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

تمدن حقوقی

دوره ۹ - شماره ۲۷ - بهـار ۱۴۰۵

Legal Civilization
Vol. 9, No. 27, Spring 2026
Pages: 305-320
Article Type: Promotional Article
https://www.pzhfars.ir/article_242433.html
doi: 10. 22034/lc. 2026. 578377. 1753

تمدن حقوقی
دوره ۹، شماره ۲۷، بهار ۱۴۰۵
صفحات: ۳۲۰-۳۰۵
نوع مقاله: ترویجی

ویژگی‌ها و خصوصیات جرائم سایبری در نظام کیفری ایران

Features and Characteristics of Cybercrimes in the Iranian Criminal System

سیده الهه بابونکی
کارشناس ارشد حقوق کیفری و جرم‌شناسی، دانشگاه تابناک، لامرد، ایران
babonaki54@gmail.com

Seyedeh Elaheh Babonaki
Master of Criminal Law and Criminology, Tabnak University, Lamerd, Iran

دریافت مقاله: ۱۴۰۵/۰۱/۱۹ - بازنگری مقاله: ۱۴۰۵/۰۲/۰۳ - پذیرش مقاله: ۱۴۰۵/۰۳/۱۳

Received: 2026/04/08 - Review: 2026/04/23 - Accepted: 2026/06/03

چکیده

گسترش فناوری‌های نوین و درهم‌تنیدگی کنش‌های انسانی در فضای دیجیتال، پیامدهای متنوعی را برای نظم اجتماعی به همراه داشته است. هرچند محیط دیجیتال ظرفیت‌های گسترده‌ای برای توسعه، ارتباطات و خدمات عمومی فراهم می‌کند، اما همین بستر می‌تواند مورد سوءاستفاده قرار گرفته و زمینه‌ساز شکل‌گیری گونه‌های جدیدی از بزهکاری شود. ازاین‌رو، تحلیل علمی این فضا و پیامدهای آن برای عدالت اجتماعی و امنیت جمعی ضرورتی انکارناپذیر است. در دهه‌های اخیر، سیاست‌گذاران، حقوقدانان و جرم‌شناسان با هدف‌شناسایی مصادیق مجرمانه در فضای سایبری، تعیین ضمانت‌اجراهای مناسب، طراحی سازوکارهای پیش‌گیرانه و ارتقای آگاهی عمومی وارد این حوزه شده‌اند. این نوع جرائم، به دلیل ویژگی‌های خاص فضای مجازی از جمله ناشناس بودن، عدم محدودیت جغرافیایی و سرعت رشد، علاوه بر تهدید امنیت فکری و مالی جامعه، نگرانی‌های جدی در حوزه سیاست‌گذاری ایجاد کرده‌اند. این پژوهش با روش توصیفی-تحلیلی با تمرکز بر ماهیت و ویژگی‌های محیط دیجیتال، به مفهوم‌شناسی و طبقه‌بندی جرائم سایبری پرداخته است.

واژگان کلیدی: جرائم سایبری، بزه‌دیده‌گی سایبری، علت‌شناسی جرم.

Abstract

The expansion of new technologies and the intertwining of human actions in the digital space have brought about diverse consequences for social order. Although the digital environment provides extensive capacities for development, communication, and public services, this same platform can be abused and pave the way for the formation of new types of crime. Therefore, scientific analysis of this space and its consequences for social justice and collective security is an undeniable necessity. In recent decades, policymakers, lawyers, and criminologists have entered this field with the aim of identifying criminal instances in cyberspace, determining appropriate enforcement guarantees, designing preventive mechanisms, and promoting public awareness. Due to the specific characteristics of cyberspace, such as anonymity, lack of geographical restrictions, and rapid growth, these types of crimes have created serious concerns in the field of policymaking, in addition to threatening the intellectual and financial security of society. This research, using a descriptive-analytical method, focuses on the nature and characteristics of the digital environment, and addresses the conceptualization and classification of cybercrimes.

Keywords: Cybercrimes, Cyber Victimization, Crime Etiology.

ارجاع:
بابونکی، سیده الهه؛ (۱۴۰۵)، ویژگی‌ها و خصوصیات جرائم سایبری در نظام کیفری ایران، تمدن حقوقی، شماره ۲۷.

مقدمه

انسان‌ها همیشه در مسیر تکامل گام برداشته‌اند؛ ابتدا ابزارها و اختراعات مختلف، تغییر شیوه زیست، ارتقای سطح رفاه خانوادگی و پایه‌گذاری آداب و سنت‌های اجتماعی؛ همه این‌ها نشانه‌ای از توسعه پایدار جامعه‌اند. با ورود به عصر اولیه آتش، محل سکونت از دل کوه‌ها و مخفیگاه‌های طبیعی به سمت فضاهای بازتر منتقل شد و روش‌های تغذیه انسان دچار تغییر شد. با کشف آهن و آغاز عصر فلزات، ابزارها از حالت سنتی خارج شدند و وسایل فلزی جای آن‌ها را گرفتند. در قرن‌های هفدهم و هجدهم میلادی، با شروع دوران صنعتی و فناوری، هدف اصلی تمرکز روی افزایش کارایی و سود اقتصادی بود و تغییرات گسترده‌ای پدید آمد. وسایل جدید برای گسترش ظرفیت تولید و رقابت‌های صنعتی اختراع شد و کلیه سیاست‌های دولتی به همین تحول‌ها وابسته گردید.

اما در اواخر قرن بیستم میلادی و ورود به عصر فراصنعتی، جهان با پدیده‌ای شگرف به‌رغم محدودیت‌های قبلی روبه‌رو شد: فضای مجازی یا جهان سایبری که با پیشرفته‌های علمی و فناوری نو به وجود آمد و دنیا را دگرگون کرد. به دنبال این پدیده، روابط انسانی نیز به‌طور گسترده‌ای به این فضا کشانده شد: تبلیغات، فعالیت‌های اقتصادی، تجارت، بانکداری، آموزش و اطلاع‌رسانی همگانی از جمله جنبه‌های فعال در این جهان تازه‌اند.

فضای سایبر با همه گستردگی و جهان شمول بودنش و نیز تأثیرات مثبتی که در زندگی انسان بر جای گذاشته است، از تیررس علم حقوق خارج نبوده و به محض ظهور این فضا و آغاز فعالیت‌های انسان در این دنیای جدید، علم حقوق و ابزارهای آن نیز وارد عمل شدند و به بررسی ابعاد این فضا از نگاه حقوقی پرداختند. به عبارت دیگر، بروز اتفاقاتی در دنیای مجازی از جمله ارتکاب جرائم سایبری، تبعات و آثار منفی و مخرب فرهنگی این محیط، دخالت علم حقوق را ضرورت بخشیده است که در این راستا مداقه در ماهیت فضای سایبر، شناخت علل و عوامل شکل‌گیری جرائم سایبری و شکل‌دهی تدابیر کنشی و واکنشی متناسب با خصوصیات این فضا از دلایل و ضروریات تدوین این پژوهش محسوب می‌گردد.

در این پژوهش تلاش می‌شود تا فضای سایبر و ویژگی‌های فضای سایبر تبیین و روشن گردد، به بیانی دیگر آشنایی با ماهیت ابزارهایی که واسطه ورود انسان به این فضا هستند و همچنین اطلاع از ویژگی‌های خاص فضای سایبر که باعث تبدیل شدن این فضا به بستری مناسب در جهت اقدامات مجرمانه گشته و نیز توجه به اهداف و ارزش‌های مدنظر برنامه‌ریزان و هدایت‌کنندگان این فضا تا حد زیادی منجر به طرح‌ریزی سیاست جنایی مناسبی در این زمینه خواهد شد.

با ورود رایانه به زندگی روزمره، این فناوری هم مزایای زیادی دارد و هم چالش‌هایی، به‌ویژه در حوزه امنیت و جرائم سایبری، بروز می‌کند. رایانه ابزار اصلی برای تسهیل امور و دسترسی آسان به اطلاعات است، ولی در صورت سوءاستفاده، می‌تواند مشکلات فراوانی ایجاد کند. به همین دلیل، تنظیم‌گری و مدیریت این پدیده از مسئولیت‌های بنیادی علم حقوق است تا از وقوع جرائم و ناامن شدن فضاهای اجتماعی جلوگیری کند. امروزه، اقصی نقاط جهان از اینترنت در زمینه‌های مختلف سیاسی، فرهنگی، اقتصادی و اجتماعی بهره می‌برند. فناوری‌های ارتباطی، در کنار مزایای بی‌شماری که برای بهبود فرایندها و زندگی فردی دارند، موجب ظهور خطرات و جرائم جدیدی شده‌اند که به‌عنوان جرائم سایبری شناخته می‌شوند. این جرائم، برخلاف تئوری، نیازمند راهکارهای عملی و قابل اجرا هستند تا بتوانند امنیت فضای مجازی و اعتماد عمومی را حفظ کنند.

۱- ویژگی‌های جرائم سایبری

۱-۱- نامحدود بودن فضای سایبر

فضای سایبر فاقد مرزهای جغرافیایی یا فیزیکی مشخص است. برخلاف دنیای واقعی که تعداد افراد و محدوده حضور آن‌ها قابل شمارش و کنترل است، این فضا هیچ مرز طبیعی ندارد. این ویژگی در نگاه اول یک مزیت بزرگ به شمار می‌رود؛ زیرا امکان دسترسی سریع، گسترده و آسان به اطلاعات و خدمات را فراهم می‌کند. اما همین بی‌مرزی، در صورت سوءاستفاده، به ابزاری قدرتمند برای مجرمان تبدیل می‌شود. مجرمان سایبری به‌راحتی می‌توانند هویت واقعی خود را پنهان کنند، هویت جعلی بسازند یا مدام تغییر دهند و از مسئولیت مستقیم فرار کنند (برنت ای. تروی، ۱۳۸۵، ۶۲۶).

۱-۲- ناملموس بودن فضای سایبر

فضای سایبر هیچ وجود فیزیکی و قابل لمسی ندارد. این ویژگی آن را از محیط واقعی متمایز و درعین‌حال خطرناک‌تر می‌سازد. نبود حضور فیزیکی و ملموس نیروی انتظامی یا پلیس در این فضا: عاملی که حس بازدارندگی را به‌شدت کاهش می‌دهد. مجرم احساس آزادی و امنیت بیشتری می‌کند و ارتکاب جرم در ذهن او آسان‌تر جلوه می‌کند. البته در سال‌های اخیر واحدهای تخصصی پلیس سایبری[1] در کشورهای مختلف شکل گرفته‌اند که به‌صورت نامریی و نرم در فضای مجازی گشت‌زنی می‌کنند و اقدامات پیشگیرانه یا مقابله‌ای انجام می‌دهند. عدم مواجهه مستقیم بزه‌دیده با مرتکب: در جرائمی مانند هک، کراکینگ یا نفوذ، هیچ مجاورت فیزیکی یا حتی دیداری بین طرفین وجود ندارد (فضلی، ۱۳۸۹، ۷۰). تأخیر در آشکار شدن آثار جرم: بسیاری از خسارات و آسیب‌ها با گذر زمان مشخص می‌شوند که این امر سرعت واکنش و پیشگیری مؤثر را کاهش می‌دهد.

۱- با نام‌هایی مانند پلیس فتا، پلیس سایبری، پلیس شبکه، پلیس وب و...

۱-۳- توسعه سریع و تغییرپذیری مداوم

ماهیت پویا و پیشرفت لحظه‌به‌لحظه فناوری‌های مرتبط با فضای سایبر باعث شده هر روز ابزارها، برنامه‌ها، سرویس‌ها و پلتفرم‌های جدیدی پدید آید. این سرعت تحول، لزوم برنامه‌ریزی دقیق و به‌روز برای استفاده سالم و امن از این ابزارها را ضروری می‌سازد. اما همین دسترسی سریع و آسان به محتوای بسیار گسترده، گاهی اوقات اقدامات کنترلی و مقابله‌ای را ناکارآمد می‌کند و فرصت سوءاستفاده از این فناوری‌های نوین را در مسیرهای انحرافی فراهم می‌آورد (میرترابی و همکاران، ۱۳۹۹). به علاوه، پیشرفت مداوم اجزا و زیرساخت‌های سایبری باعث می‌شود تدوین قوانین کلی و ثابت برای این فضا عملاً بی‌اثر باشد، زیرا به‌سادگی می‌توان بدون نقض صریح قانون، رفتارهای مجرمانه انجام داد. وضع قوانین جزیی و موردی برای هر نوع جرم جدید نیز به دلیل سرعت بالای ظهور مصادیق تازه، تقریباً غیرممکن است.

۱-۴- پیچیدگی و تخصصی بودن فضای سایبر

فضای سایبر به‌شدت تخصصی است؛ هرچند ورود به آن برای افراد عادی با یک رایانه یا گوشی هوشمند بسیار آسان شده، اما درک عمیق و مدیریت مؤثر آن نیازمند دانش و مهارت‌های تخصصی است. این پیچیدگی در زمینه‌های زیر خود را نشان می‌دهد: طراحی و برنامه‌نویسی سامانه‌های پیشرفته؛شناسایی و تحلیل اقدامات مخرب و حملات سایبری؛ ایجاد و حفظ امنیت در استفاده روزمره؛ تشخیص، ردیابی و مقابله با مجرمان سایبری حرفه‌ای؛ ارزیابی تأثیرات فرهنگی، اجتماعی و روانی گسترده فضای سایبر بر افراد و جامعه. بدون وجود تخصص متناسب با این سطح از پیچیدگی، امکان مدیریت ایمن و مقابله مؤثر با تهدیدات تقریباً وجود ندارد.

۱-۵- دسترسی آسان و سریع

یکی از بارزترین ویژگی‌های فضای سایبر، امکان ورود و استفاده بسیار ساده و سریع از آن است.

امروزه افراد با ابزارهای زیر به‌راحتی به تمامی امکانات این فضا دسترسی دارند: رایانه شخصی؛ کافی‌نت‌ها؛ تلفن همراه هوشمند متصل به اینترنت. این دسترسی بدون محدودیت جغرافیایی و با هزینه اندک، در کنار جذابیت بالای محتوای موجود در فضای مجازی، می‌تواند به‌ویژه در میان کودکان، نوجوانان و جوانان زمینه‌ساز انحرافات اخلاقی، اعتیاد به اینترنت و حتی شکل‌گیری جرائم سایبری شود. این ویژگی دسترسی آسان، در کنار جذابیت و آسیب‌پذیری بالای فضای سایبر، یکی از عوامل اصلی افزایش سریع جرائم و انحرافات در این محیط به شمار می‌رود.

۱-۶- گستردگی روزافزون وابستگی به فضای سایبر

یکی دیگر از ویژگی‌های برجسته فضای سایبر، وابستگی شدید و فزاینده زندگی روزمره انسان‌ها به این محیط است. در دنیای امروز، با پیشرفت سریع فناوری و خودکارسازی گسترده فعالیت‌های تولیدی، تجاری، مالی و اقتصادی استفاده از فضای مجازی برای ساده‌سازی و سرعت بخشیدن به فرایندها به‌طور چشمگیری افزایش یافته است. این وابستگی گسترده، جایگاه فضای سایبر را در جهان معاصر به‌شدت حساس، راهبردی و تعیین‌کننده کرده است؛ به‌گونه‌ای که هرگونه اختلال، نفوذ یا حمله در این فضا می‌تواند پیامدهای بسیار وسیع و حتی فاجعه‌بار در زندگی واقعی به دنبال داشته باشد. به همین دلیل، امنیت و پایداری فضای سایبر دیگر صرفاً یک موضوع فنی نیست، بلکه به یکی از مهم‌ترین مؤلفه‌های امنیت ملی، اقتصادی و اجتماعی کشورها تبدیل شده است (میرترابی و همکاران، ۱۳۹۱).

۲- انواع جرائم سایبری

۲-۱- کلاهبرداری رایانه‌ای

کمیته تخصصی جرائم رایانه‌ای شورای اروپا کلاهبرداری رایانه‌ای را این‌گونه تعریف کرده است: هرگونه وارد کردن، تغییر، حذف، مسدودسازی داده‌ها یا برنامه‌های رایانه‌ای یا هر نوع مداخله دیگر در فرایند پردازش داده‌ها که بر نتیجه پردازش تأثیر بگذارد و منجر به ضرر مالی یا هرگونه تصرف غیرقانونی در اموال دیگری شود، به قصد تحصیل منفعت اقتصادی نامشروع برای خود یا شخص ثالث

یا به قصد محروم کردن غیرقانونی صاحب مال از اموالش. کلاهبرداری رایانه‌ای یکی از مهم‌ترین مصادیق سوءاستفاده‌های اقتصادی در حوزه جرائم رایانه‌ای محسوب می‌شود. این جرم شامل انواع مختلفی از سوءاستفاده‌ها می‌گردد، از جمله سوءاستفاده از شبکه‌های تلفنی؛ سوءاستفاده از دستگاه‌های خودپرداز و صندوق‌های پرداخت الکترونیکی؛ سوءاستفاده از کارت‌های اعتباری و کارت‌های پلاستیکی پرداخت.

۲-۲- جعل رایانه‌ای

تعریف ارائه‌شده توسط کمیته تخصصی شورای اروپا از جعل رایانه‌ای به شرح زیر است: وارد کردن، تغییر، حذف یا مسدودسازی داده‌ها یا برنامه‌های رایانه‌ای یا هرگونه مداخله دیگر در پردازش داده‌ها، در شرایطی که طبق قوانین ملی، چنین عملی معادل جعل تلقی می‌شود، در صورتی که با همان اهدافی انجام گیرد که در جعل سنتی مدنظر قانون‌گذار بوده است. جعل رایانه‌ای در حقیقت جعل در حوزه داده‌ها است. همان‌گونه که در جعل اسناد سنتی، عمل مجرمانه بر روی سند اثر می‌گذارد، در این جا نیز عمل مجرمانه مستقیماً داده‌ها یا اطلاعات دیجیتالی را هدف قرار می‌دهد. جعل رایانه‌ای اصولاً با نیت مستقیم ایراد خسارت مالی یا تحصیل منفعت اقتصادی انجام نمی‌شود. هدف اصلی آن اغلب دستکاری ادله قضایی، تغییر اسناد رسمی، تقلب در مدارک، یا ایجاد تغییرات در اطلاعات به منظور فریب در فرایندهای حقوقی یا اداری است. در برخی کشورها مانند هلند، نروژ و سوئیس، سوءاستفاده از کارت‌های اعتباری نیز در دسته‌بندی جعل رایانه‌ای قرار می‌گیرد (باستانی، ۱۳۸۶، ۶۰).

۲-۳- ایجاد خسارت در داده‌ها و برنامه‌های رایانه‌ای

این شکل از رفتار مجرمانه شامل دسترسی غیرمجاز[۲] به سامانه‌ها و استفاده از ابزارهای مخرب مانند ویروس، کرم رایانه‌ای، بمب منطقی و دیگر بدافزارها است که با هدف وارد کردن خسارت انجام

۲- مستقیم یا غیرمستقیم

می‌گیرند. این خسارت می‌تواند به شکل‌های زیر باشد: حذف داده‌ها؛ آسیب‌رساندن به ساختار اطلاعات؛ مخدوش کردن محتوای فایل‌ها؛ متوقف کردن یا مختل کردن عملکرد برنامه‌ها. در این نوع جرم نیازی به وجود عنصر قصد متقلبانه نیست، هدف صرفاً تخریب یا اخلال است. تخریب داده‌ها گاهی از طریق حمله فیزیکی به تجهیزات رایانه‌ای صورت می‌گیرد و گاهی به روش‌های کاملاً دیجیتالی و فنی[۳] اجرا می‌شود. خطرناک‌ترین این ابزارها، ویروس‌هایی هستند که قابلیت تکثیر خودکار داشته و به‌طور گسترده فایل‌ها و برنامه‌های دیگر را آلوده و تخریب می‌کنند (باستانی، ۱۳۸۶، ۶۴).

۲-۴- اخاذی رایانه‌ای

هرگونه اصلاح، متوقف‌سازی یا حذف غیرمجاز داده‌ها یا عملیات رایانه‌ای که به‌طور آشکار عملکرد عادی یک سیستم را مختل کند، اخاذی رایانه‌ای نامیده می‌شود. اخاذی رایانه‌ای می‌تواند اهداف گوناگونی داشته باشد، از جمله: کسب مزیت رقابتی اقتصادی نسبت به رقبا؛ پیشبرد اهداف تروریستی یا ایدئولوژیک؛ سرقت داده‌ها یا برنامه‌ها به منظور اخاذی و تهدید. عنصر اصلی و محوری جرم اخاذی رایانه‌ای، قصد اخلال و جلوگیری از عملکرد صحیح سیستم رایانه‌ای یا سیستم ارتباطی است.

۲-۵- نفوذ غیرمجاز رایانه‌ای

این نوع رفتار مجرمانه شامل دسترسی غیرمجاز به رایانه‌ها و سامانه‌های رایانه‌ای است. این نوع نفوذ با هدف مستقیم بهره‌برداری مالی انجام نمی‌گیرد. از نظر سنی نیز بیشتر افراد مرتکب در این دسته، جوانان در بازه سنی پانزده سال تا بیست و چهار سال هستند. امروزه نه‌تنها رایانه‌ها، بلکه سیستم‌های مخابراتی پیشرفته نیز در معرض نفوذ از راه دور قرار دارند. نفوذگران با دسترسی به یک گره مخابراتی می‌توانند به کل شبکه ارتباطی یک شهر یا حتی یک کشور نفوذ کرده و از آن به شیوه‌های مختلف سوءاستفاده کنند.

۳- ویروس، کرم، بمب منطقی و مانند آن

۲-۶- استراق سمع غیرمجاز

در کنار روش‌های سنتی جاسوسی، امروزه نوع جدیدی از جاسوسی با عنوان جاسوسی داده‌های رایانه‌ای به‌وجود آمده است. یکی از مصادیق مهم این جرم نوظهور، استراق سمع اطلاعات در حین انتقال در شبکه‌های رایانه‌ای است. در بیشتر نظام‌های حقوقی کشورها، حمایت‌های موجود از مکالمات تلفنی شفاهی[۴] به ارتباطات الکترونیکی و شبکه‌های رایانه‌ای نیز گسترش یافته است. تعریف رایج استراق سمع غیرمجاز چنین است: «هرگونه شنود، ضبط، قطع یا اختلال در محتوای ارتباطات[۵] در یک سیستم یا شبکه رایانه‌ای، بدون داشتن مجوز قانونی و با استفاده از ابزارهای فنی».

۲-۷- سرقت و تکثیر غیرمجاز برنامه‌های رایانه‌ای حمایت‌شده

تولید یک نرم‌افزار رایانه‌ای معمولاً زمان، هزینه و سرمایه فکری قابل توجهی می‌طلبد. به همین دلیل، تکثیر غیرمجاز، توزیع یا استفاده بدون اجازه از آن، خسارت اقتصادی سنگینی به صاحب حق قانونی وارد می‌کند. این رفتار مجرمانه در دسته جرائم علیه اموال و مالکیت قرار می‌گیرد و شباهت زیادی به سرقت، کپی غیرمجاز و تصاحب غیرقانونی اموال در حقوق سنتی دارد. در ادبیات رایج به آن «سرقت نرم‌افزار»، «دزدی نرم‌افزار» یا «ربایش برنامه» گفته می‌شود. در سال‌های اخیر، حجم و سرعت رشد این نوع تخلف به‌شدت افزایش یافته و حجم قابل توجهی از جرائم رایانه‌ای را به خود اختصاص داده است. سازوکارهای حقوقی و اداری موجود در بسیاری از کشورها هنوز نتوانسته‌اند به‌طور مؤثر و قاطع با این پدیده مقابله کنند. تعریف پیشنهادی بر اساس توصیه‌های شورای اروپا: «تکثیر، توزیع، عرضه عمومی یا هرگونه انتشار غیرمجاز یک برنامه رایانه‌ای که طبق قانون از حقوق مالکیت معنوی برخوردار است».

۴- ممنوعیت استراق سمع

۵- ورودی یا خروجی

۲-۸- پورنوگرافی غیرمجاز رایانه‌ای

از نظر لغوی، پورنوگرافی به هرگونه نوشته، تصویر، فیلم یا محتوای جنسی اطلاق می‌شود که فاقد ارزش ادبی، هنری، علمی یا سیاسی باشد. با گسترش فناوری رایانه و اینترنت، این جرم کلاسیک وارد بستر دیجیتال شده و به دلیل ویژگی‌های منحصربه‌فرد شبکه‌های جهانی[۶] ابعاد بی‌سابقه‌ای یافته است. امروزه سایت‌ها، پست‌های الکترونیکی، گروه‌های تلگرامی، کانال‌ها و حتی صندوق‌های پستی دیجیتال به‌طور گسترده برای تبلیغ، توزیع و فروش محتوای پورنوگرافیک استفاده می‌شوند. نوع دیگری از این جرم، آزار جنسی سایبری در محیط کار است؛ به این صورت که مجرم با کنترل رایانه متصل به اینترنت قربانی، او را مجبور به مشاهده محتوای پورنوگرافیک می‌کند یا با ارسال گسترده چنین محتوایی او را تحت فشار روانی قرار می‌دهد. بزه‌دیدگان اصلی این جرم اغلب کودکان و نوجوانان[۷] و زنان هستند؛ گروه سنی قربانیان گاهی از حدود هفت سالگی آغاز می‌شود.

۲-۹- جرائم چندرسانه‌ای

از نظر لغوی و فنی، چندرسانه‌ای[۸] به معنای ترکیب هم‌زمان عناصر مختلف رسانه‌ای شامل متن، صدا، تصویر ثابت، انیمیشن و ویدئو است. این نوع جرائم عمدتاً به نسل سوم جرائم رایانه‌ای[۹] تعلق دارند و تقریباً همیشه در محیط مجازی و شبکه‌های بین‌المللی قابل ارتکاب هستند. رفتارهای مجرمانه رایج در این حوزه شامل موارد زیر می‌شود: جرائم علیه تمامیت و آزادی جنسی[۱۰]؛ اقدامات علیه نظم عمومی[۱۱]؛ جعل، تحریف و دستکاری اخبار، متون، تصاویر و اطلاعات در شبکه‌های اینترنتی و پایگاه‌های داده.

۶- گستردگی، سرعت، ناشناس بودن و دسترسی آسان

۷- دختر و پسر

8- Multimedia

۹- جرائم در فضای سایبر

۱۰- پورنوگرافی کودکان، محتوای جنسی غیرقانونی

۱۱- فعالیت‌های سیاسی غیرمجاز، تبلیغات تروریستی

ویژگی‌های متمایز جرائم چندرسانه‌ای نسبت به سایر جرائم سایبری: برخلاف بسیاری از جرائم رایانه‌ای کلاسیک، معمولاً خسارت اقتصادی مستقیم و قابل محاسبه سنگینی به بار نمی‌آورند؛ مرکز ثقل این جرائم، آسیب به ارزش‌ها، اخلاق عمومی، نظم اجتماعی و تمامیت روانی افراد است نه صرفاً منافع مالی؛ بزه‌دیدگان اغلب نامحدود، ناشناس و پراکنده هستند؛ این جرائم به‌طور بارز فراملی و فراسرزمینی هستند؛ به‌گونه‌ای که محل ارتکاب جرم تقریباً هیچ تأثیری بر ماهیت مجرمانه آن ندارد و امکان ردیابی و تعقیب را به‌شدت دشوار می‌سازد.

۳- انواع جرائم سایبری در محیط مجازی

جرائم قابل ارتکاب در فضای سایبر شامل دو گروه اصلی هستند: جرائم سنتی که به شکل کاملاً نوین و در بستر دیجیتال اجرا می‌شوند و جرائم کاملاً جدید و بی‌سابقه که تنها در محیط مجازی امکان تحقق دارند. این تنوع و ماهیت خاص جرائم سایبری، مفاهیم و ساختارهای سنتی حقوق کیفری را به چالش کشیده و نیازمند تحولات اساسی در ادبیات حقوقی شده است. در یک تقسیم‌بندی کلی می‌توان جرائم سایبری را به دسته‌های زیر تقسیم کرد (باستانی، ۱۳۸۶، ۶۸).

جرائم سنتی در بستر دیجیتال شامل: جاسوسی سایبری، اخای رایانه‌ای، جعل دیجیتال، کلاهبرداری سایبری، تخریب داده‌ها، افترا و نشر اکاذیب در فضای مجازی، پولشویی دیجیتال و قاچاق سایبری. جرائم علیه حقوق مالکیت معنوی و نرم‌افزار شامل: نقض کپی‌رایت، تکثیر غیرمجاز برنامه‌ها، سرقت نرم‌افزار. جرائم علیه امنیت و محرمانگی داده‌ها. جرائم مرتبط با تجارت الکترونیک به‌ویژه سوءاستفاده در پرداخت‌های الکترونیکی. جرائم در حوزه بانکداری الکترونیک. جرائم مخابراتی و ماهواره‌ای. جرائم علیه محتوا به‌ویژه پورنوگرافی کودکان، پورنوگرافی غیرقانونی و محتوای جنسی مجرمانه. سایبرتروریسم شامل جرائم علیه امنیت ملی و بین‌المللی از طریق فضای سایبر.

۳-۱- کلاهبرداری با کارت اعتباری در فضای سایبر

بر اساس مطالعات انجام شده، یکی از شایع‌ترین جرائم گزارش‌شده در فضای سایبر طی سال‌های اخیر، کلاهبرداری و سوءاستفاده از کارت‌های اعتباری بوده است. دلایل جذابیت بالای این جرم عبارتند از: وسوسه مالی بالا؛ دسترسی بسیار آسان؛ عدم نیاز به مهارت فنی پیچیده. هکرها یا کلاهبرداران اغلب تنها با یک رایانه، مودم و اتصال ساده به اینترنت می‌توانند در مدت کوتاهی از اطلاعات کارت‌های اعتباری سوءاستفاده کنند.

۳-۲- افتراء و نشر اطلاعات از طریق پست الکترونیک

ایمیل یکی از پرکاربردترین و گسترده‌ترین سرویس‌های اینترنت است که امکان ارسال انواع محتوا[۱۲] را فراهم می‌کند. هر کاربر با یک آدرس ایمیل مشخص در شبکه جهانی شناخته می‌شود. دسترسی به رمز عبور یک ایمیل می‌تواند امکان سوءاستفاده، جعل هویت و ارسال محتوای مجرمانه را فراهم کند. نشر افترا، اکاذیب، توهین، تهدید یا انتشار اطلاعات کذب علیه اشخاص از طریق ایمیل بسیار رایج است. کنترل و ردیابی این پیام‌ها به دلیل حجم بسیار بالای ایمیل‌های ارسالی روزانه، عملاً بسیار دشوار و تنها در موارد محدود امکان‌پذیر است (دزیانی، ۱۳۸۰: ۴۰).

۳-۳- تطهیر پول نامشروع رایانه‌ای در سایبر

پولشویی یکی از جرائم کلاسیک با سابقه طولانی است که با پیدایش اینترنت و شبکه‌های ارتباطی جهانی، شکل‌های جدیدی به خود گرفته است. باندهای سازمان‌یافته از طریق ایمیل یا سایت‌ها، بدون هیچ رد و نشانه‌ای، از افراد درخواست می‌کنند مبالغی را به حساب شخص ثالثی واریز کنند. در ازای آن، درصدی به‌عنوان کارمزد پرداخت می‌شود و روش استرداد پول با ظاهری مشروع[۱۳] هماهنگ می‌گردد.

۱۲- متن، صدا، تصویر و ویدئو

۱۳- معمولاً در قالب تجارت الکترونیک

۳-۴- سایبر تروریسم

در حال حاضر، بخشی از اقدامات تروریستی از طریق دسترسی غیرمجاز به اطلاعات حساس و سامانه‌های حیاتی انجام می‌شود.

تروریست‌های سایبری تنها با استفاده از کیبورد و ماوس می‌توانند: به سامانه‌های امنیتی نفوذ کنند؛ سیستم‌های ناوبری هوایی را مختل سازند؛ شبکه برق سراسری را از کار بیندازند؛ سامانه‌های کنترل منابع غذایی یا آب را دستکاری کنند.

۳-۵- قاچاق مواد مخدر از طریق سایبر

یکی از جرائم بسیار جدی و رو به رشد که هم در سطح ملی و هم در سطح بین‌المللی توجه زیادی را به خود جلب کرده، قاچاق و معامله مواد مخدر از طریق فضای مجازی است. با گسترش شبکه‌های ارتباطی، دسترسی آسان به اینترنت و ابزارهای پیام‌رسان، امروزه تقریباً تمام مراحل مرتبط با قاچاق مواد مخدر در بستر دیجیتال انجام می‌شود؛ از جمله: یافتن و ارتباط با تأمین‌کنندگان؛ مذاکره و توافق بر سر قیمت و مقدار؛ معرفی واسطه‌ها و توزیع‌کنندگان؛ جذب خریداران و مصرف‌کنندگان؛ هماهنگی برای تحویل کالا؛ دریافت و پرداخت وجوه. به دلیل ماهیت ناشناس، فراملی و رمزنگاری‌شده بسیاری از ارتباطات اینترنتی، کشف هویت فروشندگان و خریداران توسط پلیس و نهادهای انتظامی بسیار دشوار و در موارد زیادی عملاً غیرممکن است.

۳-۶- سوءاستفاده از کودکان در سایبر سپیس

یکی از سنگین‌ترین و نگران‌کننده‌ترین جرائم سایبری، سوءاستفاده جنسی از کودکان و تولید و انتشار محتوای پورنوگرافی کودکان در محیط مجازی است. کارشناسان پیش‌بینی کرده‌اند که در سال‌های آینده ده‌ها میلیون کودک به‌صورت فعال و روزانه از اینترنت استفاده خواهند کرد. این وضعیت، فرصت بسیار مناسبی برای بزهکاران سایبری ایجاد می‌کند تا از سادگی، اعتماد و عدم تجربه کودکان

سوءاستفاده نمایند. بزهکاران ابتدا اعتماد کودک را جلب می‌کنند، سپس او را به ارسال تصاویر یا انجام رفتارهای جنسی ترغیب کرده و نهایتاً این محتواها را ضبط و در سایت‌های مستهجن منتشر می‌سازند.

نتیجه

فضای مجازی به‌عنوان پدیده‌ای تحول‌آفرین، در بازه زمانی کوتاهی توانست جایگاهی اساسی در سبک زندگی بشری پیدا کند و الگوهای سنتی تعاملات اجتماعی، اقتصادی و فرهنگی را دگرگون سازد. بااین‌حال، همچون سایر دستاوردهای فناورانه، این فضا علاوه بر فرصت‌های بی‌شمار، زمینه‌ساز بروز چالش‌ها و پیامدهای ناخواسته نیز بوده است. فناوری اطلاعات و ارتباطات امکان ارتکاب انواع جدیدی از جرائم با پیچیدگی و گستردگی بی‌سابقه را فراهم آورده و امروزه در اختیار افرادی قرار گرفته که از آن به‌عنوان ابزاری برای نقض هنجارهای اجتماعی و قانونی سوءاستفاده می‌کنند.

در شرایط کنونی، دو واقعیت اجتناب‌ناپذیر وجود دارد: نخست آن‌که حذف کامل فناوری‌های دیجیتال از چرخه زندگی روزمره بشر دیگر غیرممکن است؛ و دوم آن‌که پاک‌سازی مطلق این فضا از حضور عناصر مجرم نیز از عهده هیچ نظامی خارج است. ازاین‌رو، تنها راه‌حل معقول و عملی، کاهش تدریجی مخاطرات و مدیریت هوشمند چالش‌های پیش‌روی جوامع در برابر جرائم سایبری محسوب می‌شود. اولین گام در این مسیر،شناسایی دقیق ریشه‌ها و عوامل تسهیل‌کننده بروز جرائم دیجیتال است تا با درک مکانیزم‌های عملکردی این فضا، مسیرهای ارتکاب جرم به‌صورت هدفمند مسدود گردد. در این زمینه، تأکید بر اقدامات پیشگیرانه غیرکیفری و گسترش رویکردهای ترمیمی در نظام عدالت به جای تکیه صرف بر مجازات‌های سنتی و کیفری که اغلب اثربخشی محدودی دارند از اهمیت ویژه‌ای برخوردار است.

اگرچه تدابیر پیشگیرانه غیرکیفری شامل اقدامات اجتماعی و وضعی دارای محدودیت‌هایی هستند، اما انکار نقش آن‌ها در کاهش جرائم سایبری غیرمنطقی است. کلید موفقیت در این حوزه، طراحی تدابیر هوشمندانه و هدفمند است تا با رفع تدریجی موانع موجود، بازدهی این اقدامات به

حداکثر برسد. تمرکز بر پیشگیری غیرکیفری هم در بعد اجتماعی[۱۴] و هم در بعد وضعی[۱۵] می‌تواند زمینه‌ساز کاهش ریشه‌ای جرائم سایبری باشد. سیاست‌های پیشنهادی برای مبارزه مؤثر با جرائم سایبری، پیشگیری از جرائم سایبری در ابعاد شغلی[۱۶]، اداری و اجتماعی، وابسته به کارایی و ایمنی زیرساخت‌های فناوری اطلاعات است. در این راستا، پیشگیری از طریق حقوق اداری و مدنی باید بر پیگیری‌های صرفاً کیفری اولویت یابد. در کنار تدوین استراتژی جامع امنیتی، راه‌حل‌های قانونی باید با ابزارهای فراقضایی مانند تدابیر امنیتی اختیاری توسط کاربران همراه شود. همچنین، اجرای مؤثر تدابیر امنیتی مستلزم همگامی با تحولات فناوری است.

در مجموع، سیاست‌های جنایی کارآمد برای مقابله با جرائم سایبری باید مبتنی‌بر سه اصل زیر باشد: افزایش آگاهی سازمان‌ها و بنگاه‌های اقتصادی درباره آسیب‌پذیری‌های سیستم‌های رایانه‌ای و ترغیب آن‌ها به به‌کارگیری راهکارهای امنیتی پیشرفته. تقویت استانداردهای امنیتی، کاهش موقعیت‌های مستعد جرم، محدود کردن دسترسی به ابزارهای فنی قابل سوءاستفاده، و ایجاد انگیزه برای گزارش‌دهی بزه‌دیدگان. بازنگری در قوانین داخلی و هماهنگی با مقررات بین‌المللی، همراه با توسعه همکاری‌های فرامرزی در زمینه‌شناسایی، تعقیب و محاکمه مرتکبان جرائم سایبری.

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

تعارض منافع: تعارض منافع در این مقاله وجود ندارد.

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

۱۴- ارتقای فرهنگ امنیتی

۱۵- تقویت زیرساخت‌های فنی

۱۶- تجاری

منابع

ـ باستانی، برومند، ۱۳۸۶، **جرایم کامپیوتری و اینترنتی**، چاپ دوم، تهران، انتشارات بهنامی.

ـ تروی، برنت، ای.، ۱۳۸۵، **ترسیم شخصیت جنایی مجرم**، ترجمه اکبر استرکی، چاپ اول، تهران، انتشارات مرکز تحقیقات کاربردی ناجا.

ـ فضلی، مهدی، ۱۳۸۹، **مسئولیت کیفری در فضای سایبر**، چاپ اول، تهران، انتشارات خرسندی.

ـ میرترابی، هدیه سادات؛ شیرزاد، هادی؛ آقاکاشی، وهاب، ۱۳۹۹، نقش پلیس در پیشگیری از جرائم سایبری با تأکید بر قوانین موضوعه، **فصلنامه مطالعات بین‌المللی پلیس**، شماره ۴۴.

Legal Civilization

ISSN: 2873-1841
ISSN: 2873-1922

No.27- Spring 2026