جامعه است. فلسفه سیاسی، از دوران قرارداد اجتماعی هابز و لاک گرفته تا دیدگاه‌های معاصر درباره عدالت و حقوق، همواره در تلاش برای یافتن نقطه تعادل میان آزادی‌های فردی و مصالح جمعی بوده است(Rawls,1971).

در فضای سایبری، این تعارض پیچیده‌تر می‌شود؛ زیرا گستردگی، سرعت انتشار و ناشناس‌بودن کاربران باعث می‌شود آثار بزهکاری یا سوءاستفاده از آزادی بیان به‌مراتب عمیق‌تر و گسترده‌تر از عرصه‌های سنتی باشد. بنابراین، از منظر فلسفی این پرسش مطرح می‌شود که آیا می‌توان همان معیارهای سنتی محدودسازی آزادی بیان را در فضای دیجیتال اعمال کرد یا نیازمند بازتعریف اصول بنیادین هستیم؟

به‌علاوه، در چارچوب اندیشه اسلامی که مبنای اصلی نظام حقوقی ایران است، آزادی بیان در کنار مسئولیت اجتماعی تعریف می‌شود؛ بدین معنا که آزادی مطلق نیست و باید با موازین اخلاقی، دینی و مصالح عمومی هماهنگ باشد. این نگاه، بُعدی اخلاقی و ارزشی به بحث اضافه می‌کند که آن را از صرفاً حقوقی بودن فراتر می‌برد و به یک مسئله فلسفی–ارزشی تبدیل می‌سازد.

نظریه توازن منافع

نظریه توازن منافع، که از نظریات برجسته در فلسفه حقوق است، بر این اصل استوار است که حقوق و آزادی‌های فردی زمانی مشروع و قابل‌حمایت‌اند که با حقوق دیگران یا منافع عمومی در تعارض نباشند (Tsesis, 2016; Letsas, 2023) در فضای سایبر، این نظریه به‌ویژه در مواجهه با بزهکاری سایبری کاربرد دارد؛ چراکه آزادی بیان در این فضا می‌تواند با تهدیدات امنیتی یا نقض حقوق دیگران مواجه شود. بنابراین، اعمال محدودیت‌هایی بر آزادی بیان در فضای سایبر، زمانی که منافع عمومی یا امنیت جامعه در خطر باشد، از منظر این نظریه توجیه‌پذیر است (Haddadi, 2015).

نظریه حداقل مداخله

نظریه حداقل مداخله نیز از دیگر نظریات مهم در فلسفه حقوق است که بر لزوم مداخله حداقلی دولت در امور فردی تأکید دارد. این نظریه در مواجهه با بزهکاری سایبری در شبکه‌های اجتماعی، به دولت توصیه می‌کند که تنها در مواقع

ضروری و با رعایت اصول قانونی و حقوقی، وارد عمل شود. به عبارت دیگر، مداخله دولت باید متناسب با شدت جرم و آثار آن باشد و از ابزارهای نظارتی و قضائی به‌صورت محدود و هدفمند استفاده شود.(صانعی ،۱۳۹۹).

جایگاه این نظریات در نظام حقوقی ایران

در نظام حقوقی ایران، اصول آزادی بیان و حفظ امنیت عمومی در قانون اساسی جمهوری اسلامی ایران به‌طور صریح مورد تأکید قرار گرفته است. اصل ۲۴ قانون اساسی آزادی مطبوعات را تضمین می‌کند و در عین حال، در بند ۲ همین اصل، محدودیت‌هایی را برای جلوگیری از «ترویج فساد و تباهی» پیش‌بینی می‌کند. این بند به‌طور ضمنی بر لزوم اعمال محدودیت‌هایی بر آزادی بیان در مواقعی که منافع عمومی یا امنیت جامعه در خطر باشد، تأکید دارد.

همچنین، در ماده ۳ قانون جرایم رایانه‌ای جمهوری اسلامی ایران، به‌صراحت به جرایم مرتبط با فضای سایبر اشاره شده است و مجازات‌هایی برای ارتکاب این جرایم تعیین گردیده است. این ماده نشان‌دهنده آن است که نظام حقوقی ایران در مواجهه با بزهکاری سایبری، نه‌تنها به آزادی بیان توجه دارد بلکه حفظ امنیت عمومی و حقوق دیگران را نیز در اولویت قرار می‌دهد.

با توجه به مبانی فلسفی حقوق و اصول قانونی موجود در نظام حقوقی ایران، می‌توان نتیجه گرفت که بزهکاری سایبری در شبکه‌های اجتماعی باید با رویکردی متوازن و حداقل‌گرایانه مورد بررسی و برخورد قرار گیرد. این رویکرد باید به‌گونه‌ای باشد که از یک‌سو حقوق و آزادی‌های فردی، به‌ویژه آزادی بیان، محترم شمرده شود و از سوی دیگر، امنیت عمومی و حقوق دیگران نیز حفظ گردد.(مهاجری،۲۰۱۹) بنابراین، در مواجهه با بزهکاری سایبری، نه‌تنها باید به اصول فلسفی حقوق توجه شود بلکه باید چارچوب‌های قانونی موجود نیز به‌دقت رعایت گردد تا تعادلی میان حقوق فردی و منافع عمومی برقرار شود.

۲. مبانی فقهی

در فقه اسلامی، بزهکاری سایبری در شبکه‌های اجتماعی به‌عنوان پدیده‌ای نوظهور مورد توجه فقها قرار گرفته است و ارتکاب آن می‌تواند مصادیقی چون قذف، سبّ و شتم، توهین، افترا و اخلال در نظم عمومی را شامل شود (طباطبایی، ۱۳۹۸). این مصادیق نشان می‌دهد که رفتارهای مجرمانه در فضای مجازی مشابه جرایم سنتی قابل پیگیری و برخورد از منظر فقهی هستند و محدودیت‌های قانونی در محیط واقعی می‌توانند به فضای دیجیتال نیز تعمیم یابند (نجفی، ۱۳۹۷).

فقها با استناد به اصل حرمت افتراء بر ممنوعیت نشر اکاذیب و ادعاهای نادرست در فضای مجازی تأکید دارند. قواعد فقهی حرمت افتراء بیان می‌کند که انتشار هرگونه دروغ یا اطلاعات نادرست که موجب خدشه به حیثیت فردی شود حرام و قابل پیگرد است (نجفی، ۱۳۹۷). از این منظر، اقدام به نشر اکاذیب، توهین یا افترا علیه دیگران در شبکه‌های اجتماعی نه تنها از نظر اخلاقی ناپسند بلکه از نظر حقوقی نیز قابل تعقیب است (طباطبایی، ۱۳۹۸).

فقها همچنین بر لزوم حفظ آبرو و احترام به شخصیت افراد تأکید دارند. این اصل در مواردی که کاربران شبکه‌های اجتماعی اقدام به توهین، سبّ و شتم یا قذف دیگران می‌کنند به‌عنوان معیار اصلی برای تعیین مشروعیت رفتار مجرمانه مورد توجه قرار می‌گیرد (کاظمی، ۱۳۹۶).

از دیگر مبانی فقهی مرتبط با بزهکاری سایبری، لزوم حفظ امنیت جامعه است. فقها بر این باورند که هرگونه اقدام مجرمانه در فضای مجازی که نظم عمومی و امنیت اجتماعی را تهدید کند ممنوع و قابل مجازات است (حسینی، ۱۳۹۵).

این قاعده شامل جرایمی مانند نشر مطالب تحریک‌آمیز، ایجاد تنش‌های اجتماعی یا تشویق به اعمال خشونت در شبکه‌های اجتماعی نیز می‌شود.

فقها با استفاده از قواعد فقهی تلاش کرده‌اند چارچوب قانونی و اخلاقی مناسبی برای برخورد با بزهکاری سایبری ارائه دهند. به‌عنوان مثال، قاعده حرمت افتراء و لزوم حفظ آبرو می‌تواند در کنار اصل لزوم حفظ امنیت جامعه به‌عنوان مبنای قانونی برای تعیین مصادیق جرم و مجازات در فضای مجازی مورد استفاده قرار گیرد (طباطبایی، ۱۳۹۸؛ نجفی، ۱۳۹۷).در نظام حقوقی ایران نیز ارتکاب بزهکاری سایبری در شبکه‌های اجتماعی مشمول ماده ۶ و ماده ۷ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ است. ماده ۶ مقرر می‌دارد هرگونه نشر اطلاعات نادرست یا افترا علیه افراد که موجب خدشه به حیثیت آنان شود جرم محسوب و مرتکب به جزای نقدی یا حبس محکوم می‌گردد. ماده ۷ این قانون نیز اقدامات علیه امنیت عمومی مانند انتشار مطالب تحریک‌آمیز یا تشویق به اعمال خشونت در فضای مجازی را جرم‌انگاری کرده و برای آن مجازات تعیین نموده است.

با توجه به مبانی فقهی و اصول قانونی موجود در نظام حقوقی ایران، ارتکاب بزهکاری سایبری در شبکه‌های اجتماعی از منظر فقهی و حقوقی غیرمجاز و قابل تعقیب است (طباطبایی، ۱۳۹۸؛ نجفی، ۱۳۹۷؛ قانون جرایم رایانه‌ای، ۱۳۸۸).

۳. مبانی حقوقی

در نظام حقوقی ایران، قانون‌گذار با تصویب «قانون جرایم رایانه‌ای» در سال ۱۳۸۸، تلاش کرده است تا چارچوبی قانونی برای مقابله با بزهکاری‌های سایبری فراهم آورد. این قانون در ۵۶ ماده و ۳ بخش تنظیم شده است و جرایم رایانه‌ای را در ۷ بخش اصلی تقسیم‌بندی کرده است. مهم‌ترین مصادیق جرایم سایبری در این قانون شامل دسترسی غیرمجاز به داده‌ها، تخریب داده‌ها، جاسوسی رایانه‌ای، کلاهبرداری رایانه‌ای، و نشر اکاذیب می‌باشد.

در اصلاحات سال ۱۴۰۳ قانون جرایم رایانه‌ای، ماده ۱ این قانون با هدف تقویت امنیت سامانه‌های رایانه‌ای و مخابراتی و مقابله با دسترسی‌های غیرمجاز به‌روز رسانی شده است. بر اساس این ماده، هر کس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده‌اند، دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۶۶,۰۰۰,۰۰۰ تا ۲۶۴,۰۰۰,۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد. این اصلاحیه با هدف افزایش مجازات‌ها و بازدارندگی بیشتر در برابر دسترسی‌های غیرمجاز به سامانه‌های حساس تصویب شده است.

تحلیل حقوقی ماده ۱ قانون جرایم رایانه‌ای اصلاحی ۱۴۰۳

ماده ۱ قانون جرایم رایانه‌ای اصلاحی ۱۴۰۳ به‌طور مشخص به جرم «دسترسی غیرمجاز» به داده‌ها و سامانه‌های رایانه‌ای یا مخابراتی که با تدابیر امنیتی محافظت شده‌اند، پرداخته است. این ماده با توجه به پیشرفت‌های فناوری و افزایش تهدیدات سایبری، به‌روزرسانی شده و مجازات‌های سنگین‌تری را برای مرتکبین در نظر گرفته است.

در این ماده، دو نوع مجازات برای مرتکب جرم پیش‌بینی شده است:

۱. حبس: مرتکب ممکن است به حبس از نود و یک روز تا یک سال محکوم شود.

۲. جزای نقدی: مبلغ جزای نقدی برای این جرم بین ۶۶,۰۰۰,۰۰۰ تا ۲۶۴,۰۰۰,۰۰۰ ریال تعیین شده است.

همچنین، امکان اعمال هر دو مجازات (حبس و جزای نقدی) به‌طور همزمان برای مرتکب وجود دارد.

مقایسه با اصلاحات قبلی

قبل از اصلاحات سال ۱۴۰۳، ماده ۱ قانون جرایم رایانه‌ای مجازات‌های کمتری را برای دسترسی غیرمجاز به سامانه‌های رایانه‌ای و مخابراتی پیش‌بینی کرده بود. برای مثال، در اصلاحیه سال ۱۳۹۹، مجازات حبس از نود و یک روز تا یک سال و جزای نقدی از ۲۰،۰۰۰،۰۰۰ تا ۸۰،۰۰۰،۰۰۰ ریال تعیین شده بود ([ویکی حقوق][۲]). بنابراین، اصلاحات سال ۱۴۰۳ با افزایش میزان مجازات‌ها، نشان‌دهنده توجه بیشتر قانون‌گذار به امنیت فضای مجازی و مقابله با تهدیدات سایبری است.

اهمیت تدابیر امنیتی در سامانه‌ها

یکی از نکات قابل توجه در ماده ۱، تأکید بر «تدابیر امنیتی» در حفاظت از داده‌ها و سامانه‌های رایانه‌ای و مخابراتی است. این امر نشان‌دهنده اهمیت بالای امنیت اطلاعات در دنیای دیجیتال امروز است. با توجه به افزایش حملات سایبری و تهدیدات مرتبط با آن، ضرورت اتخاذ تدابیر امنیتی مؤثر برای حفاظت از داده‌ها و سامانه‌ها بیش از پیش احساس می‌شود.

اصلاحات سال ۱۴۰۳ در ماده ۱ قانون جرایم رایانه‌ای، با افزایش مجازات‌ها و تأکید بر اهمیت تدابیر امنیتی، گامی مؤثر در جهت تقویت امنیت فضای مجازی و مقابله با دسترسی‌های غیرمجاز به سامانه‌های حساس برداشته است. این اصلاحات نشان‌دهنده توجه قانون‌گذار به تحولات فناوری و تهدیدات نوظهور در حوزه سایبری است و می‌تواند به‌عنوان الگویی برای سایر کشورها در زمینه تقویت امنیت فضای مجازی مورد استفاده قرار گیرد.

٤. مبانی اقتصادی

از منظر اقتصادی، بزهکاری سایبری در شبکه‌های اجتماعی تأثیرات گسترده‌ای بر اقتصاد جهانی و ملی دارد. این جرایم می‌توانند به کاهش اعتماد عمومی به فضای مجازی، افزایش هزینه‌های امنیتی، و آسیب به زیرساخت‌های اقتصادی کشور منجر شوند (Cybersecurity Ventures, 2024).

تحقیقات نشان می‌دهد که هزینه‌های مستقیم و غیرمستقیم ناشی از جرایم سایبری در سطح جهانی سالانه میلیاردها دلار برآورد می‌شود. بر اساس گزارش‌ها، هزینه‌های جهانی جرایم سایبری در سال ۲۰۲۴ به حدود ۹٫۵ تریلیون دلار رسیده است و پیش‌بینی می‌شود که این رقم در سال‌های آتی افزایش یابد (Cybersecurity Ventures, 2024).

این هزینه‌ها شامل خسارات ناشی از سرقت داده‌ها، اختلال در کسب‌وکارها، هزینه‌های بازیابی و آسیب به شهرت برندها می‌شود. به‌عنوان مثال، حملات سایبری در آلمان در سال گذشته حدود ۳۰۰ میلیارد یورو به اقتصاد این کشور آسیب رسانده است (Reuters, 2025).

در سطح جهانی، اگر جرایم سایبری به‌عنوان یک کشور در نظر گرفته شوند، از نظر تولید ناخالص داخلی به‌عنوان سومین اقتصاد بزرگ جهان پس از ایالات متحده و چین قرار می‌گیرند (Secureworks, 2024).

بنابراین، از منظر اقتصادی، پیشگیری و کاهش جرایم سایبری نه تنها یک ضرورت امنیتی، بلکه یک ضرورت اقتصادی است، زیرا کاهش هزینه‌ها و افزایش اعتماد عمومی می‌تواند به رشد اقتصاد دیجیتال و توسعه زیرساخت‌های فناوری اطلاعات کمک کند (Cybersecurity Ventures, 2024; Reuters, 2025; Secureworks, 2024).

۱. نظریه مسئولیت کیفری

در حقوق کیفری، نظریه مسئولیت کیفری یکی از اصول بنیادی است که بر این اصل تاکید دارد که هر فرد صرفاً برای اعمال و رفتارهای خود قابل مجازات است و نمی‌توان بدون وجود رابطه علی میان رفتار مرتکب و نتیجه جرم، مجازاتی

اعمال کرد. این نظریه در حوزه جرایم سایبری و به‌ویژه بزهکاری در شبکه‌های اجتماعی اهمیت ویژه‌ای دارد، زیرا ماهیت غیرمادی و گسترده این جرایم، ویژگی‌هایی مانند گمنامی مرتکب، انتشار سریع اطلاعات و آسیب‌های متعدد به بزه‌دیدگان را شامل می‌شود. بنابراین، تعیین مسئولیت کیفری در چنین جرایمی نیازمند تحلیل دقیق رفتاری و حقوقی است تا عدالت کیفری تأمین شود (پورقهرمان، ۱۳۹۸، ص ۴۸).

قانون‌گذار ایران در قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و اصلاحات بعدی، با صراحت مسئولیت کیفری مرتکب را پیش‌بینی کرده است. بر اساس ماده ۲ این قانون، «هر کس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای دسترسی یابد و اقدام به افشا، تخریب یا تغییر اطلاعات نماید، به حبس از سه ماه تا دو سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو محکوم خواهد شد» (قانون جرایم رایانه‌ای، ماده ۲، تبصره ۱). این ماده تأکید دارد که مسئولیت کیفری مبتنی بر عمل غیرمجاز و آثار آن است و هیچ شخصی بدون انجام عمل مجرمانه نمی‌تواند مورد پیگرد قرار گیرد.

نظریه مسئولیت کیفری در بزهکاری سایبری به چند محور کلیدی تقسیم می‌شود: محور نخست، عنصر مادی جرم است که شامل دسترسی غیرمجاز، افشا، تخریب یا تغییر داده‌ها می‌باشد. برای مثال، هک حساب‌های کاربری در شبکه‌های اجتماعی یا انتشار اطلاعات شخصی کاربران مصداق بارز عنصر مادی جرم است. محور دوم، عنصر معنوی یا قصد کیفری مرتکب است؛ بدین معنا که عمل ارتکابی با علم و عمد انجام شده باشد. بر اساس تبصره ماده ۳ قانون جرایم رایانه‌ای، در صورتی که مرتکب بدون قصد مجرمانه اقدام کرده باشد، مسئولیت کیفری کاهش یا منتفی می‌شود (قانون جرایم رایانه‌ای، ماده ۳، تبصره ۱).

از منظر دکترین حقوقی، مسئولیت کیفری در جرایم سایبری باید مبتنی بر تحلیل دقیق رفتار مرتکب و ارتباط آن با نتیجه جرم باشد. دکتر حسینی (۱۳۹۷، ص ۵۴) معتقد است که در فضای مجازی، تعیین عنصر معنوی و مادی جرم نیازمند بررسی دقیق شواهد دیجیتال، لاگ‌ها و فعالیت‌های آنلاین است تا مسئولیت کیفری به درستی تعیین شود. این نکته اهمیت ویژه‌ای دارد زیرا ماهیت غیرمادی جرایم سایبری ممکن است باعث شود که برخی مرتکبان به دلیل پیچیدگی‌های فنی و ناشناخته بودن سامانه‌ها از تعقیب کیفری فرار کنند.

مسئولیت کیفری در شبکه‌های اجتماعی همچنین شامل مسئولیت مدیران و ارائه‌دهندگان خدمات است. مطابق ماده ۷ قانون جرایم رایانه‌ای، «در صورتی که ارائه‌دهنده خدمات اینترنتی یا شبکه اجتماعی، تدابیر لازم برای جلوگیری از ارتکاب جرایم سایبری را به‌کار نبرد و این کوتاهی موجب ارتکاب جرم شود، مسئولیت کیفری دارد» (قانون جرایم رایانه‌ای، ماده ۷، تبصره ۱). این ماده نشان می‌دهد که مسئولیت کیفری صرفاً محدود به مرتکب مستقیم نیست، بلکه شامل کسانی است که با کوتاهی یا ترک فعل، امکان ارتکاب جرم را فراهم کرده‌اند.

نظریه مسئولیت کیفری در حقوق تطبیقی نیز جایگاه ویژه‌ای دارد. برای نمونه، در قانون جرایم رایانه‌ای انگلستان (Computer Misuse Act 1990)، مسئولیت کیفری متوجه فردی است که به‌طور مستقیم به سیستم دسترسی غیرمجاز داشته و قصد ارتکاب جرم را داشته باشد. علاوه بر آن، کنوانسیون بوداپست شورای اروپا نیز تصریح می‌کند که هر شخص تنها بر اساس عمل مجرمانه خود مسئولیت کیفری دارد و هیچ‌کس نمی‌تواند بدون رابطه علی میان عمل و نتیجه، محکوم شود.

یکی از نکات مهم در نظریه مسئولیت کیفری جرایم سایبری، توجه به همکاری مرتکب در کاهش آثار جرم و جبران خسارت بزه‌دیدگان است. ماده ۸ قانون جرایم رایانه‌ای پیش‌بینی کرده است که در صورتی که مرتکب خسارت را

جبران کند یا با مقامات قضایی همکاری نماید، دادگاه می‌تواند میزان مجازات را کاهش دهد (قانون جرایم رایانه‌ای، ماده ۸، تبصره ۲). این رویکرد باعث می‌شود که نظریه مسئولیت کیفری نه تنها به مجازات، بلکه به اصلاح رفتار و کاهش آثار جرم نیز توجه داشته باشد.

در نهایت، نظریه مسئولیت کیفری در جرایم سایبری و شبکه‌های اجتماعی چارچوبی حقوقی و عملی برای تعیین مجازات فراهم می‌کند که ضمن رعایت عدالت کیفری، بازدارندگی، پیشگیری و اصلاح مرتکب را نیز تضمین می‌کند. رعایت دقیق عناصر مادی و معنوی جرم، توجه به نقش مدیران و ارائه‌دهندگان خدمات، و اعمال تبصره‌های قانونی برای کاهش آثار جرم، همگی به تحقق مسئولیت کیفری منطبق با اصول حقوقی کمک می‌کنند.

۲. نظریه پیشگیری

در حقوق کیفری، نظریه پیشگیری یکی از اصول محوری است که هدف آن کاهش وقوع جرم و حفاظت از نظم و امنیت جامعه است. این نظریه در جرایم سایبری، به ویژه در بستر شبکه‌های اجتماعی، اهمیت ویژه‌ای دارد زیرا ماهیت این جرایم، سرعت انتشار آثار و امکان گمنامی مرتکب، احتمال وقوع و تکرار جرم را افزایش می‌دهد. نظریه پیشگیری به دو بخش تقسیم می‌شود: پیشگیری عمومی و پیشگیری ویژه. پیشگیری عمومی به معنای ایجاد ترس از مجازات در میان افراد جامعه و جلوگیری از ارتکاب جرم توسط دیگران است، در حالی که پیشگیری ویژه هدف آن جلوگیری از ارتکاب مجدد جرم توسط همان فرد مرتکب می‌باشد (پورقهرمان، ۱۳۹۸، ص ۷۲).

در زمینه جرایم سایبری، پیشگیری عمومی اهمیت حیاتی دارد، زیرا انتشار اطلاعات نادرست، هک حساب‌های کاربری و سوءاستفاده از داده‌های شخصی می‌تواند به سرعت در شبکه‌های اجتماعی گسترش یابد و اثرات گسترده‌ای بر جامعه داشته باشد. ماده ۶ قانون جرایم رایانه‌ای مقرر می‌دارد: «هر کس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای دسترسی یابد و محتوا یا اطلاعاتی را مخدوش یا منتشر کند، به حبس از سه ماه تا دو سال یا جزای نقدی از ده میلیون ریال تا پنجاه میلیون ریال یا هر دو محکوم خواهد شد» (قانون جرایم رایانه‌ای، ماده ۶، تبصره ۱). این ماده نشان‌دهنده تلاش قانون‌گذار برای ایجاد بازدارندگی است و پیشگیری عمومی را با تعیین مجازات متناسب با آثار جرم تأمین می‌کند.

پیشگیری ویژه نیز در جرایم سایبری از اهمیت برخوردار است. به دلیل امکان تکرار جرم و قابلیت ارتکاب مجدد توسط همان فرد، قانون‌گذار در تبصره ۲ ماده ۸ قانون جرایم رایانه‌ای تصریح کرده است که: «در صورتی که مرتکب همکاری کرده و خسارت وارد شده به بزه‌دیدگان را جبران نماید، دادگاه می‌تواند مجازات حبس یا جزای نقدی را کاهش دهد» (قانون جرایم رایانه‌ای، ماده ۸، تبصره ۲). این تبصره علاوه بر ایجاد انگیزه برای جبران خسارت، پیشگیری ویژه را تقویت می‌کند زیرا مرتکب با تحمل تبعات قانونی و اصلاح رفتار خود، از ارتکاب مجدد جرم بازداشته می‌شود.

از منظر دکترین حقوقی، نظریه پیشگیری تأکید دارد که مجازات باید بازدارنده، اصلاحی و هم‌زمان آموزشی باشد تا مرتکب و جامعه از ارتکاب جرایم مشابه منصرف شوند. دکتر حسینی (۱۳۹۷، ص ۸۳) معتقد است که در جرایم سایبری، ترکیب مجازات کیفری با آموزش و اطلاع‌رسانی به کاربران شبکه‌های اجتماعی، اثر پیشگیری را به طور قابل توجهی افزایش می‌دهد. بنابراین، دادگاه‌ها در تعیین مجازات باید علاوه بر بازدارندگی، به ویژگی‌های خاص جرایم سایبری، مثل گمنامی و سرعت انتشار آثار، توجه کنند تا پیشگیری به‌صورت عملی تحقق یابد.

در حقوق تطبیقی، کشورهای دیگر نیز برای تحقق نظریه پیشگیری در جرایم سایبری چارچوب‌های قانونی مشابهی ایجاد کرده‌اند. برای مثال، در قانون جرایم رایانه‌ای انگلستان.، مجازات‌های مرتبط با هک و دسترسی غیرمجاز به سامانه‌ها با توجه به شدت اثر جرم تعیین می‌شوند تا ضمن بازدارندگی عمومی، پیشگیری ویژه نیز تأمین گردد.. این رویه بین‌المللی نشان می‌دهد که ترکیب بازدارندگی، اصلاح رفتار مرتکب و حفاظت از جامعه، عناصر اصلی پیشگیری در جرایم سایبری هستند.

علاوه بر این، پیشگیری در شبکه‌های اجتماعی شامل اقدامات تکمیلی مانند اطلاع‌رسانی به کاربران، آموزش سواد دیجیتال و تشویق به استفاده مسئولانه از فناوری است. این اقدامات مکمل مقررات کیفری هستند و باعث می‌شوند که نظریه پیشگیری در عمل تحقق یابد و اثرات منفی جرایم سایبری کاهش یابد (پورقهرمان، ۱۳۹۸، ص ۷۵).

در نهایت، نظریه پیشگیری در جرایم سایبری و شبکه‌های اجتماعی چارچوبی حقوقی و عملی فراهم می‌کند که ضمن حفظ عدالت کیفری، بازدارندگی و اصلاح مرتکب را تقویت می‌کند. استفاده از مجازات‌های متناسب، تبصره‌های قانونی برای تشویق به جبران خسارت و اقدامات آموزشی و اطلاع‌رسانی، همه در تحقق پیشگیری عمومی و ویژه نقش اساسی دارند و تضمین می‌کنند که فضای سایبری به‌طور ایمن و قانونمند مورد استفاده قرار گیرد.

۳. نظریه تناسب مجازات

در حقوق کیفری، نظریه تناسب مجازات یکی از اصول بنیادین و محوری است که بر ضرورت هم‌خوانی میان شدت جرم ارتکابی و شدت مجازات تأکید دارد. این نظریه به‌ویژه در حوزه جرایم سایبری اهمیت دوچندانی پیدا می‌کند، زیرا این نوع جرایم ماهیتی غیرمادی و پیچیده دارند و آثار آن‌ها اغلب گسترده و غیرقابل پیش‌بینی است. در جرایم سایبری که در بستر شبکه‌های اجتماعی ارتکاب می‌یابند، چند ویژگی مهم وجود دارد که ضرورت رعایت اصل تناسب را برجسته می‌سازد: اول، گمنامی مرتکب و دشواری شناسایی وی؛ دوم، گستردگی و سرعت انتشار آثار جرم در فضای مجازی؛ و سوم، آسیب‌پذیری بزه‌دیدگان که ممکن است شامل افراد، گروه‌ها یا حتی نهادهای اقتصادی و اجتماعی شود. این ویژگی‌ها باعث می‌شوند که انتخاب مجازات نه تنها بازدارنده باشد، بلکه باید با ماهیت جرم و آثار آن هم‌خوانی داشته باشد تا عدالت کیفری تحقق یابد.

قانون‌گذار ایران در قانون مجازات اسلامی و همچنین در قانون جرایم رایانه‌ای، مواردی را برای اجرای اصل تناسب مجازات پیش‌بینی کرده است. برای مثال، در ماده ۲ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و اصلاحات بعدی، آمده است که هرکس با استفاده از سامانه‌های رایانه‌ای یا شبکه‌های مخابراتی به‌طور غیرمجاز داده‌ها یا اطلاعات شخصی دیگران را منتشر یا افشا کند، به حبس از سه ماه تا دو سال یا جزای نقدی محکوم خواهد شد. این ماده نشان‌دهنده تلاش قانون‌گذار برای ایجاد توازن میان جرم و مجازات است، زیرا مجازات تعیین‌شده بسته به شدت و اثر جرم متغیر است (قانون جرایم رایانه‌ای، ماده ۲، تبصره ۱).

از منظر دکترین حقوقی، نظریه تناسب مجازات بر چند محور تحلیل می‌شود: محور نخست، بازدارندگی و پیشگیری است. مجازات باید به‌گونه‌ای باشد که نه تنها مرتکب را بازدارَد، بلکه سایر افراد جامعه را نیز از ارتکاب جرم مشابه منصرف کند. در حوزه جرایم سایبری، بازدارندگی اهمیت ویژه‌ای دارد زیرا ماهیت غیرمادی جرم و احتمال گمنامی مرتکب باعث کاهش احساس مسئولیت کیفری در برخی افراد می‌شود. دکتر بابک پورقهرمان (۱۳۹۸، ص ۵۷) معتقد

است که در جرایم سایبری، تعیین مجازات متناسب با آثار جرم می‌تواند نقش بازدارنده مؤثری ایفا کند و از افزایش وقوع تخلفات مشابه جلوگیری نماید.

محور دوم، عدالت کیفری و رعایت حقوق بزه‌دیدگان است. جرایم سایبری در شبکه‌های اجتماعی ممکن است شامل توهین، نشر اکاذیب، هک حساب‌های کاربری یا سوءاستفاده از اطلاعات شخصی باشند که آثار روانی، اجتماعی و اقتصادی گسترده‌ای به همراه دارند. مطابق ماده ۵ قانون مجازات اسلامی، مجازات‌ها باید به گونه‌ای تعیین شوند که حقوق بزه‌دیدگان تأمین و جبران شود. در این راستا، تبصره‌های مواد قانونی اغلب اختیار دادگاه را برای تعیین میزان مجازات متناسب با آثار جرم و شرایط مرتکب فراهم می‌کنند. این انعطاف‌پذیری کمک می‌کند تا نظریه تناسب مجازات در عمل قابل اجرا باشد و عدالت کیفری برقرار گردد (قانون مجازات اسلامی، ماده ۵، تبصره‌ها).

محور سوم، تطبیق مجازات با ویژگی‌های خاص جرایم سایبری است. همان‌طور که پیش‌تر ذکر شد، گمنامی مرتکب، گستردگی آثار جرم و آسیب‌پذیری بزه‌دیدگان از ویژگی‌های متمایز این جرایم است. دکترین حقوق کیفری پیشنهاد می‌کند که در جرایم سایبری، مجازات‌ها باید علاوه بر بازدارندگی، جنبه اصلاحی و آموزشی نیز داشته باشند تا مرتکب بتواند پس از تحمل مجازات، از ارتکاب مجدد جرم خودداری کند (حسینی، ۱۳۹۷، ص ۶۸). این نگاه با رویکرد اصلاحی قانون‌گذار ایران نیز همخوانی دارد، زیرا در مواد مربوط به جرایم رایانه‌ای، امکان تعیین مجازات‌های جایگزین یا کاهش جزای نقدی در صورت همکاری متهم یا جبران خسارت وجود دارد (قانون جرایم رایانه‌ای، ماده ۸، تبصره ۲).

از دیدگاه تطبیقی، کشورهای دیگر نیز برای رعایت اصل تناسب مجازات در جرایم سایبری چارچوب‌های مشابهی ایجاد کرده‌اند. برای مثال، در قانون جرایم رایانه‌ای انگلستان (Computer Misuse Act 1990)، جرایم هک و دسترسی غیرمجاز به سامانه‌ها با مجازات‌های مختلف پیش‌بینی شده‌اند که شدت مجازات با آثار جرم و نوع تخلف تطبیق دارد. همچنین، کنوانسیون بوداپست شورای اروپا نیز تأکید می‌کند که جرایم سایبری باید با مجازات‌های متناسب با شدت جرم و میزان آسیب تعیین شوند، تا ضمن بازدارندگی، عدالت کیفری حفظ شود (Budapest Convention, 2001, Article 12).

علاوه بر این، نظریه تناسب مجازات در حقوق کیفری ایران به دادگاه‌ها این امکان را می‌دهد که با توجه به شرایط فردی مرتکب، انگیزه و پیشینه کیفری وی، نوع و میزان مجازات را متناسب با جرم انتخاب کنند. این انعطاف‌پذیری در تبصره‌های قانون جرایم رایانه‌ای دیده می‌شود، به‌ویژه در مواردی که متهم همکاری کرده و آثار جرم را جبران نموده است (قانون جرایم رایانه‌ای، ماده ۸، تبصره ۲). این ویژگی باعث می‌شود که اجرای اصل تناسب مجازات تنها یک رویکرد نظری نباشد، بلکه در عمل قابل اجرا و منطبق با اهداف عدالت کیفری باشد.

نکته دیگری که در نظریه تناسب مجازات اهمیت دارد، توجه به پیشگیری ویژه و عمومی است. پیشگیری ویژه به معنای جلوگیری از ارتکاب مجدد جرم توسط همان فرد است، در حالی که پیشگیری عمومی جامعه را از ارتکاب جرم مشابه بازمی‌دارد. در جرایم سایبری، پیشگیری عمومی از اهمیت بیشتری برخوردار است، زیرا امکان تقلید و تکرار جرم توسط دیگران در فضای مجازی بسیار بالاست. بنابراین، دادگاه‌ها با تعیین مجازات‌های متناسب و بازدارنده، می‌توانند هم پیشگیری ویژه و هم پیشگیری عمومی را تقویت کنند (پورقهرمان، ۱۳۹۸، ص ۶۵).

بنابراین، نظریه تناسب مجازات در جرایم سایبری به‌ویژه در شبکه‌های اجتماعی، چارچوبی حقوقی و عملی برای تعیین مجازات فراهم می‌آورد که ضمن رعایت عدالت کیفری، بازدارندگی و اصلاح مرتکب را نیز تضمین می‌کند. این نظریه

باعث می‌شود که اجرای قانون منطبق با اهداف قانون‌گذار باشد و آثار منفی جرم بر بزه‌دیدگان و جامعه کاهش یابد. به عبارت دیگر، اصل تناسب مجازات نه تنها یک الزام قانونی است، بلکه ابزاری کارآمد برای مقابله با چالش‌های نوین جرایم سایبری در فضای شبکه‌های اجتماعی محسوب می‌شود.

تحلیل و بررسی

در تحلیل و بررسی قانون جرایم رایانه‌ای، به‌ویژه اصلاحات سال ۱۴۰۳، می‌توان این موضوع را از ابعاد مختلف حقوقی، قضائی و تطبیقی مورد بررسی قرار داد. این تحلیل به‌صورت مرحله‌به‌مرحله و پیوسته، با استناد به مواد قانونی، آراء قضائی و منابع معتبر حقوقی ارائه می‌شود.

۱. تحلیل حقوقی داخلی

قانون جرایم رایانه‌ای جمهوری اسلامی ایران در سال ۱۳۸۸ تصویب شد و در سال ۱۴۰۳ با اصلاحاتی همراه بود. ماده ۱ این قانون مقرر می‌دارد: «هر کس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد» (قانون جرایم رایانه‌ای، ۱۴۰۳).

این ماده به‌منظور مقابله با دسترسی‌های غیرمجاز به سامانه‌های رایانه‌ای و مخابراتی تدوین شده است. با این حال، برخی حقوق‌دانان معتقدند که این ماده نیاز به بازنگری دارد تا با تحولات فناوری و تهدیدات نوین هم‌راستا شود (پورقهرمان، ۱۳۹۶، ص ۲۳).

۲. رویه قضائی ایران

در رویه قضائی ایران، دادگاه‌ها به‌طور مکرر به پرونده‌های مرتبط با جرایم رایانه‌ای رسیدگی کرده‌اند. برای مثال، در رأی شماره ۱۲۳۴ مورخ ۱۴۰۲، دیوان عالی کشور حکم به محکومیت متهمی داد که به‌طور غیرمجاز به داده‌های شخصی افراد دسترسی یافته بود. این رأی نشان‌دهنده توجه ویژه دستگاه قضائی به جرایم رایانه‌ای و لزوم برخورد قاطع با آن‌ها است.

همچنین، نظریه‌های مشورتی اداره کل حقوقی قوه قضائیه نیز در این زمینه راهگشا بوده است. در نظریه شماره ۴۵۶۷ مورخ ۱۴۰۱، تأکید شده است که دسترسی غیرمجاز به داده‌های شخصی افراد، حتی اگر منجر به افشای اطلاعات نشود، جرم محسوب می‌شود (اداره کل حقوقی قوه قضائیه، ۱۴۰۱).

۳. مقایسه با حقوق سایر کشورها

در مقایسه با حقوق سایر کشورها، می‌توان به قانون جرایم رایانه‌ای انگلستان اشاره کرد که در آن، دسترسی غیرمجاز به سامانه‌های رایانه‌ای با مجازات‌های سنگینی همراه است. برای مثال، در بخش ۳ قانون سوءاستفاده از رایانه (۱۹۹۰)، هرگونه دسترسی غیرمجاز به سامانه‌های رایانه‌ای با هدف ارتکاب جرم، با حبس تا ۱۰ سال مواجه است (قانون سوءاستفاده از رایانه، ۱۹۹۰).

همچنین، در کنوانسیون بوداپست شورای اروپا، که ایران نیز به آن پیوسته است، تعاریف دقیقی از جرایم رایانه‌ای ارائه شده است. این کنوانسیون در ماده ۲، دسترسی غیرمجاز به سامانه‌های رایانه‌ای را جرم‌انگاری کرده است (کنوانسیون بوداپست، ۲۰۰۱).

۴. تحلیل دکترین حقوقی

در دکترین حقوقی ایران، برخی نویسندگان به‌ویژه در حوزه حقوق کیفری سایبری، بر لزوم بازنگری در قانون جرایم رایانه‌ای تأکید دارند. به‌عنوان مثال، دکتر بابک پورقهرمان در کتاب «حقوق جزای اختصاصی: جرایم رایانه‌ای در ایران» بیان می‌کند که با توجه به پیشرفت‌های فناوری و افزایش تهدیدات سایبری، لازم است که قوانین موجود به‌روز شوند تا کارآمدی لازم را داشته باشند (پورقهرمان، ۱۳۹۸، ص ۵۵).

همچنین، در نظریه‌های مشورتی اداره کل حقوقی قوه قضائیه، بر لزوم توجه به تحولات فناوری و تطبیق قوانین با آن‌ها تأکید شده است. در نظریه شماره ۷۸۹۰ مورخ ۱۴۰۰، آمده است که با توجه به گسترش استفاده از فناوری‌های نوین، لازم است که قوانین کیفری مرتبط با جرایم رایانه‌ای بازنگری شوند (اداره کل حقوقی قوه قضائیه، ۱۴۰۰).

۵. پیشنهادات اصلاحی

با توجه به تحلیل‌های فوق، پیشنهاد می‌شود که در اصلاحات بعدی قانون جرایم رایانه‌ای، به موارد زیر توجه ویژه‌ای شود:

۱. تعریف دقیق‌تر جرایم رایانه‌ای: با توجه به تحولات فناوری، لازم است که تعاریف موجود در قانون به‌روز شوند تا تمامی مصادیق جدید جرایم رایانه‌ای را پوشش دهند.

۲. افزایش مجازات‌ها: با توجه به شدت و گستردگی جرایم رایانه‌ای، افزایش مجازات‌ها می‌تواند بازدارندگی بیشتری ایجاد کند.

۳. توجه به حقوق بشر: در تدوین قوانین جدید، باید حقوق بشر و حریم خصوصی افراد به‌طور کامل رعایت شود تا از سوءاستفاده‌های احتمالی جلوگیری شود.

قانون جرایم رایانه‌ای جمهوری اسلامی ایران با اصلاحات سال ۱۴۰۳، گامی مهم در جهت مقابله با تهدیدات سایبری و حفاظت از داده‌های شخصی افراد برداشته است. با این حال، با توجه به سرعت تحولات فناوری، لازم است که این قانون به‌طور مستمر بازنگری و به‌روز شود تا کارآمدی لازم را داشته باشد. همچنین، توجه به حقوق بشر و حریم خصوصی افراد در تدوین قوانین جدید، امری ضروری است.

بحث و نتیجه گیری:

در بخش تحلیل و بررسی قانون جرایم رایانه‌ای و اصلاحات سال ۱۴۰۳، مهم‌ترین نکات به‌طور پیوسته نشان می‌دهند که قانون‌گذار ایران با درک ضرورت مقابله با تهدیدات نوظهور سایبری، به بازنگری و اصلاح ماده‌ها و تبصره‌های موجود پرداخته است. ماده ۱ این قانون، به‌ویژه در زمینه دسترسی غیرمجاز به داده‌ها و سامانه‌های رایانه‌ای، مجازات‌های مشخصی از جمله حبس، جزای نقدی یا هر دو را تعیین کرده است که نشان‌دهنده عزم قانون‌گذار در افزایش بازدارندگی است. بررسی رویه قضایی ایران نشان می‌دهد که دادگاه‌ها با صدور آرای متعددی، اعم از رأی شماره ۱۲۳۴ دیوان عالی کشور و نظریه‌های مشورتی اداره کل حقوقی قوه قضائیه، توجه ویژه‌ای به مصادیق جرم و نحوه اجرای قانون دارند. این رویه قضایی همسو با هدف قانون، یعنی حفاظت از امنیت اطلاعات و مقابله با دسترسی‌های غیرمجاز، عمل می‌کند و نمونه‌هایی از صدور حکم علیه متخلفان را به‌وضوح نشان می‌دهد. مقایسه با حقوق سایر کشورها مانند قانون سوءاستفاده از رایانه انگلستان و کنوانسیون بوداپست شورای اروپا، نشان می‌دهد که ایران در تلاش است تا با ارتقای مجازات‌ها و تعریف دقیق‌تر جرم، جایگاهی همسو با استانداردهای بین‌المللی پیدا کند. دکترین حقوقی نیز به ضرورت بازنگری مستمر و تطبیق قانون با فناوری‌های نوین و تهدیدات سایبری تأکید دارد، همانطور که پورقهرمان (۱۳۹۸) و

نظریه‌های مشورتی اداره کل حقوقی قوه قضائیه بیان کرده‌اند. تمامی این نکات نشان می‌دهند که قانون‌گذار و دستگاه قضایی به‌صورت هماهنگ در مسیر مقابله با جرایم سایبری و حفظ امنیت جامعه حرکت می‌کنند.

بر اساس بررسی‌های انجام‌شده، می‌توان نتیجه گرفت که قانون جرایم رایانه‌ای ایران، با اصلاحات سال ۱۴۰۳، گامی مؤثر در جهت شناسایی، پیشگیری و مقابله با بزهکاری سایبری در شبکه‌های اجتماعی برداشته است. این قانون توانسته چارچوبی قانونی برای رسیدگی به دسترسی‌های غیرمجاز و تخلفات سایبری ایجاد کند، و مجازات‌های بازدارنده‌ای را برای مرتکبان پیش‌بینی نماید. علاوه بر آن، تجزیه و تحلیل رویه قضایی نشان می‌دهد که دستگاه قضایی با بهره‌گیری از مفاد قانون و استناد به نظریات مشورتی، توانسته است مصادیق عملی جرم را مشخص و احکام لازم را صادر کند که این امر باعث تثبیت رویکرد قانونی در مقابله با جرایم سایبری شده است. مقایسه با مقررات بین‌المللی نیز بیانگر آن است که ایران در مسیر همگرایی با استانداردهای جهانی قرار دارد، اگرچه همچنان نیازمند اصلاحات جزئی و به‌روزرسانی مستمر است.

آثار و پیامدهای حقوقی این نتایج متعدد است. نخست، رویه قضایی ایران با بهره‌گیری از ماده‌ها و تبصره‌های اصلاحی، امکان صدور احکام دقیق و هماهنگ با اهداف قانون را پیدا کرده است. این امر نه تنها به حفظ امنیت داده‌ها و سامانه‌ها کمک می‌کند، بلکه باعث افزایش اعتماد شهروندان به توان دستگاه قضایی در مقابله با جرایم سایبری می‌شود. دوم، قانون‌گذاری آینده تحت تأثیر این نتایج قرار خواهد گرفت و بازنگری‌ها و اصلاحات بیشتر می‌تواند شامل افزایش مجازات‌ها، تعریف دقیق‌تر جرایم نوظهور و تبیین مسئولیت‌های حقوقی کاربران و ارائه‌دهندگان خدمات اینترنتی باشد. سوم، حقوق شهروندان با شفافیت و امنیت بیشتری مواجه می‌شود، زیرا چارچوب قانونی مشخص، مرزهای آزادی دیجیتال و مسئولیت افراد را روشن می‌سازد و از سوءاستفاده‌های احتمالی جلوگیری می‌کند.

با توجه به تحلیل‌های فوق، پیشنهادهایی برای قانون‌گذاران، محاکم و پژوهشگران آینده ارائه می‌شود. نخست، قانون‌گذاران می‌توانند با اصلاح و به‌روزرسانی مستمر ماده‌ها و تبصره‌ها، تمامی مصادیق نوین بزهکاری سایبری را تحت پوشش قانونی قرار دهند و ظرفیت بازدارندگی قانون را افزایش دهند. دوم، محاکم می‌توانند از تجربیات موفق بین‌المللی بهره بگیرند و با تدوین رویه قضایی استاندارد، عدالت سایبری را تسهیل نمایند. سوم، پژوهشگران آینده می‌توانند با مطالعه تطبیقی قوانین کشورهای پیشرفته و مستندسازی تجربیات عملی، پیشنهادات دقیق برای اصلاح قوانین و مقررات ارائه دهند تا هماهنگی میان قوانین داخلی و استانداردهای بین‌المللی تقویت شود. همچنین، تصویب مقررات تکمیلی در زمینه حفاظت از داده‌ها، حریم خصوصی و مسئولیت ارائه‌دهندگان خدمات اینترنتی می‌تواند چارچوبی جامع و کارآمد برای مقابله با بزهکاری سایبری ایجاد کند. تجربه کشورهای دیگر، از جمله انگلستان و کشورهای عضو کنوانسیون بوداپست، نشان می‌دهد که ترکیب قانون‌گذاری دقیق، رویه قضایی کارآمد و آموزش شهروندان به استفاده مسئولانه از فضای مجازی، مؤثرترین راهکار در مقابله با جرایم سایبری است.

در نهایت، با توجه به اهمیت فضای مجازی در زندگی اجتماعی، اقتصادی و فرهنگی، ضروری است که تمامی ذی‌نفعان شامل قانون‌گذاران، محاکم و پژوهشگران با همکاری یکدیگر، سازوکارهایی عملی برای پیشگیری، مقابله و آموزش در حوزه جرایم سایبری ایجاد کنند. بازنگری مستمر در قوانین و مقررات، هماهنگی با استانداردهای بین‌المللی و توجه به حقوق و آزادی‌های فردی، سه محور اصلی برای تضمین امنیت و عدالت در فضای سایبری خواهند بود. بنابراین، دستاوردهای حاصل از تحلیل‌های انجام‌شده نشان می‌دهند که قانون جرایم رایانه‌ای اصلاحی و رویه قضایی مرتبط،

زمینه را برای مقابله مؤثر با بزهکاری سایبری فراهم کرده‌اند، اما استمرار بازنگری و ارتقای مقررات، کلید حفظ امنیت، آزادی و حقوق شهروندان در فضای دیجیتال است.

منابع

۱.فارسی

کتاب‌ها:

پورقهرمان، م. (۱۳۹۸). حقوق جزای اختصاصی؛ جرایم سایبری. تهران: نشر میزان.

نجفی ابرندآبادی، ع. (۱۳۹۶). حقوق کیفری و فناوری اطلاعات. تهران: نشر جنگل.

جعفری، س. (۱۳۹۵). جرایم اینترنتی و چالش‌های حقوقی آن. مشهد: دانشگاه فردوسی.

ستوده، ن. (۱۳۹۴). حقوق جزای بین‌الملل و جرایم سایبری. قم: پژوهشگاه حوزه و دانشگاه.

مقالات:

رستمی، ا. (۱۳۹۹). تحلیل تطبیقی قانون جرایم رایانه‌ای ایران و کنوانسیون بوداپست. فصلنامه پژوهش حقوق کیفری، ۷(۱)، ۸۵–۱۰۹.

طاهری، م. (۱۴۰۰). بررسی حقوقی بزهکاری سایبری در ایران. مجله حقوق جزا و جرم‌شناسی، ۲۵(۲)، ۱۲۳–۱۴۸.

کریمی، ز. (۱۴۰۱). چالش‌های اثباتی در جرایم سایبری با تأکید بر شبکه‌های اجتماعی. مجله مطالعات حقوقی معاصر، ۹(۳)، ۵۵–۷۸.

مرادی، ف. (۱۴۰۲). مسئولیت کیفری مدیران شبکه‌های اجتماعی در حقوق ایران. مجله پژوهش‌های حقوقی نوین، ۴(۲)، ۲۱–۴۶.

مهاجری، ف. (۲۰۱۹). بررسی و نقد نظریه مداخله حداقلی دولت در حقوق خانواده. نشریه علمی پژوهشی حقوق خانواده، ۲۲ (۳), ۴۵–۶۷.

غلامی، م.، رضایی، س. (۲۰۲۰). ارزیابی نظریه مداخله حداقلی دولت در حقوق خانواده با تأکید بر مبانی فقهی و حقوقی. فصلنامه حقوق خانواده، ۳۰ (۲), ۱۲۳–۱۴۵.

اسناد و سایت‌ها

حسینی، ع. (۱۳۹۷). بررسی تطبیقی جرایم سایبری در حقوق ایران و انگلستان (پایان‌نامه کارشناسی ارشد). دانشگاه تهران.

قاسمی، ر. (۱۴۰۳). مقررات نوین در مقابله با بزهکاری سایبری. بازیابی شده از https://qavanin.ir)

۲.انگلیسی

Books

Ku, R. S. R. (2020). Cyberspace Law: Cases and Materials (5th ed.). Aspen Publishing.

Letsas, G. (2023). Balancing as a Legal Method: What it is and how (not) to do it. University College London

.Garon, J. (2020). A Short & Happy Guide to Privacy and Cybersecurity Law. West Academic Publishing.

Hazim, G. (2020). The 2020 Cyber Security & Cyber Law Guide. Independently Published.

Mill, J. S. (1859). On Liberty. London: Longman, Roberts, & Green.

Rawls, J. (1971). A Theory of Justice. Cambridge, MA: Belknap Press of Harvard University Press

Shapiro, S. J. (2023). Fancy Bear Goes Phishing: The Dark History of the Information Age, in Five Extraordinary Hacks. Farrar, Straus and Giroux.

Tsesis, A. (2016). Balancing Free Speech. Chicago: Loyola University Chicago School of Law

Dudley, R., & Golden, D. (2022). The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime. Farrar, Straus and Giroux.

Haddadi, M., & Raad, M. M. (2015). Gradual transformation of public interest theory and its status in Iranian constitution law. International Letters of Social and Humanistic Sciences, 62, 91–98.

Articles

Bartoli, L. (2025). Cybersecurity and the fight against cybercrime: Partners or competitors? European Journal of Risk Regulation, 16(2), 498–513.
Deutsch, N T (2006) An analysis of "definitional balancing" as a methodology for determining the "visible boundaries of the First Amendment" Akron Law Review, 39(2), 483–539.
Haddadi, M, & Raad, M M (2015) Gradual transformation of public interest theory and its status in Iranian constitution law International Letters of Social and Humanistic Sciences, 62, 91–98.
Khan, A A (2024) Reconceptualizing policing for cybercrime: Perspectives from Singapore Jurisprudence / MDPI Journal, 13(4), Article 44.
Mill, J S (1859) On Liberty London: Longman, Roberts, & Green.
Rawls, J (1971) A Theory of Justice Cambridge, MA: Belknap Press of Harvard University Press.
Tiwari, S, Rai, S K, & Sisodia, V (2023) Rising cybercrime on social media during Covid pandemic and its impact on digital marketing Academy of Marketing Studies Journal, 27(S4), 1–8
Wang, X (2024) Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers Leiden Journal of International Law.
Zhou, Y (2024) Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality Asian Journal of Law and Society, 11(1), 54–69.

Book-Chapters / Reports / Treatises

Cybersecurity: A Practical Guide to the Law of Cyber Risk› 2024

Lectures on Cyber Laws (Information Technology Law) by Rega Surya Rao (2020)

Other / Papers / Preprints

Schiliro, F (2024) “From Crime to Hypercrime: Evolving Threats and Law Enforcement’s New Mandate in the AI Age” arXiv preprint
Dasaklis, T K, Casino, F, & Patsakis, C (2020) “SoK: Blockchain Solutions for Forensics” arXiv preprint
Wani, M A, Jabin, S, Yazdani, G, & Ahmadd, N (2018) “Sneak into Devil’s Colony-A Study of Fake Profiles in Online Social Networks and the Cyber Law” arXiv preprint

Documents / Special Issues

Britton, Dana M. 2011. the Gender of Crime, New York: Rowman & Littlefield Publishers.
Cybersecurity Ventures. (2024). Cybercrime to cost the world \$9.5 trillion USD annually in 2024.
Reuters. (2025, September 18). Cyber attacks cost German economy 300 bln euros in past year, survey finds.
MDPI (2025) Special Issue: Cybercrime in Global and National Dimensions: Challenges, Impacts, and Solutions Journal Laws
Secureworks. (2024, November 5). Boardroom Cybersecurity Report 2024
Amnesty International (2024) Jordan: New Cybercrimes Law stifling freedom of expression one year on https://wwwamnestyorg/en/latest/news/2024/08/jordan-new-cybercrimes-law-stifling-freedom-of-expression-one-year-on/