فصلنامه علمی مطالعات حقوق و علوم قضایی
سال دوم، شماره ۴، تابستان ۱۴۰۴، ص ۴۶۸-۴۳۸

Journal of Law and Judicial Studies
http://www.Ljournal.ir

واکاوی هویت‌یابی نوجوانان در فضای سایبری از یادگیری آنلاین تا ارتکاب جرایم سایبری

مرجان باستان فارسانی [۱]

تاریخ دریافت: ۱۴۰۴/۰۲/۰۱ تاریخ چاپ: ۱۴۰۴/۰۵/۲۸

چکیده

با گسترش فضای مجازی، بزهکاری سایبری به‌ویژه در میان نوجوانان به یکی از نگرانی‌های مهم در حوزه پیشگیری از جرم تبدیل شده است. پژوهش حاضر به بررسی نقش میزان دانش نوجوانان نسبت به قوانین مرتبط با جرایم رایانه‌ای و نیز تجربه‌های آنان در فضای آنلاین بر تمایل آن‌ها به انجام دسترسی‌های غیرمجاز می‌پردازد. یافته‌ها حاکی از آن است که تجربه‌های منفی در فضای مجازی، نظیر قربانی شدن در حملات سایبری، می‌تواند زمینه‌ساز بروز رفتارهای متقابل مجرمانه از سوی نوجوانان باشد. در حالی که تصور می‌شود آگاهی از قوانین می‌تواند مانعی در برابر ارتکاب جرم باشد، یافته‌ها حاکی از آن است که صرف آشنایی با قوانین لزوماً به کاهش رفتارهای غیرقانونی منجر نمی‌شود و در برخی موارد ممکن است حتی با افزایش گرایش به ارتکاب دسترسی غیرمجاز همراه باشد. این امر بیانگر آن است که درک عملی از پیامدهای مجرمانه و تقویت حس مسئولیت‌پذیری در فضای سایبری، نقشی کلیدی در پیشگیری از بزهکاری سایبری در میان نوجوانان ایفا می‌کند. رویکرد این پژوهش توصیفی-تحلیلی می‌باشد و گردآوری مطالب با استفاده از کتب و منابع الکترونیکی معتبر صورت گرفته است.

واژگان کلیدی

بزهکاری سایبری؛ نوجوانان؛ دسترسی غیرمجاز؛ قانون جرایم رایانه‌ای؛ پیشگیری از جرم.

[۱] کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آزاد شهرکرد، شهرکرد، ایران. (marjan.bastan.1401@gmail.com)

۱-مقدمه:

در عصر حاضر، گسترش فناوری‌های نوین ارتباطی، به‌ویژه اینترنت و شبکه‌های اجتماعی، فرصت‌ها و تهدیدهای بی‌سابقه‌ای را برای نوجوانان به همراه داشته است. یکی از چالش‌های مهم در این زمینه، افزایش روزافزون بزهکاری سایبری در میان نوجوانان است؛ پدیده‌ای که نه‌تنها نظم حقوقی و امنیت روانی کاربران فضای مجازی را تهدید می‌کند، بلکه بازتابی از تحولات فرهنگی، اجتماعی و روان‌شناختی در نسل جدید به شمار می‌رود. بزهکاری سایبری در نوجوانان اغلب به‌صورت فعالیت‌هایی چون هک، نفوذ به حساب‌های دیگران، انتشار اطلاعات محرمانه، تهدید، آزار اینترنتی و کلاهبرداری‌های آنلاین بروز می‌یابد و با توجه به وضعیت ویژه‌ی سنی و رشد شخصیتی نوجوانان، برخورد صرف کیفری با این پدیده، راهکاری ناکارآمد و حتی آسیب‌زا تلقی می‌شود. در این راستا، با گسترش سریع فناوری‌های دیجیتال و افزایش وابستگی جوامع به بسترهای آنلاین، بزهکاری سایبری به یکی از مهم‌ترین چالش‌های امنیتی و اجتماعی در عصر حاضر تبدیل شده است. این نوع از بزهکاری که به‌صورت خاص شامل دسترسی غیرمجاز به سیستم‌ها، شبکه‌ها و داده‌ها، یا آسیب‌رسانی به آن‌ها می‌شود، در نظام حقوقی بریتانیا تحت «قانون سوءاستفاده رایانه‌ای»[1] تعریف شده است .(Office for National Statistics, 2023) نمونه‌هایی از این رفتارها شامل نفوذ به حساب‌های بانکی یا شبکه‌های اجتماعی، حملات انکار سرویس[2] و انتشار ویروس‌ها یا بدافزارها می‌باشد Caneppele & Aebi, 2019). در حالی که نرخ وقوع جرایم سنتی در حال کاهش است، آمارها از روند افزایشی جرایم سایبری، به‌ویژه در میان نوجوانان، حکایت دارند(.(Maras et al, 2024 نگرانی عمده آن است که برخی از نوجوانان، آگاهانه یا ناآگاهانه، در مراحل ابتدایی ورود به مسیر بزهکاری سایبری قرار دارند و در صورت عدم مداخله، ممکن است به مجرمان حرفه‌ای در این حوزه تبدیل شوند .(National Crime Agency, 2017)

بررسی‌های اخیر در انگلستان و هلند نشان می‌دهد که درصد قابل توجهی از نوجوانان سابقه دسترسی غیرمجاز یا استفاده از بدافزار را داشته‌اند .(Weulen Kranenbarg et al, 2022) انگیزه‌های گوناگونی برای ارتکاب بزهکاری سایبری در نوجوانان مطرح شده است، از جمله کنجکاوی، هیجان، احساس چالش، تمایل به یادگیری، نمایش توانمندی فنی، انتقام‌جویی، و در مواردی، منافع مالی .(Steinmetz, 2015; Chng et al, 2022) همچنین، تجربه قربانی شدن در فضای سایبری می‌تواند خود به‌عنوان عاملی در بروز رفتارهای متقابل مجرمانه عمل کند. (Kerstens & Jansen, 2016; Parti et al. 2022) این موضوع از نظریه «همپوشانی قربانی-بزهکار» حمایت می‌کند که معتقد است حضور در فضاهای مشترک آنلاین، احتمال نقش‌آفرینی همزمان در هر دو موقعیت را افزایش می‌دهد .(Weulen Kranenbarg et al. 2019) عامل مهم دیگری که در سال‌های اخیر مورد توجه پژوهشگران و سیاست‌گذاران قرار گرفته، میزان آگاهی نوجوانان از قوانین سایبری و ادراک آنان از خطرات قانونی رفتارهای خود است. برخی پژوهش‌ها نشان داده‌اند که نوجوانان و حتی بزرگسالان در بسیاری موارد از غیرقانونی بودن اعمال خود اطلاع ندارند یا خطر دستگیری و مجازات را بسیار اندک می‌دانند. (Holt et al, 2017) در مقابل، برخی مطالعات ارتباطی میان آگاهی حقوقی و کاهش رفتار مجرمانه نیافته‌اند. (Berenblum et al, 2019) بر همین اساس، برنامه

[1] Computer Misuse Act 1990
[2] DDoS

«انتخاب‌های سایبری» [3] که از سوی آژانس جرایم ملی بریتانیا از سال ۲۰۱۳ راه‌اندازی شده است، با هدف پیشگیری از ورود نوجوانان به مسیر بزهکاری سایبری طراحی شده و بر آموزش، آگاهی‌رسانی و مداخلات فردی تمرکز دارد(National Crime Agency, 2017). اهمیت این پژوهش از چند بُعد قابل تأمل است: نخست آن‌که برخلاف مطالعات سنتی جرم‌شناسی که تمرکز خود را بر جرایم فیزیکی قرار می‌دهند، این تحقیق بر تحلیل میان‌رشته‌ای بزهکاری در محیط سایبری تمرکز دارد که ماهیت، انگیزه‌ها و پیامدهای متفاوتی دارد. دوم آن‌که این پژوهش با تمرکز بر چرخه‌ی بزه‌دیده‌ـبزهکار در فضای مجازی، تلاش می‌کند تا ریشه‌های روان‌شناختی و اجتماعی رفتار مجرمانه نوجوانان را کشف کرده و بر نقش تجربه‌های قربانی‌شدن در بروز بزهکاری تأکید نماید. سوم آن‌که، با استفاده از داده‌های روزآمد و تحلیل تطبیقی، این پژوهش به دنبال ارائه راهکارهایی برای پیشگیری هوشمند، مداخلات حمایتی و سیاست‌گذاری تربیتی در حوزه عدالت نوجوانان است که با دیدگاه تنبیهی صرف تفاوت ماهوی دارد. نوآوری پژوهش نیز در ترکیب مبانی جرم‌شناسی سنتی با رویکردهای نوین سایبر جرم‌شناسی، روان‌شناسی رشد و تحلیل رفتار دیجیتال نوجوانان نهفته است که بستر مناسبی برای اصلاح سیاست‌های کیفری، آموزشی و فرهنگی در مواجهه با این پدیده نوظهور فراهم می‌سازد.

۲-مبانی نظری

پیش از بررسی موضوع اصلی پژوهش، بایستی مبانی نظری شامل تعریف، انواع و اهمیت جرایم سایبری بررسی گردد.

۲-۱-تعریف جرایم سایبری

جرایم سایبری [4] یا جرایم اینترنتی، به اعمال مجرمانه‌ای گفته می‌شود که از طریق شبکه‌های کامپیوتری و فضای مجازی انجام می‌گیرند. با پیشرفت فناوری اطلاعات و گسترش دسترسی به اینترنت، جرایم سایبری به یکی از بزرگ‌ترین چالش‌های امنیتی در سطح جهانی تبدیل شده است. این نوع جرایم نه تنها به صورت مستقیم به دارایی‌های مادی و معنوی افراد و سازمان‌ها آسیب می‌رساند، بلکه می‌تواند تهدیدی جدی برای امنیت ملی، حریم خصوصی و سلامت روانی جامعه باشد .(Wall, 2007) جرایم سایبری عبارت‌اند از هرگونه فعالیت غیرقانونی که به وسیله کامپیوتر، اینترنت یا سایر فناوری‌های دیجیتال انجام شود و موجب خسارت یا نقض حقوق افراد، سازمان‌ها یا دولت‌ها گردد. این جرایم می‌توانند شامل سرقت داده‌ها، هک، کلاهبرداری، نشر اطلاعات نادرست، نفوذ به سیستم‌های امنیتی، حملات سایبری و موارد مشابه باشند.(Brenner, 2010) فنّاوری‌های نوین فرصت‌های تازه‌ای برای ارتکاب جرم فراهم می‌کنند، اما به ندرت باعث ظهور انواع کاملاً جدیدی از جرم می‌شوند. در این راستا، این پرسش مطرح می‌شود که چه چیزی «جرم سایبری» را از جرایم سنتی متمایز می‌کند؟ واضح‌ترین تفاوت، استفاده از رایانه‌های دیجیتال است، اما این نکته به‌تنهایی برای ایجاد تمایز کافی نیست، چرا که مجرمان برای ارتکاب جرم‌هایی مانند کلاهبرداری، قاچاق تصاویر مستهجن کودکان، نقض مالکیت فکری، سرقت هویت یا تجاوز به حریم خصوصی، نیازی به رایانه ندارند؛ تمام این رفتارهای مجرمانه پیش از ظهور پیشوند «سایبر» نیز وجود داشتند. جرم سایبری، به‌ویژه آن‌هایی که از طریق اینترنت انجام می‌شوند، در حقیقت توسعه‌ای از همان رفتارهای مجرمانه پیشین است که حالا در محیطی جدید و با ابزارهای دیجیتال رخ می‌دهند. البته برخی فعالیت‌های غیرقانونی کاملاً جدید نیز در بستر فضای مجازی پدید آمده‌اند. بیشتر

[3] Cyber Choices
[4] Cybercrime

جرایم سایبری، حملاتی علیه اطلاعات افراد، شرکت‌ها یا دولت‌ها هستند. این حملات ممکن است به بدن فیزیکی آسیبی نرسانند، اما به «بدن مجازی» افراد یا سازمان‌ها ضربه می‌زنند؛ یعنی به مجموعه‌ای از اطلاعاتی که هویت دیجیتال ما را در فضای اینترنتی شکل می‌دهد. به‌عبارتی، در عصر دیجیتال، هویت مجازی ما، شامل مجموعه‌ای از شماره‌ها و شناسه‌ها در پایگاه‌های داده‌ی مختلف، به بخش حیاتی زندگی روزمره‌مان تبدیل شده است. جرم سایبری، به‌شدت بر اهمیت و آسیب‌پذیری این هویت مجازی تأکید دارد. یکی از ویژگی‌های مهم جرایم سایبری، ماهیت فرامکانی (غیربومی) آن‌هاست. یعنی اقدامات مجرمانه می‌توانند در حوزه‌های قضایی بسیار دور از یکدیگر رخ دهند. این ویژگی چالش‌های بزرگی برای نهادهای قضایی و انتظامی به‌وجود آورده است، چرا که جرایمی که در گذشته محلی یا حتی ملی بودند، اکنون نیازمند همکاری‌های بین‌المللی هستند. مثلاً اگر فردی به محتوای مستهجن کودکان دسترسی پیدا کند که روی رایانه‌ای در کشوری ذخیره شده که چنین محتوایی را ممنوع نمی‌داند، آیا آن فرد مرتکب جرم در کشوری دیگر که این محتوا را غیرقانونی می‌داند، محسوب می‌شود؟ اساساً جرم سایبری در کجا اتفاق می‌افتد؟ فضای سایبری[5] را می‌توان نسخه‌ی پیشرفته‌تر فضایی دانست که در آن یک گفت‌وگوی تلفنی اتفاق می‌افتد. اینترنت به‌عنوان یک شبکه جهانی، پناهگاه‌های متعددی در دنیای واقعی و نیز در خود شبکه برای مجرمان فراهم می‌کند، اما درست همان‌طور که کسی که روی زمین قدم می‌زند، ردپا به‌جا می‌گذارد، مجرمان سایبری هم علی‌رغم تلاش برای پنهان‌کاری، سرنخ‌هایی از هویت و مکان خود برجای می‌گذارند. البته برای پیگیری این ردپاها در سطح بین‌المللی، نیاز به معاهدات حقوقی جهانی است. در سال ۱۹۹۶، شورای اروپا با همکاری نمایندگانی از ایالات متحده، کانادا و ژاپن، پیش‌نویس یک معاهده‌ی بین‌المللی در زمینه جرایم رایانه‌ای را تهیه کرد، اما گروه‌های مدافع آزادی‌های مدنی به برخی مفاد آن، به‌ویژه الزام شرکت‌های خدمات‌دهنده اینترنتی به ذخیره‌سازی اطلاعات کاربران و تحویل آن به مقامات در صورت درخواست، اعتراض کردند. با این حال، فرایند تدوین معاهده ادامه یافت و در ۲۳ نوامبر ۲۰۰۱، «کنوانسیون شورای اروپا درباره جرایم سایبری» توسط ۳۰ کشور امضا شد. این کنوانسیون در سال ۲۰۰۴ به اجرا درآمد. پروتکل‌های تکمیلی برای پوشش فعالیت‌های تروریستی و جرایم سایبری نژادپرستانه و بیگانه‌ستیز نیز در سال ۲۰۰۲ پیشنهاد شد و در سال ۲۰۰۶ لازم‌الاجرا گردید. علاوه بر این، قوانین ملی کشورها مانند قانون "USA PATRIOT Act"ایالات متحده در سال ۲۰۰۱، به مأموران انتظامی اختیارات گسترده‌تری برای نظارت و حفاظت از شبکه‌های رایانه‌ای داده‌اند. در این راستا، جرایم سایبری به هر گونه فعالیت مجرمانه‌ای اطلاق می‌شود که در آن رایانه یا شبکه رایانه‌ای نقش اساسی ایفا می‌کند؛ چه به‌عنوان ابزار ارتکاب جرم، چه به‌عنوان هدف آن. این نوع از جرایم می‌توانند هم علیه افراد و هم علیه دولت‌ها و شرکت‌ها رخ دهند و طیف وسیعی از اقدامات را شامل می‌شوند، از سرقت اطلاعات شخصی گرفته تا حملات سازمان‌یافته علیه زیرساخت‌های حیاتی. جرایم سایبری را به صورت کلی به سه دسته تقسیم می‌شوند:

۱) جرایمی که رایانه هدف مستقیم آن‌هاست: این دسته شامل حملات علیه سیستم‌های اطلاعاتی و شبکه‌هاست، مانند نفوذ غیرمجاز (هک)، انتشار ویروس‌ها و حملات انکار سرویس.

۲) جرایمی که رایانه ابزار ارتکاب جرم است: مانند کلاهبرداری‌های اینترنتی، فیشینگ، هرزنامه‌ها[6]، پورنوگرافی کودکان، یا جعل هویت آنلاین.

[5] Cyberspace
[6] spam

۳) جرایم مرتبط با محتوا: مانند انتشار محتوای مجرمانه، نفرت‌پراکنی یا تبلیغات تروریستی در فضای مجازی.

یکی از نکات مهم در تعریف جرایم سایبری، ماهیت مرزی‌شکن آن‌ها است. برخلاف جرایم سنتی که در یک حوزه جغرافیایی خاص رخ می‌دهند، جرایم سایبری می‌توانند از راه دور و از طریق اینترنت توسط فردی در یک کشور علیه هدفی در کشوری دیگر انجام شوند. این ویژگی موجب دشواری در تعقیب، شناسایی و محاکمه مرتکبان می‌گردد؛ همچنین، این جرایم به‌سرعت در حال تحول‌اند و به موازات پیشرفت فناوری، اشکال جدیدی از آن‌ها پدید می‌آید. برخی از این جرایم مانند فیشینگ یا حملات بدافزاری، به‌گونه‌ای طراحی شده‌اند که به صورت خودکار گسترش یابند و هزاران قربانی را بدون تماس مستقیم با مرتکب، درگیر سازند. کنوانسیون بوداپست که نخستین معاهده بین‌المللی برای مقابله با جرایم سایبری است. این معاهده توسط شورای اروپا تدوین شد و بر لزوم هماهنگی جهانی در زمینه سیاست‌گذاری کیفری و همکاری‌های قضایی تأکید دارد. (Wikipedia contributors, 2024)

۲-۲-انواع جرایم سایبری

جرایم سایبری شامل مجموعه‌ای گسترده از رفتارهای مجرمانه است که در بستر فضای دیجیتال و با بهره‌گیری از فناوری اطلاعات انجام می‌گیرد. این جرایم را می‌توان در طبقات مختلفی دسته‌بندی کرد؛ از جمله کلاهبرداری رایانه‌ای که شامل دستکاری داده‌ها و تقلب‌های مالی است، بازداشت دیجیتال که اشاره به نگهداری غیرقانونی افراد در بسترهای مجازی دارد، و کارخانه‌های تقلب که مراکزی برای تولید و انتشار محتوای جعلی هستند. تروریسم سایبری نیز با هدف ایجاد رعب و ناامنی از طریق حملات فناوری‌محور انجام می‌شود، در حالی که اخاذی سایبری و باج‌افزار قربانیان را با تهدید به افشای اطلاعات یا قفل کردن داده‌ها مجبور به پرداخت پول می‌کنند؛ همچنین، قاچاق جنسی سایبری از اینترنت برای بهره‌برداری جنسی از افراد استفاده می‌کند و جنگ سایبری شامل حملات سازمان‌یافته دولت‌ها یا گروه‌ها به زیرساخت‌های حیاتی است. در مواردی نیز رایانه به‌عنوان ابزار برای ارتکاب جرایم سنتی مانند کلاهبرداری به کار می‌رود. دیگر اشکال جرایم سایبری عبارت‌اند از انتشار محتوای مستهجن یا توهین‌آمیز، تقلب تبلیغاتی از طریق کلیک‌های جعلی، آزار و اذیت آنلاین شامل تهدید یا تعقیب در فضای مجازی، و قاچاق مواد مخدر که با بهره‌گیری از بستر اینترنت انجام می‌شود. این طیف متنوع از جرایم سایبری چالش‌های گسترده‌ای را برای نهادهای قضایی، امنیتی و حقوقی در سطح ملی و بین‌المللی ایجاد کرده است. (Ibid) طبق تعریف انجمن بین‌المللی پلیس جنایی (اینترپل)، جرایم سایبری به سه دسته کلی تقسیم می‌شوند:

۱) جرایم علیه افراد (مانند آزار و اذیت اینترنتی، سرقت هویت)

۲) جرایم علیه اموال (مانند کلاهبرداری اینترنتی، سرقت مالی آنلاین)

۳) جرایم علیه دولت‌ها و سازمان‌ها (مانند حملات سایبری به زیرساخت‌های حیاتی، جاسوسی دیجیتال) (Interpol, 2013).

انواع جرایم سایبری از دیدگاهی دیگر شامل موارد زیر است:

۱) هک و نفوذ غیرمجاز به سیستم‌ها: هک به معنای دسترسی غیرمجاز به سیستم‌های کامپیوتری یا شبکه‌های دیجیتال است که معمولاً به منظور سرقت اطلاعات، تخریب داده‌ها یا جاسوسی انجام می‌شود. این نوع جرم می‌تواند امنیت سازمان‌ها، بانک‌ها، موسسات دولتی و حتی افراد را به خطر اندازد.(Casey, 2011)

۲) کلاهبرداری اینترنتی (فیشینگ و مهندسی اجتماعی): در این نوع جرایم، مجرمان با ایجاد صفحات جعلی، ایمیل‌های فریبنده یا تماس تلفنی، افراد را ترغیب می‌کنند اطلاعات حساس خود مانند رمز عبور یا شماره کارت اعتباری را افشا کنند. این روش‌ها موجب سرقت مالی و سوءاستفاده از اطلاعات شخصی می‌شوند.(Mitnick & Simon, 2002)

۳) نشر محتوای غیرقانونی و آزارهای آنلاین: انتشار محتواهای غیرقانونی مثل تصاویر و ویدئوهای مستهجن، محتوای خشونت‌آمیز، اخبار جعلی یا آزارهای سایبری[7] به خصوص در میان نوجوانان، یکی از رایج‌ترین جرایم اینترنتی است که پیامدهای روانی و اجتماعی عمیقی دارد.(Patchin & Hinduja, 2010)

۴) سرقت هویت دیجیتال: این جرم شامل استفاده غیرمجاز از اطلاعات شخصی افراد برای اهداف مختلف از جمله کلاهبرداری مالی، جعل اسناد یا فعالیت‌های مجرمانه دیگر است. سرقت هویت می‌تواند منجر به تخریب اعتبار و خسارات مالی جبران‌ناپذیری شود.(Smith, 2007)

۵) حملات مخرب[8]، ویروس‌ها و باج‌افزارها): این نوع جرایم شامل طراحی و انتشار نرم‌افزارهای مخرب است که به سیستم‌های کامپیوتری آسیب می‌زنند، اطلاعات را رمزگذاری یا حذف می‌کنند یا سیستم‌ها را از کار می‌اندازند. باج‌افزارها به تازگی یکی از بزرگ‌ترین تهدیدات امنیتی محسوب می‌شوند که مجرمان از طریق آن درخواست باج مالی می‌کنند.(Symantec, 2019)

۶) جرایم سایبری سازمان‌یافته و تروریسم سایبری: گروه‌های مجرم یا حتی دولت‌ها می‌توانند با استفاده از حملات سایبری، زیرساخت‌های حیاتی کشورها مانند شبکه‌های برق، مخابرات و سیستم‌های بانکی را هدف قرار دهند که تهدیدی برای امنیت ملی است.(Clarke & Knake, 2010)

۲-۳-اهمیت مقابله با جرایم سایبری

با افزایش وابستگی زندگی روزمره به اینترنت، آسیب‌پذیری‌ها نیز بیشتر شده است. جرایم سایبری به دلیل ویژگی‌های خاص فضای مجازی مانند عدم محدودیت جغرافیایی، سرعت بالای انتقال داده و پیچیدگی فناوری، مقابله با آن‌ها دشوارتر از جرایم سنتی است؛ (Grabosky, 2007) بنابراین، تدوین قوانین جامع، آموزش همگانی، استفاده از فناوری‌های نوین امنیتی و همکاری بین‌المللی ضروری است. از سوی دیگر، قربانیان جرایم سایبری، به ویژه نوجوانان و افراد کم‌تجربه، به علت عدم آگاهی کافی، آسیب‌پذیرتر هستند..(Alsmadi & Zarour, 2017) این امر باعث شده تا آموزش پیشگیرانه و افزایش سواد دیجیتال از اولویت‌های مهم امنیت سایبری در جهان باشد. جرایم سایبری به عنوان یکی از چالش‌های بزرگ عصر دیجیتال، تهدیدی جدی برای امنیت فردی، سازمانی و ملی محسوب می‌شوند. شناخت دقیق انواع این جرایم و افزایش آگاهی عمومی از طریق آموزش و قوانین موثر، کلید اصلی مقابله با این پدیده نوظهور است. از آنجا که فناوری با سرعت زیادی در حال پیشرفت است، نیاز به بروزرسانی مداوم دانش، مهارت‌ها و زیرساخت‌های امنیتی نیز بسیار احساس می‌شود. در این راستا، اهمیت مقابله با جرایم سایبری توسط نوجوانان یا علیه آن‌ها از ابعاد حقوقی، اجتماعی، روانی، آموزشی و امنیتی قابل بررسی است:

۱. بُعد حقوقی:

[7] Cyberbullying
[8] Malware

از منظر حقوقی، نوجوانان به‌عنوان گروهی آسیب‌پذیر، هم می‌توانند قربانی و هم مرتکب جرایم سایبری باشند. از یک سو، قربانی شدن نوجوانان در جرایمی مانند اخاذی دیجیتال، آزار آنلاین و بهره‌برداری جنسی از طریق اینترنت، به‌طور مستقیم با نقض حقوق بنیادین آن‌ها نظیر حق امنیت، حریم خصوصی و کرامت انسانی ارتباط دارد. از سوی دیگر، فقدان آموزش‌های کافی در زمینه سواد رسانه‌ای و حقوق دیجیتال، موجب می‌شود برخی نوجوانان ناآگاهانه مرتکب رفتارهای مجرمانه مانند هک، دستکاری داده‌ها یا تهدید همسالان شوند. این مسئله نیازمند بازنگری در قوانین حمایتی و سیاست‌های عدالت کیفری نوجوانان است.(Brenner, 2010)

۲. بُعد روانی و اجتماعی:

تأثیرات روانی جرایم سایبری بر نوجوانان می‌تواند بسیار جدی و حتی ویرانگر باشد. قربانی شدن در فضای مجازی ممکن است منجر به اضطراب، افسردگی، گوشه‌گیری اجتماعی و در موارد حاد، اقدام به خودکشی شود. به ویژه در سنین نوجوانی که هویت فردی در حال شکل‌گیری است، مواجهه با تهدیدات آنلاین می‌تواند پیامدهای بلندمدت بر عزت‌نفس و سلامت روان افراد داشته باشد. علاوه بر آن، نوجوانانی که مرتکب جرایم سایبری می‌شوند نیز در معرض طرد اجتماعی، رفتارهای ضد اجتماعی و افت تحصیلی قرار می‌گیرند.(Patchin & Hinduja, 2010)

۳. بُعد آموزشی:

نقش نظام‌های آموزشی در پیشگیری از جرایم سایبری، به‌ویژه در مقطع نوجوانی، بسیار حیاتی است. آگاهی‌بخشی درباره حقوق دیجیتال، شیوه‌های حفظ امنیت سایبری و آموزش استفاده مسئولانه از شبکه‌های اجتماعی می‌تواند مانعی در برابر ارتکاب یا قربانی شدن در این حوزه باشد. مدارس، والدین و نهادهای دولتی باید با همکاری یکدیگر برنامه‌های جامع آموزش سواد رسانه‌ای را در دستور کار قرار دهند تا نوجوانان نه‌تنها از تهدیدات فضای مجازی آگاه شوند، بلکه به شهروندانی دیجیتال و مسئول تبدیل گردند. (Livingstone et al, 2011)

۴. بُعد امنیتی و بین‌المللی:

با توجه به گسترش دسترسی نوجوانان به فناوری و اینترنت، آنان هم می‌توانند به هدف حملات سایبری توسط گروه‌های مجرم سازمان‌یافته تبدیل شوند، و هم گاه ناآگاهانه ابزار اجرای حملات پیچیده باشند. از این‌رو، مقابله با جرایم سایبری نوجوان‌محور نه‌تنها مسئله‌ای داخلی، بلکه موضوعی بین‌المللی است که مستلزم تدوین پروتکل‌های همکاری چندجانبه برای حفاظت از کودکان در فضای دیجیتال است.(UNICEF, 2017)

۳-بزهکاری سایبری در نوجوانان؛ بررسی عوامل مؤثر بر تمایل به دسترسی غیرمجاز

در این مبحث به بررسی علل و زمینه‌هایی پرداخته می‌شود که نوجوانان را به سمت انجام رفتارهایی مانند هک کردن، نفوذ به حساب‌های کاربری دیگران، یا دسترسی بدون مجوز به اطلاعات محرمانه سوق می‌دهد. این موضوع می‌تواند شامل تحلیل عوامل فردی مانند کنجکاوی، انگیزه‌های هیجانی، نیاز به اثبات توانمندی یا کسب هیجان، عوامل خانوادگی نظیر فقدان نظارت والدین یا ناکارآمدی ارتباطات خانوادگی، عوامل اجتماعی مانند فشار گروه همسالان و رقابت در فضای مجازی، و عوامل محیطی و آموزشی نظیر ضعف سواد دیجیتال یا فقدان آگاهی از پیامدهای قانونی باشد. عوامل مؤثر بر تمایل نوجوانان به دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای ترکیبی از عوامل روان‌شناختی، اجتماعی، خانوادگی و محیطی است. در سطح فردی، کنجکاوی زیاد، نیاز به هیجان، میل به کسب اعتبار در میان

همسالان، و انگیزه‌های مالی یا انتقامجویانه از جمله دلایل اصلی این تمایل هستند؛ همچنین، برخی نوجوانان با بهره‌مندی از مهارت‌های فنی و فقدان چارچوب‌های اخلاقی مناسب، دسترسی غیرمجاز را به‌مثابه چالشی جذاب تلقی می‌کنند. در بُعد خانوادگی، فقدان نظارت مؤثر والدین، ناهنجاری‌های خانوادگی یا فقدان آموزش‌های سایبری زمینه‌ساز این گرایش می‌شود. از منظر اجتماعی نیز، فشار گروه‌های همسال، تأثیر رسانه‌ها و فرهنگ هکری در فضای مجازی می‌تواند الگوی رفتاری نامناسبی برای نوجوانان ایجاد کند. افزون بر این، ضعف در نظام آموزشی در آموزش سواد رسانه‌ای و آگاهی‌بخشی حقوقی، نوجوانان را نسبت به پیامدهای قانونی این اقدامات بی‌توجه می‌سازد. مجموعه این عوامل، به‌ویژه در دوران پرچالش نوجوانی، بستر مساعدی برای شکل‌گیری بزهکاری سایبری از نوع دسترسی غیرمجاز فراهم می‌آورد.

۳-۱-تأثیر تجربه‌های قربانی شدن در فضای مجازی بر گرایش به بزهکاری سایبری

تجربه‌های قربانی شدن در فضای مجازی، مانند آزار و اذیت آنلاین، تهدید، افشای اطلاعات شخصی یا تحقیر در شبکه‌های اجتماعی، می‌تواند تأثیر قابل‌توجهی بر گرایش نوجوانان به بزهکاری سایبری داشته باشد. این تجربه‌ها گاه احساس انتقام، خشم، بی‌اعتمادی به دیگران، یا تمایل به بازپس‌گیری کنترل از دست‌رفته را در نوجوان ایجاد می‌کنند و در برخی موارد منجر به تبدیل شدن قربانی به مرتکب می‌شوند. نوجوانانی که خود را در برابر آسیب‌های فضای مجازی ناتوان می‌بینند، ممکن است با انجام اقدامات تلافی‌جویانه، مانند هک کردن، نفوذ به حساب دیگران یا انتشار اطلاعات، به‌دنبال جبران آسیب روانی واردشده باشند؛ همچنین، قربانی شدن می‌تواند به عادی‌سازی خشونت و نقض حریم خصوصی در ذهن نوجوان بینجامد، به‌گونه‌ای که ارتکاب بزهکاری سایبری دیگر امری غیراخلاقی تلقی نشود. این چرخه قربانی بزهکار در صورت فقدان حمایت روانی و اجتماعی مناسب، ممکن است به تقویت رفتارهای انحرافی در فضای مجازی بینجامد.

۳-۱-۱-همپوشانی نقش بزه‌دیده و بزهکار در فضای مجازی

در ادبیات جرم‌شناسی سنتی، نقش بزه‌دیده و بزهکار اغلب به‌صورت دوگانه در نظر گرفته می‌شود، اما در بستر فضای مجازی، مرز میان این دو نقش به‌شدت تضعیف شده است. نوجوانان فعال در محیط‌های آنلاین ممکن است به‌طور همزمان قربانی و عامل رفتارهای مجرمانه باشند. پژوهش‌های جدید نشان می‌دهد که تجربه‌های منفی نظیر مورد حمله قرار گرفتن در بازی‌های آنلاین، سرقت حساب کاربری، یا آزار سایبری می‌تواند تأثیر روانی عمیقی بر نوجوان گذاشته و زمینه‌ساز بروز رفتارهای تلافی‌جویانه شود. (Kerstens & Jansen, 2016) این واکنش‌ها گاه از مرزهای اخلاقی فراتر رفته و شکل رفتار مجرمانه مانند دسترسی غیرمجاز به حساب‌های دیگران را به خود می‌گیرد. لازم به ذکر است، در فضای مجازی، مرز میان بزه‌دیده و بزهکار اغلب شفاف و مطلق نیست؛ بلکه بسیاری از نوجوانان ممکن است به‌طور همزمان یا متوالی هر دو نقش را تجربه کنند. این پدیده که با عنوان «همپوشانی نقش بزه‌دیده و بزهکار» شناخته می‌شود، بیانگر آن است که نوجوانی که روزی هدف آزار یا تجاوز به حریم خصوصی‌اش بوده، ممکن است در واکنش به آن، دست به اقدامات مجرمانه‌ای همچون تهدید، نفوذ به حساب دیگران، یا افشای اطلاعات شخصی دیگران بزند. این واکنش اغلب از احساس بی‌عدالتی، بی‌قدرتی یا تمایل به تلافی‌جویی نشأت می‌گیرد. در واقع، قربانیان برخی از شدیدترین حملات سایبری، بعدها ممکن است درصدد بازگرداندن «تعادل روانی» از طریق ارتکاب همان نوع رفتارهای مجرمانه در فضای آنلاین برآیند. افزون بر آن، برخی نوجوانان بدون درک کامل از پیامدهای حقوقی و اخلاقی رفتار خود، وارد چرخه معیوبی از تعاملات پرخاشگرانه می‌شوند که در آن نقش‌ها به‌طور مداوم جابه‌جا می‌شود؛ امروز قربانی

آزار آنلاین‌اند، فردا در پاسخ به همان آزار، خود به تهدیدکننده یا هکر تبدیل می‌شوند. این همپوشانی نشان می‌دهد که در فضای مجازی، بزهکاری می‌تواند ناشی از واکنش به آسیب باشد نه صرفاً میل به تخلف. در نتیجه، سیاست‌های پیشگیرانه باید بر درمان زودهنگام آسیب روانی قربانیان، آموزش سواد رسانه‌ای و ارتقای تاب‌آوری روانی نوجوانان متمرکز شود تا از تبدیل بزه‌دیده به بزهکار جلوگیری گردد. در نتیجه پژوهش‌ها در حوزه جرم‌شناسی سایبری نیز بر ضرورت مداخلات بین‌رشته‌ای روان‌شناختی، حقوقی و اجتماعی برای قطع این چرخه تأکید دارند. در نتیجه، درک دقیق همپوشانی بزه‌دیدگی و بزهکاری در فضای مجازی به ما کمک می‌کند تا به‌جای تمرکز صرف بر مجازات، به علل رفتاری و زمینه‌های ساختاری بزهکاری سایبری توجه کنیم و نوجوانان را نه فقط به‌عنوان مجرم، بلکه به‌عنوان قربانیانی با نیازهای حمایتی ببینیم.

۳-۱-۲-نظریه یادگیری اجتماعی[9] و گرایش به تلافی آنلاین[10]

یکی از چارچوب‌های نظری قابل استفاده برای تحلیل این پدیده، نظریه یادگیری اجتماعی آکرز است که تأکید می‌کند رفتار مجرمانه نتیجه فرآیندهای یادگیری در محیط‌های اجتماعی است(.(Akers, 2017 نوجوانانی که خود قربانی جرائم سایبری بوده‌اند، در معرض یادگیری الگوهای رفتاری تهاجمی یا مقابله‌جویانه قرار دارند، به‌ویژه اگر در جوامع مجازی پیرامون آنان، اقدامات بزهکارانه مشروع جلوه کند. در چنین فضایی، دسترسی غیرمجاز می‌تواند به‌مثابه ابزار تلافی یا احقاق عدالت شخصی در نظر گرفته شود. مطالعات تجربی نیز این ارتباط را تأیید کرده‌اند؛ به‌گونه‌ای که نوجوانان قربانی نسبت به سایرین تمایل بیشتری به اقدامات هکری و نفوذ به حساب دیگران دارند Weulen (Kranenbarg et al, 2019).

نظریه یادگیری اجتماعی که توسط آلبرت بندورا ارائه شد، یکی از مهم‌ترین نظریه‌ها در تبیین علل شکل‌گیری رفتارهای مجرمانه و انحرافی، به‌ویژه در نوجوانان است. بر اساس این نظریه، رفتارهای اجتماعی از طریق یادگیری مشاهده‌ای[11]، یعنی مشاهده، تقلید و تقویت، در افراد شکل می‌گیرد. به عبارت دیگر، نوجوانان با مشاهده رفتار دیگران، به‌ویژه الگوهای مهم مانند دوستان، اعضای خانواده یا شخصیت‌های محبوب در فضای مجازی و دریافت پاداش یا اجتناب از تنبیه، یاد می‌گیرند که چه رفتاری در محیط اجتماعی قابل‌قبول یا حتی مطلوب است. در فضای سایبری، این فرآیند یادگیری به‌طور فزاینده‌ای از طریق رسانه‌های اجتماعی، انجمن‌های آنلاین و ارتباطات مجازی صورت می‌گیرد. در این چارچوب، گرایش نوجوانان به تلافی آنلاین نیز قابل تحلیل است. نوجوانانی که در معرض آزار، تهدید، تحقیر یا نقض حریم خصوصی در فضای مجازی قرار گرفته‌اند، ممکن است به‌جای پیگیری حقوقی یا گزارش به والدین یا نهادهای مسئول، به‌صورت خودخواسته وارد فرآیند تلافی‌جویی شوند. نظریه یادگیری اجتماعی توضیح می‌دهد که اگر این نوجوانان در محیط اطراف خود یا در فضای آنلاین مشاهده کنند که رفتارهای تلافی‌جویانه نه‌تنها تنبیه نمی‌شود بلکه موجب اعتبار، حمایت یا همدلی دیگران می‌گردد، احتمال تکرار و درونی‌سازی این رفتار افزایش می‌یابد. به‌ویژه در سنین نوجوانی، که نیاز به اثبات خویشتن، هویت‌یابی و تعلق به گروه اهمیت ویژه‌ای دارد، این نوع پاسخ‌های خشونت‌آمیز می‌تواند مشروعیت ذهنی پیدا کند؛ همچنین، الگوبرداری از رفتارهای پرخاشگرانه دیجیتال در رسانه‌ها یا

[9] Social Learning Theory
[10] Online Retaliation
[11] Observational Learning

گروه‌های مجازی که خشونت یا انتقام را به‌عنوان راه‌حلی موجه یا حتی قهرمانانه تصویر می‌کنند، می‌تواند گرایش به تلافی آنلاین را تشدید کند. در نتیجه، بسترهای یادگیری و تقویت رفتاری در فضای مجازی، به‌ویژه بدون حضور نظارت والدین یا مربیان، زمینه‌ساز عادی‌سازی خشونت سایبری و افزایش رفتارهای مجرمانه واکنشی در نوجوانان می‌شود. از این رو، نظریه یادگیری اجتماعی نه‌تنها به ما در فهم علل بزهکاری سایبری کمک می‌کند، بلکه تأکید دارد که پیشگیری مؤثر نیازمند بازتعریف الگوهای رفتاری در محیط‌های مجازی و واقعی، تقویت آموزش‌های اخلاقی و مسئولیت‌پذیری دیجیتال، و کنترل اجتماعی غیررسمی از سوی همسالان و خانواده است. (Bandura, A, 1977) یکی از مهم‌ترین مطالعات تجربی در زمینه بزهکاری سایبری با تمرکز بر نقش خودکنترلی[۱۲] و همنشینی با همسالان منحرف[۱۳] است. این مقاله با بهره‌گیری از نظریه‌های جرم‌شناسی، به‌ویژه نظریه یادگیری اجتماعی و نظریه خودکنترلی گاتفردسون و هیرشی، تأثیر این دو متغیر را بر رفتارهای مجرمانه با فناوری پیشرفته مانند هک، دسترسی غیرمجاز به اطلاعات، و ایجاد بدافزار بررسی می‌کند. یافته‌های مقاله نشان می‌دهند که نوجوانان یا جوانانی که سطح پایین‌تری از خودکنترلی دارند (یعنی تمایل به رفتارهای آنی، پرخاشگرانه و بدون ارزیابی پیامدها) بیشتر در معرض ارتکاب جرایم سایبری هستند. این تأیید مستقیمی بر نظریه خودکنترلی است که رفتارهای مجرمانه را نتیجه‌ی ناتوانی در مقاومت در برابر وسوسه‌های آنی می‌داند؛ همچنین، ارتباط با دوستانی که خودشان درگیر بزهکاری سایبری هستند، نقش مهمی در افزایش احتمال ارتکاب این نوع جرایم دارد. این عامل دقیقاً با نظریه یادگیری اجتماعی هم‌راستا است که رفتار انحرافی را محصول یادگیری از محیط و الگوهای رفتاری اطراف می‌داند. نوآوری مقاله در این است که به‌جای بررسی جداگانه نظریه‌ها، یک مدل تلفیقی ارائه می‌دهد که نشان می‌دهد چگونه ترکیب خودکنترلی پایین و معاشرت با دوستان بزهکار می‌تواند اثرات هم‌افزایی داشته باشد و فرد را بیش از پیش مستعد انجام رفتارهای مجرمانه در فضای دیجیتال کند. در این راستا، اهمیت مداخلات پیشگیرانه در سطح آموزش، تربیت خانوادگی و کنترل محیطی پیرامون نوجوانان بایستی مد نظر قرار گرفته شود، به‌ویژه آموزش مهارت‌های کنترل هیجانی و انتخاب صحیح گروه دوستی می‌تواند در کاهش بزهکاری سایبری مؤثر باشد. (Bossler, A. M., & Holt, T. J, 2010)

۳-۱-۳-سازوکارهای روانی زمینه‌ساز گذار از قربانی به بزهکار

یکی از پدیده‌های مهم و پیچیده در جرم‌شناسی سایبری، هم‌پوشانی نقش قربانی و بزهکار است، به‌ویژه در میان نوجوانان. بسیاری از افرادی که در فضای مجازی مرتکب بزه می‌شوند، پیش‌تر خود در جایگاه قربانی تجربه‌های آسیب‌زایی داشته‌اند. گذار از نقش قربانی به بزهکار، به‌ویژه در بستر فضای مجازی، اغلب ناشی از سازوکارهای روان‌شناختی دفاعی و هیجانی است که در پاسخ به تجربه آزار، تحقیر یا طرد اجتماعی فعال می‌شوند. پدیده گذر از وضعیت قربانی به بزهکار ممکن است ریشه در واکنش‌های روانی مانند خشم، ترس، و احساس بی‌عدالتی داشته باشد. نوجوانی که خود را بی‌پناه یا مورد بی‌توجهی نهادهای حمایتی می‌بیند، ممکن است با تکیه بر توان فنی یا مشاوره گرفتن از همسالان، مسیر مقابله فردی را در پیش گیرد. فقدان حمایت اجتماعی، تجربه شرمندگی یا بی‌اعتباری در محیط‌های مجازی و فشار گروه همسالان، همگی از عواملی‌اند که این گذار را تسهیل می‌کنند نخستین سازوکار مهم، درونی‌سازی خشم و احساس بی‌عدالتی است. نوجوانی که قربانی آزار آنلاین مانند تمسخر، تهدید یا افشای اطلاعات خصوصی شده

[12] Self-Control
[13] Deviant Peer Association

است، ممکن است به‌جای پردازش سالم تجربه و جستجوی راه‌حل‌های قانونی یا حمایتی، خشم فروخورده خود را با رفتاری تلافی‌جویانه به شکل سایبری تخلیه کند. در این شرایط، فرد با همانندسازی با عامل آزار، وارد چرخه بازتولید خشونت می‌شود، یعنی از قربانی به عامل خشونت جدید بدل می‌گردد. سازوکار دیگر، تحریف شناختی و توجیه اخلاقی است. قربانیان سابق ممکن است با تحریف قضاوت اخلاقی، رفتار انتقام‌جویانه خود را مشروع جلوه دهند؛ برای نمونه، این باور که «اگر من آسیب دیده‌ام، حق دارم مقابله به مثل کنم» یا «دیگران هم این کار را می‌کنند»، باعث کاهش احساس گناه و افزایش آمادگی روانی برای ارتکاب جرم می‌شود. این نوع تساهل شناختی می‌تواند زمینه‌ساز گرایش به حملات سایبری، توهین، افشای اطلاعات دیگران یا مشارکت در گروه‌های بزهکار آنلاین باشد؛ همچنین، نقش احساس بی‌قدرتی و نیاز به بازسازی هویت را نمی‌توان نادیده گرفت. قربانی شدن در فضای مجازی، به‌ویژه برای نوجوانان، می‌تواند موجب تضعیف حس ارزشمندی و کاهش اعتمادبه‌نفس شود. در چنین شرایطی، بعضی افراد برای بازسازی هویت اجتماعی یا بازگرداندن احساس کنترل، به کنش‌های مجرمانه سایبری مانند هک کردن، افشای اطلاعات دیگران، یا مشارکت در کمپین‌های نفرت‌پراکنی روی می‌آورند؛ (Parti et al, 2022) بنابراین، تجربه قربانی شدن در فضای مجازی نه‌تنها یک پیامد منفی است، بلکه در غیاب مداخلات حمایتی، می‌تواند عاملی خطرناک در توسعه بزهکاری سایبری نوجوانان باشد. در مجموع، این سازوکارهای روان‌شناختی، از جمله خشم فروخورده، تحریف شناختی، همانندسازی با بزهکار، نیاز به بازسازی قدرت و کنترل، و توجیه اخلاقی می‌توانند مسیر گذار از قربانی به بزهکار را تسهیل کنند، به‌ویژه در فضای مجازی که نظارت مستقیم ضعیف‌تر و پیامدهای فوری کمتر قابل لمس است. برای پیشگیری از این گذار، مداخلاتی مانند آموزش مهارت‌های مقابله‌ای، تقویت تاب‌آوری روانی و حمایت اجتماعی از قربانیان سایبری اهمیت ویژه دارد.

۳-۲-نقش دانش و آگاهی نسبت به قانون در ارتکاب یا پیشگیری از بزهکاری سایبری

یکی از عوامل مهم و اثرگذار در حوزه پیشگیری از بزهکاری سایبری، دانش و آگاهی افراد، به‌ویژه نوجوانان، نسبت به قوانین و مقررات فضای مجازی است. آگاهی از پیامدهای قانونی اعمالی مانند هک کردن، افشای اطلاعات شخصی دیگران، ارسال محتوای توهین‌آمیز یا شرکت در معاملات غیرقانونی آنلاین، می‌تواند به‌عنوان بازدارنده‌ای مؤثر عمل کند. بسیاری از نوجوانان به دلیل ناآگاهی از اینکه رفتارهای‌شان مصداق جرم است، ناخواسته وارد مسیر بزهکاری می‌شوند. این موضوع نشان می‌دهد که آموزش حقوقی و آشنایی با چارچوب‌های قانونی می‌تواند از ارتکاب رفتارهای مجرمانه پیشگیری کند. در نقطه مقابل، فقدان آموزش‌های کافی در زمینه حقوق فضای مجازی باعث شکل‌گیری نوعی برداشت سطحی و سهل‌انگارانه نسبت به قانون در بستر آنلاین می‌شود. برای مثال، فردی ممکن است تصور کند که استفاده از نرم‌افزارهای کرک شده، انتشار تصاویر شخصی دیگران، یا ورود غیرمجاز به حساب‌های کاربری دیگران تنها «شوخی آنلاین» است و فاقد بار کیفری است. این‌گونه برداشت‌ها ناشی از خلأ آگاهی حقوقی و فرهنگی در میان کاربران نوجوان و حتی برخی بزرگسالان است. نکته مهم‌تر آن است که دانش حقوقی تنها به شناخت متن قانون محدود نمی‌شود، بلکه شامل درک مفهوم مسئولیت کیفری، رعایت حریم خصوصی و تبعات اجتماعی و اخلاقی رفتارهای سایبری نیز هست. این نوع درک به افراد کمک می‌کند تا خود را در جایگاه دیگران قرار دهند و از ارتکاب اعمالی که موجب آسیب به دیگران می‌شود، اجتناب ورزند؛ بنابراین، توسعه سواد حقوقی دیجیتال، می‌تواند زمینه‌ساز تقویت

اخلاق دیجیتال و مسئولیت‌پذیری آنلاین باشد. از نظر جرم‌شناسی پیشگیرانه، آموزش عمومی و حقوقی در مدارس، خانواده‌ها، و رسانه‌ها می‌تواند در پیشگیری اولیه از بزهکاری سایبری نقشی حیاتی ایفا کند. آگاهی از قوانین خاص مانند قانون جرایم رایانه‌ای ایران مصوب ۱۳۸۸ یا کنوانسیون بوداپست درباره جرایم سایبری، موجب درک بهتر مرزهای قانونی در رفتارهای دیجیتال خواهد شد. در نتیجه، افزایش آگاهی حقوقی را می‌توان یکی از مؤثرترین راهبردهای غیرکیفری برای کاهش بزهکاری سایبری در میان نوجوانان و جوانان دانست.

۳-۲-۱-تناقض آگاهی قانونی و ارتکاب عمل مجرمانه

یکی از پدیده‌های پیچیده در زمینه بزهکاری سایبری، تناقض میان آگاهی قانونی و ارتکاب عمل مجرمانه است؛ به این معنا که بسیاری از افراد، به‌ویژه نوجوانان و جوانان، با وجود داشتن شناخت نسبتاً کافی از قوانین مربوط به فضای مجازی، همچنان دست به ارتکاب جرایم سایبری می‌زنند. این تناقض نشان می‌دهد که صرف داشتن دانش و آگاهی از قوانین، تضمینی برای پرهیز از رفتارهای مجرمانه نیست و عوامل روانی، اجتماعی و فرهنگی دیگر نیز در تصمیم‌گیری فرد نقش مهمی ایفا می‌کنند. یکی از یافته‌های جالب توجه در مطالعات جدید، تحت عنوان " Cybercrime: The Human Factor"، آن است که آگاهی نوجوانان از قوانین مرتبط با جرائم سایبری لزوماً منجر به کاهش رفتارهای مجرمانه نمی‌شود؛ بلکه در برخی موارد، افزایش آگاهی حتی با احتمال بیشتر ارتکاب تخلف همراه بوده است؛ یکی از دلایل این تناقض، احساس عدم پاسخگویی و فقدان نظارت کافی در فضای مجازی است. افراد ممکن است باور کنند که حتی اگر عملشان غیرقانونی باشد، شناسایی و پیگرد قانونی آنها دشوار است یا اینکه مجازات‌های اعمال شده بازدارندگی لازم را ندارند. این تصور باعث می‌شود که علی‌رغم آگاهی قانونی، ریسک ارتکاب جرم را بپذیرند. علاوه بر این، فضای مجازی ماهیتی غیرمتمرکز و غیرقابل لمس دارد که امکان فرار از پیگرد قانونی را برای بزهکاران آسان‌تر می‌کند. علاوه بر این، عوامل انگیزشی مانند هیجان‌جویی، فشار همسالان، یا انگیزه‌های اقتصادی و انتقام‌جویی می‌توانند بر آگاهی قانونی غلبه کنند و فرد را به سمت ارتکاب جرم سوق دهند. برای مثال، نوجوانی که تحت فشار گروه دوستان است یا به دنبال کسب درآمد سریع از طریق روش‌های غیرقانونی است، ممکن است ریسک‌های قانونی را نادیده بگیرد؛ همچنین، برخی افراد در واکنش به تجربیات منفی مانند قربانی شدن در فضای مجازی، انگیزه تلافی جویی پیدا کرده و قوانین را به‌عنوان مانعی قابل چشم‌پوشی می‌بینند. (Skinner & Fream, 1997).

پژوهش اخیر منتشرشده در مجله "Journal of Criminal Justice" نیز به این نکته اشاره دارد که نوجوانان با دانش بالاتر درباره قانون "Computer Misuse Act" در بریتانیا، در برخی موارد تمایل بیشتری به آزمایش مرزهای قانونی از خود نشان داده‌اند (Maras et al, 2024). این پدیده می‌تواند ناشی از درک نادرست از قابلیت کشف جرم، یا اعتماد بیش از حد به توان فنی خود باشد؛ بنابراین، برای کاهش این تناقض، ضروری است که علاوه بر افزایش آگاهی قانونی، مداخلات روانی، اجتماعی و فرهنگی نیز در نظر گرفته شود تا عوامل زمینه‌ای و انگیزشی بزهکاری کاهش یابد. ایجاد فضایی که فرد احساس کند رفتارهایش تحت نظارت است، همچنین تقویت حس مسئولیت‌پذیری اخلاقی و اجتماعی می‌تواند تأثیر بیشتری در کاهش جرایم سایبری نسبت به صرف آموزش حقوقی داشته باشد. این نکته اهمیت رویکردهای جامع و چندجانبه در پیشگیری از بزهکاری سایبری را نشان می‌دهد.

۳-۲-۲- تمایز میان آگاهی حقوقی و درک خطرات اجتماعی

آگاهی حقوقی به معنای شناخت و فهم قوانین و مقررات موجود درباره رفتارهای مجاز و غیرمجاز در فضای مجازی است؛ یعنی فرد می‌داند چه کارهایی از نظر قانون جرم محسوب می‌شوند و چه پیامدهای کیفری برای آنها تعریف شده است. این نوع آگاهی بیشتر جنبه رسمی و قانونی دارد و به فرد اطلاعات دقیق درباره چارچوب‌های حقوقی ارائه می‌دهد. برای مثال، نوجوانی که با قانون جرایم رایانه‌ای آشناست، می‌داند که هک کردن حساب کاربری دیگران یا سرقت اطلاعات، عملی غیرقانونی است و ممکن است مجازات داشته باشد، اما درک خطرات اجتماعی فراتر از شناخت قوانین است و به شناخت تأثیرات گسترده‌تر رفتارها بر جامعه، روابط انسانی و سلامت روانی اشاره دارد. فردی که درک خطرات اجتماعی بالایی دارد، می‌فهمد که بزهکاری سایبری نه تنها از نظر قانونی ناپسند و مجرمانه است، بلکه می‌تواند به آسیب‌های روانی، اجتماعی و اقتصادی برای خود و دیگران منجر شود. برای مثال، می‌داند که آزار و اذیت آنلاین (سایبری) می‌تواند باعث ایجاد اضطراب، افسردگی و انزوای اجتماعی در قربانیان شود و در نتیجه روابط اجتماعی و کیفیت زندگی افراد را به شدت تحت تأثیر قرار دهد. این تمایز اهمیت زیادی دارد، چرا که صرفاً داشتن آگاهی حقوقی نمی‌تواند به‌تنهایی از بزهکاری سایبری پیشگیری کند. فرد ممکن است بداند که فلان رفتار جرم است، اما چون درک درستی از پیامدهای اجتماعی و انسانی آن نداشته باشد، همچنان به آن عمل ادامه دهد. برعکس، وقتی درک خطرات اجتماعی قوی باشد، احتمال این که فرد به‌دلیل حساسیت نسبت به آسیب‌های وارد شده به دیگران و جامعه، از ارتکاب عمل مجرمانه خودداری کند، بیشتر است؛ بنابراین، آموزش‌های پیشگیرانه باید به‌گونه‌ای طراحی شود که علاوه بر آموزش قوانین، آگاهی‌های اجتماعی، اخلاقی و روانی را نیز تقویت کند تا تأثیرگذاری واقعی و پایداری داشته باشد. لازم به ذکر است، آگاهی صرف از قواعد قانونی لزوماً منجر به بازدارندگی مؤثر نمی‌شود، مگر آنکه این آگاهی با درک پیامدهای اجتماعی، روانی، و فردی همراه باشد. در واقع، نوجوان ممکن است بداند که دسترسی غیرمجاز عملی غیرقانونی است، اما اگر این اقدام در میان گروه همسالانش به‌عنوان رفتاری قهرمانانه یا هوشمندانه تلقی شود، انگیزه بازدارنده قانون تضعیف می‌گردد.(Berenblum et al, 2019) بر همین اساس، برخی مداخلات پلیسی از جمله برنامه " Cyber Choices" تلاش دارند تا علاوه بر آموزش قانون، نوجوانان را نسبت به پیامدهای اجتماعی و حرفه‌ای رفتارهایشان نیز آگاه سازند.(National Crime Agency, 2017) در نهایت، ترکیب آگاهی حقوقی با درک عمیق‌تر از پیامدهای اجتماعی می‌تواند باعث شکل‌گیری رفتارهای مسئولانه‌تر در فضای مجازی شود و نوجوانان را نسبت به تبعات رفتاری خود در دنیای دیجیتال حساس‌تر سازد. این رویکرد جامع، علاوه بر افزایش آگاهی، موجب ارتقای تاب‌آوری و مهارت‌های اجتماعی نوجوانان شده و به پیشگیری مؤثرتر از بزهکاری سایبری کمک می‌کند.

۳-۲-۳-نقش آموزش تعاملی و برنامه‌های پیشگیرانه

برنامه‌های آموزشی صرفاً مبتنی بر انتقال اطلاعات قانونی نمی‌توانند به‌تنهایی در پیشگیری از بزهکاری مؤثر باشند. آنچه اثربخشی این برنامه‌ها را افزایش می‌دهد، روش تعاملی، استفاده از روایت‌های واقعی، و شبیه‌سازی سناریوهای عملی است. پژوهش‌های تجربی در این زمینه نشان می‌دهد که روش‌های آموزشی تعاملی با مشارکت پلیس، روان‌شناس و متخصصان فناوری اطلاعات می‌تواند درک عمیق‌تری از خطرات و پیامدهای جرائم سایبری در نوجوانان ایجاد کند .(vander Wagen et al, 2021) بر این اساس، سیاست‌گذاران باید از شیوه‌های خلاقانه، مانند بازی‌سازی آموزشی، بهره گیرند، تا فهم نوجوانان از بزهکاری، از سطح نظری به سطح عاطفی و رفتاری ارتقاء یابد. آموزش تعاملی

یکی از مؤثرترین روش‌ها برای ارتقای آگاهی و تغییر رفتار در زمینه پیشگیری از بزهکاری سایبری است. برخلاف روش‌های سنتی آموزش که معمولاً به صورت یک‌طرفه و حفظ مطالب صرف ارائه می‌شوند، آموزش تعاملی دانش‌آموزان و نوجوانان را به مشارکت فعال دعوت می‌کند. این روش‌ها شامل بازی‌های آموزشی، شبیه‌سازی موقعیت‌های واقعی، بحث گروهی و تمرین مهارت‌های حل مسئله هستند که به یادگیرندگان کمک می‌کند تا مفاهیم حقوقی، اخلاقی و اجتماعی فضای مجازی را به صورت کاربردی و عمیق‌تر درک کنند. تجربه مستقیم و عملی در محیط آموزش موجب می‌شود یادگیرندگان نه تنها قوانین را بشناسند، بلکه چگونگی مواجهه با چالش‌های واقعی فضای مجازی را نیز فرا بگیرند. برنامه‌های پیشگیرانه جامع که بر مبنای آموزش تعاملی طراحی شده‌اند، علاوه بر افزایش دانش حقوقی و آگاهی از خطرات سایبری، تمرکز ویژه‌ای بر توسعه مهارت‌های اجتماعی و روانی دارند. این برنامه‌ها می‌توانند شامل آموزش مهارت‌های کنترل خشم، مدیریت هیجان، تقویت خودکنترلی و افزایش حس مسئولیت‌پذیری دیجیتال باشند که نقش مهمی در کاهش گرایش به بزهکاری سایبری ایفا می‌کنند. به علاوه، برنامه‌های پیشگیرانه معمولاً خانواده‌ها و معلمان را نیز درگیر می‌کنند تا در کنار نوجوانان، یک شبکه حمایتی گسترده ایجاد شود که رفتارهای پرخطر را کاهش دهد. همان طور که بیان گردید، تحقیقات نشان داده‌اند که آموزش تعاملی و برنامه‌های پیشگیرانه ساختاریافته می‌توانند به طور قابل توجهی رفتارهای پرخطر آنلاین را کاهش داده و باعث افزایش تاب‌آوری نوجوانان در برابر فشارهای گروهی و انگیزه‌های غیرقانونی شوند. این روش‌ها، ضمن ایجاد فضای امن برای یادگیری و تجربه، به نوجوانان امکان می‌دهد تا خودشان را در موقعیت‌های مختلف تصور کرده و پیامدهای رفتارش را بهتر درک کنند. به این ترتیب، آموزش تعاملی نه تنها موجب افزایش دانش می‌شود، بلکه رفتارهای پیشگیرانه و انتخاب‌های هوشمندانه‌تر در فضای سایبری را نیز ترویج می‌دهد.

۳-۳-تأثیر ویژگی‌های روان‌شناختی و اجتماعی بر بزهکاری سایبری نوجوانان

ویژگی‌های روان‌شناختی فرد نقش محوری در شکل‌گیری رفتارهای بزهکارانه در فضای مجازی دارد. نوجوانانی که دچار اختلالاتی نظیر ضعف در خودکنترلی، تکانش‌گری، پرخاشگری یا احساس ناکامی مکرر هستند، معمولاً آمادگی بیشتری برای ارتکاب جرایم سایبری دارند. مطالعات متعدد نشان می‌دهد که فقدان کنترل نفس و تعامل با همسالان منحرف، احتمال گرایش به بزهکاری سایبری را به طور قابل‌توجهی افزایش می‌دهد. نوجوانانی که فاقد مهارت‌های مدیریت هیجان هستند یا از عزت‌نفس پایینی رنج می‌برند، ممکن است برای جبران خلأهای روانی یا کسب قدرت، به فعالیت‌های غیرقانونی در فضای مجازی روی آورند، مانند هک کردن، آزار و اذیت سایبری یا انتشار اطلاعات خصوصی دیگران. از سوی دیگر، عوامل اجتماعی نظیر فشار گروه همسالان، فقدان نظارت والدین، محیط مدرسه ناسالم و محرومیت از منابع حمایتی نیز تأثیر مستقیمی بر شکل‌گیری بزهکاری سایبری در نوجوانان دارند. نوجوانان به شدت تحت تأثیر هنجارهای گروهی قرار دارند، به‌ویژه در فضای آنلاین که هویت افراد می‌تواند پنهان بماند و رفتارهای پرخطر با تشویق دیگران همراه شود. وقتی فضای مجازی به محیطی برای دریافت تأیید اجتماعی، قدرت‌نمایی یا تخلیه هیجانات تبدیل شود، نوجوانانی که در محیط خانواده یا جامعه دچار احساس طرد، تبعیض یا نادیده‌انگاری هستند، ممکن است بیش از سایرین به رفتارهای بزهکارانه سایبری روی آورند؛ همچنین، تجارب منفی مانند قربانی شدن در فضای مجازی، تجربه طرد اجتماعی یا مورد تمسخر قرار گرفتن در شبکه‌های اجتماعی می‌تواند به بروز رفتارهای

انتقامجویانه منجر شود. در چنین شرایطی، نوجوان ممکن است به‌عنوان مکانیزم دفاعی یا جبرانی، خود نیز به بزهکار سایبری تبدیل شود. این پدیده به‌ویژه در شرایطی رخ می‌دهد که سیستم‌های حمایتی از قربانیان ضعیف باشند و راهکاری برای بیان خشم یا جبران آسیب‌ها وجود نداشته باشد. در مجموع، ترکیب عوامل روان‌شناختی (مانند ضعف در خودکنترلی یا هیجان‌خواهی) با عوامل اجتماعی (مانند فشار گروهی یا ضعف نظارت خانوادگی) می‌تواند بستر مساعدی برای بزهکاری سایبری نوجوانان فراهم آورد؛ بنابراین، مداخلات مؤثر باید چندبعدی باشند و هم به درمان مشکلات فردی و روانی بپردازند و هم در جهت ارتقای محیط‌های اجتماعی ایمن، حمایتگر و آگاه تلاش کنند. چنین رویکردی می‌تواند به کاهش معنادار رفتارهای پرخطر سایبری در میان نوجوانان بینجامد.

۳-۳-۱-نقش کنترل نفس پایین و ناتوانی در تنظیم هیجانات

کنترل نفس پایین[14] یکی از شاخص‌ترین متغیرهای روان‌شناختی در تبیین رفتارهای بزهکارانه، به‌ویژه در فضای مجازی است. نوجوانانی که از سطح پایین خودکنترلی برخوردارند، معمولاً به‌سختی می‌توانند در برابر وسوسه‌ها، محرک‌های آنی و پاداش‌های فوری مقاومت کنند. در فضای مجازی که فرصت‌های متعددی برای رفتارهای پرخطر همچون هک کردن، توهین سایبری، یا نشر اطلاعات محرمانه وجود دارد، این دسته از نوجوانان بیشتر در معرض ارتکاب بزه قرار می‌گیرند. نوجوانانی با خودکنترلی پایین، تمایل بیشتری به همراهی با همسالان منحرف دارند و در نتیجه بیشتر درگیر جرایم سایبری می‌شوند. در این شرایط، فقدان مهارت در پیش‌بینی پیامدهای بلندمدت و گرایش به لذت‌های آنی، عامل مهمی در شکل‌گیری رفتار مجرمانه محسوب می‌شود. در این راستا، مطالعات متعددی در حوزه روان‌شناسی جنایی نشان داده‌اند که کنترل نفس پایین یکی از قوی‌ترین پیش‌بینی‌کننده‌های رفتارهای مجرمانه در فضای سایبری است. نوجوانانی که توانایی محدودی در مدیریت هیجانات، به‌ویژه خشم، حسادت یا تحقیر دارند، بیشتر مستعد انجام اعمالی همچون نفوذ غیرمجاز به حساب‌های کاربری هستند. تنظیم هیجانات[15] به توانایی فرد در مدیریت، کنترل و پاسخ‌دهی متعادل به احساسات منفی یا شدید گفته می‌شود. نوجوانانی که در این زمینه دچار ضعف هستند، در مواجهه با موقعیت‌های استرس‌زا، تهدیدآمیز یا تحقیرکننده، بیشتر دچار واکنش‌های افراطی می‌شوند. در فضای مجازی، این ضعف می‌تواند خود را به شکل انتقام‌جویی سایبری، آزار دیگران، یا انجام حملات کلامی و تصویری نشان دهد. ناتوانی در تنظیم هیجانات به‌ویژه در مواجهه با محرک‌هایی مانند طرد اجتماعی، قلدری اینترنتی یا شکست‌های ارتباطی می‌تواند موجب بروز رفتارهای تهاجمی آنلاین شود. برخی از نوجوانان در چنین شرایطی برای تخلیه هیجانی خود، به انتشار محتواهای مخرب یا نفوذ غیرمجاز به حساب‌های دیگران روی می‌آورند، بدون آنکه پیامدهای حقوقی یا اخلاقی آن را به‌درستی درک کنند؛ بنابراین، آموزش مهارت‌های تنظیم هیجان و تقویت تاب‌آوری روانی می‌تواند نقش مهمی در پیشگیری از بزهکاری سایبری داشته باشد .(Nodeland, 2020) این موضوع به‌ویژه زمانی حاد می‌شود که فرد احساس کند در فضای حقیقی یا مجازی نادیده گرفته شده است و از این طریق در پی بازیابی احساس کنترل یا ارزش فردی خود است.

[14] low self-control
[15] Emotion Regulation

۳-۳-۲-تأثیرات گروه همسالان و فشار اجتماعی در فضای مجازی

گروه همسالان یکی از مهم‌ترین عوامل اجتماعی مؤثر بر رفتار نوجوانان است، به‌ویژه در دوران نوجوانی که نیاز به تعلق، تأیید اجتماعی و شناسایی با گروه هم‌سن‌وسالان به اوج خود می‌رسد. در فضای مجازی، این وابستگی به گروه همسالان می‌تواند تأثیرات عمیق‌تری نیز داشته باشد، چرا که نوجوانان در این محیط‌ها اغلب با محتوایی مواجه می‌شوند که هنجارهای غیرقانونی یا ضداجتماعی را ترویج می‌کند. زمانی که یک نوجوان مشاهده می‌کند دوستان یا اعضای گروهش بدون عواقب جدی به هک کردن، شوخی‌های مخرب اینترنتی یا ارسال محتوای تحقیرآمیز اقدام می‌کنند، احتمال زیادی وجود دارد که او نیز برای پذیرش در گروه یا جلوگیری از طرد، دست به اعمال مشابه بزند. همان طور که بیان گردید، طبق نظریه یادگیری اجتماعی، مشاهده و تقلید رفتارهای دیگران در بسترهای اجتماعی، به‌ویژه وقتی با تقویت مثبت همراه باشد، نقشی اساسی در یادگیری و تکرار آن رفتارها ایفا می‌کند.

فشار اجتماعی در فضای مجازی اشکال جدیدی به خود می‌گیرد که از طریق پیام‌های گروهی، چالش‌های مجازی (مانند "چالش هک")، یا ترندهای توهین‌آمیز منتقل می‌شود. نوجوانان به‌ویژه زمانی که با ترس از تحقیر، نادیده‌گرفته‌شدن یا از دست دادن محبوبیت مجازی مواجه می‌شوند، ممکن است علی‌رغم شناخت از نادرست‌بودن یک عمل، به آن تن دهند. این نوع فشار اجتماعی اغلب به‌شکل پنهان یا روانی عمل می‌کند، به‌گونه‌ای که فرد احساس می‌کند در صورت مخالفت با هنجارهای گروه، از نظر اجتماعی منزوی خواهد شد. چنین فرایندهایی می‌توانند نوجوان را به سمت مشارکت در جرایم سایبری مانند ارسال پیام‌های تهدیدآمیز، افشای اطلاعات خصوصی دیگران یا مشارکت در حملات گروهی سوق دهند. بنابراین، آموزش مهارت «نه گفتن»، تقویت هویت فردی و آگاهی‌بخشی درباره اثرات قانونی این اقدامات، از ابزارهای کلیدی برای کاهش تأثیر فشار اجتماعی در فضای سایبری است.

در میان نوجوانان، هویت فردی اغلب در تعامل با گروه همسالان شکل می‌گیرد. فضای مجازی محیطی فراهم می‌آورد که در آن ارزش‌گذاری رفتارهای پرخطر، از جمله نفوذ به سیستم‌های دیگران، به‌عنوان نشانه‌ای از مهارت، قدرت یا محبوبیت تلقی شود. پژوهش‌ها نشان می‌دهد که نوجوانانی که در گروه‌های دارای ارزش‌گذاری منفی نسبت به قانون عضویت دارند، احتمال ارتکاب بزهکاری سایبری در آنان بیشتر است .(Holt et al, 2012) این تأثیر با حضور در انجمن‌ها و فروم‌های آنلاین که دانش فنی غیرقانونی را ترویج می‌دهند، تشدید می‌گردد.

۳-۳-۳-پدیده گمنامی و گسست از پیامدهای رفتاری

یکی از ویژگی‌های منحصربه‌فرد فضای سایبری، امکان ناشناس ماندن کاربران است. این گمنامی می‌تواند سبب بروز پدیده‌ای به‌نام «گسست اخلاقی» شود که در آن فرد، به‌دلیل عدم رویارویی مستقیم با پیامدهای رفتار خود، احساس مسئولیت اخلاقی نمی‌کند. این ویژگی، از سویی باعث آزادی بیان و حفاظت از حریم خصوصی می‌شود، اما از سوی دیگر، می‌تواند بستری برای بروز رفتارهای ضد اجتماعی و مجرمانه فراهم سازد. زمانی که یک فرد احساس می‌کند شناسایی نمی‌شود و تحت نظارت مستقیم قرار ندارد، احتمال بیشتری وجود دارد که به اعمالی چون توهین، فریب، هک، تهدید و انتشار اطلاعات کذب دست بزند. این حالت روان‌شناختی در ادبیات جرم‌شناسی سایبری، به‌عنوان «گسست از پیامدهای رفتاری» شناخته می‌شود؛ به این معنا که فرد، به‌واسطه قطع ارتباط ذهنی با پیامدهای قانونی، اخلاقی و اجتماعی عمل خود، جرأت ارتکاب آن را پیدا می‌کند. نوجوان ممکن است دسترسی غیرمجاز را تنها یک بازی فنی بداند، نه عملی مجرمانه با تبعات حقوقی و اخلاقی. همین گسست میان عمل و پیامد، در کنار فقدان نظارت والدین یا نهادهای

رسمی، بستر مستعدی برای رشد بزهکاری در محیط‌های آنلاین فراهم می‌آورد. در این راستا، بزهکاری سایبری در نوجوانان پدیده‌ای چندبُعدی و پیچیده است که نه‌تنها از فاکتورهای قانونی و فنی، بلکه از عوامل روانی، اجتماعی و تربیتی تأثیر می‌پذیرد. تجربه قربانی شدن، گروه همسالان، ناشناسی در فضای آنلاین و حتی دانش ناقص یا سوءتفسیر شده از قانون، همگی نقش‌های مؤثری در گرایش نوجوانان به اعمالی همچون دسترسی غیرمجاز ایفا می‌کنند. برای پیشگیری مؤثر، باید از سیاست‌های چندجانبه شامل آموزش تعاملی، اصلاح بسترهای اجتماعی آنلاین، و تقویت مهارت‌های خودکنترلی نوجوانان بهره گرفت. از منظر روان‌شناختی، گمنامی نوعی "پرده روانی" ایجاد می‌کند که مسئولیت‌پذیری فرد را کاهش می‌دهد. زمانی که نوجوانان در محیطی قرار می‌گیرند که نام، چهره و موقعیت مکانی آن‌ها پنهان است، حس پاسخ‌گویی[16] در آن‌ها کمرنگ می‌شود. به‌ویژه در سنین نوجوانی که بخش‌های مربوط به آینده‌نگری و درک نتایج بلندمدت در مغز هنوز به‌طور کامل رشد نیافته‌اند، گمنامی می‌تواند آثار تشدیدکننده‌ای داشته باشد. برای نمونه، نوجوانی که در فضای مجازی اقدام به توهین یا افشای تصاویر خصوصی یک همسال می‌کند، ممکن است تحت تأثیر حس گسست از واقعیت، عمل خود را تنها یک شوخی یا سرگرمی بی‌ضرر تلقی کرده و از تأثیر مخرب آن بر قربانی آگاه نباشد. (Morris & Blackburn, 2009)

افزون بر این، پژوهش‌ها نشان داده‌اند که گمنامی نه تنها موجب بروز رفتارهای پرخطر می‌شود، بلکه در درازمدت می‌تواند احساس همدلی را در افراد کاهش داده و الگوهای رفتاری نامطلوب را تقویت کند. این موضوع در نظریه «کاهش بازداری اجتماعی» مطرح شده توسط سولر[17] نیز بررسی شده است، که نشان می‌دهد کاربران آنلاین در محیط‌های گمنام، راحت‌تر مرزهای اخلاقی و اجتماعی را نقض می‌کنند؛ بنابراین، شناخت این پدیده و تلاش برای ایجاد محیط‌های نظارتی و آموزشی مؤثر برای نوجوانان، می‌تواند به کاهش بزهکاری سایبری ناشی از گمنامی کمک کند. (Suler ,2004)

٤- بررسی عوامل مؤثر بر بزهکاری سایبری نوجوانان: تحلیل عوامل شخصی، خانوادگی و حقوقی

عوامل مؤثر بر بزهکاری سایبری نوجوانان را می‌توان در سه سطح شخصی، خانوادگی و حقوقی تحلیل کرد که هرکدام به‌طور مستقیم یا غیرمستقیم در شکل‌گیری رفتار مجرمانه نقش دارند. در سطح شخصی، ویژگی‌هایی مانند کنترل نفس پایین، ناتوانی در تنظیم هیجانات، اضطراب اجتماعی، و تجربه‌های قربانی شدن در فضای مجازی می‌توانند نوجوان را به‌سمت بزهکاری سوق دهند. در سطح خانوادگی، نظارت ضعیف والدین، ارتباط عاطفی کم، درگیری‌های خانوادگی و فقدان آموزش‌های لازم درباره استفاده ایمن از فناوری، زمینه‌ساز گرایش نوجوان به گروه‌های منحرف در فضای مجازی می‌شود. از سوی دیگر، در سطح حقوقی، فقدان آگاهی کافی نوجوانان نسبت به قوانین جرایم رایانه‌ای، یا برداشت‌های اشتباه از پیامدهای حقوقی اعمالشان، باعث می‌شود تا آن‌ها اعمال غیرقانونی مانند هک، ارسال پیام‌های تهدیدآمیز یا انتشار محتوای خصوصی دیگران را جدی نگیرند. در مجموع، هم‌پوشانی و تعامل این سه دسته عامل، در کنار گمنامی فضای مجازی، ریسک بزهکاری سایبری در نوجوانان را افزایش می‌دهد.

[16] accountability
[17] Suler

٤-١-عوامل شخصی مؤثر بر بزهکاری سایبری نوجوانان

عوامل شخصی مؤثر بر بزهکاری سایبری نوجوانان به ویژگی‌های روان‌شناختی، رفتاری و شناختی آنان بازمی‌گردد و نقش مهمی در تمایل یا بازداری آن‌ها از ارتکاب جرایم سایبری دارد. نوجوانانی که دارای کنترل نفس پایین هستند، بیشتر در معرض تصمیم‌گیری‌های هیجانی و ناگهانی قرار می‌گیرند و ممکن است بدون ارزیابی پیامدهای قانونی یا اخلاقی، وارد فعالیت‌های مجرمانه سایبری شوند؛ همچنین، ناتوانی در تنظیم هیجانات مانند خشم، اضطراب یا احساس طرد اجتماعی، می‌تواند آن‌ها را به واکنش‌های تلافی‌جویانه آنلاین یا آزار سایبری سوق دهد. علاوه بر این، تجربه‌های قبلی قربانی شدن در فضای مجازی می‌تواند احساس بی‌اعتمادی و آسیب‌پذیری را در نوجوانان افزایش دهد و موجب شود که خود نیز در نقش بزهکار ظاهر شوند؛ پدیده‌ای که به «چرخه قربانی ـ بزهکار» معروف است؛ همچنین، سطح پایین همدلی، اعتماد به نفس شکننده و تمایل به هیجان‌جویی یا ماجراجویی دیجیتال نیز از جمله عوامل شخصی‌ای هستند که با افزایش احتمال مشارکت در رفتارهای سایبری غیرقانونی مرتبط‌اند. این عوامل در صورت فقدان مداخلات حمایتی، زمینه‌ساز تشدید بزهکاری در فضای مجازی خواهند بود.

٤-١-١-ویژگی‌های روان‌شناختی نوجوانان

نوجوانان در مرحله‌ای از زندگی قرار دارند که تغییرات جسمانی و روانی زیادی را تجربه می‌کنند؛ این تغییرات شامل افزایش هیجان‌پذیری، ضعف در کنترل رفتار و ناتوانی در تمایز کامل بین درست و نادرست است. در این دوره، کنجکاوی شدید و نیاز به اثبات خود، آن‌ها را مستعد رفتارهای پرخطر از جمله بزهکاری سایبری می‌کند. این ویژگی‌ها باعث می‌شود نوجوانان بیشتر در معرض تاثیرپذیری منفی از محیط‌های مجازی قرار گیرند.

٤-١-٢- ضعف آگاهی قانونی و اخلاقی

یکی از عوامل مهم و تأثیرگذار در بروز بزهکاری سایبری در میان نوجوانان، ضعف در آگاهی قانونی است. بسیاری از نوجوانان به‌طور دقیق از قوانین مرتبط با جرایم سایبری، از جمله قانون جرایم رایانه‌ای، حمایت از داده‌های شخصی، یا ممنوعیت دسترسی غیرمجاز به اطلاعات محرمانه، اطلاع ندارند. در نتیجه، ممکن است اقداماتی مانند ورود به حساب‌های کاربری دیگران، دستکاری در داده‌های رایانه‌ای، یا ارسال تهدیدهای آنلاین را «شوخی» یا «بازی» تلقی کرده و از ماهیت مجرمانه آن بی‌خبر باشند. این کمبود دانش حقوقی موجب می‌شود که درک نوجوان از مرز میان رفتار قانونی و غیرقانونی، مبهم و ناقص باشد، به‌ویژه در محیطی مانند فضای مجازی که حدود و قواعد آن برای بسیاری نامشخص است. نوجوانان به دلیل کمبود تجربه و ضعف در درک قوانین، آگاهی قانونی و اخلاقی کمتری دارند. آن‌ها ممکن است بدون اطلاع از پیامدهای رفتاری خود در فضای مجازی، مرتکب اعمال غیرقانونی شوند یا از روی تقلید، اقدام به جرایم سایبری کنند. این ضعف در شناخت حقوق و مسئولیت‌های قانونی، عامل مهمی در بروز بزهکاری‌های اینترنتی است. از سوی دیگر، ضعف در آگاهی اخلاقی نیز نقش تعیین‌کننده‌ای در شکل‌گیری رفتارهای آسیب‌زا در فضای سایبری دارد. نوجوانانی که در فرایند رشد خود آموزش‌های اخلاقی کافی دریافت نکرده‌اند یا فاقد الگوهای رفتاری سالم هستند، ممکن است برای جلب توجه، اعمال قدرت، یا پاسخ به احساسات سرکوب‌شده، به رفتارهایی چون قلدری سایبری، انتشار تصاویر خصوصی دیگران یا تهدید آنلاین روی آورند. فقدان آگاهی اخلاقی به این معناست که فرد به اصولی چون احترام به حریم خصوصی، کرامت انسانی، و مسئولیت‌پذیری اجتماعی پایبند نیست یا آن‌ها را در بستر مجازی جدی نمی‌گیرد. این امر به‌ویژه زمانی تشدید می‌شود که محیط مجازی به نوجوان این تصور را بدهد که

رفتار او پیامد مستقیم یا قابل رهگیری ندارد. در مجموع، پیوند میان ناآگاهی قانونی و اخلاقی، بستری مناسب برای شکل‌گیری بزهکاری سایبری در نوجوانان فراهم می‌کند. برای پیشگیری از این وضعیت، ضروری است آموزش‌های مستمر حقوقی و اخلاقی متناسب با سن، تجربه و سطح سواد دیجیتال نوجوانان در مدارس و خانواده‌ها اجرا شود تا آگاهی و مسئولیت‌پذیری آنان در مواجهه با فضای مجازی افزایش یابد.

٤-١-٣-هوش و توانمندی‌های فنی نوجوانان

برخلاف تصور عمومی، بزهکاران سایبری نوجوان غالباً دارای سطح بالایی از مهارت‌های فنی و اطلاعاتی در حوزه فناوری اطلاعات هستند. آن‌ها به علت تسلط بر فناوری‌های شبکه و کامپیوتر، توانایی انجام جرایم پیچیده سایبری را دارند. ابن امر نشان می‌دهد که پیشگیری صرفاً با تاکید بر آگاهی عمومی کافی نیست و باید مهارت‌های تخصصی آن‌ها نیز مورد توجه قرار گیرد. مطالعه‌ای در این خصوص صورت گرفته است که نشان می‌دهد که با گسترش استفاده نوجوانان از اینترنت و فناوری‌های دیجیتال، آگاهی آنان نسبت به خطرات فضای مجازی و انواع جرایم سایبری همچون هک، سرقت اطلاعات، کلاهبرداری اینترنتی و آزارهای آنلاین، از اهمیت ویژه‌ای برخوردار است. نتایج پژوهش حاکی از آن است که بسیاری از نوجوانان هنوز به‌طور کامل با مفهوم و دامنه جرایم سایبری آشنا نیستند و در نتیجه، آسیب‌پذیری آنها در برابر تهدیدات سایبری افزایش می‌یابد. علاوه بر این، یافته‌ها نشان می‌دهد که نوجوانانی که از آموزش‌های پیشگیرانه و آگاهی‌بخشی‌های هدفمند بهره‌مند شده‌اند، رفتارهای امن‌تری در فضای مجازی از خود نشان می‌دهند و کمتر در معرض خطرات سایبری قرار می‌گیرند. پژوهش تاکید دارد که خانواده‌ها، مدارس و نهادهای مرتبط باید به طور فعال در آموزش نوجوانان درباره امنیت سایبری، حقوق دیجیتال و نحوه مواجهه با تهدیدات مجازی نقش ایفا کنند تا نوجوانان بتوانند با مسئولیت‌پذیری بیشتر از فضای مجازی بهره‌مند شوند. از دیگر یافته‌های مهم این تحقیق، تاثیر منفی کمبود آگاهی سایبری در بروز رفتارهای پرخطر نوجوانان است که می‌تواند به وقوع جرایم سایبری منجر شود. به همین دلیل، پژوهشگران توصیه می‌کنند که برنامه‌های آموزشی و کمپین‌های اطلاع‌رسانی باید در سطح گسترده‌تر اجرا شوند تا فرهنگ استفاده ایمن از فناوری‌های دیجیتال در میان نوجوانان نهادینه شود و از آسیب‌های احتمالی پیشگیری شود .(Swamy, 2018)

٤-٢-تأثیر عوامل خانوادگی و آموزشی بر بزهکاری سایبری

عوامل خانوادگی و آموزشی نقش بسیار مؤثری در پیشگیری یا تشدید بزهکاری سایبری در نوجوانان دارند، چرا که خانواده نخستین نهاد اجتماعی‌سازی و آموزش و مدرسه نخستین محیط ساختارمند برای یادگیری هنجارها و ارزش‌هاست. در خانواده‌هایی که نظارت والدین ضعیف است، روابط عاطفی سرد یا تنش‌زا وجود دارد، و دسترسی نوجوان به فضای مجازی بدون کنترل و هدایت صورت می‌گیرد، احتمال ارتکاب به رفتارهای سایبری مجرمانه افزایش می‌یابد. از سوی دیگر، ناآگاهی والدین از تهدیدهای فضای مجازی یا بی‌توجهی به آموزش سواد رسانه‌ای، باعث می‌شود نوجوان بدون چارچوب و راهنمایی وارد این فضا شود. در بُعد آموزشی نیز، کمبود برنامه‌های آموزش حقوقی، اخلاقی و دیجیتال در مدارس، ضعف در تربیت شهروند دیجیتال مسئول و فقدان گفت‌وگوی انتقادی درباره خطرات و مسئولیت‌های استفاده از اینترنت، نوجوان را در برابر انحرافات سایبری آسیب‌پذیر می‌سازد؛ بنابراین، تعامل خانواده و نظام آموزشی در ایجاد محیطی آگاه، ایمن و پاسخگو برای نوجوانان، در پیشگیری از بزهکاری سایبری نقشی کلیدی دارد.

٤-۲-۱-نقش کم‌توجهی والدین و فقدان نظارت

یکی از مهم‌ترین عوامل خانوادگی مؤثر بر بزهکاری سایبری نوجوانان، کم‌توجهی والدین و فقدان نظارت مؤثر بر فعالیت‌های دیجیتال فرزندان است. در دوران نوجوانی که هویت‌سازی فرد شکل می‌گیرد و میل به استقلال افزایش می‌یابد، فقدان ارتباط مثبت و نظارت هوشمندانه از سوی والدین، نوجوان را در معرض خطرات مختلفی از جمله گرایش به فعالیت‌های غیرقانونی سایبری قرار می‌دهد. نوجوانانی که احساس می‌کنند خانواده نسبت به آنان بی‌تفاوت است یا درک و همراهی عاطفی کافی را از سوی والدین دریافت نمی‌کنند، بیشتر به سمت گروه‌های مجازی جایگزین کشیده می‌شوند؛ گروه‌هایی که ممکن است ارزش‌ها و الگوهای منحرف یا مجرمانه را تقویت کنند. مطالعات نشان می‌دهد بسیاری از نوجوانان در خانواده‌هایی رشد می‌کنند که والدین دانش کافی درباره فناوری و اینترنت ندارند یا به فعالیت‌های آنلاین فرزندانشان توجه چندانی ندارند. این کم‌توجهی موجب می‌شود نوجوانان بدون کنترل و آموزش صحیح در معرض خطرات فضای مجازی قرار گیرند .(Zhao, 2018) در نتیجه، فقدان نظارت خانواده یکی از مهم‌ترین عوامل افزایش بزهکاری سایبری در میان نوجوانان است. علاوه بر کم‌توجهی عاطفی، نظارت ضعیف والدین بر نحوه استفاده نوجوانان از اینترنت، شبکه‌های اجتماعی و ابزارهای دیجیتال زمینه را برای ارتکاب جرایم سایبری فراهم می‌سازد. فقدان قوانین خانگی مشخص در مورد زمان استفاده از اینترنت، محتوای مجاز و غیرمجاز، و عدم آگاهی والدین از فعالیت‌های آنلاین فرزندان، باعث می‌شود نوجوانان بدون درک پیامدهای حقوقی و اخلاقی، وارد رفتارهایی چون هک، نفوذ به حریم خصوصی دیگران، یا مشارکت در قلدری سایبری شوند. در بسیاری از موارد، والدین حتی از وجود چنین رفتارهایی بی‌خبرند تا زمانی که تبعات آن آشکار شود. از سوی دیگر، بی‌سوادی در فضای دیجیتال یا شکاف نسلی والدین در مواجهه با فناوری‌های نوین نیز مانعی جدی در برابر نظارت مؤثر است. بسیاری از والدین به دلیل ناآشنایی با ماهیت شبکه‌های اجتماعی، اپلیکیشن‌ها و شیوه‌های برقراری ارتباط مجازی، توانایی لازم برای درک خطرات یا راهنمایی نوجوانان را ندارند. در حالی که نظارت در فضای مجازی به معنای کنترل سخت‌گیرانه نیست، بلکه نیازمند رابطه‌ای بر پایه اعتماد، آموزش و گفت‌وگوی باز است. در نتیجه، می‌توان بیان نمود که نقش حمایتی، نظارتی و تربیتی والدین عاملی بنیادین در کاهش گرایش نوجوانان به بزهکاری سایبری است و هر گونه خلأ در این زمینه، زمینه‌ساز انحرافات رفتاری خواهد بود.

٤-۲-۲-مشکلات ساختار خانواده

ساختار نامتعادل خانواده، مانند فقدان یکی از والدین، وجود خشونت خانوادگی یا تربیت افراطی و سهل‌انگارانه، نقش مهمی در ایجاد بزهکاری سایبری نوجوانان دارد. این شرایط باعث بروز مشکلات روانی و اجتماعی در نوجوانان شده و آن‌ها را به سمت رفتارهای پرخطر و حتی مجرمانه سوق می‌دهد؛ (Ibid) چرا که ساختار خانواده، به عنوان نخستین نهاد تربیتی و اجتماعی‌ساز فرد، نقش کلیدی در شکل‌گیری شخصیت، ارزش‌ها و هویت نوجوان ایفا می‌کند. زمانی که این ساختار با مشکلاتی نظیر طلاق، جدایی عاطفی والدین، درگیری‌های مکرر خانوادگی، یا خانواده‌های تک‌والد مواجه باشد، نوجوانان در معرض فشارهای روانی و احساس ناامنی عاطفی قرار می‌گیرند. این وضعیت می‌تواند آنان را به جست‌وجوی پناهگاهی در فضای مجازی سوق دهد؛ فضایی که در آن ممکن است با گروه‌های منحرف، چالش‌های خطرناک، یا رفتارهای غیرقانونی روبرو شوند. در چنین شرایطی، نوجوان به جای دریافت الگوهای رفتاری سالم از خانواده، ممکن است دچار سردرگمی ارزشی شده و آسیب‌پذیری او نسبت به بزهکاری افزایش یابد. از سوی دیگر،

خانواده‌هایی که ساختار اقتدار و مرزهای رفتاری مشخصی ندارند، یعنی در آن‌ها قوانین تربیتی سست یا متضاد است، معمولاً موفق به اعمال نظارت مؤثر بر فرزندان خود نمی‌شوند. در این خانواده‌ها، ممکن است نوجوانان بدون راهنمایی درست، آزادی بی‌حد و مرز در استفاده از ابزارهای دیجیتال داشته باشند یا حتی احساس کنند برای جلب توجه، باید دست به اقدامات غیرعادی یا مجرمانه در فضای مجازی بزنند؛ همچنین در خانواده‌هایی که ارزش‌های اخلاقی، مسئولیت‌پذیری و آموزش‌های حقوقی نادیده گرفته می‌شود، نوجوانان درک روشنی از تبعات رفتاری خود نخواهند داشت؛ بنابراین، اختلال در ساختار خانواده می‌تواند به‌طور مستقیم یا غیرمستقیم، یکی از زمینه‌سازان اصلی بزهکاری سایبری نوجوانان باشد.

٤-۲-۳- ناکارآمدی نظام آموزشی در پیشگیری

نظام آموزشی غالباً بر آموزش‌های نظری و تمرکز بر نمرات تحصیلی استوار است و به مسائل تربیتی، روان‌شناسی و اخلاقی به اندازه کافی پرداخته نمی‌شود. عدم ارائه آموزش‌های تخصصی درباره خطرات فضای سایبری و ضعف در حمایت روانی از دانش‌آموزان، زمینه‌ساز افزایش آسیب‌پذیری آن‌ها در برابر جرایم سایبری است. به‌علاوه، وجود تبعیض و محرومیت در محیط‌های آموزشی می‌تواند نوجوانان را به رفتارهای پرخطر سوق دهد. نظام آموزشی به‌عنوان یکی از مهم‌ترین نهادهای اجتماعی، نقش محوری در آموزش مهارت‌های زندگی، آگاهی حقوقی و اخلاقی، و تربیت شهروندی دیجیتال دارد. با این حال، در بسیاری از کشورها، نظام آموزشی هنوز نتوانسته به‌طور مؤثر با چالش‌های فضای مجازی و جرایم سایبری نوجوانان مقابله کند. کمبود برنامه‌های آموزشی تخصصی و هدفمند درباره استفاده ایمن و مسئولانه از فناوری‌های دیجیتال، ضعف در آموزش سواد رسانه‌ای و قانونی و عدم تأکید کافی بر خطرات و پیامدهای بزهکاری سایبری باعث می‌شود نوجوانان بدون آمادگی لازم وارد فضای مجازی شوند. این خلأ آموزشی، نوجوانان را در برابر وسوسه‌های دیجیتال آسیب‌پذیر کرده و نقش پیشگیری آموزش را تضعیف می‌کند. علاوه بر این، نظام آموزشی گاه در ارائه مهارت‌های اجتماعی و هیجانی مرتبط با خودکنترلی، همدلی و مدیریت تعارض به نوجوانان کوتاهی می‌کند؛ مهارت‌هایی که در مقابله با انگیزه‌های بزهکارانه سایبری از اهمیت ویژه‌ای برخوردارند. فقدان فرصت‌های کافی برای بحث و تبادل نظر درباره مسائل اخلاقی و حقوقی فضای مجازی در محیط مدرسه، نوجوانان را درکافی بودن اطلاعات و دانش لازم برای اتخاذ رفتارهای سالم در فضای سایبری دچار سردرگمی می‌کند؛ همچنین ضعف همکاری میان مدارس، خانواده‌ها و نهادهای تخصصی، منجر به فقدان هماهنگی و پیگیری مستمر برنامه‌های پیشگیری می‌شود. به همین دلیل، ناکارآمدی نظام آموزشی در فراهم کردن بسترهای مناسب پیشگیری، یکی از موانع مهم در کاهش بزهکاری سایبری در میان نوجوانان است که نیازمند اصلاحات و توجه ویژه می‌باشد. در ایران، با توجه به اهمیت روزافزون فضای مجازی و افزایش جرایم رایانه‌ای، نظام آموزشی و مدارس نقش کلیدی در آشنایی نوجوانان با قوانین مرتبط با جرایم سایبری ایفا می‌کنند. قانون جرایم رایانه‌ای ایران (مصوب ۱۳۸۸)، چارچوب حقوقی مهمی برای مقابله با تخلفات فضای مجازی فراهم آورده است؛ اما آگاهی عمومی و به‌ویژه آگاهی نوجوانان و کاربران جوان از این قوانین، هنوز به حد کافی نیست. مدارس به عنوان اولین نهاد رسمی آموزش و پرورش، مسئولیت آموزش حقوق دیجیتال، قوانین مربوط به استفاده از فناوری اطلاعات، و پیامدهای حقوقی تخلفات اینترنتی را بر عهده دارند تا دانش‌آموزان با آگاهی کامل از حدود و مسئولیت‌های قانونی خود، در فضای مجازی فعالیت کنند. برگزاری کلاس‌های

سواد رسانه‌ای، حقوق فناوری اطلاعات و آموزش‌های تخصصی درباره امنیت سایبری و قوانین جرایم رایانه‌ای در مدارس می‌تواند نقش پیشگیرانه مهمی داشته باشد. این آموزش‌ها علاوه بر افزایش دانش حقوقی، به شکل‌گیری نگرش مسئولانه و اخلاقی نسبت به استفاده از فضای مجازی کمک می‌کند و نوجوانان را از گرفتار شدن در دام رفتارهای مجرمانه یا خطرناک سایبری محافظت می‌کند. در این راستا، فقدان برنامه‌های مدون و کارآمد آموزشی در مدارس و ضعف ارتباط بین آموزش‌های قانونی و واقعیت‌های فضای مجازی، موجب شده است که نوجوانان به‌صورت تجربی و بدون شناخت کامل قوانین، با خطرات این حوزه مواجه شوند؛ بنابراین، تقویت جایگاه نظام آموزشی در انتقال دانش قانونی و افزایش فرهنگ حقوقی در میان دانش‌آموزان، یک ضرورت اساسی در پیشگیری از بزهکاری سایبری است.

٤-۳- نقش عوامل حقوقی و محیطی در کنترل بزهکاری سایبری نوجوانان

نقش عوامل حقوقی در کنترل بزهکاری سایبری نوجوانان از طریق تدوین و اجرای قوانین بازدارنده، آموزش حقوقی و ایجاد پاسخ‌های کیفری متناسب تحقق می‌یابد. قوانین مرتبط با جرایم رایانه‌ای، نظیر قانون جرایم رایانه‌ای مصوب ۱۳۸۸ در ایران در صورتی می‌توانند در کاهش بزهکاری سایبری نوجوانان مؤثر باشند که هم از نظر ماهوی روشن و متناسب با تحولات فناوری باشند، و هم از نظر اجرایی با سیستم‌های پیشگیری و حمایت نوجوانان هم‌افزا عمل کنند. به‌ویژه قوانین باید میان مسئولیت کیفری نوجوانان و سیاست‌های تربیتی و بازپرورانه توازن برقرار کنند. علاوه بر آن، آموزش حقوقی در مدارس، تولید محتواهای قابل‌فهم برای نوجوانان، و آشنایی با تبعات قانونی رفتارهای پرخطر در فضای مجازی، می‌تواند نقش پیشگیرانه بسیار مهمی ایفا کند. در کنار عوامل حقوقی، محیط اجتماعی نوجوانان نیز تأثیر عمده‌ای در پیشگیری یا تقویت گرایش به بزهکاری سایبری دارد. فضای خانواده، مدرسه، همسالان و حتی جامعه مجازی (شبکه‌های اجتماعی) می‌توانند محیط‌هایی امن و تربیتی یا برعکس، بسترهای خطرآفرین برای ارتکاب بزه باشند. نظارت والدین، گفت‌وگوی باز با نوجوانان درباره تجربه‌های آنلاین، ارتباط مؤثر معلمان و مشاوران مدرسه با دانش‌آموزان، و ایجاد هویت مثبت دیجیتال در نوجوان، از جمله عناصر محیطی مؤثر در کاهش تمایل به رفتارهای مجرمانه سایبری است؛ همچنین تقویت زیرساخت‌های نظارتی و فیلترینگ هوشمند، در کنار آموزش تعاملی، می‌تواند شرایط محیطی را به‌گونه‌ای شکل دهد که نوجوانان هم دانش لازم را داشته باشند و هم در یک محیط ایمن‌تر رشد کنند. به این ترتیب، تلفیق عوامل حقوقی و محیطی، شرط اساسی در کنترل پایدار و اثربخش بزهکاری سایبری در میان نوجوانان است.

٤-۳-۱-نواقص قانونی در مواجهه با بزهکاری سایبری

قوانین موجود در بسیاری از کشورها، فاقد مقررات ویژه برای مقابله با بزهکاری سایبری نوجوانان هستند. قانون مجازات فعلی در حوزه جرایم سایبری، عمدتاً برای مجرمان بالغ تدوین شده و سطح مجازات‌ها نیز متناسب با آثار زیانبار این جرایم نیست. این خلأ قانونی باعث شده است که نوجوانان کمتر تحت پیگرد قرار گرفته و در نتیجه جرایم آن‌ها به شکل جدی کنترل نشود. در نظام حقوقی ایران، اگرچه قانون جرایم رایانه‌ای مصوب ۱۳۸۸ و قانون مجازات اسلامی مصوب ۱۳۹۲ ابزارهای قانونی مهمی برای مقابله با جرایم سایبری فراهم کرده‌اند، اما نواقص قابل‌توجهی در زمینه مواجهه با بزهکاری سایبری نوجوانان مشاهده می‌شود. یکی از مهم‌ترین این نواقص، فقدان مقررات خاص و مجزای ناظر بر رفتار مجرمانه نوجوانان در فضای مجازی است. قانون جرایم رایانه‌ای بیشتر ناظر بر کلیات جرم‌انگاری در بستر فضای دیجیتال است و توجهی به سن، انگیزه، یا وضعیت رشد روانی و اجتماعی نوجوانان ندارد؛ حال آنکه این گروه

سنی نیازمند برخورد متمایز با رویکرد تربیتی و بازپرورانه هستند. از سوی دیگر، قانون مجازات اسلامی در ماده ۸۸ تا ۹۵ درباره اطفال و نوجوانان مقرراتی دارد، اما این مقررات کلی‌اند و در خصوص جرایم نوپدید، از جمله بزهکاری در فضای مجازی، به‌روشنی قابل تطبیق نیستند. برای مثال، در جرایمی مانند هک، نشر محتوای غیراخلاقی یا کلاهبرداری اینترنتی که توسط نوجوانان انجام می‌شود، قضات با فقدان معیارهای تخصصی برای ارزیابی میزان مسئولیت کیفری، نقش تربیتی محیط مجازی، یا شدت تأثیر همسالان و الگوبرداری از شبکه‌ها مواجه‌اند؛ همچنین نظام قانونی ایران فاقد نهادهای تخصصی چون «دادگاه‌های سایبری ویژه نوجوانان» یا برنامه‌های بازپرورانه در فضای دیجیتال است. در مجموع، هرچند قوانین موجود ظرفیت‌های ابتدایی برای برخورد با جرایم رایانه‌ای دارند، اما برای پاسخ‌گویی مؤثر به پدیده پیچیده و در حال تحول بزهکاری سایبری نوجوانان نیاز به اصلاحات ساختاری در قوانین، تدوین دستورالعمل‌های تخصصی برای دادرسی نوجوانان در فضای مجازی و ایجاد پیوند میان حقوق جزا، روان‌شناسی رشد و سیاست‌های پیشگیرانه احساس می‌شود.

٤-٣-٢- خلأهای قانونی در تعاریف و دامنه جرم

در قوانین جاری، دامنه تعاریف جرایم سایبری محدود بوده و بسیاری از جرایم مهم در حوزه‌های مختلف اقتصادی، سیاسی و اجتماعی به‌صورت کامل پوشش داده نشده‌اند. همچنین قانون تأکید زیادی بر قصد مجرمانه دارد و رفتارهای ناشی از سهل‌انگاری که می‌تواند آسیب جدی وارد کند، کمتر مورد توجه قرار گرفته است. این موضوع موجب عدم برخورد کامل با رفتارهای آسیب‌رسان در فضای سایبری شده است.

٤-٣-٣- محیط سایبری ناامن و ضعف نظارت

فضای مجازی به دلیل ماهیت باز، ناشناس بودن کاربران و کمبود نظارت موثر، بستری مناسب برای بروز بزهکاری نوجوانان است. فرهنگ‌های منفی و محتوای نامناسب در اینترنت به راحتی در دسترس نوجوانان قرار دارند و فقدان قانون‌گذاری دقیق و نظارت قوی، باعث تشویق رفتارهای مجرمانه در این گروه سنی می‌شود .(Zhao, 2018) این امر ضرورت تقویت نظارت دولتی و فرهنگی را برجسته می‌کند. محیط سایبری ناامن و ضعف نظارت دو عامل کلیدی در گسترش بزهکاری سایبری در میان نوجوانان به‌شمار می‌آیند. فضای مجازی، به‌ویژه در بستر شبکه‌های اجتماعی و پیام‌رسان‌ها، به‌دلیل ماهیت بی‌مرز، ناشناس و کنترل‌ناپذیر خود، بستری مساعد برای رفتارهای پرخطر یا مجرمانه فراهم می‌کند. نوجوانان، به‌دلیل کنجکاوی، هیجان‌طلبی و گاه ناآگاهی از پیامدهای قانونی و اخلاقی اعمالشان، در این فضا ممکن است به‌راحتی درگیر فعالیت‌های غیرمجاز مانند دسترسی غیرمجاز به داده‌ها، انتشار محتوای مستهجن، تهدید و آزار سایبری، یا مشارکت در چالش‌های مجرمانه شوند. از سوی دیگر، ضعف نظارت والدین، مدرسه و نهادهای رسمی بر فعالیت نوجوانان در فضای مجازی، عملاً نظارت پیشگیرانه را تضعیف کرده است. بسیاری از والدین یا ابزارهای لازم برای کنترل استفاده فرزندان از اینترنت را ندارند، یا آگاهی کافی از خطرات بالقوه این فضا ندارند. در سطح مدرسه نیز، آموزش رسمی و منسجمی برای آگاه‌سازی نوجوانان نسبت به حقوق دیجیتال، حریم خصوصی، و پیامدهای بزهکاری سایبری طراحی نشده است؛ همچنین، فقدان پلتفرم‌های ملی امن، عدم اجرای دقیق سیاست‌های فیلترینگ هوشمند، و عدم ایجاد هویت دیجیتال قابل‌پیگیری، باعث شده تا نوجوانان در محیطی فعالیت کنند که امکان شناسایی، هشدار، یا مداخله پیشگیرانه در آن بسیار محدود است. در چنین شرایطی، محیط سایبری برای نوجوان به فضایی پرریسک تبدیل می‌شود؛ جایی که می‌تواند هم به‌عنوان قربانی آسیب ببیند و هم به‌عنوان بزهکار به‌طور ناآگاهانه وارد مسیر مجرمانه

شود؛ بنابراین، راه‌حل در تقویت سیاست‌های نظارت هوشمند، آموزش مهارت‌های دیجیتال و ایجاد سامانه‌های حمایتی متناسب با نیازهای نوجوانان نهفته است.

۵-پیشگیری و کنترل بزهکاری سایبری نوجوانان

پیشگیری و کنترل بزهکاری سایبری نوجوانان از ابعاد اجتماعی، روان‌شناختی، حقوقی و امنیتی دارای اهمیت بالایی است، زیرا نوجوانان به‌عنوان قشر در حال رشد و شکل‌گیری هویت، بیش از سایر گروه‌ها در معرض تأثیرپذیری از فضای مجازی و آسیب‌های ناشی از آن قرار دارند. در بعد اجتماعی، ارتکاب جرایم سایبری توسط نوجوانان می‌تواند منجر به طرد از مدرسه، خانواده و جامعه شود. در بُعد روانی، تجربه شکست، شرم، و انگ اجتماعی ممکن است مسیر رشد سالم آنان را منحرف کند؛ همچنین، از منظر حقوقی و امنیتی، فقدان کنترل بر بزهکاری سایبری در این گروه سنی می‌تواند منجر به شکل‌گیری باندهای مجازی، افزایش جرایم سازمان‌یافته سایبری و چالش برای نهادهای انتظامی و قضایی شود. از این رو، سرمایه‌گذاری در سیاست‌های پیشگیرانه، آموزش حقوق دیجیتال، تقویت مهارت‌های روانی اجتماعی، و ایجاد سازوکارهای حمایتی، ضرورتی اساسی در مسیر تربیت شهروندان دیجیتال مسئول به‌شمار می‌رود.

۵-۱-نقش خانواده در پیشگیری از بزهکاری سایبری نوجوانان

۵-۱-۲-ضرورت توجه خانواده به آموزش فضای مجازی برای فرزندان

خانواده‌ها باید با همکاری مدارس و جامعه نظارت دقیق‌تری بر نحوه استفاده نوجوانان از اینترنت داشته باشند. ایجاد محیطی گرم، سالم و همراه با حمایت عاطفی در خانواده، می‌تواند شخصیت سالم و متعادلی را در نوجوانان پرورش دهد که به دنبال تحریک‌های ناسالم در فضای مجازی نباشند. این حمایت باعث کاهش تمایل نوجوانان به ورود به فعالیت‌های مجرمانه در فضای سایبری می‌شود.

۵-۱-۲-ارتقای دانش والدین در زمینه فناوری اطلاعات

با گسترش اینترنت، والدین نیز باید دانش و مهارت‌های لازم در زمینه فناوری اطلاعات را کسب کنند تا بتوانند همگام با فرزندان خود حرکت کرده و فاصله نسلی را کاهش دهند. آگاهی والدین از فضای مجازی، به آنان کمک می‌کند تا نظارت و راهنمایی مؤثرتری نسبت به فرزندان داشته باشند.

۵-۱-۳- تغییر نگرش و سبک تربیتی والدین

والدین باید رویکرد خود را نسبت به اینترنت و استفاده فرزندان از آن اصلاح کنند و به جای ممنوعیت مطلق، با نوجوانان خود گفت‌وگو و تعامل دوستانه داشته باشند. شناخت درست ویژگی‌های روانی نوجوانان و ایجاد فضای گفتگو و اعتماد، می‌تواند مانع از بروز رفتارهای ضد اجتماعی و بزهکاری در فضای سایبری شود.

۵-۲- تقویت آموزش و مدیریت مدارس در کاهش بزهکاری سایبری

۵-۲-۱- گسترش آموزش‌های ارزشی و روانشناسی

مدارس باید آموزش‌های مربوط به جهان‌بینی صحیح، اخلاق و ارزش‌های انسانی را تقویت کنند و آموزش‌های حقوقی و فرهنگی فضای مجازی را به صورت منظم در برنامه‌های خود بگنجانند. ارائه مشاوره روانشناسی به صورت منظم نیز می‌تواند سلامت روانی دانش‌آموزان را بهبود بخشد.

۵-۲-۲-تأکید بر آموزش امنیت سایبری در کلاس‌های کامپیوتر

تدریس تخصصی مباحث امنیت شبکه و قانون‌مداری در مدارس می‌تواند آگاهی دانش‌آموزان را نسبت به اهمیت حفظ امنیت اطلاعات و رعایت قوانین فضای سایبری افزایش دهد و آنان را نسبت به عواقب اقدامات مجرمانه هشدار دهد.

۵-۲-۳-بهبود فضای آموزشی و مدیریت مدرسه

ایجاد برنامه‌های فوق‌برنامه متنوع و تشویق دانش‌آموزان به مشارکت در فعالیت‌های هنری، ورزشی و اجتماعی به کاهش وابستگی آنان به اینترنت کمک می‌کند. همچنین، تغییر نگرش مدیریت مدارس به سمت رویکردهای باز و انعطاف‌پذیر و تقویت تیم آموزشی با تمرکز بر آموزش اخلاق و فضای مجازی، محیطی سالم‌تر برای دانش‌آموزان فراهم می‌کند.

۵-۳-نقش دولت و جامعه در بهبود قوانین و مدیریت فضای سایبری

نقش دولت و جامعه در بهبود قوانین و مدیریت فضای سایبری از ابعاد حقوقی، فرهنگی، آموزشی و فناورانه اهمیت اساسی دارد، زیرا توسعه فضای مجازی بدون تنظیم‌گری مؤثر، زمینه‌ساز گسترش بزهکاری به‌ویژه در میان نوجوانان است. دولت با تدوین و به‌روزرسانی قوانین متناسب با تحولات فناوری، تقویت پاسخ‌گویی قضایی و ایجاد نهادهای نظارتی کارآمد، می‌تواند خلأهای قانونی موجود را پوشش دهد. در بُعد فرهنگی و آموزشی، دولت و جامعه باید از طریق رسانه‌ها، نهادهای آموزشی و خانواده‌ها در جهت نهادینه‌سازی فرهنگ استفاده مسئولانه از اینترنت گام بردارند. همچنین، حمایت از تولید ابزارها و پلتفرم‌های بومی امن، و فراهم‌سازی زیرساخت‌های فنی برای نظارت هوشمند و پیشگیری از جرایم سایبری، از دیگر مسئولیت‌های حیاتی دولت در مدیریت صحیح این فضا است. در نهایت، مشارکت جامعه مدنی، سازمان‌های مردم‌نهاد و نخبگان در گفتمان‌سازی، آگاه‌سازی عمومی و مطالبه‌گری برای شفافیت بیشتر در سیاست‌های سایبری، نقشی مکمل در این فرآیند ایفا می‌کند.

۵-۳-۱-توسعه قوانین و مقررات مربوط به جرایم سایبری نوجوانان

دولت باید قوانین مربوط به جرایم سایبری را گسترش دهد و تنبیهات متناسب با شدت جرایم و نقش نوجوانان را تعیین کند. به‌خصوص باید جرایم ناشی از سهل‌انگاری و نادیده گرفتن مسئولیت‌های امنیتی نیز مشمول مجازات شوند.

۵-۳-۲-نظارت دقیق‌تر و سرمایه‌گذاری در فناوری امنیت سایبری

مراجع ذی‌ربط باید بودجه‌های لازم برای ارتقای فناوری‌های امنیت سایبری را فراهم کرده و نظارت مستمر بر فعالیت‌های فضای مجازی و مراکز عمومی مانند کافی‌نت‌ها را افزایش دهند. به‌کارگیری فناوری‌های پیشرفته می‌تواند مانع از گسترش بزهکاری‌های اینترنتی شود.

۵-۳-۳-پاک‌سازی محیط سایبری و ارتقای فرهنگ استفاده صحیح از اینترنت

مسئولان باید با استفاده از قدرت قانونی، محیط اینترنت را پاک‌سازی کنند و فرهنگ استفاده صحیح و اخلاقی از فضای مجازی را ترویج نمایند. ایجاد قوانین سختگیرانه برای مراکز خدمات اینترنتی و آموزش جامعه در زمینه اهمیت امنیت سایبری، به کاهش جرایم در این حوزه کمک می‌کند.

٦-عوامل مؤثر در پیشگیری از جرایم سایبری علیه نوجوانان

٦-١-آموزش و آگاهی‌رسانی به‌عنوان ابزارهای کلیدی پیشگیری

٦-١-١-نقش آموزش در افزایش آگاهی نوجوانان

یکی از مؤثرترین راهکارها برای مقابله با جرایم سایبری علیه نوجوانان، آموزش هدفمند و سیستماتیک در زمینه امنیت سایبری است. آموزش‌های مستمر در مدارس می‌توانند سطح دانش نوجوانان درباره تهدیدات آنلاین، نظیر فیشینگ، بدافزارها و سوءاستفاده‌های هویتی را افزایش دهند. مطالعات نشان می‌دهند که آموزش‌های تعاملی در محیط مدرسه به بهبود رفتارهای پیشگیرانه در نوجوانان کمک می‌کنند Lapuh Bele, Dimc, Rozman, & Sladoje Jemec, (2014).

٦-١-٢- اهمیت مشارکت والدین و معلمان در فرآیند آموزشی

پیشگیری مؤثر از جرایم سایبری مستلزم مشارکت فعال والدین و معلمان در فرآیند آموزش است. زمانی که خانواده‌ها از تهدیدات آنلاین آگاهی کافی داشته باشند، می‌توانند نظارت مؤثرتری بر فعالیت‌های اینترنتی فرزندان خود داشته باشند. هم‌چنین، معلمان به‌عنوان افراد تأثیرگذار در محیط‌های آموزشی می‌توانند با ارائه آموزش‌های مناسب، نقش مهمی در انتقال دانش امنیت سایبری ایفا کنند .(CFISA, 2018)

٦-١-٣-استفاده از فناوری‌های نوین در آموزش

استفاده از فناوری‌های نوین مانند بازی‌سازی آموزشی و واقعیت مجازی، جذابیت آموزش مفاهیم امنیت سایبری را برای نوجوانان افزایش داده و باعث مشارکت فعال‌تر آنان می‌شود. پژوهش‌ها نشان داده‌اند که بهره‌گیری از محیط‌های تعاملی، موجب ارتقاء توانایی تحلیل خطرات سایبری توسط نوجوانان شده و آن‌ها را به تصمیم‌گیری صحیح در فضای آنلاین ترغیب می‌کند .(Scholefield & Shepherd, 2019)

٦-٢-توسعه مهارت‌های فردی و اجتماعی برای مقابله با تهدیدات سایبری

٦-٢-١-تقویت مهارت‌های تفکر انتقادی و تصمیم‌گیری

توانایی تفکر انتقادی و تحلیل موقعیت از جمله مهارت‌هایی هستند که نوجوانان را قادر می‌سازند تهدیدات سایبری را شناسایی کرده و واکنش مناسبی نشان دهند. نوجوانانی که این مهارت‌ها را در مدرسه یا خانواده کسب کرده‌اند، در مواجهه با موقعیت‌هایی مانند درخواست ارسال اطلاعات شخصی یا کلیک بر روی پیوندهای مشکوک، تصمیم‌های مسئولانه‌تری می‌گیرند.(GeeksforGeeks, 2025)

٦-٢-٢-ارتقاء مهارت‌های ارتباطی و اجتماعی

مهارت‌های اجتماعی قوی مانند توانایی نه گفتن، اعتماد به نفس، و مدیریت روابط، می‌توانند نوجوانان را در برابر سوءاستفاده‌های آنلاین مقاوم‌تر کنند. تحقیقات حاکی از آن است که قربانیان بسیاری از جرایم سایبری، فاقد مهارت‌های ارتباطی مؤثر بوده‌اند و از این رو، آموزش این مهارت‌ها به‌عنوان سپری در برابر تهدیدات مجازی تلقی می‌شود .(Schilder, 2015)

٦-۲-۳- ترویج رفتارهای مسئولانه در فضای مجازی

تربیت نوجوانانی که نسبت به رفتار خود در فضای مجازی مسئولیت‌پذیر هستند، می‌تواند سطح جرایم سایبری را به شکل قابل‌توجهی کاهش دهد. آموزش در مورد رعایت حریم خصوصی دیگران، اخلاق ارتباطی در شبکه‌های اجتماعی، و احترام به قوانین کپی‌رایت باید از سنین پایین آغاز شود .(Terranova Security, 2023)

٦-۳- نقش سیاست‌ها و برنامه‌های دولتی در پیشگیری از جرایم سایبری

٦-۳-۱-تدوین و اجرای سیاست‌های جامع امنیت سایبری

حمایت ساختاری دولت‌ها از امنیت سایبری در قالب سیاست‌گذاری‌های کلان می‌تواند چارچوبی منسجم برای آموزش، پیشگیری و مقابله با جرایم سایبری علیه نوجوانان فراهم آورد. این سیاست‌ها باید با محوریت نهادهای آموزشی، قضایی و ارتباطی تنظیم شوند.

٦-۳-۲- حمایت از برنامه‌های پیشگیری و مداخله زودهنگام

برنامه‌هایی مانند «سفیران سایبری» در مدارس که نوجوانان را به‌عنوان عوامل آگاه‌کننده و پشتیبان همسالان خود آموزش می‌دهند، نمونه‌هایی موفق از مداخله زودهنگام به شمار می‌روند. این ابتکارات می‌توانند فرهنگ پیشگیری را در مدارس نهادینه سازند .(Wired, 2022)

٦-۳-۳-همکاری بین‌المللی برای مقابله با تهدیدات فرامرزی

ماهیت فرامرزی جرایم سایبری، نیازمند همکاری میان‌دولتی برای تبادل اطلاعات، اجرای قوانین هماهنگ و پیگیری حقوقی مجرمان است. سازمان ملل و نهادهای بین‌المللی دیگر نقش حیاتی در این هماهنگی جهانی دارند (UNODC, n.d.) .

نتیجه گیری

فرایند هویت‌یابی نوجوانان در فضای سایبری پدیده‌ای پیچیده و چندوجهی است که از تجربه‌های مثبت مانند یادگیری آنلاین، توسعه مهارت‌های دیجیتال، و تعاملات خلاقانه آغاز شده و در صورت فقدان نظارت، آموزش و حمایت روانی و حقوقی مناسب، ممکن است به انحراف و ارتکاب بزهکاری سایبری منتهی شود. نوجوانان در این فضا همزمان نقش یادگیرنده، تجربه‌گر، و در برخی موارد بزه‌دیده یا بزهکار را ایفا می‌کنند. در شرایطی که ساختار خانواده با چالش‌هایی نظیر فقدان نظارت و ناتوانی در آموزش سواد دیجیتال مواجه است، و نظام آموزشی نیز قادر به پاسخ‌گویی به تحولات فناورانه نیست، احتمال لغزش نوجوانان در مسیر رفتارهای پرخطر و مجرمانه سایبری افزایش می‌یابد. عواملی چون ضعف کنترل نفس، فشار گروه همسالان، احساس گمنامی، و ناتوانی در درک پیامدهای اجتماعی و قانونی رفتارهای آنلاین، از جمله زمینه‌هایی است که گذار از هویت یادگیرنده به هویت متخلف را تسهیل می‌کند؛ همچنین، ناهماهنگی بین آگاهی قانونی و درک اخلاقی نوجوانان، به‌ویژه در فقدان آموزش رسمی، یکی از خلأهای جدی در پیشگیری از بزهکاری است؛ بنابراین، مقابله با این پدیده نیازمند سیاست‌گذاری چندسطحی است: اصلاح و تکمیل قوانین سایبری، آموزش تعاملی در مدارس، ارتقاء سطح آگاهی والدین، و فراهم کردن زیرساخت‌های نظارتی و حمایتی مؤثر توسط دولت. تنها با پذیرش مسئولیت مشترک خانواده، مدرسه، دولت و جامعه مدنی می‌توان به ساخت جامعه‌ای امن‌تر، آگاه‌تر و مسئول‌تر در فضای دیجیتال دست یافت. افزون بر این، بررسی پیوند میان هویت‌یابی دیجیتال و بزهکاری سایبری نوجوانان نشان می‌دهد که فضای مجازی نه‌تنها بستری برای رشد و خودبیانگری آنان فراهم کرده، بلکه با ایجاد

فرصت‌هایی برای تجربه نقش‌های جدید، از جمله نقش بزهکار یا قربانی، مرزهای رفتاری آنان را نیز تغییر داده است. در محیطی که هنجارهای اجتماعی به‌وضوح تعریف نشده‌اند و پیامدهای اعمال به‌صورت آنی و ملموس درک نمی‌شود، نوجوانان بیشتر در معرض تجربه کنش‌های پرخطر و قانون‌گریز قرار می‌گیرند. در این میان، همپوشانی نقش بزه‌دیده و بزهکار و انتقال از تجربه قربانی‌شدن به انجام رفتارهای تلافی‌جویانه، یکی از مسیرهای رایج در بروز بزهکاری سایبری نوجوانان است که نشان‌دهنده پیچیدگی‌های روانی و اجتماعی این پدیده است. در نهایت، باید تأکید کرد که برنامه‌های پیشگیرانه و سیاست‌های حمایتی، تنها زمانی مؤثر خواهند بود که با شناخت دقیق از نیازها، ویژگی‌های رشدی، و زمینه‌های روانی-اجتماعی نوجوانان طراحی شوند. آموزش حقوق دیجیتال، سواد رسانه‌ای، مهارت‌های تنظیم هیجان و کنترل خشم، و تقویت هویت مثبت در فضای آنلاین، از جمله رویکردهایی هستند که می‌توانند احتمال ورود نوجوانان به مسیر بزهکاری سایبری را کاهش دهند. همچنین، توسعه نهادهای حمایتی برای گزارش‌دهی، مشاوره روانی، و بازپروری نوجوانان متخلف، از ضرورت‌های انکارناپذیر یک سیاست کیفری مؤثر و انسانی در مواجهه با این پدیده نوپدید است. در نتیجه، پیشگیری از بزهکاری سایبری در گروی یک نگاه جامع، میان‌رشته‌ای و آینده‌نگر است که تمامی ابعاد روانی، اجتماعی، فرهنگی و قانونی را دربر بگیرد. در پایان این پژوهش، چند پیشنهاد کاربردی و مبتنی بر تحلیل‌های صورت‌گرفته برای پیشگیری و کنترل بزهکاری سایبری نوجوانان ارائه می‌شود:

۱) گنجاندن آموزش حقوق سایبری در برنامه درسی مدارس: لازم است آموزش‌های رسمی در زمینه حقوق دیجیتال، مسئولیت‌های قانونی، سواد رسانه‌ای، و مهارت‌های مقابله با خطرات فضای مجازی از مقاطع پایه وارد نظام آموزشی شود.

۲) برگزاری کارگاه‌های آموزشی برای والدین و معلمان: توانمندسازی والدین و کادر آموزشی در شناسایی رفتارهای پرخطر دیجیتال و ایجاد ارتباط مؤثر با نوجوانان می‌تواند نقش مهمی در پیشگیری ایفا کند.

۳) توسعه سامانه‌های نظارتی و حمایتی آنلاین: ایجاد پلتفرم‌هایی برای گزارش‌گیری محرمانه از قربانیان، ارائه مشاوره رایگان، و مداخله سریع در رفتارهای پرخطر نوجوانان اهمیت زیادی دارد.

۴) اصلاح و تکمیل قوانین جرایم رایانه‌ای با تأکید بر نوجوانان: پیشنهاد می‌شود قوانین مربوط به بزهکاری سایبری، با در نظر گرفتن ویژگی‌های سنی، روانی و تربیتی نوجوانان بازنگری شده و مقررات حمایتی برای بازپروری آنان تدوین گردد.

۵) ترویج الگوهای هویتی مثبت در فضای مجازی: باید از طریق رسانه‌ها و شبکه‌های اجتماعی می‌توان با معرفی الگوهای موفق نوجوانانه در حوزه‌های علمی، فرهنگی و اجتماعی، الگوسازی مؤثری برای استفاده مثبت از اینترنت انجام داد.

۶) همکاری بین‌نهادی و بین‌المللی: مقابله با بزهکاری سایبری نوجوانان نیازمند همکاری میان نهادهای آموزشی، قضایی، فناوری، روان‌شناسی، و نهادهای بین‌المللی در جهت تبادل اطلاعات و طراحی راهکارهای هماهنگ است.

منابع و مآخذ

1) Akers, R. L. (2017). Social learning and social structure: A general theory of crime and deviance. Routledge.

2) Alsmadi, I., & Zarour, M. (2017). Cybercrime and Cybersecurity Awareness: An Empirical Study. International Journal of Computer Science and Network Security, 17(8), 56-63.
3) Bandura, A. (1977). Social Learning Theory. Englewood Cliffs, NJ: Prentice-Hall. From: https://openlibrary.org/works/OL15804604W/Social_learning_theory
4) Berenblum, T, Cohen, N., & Perry, S. (2019). The role of legal knowledge in cybercrime: A comparative study. Journal of Cybersecurity, 5(1). https://doi.org/10.1093/cybsec/tyz005
5) Bossler, A. M., & Holt, T. J. (2010). The effect of self-control on deviant peer association and high-tech offending. Journal of Criminal Justice, 38(3), 347–355. https://doi.org/10.1016/j.jcrimjus.2010.03.001
6) Brenner, S. W. (2010). Cybercrime: Criminal threats from cyberspace (2nd ed.). Praeger.
7) Caneppele, S., & Aebi, M. F. (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. Policing: A Journal of Policy and Practice, 13(1), 66–79. https://doi.org/10.1093/police/pax055
8) Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet (3rd ed.). Academic Press.
9) CFISA. (2018). How to improve cybersecurity awareness in educational institutions. https://cfisa.com/how-to-improve-cybersecurity-awareness-in-educational-institutions/
10) Chng, G. S., Li, D., Liau, A. K., & Khoo, A. (2022). Motives and pathways of cyber offending among adolescents. Youth & Society, 54(1), 67–89. https://doi.org/10.1177/0044118X20977303
11) CISA. (n.d.). Cybersecurity awareness program. https://www.cisa.gov/resources-tools/programs/cisa-cybersecurity-awareness-program
12) Clarke, R. A., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. Ecco.
13) GeeksforGeeks. (2025). Cybercrime causes and measures to prevent them. https://www.geeksforgeeks.org/cybercrime-causes-and-measures-to-prevent-it/
14) Grabosky, P. (2007). Electronic Crime. Routledge.
15) Holt, T. J., Bossler, A. M., & May, D. C. (2017). Predicting the likelihood of cybercrime victimization and offending among adolescents. Youth & Society, 49(7), 814–837. https://doi.org/10.1177/0044118X14599485
16) Holt, T. J., Burruss, G. W., & Bossler, A. M. (2012). Social learning and cyber-deviance: Examining the importance of a full social learning model in the virtual world. Journal of Crime and Justice, 35(1), 31–61.
17) Interpol. (2013). Cybercrime: The challenge of tomorrow. Retrieved from https://www.interpol.int/en/Crimes/Cybercrime
18) Kerstens, J., & Jansen, J. (2016). Cyber victimization and online deviant behavior among adolescents. Computers in Human Behavior, 57, 247–255. https://doi.org/10.1016/j.chb.2015.12.035
19) Lapuh Bele, J. Dimc, M., Rozman, D, & Sladoje Jemec, A. (2014). Raising awareness of cybercrime - The use of education as a means of prevention and protection. ERIC. https://files.eric.ed.gov/fulltext/ED557216.pdf
20) Livingstone, S., Haddon, L., Görzig, A., & Ólafsson, K. (2011). Risks and safety on the internet: The perspective of European children. London: LSE, EU Kids Online. Retrieved from https://eprints.lse.ac.uk/33731/

21) Maras, P., Sweiry, E., Villadsen, A., & Fitzsimons, E. (2024). Exploring adolescents' involvement in cybercrime: Evidence from the Millennium Cohort Study. Centre for Longitudinal Studies, UCL. https://cls.ucl.ac.uk/wp-content/uploads/2024/01/Cybercrime-MCS-briefing-2024.pdf
22) Mitnick, K. D., & Simon, W. L. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.
23) Morris, R. G., & Blackburn, A. G. (2009). The role of social bonding and control variables in explaining cybercrime among adolescents. Criminal Justice Review, 34(1), 22–45.
24) National Crime Agency. (2017). Cyber Choices: Helping people make informed choices and use their cyber skills positively. https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyber-choices
25) National Crime Agency. (2017). Cyber Choices: Preventing young people from becoming cyber criminals. Retrieved from https://nationalcrimeagency.gov.uk
26) Nodeland, B. (2020). Personality traits and cybercrime: A meta-analytic review. International Journal of Cyber Criminology, 14(2), 519–538. https://doi.org/10.5281/zenodo.4057695
27) Office for National Statistics. (2023, April 27). Crime in England and Wales: year ending December 2022. From: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdecember2022
28) Parti, K., Molnár, E., & Neumann, E. (2022). Online deviance and digital socialization: A developmental criminology perspective. Crime, Law and Social Change, 78(4), 365–382. https://doi.org/10.1007/s10611-021-10006-2
29) Patchin, J. W., & Hinduja, S. (2010). Cyberbullying and self-esteem. Journal of School Health, 80(12), 614–621. https://doi.org/10.1111/j.1746-1561.2010.00540.x
30) Schilder, J. D. (2015). Cyber-crimes against adolescents: Bridges between a psychological and a design approach. ResearchGate. https://www.researchgate.net/publication/273123979
31) Scholefield, S., & Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness. arXiv. https://arxiv.org/abs/1903.08454
32) Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college students. Journal of Research in Crime and Delinquency, 34(4), 495–518.
33) Smith, R. G. (2007). Identity theft and fraud: The legal issues. Journal of Law and Policy, 19, 79-101.
34) Suler, J. (2004). The online disinhibition effect. CyberPsychology & Behavior, 7(3), 321–326. https://doi.org/10.1089/1094931041291295
35) Swamy, D. (2018). Awareness of cyber crime among teenagers. Recent Scientific. Retrieved from https://recentscientific.com/awareness-cyber-crime-among-teenagers
36) Symantec. (2019). Internet Security Threat Report. Symantec Corporation.
37) Terranova Security. (2023). The importance of cyber security awareness in education. https://www.terranovasecurity.com/blog/cyber-security-awareness-in-education
38) UNICEF. (2017). The State of the World's Children 2017: Children in a Digital World. Retrieved from https://www.unicef.org/reports/state-worlds-children-2017
39) UNODC. (n.d.). Cybercrime Module 5: Key issues. https://www.unodc.org/e4j/zh/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html
40) van der Wagen, W., Leukfeldt, E. R., & Stol, W. P. (2021). Awareness, attitude, and behavior: Cyber security education in practice. Computers & Security, 105, 102228.

41) Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity.
42) Weulen Kranenbarg, M., Holt, T. J., & Leukfeldt, E. R. (2019). Offenders and victims in the digital age. European Journal of Criminology, 16(3), 307–328. https://doi.org/10.1177/1477370818773613
43) Weulen Kranenbarg, M., Holt, T. J., & Leukfeldt, R. (2022). Examining cyber offending among computer science students in the Netherlands. Deviant Behavior, 43(8), 967–984. https://doi.org/10.1080/01639625.2020.1816965
44) Wikipedia contributors. (2024, May 31). Cybercrime. In Wikipedia, The Free Encyclopedia. Retrieved from https://en.wikipedia.org/wiki/Cybercrime
45) Wired. (2022). In the fight against scams, 'Cyber Ambassadors' enter the chat. https://www.wired.com/story/cyber-ambassadors-india
46) Zhao, Y. (2018). Research on Juvenile Cybercrime. International Journal of Mathematics and Systems Science, 4(2), 186-194.https://systems.enpress-publisher.com/index.php/IJMSS/article/viewFile/2439/1617

Exploring Adolescent Identity in Cyberspace, from Online Learning to Committing Cybercrimes

Marjan Bastan Farsani

Abstract

With the expansion of cyberspace, cybercrime, especially among adolescents, has become a major concern in the field of crime prevention. The present study examines the role of adolescents' knowledge of laws related to computer crimes and their experiences in online space on their tendency to commit unauthorized access. The findings indicate that negative experiences in cyberspace, such as being a victim of cyberattacks, can lead to the emergence of criminal counter-behavior by adolescents. While it is believed that awareness of the laws can be a barrier to committing crimes, the findings indicate that mere familiarity with the laws does not necessarily lead to a reduction in illegal behaviors and in some cases may even be associated with an increased tendency to commit unauthorized access. This indicates that a practical understanding of criminal consequences and strengthening a sense of responsibility in cyberspace plays a key role in preventing cybercrime among adolescents. The approach of this research is descriptive-analytical and the data collection was done using reliable books and electronic resources.

Keywords

Cybercrime; Adolescents; Unauthorized Access; Computer Crime Law; Crime Prevention.