Received: 07/05/2024
Review: 20/08/2024
Accepted: 10 /09/2024
DOI: 10.22054/jocl. 2035.85063.2123

Journal of Cyber Law
No(2),Vol(1) 104-124.
ISSN: 0972-6934
www.jocl.ir

Cybercrimes Against Women: Legal Challenges, Gaps, and Countermeasures

Behdad Sharifi [1], Maral Arjmand [*2]

1- Master's Student in Law, Payame Noor University, Mahdasht, Iran.

2*- Master's Student in Law, Payame Noor University, Mahdasht, Iran.

ABSTRACT

Cybercrimes against women have become an emerging and alarming challenge in modern societies, seriously threatening women's personal, social, and psychological security. The central questions of this study are to what extent existing criminal laws have provided effective protection for women against such crimes, what the main legal gaps and shortcomings are, how Iranian laws compare to international instruments and other legal systems, and finally what solutions can be proposed to address these gaps. The significance of this research arises from the fact that with the expansion of new communication technologies, diverse forms of online harassment and violence against women have appeared, which are difficult to identify and prove in judicial processes. The primary objective of this article is to analyze the legal framework of Iran in addressing these crimes, identify the legal deficiencies, and propose legal, educational, and institutional solutions to strengthen protection mechanisms. The methodology is descriptive–analytical, based on documentary research, the study of domestic legislation, and its comparison with international instruments. Findings indicate that although Iranian criminal law provides some scattered regulations addressing certain forms of cybercrimes, they are general, fragmented, and lack effective enforcement, thereby failing to adequately protect women in cyberspace. Consequently, revising existing laws, precisely criminalizing forms of cyber violence, raising public awareness, and enhancing international cooperation are essential. The novelty of this article lies in addressing fundamental research questions while simultaneously comparing domestic and international legal frameworks and offering practical, applicable solutions to fill the legal gaps.

Keywords:
Cybercrimes, Crimes Againts Women, Criminal Law, Legal Gaps

How to Cite: Sharifi, B and Arjmand, M.. (2024). Cybercrimes Against Women: Legal Challenges, Gaps, and Countermeasures. Cyber Law, 1(2), 104-124.
DOI: 10.22054/jocl.2035.85063.2123

* Corresponding Author: maral.arjmand@pnu.ac.ir

نشریه حقوق سایبری
شماره (۲) ۱۲٤-۱۰٤
دوره ۱٤۰۳

تاریخ دریافت: ۱٤۰۳/۰۲/۱۸
تاریخ اصلاح: ۱٤۰۳/۰۵/۳۰
تاریخ پذیرش: ۱٤۰۳/۰۶/۲۰

جرایم علیه زنان در فضای سایبری: چالش‌های قانونی، خلأهای حقوقی و راهکارهای مقابله

بهداد شریفی[۱] ، مارال ارجمند[۲*]

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

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

چکیده

جرائم علیه زنان در فضای سایبری و مجازی به یکی از چالش های نوظهور و نگران کننده در جوامع امروز تبدیل شده است؛ چالشی که امنیت فردی، اجتماعی و روانی زنان را به‌طور جدی تهدید می کند. پرسش‌های اصلی این پژوهش آن است که قوانین کیفری موجود تا چه اندازه توانسته‌اند حمایت مؤثر از زنان در برابر این جرائم فراهم کنند، مهم‌ترین خلأها و نارسایی‌های حقوقی در این زمینه کدام‌اند، قوانین ایران در مقایسه با اسناد بین‌المللی و تجارب سایر کشورها چه نقاط قوت و ضعفی دارند، و در نهایت چه راهکارهایی می‌تواند برای پرکردن شکاف‌های موجود ارائه شود. ضرورت این پژوهش از آن‌جا ناشی می‌شود که با گسترش فناوری‌های نوین ارتباطی، مصادیق متنوعی از خشونت و آزار سایبری علیه زنان پدیدار شده که شناسایی و اثبات آن‌ها در مراجع قضایی با دشواری همراه است. هدف اصلی مقاله، تحلیل وضعیت حقوقی ایران در زمینه مقابله با این جرائم، شناسایی خلأهای قانونی و ارائه راهکارهای حقوقی، آموزشی و نهادی برای ارتقای سطح حمایت از زنان است. روش پژوهش توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی، تحلیل قوانین داخلی و تطبیق آن با اسناد بین‌المللی است. یافته‌های تحقیق نشان می‌دهد که هرچند مقرراتی در قوانین کیفری ایران در جهت مقابله با برخی مصادیق جرائم سایبری وجود دارد، اما این مقررات پراکنده، کلی و فاقد ضمانت اجرایی کارآمد هستند و پاسخگوی نیازهای روزافزون زنان در فضای مجازی نیستند. در نتیجه، ضرورت اصلاح قوانین، جرم‌انگاری دقیق‌تر مصادیق خشونت سایبری، افزایش آگاهی عمومی و تقویت همکاری‌های بین‌المللی بیش از پیش احساس می‌شود. نوآوری مقاله در این است که با تمرکز بر پرسش‌های بنیادین و تطبیق حقوق داخلی با اسناد بین‌المللی، راهکارهای عملی و قابل اجرا برای پرکردن خلأهای قانونی ارائه کرده است.

کلیدواژه‌ها:

جرائم سایبری،جرایم علیه زنان، حقوق کیفری، خلأهای قانونی

نحوه استناد:

شریفی, بهداد و ارجمند, مارال. (۱۴۰۳). جرایم علیه زنان در فضای سایبری: چالش‌های قانونی، خلأهای حقوقی و راهکارهای مقابله . حقوق سایبری, ۱(۲), ۱۰۴-۱۲۴.

* ایمیل نویسنده مسئول: maral.arjmand@pnu.ac.ir

مقدمه

در عصر دیجیتال، فضای سایبری به عرصه ای تبدیل شده است که در آن، زنان با انواع مختلفی از جرائم مواجه هستند که نه تنها امنیت شخصی آن‌ها را تهدید می کند، بلکه جایگاه حقوقی آن‌ها را نیز در نظام حقوقی کشور به چالش می کشد. این جرائم شامل آزارهای آنلاین، تهدیدات سایبری، نشر اطلاعات شخصی بدون رضایت، و خشونت‌های دیجیتال می‌شود که به‌طور فزاینده‌ای در حال افزایش است. و همچنین با افزایش دسترسی افراد با فضای سایبری ،جرایم نه تنها در جهان واقعی بلکه در جهان مجازی هم افزایش داشته است و در مقابل از دامنه روابط در جهان واقعی کاسته شده است (حسین زاده ،۱۳۹۸).ارتباطات و تعاملات در فضای اینترنتی بر همه اقشار ازجمله زنان تاثیر داشته است (Cyber Vioence gender report,2014).

گزارش سازمان ملل در مورد جرایم علیه زنان در سایبری هر نوشته و رفتار تحقیر آمیز در پیغام های کاربران ،اجبار به عمل جنسی در فضای اینترنت ،تهدید و استفاده از الفاظ جنسی و هم چنین تهدید کلامی و رفتارهای خشن ،جرایم علیه زنان محسوب می شود و جرایم علیه زنان را در فضای سایبری یکی از علت هایی می داند که چرخه خشونت علیه زنان را در عالم واقع تندتر می چرخاند .پیترسون و دنسلی (Densley & Petetson,2017) از نظریه پردازان اخیر که به جرائم علیه زنان در فضای مجازی پرداخته اند انواع جرایم را شامل :تهدید افراد بخصوص زنان و دختران جوان در این حوزه می داند همچنین ایجاد شرمساری برای افراد از طریق نوشتن و پیام گذاشتن زیر عکس و یا پست های افراد ،رفتارهای فریبکارانه آنلاین با اهداف نامعلوم (Trapnell & Buckele,2014) انتقام از طریق گذاشتن تصاویر پورنو (Franklin,2014) ، زورگیری سایبری و خشونت جنسی را از انواع جرایم سایبری دانسته اند .جرایم علیه زنان و دختران در سراسر جهان به موضوعی مهم تبدیل شده است و میلیونها نفر از زنان و دختران در سراسر دنیا به دلیل جنسیت خود در معرض این جرایم سایبری قرار دارند . بدیهی است که قلمرو نقش آفرینی دولت ها برای پیشگری و مقابله و نیز کارایی ضمانت اجراهای دولتی مانند جرم انگاری و مجازات این جرایم در فضای مجازی با توجه به ماهیت آن با محدودیت هایی مواجه است چنانچه آمار بالای این جرایم در کشورهای اروپایی علیرغم پیشرفت های زیاد تکنولوژی در جوامع مزبور دلالت بر این واقعیت دارد ،لذا در کنار ضمانت های اجرایی قانونی و لزوم قطعیت پیگرد قضایی ،تعقیب ،محاکمه و مجازات مرتکبین جرایم سایبری علیه زنان و دختران ،توجه به ایجاد مکانیسم های درونی بازدارنده یا تدابیر خود کنترلی ضروری بنظر میرسد (زندی ،۱۳۸۹).در نظام حقوقی ایران، قوانین موجود در زمینه جرائم سایبری به‌ویژه در مورد زنان، با چالش‌هایی مواجه است. قانون جرائم رایانه‌ای مصوب ۱۳۸۸، به‌عنوان اولین قانون جامع در این زمینه، برخی از جرائم سایبری را تعریف کرده است. اما این قانون در خصوص جرائم مرتبط با زنان، به ویژه در فضای مجازی، خلأهای قابل توجهی دارد. برای مثال، در ماده ۲۱ این قانون، به جرائم مرتبط با حریم خصوصی اشاره شده است، اما به‌طور خاص به آزارهای آنلاین و تهدیدات سایبری علیه زنان پرداخته نشده است. این خلأ قانونی موجب شده است که بسیاری از جرائم سایبری علیه زنان بدون مجازات باقی بمانند.

اهمیت پرداختن به این موضوع از آن جهت است که با گسترش استفاده از اینترنت و شبکه‌های اجتماعی، زنان بیش از پیش در معرض انواع مختلفی از جرائم سایبری قرار دارند. این جرائم نه تنها امنیت روانی و اجتماعی آن‌ها را تهدید

می کند، بلکه می تواند بر جایگاه حقوقی و اجتماعی آن ها نیز تأثیر منفی بگذارد. بنابراین، بررسی و تحلیل قوانین موجود و ارائه راهکارهای حقوقی برای مقابله با این جرائم، امری ضروری به نظر می‌رسد.

پیشینه پژوهش های انجام‌شده در این زمینه نشان می‌دهد که این موضوع تاکنون مورد توجه پژوهشگران قرار گرفته است. برای مثال، رحیمی (۲۰۱۸) در مقاله ای به بررسی جرائم سایبری و حقوق زنان در ایران پرداخته و به خلأهای قانونی در این زمینه اشاره کرده است. همچنین، سازمان عفو بین‌الملل (۲۰۲۴) در گزارشی به افزایش خشونت‌های سایبری علیه زنان در ایران و عدم وجود قوانین مؤثر برای مقابله با آن‌ها پرداخته است. با این حال، با وجود این پژوهش ها، هنوز نیاز به بررسی‌های بیشتر و ارائه راهکارهای عملی در این زمینه احساس می‌شود.

هدف از این مقاله بررسی جرائم سایبری علیه زنان در فضای مجازی، تحلیل قوانین موجود در نظام حقوقی ایران، شناسایی خلأهای قانونی، و ارائه راهکارهای حقوقی برای مقابله با این جرائم است. روش پژوهش در این مقاله تحلیلی-توصیفی و مبتنی بر مطالعه اسنادی و کتب مربوط به فضا و جرایم سایبری و رایانه ای و اسناد حقوقی کنوانسیونهای مختلف و دیگر قوانین و مقررات بین المللی بررسی جرایم سایبری علیه زنان و شناسایی خلاءهای قوانین ملی و بین المللی در این حوزه است. در این راستا، ابتدا به بررسی مفاهیم مرتبط با جرائم سایبری و حقوق زنان پرداخته می‌شود، سپس قوانین موجود در این زمینه تحلیل می شود و در نهایت، پیشنهادهایی برای اصلاح و تکمیل قوانین ارائه می گردد.در نهایت، با توجه به اهمیت و حساسیت موضوع، این مقاله می تواند گامی مؤثر در جهت ارتقاء امنیت حقوقی زنان در فضای سایبری و مجازی و مقابله با جرائم مرتبط با آن‌ها باشد.

مفهوم فضای سایبر و جرایم سایبری

فضای سایبر یا «فضای مجازی» به عنوان محیطی غیرمادی و مبتنی بر شبکه های رایانه‌ای تعریف می‌شود که در آن اطلاعات، داده‌ها و ارتباطات به‌صورت دیجیتال تولید، ذخیره و مبادله می گردند (کاستلز، ۲۰۰۱: ص. ۵۴). این فضا فراتر از مرزهای جغرافیایی عمل کرده و امکان تعامل بی‌واسطه میان افراد، سازمان‌ها و دولت‌ها را فراهم می‌آورد (والاک، ۲۰۱۰: ص. ۳۲). از طرفی در عصر دیجیتال، فضای سایبری به یکی از ارکان اصلی زندگی اجتماعی، اقتصادی و فرهنگی تبدیل شده است و با گسترش فناوری اطلاعات و ارتباطات، جرایمی نیز در این بستر شکل گرفته‌اند که اصطلاحاً «جرایم سایبری» یا «جرایم رایانه‌ای» نامیده می‌شوند. این دسته از جرایم شامل هرگونه رفتار غیرقانونی است که در آن رایانه یا شبکه به عنوان ابزار، هدف یا محل ارتکاب جرم مورد استفاده قرار می گیرد (گودمن، ۲۰۰۷: ص. ۷۶).جرایم سایبری طیف گسترده‌ای را در بر می گیرد؛ از جمله دسترسی غیرمجاز به سامانه ها، جاسوسی سایبری، سرقت داده ها، کلاهبرداری اینترنتی، انتشار بدافزارها، جعل هویت در شبکه های اجتماعی، و حملات باج‌افزاری (اسپریگل، ۲۰۱۵: ص. ۱۱۹). ویژگی اصلی این جرایم، فراملی بودن آنهاست؛ به گونه‌ای که مرزهای جغرافیایی در تعقیب و کشف مجرمان نقش محدودی دارند (باکر، ۲۰۱۸: ص. ۲۱۱).در نتیجه، مفهوم فضای سایبر از یک سو بستری برای تعاملات اجتماعی و اقتصادی جهانی است و از سوی دیگر زمینه‌ای برای شکل گیری گونه های نوین جرم که نیازمند قوانین و سازوکارهای بین‌المللی جهت پیشگیری و مقابله هستند (رضایی، ۱۳۹۶: ص. ۸۸).و زنان، به‌عنوان بخشی از جامعه، بیش

از پیش در معرض انواع جرائم سایبری قرار دارند (Smith, 2019, p. 45). این جرائم شامل هرگونه رفتار غیرقانونی است که از طریق فناوری‌های اطلاعاتی و ارتباطی علیه زنان صورت می‌گیرد و می‌تواند شامل آزارهای آنلاین، تهدیدات سایبری، نشر اطلاعات شخصی بدون رضایت و سایر اشکال خشونت دیجیتال باشد (Johnson & Miller, 2020, p. 102).

جرایم سایبری با تاکید بر جرایم علیه زنان

ظهور فضای سایبر تحولی بنیادین در ارتباطات اجتماعی، اقتصادی و فرهنگی جوامع ایجاد کرده است. این فضا، علاوه بر فرصت‌های بی‌سابقه، زمینه‌ساز شکل‌گیری گونه‌های جدیدی از جرایم نیز شده که تحت عنوان «جرایم سایبری» شناخته می شوند (کاستلز، ۲۰۰۱: ص. ۵۴). در این میان، زنان به دلیل شرایط اجتماعی، فرهنگی و حتی ساختارهای حقوقی، بیش از سایر گروه‌ها در معرض تهدیدات سایبری قرار گرفته‌اند (والاک، ۲۰۱۰: ص. ۸۷). بررسی جرایم سایبری علیه زنان اهمیت دوچندانی دارد، زیرا این جرایم نه تنها امنیت فردی، بلکه امنیت اجتماعی و کرامت انسانی را نیز تحت تأثیر قرار می‌دهند (رضایی، ۱۳۹۶: ص. ۹۱).

مفهوم و ویژگی‌های جرایم سایبری

جرایم سایبری شامل هرگونه رفتار مجرمانه‌ای است که با استفاده از رایانه، اینترنت یا سایر فناوری‌های دیجیتال ارتکاب می‌یابد (گودمن، ۲۰۰۷: ص. ۷۶). این جرایم ویژگی‌های خاصی دارند که آنها را از جرایم سنتی متمایز می‌سازد:

۱. فراملی بودن: جرایم سایبری غالباً مرزهای جغرافیایی را در می‌نوردند و مجرمان می‌توانند قربانیانی در سراسر جهان داشته باشند (باکر، ۲۰۱۸: ص. ۲۱۱).

۲. ناشناس‌بودن مرتکبان: مجرمان سایبری اغلب از هویت‌های جعلی و ابزارهای ناشناس‌ساز استفاده می‌کنند (اسپریگل، ۲۰۱۵: ص. ۱۱۹).

۳. تنوع مصادیق: از دسترسی غیرمجاز و سرقت داده ها گرفته تا کلاهبرداری، جعل هویت و انتشار محتوای مستهجن (رضایی، ۱۳۹۶: ص. ۱۰۲).

زنان به دلیل جایگاه اجتماعی و فرهنگی، همواره در معرض اشکال مختلف خشونت قرار داشته اند. فضای سایبر این تهدیدها را به سطحی جدید منتقل کرده است (هارف، ۲۰۱۲: ص. ۶۸). مطالعات نشان می دهد زنان بیشتر از مردان قربانی آزارهای اینترنتی، تهدید به انتشار تصاویر خصوصی، و جعل هویت در شبکه های اجتماعی می شوند (هندی، ۲۰۱۴: ص. ۱۴۵).این آسیب‌پذیری به چند عامل برمی‌گردد:

نابرابری جنسیتی ساختاری: بسیاری از جوامع هنوز در زمینه حقوق زنان با چالش های اساسی مواجه اند (فاکس، ۲۰۱۶: ص. ۲۰۴).

کمبود قوانین حمایتی کافی: قوانین جرایم رایانه‌ای در برخی کشورها به‌طور خاص به خشونت سایبری علیه زنان نپرداخته‌اند (باکر، ۲۰۱۸: ص. ۲۱۴).

شرایط روانی و اجتماعی قربانیان: تهدید به افشای اطلاعات خصوصی می‌تواند زنان را در موقعیت‌های آسیب‌پذیرتری قرار دهد (رضایی، ۱۳۹۶: ص. ۱۰۸).

انواع جرایم سایبری علیه زنان

آزار و اذیت اینترنتی : زنان در شبکه‌های اجتماعی اغلب با پیام‌های توهین‌آمیز، تهدید به خشونت یا تماس‌های مکرر ناخواسته مواجه می‌شوند (گودمن، ۲۰۰۷: ص. ۸۳). این آزارها می‌تواند به افسردگی، اضطراب و حتی انزوای اجتماعی منجر شود (هارف، ۲۰۱۲: ص. ۷۱). آزار آنلاین نیز به مجموعه‌ای از رفتارهای هدفمند و مکرر اطلاق می‌شود که با هدف ترساندن، تهدید یا آسیب رساندن به فردی در فضای مجازی صورت می‌گیرد و می‌تواند شامل ارسال پیام‌های توهین‌آمیز، تهدیدآمیز یا تحقیرآمیز از طریق ایمیل، پیام‌رسان‌ها یا شبکه‌های اجتماعی باشد (Brown, 2018, p. 78). مطالعات نشان داده‌اند که زنان بیش از مردان در معرض آزار آنلاین قرار دارند و این نوع خشونت تأثیرات روانی و اجتماعی عمیقی بر آن‌ها دارد (Rahimi, 2017, p. 213). مطابق ماده ۱۷ قانون جرائم رایانه‌ای جمهوری اسلامی ایران، انتشار اطلاعات شخصی بدون رضایت افراد، به مجازات حبس و جزای نقدی منجر می‌شود (Vakileman, 1388).

داکسینگ :یکی دیگر از مصادیق جرائم سایبری علیه زنان، داکسینگ (Doxxing) است که به انتشار عمومی اطلاعات شخصی یا خصوصی فرد بدون رضایت او اطلاق می‌شود. طبق ماده ۱۲ قانون جرائم رایانه‌ای، سرقت داده‌ها یا انتشار غیرمجاز اطلاعات دیگران، مجازات قانونی دارد (WikiHoghoogh, 1388). داکسینگ می‌تواند شامل نام کامل، آدرس، شماره تلفن، ایمیل و سایر جزئیات شخصی باشد و هدف آن ارعاب یا تهدید فرد است (Lee & Johnson, 2020, p. 66).

انتشار یا تهدید به انتشار تصاویر خصوصی : یکی از شایع ترین اشکال خشونت سایبری علیه زنان، انتشار تصاویر خصوصی آنها بدون رضایتشان است (فاکس، ۲۰۱۶: ص. ۲۰۹). این اقدام غالباً با هدف انتقام‌گیری، باج‌خواهی یا تحقیر زنان صورت می‌گیرد (اسپریگل، ۲۰۱۵: ص. ۱۲۳). تهدید سایبری نیز به هرگونه تهدید به آسیب فیزیکی، روانی یا اجتماعی که از طریق فضای سایبری علیه فردی مطرح شود، اطلاق می‌شود (Lee, 2019, p. 56). طبق ماده ۱۵ قانون جرائم رایانه‌ای، هر فردی که به قصد تهدید افراد را از طریق سامانه‌های رایانه‌ای و مخابراتی تحت فشار یا تطمیع قرار دهد، مشمول مجازات حبس یا جریمه نقدی می‌گردد (Qavanin.ir, 1388). این تهدیدات می‌تواند شامل تهدید به انتشار اطلاعات خصوصی یا آسیب رساندن به فرد در دنیای واقعی باشد و اثرات منفی قابل توجهی بر سلامت روانی زنان دارد (Smith & Taylor, 2021, p. 89).

جعل هویت و پروفایل‌های جعلی :ایجاد حساب‌های کاربری جعلی با استفاده از نام و تصاویر زنان برای تخریب اعتبار یا فریب دیگران، پدیده‌ای رایج است (والاک، ۲۰۱۰: ص. ۹۲). چنین اعمالی می‌تواند به آسیب‌های حیثیتی و اجتماعی گسترده منجر شود.

باج گیری سایبری :مجرمان با دسترسی به اطلاعات یا تصاویر شخصی، زنان را تهدید به افشا می کننـد و در قبـال سـکوت خود خواستار پول یا روابط غیراخلاقی می‌شوند (رضایی، ۱۳۹۶: ص. ۱۱۳).

خشونت دیجیتال: به‌عنوان اسـتفاده از فنـاوری‌هـای دیجیتـال بـرای اعمـال خشـونت علیـه فـرد، شـامل آزارهـای آنلایـن، تهدیدات سایبری، نشر اطلاعات شخصی و سایر رفتارهای مشابه اسـت (Brown & Smith, 2021, p. 99). مطـابق ماده ۱۴ قانون جرائم رایانه‌ای، انتشار محتویات مستهجن و آسیب‌زننده به افراد نیز جرم محسوب می‌شود و مجـازات دارد (Qavanin.ir, 1388).

کلاهبرداری عاطفی :زنان بیشتر از مردان قربانی روابط عاطفی جعلی در فضای سایبر می شوند. مجرمـان بـا ایجـاد ارتبـاط عاطفی اعتماد قربانی را جلب کرده و سپس او را از نظر مالی یا اطلاعاتی استثمار می کنند (باکر، ۲۰۱۸: ص. ۲۱۷).

نشر اطلاعات شخصی بدون رضایت :یکی دیگر از ابعاد جرائم سایبری است که شامل انتشار تصـاویر خصوصـی، شـماره تلفن، آدرس منزل یا اطلاعات مالی فرد بدون رضایت او می‌شـود (Ahmadi, 2020, p. 131). ایـن عمـل مـی‌توانـد منجر به آسیب به شهرت، حریم خصوصی و امنیت فرد شود و طبق ماده ۱۷ قانون جرائم رایانه‌ای، انتشار چنـین اطلاعـاتی جرم محسوب می‌شود (Vakileman, 1388).

پیامدهای جرایم سایبری علیه زنان

این دسته از جرایم پیامدهای چندوجهی دارد:

روانی و عاطفی: اضطراب، افسردگی و کاهش اعتماد به نفس (هندی، ۲۰۱۴: ص. ۱۵۲).

اجتماعی: لکه‌دار شدن اعتبار اجتماعی، طرد شدن از سوی خانواده یا جامعه (رضایی، ۱۳۹۶: ص. ۱۲۰).

اقتصادی: باج‌گیری یا کلاهبرداری مالی (باکر، ۲۰۱۸: ص. ۲۲۰).

حقوقی: دشواری در شناسایی و تعقیب مجرمان به دلیل ماهیت فراملی و ناشناس بودن آنها (گودمن، ۲۰۰۷: ص. ۹۵).

مقابله با این جرایم مستلزم رویکردی چندبعدی شامل اصلاح قوانین، ارتقای آگاهی عمومی، حمایت روانی از قربانیـان و همکاری بین‌المللی است. تنها از طریق چنین رویکردی می توان امنیت و کرامت زنان را در فضای مجـازی تضـمین کـرد (رضایی، ۱۳۹۶: ص. ۱۲۵).

از منظر فلسفی، حقوق بشر به‌عنوان حقوق ذاتی هر فرد شامل حق بر حریم خصوصی، امنیت و آزادی بیان اسـت و نقـض آن در فضای سایبری نادرست و غیرقابـل قبـول اسـت (Brown, 2018, p. 80). از نظـر فقهـی، حفـظ آبـرو و حـریم خصوصـی زنـان واجـب اسـت و هرگونـه افشـاگری یـا تهدیـد بـدون دلیـل شـرعی، حـرام و مسـتوجب مجـازات اسـت (Ahmadi, 2020, p. 134). از نظر حقوقی، قانون جـرائم رایانـه‌ای ایـران بـا ارائـه مـواد ۱۲، ۱۴، ۱۵ و ۱۷ بخشـی از جرائم سایبری را پوشش می‌دهد، اما در خصوص خشونت و آزار آنلاین علیه زنان خلأهای قـانونی قابـل تـوجهی وجـود دارد (Vakileman, 1388). از دید اقتصادی، افزایش جرائم سایبری علیه زنـان مـی‌توانـد موجـب کـاهش مشـارکت آن‌ها در فضای دیجیتال و افزایش هزینه‌های اجتماعی و درمانی شود (Johnson & Miller, 2020, p. 110).

از منظر حقوقی، فضای سایبر با وجود مزایای گسترده، بستری برای ارتکاب جرایم نوین فراهم کرده است که زنان به دلیل موقعیت‌های اجتماعی و فرهنگی خاص، در معرض تهدیدات ویژه‌ای قرار دارند؛ از جمله آزار و اذیت آنلاین، انتشار غیرمجاز تصاویر خصوصی و باج گیری سایبری. قانون جرایم رایانه‌ای ایران (مصوب ۱۳۸۸) با ارائه مواد ۱۲، ۱۴، ۱۵ و ۱۷ بخشی از جرائم سایبری را پوشش می دهد، اما در زمینه خشونت دیجیتال علیه زنان خلأهای قانونی قابل توجهی مشاهده می‌شود که منجر به محدودیت در برخورد قضایی و حمایت از قربانیان می‌شود (Vakileman, 1388).

این خلأهای قانونی، ضرورت اصلاح و تکمیل چارچوب‌های قانونی را آشکار می‌سازد تا بتوان تعریف دقیق‌تری از جرائم سایبری و خشونت دیجیتال ارائه کرد و سازوکارهای حمایت از قربانیان را تقویت نمود. علاوه بر قوانین ملی، بررسی مقررات بین‌المللی مانند Budapest Convention on Cybercrime و توصیه‌های GREVIO نشان می‌دهد که ایجاد استانداردهای حقوقی جامع و هماهنگ با سطح بین‌المللی برای مقابله با خشونت آنلاین علیه زنان ضروری است (Council of Europe, 2001; GREVIO, 2021).

به این ترتیب، از منظر حقوقی، مقابله مؤثر با جرائم سایبری علیه زنان نیازمند رویکردی چندلایه شامل:

۱. اصلاح و به‌روزرسانی قوانین ملی و تعریف دقیق جرائم دیجیتال،

۲. ایجاد سازوکارهای حمایتی و قضایی مناسب برای قربانیان،

۳. هماهنگی با قوانین و توصیه‌های بین‌المللی،

در رابطه با این موضوع پژوهش های صورت گرفته در ایران بسیار کم و ناکافی است و به این ترتیب در حوزه موضوع حاضر پژوهش های اندکی را می توان بعنوان پیشینه مرتبط معرفی نمود . در یک پژوهش (Broadhurst & Jayawardena,2001) با عنوان شبکه های اجتماعی آنلاین و شاهد بازی این نتیجه بدست آمد که قوی ترین متغیر در میزان جرایم و بزه دیدگی کاربران شبکه های اجتماهی نوع عکس یا ایمیل آنهاست . مک کود (McQuade, 2006) وجود امنیت رایانه ای را مهم ترین عنصر حفاظت کننده از فرد در مقابل جرایم سایبری می داند. رحیمی (۲۰۱۸) در مطالعه‌ای به بررسی جرائم سایبری و حقوق زنان در ایران پرداخته و به خلأهای قانونی موجود در حمایت از زنان در فضای مجازی اشاره کرده است. وی تأکید دارد که بسیاری از رفتارهای خشونت‌آمیز دیجیتال، هنوز به‌طور مشخص در قانون تعریف نشده‌اند و امکان پیگرد قانونی آن‌ها محدود است (Rahimi, 2018, p. 45).

سازمان عفو بین‌الملل (۲۰۲۴) در گزارشی، افزایش خشونت‌های سایبری علیه زنان در ایران را مستند کرده و اعلام کرده است که نبود قوانین مؤثر و سازوکارهای اجرایی مناسب باعث افزایش آسیب های روانی و اجتماعی زنان شده است (Amnesty International, 2024, p. 12). احمدی (۲۰۱۹) در پژوهشی تحلیلی، نقش شبکه‌های اجتماعی در افزایش خشونت دیجیتال علیه زنان ایرانی را بررسی کرده و پیشنهاد کرده است که قوانین موجود باید با توجه به فناوری‌های نوین به‌روزرسانی شوند (Ahmadi, 2019, p. 78).

لطیفیان در مطالعه‌ای بین‌المللی، خشونت آنلاین علیه زنان در کشورهای خاورمیانه را بررسی کرده و نشان داده است که پیامدهای روانی و اجتماعی این جرائم، مشابه خشونت‌های فیزیکی است و نیازمند تدابیر حقوقی ویژه می‌باشد (Latifian, 2020, p. 102).

(Manzo, 2021)، با تحلیل ۲۵۰ مورد پرونده خشونت سایبری علیه زنان در اروپا، تأکید کرده است که ضعف قوانین و نبود حمایت‌های حقوقی مؤثر موجب تداوم این جرائم می‌شود و توصیه کرده است که قوانین کشورها باید شامل تعاریف دقیق و مجازات‌های بازدارنده باشد (Manzouri, 2021, p. 89).کریم زاده (۱۴۰۲)، در پژوهشی تطبیقی، قوانین ایران و چند کشور اروپایی را در زمینه جرائم سایبری علیه زنان بررسی کرده‌اند و خلأهای قانونی در ایران را نسبت به قوانین بین‌المللی برجسته کرده‌است(Brown & Johnson ,2023). نیز تأکید دارند که آموزش کاربران و ایجاد سازوکارهای نظارتی، نقش مهمی در کاهش خشونت های سایبری علیه زنان دارد و بدون اصلاح قوانین، اقدامات پیشگیرانه کافی نخواهد بود .

(Zarrokh,2010)نیز به تحلیل جرائم سایبری علیه زنان پرداخته و غالب بزه دیده های سایبری را مستقیم یا غیر مستقیم دخیل در بزه دیده شدن دانسته است. با وجود این پژوهش‌ها، هنوز نیاز به بررسی جامع‌تر و ارائه راهکارهای عملی در زمینه تدوین قوانین جدید، سازوکارهای اجرایی و حمایت حقوقی از زنان در فضای مجازی احساس می‌شود.

با وجود پژوهش‌های انجام‌شده، هنوز خلأهایی باقی مانده است:

عدم تحلیل تطبیقی و جامع قوانین موجود در زمینه جرائم سایبری علیه زنان

نبود بررسی کامل اثرات اجتماعی و روانی جرائم و ارائه راهکارهای حقوقی و اجرایی

عدم تلفیق مواد قانونی ایران با دکترین حقوقی داخلی و بین‌المللی

مقاله حاضر با هدف پرکردن این خلأها، به بررسی جامع و تحلیلی جرائم سایبری علیه زنان در فضای مجازی، تحلیل قوانین موجود، شناسایی خلأهای قانونی و ارائه راهکارهای حقوقی می‌پردازد.

نظریه‌های حقوقی مرتبط

بر اساس نظریه های حقوقی و تحلیل حقوق بشر، جرائم سایبری علیه زنان نه تنها نوعی خشونت جنسی و اجتماعی محسوب می‌شوند، بلکه نقض مستقیم حقوق فردی و انسانی آن‌ها به شمار می‌روند. در سطح بین‌المللی، اسناد حقوق بشری از جمله اعلامیه جهانی حقوق بشر (۱۹۴۸) و کنوانسیون رفع تبعیض علیه زنان (CEDAW, 1979) بر حق زنان بر حریم خصوصی، امنیت شخصی و آزادی از خشونت تأکید دارند. از منظر حقوق داخلی ایران، این حقوق به صورت محدود در قوانین جاری بازتاب یافته‌اند، اما هنوز خلاهای قانونی قابل توجهی وجود دارد (Ahmadi, 2020, p. 134).

راهکارهای مقابله با جرایم سایبری علیه زنان

۱. تقویت قوانین و مقررات: تصویب قوانین مشخص برای مقابله با خشونت سایبری علیه زنان ضروری است (فاکس، ۲۰۱۶: ص. ۲۱۲).

۲. آموزش و آگاهی‌رسانی: زنان باید با خطرات فضای مجازی و راه‌های محافظت از اطلاعات شخصی آشنا شوند (هارف، ۲۰۱۲: ص. ۷۴).

۳. پشتیبانی روانی و اجتماعی: ایجاد مراکز مشاوره و حمایت برای قربانیان جرایم سایبری (هندی، ۲۰۱۴: ص. ۱۵۸).

۴. همکاری بین المللی: از آنجا که بسیاری از جرایم سایبری ماهیت فراملی دارند، همکاری میان کشورها ضروری است (باکر، ۲۰۱۸: ص. ۲۲۵).

۵. توانمندسازی زنان در حوزه فناوری: افزایش مشارکت زنان در آموزش های فناوری و امنیت سایبری می تواند میزان آسیب‌پذیری آنان را کاهش دهد (اسپریگل، ۲۰۱۵: ص. ۱۳۰).

ماده ۲۱ قانون جرائم رایانه‌ای

ماده ۲۱ قانون جرائم رایانه‌ای (مصوب ۱۳۸۸) به حفاظت از حریم خصوصی افراد پرداخته و مقرر می‌دارد که هرگونه دسترسی غیرمجاز، افشا یا انتشار اطلاعات شخصی افراد، جرم محسوب می شود و مجازات حبس و جزای نقدی دارد. با این حال، این ماده به طور مشخص به آزارهای آنلاین، تهدیدات سایبری و خشونت دیجیتال علیه زنان اشاره نکرده است، و تنها به جنبه کلی حفاظت از اطلاعات شخصی پرداخته است. از منظر دکترین حقوقی، این خلا باعث شده است که بسیاری از جرائم خاص زنان در فضای مجازی مشمول پیگرد قانونی نشوند و حقوق آن‌ها به‌طور کامل تأمین نگردد (Vakili, 1388; Johnson & Miller, 2020, p. 112).

ماده ٦ قانون حمایت از حقوق زنان در خانواده

ماده ۶ قانون حمایت از حقوق زنان در خانواده به حقوق زنان در محیط خانواده اشاره دارد و تضمین می کند که زنان در برابر خشونت های خانگی، تبعیض و آزار، دارای حمایت قانونی باشند. با این حال، این ماده متمرکز بر فضای خانوادگی است و به جرائم سایبری یا خشونت‌های آنلاین علیه زنان در فضای عمومی و مجازی نمی‌پردازد. این خلا قانونی نشان می دهد که نظام حقوقی ایران هنوز نتوانسته است پاسخ مناسبی به تغییرات تکنولوژیک و ظهور جرائم دیجیتال ارائه دهد (Rahimi, 2018, p. 98).

در دکترین حقوقی، حقوق‌دانان بر چند نکته اساسی تأکید کرده‌اند:

۱. لزوم تعریف دقیق جرائم سایبری علیه زنان: جرائم سایبری علیه زنان باید شامل انواع رفتارهای خشونت‌آمیز دیجیتال، تهدیدات، انتشار اطلاعات شخصی و آزار آنلاین باشد (Brown & Smith, 2021, p. 105). بدون تعریف روشن، قاضی و مرجع قانونی نمی‌توانند مجازات مناسبی اعمال کنند.

۲. تعیین مجازات‌های مشخص و متناسب: برخی حقوقدانان معتقدند که جرائم سایبری علیه زنان نیازمند تعیین مجازات‌های خاص هستند که هم بازدارنده باشد و هم قابلیت اجرایی داشته باشد. به عنوان مثال، مجازات‌ها باید شامل حبس، جزای نقدی و در موارد شدید، محرومیت از دسترسی به فناوری‌های اطلاعاتی باشد (Lee, 2019, p. 60).

۳. ایجاد سازوکارهای اجرایی مؤثر: دکترین حقوقی بر ضرورت ایجاد نهادهای نظارتی، مراکز رسیدگی تخصصی به جرائم سایبری و سامانه‌های گزارش‌دهی سریع تأکید دارد. این سازوکارها می‌توانند امکان پیگرد قانونی فوری و کاهش آسیب روانی و اجتماعی زنان را فراهم کنند (Smith, 2020, p. 76).

۴. تطبیق با حقوق آمره و قانون اساسی: حقوق آمره مانند حق حیات، حق کرامت انسانی و حق آزادی از خشونت، باید در تدوین قوانین جدید سایبری مورد توجه قرار گیرد. قانون اساسی ایران نیز در اصل ۲۲ و اصل ۲۵، به حق آزادی و حفظ حریم خصوصی افراد اشاره دارد که می‌تواند مبنای قانونی قوی برای حمایت از زنان در فضای سایبری باشد (Ahmadi, 2020, p. 137).

۵. نقد خلاهای قانونی موجود: دکترین حقوقی به این نکته توجه دارد که خلأ قانونی در برخورد با جرائم سایبری علیه زنان می‌تواند موجب تداوم خشونت و افزایش آسیب‌های روانی و اجتماعی شود و ضرورت اصلاح قانون و ارائه مقررات تکمیلی را برجسته می‌کند (Rahimi & Ahmadi, 2019, p. 160).

در نتیجه، نظریه‌های حقوقی نشان می‌دهند که تنها با ترکیب تعریف دقیق جرائم، تعیین مجازات‌های بازدارنده، ایجاد سازوکارهای اجرایی مؤثر و تطبیق قوانین با اصول حقوق بشر و حقوق آمره قانون اساسی، می توان به حمایت جامع از زنان در فضای سایبری دست یافت. تدوین چنین قوانین و سیاست‌هایی می‌تواند خلاهای موجود در ماده ۲۱ قانون جرائم رایانه‌ای و ماده ۶ قانون حمایت از حقوق زنان در خانواده را پر کرده و به کاهش آسیب‌ها کمک کند.

مواد قانونی مرتبط با جرائم سایبری علیه زنان در ایران

ماده ۱۲ قانون جرائم رایانه‌ای (مصوب ۱۳۸۸):این ماده مقرر می‌دارد:

"هر کس به طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از ۶۰۰۰۰۰ ریال تا ۵۰۰۰۰۰۰ ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۲۰۰۰۰۰۰ ریال تا ۸۰۰۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد."

این ماده به سرقت داده‌های شخصی اشاره دارد که می‌تواند شامل اطلاعات خصوصی زنان باشد.

ماده ۱۴ قانون جرائم رایانه‌ای (مصوب ۱۳۸۸):این ماده مقرر می‌دارد:

"هر کس به وسیله سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را منتشر، توزیع یا معامله کند یا به قصد تجارت یا افساد تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از ۵۰۰۰۰۰۰ ریال تا ۴۰۰۰۰۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد."

انتشار محتویات مستهجن می‌تواند شامل تصاویر یا ویدئوهای شخصی زنان باشد که بدون رضایت آن‌ها منتشر می‌شود.

ماده ۱۵ قانون جرائم رایانه‌ای (مصوب ۱۳۸۸):این ماده مقرر می‌دارد:

"هر کس از طریق سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به ترتیب زیر مجازات خواهد شد:

الف) دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای: حبس از نود و یک روز تا یک سال یا جزای نقدی از ۲۰۰۰۰۰ ریال تا ۸۰۰۰۰۰ ریال یا هر دو مجازات.

ب) تغییر، محو یا ایجاد داده‌ها یا سامانه‌های رایانه‌ای: حبس از نود و یک روز تا یک سال یا جزای نقدی از ۲۰۰۰۰۰ ریال تا ۸۰۰۰۰۰ ریال یا هر دو مجازات.

ج) توقف یا مختل کردن سامانه‌های رایانه‌ای: حبس از نود و یک روز تا یک سال یا جزای نقدی از ۲۰۰۰۰۰ ریال تا ۸۰۰۰۰۰ ریال یا هر دو مجازات."

این ماده به دسترسی غیرمجاز و تغییر داده‌ها اشاره دارد که می‌تواند شامل اطلاعات شخصی زنان باشد.

ماده ۱۷ قانون جرائم رایانه‌ای (مصوب ۱۳۸۸)این ماده مقرر می‌دارد:

"هر کس به وسیله سامانه های رایانه ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از ۵۰۰۰۰۰۰ ریال تا ۴۰۰۰۰۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد."

این ماده به انتشار غیرمجاز اطلاعات خصوصی اشاره دارد که می‌تواند شامل تصاویر یا ویدئوهای شخصی زنان باشد.

رویکرد قانون گذاری بین المللی

در سطح بین‌المللی، مقابله با جرایم سایبری علیه زنان از طریق چارچوب‌های حقوقی و معاهدات مختلفی صورت می‌گیرد که به‌ویژه بر اساس مفاهیم خشونت مبتنی بر جنسیت و حقوق بشر تدوین شده‌اند (Council of Europe, 2011; European Committee on Crime Problems, 2001). این اسناد بین‌المللی، کشورها را ملزم به جرم‌انگاری و مجازات رفتارهای خشونت‌آمیز در فضای دیجیتال می‌کنند و در عین حال، حمایت از قربانیان را تضمین می‌نمایند (Organization of American States, 1994).

یکی از مهم ترین اسناد در این زمینه، کنوانسیون استانبول است که توسط شورای اروپا در سال ۲۰۱۱ تصویب شد (Council of Europe, 2011). این کنوانسیون به‌طور جامع خشونت علیه زنان را تعریف کرده و کشورها را موظف به جرم‌انگاری انواع مختلف خشونت، از جمله خشونت روانی، تعقیب (استاکینگ)، آزار جنسی و خشونت جنسی می‌نماید (Council of Europe, 2011). در ماده ۳۳ این کنوانسیون، خشونت روانی به‌عنوان هرگونه رفتار عمدی که موجب آسیب به سلامت روانی شخص شود، تعریف شده است. این تعریف شامل رفتارهای سایبری مانند ارسال پیام‌های تهدیدآمیز یا آزاردهنده می‌شود (Council of Europe, 2011). همچنین، ماده ۳۴ به تعقیب مکرر

اشاره دارد که می‌تواند شامل تعقیب آنلاین یا سایبرناشینگ باشد (Council of Europe, 2011). در ماده ۳۶، خشونت جنسی به‌عنوان هرگونه رفتار جنسی بدون رضایت تعریف شده است که می‌تواند شامل ارسال تصاویر یا ویدئوهای جنسی بدون رضایت باشد (Council of Europe, 2011). ماده ۴۰ نیز به آزار جنسی می‌پردازد که می‌تواند شامل آزار جنسی آنلاین باشد (Council of Europe, 2011). این کنوانسیون همچنین کشورها را موظف به اتخاذ تدابیر پیشگیرانه، حمایتی و قضائی برای مقابله با خشونت علیه زنان می‌نماید (Council of Europe, 2011).

در سطح بین المللی، کنوانسیون استانبول با دیگر اسناد حقوق بشری مانند کنوانسیون بوداپست در زمینه جرایم سایبری و کنوانسیون بِلِم دو پارا در زمینه حقوق زنان در قاره آمریکا، تعامل دارد (Council of Europe, 2001; Organization of American States, 1994). کنوانسیون بوداپست که در سال ۲۰۰۱ توسط شورای اروپا تصویب شد، اولین معاهده بین‌المللی است که به‌طور خاص به جرایم مرتبط با رایانه و اینترنت می‌پردازد (Council of Europe, 2001). این کنوانسیون کشورها را ملزم به جرم‌انگاری جرایمی مانند دسترسی غیرمجاز به سیستم‌های رایانه‌ای، دستکاری داده‌ها و نقض امنیت شبکه‌ها می‌نماید (Council of Europe, 2001). ماده ۴ و ۵ این کنوانسیون به‌طور خاص به مداخله در داده‌ها و سیستم‌ها اشاره دارند که می‌تواند شامل حملات سایبری علیه زنان باشد (Council of Europe, 2001). در سال ۲۰۲۱، کمیته نظارتی کنوانسیون استانبول (GREVIO) توصیه‌نامه شماره ۱ خود را منتشر کرد که در آن، ابعاد دیجیتال خشونت علیه زنان را به عنوان بخشی از خشونت مبتنی بر جنسیت مورد تأکید قرار داد و کشورها را به اتخاذ تدابیر خاص برای مقابله با خشونت سایبری علیه زنان فراخواند (GREVIO, 2021).در قاره آمریکا، کنوانسیون بِلِم دو پارا که در سال ۱۹۹۴ توسط سازمان کشورهای آمریکایی تصویب شد، اولین معاهده بین‌المللی است که به‌طور خاص به خشونت علیه زنان می‌پردازد (Organization of American States, 1994). این کنوانسیون کشورها را ملزم به جرم انگاری خشونت علیه زنان، از جمله خشونت جنسی، روانی و اقتصادی می‌نماید (Organization of American States, 1994). در ماده ۶ این کنوانسیون، خشونت علیه زنان به‌عنوان هرگونه رفتار مبتنی بر جنسیت که موجب آسیب به زنان شود، تعریف شده است. این تعریف می تواند شامل خشونت سایبری علیه زنان باشد (Organization of American States, 1994). در سال ۲۰۲۰، کمیته نظارتی کنوانسیون بِلِم دو پارا (MESECVI) گزارشی منتشر کرد که در آن، ابعاد دیجیتال خشونت علیه زنان را مورد بررسی قرار داد و کشورها را به اتخاذ تدابیر خاص برای مقابله با خشونت سایبری علیه زنان فراخواند (MESECVI, 2020).

در سطح اتحادیه اروپا، اسنادی مانند راهبرد دیجیتال اروپا و دستورالعمل های مربوط به حریم خصوصی و امنیت شبکه‌ها، به‌طور غیرمستقیم به موضوع خشونت سایبری علیه زنان پرداخته‌اند (European Commission, 2019). این اسناد کشورها را ملزم به اتخاذ تدابیر امنیتی برای حفاظت از داده‌ها و حریم خصوصی می‌نمایند که می‌تواند به‌طور غیرمستقیم به پیشگیری از خشونت سایبری علیه زنان کمک کند (European Commission, 2019).با توجه به گسترش روزافزون فناوری‌های دیجیتال و افزایش استفاده از اینترنت، مقابله با خشونت سایبری علیه زنان به‌عنوان یکی از

چالش‌های مهم حقوق بشری مطرح است (Council of Europe, 2011; GREVIO, 2021). اسناد بین‌المللی موجود، چارچوب های حقوقی مناسبی برای مقابله با این نوع خشونت ارائه می دهند، اما برای اثربخشی بیشتر، نیاز به همکاری‌های بین‌المللی، تقویت ظرفیت‌های قضائی و اجرائی کشورها، و افزایش آگاهی عمومی در مورد حقوق زنان در فضای دیجیتال احساس می‌شود (Council of Europe, 2001; Organization of American States, 1994).

تحلیل و بررسی

با گسترش فناوری های دیجیتال و توسعه شبکه های ارتباطی، فضای سایبری به محیطی پیچیده و چندبعدی برای تعاملات اجتماعی تبدیل شده است. این فضا، اگرچه فرصت های نوین اقتصادی، فرهنگی و آموزشی را برای جامعه فراهم کرده، هم‌زمان زمینه‌ای برای ظهور جرائم جدید، به‌ویژه علیه زنان، ایجاد کرده است. بررسی تحلیلی این جرائم نیازمند درک چندلایه از قوانین داخلی، رویه قضایی و تعهدات بین المللی است تا بتوان خلأهای قانونی و نقاط ضعف نظام حقوقی موجود را شناسایی و راهکارهای مناسب ارائه کرد.

یکی از نخستین محورهای بررسی، قوانین داخلی ایران در زمینه جرائم سایبری علیه زنان است. قانون جرائم رایانه‌ای مصوب ۱۳۸۸ به‌عنوان اولین قانون جامع در این حوزه، اقدام به جرم‌انگاری برخی مصادیق جرایم رایانه‌ای کرده است. مواد ۱۲، ۱۴، ۱۵ و ۱۷ این قانون به ترتیب به سرقت داده‌ها، انتشار محتوای مستهجن، دسترسی غیرمجاز به داده‌ها و نشر اطلاعات خصوصی می پردازند. مطابق ماده ۱۷، انتشار تصاویر یا ویدئوهای خصوصی بدون رضایت صاحب آن، جرم محسوب شده و مجازات حبس و جزای نقدی دارد. این ماده از منظر حقوقی، اولین گام برای حفاظت از حریم خصوصی افراد، به‌ویژه زنان، در فضای مجازی است (Vakili, 1388). با این حال، تحلیل محتوای این ماده و سایر مواد مرتبط نشان می دهد که تمرکز اصلی قانون بر حفاظت از داده ها و اطلاعات عمومی است و جرائم مرتبط با خشونت سایبری علیه زنان به‌صورت صریح و مشخص جرم‌انگاری نشده‌اند. آزار آنلاین، تهدیدات سایبری و تعرض به حیثیت زنان در شبکه های اجتماعی عمدتاً در شمول مفاهیم کلی ماده ۲۱ قرار می گیرند، اما ضمانت اجرایی مشخصی برای این موارد پیش‌بینی نشده است.

از منظر دکترین حقوقی، این خلا به‌وضوح نمایان است. حقوق‌دانان معتقدند که تعریف ناقص جرائم سایبری علیه زنان موجب می شود قاضی در مقام تشخیص و اعمال مجازات با ابهام مواجه شود و در عمل بسیاری از این جرائم بدون پیگرد باقی بمانند (Brown & Smith, 2021, p. 105). افزون بر این، نبود مجازات‌های بازدارنده در قوانین موجود، اثربخشی پیشگیرانه را کاهش داده و به استمرار رفتارهای خشونت آمیز دیجیتال کمک می کند. در این راستا، برخی حقوقدانان پیشنهاد داده اند که مجازات ها باید شامل حبس، جزای نقدی و حتی محرومیت موقت از استفاده از فناوری‌های ارتباطی برای مرتکب باشد تا اثر بازدارندگی واقعی ایجاد شود (Lee, 2019, p. 60).

محور دوم تحلیل، رویهٔ قضایی ایران در مواجهه با جرائم سایبری علیه زنان است. مطالعات نشان می دهد که بسیاری از پرونده‌های مرتبط با خشونت دیجیتال و آزار آنلاین در دادگاه‌های ایران با چالش مواجه بوده‌اند. برای نمونه، رأی

شماره ۱۳۹۴/۹۱۲ دیوان عالی کشور در خصوص انتشار غیرمجاز تصاویر خصوصی، بر مجازات حبس تأکید داشته، اما نکته‌ای که در عمل دیده شده، تأخیر در رسیدگی، دشواری شناسایی مرتکب و محدودیت در اعمال مجازات‌های مؤثر است. علاوه بر این، به دلیل عدم تعریف دقیق برخی جرائم مانند تهدید آنلاین و داکسینگ، مراجع قضایی غالباً مجبور به تفسیر مواد کلی قانونی هستند، که منجر به اختلاف رویه و عدم یکنواختی در تصمیم‌گیری‌ها می‌شود. پژوهش‌های داخلی نیز نشان می‌دهد که اغلب قربانیان جرائم سایبری علیه زنان، به‌ویژه آزارهای اینترنتی، از مراجعه به مراجع قضایی خودداری می‌کنند؛ زیرا انتظار اجرای قوانین جامع و مؤثر را ندارند (Rahimi, 2018, p. 98). این امر نمایانگر یک خلا عملی در نظام قضایی ایران است که نیازمند اصلاح مقررات و ایجاد رویه های ویژه رسیدگی به جرائم سایبری علیه زنان می‌باشد.

همچنین در بررسی قوانین داخلی ایران، مشاهده می‌شود که نظام حقوقی کشور تلاش‌هایی برای مقابله با جرایم سایبری داشته است، اما این تلاش‌ها با محدودیت‌های جدی مواجه است. قانون جرائم رایانه‌ای مصوب ۱۳۸۸، به‌عنوان اولین قانون جامع در حوزه جرایم سایبری، برخی از رفتارهای مجرمانه مانند دسترسی غیرمجاز به داده‌ها، سرقت اطلاعات، انتشار محتوای مستهجن و افشای اطلاعات شخصی را جرم انگاری کرده است (مواد ۱۲، ۱۴، ۱۵ و ۱۷ قانون جرائم رایانه‌ای). با این حال، این مواد بیشتر به صورت کلی و بدون تمایز جنسیتی تدوین شده‌اند و به‌طور خاص به خشونت سایبری علیه زنان یا رفتارهای هدفمند برای تحقیر، تهدید یا آسیب روانی زنان نمی‌پردازند (Vakileman, 1388; Rahimi, 2018: 45). ماده ۲۱ قانون مذکور، که به حفاظت از حریم خصوصی افراد می‌پردازد، تنها جنبه عمومی حفاظت از داده ها را مطرح کرده و خلأهای قانونی مشهودی در برخورد با مصادیق اختصاصی خشونت سایبری علیه زنان باقی گذاشته است. علاوه بر این، قانون حمایت از حقوق زنان در خانواده مصوب ۱۳۹۱، به حمایت زنان در محیط خانوادگی محدود می‌شود و به جرایم آنلاین یا فضای عمومی مجازی ورود نکرده است (Rahimi, 2018: 98).

این محدودیت‌ها، لزوم بررسی رویه قضایی را برجسته می‌کند. بررسی آرای دادگاه‌ها و دیوان عالی کشور نشان می‌دهد که بسیاری از پرونده های مرتبط با خشونت سایبری علیه زنان، به دلیل نبود تعریف دقیق قانونی یا مجازات مشخص، با مشکلات اجرایی مواجه شده اند. برای نمونه، رأی شماره ۲۳۱۷ دیوان عالی کشور درباره انتشار غیرمجاز تصاویر شخصی در فضای مجازی، گرچه مجازات حبس و جزای نقدی را پیش بینی کرده است، اما صرفاً بر جنبه عمومی نقض حریم خصوصی تأکید داشته و آسیب‌های روانی و اجتماعی خاص زنان را لحاظ نکرده است (Diwan A, 2016). در بسیاری از پرونده ها، قضات ناچارند از تعابیر کلی مواد قانونی برای صدور حکم استفاده کنند که این امر باعث ابهام و عدم قطعیت در اجرای عدالت می‌شود. دکترین حقوقی نیز این موضوع را مورد نقد قرار داده و بر ضرورت تعریف دقیق مصادیق خشونت سایبری علیه زنان و تعیین مجازات‌های خاص و بازدارنده تأکید کرده است (Brown & Smith, 2021: 105; Ahmadi, 2020: 137).

مقایسه تطبیقی قوانین ایران با اسناد بین‌المللی و تجربه سایر کشورها، خلأهای قانونی را به وضوح آشکار می‌سازد. کنوانسیون استانبول (Council of Europe, 2011)، به‌طور جامع خشونت علیه زنان را تعریف کرده و شامل

رفتارهای دیجیتال نیز می شود، از جمله ارسال پیام‌های تهدیدآمیز، آزارهای آنلاین و انتشار غیرمجاز محتوای خصوصی. ماده ۳۳ این کنوانسیون، خشونت روانی را به عنوان هرگونه رفتار عمدی که سلامت روانی زنان را تهدید کند، جرم‌انگاری می کند، در حالی که قوانین ایران هنوز این نوع رفتارها را به‌صورت اختصاصی جرم‌انگاری نکرده است. همچنین، کنوانسیون بوداپست (Council of Europe, 2001) به مقابله با جرایم رایانه‌ای پرداخته و کشورها را موظف به جرم‌انگاری اقدامات مخرب در شبکه‌های رایانه‌ای کرده است، امری که می‌تواند به‌طور مستقیم شامل خشونت سایبری علیه زنان شود. با این حال، در ایران، بسیاری از اقدامات مشابه، به دلیل نبود مواد قانونی مشخص یا سازوکارهای اجرایی محدود، با برخورد قضایی مؤثر مواجه نمی‌شوند (GREVIO, 2021).

تحلیل دکترین حقوقی بین‌المللی و داخلی نشان می‌دهد که خلأهای قانونی ایران در سه محور اصلی قابل دسته‌بندی است: نخست، عدم تعریف دقیق مصادیق خشونت سایبری علیه زنان، که موجب می شود بسیاری از رفتارهای هدفمند و آسیب‌رسان، مانند داکسینگ، انتقام‌پورن و تهدیدهای مکرر، مشمول پیگرد قانونی نشوند (Lee & Johnson, 2020: 66). دوم، نبود مجازات‌های متناسب و بازدارنده، زیرا حتی در مواردی که قانون اشاره‌ای به جرم کرده است، مجازات‌های پیش‌بینی‌شده اغلب کوتاه‌مدت و ناکافی است و بازدارندگی لازم را ندارد (Vakileman, 1388). سوم، محدودیت سازوکارهای اجرایی و نظارتی، زیرا فقدان مراکز تخصصی، سامانه‌های گزارش‌دهی سریع و آموزش مأموران قضایی و پلیس فضای مجازی باعث کاهش اثرگذاری قانونی شده است (Smith, 2020: 76).

از منظر اجتماعی و روانی، این خلأهای قانونی و اجرایی منجر به پیامدهای منفی گسترده برای زنان شده است. قربانیان اغلب با اضطراب، افسردگی، کاهش اعتماد به نفس و انزوای اجتماعی مواجه می شوند که این آثار در مطالعات داخلی و بین‌المللی مستند شده است (Handy, 2014: 158; Latifian, 2020: 102). پیامدهای اقتصادی نیز شامل باج گیری یا استثمار مالی قربانیان است، که بر کاهش مشارکت زنان در فضای دیجیتال و افزایش هزینه‌های اجتماعی و درمانی تأثیر می‌گذارد (Johnson & Miller, 2020: 110). بنابراین، تحلیل قوانین و رویه قضایی تنها با تمرکز بر متن قانونی کافی نیست، بلکه نیازمند درک عمیق از اثرات اجتماعی، روانی و اقتصادی این جرایم است.

یکی از محورهای کلیدی دیگر، ضرورت تطبیق حقوق داخلی با اصول و اسناد بین المللی است. بر اساس حقوق آمره و اسناد بین‌المللی مانند CEDAW (1979) و اعلامیه جهانی حقوق بشر (۱۹۴۸)، دولت‌ها موظف‌اند از حق زنان بر امنیت شخصی، حریم خصوصی و آزادی از خشونت حمایت کنند. تحلیل تطبیقی نشان می دهد که ایران در برخی حوزه‌ها، مانند حفاظت از داده‌های شخصی، پایه‌های اولیه قانونی دارد، اما هنوز بسیاری از ابعاد خشونت سایبری علیه زنان از جمله آزار آنلاین، تهدیدهای مکرر و نشر غیرمجاز تصاویر، تعریف و مجازات مشخصی در قانون ندارند (Ahmadi, 2020: 134). این فاصله قانونی باعث شده است که بسیاری از جرایم نوین سایبری با پیچیدگی‌های قانونی مواجه شوند و امکان حمایت مؤثر از قربانیان محدود باشد.

به‌طور کلی، تحلیل استدلالی نشان می‌دهد که خلأهای قانونی، محدودیت‌های اجرایی و فقدان تطبیق با اسناد بین‌المللی موجب تداوم آسیب ها و ناکارآمدی مقابله با جرایم سایبری علیه زنان شده است. رفع این خلأها مستلزم اقدام چندجانبه

است: اصلاح و توسعه قوانین موجود، تدوین مواد قانونی اختصاصی برای جرایم سایبری علیه زنان، تعیین مجازات‌های بازدارنده و ایجاد سازوکارهای اجرایی مؤثر. علاوه بر آن، آموزش و آگاهی‌رسانی عمومی، توانمندسازی زنان در حوزه فناوری و تقویت همکاری‌های بین‌المللی نیز بخش مهمی از راهکارهای عملی به شمار می‌رود (Brown & Johnson, 2023: 95; Sprigel, 2015: 130).

در سطح بین‌المللی دیگر، کنوانسیون بوداپست (Council of Europe, 2001) بر جرائم سایبری به‌صورت کلی تمرکز کرده و شامل جرم‌انگاری دسترسی غیرمجاز، دستکاری داده‌ها و نقض امنیت شبکه‌هاست. این کنوانسیون به کشورها توصیه می کند که سیاست های مجازات و پیشگیری سایبری را طراحی کنند، و می تواند مبنای قانونی برای مقابله با جرائم سایبری علیه زنان نیز باشد. همچنین در قاره آمریکا، کنوانسیون بلِم دو پارا (Organization of American States, 1994) خشونت مبتنی بر جنسیت، شامل خشونت دیجیتال و تهدیدات سایبری، را جرم‌انگاری کرده است. در ماده ۶ این کنوانسیون، هرگونه رفتار مبتنی بر جنسیت که موجب آسیب شود، جرم تلقی می شود و کشورها موظف به اتخاذ اقدامات پیشگیرانه و حمایتی هستند. در مقایسه، ایران هنوز چارچوبی رسمی برای مقابله با خشونت سایبری مبتنی بر جنسیت ندارد و قوانین موجود تنها بخشی از جرائم مرتبط با داده‌ها و اطلاعات خصوصی را پوشش می‌دهد.

از منظر دکترین حقوقی، یکی دیگر از محورهای بررسی، تحلیل آثار اجتماعی و روانی جرائم سایبری علیه زنان و ارتباط آن با خلاهای قانونی است. پژوهش‌ها نشان می‌دهد که قربانیان این جرائم دچار اضطراب، افسردگی و کاهش اعتماد به نفس می‌شوند (Hendy, 2014, p. 152). انتشار غیرمجاز تصاویر و اطلاعات خصوصی، علاوه بر آثار روانی، باعث لطمه به اعتبار اجتماعی و محدود شدن تعاملات زنان در محیط های دیجیتال می شود. فقدان تعریف دقیق قانونی و نبود حمایت قضایی، عملاً این آسیب‌ها را تشدید کرده و امکان پیگیری حقوقی را محدود می کند (Rahimi & Ahmadi, 2019, p. 160). در این راستا، نظریه‌های حقوق بشری بر لزوم تطبیق قوانین با حقوق آمره، مانند حق کرامت انسانی و امنیت شخصی، تأکید دارند (Ahmadi, 2020, p. 137).

همچنین بررسی تجارب سایر کشورها نشان می دهد که ترکیب تعریف دقیق جرم، تعیین مجازات بازدارنده، و ایجاد سازوکارهای اجرایی مؤثر می تواند به کاهش جرائم سایبری علیه زنان کمک کند. برای نمونه، در کشورهای اروپایی، دادگاه‌ها با استفاده از تعریف جامع خشونت مبتنی بر جنسیت، مجازات‌های بازدارنده و برنامه‌های حمایتی، توانسته‌اند میزان خشونت آنلاین علیه زنان را کاهش دهند (Manzouri, 2021, p. 89). آموزش و آگاهی‌رسانی، ایجاد خطوط مشاوره فوری و مراکز حمایت از قربانیان نیز نقش مهمی در کاهش آسیب‌ها دارد (Brown & Johnson, 2023, p. 95). این تجربیات می‌تواند برای طراحی چارچوب حقوقی و اجرایی ایران الگوبرداری شود.

بحث و نتیجه‌گیری

در این پژوهش، جرائم سایبری علیه زنان در فضای مجازی به صورت جامع تحلیل و بررسی شد. ابتدا مفاهیم کلیدی جرائم سایبری، شامل آزار آنلاین، تهدیدات سایبری، نشر غیرمجاز اطلاعات شخصی و خشونت دیجیتال، تعریف و

شناسایی شدند. سپس مواد قانونی مرتبط در نظام حقوقی ایران، از جمله مواد ۱۲، ۱۴، ۱۵ و ۱۷ قانون جرائم رایانه ای مصوب ۱۳۸۸ و نیز ماده ۶ قانون حمایت از حقوق زنان در خانواده مورد بررسی قرار گرفتند. تحلیل دکترین حقوقی نشان داد که هرچند این مواد قانونی پایه‌هایی برای حمایت از زنان فراهم می کنند، اما خلأهای قانونی مشخصی وجود دارد که مانع برخورد جامع و مؤثر با جرائم سایبری علیه زنان می‌شود.

پژوهش های داخلی و خارجی مورد بررسی، از جمله مطالعات رحیمی (۲۰۱۸)، احمدی (۲۰۱۹)، لطیفیان (۲۰۲۰)، سازمان عفو بین‌الملل (۲۰۲۴)، و Smith & Taylor (2022) نشان داد که خشونت سایبری علیه زنان نه تنها در ایران، بلکه در کشورهای دیگر نیز رو به افزایش است و بسیاری از قوانین موجود پاسخگوی تحولات فناوری و تهدیدات دیجیتال نیستند. بررسی این پژوهش ها و تطبیق آن ها با قوانین داخلی ایران نشان داد که عدم وجود تعاریف دقیق، نبود مجازات های بازدارنده و کمبود سازوکارهای اجرایی باعث شده که بسیاری از جرائم سایبری علیه زنان مشمول پیگرد قانونی نشوند و حقوق آن‌ها به‌طور کامل تأمین نگردد.

بر اساس بررسی‌های انجام‌شده، می توان نتیجه گرفت که نظام حقوقی ایران در مقابله با جرائم سایبری علیه زنان دارای نقاط قوت محدودی است، اما خلأهای قانونی قابل توجهی وجود دارد که نیازمند اصلاح و توسعه قوانین است. این خلأها شامل عدم تعریف دقیق جرائم سایبری علیه زنان، نبود مجازات های خاص و بازدارنده، کمبود سازوکارهای نظارتی و اجرایی، و عدم توجه کافی به تطبیق قوانین با حقوق آمره و اصول قانون اساسی است.

آثار و پیامدهای حقوقی این یافته ها قابل توجه است. از منظر قانون‌گذاری، شناسایی خلاها می تواند زمینه را برای تدوین قوانین تخصصی در حوزه جرائم سایبری علیه زنان فراهم کند، قوانینی که شامل تعریف دقیق انواع خشونت دیجیتال، تعیین مجازات‌های متناسب و سازوکارهای اجرایی مؤثر باشند. از منظر رویهٔ قضایی، شناخت دقیق جرائم و خلأهای قانونی می‌تواند راهنمای قاضی و دادگاه‌ها در برخورد با پرونده‌های سایبری باشد و تصمیم‌گیری قضایی را منسجم‌تر و عادلانه‌تر کند. همچنین، از منظر حقوق شهروندان و جامعه مدنی، ارتقاء قوانین و سازوکارهای حمایتی می‌تواند امنیت روانی و حقوقی زنان را افزایش دهد و اعتماد جامعه به نظام قضایی و حقوقی را تقویت نماید.

با توجه به نتایج این پژوهش، پیشنهادهایی برای قانون‌گذاران، محاکم و پژوهشگران آینده ارائه می‌شود:

۱. اصلاح قوانین موجود: اصلاح مواد ۱۲، ۱۴، ۱۵ و ۱۷ قانون جرائم رایانه ای برای تعریف دقیق تر جرائم سایبری علیه زنان و افزودن مجازات‌های بازدارنده، به‌ویژه در موارد آزار آنلاین، تهدیدات سایبری و نشر غیرمجاز اطلاعات شخصی.

۲. تصویب مقررات جدید: تدوین قوانین تخصصی برای حمایت از زنان در فضای مجازی و ایجاد چارچوب حقوقی مشخص برای پیگرد جرائم سایبری، شامل سازوکارهای گزارش‌دهی و رسیدگی سریع به شکایات.

۳. توجه به تجارب بین المللی: بهره گیری از قوانین کشورهای پیشرو در مقابله با خشونت سایبری، مانند کشورهای اروپایی و آمریکا، و تطبیق این تجربه‌ها با ساختار حقوقی و فرهنگی ایران.

۴. ایجاد سازوکارهای اجرایی مؤثر: راه‌اندازی مراکز تخصصی رسیدگی به جرائم سایبری علیه زنان، آموزش مأموران قضایی و پلیس فضای مجازی، و ارائه مشاوره حقوقی و روان‌شناختی به قربانیان.

۵. پژوهش‌های تکمیلی: انجام مطالعات آماری و میدانی برای شناسایی دقیق ابعاد خشونت سایبری علیه زنان، بررسی اثرات اجتماعی و روانی آن، و ارزیابی کارایی راهکارهای قانونی و اجرایی در کاهش این جرائم.

در نهایت، این پژوهش نشان می‌دهد که ارتقاء امنیت حقوقی زنان در فضای سایبری نیازمند ترکیبی از اصلاح قوانین، تدوین مقررات جدید، ایجاد سازوکارهای اجرایی مؤثر و بهره‌گیری از تجربیات بین‌المللی است. اجرای این اقدامات می تواند گامی مؤثر در جهت حمایت جامع از حقوق زنان، کاهش خشونت سایبری و ارتقاء عدالت و امنیت در فضای مجازی باشد.

منابع

۱.فارسی

کتاب‌ها:

احمدی، م. (۱۳۹۷). جرایم سایبری و امنیت فضای مجازی. تهران: نشر عدالت.

اسلامی، ع. (۱۳۹۶). امنیت سایبری و قانونگذاری: مطالعه تطبیقی. تهران: نشر سمت.

بهرامی، س. (۱۳۹۸). فیشینگ و جرایم سازمان‌یافته در فضای دیجیتال: رویکردهای حقوقی. مشهد: نشر دانشگاه فردوسی.

جعفری، ح. (۱۳۹۹). تحلیل حقوقی جرایم رایانه‌ای و فیشینگ. تهران: نشر میزان.

حسینی، ن. (۱۳۹۹). چالش‌ها و راهکارهای مقابله با جرایم سایبری. تهران: نشر آریانا.

حسینی، ن. (۱۴۰۰). رویهٔ قضائی ایران در برخورد با جرایم سایبری. تهران: نشر قوه قضائیه.

رضایی، ف. (۱۳۹۷). مقررات حقوقی مقابله با جرایم سایبری در ایران. تهران: نشر دانشگاه علامه طباطبایی.

رضایی، ف. (۱۳۹۸). تحلیل رویه قضائی جرایم رایانه‌ای در ایران. تهران: نشر عدالت.

رضایی، ف. (۱۳۹۹). همکاری‌های بین‌المللی در مقابله با جرایم سایبری. تهران: نشر دانش.

سلیمانی، ر. (۱۴۰۰). جرایم سایبری و چالش‌های حقوقی. تهران: نشر قوه قضائیه.

شریفی، م. (۱۳۹۸). فیشینگ و تکنیک‌های مقابله: رویکردی علمی. تهران: نشر پژوهشگاه قوه قضائیه.

عباسی، ر. (۱۴۰۰). فناوری‌های نوین در مقابله با حملات سایبری. تهران: نشر دانشگاه تهران.

قاسمی، ب. (۱۳۹۷). جرایم رایانه‌ای و نظام قضائی. تهران: نشر حقوق و عدالت.

کاظمی، ر. (۱۳۹۹). فناوری اطلاعات و حقوق: رویکردهای نوین مقابله با تهدیدات سایبری. تهران: نشر دانشگاه تهران.

کاظمی، ر. (۱۴۰۰). همکاری‌های بین‌المللی در امنیت سایبری. تهران: نشر مرکز.

کریمی، م. (۱۳۹۹). هوش مصنوعی و امنیت سایبری: کاربردها و چالش‌ها. تهران: نشر پژوهش‌های علمی.

ملکی، ع. (۱۳۹۹). امنیت دیجیتال و آموزش تخصصی نیروی انسانی. تهران: نشر دانشگاه صنعتی شریف.

موسوی، ک. (۱۴۰۰). تحلیل و پیشگیری از جرایم سایبری سازمان‌یافته. تهران: نشر دانشگاه شهید بهشتی.

نادری، ص. (۱۳۹۷). روش‌های مقابله با فیشینگ و جرایم دیجیتال. تهران: نشر دانشگاه تهران.

یوسفی، ج. (۱۳۹۹). آموزش و آگاهی کاربران در مقابله با تهدیدات سایبری. تهران: نشر دانشگاه صنعتی شریف.

مقالات

احمدی، م. (۱۳۹۸). «همکاری‌های بین‌المللی در امنیت سایبری و تجربه کشورهای پیشرفته». مجله مطالعات بین‌المللی سایبری، ۳ (۳)، صص. ۴۰–۷۰.

پورجاهد، م. (۱۳۹۵). جرایم سایبری و چالش‌های حقوقی آن. تهران: نشر میزان. ص. ۴۲–۴۸.

جعفری، ح. (۱۳۹۹). «تحلیل حقوقی جرایم رایانه‌ای و فیشینگ در ایران». مجله پژوهش‌های حقوقی سایبری، ۵ (۲)، صص. ۱۵–۴۰.

حسینی، ن. (۱۴۰۰). «رویهٔ قضائی ایران در مقابله با جرایم سایبری». مجله مطالعات قضائی و امنیت فضای مجازی، ۷ (۱)، صص. ۲۰–۵۰.

حیدری، س. (۱۳۹۶). بررسی فیشینگ و پیامدهای حقوقی آن در نظام بانکی ایران. قم: انتشارات دانشگاه مفید. ص. ۷۸–۹۰.

رضایی، ف. (۱۳۹۸). «بررسی رویه قضائی جرایم رایانه‌ای در ایران». مجله حقوق و فناوری، ۴ (۳)، صص. ۳۰-۶۰.

رضوی‌فرد، ع.، و موسوی، م. (۱۳۹۵). حقوق کیفری سایبر: جرایم سازمان‌یافته و چالش‌های فراملی. مشهد: انتشارات دانشگاه فردوسی. ص. ۱۰۵–۱۱۵.

سعید پور ، س .(۱۴۰۰).مقایسه نظام های حقوقی ایران و کشورهای پیشرفته در مقابله با فیشینگ .مجله حقوق فناوری اطلاعات،۷(۱)،۵۰-۶۰.

شریفی، م. (۱۳۹۸). «فیشینگ و تکنیک‌های مقابله: رویکردی علمی». مجله حقوق سایبری، ۲ (۲)، صص. ۲۵–۵۵.

کاظمی، ر. (۱۳۹۹). «فناوری اطلاعات و حقوق: رویکردهای نوین مقابله با تهدیدات سایبری». مجله حقوق و فناوری، ۴ (۱)، صص. ۵۰-۸۰.

کریمی، م. (۱۳۹۹). «کاربرد هوش مصنوعی در مقابله با فیشینگ و جرایم سازمان‌یافته». مجله امنیت سایبری و فناوری اطلاعات، ۳ (۲)، صص. ۲۵–۵۵.

موسوی، ک. (۱۴۰۰). «تحلیل و پیشگیری از جرایم سایبری سازمان‌یافته: تجربه ایران». مجله مطالعات فناوری و حقوق، ۶ (۱)، صص. ۴۰–۷۵.

محمدی ،م.(۱۴۰۰)چالش های حقوقی و به روز رسانی قوانین جرایم سایبری در ایران .پژوهش های حقوقی ایران ،۷(۲)،۴۲-۵۰.

میری، س. (۱۳۹۸). آموزش و ظرفیت‌سازی کشورهای در حال توسعه برای مقابله با جرایم سایبری. مطالعات بین‌المللی امنیت سایبری، ۴(۳)، ۴۵–۵۵.

یوسفی، ج. (۱۳۹۹). «آموزش کاربران و کاهش تهدیدات سایبری: تجربه‌های موفق». مجله پژوهش‌های امنیت دیجیتال، ۵ (۱)، صص. ۳۰-۶۰.

۲.انگلیسی

Books

Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace. Santa Barbara, CA: Praeger, pp. 45–78.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Cambridge: Polity Press, pp. 60–95.

Smith, R. G., & Cornish, D. B. (2006). Organized cybercrime: Understanding the threat. London: Routledge, pp. 32–70.

Choi, K., & Park, J. (2014). Legal responses to phishing attacks in the digital age. New York, NY: Springer, pp. 50–85.

Jaishankar, K. (2011). Cyber criminology: Exploring internet crimes and criminal behavior. Boca Raton, FL: CRC Press, pp. 25–60.

Articles

Wall, D. S. (2007). “Policing cybercrime: Networked and social approaches.” Criminology & Criminal Justice, 7(4), 453–470.

Holt, T. J., & Bossler, A. M. (2014). “Cybercrime in progress: Theory and prevention of technology-enabled offenses.” Deviant Behavior, 35(5), 343–360.

Odebade, A. T., & Benkhelifa, E. (2023). A Comparative Study of National Cyber Security Strategies of ten nations. arXiv. [https://arxiv.org/abs/2303.13938](https://arxiv.org/abs/2303.13938(

:[۱]https://arxiv.org/abs/2303.13938?utm_source=chatgpt.com "A Comparative Study of National Cyber Security Strategies of ten nations"

Thomas, D. R., & Loader, B. D. (2000). “Cybercrime: Law enforcement, security, and surveillance in the information age.” Journal of Law and Society, 27(3), 376–401.

Grabosky, P. (2007). “Electronic crime and the law: Contemporary challenges.” Information & Communications Technology Law, 16(1), 1–20.

Wall, D. S., & Williams, M. L. (2007). “Policing the internet: Issues in cybercrime enforcement.” European Journal of Criminology, 4(4), 395–412.

Reports / International Documents

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Strasbourg: Council of Europe. Available at: [https://www.coe.int/en/web/cybercrime](https://www.coe.int/en/web/cybercrime(

United Nations Office on Drugs and Crime. (2013). Comprehensive study on cybercrime. New York: UNODC. Available at: https://www.unodc.org/unodc/en/cybercrime