مرکز وکلای قوه قضاییه خراسان رضوی

فصلنامه علمی تخصصی حقوق وکیل دعاوی

وابسته به مرکز وکلای قوه قضاییه خراسان رضوی

دوره ۱، شماره ۲، تابستان ۱۴۰۴، صص: ۹۴-۷۳

تحلیل جرم‌شناختی و بزه‌دیده‌شناختی جرائم سایبری علیه کودکان و نوجوانان: با تأکید بر پدوفیلی دیجیتال

نویسندگان:

سمیه سادات شریعتی

URL: https://www.vakildaavirazavi.ir/

DOI: https://doi.org/10.22034/vd.2025.729004

فصلنامه علمی تخصصی حقوق وکیل دعاوی

Journal of Vakil Daavi

دوره یک، شماره دوم، تابستان ۱۴۰۴، صص: ۹۴-۷۳

Vol 1, No 2, 2025, P: 73-94

تحلیل جرم‌شناختی و بزه‌دیده‌شناختی جرائم سایبری علیه کودکان و نوجوانان: با تأکید بر پدوفیلی دیجیتال

سمیه سادات شریعتی

دانشجو مقطع دکتری، رشته حقوق جزا و جرم‌شناسی، واحد مشهد، دانشگاه آزاد اسلامی، مشهد، ایران
Email: s.shariati1921@gmail.com

چکیده

با گسترش نفوذ اینترنت و فناوری‌های دیجیتال در زندگی روزمره، کودکان و نوجوانان به‌طور فزاینده‌ای در معرض تهدیدات و آسیب‌های فضای مجازی قرارگرفته‌اند. این مقاله با رویکردی تحلیلی-توصیفی و با استفاده از منابع کتابخانه‌ای، به بررسی چندبعدی جرائم سایبری علیه این گروه سنی آسیب‌پذیر می‌پردازد. پژوهش حاضر در سه محور اصلی سازمان‌دهی شده است: نخست، تحلیل جرم‌شناسی که به بررسی گونه‌شناسی، انگیزه‌ها و شیوه‌های عمل مجرمان سایبری می‌پردازد؛ دوم، تحلیل بزه‌دیده‌شناختی که عوامل خطرساز، انواع بزه‌دیدگی و پیامدهای عمیق آن بر قربانیان را واکاوی می‌کند؛ و سوم، تمرکز ویژه بر پدیده "پدوفیلی دیجیتال" به‌عنوان یکی از وخیم‌ترین اشکال این جرائم. یافته‌ها نشان می‌دهد که مجرمان سایبری طیف متنوعی را از مجرمان دارای اختلال پدوفیلی تا نوجوانان کنجکاو و حتی آشنایان قربانی در برمی‌گیرند و از فنون پیچیده‌ای مانند اغفال آنلاین برای به دام انداختن قربانیان خود استفاده می‌کنند. از سوی دیگر، آسیب‌پذیری کودکان ناشی از ترکیبی از ویژگی‌های رشدی، فقدان نظارت والدین و ضعف در آموزش‌های مرتبط با سواد دیجیتال است. این مقاله ضمن تحلیل خلأهای موجود در چارچوب‌های حقوقی و پیشگیرانه ایران، بر ضرورت اتخاذ یک راهبرد یکپارچه و چندوجهی تأکید می‌کند که شامل اصلاحات قانونی، تقویت ظرفیت‌های پلیسی، آموزش عمومی، توانمندسازی خانواده‌ها و همکاری بین‌المللی برای حفاظت مؤثر از کودکان و نوجوانان در دنیای دیجیتال است.

واژگان کلیدی: اغفال آنلاین، بزه‌دیدگی کودکان، پدوفیلی دیجیتال، پیشگیری، جرائم سایبری، جرم‌شناسی سایبری

مقدمه

در سپهر تحولات پارادایمی هزاره سوم، انقلاب دیجیتال و ظهور فضای سایبر به مثابه یک «مکان ثانی» ساختارهای اجتماعی، فرهنگی و حقوقی را با چالش‌های بنیادین و بی‌سابقه‌ای مواجه ساخته است. این عرصه نوین که بر پایه‌های گمنامی، بی‌مرزی و سرعت استوار است، در کنار فرصت‌های شگرف خود برای توسعه و ارتباطات، به بستری حاصل‌خیز برای تکوین و گسترش اشکال نوینی از بزهکاری مبدل شده است که نظام‌های عدالت کیفری سنتی را در پاسخگویی مؤثر به آن، دچار استیصال می‌کند. در این میان، آسیب‌پذیرترین گروه اجتماعی، یعنی کودکان و نوجوانان که به عنوان «بومیان دیجیتال» شناخته می‌شوند، در خط مقدم این تهدیدات قرار دارند. این نسل، در حالی که با شهود و مهارتی مثال‌زدنی در این فضا زیست می‌کند، به دلیل فقدان بلوغ شناختی، آسیب‌پذیری‌های عاطفی و کمبود تجربه، به اهداف اصلی مجرمان سایبری بدل شده‌اند؛ مجرمانی که از خصایص منحصربه‌فرد این فضا برای پنهان‌سازی هویت، عبور از مرزهای جغرافیایی و دسترسی مستقیم به حریم خصوصی قربانیان خود بهره می‌جویند (امیریان‌فارسانی و مالمیر، ۱۳۹۵: ۴۵).

مسئله محوری این است که جرائم سایبری علیه اطفال و نوجوانان، صرفاً نسخه دیجیتالی جرائم سنتی نیستند، بلکه پدیده‌هایی با ماهیت، پویایی و پیامدهای متمایزند. طیف این جرائم از قلدری سایبری[1] و مزاحمت آنلاین[2] تا وخیم‌ترین صور آن یعنی اغفال آنلاین برای مقاصد جنسی[3]، زورگیری جنسی[4] و تولید و توزیع محتوای سوءاستفاده جنسی از کودکان (CSAM[5]) را در بر می‌گیرد. پیچیدگی این پدیده، تحلیل تک‌بعدی و صرفاً حقوقی-کیفری را ناکارآمد می‌سازد. تقلیل این معضل به مجموعه‌ای از عناوین مجرمانه و مجازات‌ها، بدون درک عمیق از ریشه‌های روان‌شناختی و جامعه‌شناختی آن، به معنای نادیده گرفتن ابعاد پیشگیرانه و حمایتی سیاست جنایی است. از این رو، اتخاذ یک رویکرد میان‌رشته‌ای که بتواند به صورت همزمان به تحلیل «فاعل جرم» و «قربانی جرم» بپردازد، امری اجتناب‌ناپذیر است. اینجاست که دو شاخه مکمل جرم‌شناسی، با تمرکز بر اتیولوژی (سبب‌شناسی) جرم و ویژگی‌های بزهکار، و بزه‌دیده‌شناسی، با تمرکز بر فرآیند بزه‌دیدگی و عوامل آسیب‌پذیری قربانی، به مثابه ابزارهای تحلیلی قدرتمند برای کالبدشکافی این پدیده ظاهر می‌شوند (حق‌پناهان، ۱۴۰۳: ۳۴).

این مقاله در پرتو چنین ضرورتی، در پی آن است تا با بهره‌گیری از یک چارچوب تحلیلی دوگانه، به واکاوی جرم‌شناختی و بزه‌دیده‌شناختی جرائم سایبری علیه کودکان و نوجوانان بپردازد. پرسش‌های بنیادینی که این پژوهش به دنبال پاسخگویی به آن‌هاست، عبارتند از: ویژگی‌های روان‌شناختی، اجتماعی و شیوه‌های عمل[6]

1 cyberbullying
2 cyberstalking
3 online grooming
4 sextortion
5 child sexual abuse material
6 modus operandi

مجرمان سایبری علیه کودکان چیست؟ چه عواملی در سطح فردی، خانوادگی و فناورانه، کودکان و نوجوانان را به بزه‌دیدگان بالقوه در فضای مجازی تبدیل می‌کند و پیامدهای این بزه‌دیدگی کدامند؟ در این میان، پدیده «پدوفیلی دیجیتال» به عنوان یکی از سازمان‌یافته‌ترین و مخرب‌ترین اشکال این جرائم، چه مشخصات منحصربه‌فردی دارد و چگونه از بستر فناوری برای تحقق امیال مجرمانه بهره می‌برد؟ این پژوهش با تمرکز ویژه بر این پدیده، استدلال می‌کند که پدوفیلی دیجیتال صرفاً یک رفتار مجرمانه نیست، بلکه تجلی یک اختلال روانی-جنسی پیچیده در محیطی است که امکانات بی‌سابقه‌ای برای پنهان‌کاری، شبکه‌سازی و تشدید انحراف را فراهم می‌آورد و آسیب‌های روانی ماندگار و جبران‌ناپذیری بر قربانیان تحمیل می‌کند (کریمی، ۱۳۹۷).

بر این اساس، ساختار مقاله به گونه‌ای طراحی شده است که در ابتدا، به تحلیل جرم‌شناختی پدیده پرداخته و به گونه‌شناسی مجرمان، انگیزه‌های آنان و تاکتیک‌های پیچیده اغفال آنلاین می‌پردازد. در گام بعدی، از منظر بزه‌دیده‌شناسی، عوامل خطرساز و آسیب‌پذیری‌های کودکان و نوجوانان در فضای سایبر و همچنین آثار و پیامدهای عمیق بزه‌دیدگی بر سلامت روانی و اجتماعی آنان مورد بررسی قرار خواهد گرفت. بخش محوری پژوهش به کالبدشکافی پدیده «پدوفیلی دیجیتال»، مبانی روان‌شناختی آن و نحوه تجلی آن در فضای مجازی اختصاص خواهد یافت. در نهایت، با نگاهی به نظام حقوقی ایران و اسناد بین‌المللی، خلأهای موجود در پاسخ‌های کیفری و پیشگیرانه تحلیل شده و راهبردهایی برای تدوین یک سیاست جنایی یکپارچه، پیشگیرانه و حمایتی در راستای صیانت از حقوق بنیادین کودکان در عصر دیجیتال ارائه خواهد شد.

تحلیل جرم‌شناختی: بررسی ویژگی‌ها و انگیزه‌های مجرمان سایبری

برای درک عمیق جرائم سایبری علیه کودکان، نخست باید به سراغ عاملان این جرائم رفت. برخلاف تصور عمومی که مجرم را یک "غریبه خطرناک" در گوشه‌ای تاریک از اینترنت ترسیم می‌کند، تحقیقات جرم‌شناختی نشان می‌دهد که هویت، انگیزه‌ها و روش‌های عمل این افراد بسیار متنوع و پیچیده است. تحلیل جرم‌شناختی به ما کمک می‌کند تا با شناخت این پیچیدگی‌ها، از کلیشه‌ها فراتر رفته و به راهکارهای پیشگیرانه و مقابله‌ای دقیق‌تری دست یابیم (ابوذری، ۱۳۹۵: ۱۱۲).

گونه‌شناسی مجرمان سایبری علیه کودکان

مجرمان سایبری که کودکان و نوجوانان را هدف قرار می‌دهند، یک گروه همگن نیستند. می‌توان آن‌ها را بر اساس انگیزه، رابطه با قربانی و نوع جرم ارتکابی به چند دسته اصلی تقسیم کرد:

- مجرمان با تمایلات پدوفیلیک: این گروه، خطرناک‌ترین دسته از مجرمان را تشکیل می‌دهند. انگیزه اصلی آن‌ها، ارضای تمایلات جنسی نسبت به کودکان است. پدوفیلی یک اختلال روانی-جنسی (پارافیلیا) تعریف

می‌شود که مشخصه آن، خیال‌پردازی‌ها، امیال یا رفتارهای جنسی مکرر و شدید نسبت به کودکان پیش از بلوغ است (حق‌پناهان، ۱۴۰۳: ۹۸). این افراد از فضای مجازی برای سه هدف عمده استفاده می‌کنند: دسترسی و به اشتراک‌گذاری محتوای سوءاستفاده جنسی از کودکان (CSAM)، برقراری ارتباط و اغفال کودکان و عادی‌سازی و توجیه رفتار خود در جوامع آنلاین همفکر. تحقیقات نشان داده است که جرائم مرتبط با پورنوگرافی کودکان، یک شاخص تشخیصی معتبر برای شناسایی تمایلات پدوفیلیک است، زیرا این مجرمان در مقایسه با سایر مجرمان جنسی، برانگیختگی جنسی بیشتری نسبت به کودکان نشان می‌دهند (ستو[1] و همکاران، ۲۰۰۶).

- مجرمان نوجوان: یک یافته شگفت‌آور و مهم در جرم‌شناسی سایبری این است که بخش قابل توجهی از عاملان جرائم آنلاین علیه کودکان، خودشان زیر ۱۸ سال سن دارند. یک فراتحلیل جامع نشان داد که حدود ۴۴ درصد از مجرمان در جرائم اینترنتی علیه کودکان، نوجوان هستند (هویت مرتکبین در جرایم آنلاین علیه کودکان[2]، ۲۰۲۳). انگیزه‌های این گروه می‌تواند بسیار متفاوت از بزرگسالان باشد و شامل کنجکاوی جنسی، فشار همسالان، قلدری، انتقام‌جویی یا رفتارهای پرخطر اکتشافی باشد. اگرچه نیت آن‌ها ممکن است به اندازه مجرمان پدوفیلیک بدخواهانه نباشد، اما آسیب‌های ناشی از اقدامات آن‌ها (مانند انتشار تصاویر خصوصی یا زورگیری جنسی) می‌تواند به همان اندازه ویرانگر باشد.

- آشنایان و اعضای خانواده: کلیشه "خطر غریبه‌ها[3]" در فضای مجازی تا حد زیادی گمراه‌کننده است. همان فراتحلیل ذکر شده نشان داد که حدود ۶۸ درصد از مجرمان آنلاین، برای کودک آشنا هستند و شامل دوستان، همکلاسی‌ها، آشنایان خانوادگی و حتی اعضای خانواده می‌شوند. این افراد از اعتماد و دسترسی خود به کودک برای سوءاستفاده بهره می‌برند که این امر فرآیند شناسایی و گزارش جرم را برای قربانی بسیار دشوارتر می‌سازد.

- مجرمان فرصت‌طلب: این دسته لزوماً دارای تمایلات جنسی انحرافی نیستند، اما از آسیب‌پذیری کودکان برای منافع دیگر سوءاستفاده می‌کنند. انگیزه‌های آن‌ها می‌تواند مالی (مانند زورگیری جنسی یا کلاهبرداری)، روانی (مانند قلدری سایبری برای کسب قدرت و کنترل) یا ایدئولوژیک (مانند جذب نوجوانان به گروه‌های افراطی) باشد.

انگیزه‌های روانی و اجتماعی مجرمان

عوامل متعددی در سطح فردی و اجتماعی، افراد را به سمت ارتکاب جرائم سایبری علیه کودکان سوق می‌دهد:

- عوامل روان‌شناختی:

- اختلالات روانی: همانطور که اشاره شد، پدوفیلی یک اختلال بالینی است که ریشه‌های عمیق روانی و حتی

1 Seto
2 Perpetrators› Identity in Online Crimes Against Children
3 stranger danger

عصب‌شناختی دارد. مطالعات جدید با استفاده از تصویربرداری عصبی و یادگیری ماشین، الگوهای ساختاری متفاوتی را در مغز مجرمان پدوفیل در مقایسه با افراد عادی شناسایی کرده‌اند که می‌تواند به درک بهتر مبانی بیولوژیک این اختلال کمک کند (پوپوویچ[1] و همکاران، ۲۰۲۳).

- تحریف‌های شناختی: مجرمان جنسی اغلب از مکانیسم‌های دفاعی و تحریف‌های شناختی برای توجیه رفتار خود استفاده می‌کنند. جملاتی مانند "کودک خودش می‌خواست"، "این فقط یک کنجکاوی بی‌ضرر است" یا "او به سنی رسیده که این چیزها را بفهمد" نمونه‌هایی از این توجیهات هستند که احساس گناه را کاهش داده و ادامه رفتار مجرمانه را ممکن می‌سازند (ابوذری، ۱۳۹۵: ۱۵۴).

- فقدان همدلی و کنترل تکانه: بسیاری از این مجرمان در درک و احساس عواطف دیگران (همدلی) دچار نقص هستند و توانایی کمی در کنترل تکانه‌ها و امیال آنی خود دارند. این ویژگی‌ها، ارتکاب اعمال آسیب‌زا علیه دیگران را برایشان آسان‌تر می‌کند (حق‌پناهان، ۱۴۰۳: ۱۲۰).

- عوامل اجتماعی و محیطی (مرتبط با فضای سایبر):

- اثر بازدارندگی‌زدایی آنلاین[2]: فضای مجازی دارای ویژگی‌هایی است که به تضعیف بازدارنده‌های روانی و اجتماعی منجر می‌شود. ناشناس بودن، نامرئی بودن و عدم وجود سرنخ‌های ارتباطی غیرکلامی باعث می‌شود افراد رفتارهایی را آنلاین انجام دهند که هرگز در دنیای واقعی به آن دست نمی‌زنند (مدیری و واثقی‌پناه، ۱۳۹۶: ۸۸). این پدیده به مجرمان اجازه می‌دهد تا بدون ترس از شناسایی و قضاوت اجتماعی، امیال تاریک خود را بروز دهند.

- دسترسی و تقویت اجتماعی: اینترنت دسترسی بی‌سابقه‌ای به محتوای غیرقانونی (CSAM) فراهم کرده و از سوی دیگر، بستری برای شکل‌گیری "جوامع آنلاین" از افراد همفکر ایجاد نموده است. در این انجمن‌ها و گروه‌های چت رمزگذاری‌شده، مجرمان نه تنها به تبادل اطلاعات و محتوا می‌پردازند، بلکه هویت انحرافی خود را تقویت کرده و احساس می‌کنند که رفتارشان "عادی" و پذیرفته‌شده است (صفرزاده رودسری، ۱۳۹۶: ۷۱).

- جهانی بودن و ضعف نظارت: ماهیت فرامرزی اینترنت، تعقیب قانونی مجرمان را بسیار دشوار می‌سازد. تفاوت در قوانین کشورها، مشکلات مربوط به صلاحیت قضایی و عدم همکاری کافی شرکت‌های فناوری، محیطی کم‌خطر و پرجاذبه برای فعالیت مجرمانه ایجاد کرده است (گرکی، ۱۳۸۹: ۵۴).

شیوه‌های عمل

مجرمان سایبری از تاکتیک‌های متنوع و فریبنده‌ای برای هدف قرار دادن کودکان استفاده می‌کنند که مهم‌ترین

1 Popovic
2 online disinhibition effect

است. این فرآیند، مجموعه‌ای از اقدامات حساب‌شده برای جلب اعتماد کودک،Groomingآن‌ها "اغفال آنلاین" یا کاهش مقاومت‌های او و آماده‌سازی وی برای سوءاستفاده جنسی است. یک مطالعه بر روی مکالمات پدوفیل‌ها در فضای مجازی، مراحل اصلی این فرآیند را شناسایی کرده است (گوپتا[1] و همکاران، ۲۰۱۲):

۱. هدف‌گیری: مجرم، کودکی را که به نظر آسیب‌پذیر می‌رسد (مثلاً کودکانی که در پروفایل خود ابراز تنهایی یا ناراحتی کرده‌اند) شناسایی می‌کند.

۲. ایجاد رابطه و جلب اعتماد: این مرحله، حیاتی‌ترین و طولانی‌ترین بخش فرآیند است. مجرم با ابراز علاقه به سرگرمی‌های کودک، همدردی با مشکلات او و دادن هدایا، خود را به عنوان یک دوست یا حامی دلسوز جا می‌زند.

۳. منزوی کردن قربانی: مجرم تلاش می‌کند تا کودک را از والدین و دوستانش جدا کند و خود را به تنها فرد قابل اعتماد در زندگی او تبدیل کند. او ممکن است از کودک بخواهد که مکالماتشان را مخفی نگه دارد.

۴. جنسی‌سازی رابطه: پس از جلب اعتماد کامل، مجرم به تدریج مکالمات را به سمت موضوعات جنسی سوق می‌دهد، جوک‌های نامناسب تعریف می‌کند یا تصاویر جنسی ارسال می‌کند تا حساسیت‌زدایی کرده و مرزهای کودک را جابجا کند.

۵. شروع تماس جنسی: این مرحله می‌تواند به صورت آنلاین (مانند درخواست برای ارسال تصاویر برهنه یا انجام اعمال جنسی در برابر وب‌کم) یا با برنامه‌ریزی برای یک ملاقات حضوری صورت گیرد.

۶. حفظ راز و کنترل: پس از شروع سوءاستفاده، مجرم با تهدید به افشای تصاویر یا رازها، قربانی را وادار به سکوت و ادامه رابطه می‌کند.

علاوه بر گرومینگ، زورگیری جنسی نیز یک شیوه عمل رایج است. در این روش، مجرم پس از فریب قربانی برای ارسال تصاویر یا ویدئوهای خصوصی، او را تهدید می‌کند که در صورت عدم برآورده کردن خواسته‌های بیشتر (مالی یا جنسی)، این محتوا را برای خانواده و دوستانش منتشر خواهد کرد. این جرائم غالباً در بستر شبکه‌های اجتماعی محبوب مانند اینستاگرام و تلگرام، و همچنین پلتفرم‌های بازی آنلاین رخ می‌دهد (مقاله کنفرانسی «کودک‌آزاری آنلاین»، ۱۴۰۲-۱۴۰۳).

تحلیل بزه‌دیده‌شناختی: کودکان و نوجوانان به مثابه قربانیان سایبری

چرا کودکان و نوجوانان تا این حد در برابر جرائم سایبری آسیب‌پذیر هستند؟ پاسخ به این پرسش نیازمند یک تحلیل بزه‌دیده‌شناختی است که به بررسی تعامل میان ویژگی‌های قربانی، رفتار او و شرایط محیطی می‌پردازد. بزه‌دیده‌شناسی سایبری نشان می‌دهد که قربانی شدن در فضای آنلاین، یک رویداد تصادفی نیست، بلکه نتیجه

1 Gupta

تلاقی مجموعه‌ای از عوامل خطرساز است (مردانی، باوی، و موالی‌زاده، ۱۳۹۲).

عوامل آسیب‌پذیری و خطرساز

آسیب‌پذیری کودکان و نوجوانان در فضای سایبر از سه منبع اصلی نشأت می‌گیرد: ویژگی‌های فردی و رشدی، عوامل خانوادگی و اجتماعی، و عوامل مرتبط با فناوری.

- ویژگی‌های فردی و رشدی:

- کنجکاوی و نیاز به استقلال: دوره نوجوانی، زمان هویت‌یابی، استقلال‌طلبی و کاوشگری است. نوجوانان به طور طبیعی تمایل دارند مرزها را جابجا کرده و روابط جدیدی را خارج از حلقه خانواده تجربه کنند. این ویژگی رشدی، آن‌ها را به سمت برقراری ارتباط با افراد ناشناس در فضای مجازی سوق می‌دهد (اولز، ۱۴۰۰: ۶۵).

- ساده‌لوحی و فقدان درک خطر: کودکان، به ویژه در سنین پایین‌تر، فاقد بلوغ شناختی لازم برای تشخیص نیت‌های فریبکارانه، درک خطرات بلندمدت به اشتراک‌گذاری اطلاعات شخصی و شناسایی تاکتیک‌های دستکاری هستند. آن‌ها به راحتی به بزرگسالانی که خود را دوست و مهربان نشان می‌دهند، اعتماد می‌کنند (رفیعی کشتلی، ۱۳۹۰).

- مشکلات روانی پیشین: تحقیقات نشان می‌دهد کودکانی که از مشکلات روانی مانند عزت نفس پایین، افسردگی، اضطراب اجتماعی یا سابقه سوءاستفاده در دنیای واقعی رنج می‌برند، اهداف آسان‌تری برای مجرمان سایبری هستند. این کودکان ممکن است برای کسب تأیید، محبت و توجهی که در زندگی واقعی دریافت نمی‌کنند، به فضای مجازی پناه ببرند و در نتیجه، بیشتر در معرض خطر اغفال قرار گیرند (رحمتی و سیفی، ۱۴۰۰).

- عوامل خانوادگی و اجتماعی:

- فقدان نظارت والدین و ضعف در ارتباط: یکی از مهم‌ترین عوامل خطرساز، عدم نظارت کافی والدین بر فعالیت‌های آنلاین فرزندانشان است. این نظارت نباید به معنای جاسوسی باشد، بلکه باید در قالب یک رابطه باز و مبتنی بر اعتماد صورت گیرد که در آن، کودک احساس امنیت کند تا مشکلات و تجربیات آنلاین خود را با والدینش در میان بگذارد. فقدان سازوکارهای حمایتی و ناآگاهی والدین از راه‌های نفوذ مجازی، کودکان را به شدت در معرض بزه‌دیدگی قرار می‌دهد (میرزامحمدی، ۱۴۰۲). ترکیبی از فقر نظارتی و بی‌اطلاعی خانواده‌ها، آسیب‌پذیری کودکان را مضاعف می‌کند (مردانی، باوی، و موالی‌زاده، ۱۴۰۲).

- انزوای اجتماعی و فقدان حمایت: کودکانی که در محیط واقعی خود احساس تنهایی می‌کنند یا از شبکه حمایتی قوی از دوستان و خانواده برخوردار نیستند، بیشتر مستعد برقراری روابط پرخطر آنلاین هستند. مطالعه موردی نشان داده است که دسترسی بدون قید و بند به فضای مجازی و ارتباط با افراد بالغ ناشناس، شاخص‌های بزهکاری و بزه‌دیدگی را تقویت می‌کند (باباحسن زاده، مقاله پژوهشی).

- شرایط اقتصادی-اجتماعی: فقر و حاشیه‌نشینی می‌تواند آسیب‌پذیری کودکان را تشدید کند. پژوهشی در ایران نشان داد که کودکان ساکن در مناطق حاشیه‌نشین به دلیل فقر زیرساختی، سواد دیجیتال پایین‌تر و دسترسی کمتر به ابزارهای محافظتی، بیشتر در معرض انواع خاصی از بزه‌دیدگی سایبری مانند سوءاستفاده جنسی قرار دارند (پوریان و همکاران، ۱۴۰۳).

- عوامل مرتبط با فناوری و محیط آنلاین:

- استفاده مشکل‌ساز از رسانه‌های اجتماعی: صرف زمان بیش از حد در شبکه‌های اجتماعی و درگیر شدن در رفتارهای آنلاین پرخطر (مانند به اشتراک‌گذاری اطلاعات شخصی، پذیرش درخواست دوستی از غریبه‌ها) به طور مستقیم با افزایش خطر بزه‌دیدگی سایبری مرتبط است. یک مطالعه نشان داد که استفاده مشکل‌ساز از رسانه‌های اجتماعی، یک پیش‌بینی‌کننده قوی برای قربانی شدن در فضای مجازی است (مارتیلا[1] و همکاران، ۲۰۲۱).

- طراحی پلتفرم‌ها: الگوریتم‌ها و ویژگی‌های بسیاری از پلتفرم‌های اجتماعی برای به حداکثر رساندن تعامل و زمان حضور کاربر طراحی شده‌اند. این طراحی می‌تواند به طور ناخواسته، کودکان را در معرض محتوای نامناسب یا تماس‌های ناخواسته از سوی افراد غریبه قرار دهد.

گونه‌شناسی بزه‌دیدگی سایبری کودکان و نوجوانان

بزه‌دیدگی در فضای مجازی اشکال گوناگونی دارد که هر یک پیامدهای خاص خود را به همراه دارد:

- سوءاستفاده جنسی آنلاین: این دسته شامل اغفال آنلاین، زورگیری جنسی، تولید و انتشار محتوای سوءاستفاده جنسی از کودکان (CSAM) و تماس جنسی آنلاین می‌شود. این جرائم عمیق‌ترین و ماندگارترین آسیب‌ها را به همراه دارند.

- قلدری سایبری: شامل ارسال پیام‌های توهین‌آمیز، انتشار شایعات، به اشتراک‌گذاری تصاویر خصوصی بدون اجازه و طرد کردن فرد از گروه‌های آنلاین است. عاملان آن معمولاً همسالان قربانی هستند.

- مزاحمت و تعقیب سایبری: شامل ارسال مکرر پیام‌های ناخواسته، تهدید و نظارت بر فعالیت‌های آنلاین قربانی است. این رفتار می‌تواند از سوی همسالان یا بزرگسالان سر بزند و احساس امنیت قربانی را به کلی از بین ببرد (رحمتی و سیفی، ۱۴۰۰).

- مواجهه با محتوای نامناسب: کودکان ممکن است به صورت تصادفی یا عمدی با محتوایی مواجه شوند که برای سن آن‌ها نامناسب است، مانند پورنوگرافی، خشونت افراطی یا محتوای افراطگرایانه. مطالعه‌ای در تهران نشان داد که مواجهه نوجوانان با محتوای پورنوگرافیک با افزایش تمایلات و رفتارهای جنسی پرخطر مرتبط است

1 Marttila

(خلج‌آبادی فراهانی، ۱۳۹۸).

پیامدهای بزه‌دیدگی سایبری

آسیب‌های ناشی از جرائم سایبری صرفاً مجازی نیستند و تأثیرات عمیق و واقعی بر زندگی قربانیان دارند. این پیامدها را می‌توان در سه سطح بررسی کرد:

- آثار روانی و عاطفی: این شایع‌ترین و جدی‌ترین دسته از پیامدهاست. قربانیان اغلب دچار اضطراب، افسردگی، اختلال استرس پس از سانحه (PTSD)، ترس و بی‌اعتمادی می‌شوند. آن‌ها همچنین ممکن است با احساس شدید گناه، شرم و انزوا دست و پنجه نرم کنند، به خصوص در موارد سوءاستفاده جنسی. این فشار روانی می‌تواند به افکار خودکشی و اقدام به خودآزاری منجر شود (کریمی، ۱۳۹۷).

- آثار اجتماعی و رفتاری: بزه‌دیدگی سایبری می‌تواند منجر به انزوای اجتماعی و کناره‌گیری کودک از دوستان و فعالیت‌های مورد علاقه‌اش شود. افت تحصیلی، از دست دادن علاقه به مدرسه و مشکل در برقراری روابط سالم از دیگر پیامدهای رایج است. همچنین، این تجربه می‌تواند به روابط خانوادگی آسیب بزند، به خصوص اگر کودک احساس کند که توسط والدینش درک یا حمایت نمی‌شود.

- آثار فیزیکی: استرس و اضطراب شدید ناشی از این تجربیات می‌تواند به شکل مشکلات جسمی مانند اختلالات خواب، اختلالات خوردن، سردرد و مشکلات گوارشی بروز کند. این علائم روان‌تنی نشان‌دهنده تأثیر عمیق آسیب روانی بر سلامت جسمی کودک است.

یکی از نکات مهم در بزه‌دیدگی، پدیده بزه‌دیدگی مکرر است. کودکانی که یک بار قربانی سوءاستفاده (آنلاین یا آفلاین) شده‌اند، در آینده در معرض خطر بیشتری برای تجربه مجدد آزار قرار می‌گیرند، زیرا ممکن است مکانیسم‌های مقابله‌ای آن‌ها تضعیف شده و عزت نفسشان آسیب دیده باشد.

تمرکز ویژه: پدوفیلی دیجیتال، ابعاد و ویژگی‌ها

در میان طیف گسترده جرائم سایبری علیه کودکان، پدوفیلی دیجیتال به دلیل ماهیت پیچیده، سازمان‌یافته و آسیب‌های عمیقی که بر جای می‌گذارد، نیازمند توجه و تحلیل ویژه‌ای است. این پدیده صرفاً یک جرم نیست، بلکه تجلی یک اختلال روانی-جنسی جدی در بستر فناوری‌های نوین است.

تعریف و مفهوم‌پردازی

پدوفیلی در روان‌پزشکی به عنوان یک اختلال پارافیلیک طبقه‌بندی می‌شود که مشخصه اصلی آن، وجود خیال‌پردازی‌ها، امیال جنسی یا رفتارهای مکرر و شدید نسبت به کودکان پیش از بلوغ (معمولاً ۱۳ ساله یا کوچکتر)

است که برای حداقل شش ماه ادامه داشته باشد و باعث ناراحتی یا اختلال عملکرد قابل توجهی برای فرد شود (امیریان‌فارسانی و مالمیر، ۱۳۹۵: ۹۲). پدوفیلی دیجیتال به معنای بروز و ارضای این تمایلات از طریق ابزارها و پلتفرم‌های دیجیتال است. بسیار مهم است که میان مجرمان پدوفیل و سایر مجرمان جنسی آنلاین تمایز قائل شویم. همه کسانی که در فضای مجازی مرتکب سوءاستفاده جنسی از کودکان می‌شوند، لزوماً دارای اختلال پدوفیلی نیستند. جرم‌شناسان معمولاً دو دسته اصلی را از هم تفکیک می‌کنند:

۱. مجرمان ترجیحی: این افراد همان مجرمان مبتلا به پدوفیلی هستند. علاقه جنسی آن‌ها به طور انحصاری یا عمدتاً معطوف به کودکان است. جرائم آن‌ها معمولاً برنامه‌ریزی شده، مکرر و شامل رفتارهایی مانند جمع‌آوری CSAM و اغفال فعالانه کودکان است.

۲. مجرمان موقعیتی: این افراد به طور اولیه به کودکان تمایل جنسی ندارند، اما تحت تأثیر شرایط خاصی (مانند دسترسی آسان، کنجکاوی، مصرف مواد مخدر یا مشکلات در روابط بزرگسالان) ممکن است مرتکب جرم علیه کودکان شوند. مجرمان نوجوان اغلب در این دسته قرار می‌گیرند.

این تمایز از آن جهت حائز اهمیت است که انگیزه‌ها، شیوه‌های عمل و به تبع آن، راهکارهای پیشگیری و درمانی برای هر گروه متفاوت است (حق‌پناهان، ۱۴۰۳: ۱۰۵).

مبانی روان‌شناختی و عصب‌شناختی پدوفیلی

اگرچه علت دقیق پدوفیلی هنوز به طور کامل شناخته نشده است، اما تحقیقات روان‌شناختی و عصب‌شناختی سرنخ‌های مهمی را ارائه می‌دهند:

- نظریه‌های روان‌شناختی: نظریه‌های مختلفی برای تبیین این اختلال مطرح شده‌اند. نظریه‌های تحولی معتقدند که این تمایلات ممکن است ریشه در تجربیات نامطلوب دوران کودکی خود فرد (مانند سابقه سوءاستفاده جنسی) یا اختلال در فرآیند طبیعی رشد روانی-جنسی داشته باشد. نظریه‌های یادگیری بیان می‌کنند که این تمایلات می‌توانند از طریق شرطی‌سازی و تقویت (مثلاً با مشاهده پورنوگرافی کودکان) شکل گرفته و تثبیت شوند. نظریه‌های شناختی نیز بر نقش تحریف‌های شناختی و سیستم‌های باوری ناکارآمد در توجیه و تداوم این رفتارها تأکید دارند (خدایی‌فر و بیرقی، ۱۳۸۸).

- شواهد عصب‌شناختی و روان‌سنجی: علم مدرن در تلاش است تا مبانی بیولوژیک این اختلال را کشف کند. مطالعات اخیر با استفاده از تصویربرداری تشدید مغناطیسی ساختاری (sMRI) و الگوریتم‌های یادگیری ماشین، توانسته‌اند الگوهای خطری را در ساختار مغز شناسایی کنند که با درجه بالایی از دقت، مجرمان پدوفیل را از افراد غیرمجرم متمایز می‌کند. این یافته‌ها نشان‌دهنده وجود تفاوت‌های عصبی-زیستی مرتبط با این اختلال است

(پوپوویچ[1] و همکاران، ۲۰۲۳). علاوه بر این، ابزارهای روان‌سنجی غیرمستقیم برای ارزیابی تمایلات جنسی به کار گرفته می‌شوند. روش‌هایی مانند زمان مشاهده (VT[2]) که مدت زمان نگاه کردن فرد به تصاویر مختلف (کودکان در مقابل بزرگسالان) را اندازه‌گیری می‌کند، و تکالیف زمان واکنش (CRT[3])، توانسته‌اند با موفقیت نسبی میان مجرمان جنسی علیه کودکان و گروه‌های کنترل تمایز قائل شوند (اشمیت، بابچیشین و لمان[4]، ۲۰۱۶؛ دامبرت و همکاران، ۲۰۱۵). این ابزارها به تشخیص و ارزیابی خطر کمک شایانی می‌کنند.

تجلی پدوفیلی در فضای دیجیتال

اینترنت به طور بنیادین، نحوه عمل مجرمان پدوفیل را دگرگون کرده و به آن‌ها امکانات بی‌سابقه‌ای داده است:

- مصرف و توزیع CSAM: اینترنت به یک کتابخانه و شبکه توزیع جهانی برای محتوای سوءاستفاده جنسی از کودکان تبدیل شده است. برای یک فرد پدوفیل، دسترسی به این محتوا نقش کلیدی در تقویت خیال‌پردازی‌ها و عادی‌سازی تمایلاتش دارد. تحقیقات تأیید کرده‌اند که ارتکاب جرائم مرتبط با CSAM، یک شاخص تشخیصی بسیار قوی برای وجود اختلال پدوفیلی است (ستو و همکاران، ۲۰۰۶). این عمل، رایج‌ترین و گسترده‌ترین تجلی پدوفیلی دیجیتال است.

- جوامع آنلاین و خرده‌فرهنگ‌ها: یکی از خطرناک‌ترین جنبه‌های اینترنت، فراهم آوردن بستری برای شکل‌گیری جوامع آنلاین از مجرمان پدوفیل است. در این انجمن‌ها که اغلب در وب تاریک یا از طریق اپلیکیشن‌های پیام‌رسان رمزگذاری‌شده فعالیت می‌کنند، این افراد به صورت ناشناس گرد هم می‌آیند. در این فضاها، آن‌ها نه تنها به تبادل CSAM می‌پردازند، بلکه تکنیک‌های اغفال کودکان را به یکدیگر آموزش می‌دهند، داستان‌های سوءاستفاده خود را به اشتراک می‌گذارند و یکدیگر را تشویق می‌کنند. این جوامع، یک "اتاق پژواک" ایجاد می‌کنند که در آن، باورهای انحرافی تقویت شده و هرگونه احساس گناه یا تردید از بین می‌رود (مدیری و واثقی‌پناه، ۱۳۹۶: ۱۲۳).

- تولید محتوای خودساخته: در سال‌های اخیر، یک تغییر نگران‌کننده از مصرف منفعلانه محتوای از پیش موجود، به سمت تولید فعالانه محتوای جدید مشاهده شده است. مجرمان با استفاده از تکنیک‌های اغفال و زورگیری جنسی، کودکان را وادار می‌کنند تا خودشان از خود تصاویر و ویدئوهای جنسی تهیه و برای مجرم ارسال کنند. این فرآیند به مجرم احساس قدرت، کنترل و "مالکیت" بیشتری بر قربانی می‌دهد و آسیب روانی بسیار عمیق‌تری را بر کودک تحمیل می‌کند.

- تهدیدات نوظهور (هوش مصنوعی و دیپ‌فیک): پیشرفت‌های اخیر در زمینه هوش مصنوعی، نگرانی‌های

1 Popovic
2 Viewing Time
3 Choice Reaction Time
4 Schmidt, Babchishin & Lehmann

جدیدی را به وجود آورده است. فناوری دیپ‌فیک[1] این قابلیت را دارد که تصاویر و ویدئوهای بسیار واقع‌گرایانه‌ای از کودکان در موقعیت‌های سوءاستفاده جنسی تولید کند، حتی اگر آن کودک هرگز در چنین موقعیتی قرار نگرفته باشد. این "CSAM ترکیبی[2]" چالش‌های عظیمی را برای نهادهای قانون‌گذار و پلیس در زمینه شناسایی، پیگرد و اثبات جرم ایجاد می‌کند (سهلانی، نیک‌نفس، و باروطی، ۱۴۰۰: ۱۵۰).

درک این ابعاد نشان می‌دهد که مقابله با پدوفیلی دیجیتال نیازمند یک رویکرد جامع است که فراتر از مسدودسازی محتوا رفته و شامل شناسایی مجرمان، از هم پاشیدن شبکه‌های آنلاین آن‌ها و تمرکز بر پیشگیری از طریق آموزش و افزایش آگاهی باشد.

چارچوب‌های حقوقی و راهبردهای پیشگیرانه

پیچیدگی و گستردگی جرائم سایبری علیه کودکان، نظام‌های حقوقی و اجتماعی را با چالشی بی‌سابقه مواجه کرده است. مقابله مؤثر با این پدیده نیازمند یک چارچوب قانونی جامع و راهبردهای پیشگیرانه چندلایه است. در این بخش، وضعیت حقوقی ایران و سپس راهبردهای کلان پیشگیری مورد تحلیل قرار می‌گیرد.

تحلیل وضعیت حقوقی در ایران

سیاست جنایی ایران در سال‌های اخیر تلاش کرده است تا خود را با تهدیدات نوظهور فضای مجازی تطبیق دهد، اما همچنان با خلأها و چالش‌های قابل توجهی روبرو است.

- قوانین موجود:

- قانون جرائم رایانه‌ای (مصوب ۱۳۸۸): این قانون، سنگ بنای حقوق کیفری سایبری ایران است. مواد ۱۴ و ۱۵ این قانون به طور خاص به محتوای مستهجن و مبتذل، از جمله سوءاستفاده جنسی از کودکان (موسوم به هرزه‌نگاری کودکان) می‌پردازد و برای تولید، توزیع و نگهداری چنین محتوایی مجازات تعیین کرده است. با این حال، این قانون بیشتر بر "محتوا" تمرکز دارد تا "رفتار" مجرمانه.

- قانون حمایت از اطفال و نوجوانان (مصوب ۱۳۹۹): این قانون یک گام مهم رو به جلو در حمایت از کودکان در برابر انواع آزار، از جمله آزار در فضای مجازی است. ماده ۸ این قانون، هرگونه آزار جنسی، بهره‌کشی، هرزه‌نگاری و معامله اطفال و نوجوانان را جرم‌انگاری کرده و ماده ۱۲ نیز هرگونه ارتباط مجازی به منظور آزار جنسی را ممنوع اعلام کرده است. این قانون تلاش کرده تا حمایت گسترده‌تری را فراهم آورد.

- خلأها و چالش‌ها:

1 Deepfake
2 Synthetic CSAM

- فقدان جرم‌انگاری صریح برخی رفتارها: مفاهیم جدیدی مانند "اغفال آنلاین[1]" به صراحت در قوانین ایران جرم‌انگاری نشده‌اند. در حالی که مراحل اولیه گرومینگ (مانند جلب اعتماد) ممکن است به خودی خود جرم نباشند، اما بخش جدایی‌ناپذیر فرآیند منجر به سوءاستفاده هستند. جرم‌انگاری این رفتار مقدماتی می‌تواند امکان مداخله پیشگیرانه را فراهم کند (مولائی کوچه‌باغ، ۱۴۰۴).

- چالش‌های اثباتی و قضایی: ماهیت غیرملموس و فرار جرائم سایبری، جمع‌آوری ادله دیجیتال را با دشواری همراه می‌سازد. ناشناس بودن مجرمان، استفاده از ابزارهای رمزنگاری و حذف سریع داده‌ها، کار را برای پلیس و دستگاه قضا سخت می‌کند. علاوه بر این، برساخت قضایی از این جرائم هنوز در حال تکامل است و برخی قضات ممکن است با رویکردهای سنتی به این پدیده‌های نوین بنگرند، در حالی که نیاز به الگوهای جدید و حمایتی برای رسیدگی به این پرونده‌ها وجود دارد (فرهادی آلاشتی، ۱۴۰۱; فرهادی آلاشتی و همکاران، ۱۴۰۲).

- مسائل مربوط به صلاحیت و همکاری بین‌المللی: از آنجا که مجرم، قربانی و سرورهای میزبان داده‌ها می‌توانند در کشورهای مختلفی باشند، تعقیب کیفری با موانع جدی مربوط به صلاحیت قضایی روبرو می‌شود. ایران برای مقابله مؤثر با این جرائم، نیازمند تقویت همکاری‌های بین‌المللی و پیوستن به کنوانسیون‌های مرتبط مانند کنوانسیون بوداپست در مورد جرائم سایبری است (گرکی، ۱۳۸۹: ۱۲۰).

- تمرکز ناکافی بر بزه‌دیده: سیاست جنایی ایران، با وجود پیشرفت‌ها، هنوز به طور کامل رویکردی بزه‌دیده‌محور را اتخاذ نکرده است. فرآیندهای دادرسی می‌توانند برای کودکان آسیب‌زا باشد و حمایت‌های روانی، اجتماعی و حقوقی کافی برای قربانیان و خانواده‌هایشان پیش‌بینی نشده است. تأکید باید از صرف مجازات مجرم، به سمت ترمیم آسیب‌های وارده بر قربانی و جبران خسارات غیرمادی او تغییر یابد (کهندانی، ۱۳۹۲؛ فروغیان و عابدی، ۱۴۰۴).

راهبردهای پیشگیری

پیشگیری همواره بر مقابله ارجحیت دارد. یک استراتژی جامع پیشگیری باید در سه سطح وضعی، اجتماعی و کیفری طراحی و اجرا شود.

- پیشگیری وضعی و فناورانه: این رویکرد به دنبال کاهش فرصت‌های ارتکاب جرم از طریق تغییر در محیط است.

- ابزارهای کنترل والدین و فیلترینگ: نصب نرم‌افزارهای نظارتی و فیلترینگ محتوا بر روی دستگاه‌های کودکان می‌تواند اولین لایه حفاظتی باشد.

1 Online Grooming

- طراحی ایمن: شرکت‌های فناوری و توسعه‌دهندگان اپلیکیشن‌ها مسئولیت دارند که ایمنی کودکان را در طراحی محصولات خود لحاظ کنند. این امر شامل مکانیزم‌های تأیید سن دقیق‌تر، تنظیمات حریم خصوصی پیش‌فرض برای کاربران زیر سن قانونی و ابزارهای گزارش‌دهی آسان و مؤثر است.

- استفاده از هوش مصنوعی برای شناسایی: فناوری AI می‌تواند برای شناسایی الگوهای مکالمات اغفال‌گرانه، اسکن و حذف خودکار CSAM و شناسایی حساب‌های کاربری مشکوک به کار گرفته شود. این رویکرد به ویژه برای پایش حجم عظیم داده‌ها در پلتفرم‌های بزرگ ضروری است (سهلانی، نیک‌نفس، و باروطی، ۱۴۰۰: ۱۶۵).

- پیشگیری اجتماعی و آموزشی: این رویکرد بر توانمندسازی افراد و جامعه برای مقابله با جرم تمرکز دارد و مؤثرترین استراتژی بلندمدت محسوب می‌شود.

- آموزش کودکان و نوجوانان (سواد دیجیتال): مهم‌ترین ابزار دفاعی، خود کودک است. آموزش مهارت‌های شهروندی دیجیتال باید به بخشی ثابت از برنامه درسی مدارس تبدیل شود. این آموزش‌ها باید شامل مواردی مانند مدیریت حریم خصوصی، تشخیص اطلاعات نادرست، شناسایی رفتارهای پرخطر و اغفال‌گرانه، و نحوه گزارش‌دهی امن مشکلات باشد (مردانی، باوی، و موالی‌زاده، ۱۴۰۲).

- توانمندسازی والدین و مربیان: والدین و معلمان خط مقدم حفاظت از کودکان هستند، اما بسیاری از آن‌ها فاقد دانش و مهارت کافی در مورد دنیای آنلاین هستند. برگزاری کارگاه‌های آموزشی برای والدین جهت آشنایی با خطرات، نحوه استفاده از ابزارهای نظارتی و چگونگی گفتگوی باز و سازنده با فرزندانشان در مورد امنیت آنلاین، امری حیاتی است (اولز، ۱۴۰۰: ۱۸۰؛ میرزامحمدی، ۱۴۰۲).

- کمپین‌های آگاهی‌بخشی عمومی: رسانه‌های عمومی باید با تولید محتوای مناسب، سطح آگاهی جامعه را در مورد واقعیت‌ها و خطرات جرائم سایبری علیه کودکان افزایش دهند. این کمپین‌ها باید بر از بین بردن کلیشه‌هایی مانند "خطر غریبه‌ها" تمرکز کرده و فرهنگ "گزارش‌دهی" را ترویج دهند و از سرزنش قربانی جلوگیری کنند.

- پیشگیری کیفری و پلیسی: این سطح از پیشگیری به نقش نظام عدالت کیفری در بازدارندگی و پاسخ به جرم می‌پردازد.

- تقویت پلیس سایبری: سرمایه‌گذاری در تجهیز و آموزش تخصصی پلیس سایبری برای رسیدگی به جرائم علیه کودکان ضروری است. این شامل آموزش در زمینه روان‌شناسی کودک، تکنیک‌های مصاحبه با قربانیان خردسال و روش‌های پیشرفته کشف جرائم دیجیتال است.

- همکاری چندنهادی: مقابله با این پدیده پیچیده نیازمند همکاری نزدیک میان پلیس، قوه قضائیه، وزارت آموزش و پرورش، سازمان‌های مردم‌نهاد، ارائه‌دهندگان خدمات اینترنتی و شرکت‌های فناوری است. ایجاد کارگروه‌های مشترک و خطوط ارتباطی سریع می‌تواند به پاسخگویی مؤثرتر کمک کند (کریمیان و حاجی ده‌آبادی، ۱۳۹۵).

- تمرکز بر بازپروری مجرمان: به ویژه در مورد مجرمان نوجوان، رویکرد صرفاً تنبیهی کارساز نیست. برنامه‌های بازپروری، مشاوره روانی و آموزش سواد دیجیتال باید برای این گروه در نظر گرفته شود تا از تکرار جرم در آینده جلوگیری شود (حق‌پناهان، ۱۴۰۳: ۲۵۰).

در نهایت، هیچ یک از این راهبردها به تنهایی کافی نیست. حفاظت از کودکان در فضای مجازی نیازمند یک رویکرد یکپارچه و مسئولیت مشترک میان همه ارکان جامعه است.

نتیجه‌گیری و پیشنهادات

این پژوهش با هدف کالبدشکافی ابعاد پیچیده جرائم سایبری علیه کودکان و نوجوانان، از دو منظر مکمل جرم‌شناسی و بزه‌دیده‌شناسی، به تحلیل این پدیده پرداخت و نشان داد که مواجهه با این معضل نیازمند فراتر رفتن از چارچوب‌های سنتی حقوق کیفری و اتخاذ یک رویکرد جامع‌نگر و پیشگیرانه است. یافته‌های این تحقیق، در وهله نخست، این تصور ساده‌انگارانه و کلیشه‌ای که مجرم سایبری را صرفاً یک «غریبه منحرف» ترسیم می‌کند، به چالش کشید. تحلیل جرم‌شناختی آشکار ساخت که پروفایل فاعلین این جرائم، طیف متنوعی از مجرمان مبتلا به اختلال پدوفیلی با انگیزه‌های ریشه‌دار روانی-جنسی تا مجرمان موقعیتی و حتی خود نوجوانان را در بر می‌گیرد. این واقعیت، دلالت‌های مهمی برای سیاست جنایی دارد؛ زیرا راهبردهای مقابله و پیشگیری باید متناسب با هر یک از این گروه‌ها طراحی شود. تمرکز صرف بر مجرمان بزرگسال و نادیده گرفتن بزهکاری نوجوانان در فضای مجازی، به معنای غفلت از بخش قابل توجهی از چرخه خشونت و آزار آنلاین است.

از سوی دیگر، تحلیل بزه‌دیده‌شناختی نشان داد که قربانی شدن کودکان در فضای مجازی، یک رویداد تصادفی نیست، بلکه برآیند تلاقی مجموعه‌ای از عوامل خطرساز در سطوح فردی، خانوادگی و فناورانه است. آسیب‌پذیری این گروه نه فقط از «ساده‌لوحی» آنان، بلکه از یک عدم تقارن بنیادین قدرت و دانش در اکوسیستم دیجیتال نشأت می‌گیرد. در یک سو، مجرمان با بهره‌گیری از گمنامی، دانش فنی و تکنیک‌های پیچیده مهندسی اجتماعی و اغفال روان‌شناختی قرار دارند و در سوی دیگر، کودکانی که علی‌رغم تسلط فنی بر ابزارهای دیجیتال، فاقد «خرد دیجیتال» و توانایی درک ریسک و تشخیص نیات سوء هستند. این شکاف عمیق، مسئولیت نهادهای حمایتی و قانون‌گذار را برای ایجاد سپرهای محافظتی مضاعف می‌کند. یافته‌ها مؤید آن است که ضعف در نظارت والدین و فقدان آموزش نظام‌مند در حوزه سواد دیجیتال، مهم‌ترین کاتالیزورهایی هستند که آسیب‌پذیری ذاتی کودکان را به بزه‌دیدگی بالفعل تبدیل می‌کنند.

تمرکز ویژه این مقاله بر «پدوفیلی دیجیتال» نشان داد که این پدیده را نمی‌توان صرفاً یک جرم سایبری تلقی کرد؛ بلکه با یک خرده‌ف فرهنگ انحرافی سازمان‌یافته مواجه هستیم که اینترنت را به ابزاری برای شبکه‌سازی، تبادل محتوای مجرمانه (CSAM)، و مهم‌تر از آن، عادی‌سازی و توجیه ایدئولوژی بیمارگونه خود تبدیل کرده است.

اینترنت برای این افراد، نه فقط یک ابزار، که یک زیست‌بوم است که در آن هویت انحرافی خود را بازتولید و تقویت می‌کنند. این امر ثابت می‌کند که رویکردهای تقلیل‌گرایانه و صرفاً «محتوامحور» که بر فیلترینگ و حذف محتوا متمرکز هستند، اگرچه ضروری‌اند، اما به هیچ وجه کافی نیستند. سیاست جنایی باید از مقابله با «محتوا» به سمت مقابله با «رفتار» و «فرآیند» مجرمانه، به ویژه جرم‌انگاری صریح و مؤثر فرآیند اغفال آنلاین، گذار کند.

در نهایت، این پژوهش با تحلیل چارچوب حقوقی ایران، به این نتیجه رسید که هرچند گام‌های مثبتی در قالب قانون جرائم رایانه‌ای و به ویژه قانون حمایت از اطفال و نوجوانان برداشته شده، اما این قوانین همچنان با نوعی تأخر تقنینی نسبت به سرعت تحولات فناوری و پیچیدگی شیوه‌های مجرمانه مواجه‌اند. خلأهای موجود در زمینه جرم‌انگاری رفتارهای مقدماتی مانند گرومینگ، چالش‌های جدی در حوزه ادله اثبات دعوی دیجیتال، و موانع مربوط به صلاحیت قضایی در جرائم فراملی، کارآمدی نظام عدالت کیفری را در مقام پاسخگویی، تضعیف کرده است. پاسخ نظام حقوقی، اغلب واکنشی و پسینی است، در حالی که ماهیت این جرائم، یک رویکرد کنشی، پیشگیرانه و بزه‌دیده‌محور را ایجاب می‌کند.

بر این اساس، این مقاله استدلال می‌کند که حفاظت از کودکان در فضای مجازی، مستلزم گذار از یک الگوی امنیت‌محور و دولت‌پایه، به سوی یک پارادایم حمایتی مبتنی بر «مسئولیت مشترک» است. این پارادایم بر ایجاد یک اکوسیستم حفاظتی سه‌جانبه (حقوقی-فناورانه-اجتماعی) استوار است: ضلع حقوقی آن نیازمند بازنگری قوانین برای جرم‌انگاری صریح رفتارهای نوین، تسهیل همکاری‌های بین‌المللی و اتخاذ رویه‌های قضایی دوستدار کودک است. ضلع فناورانه آن، شرکت‌های فناوری را ملزم به پذیرش مسئولیت اجتماعی و پیاده‌سازی اصول «ایمنی در طراحی» و استفاده از ابزارهای هوشمند برای شناسایی و گزارش محتوا و رفتارهای پرخطر می‌کند. ضلع اجتماعی-آموزشی آن نیز، به عنوان کلیدی‌ترین بخش، بر توانمندسازی کودکان، والدین و مربیان از طریق آموزش فراگیر و مستمر «سواد و شهروندی دیجیتال» به عنوان یک مهارت حیاتی در قرن بیست و یکم تأکید دارد. حفاظت از کودکان در دنیای امروز، دیگر یک گزینه نیست، بلکه یک الزام بنیادین برای تضمین حقوق اساسی و رشد سالم نسلی است که آینده دیجیتال را شکل خواهد داد. ناتوانی در ایجاد این محیط امن، نه تنها یک شکست قانونی، بلکه یک قصور اخلاقی غیرقابل بخشش برای جامعه محسوب خواهد شد.

خلاصه یافته‌ها نشان می‌دهد که:

۱. مجرمان سایبری علیه کودکان، گروهی متنوع هستند. این طیف از مجرمان دارای اختلال پدوفیلی با انگیزه‌های جنسی ریشه‌دار، تا مجرمان فرصت‌طلب و حتی نوجوانان را در بر می‌گیرد. یافته‌های پژوهشی، کلیشه "غریبه خطرناک" را به چالش می‌کشند و نشان می‌دهند که بخش قابل توجهی از مجرمان، نوجوانان و یا افراد آشنا برای قربانی هستند. شیوه‌های عمل آن‌ها، به ویژه تکنیک اغفال آنلاین، بسیار حساب‌شده و فریبنده است.

۲. بزه‌دیدگی کودکان در فضای سایبر، محصول تعامل پیچیده‌ای از عوامل خطرساز است. ویژگی‌های رشدی

و روان‌شناختی کودکان (مانند کنجکاوی و اعتماد)، در کنار عوامل محیطی مانند فقدان نظارت والدین، ضعف ارتباطات خانوادگی و استفاده مشکل‌ساز از فناوری، آسیب‌پذیری آن‌ها را به شدت افزایش می‌دهد. پیامدهای این بزه‌دیدگی، از آسیب‌های عمیق روانی مانند افسردگی و PTSD تا مشکلات اجتماعی و تحصیلی را شامل می‌شود.

۳. پدوفیلی دیجیتال یک تهدید جدی و متمایز است. این پدیده، که تجلی یک اختلال روانی در بستر فناوری است، از طریق مصرف و توزیع گسترده CSAM، شکل‌گیری جوامع آنلاین منحرف و تولید محتوای جدید از طریق زورگیری جنسی، خود را نشان می‌دهد. تحقیقات عصب‌شناختی و روان‌سنجی در حال پرده‌برداری از مبانی بیولوژیک و روان‌شناختی این اختلال هستند.

۴. چارچوب حقوقی و پیشگیرانه موجود، با وجود پیشرفت‌ها، همچنان ناکافی است. خلأهای قانونی در زمینه جرم‌انگاری رفتارهای نوظهور، چالش‌های اثباتی و قضایی، و تمرکز ناکافی بر حمایت از بزه‌دیده، از جمله ضعف‌های نظام حقوقی ایران است.

اهمیت رویکرد یکپارچه

حفاظت از کودکان در فضای مجازی، وظیفه‌ای تک‌بعدی نیست که صرفاً بر دوش پلیس یا نظام قضایی باشد. این یک مسئولیت مشترک است که نیازمند یک رویکرد جامع و هماهنگ میان دولت، قانون‌گذاران، صنعت فناوری، نظام آموزشی، نهادهای مدنی و به ویژه خانواده‌هاست. هیچ راهکار واحدی به تنهایی نمی‌تواند موفق باشد؛ اثربخشی در گرو ترکیبی هوشمندانه از اصلاحات قانونی، پیشگیری فناورانه، آموزش فراگیر و حمایت همه‌جانبه از بزه‌دیدگان است.

پیشنهادات

بر اساس یافته‌های این تحلیل، پیشنهادات زیر برای بهبود وضعیت ارائه می‌گردد:

- در حوزه تقنین و قضا:
- جرم‌انگاری صریح و مستقل "اغفال آنلاین (Grooming)" در قوانین کیفری کشور.
- بازنگری در قوانین به منظور تطبیق با تهدیدات نوظهور مانند دیپ‌فیک و تسهیل همکاری‌های حقوقی بین‌المللی.
- ایجاد دادگاه‌های تخصصی برای رسیدگی به جرائم علیه کودکان با حضور قضات و ضابطان آموزش‌دیده.
- تقویت رویکرد "عدالت ترمیمی" با تمرکز بر جبران خسارت و ترمیم روانی بزه‌دیدگان.
- در حوزه آموزش و فرهنگ‌سازی:
- ادغام اجباری و جامع "سواد دیجیتال و شهروندی آنلاین" در برنامه درسی مدارس از مقاطع ابتدایی.

- اجرای برنامه‌های ملی و مستمر برای توانمندسازی والدین و ارائه ابزارهای عملی به آن‌ها برای مدیریت فعالیت آنلاین فرزندانشان.

- راه‌اندازی کمپین‌های آگاهی‌بخشی گسترده با هدف آموزش عمومی، کاهش انگ گزارش‌دهی و ترویج فرهنگ مسئولیت‌پذیری دیجیتال.

- در حوزه فناوری و نظارت:

- الزام قانونی پلتفرم‌ها و شرکت‌های فناوری به اجرای سیاست‌های "طراحی ایمن" (Safety by Design) و همکاری فعال با نهادهای انتظامی.

- توسعه و سرمایه‌گذاری بر روی فناوری‌های مبتنی بر هوش مصنوعی برای شناسایی و حذف پیشگیرانه محتوای مجرمانه و شناسایی الگوهای رفتاری خطرناک.

- در حوزه پژوهش:

- انجام تحقیقات پیمایشی و میدانی در ایران برای درک بهتر شیوع بزه‌دیدگی سایبری، شناسایی دقیق‌تر پروفایل مجرمان و قربانیان داخلی، و ارزیابی اثربخشی برنامه‌های پیشگیرانه موجود.

آینده کودکان ما به میزان زیادی به توانایی ما در ایجاد یک محیط دیجیتال امن، مسئولانه و توانمندساز بستگی دارد. این مهم، جز با عزم ملی، همکاری بین‌بخشی و آگاهی عمومی محقق نخواهد شد.

منابع

الف) منابع فارسی

۱. ابوذری، مهرنوش. (۱۳۹۵). جرم‌شناسی جرایم سایبری. تهران: میزان.

۲. امیریان‌فارسانی، امین؛ مالمیر، محمود. (۱۳۹۵). جرم‌شناسی جرایم سایبری از منظر پیشگیری. تهران: مجد.

۳. اولز، یلدا. (۱۴۰۰). مادران رسانه‌ای، پدران دیجیتال: آیا شبکه‌های اجتماعی فرزندان ما را خراب می‌کنند؟ (ترجمه راضیه نیک‌طلب). تهران: انتشارات اگر.

۴. باباحسن زاده، نیلوفر. (مقاله پژوهشی). «بزهکاری اطفال و نوجوانان در تاثیر فضای سایبری (مطالعهٔ موردی)». فصلنامه علمی فقه و حقوق نوین.

۵. پوریان، حامد؛ احدی، فاطمه؛ بیگی، جمال. (۱۴۰۳). «گونه شناسی بزه دیدگی سایبری کودکان در مناطق زاغه‌نشین». چهارمین کنفرانس ملی پدافند سایبری.

۶. حق‌پناهان، عباس. (۱۴۰۳). جرم‌شناسی بزهکاری اطفال و نوجوانان. تهران: انتشارات مجد.

۷. خدایی‌فر، فاطمه؛ بیرقی، نرگس. (۱۳۸۸). «گزارش یک مورد درمان بیمار مبتلا به پدوفیلی همراه با عقب‌ماندگی ذهنی و اختلال خلقی دو قطبی». پژوهش‌های نوین روانشناختی.

۸. خلج‌آبادی فراهانی، فریده. (۱۳۹۸). «مواجهه با محتوای خارج عرف جنسی (پورنوگرافی) در اینترنت و فضای مجازی و تأثیرات رفتاری در نوجوانان در تهران». خانواده‌پژوهی، ۱۵(۱)، ۱۲۷-۱۵۳.

۹. رحمتی، صمد؛ سیفی، رضوان. (۱۴۰۰). «شیوع‌شناسی و بررسی عوامل خطرساز و حفاظت‌کننده مزاحمت سایبری با رویکرد تحولی: یک مطالعه مروری روایتی». رویش روانشناسی، ۱۰(۱۱).

۱۰. رفیعی کشتلی، محمود. (۱۳۹۰). بزه‌دیده کودکان در جرایم رایانه‌ای. (پایان‌نامه کارشناسی ارشد). دانشگاه قم.

۱۱. سهلانی، حسین؛ نیک‌نفس، علی؛ باروطی، اکرم. (۱۴۰۰). پایش و تحلیل جرم سایبری. تهران: دانشگاه علوم انتظامی.

۱۲. صفرزاده رودسری، میثم. (۱۳۹۶). جرایم سایبری: ظهور و بروز تا افزایش و فراوانی. تهران: آفتاب گیتی.

۱۳. فرهادی آلاشتی، زهرا. (۱۴۰۱). «برساخت قضایی کنترل جرائم سایبری کودکان و نوجوانان: به‌سوی ارائهٔ نظریه‌ای داده‌بنیاد». مطالعات حقوق کیفری و جرم‌شناسی، ۵۲(۶)، ۲۷۹-۳۰۰.

۱۴. فرهادی آلاشتی، زهرا؛ جوان جعفری بجنوردی، عبدالرضا؛ سیدزاده ثانی، سید مهدی. (۱۴۰۲). «برساخت قضایی کنترل جرائم سایبری کودکان و نوجوانان: به سوی ارائهٔ رویکردی حقوقی-جرم‌شناسانه». پژوهش حقوق کیفری، (۴۳).

۱۵. فروغیان، منصوره؛ عابدی، نفس. (۱۴۰۴). «تحلیل حقوقی بزهکاری و بزه دیدگی سایبری علیه زنان و اطفال در نظام کیفری ایران». بیستمین همایش ملی حقوق، روانشناسی، علوم اجتماعی و علوم انسانی، شیروان.

۱۶. کریمی، مژگان. (۱۳۹۷). بررسی وضعیت کودکان در جرایم هرزهنگاری و سایبری. (پایان‌نامه کارشناسی ارشد). دانشگاه آزاد اسلامی واحد شاهرود.

۱۷. کریمیان، پروانه؛ حاجی ده‌آبادی، محمدعلی. (۱۳۹۵). «بزه دیدگی کودکان و نوجوانان در فضای مجازی و راهکارهای حقوقی مقابله با آن». کنگره بین‌المللی جامع حقوق ایران.

۱۸. کهندانی، محسن. (۱۳۹۲). حمایت کیفری از کودکان و نوجوانان در قبال بزه‌دیدگی در فضای مجازی در حقوق ایران و اسناد بین‌المللی. (پایان‌نامه). موسسه علوم قضایی و خدمات اداری دادگستری.

۱۹. گرکی، مارکو. (۱۳۸۹). جرایم سایبری: راهنمایی برای کشورهای در حال توسعه. تهران: پلیس امنیت فضای تولید و تبادل اطلاعات ناجا.
۲۰. گل‌می‌نیا، محمدصادق. (۱۴۰۳). جرائم رایانه‌ای، سایبری و فضای مجازی. تهران: نسل روشن.
۲۱. مدیری، ناصر؛ واثقی‌پناه، مهرنوش. (۱۳۹۶). جرم‌شناسی سایبری: امنیت، مدل‌سازی تهدیدات و جرم‌شناسی شبکه. تهران: مهرگان قلم.
۲۲. مردانی، سعید؛ باوی، محمود؛ موالی‌زاده، سید باسم. (۱۳۹۲). زمینه‌های جرم‌شناسی جرایم سایبری علیه کودکان. (پایان‌نامه کارشناسی ارشد). دانشگاه آزاد اسلامی واحد تهران مرکزی.
۲۳. مردانی، سعید؛ باوی، محمود؛ موالی‌زاده، سید باسم. (۱۴۰۲). «زمینه‌های جرم‌شناسی جرایم سایبری علیه کودکان». مقاله نمایه شده در ElmNet.
۲۴. مقاله کنفرانسی. (حدود ۱۴۰۲-۱۴۰۳). «کودک‌آزاری آنلاین و اقدامات پیشگیرانه و حمایتی». نمایه شده در سیویلیکا.
۲۵. مودب، زکیه. (بدون تاریخ). «تأثیر فضای مجازی در افزایش خشونت جنسی کودکان و نوجوانان». مقاله پژوهشی نمایه شده در Magiran.
۲۶. مولائی کوچه‌باغ، میرمهدی. (۱۴۰۴). «بررسی حقوقی جرایم سایبری علیه کودکان و نوجوانان و مکانیسم‌های حمایتی». اولین همایش بین‌المللی مطالعات علمی در علوم انسانی، مدیریت و حقوق.
۲۷. میرزامحمدی، الهه. (۱۴۰۲). «بررسی جرم‌شناختی بزه‌دیدگی اطفال در فضای سایبری». هفتمین کنفرانس بین‌المللی فقه، حقوق، روانشناسی و علوم تربیتی.

ب) منابع انگلیسی

28. Arsawati, I. N. J., Darma, I. M. W., & Antari, P. E. D. (2021). A criminological outlook of cyber crimes in sexual violence against children in Indonesian laws. International Journal of Criminology and Sociology, 10, 26.
29. Dombert, B., Antfolk, J., Kallvik, L., Zappalà, A., Osterheider, M., Mokros, A., & Santtila, P. (2015). Identifying pedophilic interest in sex offenders against children with the indirect choice reaction time task. European Journal of Psychological Assessment.
30. Gupta, A., Kumaraguru, P., & Sureka, A. (2012). Characterizing pedophile conversations on the Internet using online grooming. arXiv preprint arXiv:1208.4324.
31. Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime victimization and problematic social media use: Findings from a nationally representative panel study. American Journal of Criminal Justice, 46, 862–881.
32. Popovic, D., Wertz, M., Geisler, C., Kaufmann, J., Lähteenvuo, M., Lieslehto, J., Schiltz, K. (2023). Patterns of risk—Using machine learning and structural neuroimaging to identify pedophilic offenders. Frontiers in Psychiatry, 14, Article 1001085.
33. Seto, M. C., et al. (2006). Child pornography offenses are a valid diagnostic indicator of pedophilia. Journal of Abnormal Psychology.
34. Schmidt, A. F., Babchishin, K. M., & Lehmann, R. J. B. (2017). A meta-analysis of viewing time measures of sexual interest in children. Archives of Sexual Behavior, 46(1), 287–300. https://doi.

org/10.1007/s10508-016-0806-3
35. Sutton, S., & Finkelhor, D. (2024). Perpetrators' identity in online crimes against children: A meta-analysis. Trauma, Violence, & Abuse, 25(3), 1756–1768. https://doi.org/10.1177/15248380231194072