Victim-Centered Prevention of Sexual Grooming of Children and Adolescents in Cyberspace

Abstract

In the contemporary era, alongside the rapid development of cyberspace and the emergence of new technologies, this domain has transformed into a realm for criminal behavior. Among different groups, children and adolescents, due to their age-specific characteristics and particular psychological conditions, are more exposed to various forms of victimization than other social groups, especially within the context of virtual space. One of the most significant manifestations of these threats is the phenomenon of "online sexual grooming and enticement," in which an adult, by employing a range of deceptive measures and leveraging psychological manipulation techniques, seeks to establish a relationship with a minor and victimize them. Although these acts are often considered preliminary crimes, they can pave the way for the commission of more severe crimes against children. This offense, which was first criminalized by the legislature in the year 2020 [1399 in the Iranian calendar], is among the emerging challenges in the cyber domain, and combating it requires the adoption of comprehensive and effective preventive strategies.

The present research, utilizing a library research method and through a systematic review of literature, has sought to analyze and explain integrated preventive strategies at both the macro and micro levels. The findings of the study indicate that the most effective preventive strategies at the macro level include implementing educational-promotional programs in the institutions of family, school, and media; reviewing and reforming legislative policies and judicial procedures; creating safe virtual environments specifically for children; and strengthening specialized cyber police units. At the micro level, key strategies include implementing parental interventions, applying smart restrictions on children's access to the virtual space, enhancing security protocols, and developing exclusive SIM cards for children.

Finally, it can be asserted that combating this phenomenon requires national resolve and the simultaneous implementation of legal, technical, and cultural strategies at all levels, thereby achieving the protection of children's privacy and guaranteeing their mental well-being in cyberspace.

Keywords: Sexual Grooming, Cyberspace, Victimization, Children and Adolescents, Prevention

پیشگیری بزه‌دیده مدار از اغفال جنسی کودکان ونوجوانان در فضای سایبر

چکیده

همگام با توسعه فزاینده فضای سایبر و گسترش شبکه‌های اجتماعی، این عرصه به بستری برای وقوع جرائم نوظهور تبدیل شده است. کودکان و نوجوانان به لحاظ ویژگی‌های رشدی و روانشناختی، در معرض آسیب‌پذیری بیشتری در برابر این تهدیدات قرار دارند. از مصادیق بارز این آسیب‌ها، «اغفال و اغوای جنسی سایبری» است که در آن فرد بزرگسال با به‌کارگیری شیوه‌های فریبنده و تکنیک‌های دستکاری روانی، درصدد ایجاد رابطه با کودک برمی‌آید. این پژوهش با بهره‌گیری از روش تحلیلی-توصیفی و با مطالعه منابع کتابخانه‌ای، به تبیین راهبردهای پیشگیرانه در دو سطح می‌پردازد. یافته‌های تحقیق نشان می‌دهد در سطح اول (راهبردهای حاکمیتی و نهادی)، راهکارهای مؤثر شامل تدوین و بازنگری قوانین بازدارنده، تقویت نهادهای نظارتی، توسعه پلتفرم‌های امن ویژه کودکان، اجرای برنامه‌های آموزشی در مدارس و رسانه‌های ملی، و گسترش گشت‌های تخصصی پلیس سایبری است. در سطح دوم (راهبردهای خانواده‌محور)، مداخلاتی نظیر مدیریت فعال دسترسی، ایمن‌سازی حساب‌های کاربری، استفاده از نرم‌افزارهای کنترلی، و اجرای برنامه‌های آموزشی در محیط خانواده شناسایی شد. در نتیجه، مقابله کارآمد با این پدیده مستلزم عزم ملی و اجرای همزمان راهکارهای حقوقی، فنی و فرهنگی در چارچوب یک نظام جامع حمایتی است تا از این طریق، صیانت از کودکان و تضمین سلامت روانی آنان در فضای سایبر میسر گردد.

واژگان کلیدی: اغفال جنسی، فضای سایبری، بزه‌دیدگی، کودکان و نوجوانان، پیشگیری

مقدمه

فضای سایبری، به مثابه یک ابرساختار جهانی پیچیده و درهم‌تنیده، متشکل از شبکه‌های رایانه‌ای، زیرساخت‌های دیجیتال و مجموعه‌ای از تعاملات انسانی است که در بستری مجازی و مبتنی بر داده صورت می‌پذیرد. پیشرفت شتابان فناوری‌های دیجیتال، به ویژه با ظهور مفاهیمی چون کلان‌داده[1] ، هوش مصنوعی، و اینترنت اشیاء، موجب تکامل کیفی این فضا از یک کانال ارتباطی ساده به یک اکوسیستم اجتماعی–فنی همه‌جانبه شده است. این تحول، تنها در بعد فنی محدود نمانده، بلکه منجر به دگرگونی ژرف در پارادایم‌های اقتصادی، فرهنگی و اجتماعی گردیده است و بازتعریف مفاهیم بنیادینی چون حریم خصوصی، هویت و شهروندی، همگی از پیامدهای این گذار به شمار می‌روند. پیشرفت فناوری‌های ارتباطی و دموکراتیزه شدن دسترسی به فضای مجازی، به کاهش مستمر و قابل‌ملاحظه سن استفاده‌کنندگان از محیط‌های دیجیتال، به‌ویژه پلتفرم‌های تعاملی، انجامیده است. در این میان، کودکان و نوجوانان به‌عنوان یکی از آسیب‌پذیرترین اقشار جامعه، مستلزم حمایت‌ها و مداخلات مراقبتی هدفمند در عرصه سایبری هستند. این ضرورت از آنجا نشئت می‌گیرد که فضای مجازی در مقایسه با جهان فیزیکی، به مراتب ناهموارتر، غیرشفاف‌تر و مملو از مخاطرات پنهان است و پیامدهای زیانبار مواجهه با آن می‌تواند آثار روانی–اجتماعی عمیق‌تر و گاه جبران‌ناپذیری بر این گروه بر جای نهد. ویژگی‌های شناختی و هیجانی کودکان و نوجوانان مانند کم‌تجربگی و دانش ناکافی، آسیب‌پذیری آنان را در برابر بزه افزایش می‌دهد. تأثیرپذیری سریع از محیط و حساسیت بالا به مخاطرات، این آسیب‌پذیری را تشدید می‌کند. در نتیجه، این گروه سهم نامتناسبی در آمار هر دو حوزه بزهکاری و بزه‌دیدگی، چه در جرائم سنتی و چه مدرن، به خود اختصاص می‌دهند(محسنی،۱٤۰۰: ۱۱۲). بی‌تردید، ضعف در دانش پایه‌ای استفاده از اینترنت، سطح نازل سواد رسانه‌ای، افشای غیرمسئولانه اطلاعات شخصی و بهره‌گیری از فضای سایبری برای مقاصد غیراخلاقی، از جمله چالش‌برانگیزترین مخاطراتی است که کاربران نوجوان را در محیط‌های دیجیتال تهدید می‌کند(ایقانی و دیگران،۱٤۰۱: ۱۱٤). بزه‌دیدگی سایبری کودکان را می‌توان به لحاظ ماهوی به انواع جنسی، عاطفی و روانی تقسیم‌بندی نمود که این طبقه‌بندی بر مبنای الگوهای رفتاری، واکنش‌ها و کیفیت تعاملات کاربران در فضای سایبری صورت پذیرفته و شدت و گستره آن متغیر است(کرامتی معز،۱۳۹۹: ۱٤). بزه‌دیدگی سایبری کودکان در شبکه‌های اجتماعی به شرایطی اطلاق می‌شود که در آن کاربران کم‌سال در حین فعالیت‌های آنلاین در معرض تعاملات پرخطر و بالقوه آسیب‌زا قرار می‌گیرند. مطالعات علمی نشان می‌دهد این پدیده عموماً شامل مواجهه با درخواست‌های جنسی نامتعارف، گفت‌وگوهای با محتوای نامناسب و تحت فشار قرار گرفتن برای افشای اطلاعات شخصی می‌شود که در پلتفرم‌هایی نظیر اینستاگرام با فراوانی بیشتری مشاهده می‌گردد.

بزه‌دیدگی جنسی را می‌توان در زمرهٔ شایع‌ترین و در عین حال مخرب‌ترین اشکال قربانی شدن به شمار آورد که اغلب با پیامدهای بلندمدت و در موارد متعددی غیرقابل جبران برای بازماندگان همراه است. این پیامدها، ماهیتی چندبعدی و گسترده داشته و طیفی از آسیب‌های جسمانی، هیجانی و نیز اختلال در سلامت روانی را در سراسر عمر بزه‌دیده در بر می‌گیرد(شاهپوری وبشیریه،۱٤۰٤: ۲۸۱).

[1] Big data

دامنه این پدیده در موارد متعددی از مرزهای تعاملات مجازی فراتر رفته و به عرصه فیزیکی گسترش می‌یابد. نمونه‌هایی همچون ارسال محتوهای غیراخلاقی به شیوه فیزیکی، انجام تماس‌های تلفنی ناخواسته یا درخواست ملاقات‌های حضوری از مصادیق این انتقال به شمار می‌روند. از منظر آسیب‌شناختی، می‌توان پیامدهای این نوع از بزه‌دیدگی را در دو محور اصلی مورد تحلیل قرار داد: اول آسیب‌های جنسی شامل اشکال مختلف بهره‌کشی و سوءاستفاده، و دوم آسیب‌های روانی-هیجانی که ناشی از فشارهای روانی و هیجانات منفی حاصل از این تعاملات می‌باشد. این پیامدها قادرند اثرات عمیق و ماندگاری بر سلامت روان و تکامل اجتماعی کودکان بر جای گذارند.

در عصر حاضر، شاهد ظهور و گسترش پدیده‌ای نگران‌کننده در حوزه آسیب‌شناسی فضای مجازی کودکان هستیم که در ادبیات پژوهشی معاصر تحت عنوان «اغوای جنسی سایبری»[1] شناخته می‌شود. این شکل خاص از بزه‌دیدگی چندبعدی که همزمان ابعاد جنسی و روانی-عاطفی را دربرمی‌گیرد، به‌عنوان یکی از چالش‌های نوظهور در حوزه حقوق کیفری، جرم شناسی و بزه‌دیده شناسی سایبری و روانشناسی کودک مورد توجه پژوهشگران قرار گرفته است. این فرآیند که پیشتر در نظام‌های حقوق کیفری کشورهای مختلف[2] و اسناد بین‌المللی متعدد[3] مورد توجه قرار گرفته بود، سرانجام در بند ۹ ماده ۱۰ قانون حمایت از اطفال و نوجوانان مصوب سال ۱۳۹۹ به صورت رسمی مورد تقنین قرار گرفت.[4] بر اساس تعریف وزارت دادگستری ایالات متحده، اغفال جنسی کودکان فرایندی سیستماتیک شامل ایجاد اعتماد با کودک و بزرگسالان مرتبط به منظور تسهیل دسترسی و ایجاد فرصت‌های انفرادی با کودک است. در اشکال شدید، این روند ممکن است به استفاده از تهدید یا اعمال زور فیزیکی برای سوءاستفاده جنسی منجر شود. مجرمان معمولاً با اتخاذ نقش مراقبتی، برقراری دوستی، یا سوءاستفاده از موقعیت‌های اعتمادی و اقتداری، به جلب پذیرش کودک می‌پردازند. این افراد عمدتاً با هدف قرار دادن کودکان کمتر تحت نظارت یا ایجاد رابطه با بزرگسالان پیرامون کودک، احتمال دستیابی به فرصت‌های انفرادی با قربانی را افزایش می‌دهند(بافقی و سرشکی،۱۴۰۱: ۲۰۳).

پژوهش حاضر با عبور از رهیافت‌های کلاسیک پیشگیری (اجتماعی و وضعی) که بر تقسیم‌بندی‌های اولیه و ثانویه متمرکز هستند، پارادایمی نوآورانه را دنبال می‌کند. محوریت این مطالعه بر شناسایی و تحلیل اقدامات عملیاتی، کارآمد و قابلیت‌گذاری است که مستقیماً بر تقویت ظرفیت‌های خودمراقبتی و تاب‌آوری کودکان در برابر بزه‌دیدگی متمرکز می‌باشند. این رویکرد مبتنی بر

---

[1] Cyber grooming/Child online grooming

[2] بنگرید به:

-Kaylor, L. E., Winters, G. M., Jeglic, E. L., & Cilli, J. (2023). **An analysis of child sexual grooming legislation in the United States**. *Psychology, Crime & Law*, *29*(9), pp:982-1000

[3] بنگرید به:

داشاب،مهریار(۱۳۹۷). **تاملی بر کنوانسیون لانزاروته شورای اروپا در خصوص حمایت از کودکان در برابر استثمار و سوء استفاده جنسی**. فصلنامه پژوهش حقوق عمومی، ۲۰(۶۰)، صص.۱۲۵-۱۵۵.

[4] «برقراری ارتباط با طفل و نوجوان در فضای مجازی به منظور هرگونه آزار جنسی یا ارتباط جنسی نامشروع به یکی از مجازات های درجه شش قانون مجازات اسلامی»

توانمندسازی فعالانه قربانیان بالقوه، گامی فراتر از مداخلات پیشگیری واکنشی محسوب شده و بر طراحی راهبردهای پرواکتیو و کاربردی تأکید می‌ورزد.

اگرچه پژوهش های متعددی در حوزه پیشگیری از بزه‌دیدگی کودکان در فضای سایبر به قلم تحریر در آمده است[1] لکن پژوهش حاضر با تمرکز ویژه بر پدیده اغفال و اغوای جنسی سایبری، به عنوان گونه‌ای خاص و پیچیده از بزه‌دیدگی مراوداتی کودکان و نوجوانان، از ادبیات عمومی پیشگیری از بزه‌دیدگی سایبری فاصله گرفته است. این مطالعه با شناسایی خلأ پژوهشی موجود در زمینه مداخلات هدفمند، درصدد ارائه راهبردهای عملیاتی و کاربردی برای مقابله با این شکل خاص از بزه‌دیدگی است که مستلزم رویکردی متمایز و تخصصی‌تر نسبت به سایر انواع بزه‌دیدگی‌های سایبری می‌باشد. سؤال اصلی پژوهش حاضر بر شناسایی کارآمدترین راهبردهای پیشگیری اجتماعی و وضعی در مقابله با بزه‌دیدگی کودکان در پدیده اغفال جنسی سایبری متمرکز است. این تمرکز تخصصی، تمایز بنیادینی با مطالعات عمومی حوزه پیشگیری از بزه‌دیدگی سایبری ایجاد کرده و ضرورت پژوهش حاضر را توجیه می‌نماید.

سطح اول: راهکارهای فرابخشی و نهادی

راهبردهای فرابخشی و نهادی، به اقدامات کلان، هماهنگ و ساختاریافته‌ای اشاره دارد که توسط نهادهای حاکمیتی و قانون‌گذار (مانند دولت، قوه قضائیه و نهادهای ناظر) طراحی و اجرا می‌شوند. این راهبردها با هدف ایجاد زیرساخت امن، چارچوب‌های حقوقی و سازوکارهای نظارتی فراگیر تدوین شده و مستلزم همکاری بین‌بخشی و سیاست‌گذاری یکپارچه برای مقابله با پدیده اغفال جنسی سایبری کودکان است. از جمله مصادیق این راهبردها می‌توان به تصویب و بازنگری قوانین بازدارنده، تقویت نهادهای نظارتی، توسعه پلتفرم‌های اختصاصی امن برای کودکان، اجرای برنامه‌های آموزشی در سطح مدارس و رسانه‌های ملی، و گسترش گشت‌های تخصصی پلیس سایبری اشاره کرد که در سه قسمت در ذیل توضیح داده خواهد شد.

۱. راهبردهای قانونی، قضایی و انتظامی

اصلاح ساختار قوانین جزایی به منظور ارتقای کارایی نظام عدالت کیفری در مواجهه با پدیده جرم، از جمله ضروریات انکارناپذیر در حوزه حقوق کیفری معاصر محسوب می‌شود(Dandurand,2014:384). با توجه به تحولات پیچیده اجتماعی و فناورانه در عصر حاضر، شاهد ظهور اشکال نوینی از بزهکاری هستیم که مستلزم بازنگری بنیادین در سیاست‌گذاری کیفری می‌باشد. قوانین موجود

---

[1] بهره‌مند و همکاران (۱۳۹۳) در پژوهشی با عنوان «***راهبردهای وضعی پیشگیری از جرایم سایبری***»، به تحلیل و واکاوی تکنیک‌های پیشگیری وضعی — مبتنی بر چارچوب نظری رونالد کلارک — پرداخته و این راهبردها را با شرایط و مقتضیات جرایم سایبری عام تطبیق و تبیین نمودند.

-در ادامه، حیدری‌نژاد (۱۳۹۷) در تحقیق خود تحت عنوان «***پیشگیری وضعی از جرایم سایبری از منظر حقوق کیفری ایران و جهان***»، به بررسی ضرورت‌ها و بسترهای اجرایی پیشگیری وضعی در نظام حقوقی ایران پرداخته و آن را در چارچوب مطالعه تطبیقی با موازین بین‌المللی مورد سنجش قرار داد.

-احمدی‌نژاد و احمدی موسوی (۱۳۹۹) در مقاله‌ای با عنوان «***راهکارهای پیشگیرانه از بزه‌دیدگی اطفال در فضای سایبری***»، ابتدا به تبیین مبانی نظری و مفهومی موضوع همت گماشته و در ادامه، با رویکردی علت‌شناسانه به تحلیل عوامل بزهدیدگی پرداختند که نهایتاً به ارائه راهکارهای پیشگیرانه عام در محیط مجازی منجر شد.

-مطالعه عباسی و رنگچی تهرانی (۱۳۹۸) با عنوان «***پیشگیری از بزه‌دیدگی کودکان و نوجوانان در مواجهه با جرایم جنسی***»، عمدتاً بر راهکارهای پیشگیری کیفری در محیط فیزیکی (واقعی) متمرکز گردیده است.

-در نهایت، رضوی فرد و همکاران (۱۳۹۷) در پژوهشی تحت عنوان «***پیشگیری از بزه‌دیدگی جنسی در شبکه‌های اجتماعی***»، راهکارهای عملی و تقنینی جهت مصونیت کودکان در پلتفرم‌های شبکه‌های اجتماعی، به‌ویژه فیسبوک و توییتر، را مورد مداقه و بررسی قرار دادند.

عمدتاً قادر به پاسخگویی مؤثر به این تحولات نبوده و این ناکارآمدی به وضوح در سطوح مختلف از پیشگیری اولیه تا مرحله اجرای احکام قضایی قابل مشاهده است(tarovet al,2023:188).

مطالعات حقوق تطبیقی نشان می‌دهد که نظام‌های پیشرفته عدالت کیفری به سمت اتخاذ رویکردهای پویا و انعطاف‌پذیر در تقنین گرایش یافته‌اند. این رویکردها عمدتاً شامل به‌روزرسانی مستمر مقررات کیفری با توجه به تحولات اجتماعی، بکارگیری فناوری‌های نوین در کشف جرایم و جمع‌آوری ادله، و همچنین استقرار مکانیسم‌های دادرسی مبتنی بر شواهد علمی می‌شود. چنین تحولاتی بیانگر ضرورت بازنگری در نظام‌های قضایی برای مواجهه مؤثر با چالش‌های نوظهور در عرصه جرائم مدرن است(Kaylor et al,2023:1000). در این میان، توجه به یافته‌های جرم‌شناسی نوین و مطالعات بزه‌دیده شناسی در تدوین سیاست‌های کیفری از اهمیت ویژه‌ای برخوردار است. از منظر دکترین حقوقی، نوسازی قوانین جزایی می‌بایست با در نظر گرفتن اصول بنیادین حقوق کیفری از جمله اصل قانونمندی جرایم و مجازات‌ها، اصل تناسب و همچنین اصل فردی کردن مجازات‌ها صورت پذیرد. این فرآیند مستلزم همکاری میان‌رشته‌ای حقوق‌دانان، جرم‌شناسان، روان‌شناسان کیفری و متخصصان فناوری اطلاعات می‌باشد. تجربیات نظام‌های حقوقی پیشرو حاکی از آن است که اصلاحات جزایی موفق عمدتاً از رویکردی همه‌جانبه و مبتنی بر پژوهش‌های تجربی بهره برده‌اند. لذا باید تأکید نمود که کارآمدسازی نظام عدالت کیفری در گرو بازتعریف هوشمندانه قوانین جزایی با توجه به مقتضیات عصر حاضر بوده و این مهم تنها از طریق اتخاذ رویکردی علمی، بین‌رشته‌ای و آینده‌نگر محقق خواهد شد. چنین تحولی مستلزم عزم جدی قانونگذاران، همراهی جامعه علمی و مشارکت نهادهای مدنی می‌باشد(Kesuma, 2024:760). با توجه به تشدید روزبه‌روزِ جرائم سایبری که قربانیان اصلی آن کودکان هستند و به شکل ویژه‌ای مسئله استثمار آنلاین آنان را نشانه رفته است، احساس نیاز به وضع قانونی ویژه و همه‌جانبه در این عرصه، شدت یافته است. چنین قانونی باید با رویکردی حمایتی و پیشگیرانه، علاوه بر تبیین شفاف مصادیق جرم، چارچوب‌های عملیاتی مؤثری را برای مهار این معضل طراحی کند. در این مسیر، استقرار سازوکارهای پیشگیرانه از قبیل ملزم کردن پلتفرم‌های اینترنتی به بهره‌گیری از سیستم‌های فیلترینگ پیشرفته و شناسایی هوشمند محتوای آسیب‌زا، گسترش برنامه‌های آموزش سواد دیجیتال برای خردسالان، اولیاء و معلمان، و همچنین راه‌اندازی پلتفرم‌های نظارتی مبتنی بر فناوری‌های نوین، از اقدامات کلیدی به شمار می‌روند. افزون بر این، لازم است این قانون نهادهای دولتی را مکلف به تشکیل ساختارهای تخصصی مانند پلیس ویژه جرائم سایبری کودکان، پایگاه‌های پایش و رصد جرائم مرتبط، و خطوط اعلام سریعِ تخلفات نماید. همچنین، با در نظر گرفتن تأثیر چشمگیر نهادهای غیردولتی در کشف و پیشگیری از اینگونه جرائم، قانون باید بسترهای حقوقی لازم برای مشارکت مؤثر این سازمان‌ها در فرآیندهای اعلام جرم، پیگیری قانونی و ارائه خدمات امدادی به آسیب دیدگان را مهیا سازد. تحقق چنین چشم‌انداز جامعی، نیازمند همکاری فرابخشی میان ارگان‌های قضائی، حکومتی و جامعه مدنی در قالب یک سیستم یکپارچه حفاظتی است تا بتواند ایمنی دیجیتال کودکان را در فضای مجازی تضمین کند. این رویکرد نه تنها نیازهای کنونی جامعه در برخورد با تهدیدات نوپدید سایبری را برطرف می‌سازد، بلکه با معیارهای بین‌المللی حمایت از حقوق کودک نیز همخوانی دارد.

اغفال جنسی سایبری کودکان به عنوان شکلی پیچیده از قربانی‌سازی دیجیتال، مستلزم پاسخ‌های تقنینی هدفمند است. خلأهای تقنینی در مورد این جرم در دو محور قابل ردیابی است: اول، دشواری‌های اثبات جرم ناشی از ماهیت پیچیده ادله دیجیتال؛ و دوم، عدم شفافیت در مسئولیت پلتفرم‌های دیجیتال. راهکارهای تقنینی پیشنهادی در چهارچوبی نظام‌مند قابل ارائه است. در سطح جرم انگاری، ضروری است تمامی رفتارهای زمینه ای اغفال جنسی و مراوادات با کودکان به‌عنوان جرمی مستقل با تعریفی جامع شناسایی شود که تمامی فضاهای نوظهور (متاورس[1]، پلتفرم‌های رمزنگاری‌شده) را پوشش دهد و مجازات‌هایی متناسب با آسیب روانی واردشده – حتی در غیاب سوءاستفاده فیزیکی – پیش‌بینی کند. در بعد اجرایی، الزام ارائه‌دهندگان خدمات به نصب سیستم‌های تشخیص الگو مبتنی بر هوش مصنوعی و گزارش‌دهی اجباری محتوای مشکوک به نهادهای ملی، همراه با ایجاد پلیس تخصصی سایبری کودکان دارای اختیارات عملیات تحت پوشش و دسترسی سریع به داده‌ها (با مجوز قضایی) ضروری است. تحول مؤثر مستلزم سه محور روزآمدسازی مقررات تقنینی، ادغام فناوری‌های پیشرفته رصد و تحلیل داده در سازوکارهای اجرایی، و نهادینه‌سازی سواد رسانه‌ای در برنامه‌های درسی ملی میباشد.

نهادهای متعددی در عرصه جامعه، نقشی اساسی در مهار پدیده جرم ایفا می‌کنند. در این میان، پلیس به عنوان نهادی محوری شناخته می‌شود که بر پایه هنجارهای حقوقیِ از پیش تعیین شده، به ویژه مستند به بند ۸ ماده ٤ قانون نیروی انتظامی جمهوری اسلامی ایران (مصوب ۱۳٦۹)، در سرتاسر فرآیند مقابله با پدیده مجرمانه، تکلیف و مسئولیت قانونی یافته است. بر این اساس، پلیس مکلف است هم در مراحل پیشینی (قبل از ارتکاب جرم) و هم در مراحل پسینی (پس از ارتکاب جرم)، در جهت کاهش و مهار این پدیده گام بردارد(خواجه نوری و نیازپور،۱٤۰۳: ۱۵۵). مورد بعد در ذیل این قسمت استقرار سازوکارهای گشت‌زنی اینترنتی و تشکیل پلیس سایبری میباشد که امکان نظارت نظام‌مند بر فعالیت‌های فضای مجازی و پیشگیری از وقوع طیف گسترده‌ای از جرائم سایبری را فراهم می‌آورد. به‌طور مثال، در ساختار پلیس فتا، واحد تخصصی با عنوان «دایره پیشگیری و سازماندهی» با به‌کارگیری کارآگاهان مجرب در زمینه علوم جنایی و فناوری اطلاعات، مسئولیت رصد مستمر پایگاه‌های اینترنتی و تحلیل محتوای منتشرشده در آنها را بر عهده دارد. این فرآیند مستلزم تأیید انطباق فنی وب‌سایت‌ها با استانداردهای امنیتی اجباری بوده و پلیس در برخورد با جرائم آشکار– شامل اما نه محدود به تبلیغ مواد روان‌گردان، انتشار محتوای مستهجن، ترویج مصرف مواد مخدر، ترویج باورهای ضد دینی و شیطان‌پرستی، و نیز تبلیغات ضد حاکمیتی مغایر با نظام سیاسی کشور– با تکیه بر چارچوب قانونی، اقدامات قضایی لازم را به اجرا می‌گذارد. این اقدامات شامل مستندسازی و گزارش‌دهی به مراجع قضایی صالح، هماهنگی با کارگروه‌های تخصصی تعیین‌شده در قوانین مرتبط، و اعمال مکانیسم‌های مسدودسازی و پالایش محتوا می‌شود(گلمحمدی خامنه،۱۳۸۵: ۱۲۱). به عنوان یکی از راهکارهای محوری در راستای پیشگیری از بزه‌دیدگی کودکان در تعاملات برخط، استقرار یگان تخصصی پلیس سایبری با مأموریت گشت‌زنی

---

[1] «**Metaverse**» متاورس به عنوان یک محیط مجازی سه‌بعدی تعاملی تعریف می‌شود که در آن کاربران قادر به برقراری ارتباط و تعامل اجتماعی هستند. این مفهوم، تقاطعی میان جهان دیجیتال و فیزیکی محسوب می‌شود و از لحاظ ریشه‌شناسی، ترکیبی از واژه یونانی «Meta» به معنای «فراتر» و بخشی از واژه انگلیسی«Universe» به معنایجهان است. به عبارت دیگر، متاورس را می‌توان جهانی فراتر از دنیای فیزیکی تلقی کرد که در آن واقعیت مجازی، واقعیت افزوده و اینترنت به هم پیوند می‌خورند تا تجربه‌ای یکپارچه و همه‌جانبه را برای کاربران فراهم آورند.

فعال در فضای مجازی (بخصوص پلتفرم های ارتباطی) پیشنهاد می‌شود. این سازوکار می‌بایست مبتنی بر بهره‌گیری از فناوری‌های نوین پایش و تحلیل داده‌های دیجیتال، به شناسایی و رصد تعاملات مخاطره‌آمیز پرداخته و با تمرکز بر تشخیص کاربران در معرض خطر و پایش رفتارهای آسیب‌زای بالقوه، عملکردی پیشگیرانه اتخاذ نماید. تلفیق راهکارهای مبتنی بر فناوری های نوین مانند هوش مصنوعی شامل الگوریتم‌های یادگیری ماشین برای تحلیل الگوهای رفتاری، تشخیص محتوای آسیب‌رسان و شناسایی نشانگرهای سوءاستفاده کارایی این نظام را از طریق قابلیت پیش‌بینی و خنثی‌سازی تهدیدات سایبری پیش از وقوع بزه به‌طور معناداری ارتقاء می‌دهد. این واحد تخصصی پلیس می‌تواند از ابزارهای مبتنی بر هوش مصنوعی برای نفوذ تحلیلی در مرحله عملیات مقدماتی جرائم پیش از وقوع و همچنین بازبینی دقیق جرائم ارتکاب یافته بهره ببرد. در راستای اقدامات پیشگیرانه، سامانه‌های خودکارسازی هوشمند، امکان کشف شبکه‌های تبانی جنایی پیش از ارتکاب جرم را از طریق پردازش انبوه داده‌ها فراهم می‌نمایند. این رویکرد موجب تمایزگذاری بنیادین میان دو راهبرد کلان می‌گردد: نخست ابزارهای متمرکز بر افراد پرخطر مبتنی بر فهرست‌های پیش‌بینانه‌گر – متشکل از شناسایی افراد با احتمال آماری بالای ارتکاب جرم به کمک الگوریتم‌ها – و دوم ابزارهای متمرکز بر مکان‌های پرخطر معروف به راهبرد پلیس نقاط کانونی(ابوذری،۱۴۰۱: ۵). با توجه به کارکردهای ثانویه این فناوری‌ها، شواهد تجربی متعددی از موفقیت در مبارزه و پیشگیری از جرائم ثبت شده است. نمونه بارز آن در حوزه اروپا، سامانه «مدیریت پایگاه بین‌المللی تصاویر استثمار جنسی کودکان»[1] تحت نظارت سازمان پلیس جهانی[2] است که به‌عنوان یک سازوکار هماهنگ‌کننده فراملی عمل می‌نماید. چنین مداخله فناورانه و پلیسی هم‌زمان، چارچوبی پیشگیرانه ایجاد می‌کند که به‌صورت فعالانه از امنیت روانی–اجتماعی کاربران کودک در زیست‌بوم دیجیتال حفاظت نموده و آسیب‌پذیری آنان در محیط‌های مجازی را کاهش می‌دهد.

۲. راهبردهای زیر ساختی و فناورانه

یکی از اقدامات اساسی در حفاظت از کودکان در برابر بزه‌دیدگی جنسی در فضای مجازی، طراحی و ایجاد محیط‌های دیجیتال ویژه خردسالان است. این نیاز از آنجا نشأت می‌گیرد که محدود کردن گسترده و همه‌جانبه دسترسی‌های متعدد فضای سایبری، علاوه بر دشواری‌های فنی اجتناب‌ناپذیر، موجب اعمال محدودیت‌های غیرمنطقی بر کاربران بزرگسال خواهد شد. بر این اساس، راهکار مؤثر، ایجاد تمایز ماهوی و ساختاری بین عرصه‌های مجازی کودکان و بزرگسالان است تا از طریق خلق بستر های رایانه‌ای امن، خودکفا و هماهنگ با مراحل رشد روانی کودکان و نوجوانان، میزان مواجهه آنان با تهدیدات بالقوه به حداقل ممکن کاهش یابد. ایجاد شبکه جهانی ویژه کودکان و نوجوانان، به عنوان سپر محافظتی در برابر جرائم جنسی سایبری، یکی از راهبردهای بنیادی محافظت از آنان به شمار می‌رود. با پدید آوردن محیط مجازی مستقل و ایمن‌سازی شده، علاوه بر تولید محتوای هدفمند متناسب با مراحل رشد، ابزارهای کنترلی پیشرفته‌ای در اختیار خانواده‌ها قرار می‌گیرد تا با نظارت مستمر، از وقوع جرایمی همچون فریب و بهره‌کشی جنسی پیشگیری نمایند(ایقانی و دیگران،۱۴۰۰: ۱۰۲۷).

در پارادایم رایج در اروپا، تفکیک کارکردیِ شبکه‌های نوجوانان، خانواده و همگانی، امکان فیلترگذاری پویای محتوای آسیب رسان و شناسایی تعاملات مشکوک را فراهم ساخته است. اگرچه زیرساخت فنی یکپارچه است، لیکن انتخاب سطح دسترسیِ اختصاصی

[1] International Child Sexual Exploitation Image Database (ICSE DB)
[2] Interpol

توسط سرپرستان، مجریِ سیاست دسترسی مبتنی بر سن می‌باشد که مهم‌ترین جلوه‌ی آن، ممانعت از مواجهه‌ی نابجای اطفال با تارنماهای دارای پتانسیل جرم انگاری است بر این پایه، ناگزیر باید تمایزی ساختاری در بهره‌مندی از پیوندگاه‌های مجازی و کلیت محتوای دیجیتال میان گروه‌های سنی تعبیه گردد. این رویکرد که در دهه‌ی اخیر به دغدغه‌ای فراملی تبدیل شده، در نظام‌های حقوقی به‌منزله‌ی مُهری تأییدشده بر ضرورت انفکاک قلمروهای سایبری کودکان و بزرگسالان جهت مهار آسیب‌های نوپدید تلقی می‌گردد. با توجه به اهمیت الگوبرداری از تجارب بین‌المللی، مطالعات تطبیقی حاکی از آن است که سایر کشورها نیز با ایجاد چنین فضاهای مجزایی، به پیاده‌سازی این مدل مبادرت نموده‌اند. در این راستا، شبکه‌ی اینترنتی «فرگ فین»[1] در آلمان به عنوان یک مطالعه‌ی موردی قابل توجه است که در سال ۲۰۰۷ با هدف ایجاد یک اکوسیستم دیجیتال کنترل‌شده برای کودکان٦ تا ۱۲ سال طراحی و پیاده‌سازی شد.[2] مکانیزم عملکرد این پلتفرم مبتنی بر «فهرست سفید»[3] است که از طریق اعمال فیلترینگ هوشمند ، فضای مرور امنی را برای کاربران خردسال فراهم می‌نماید. این سیستم نه تنها دسترسی به دامنه‌های از پیش تأییدشده را ممکن می‌سازد، بلکه با بهره‌گیری از الگوریتم‌های اعتبارسنجی چندمرحله‌ای، حتی امکان بازدید کنترل‌شده از برخی منابع طراحی‌شده برای کاربران بزرگسال را نیز فراهم می‌آورد.[4] نکته‌ی حائز اهمیت در این پروژه، استفاده از یک واسط کاربری تعاملی با شخصیت پردازی کارتونی به نام فین است که به عنوان یک عامل واسط عمل نموده و از طریق ارائه‌ی محتوای آموزشی ساختاریافته و اخبار ویژه‌ی خردسالان، فرآیند جامعه‌پذیری دیجیتالی را تسهیل می‌نماید.[5]

اجرای سیم‌کارت‌های اختصاصی کودکان نیز به‌عنوان یک مداخله فنی در چارچوب پیشگیری از جرائم سایبری، با اعمال محدودیت‌های ساختاریافته و انطباق‌یافته با مراحل رشدی، پتانسیل قابل توجهی در کاهش بزه‌دیدگی سایبری این گروه آسیب‌پذیر دارد. این سازوکار از طریق فیلترینگ هوشمند محتوایی و محدودسازی هدفمند دسترسی‌ها، محیط دیجیتال ایمن‌سازی‌شده‌ای ایجاد می‌نماید که در آن منابع و محتوا به‌صورت پالایش‌شده ارائه می‌گردد(ایقانی و دیگران،۱٤۰۰: ۱۰۲۷).

مکانیسم‌های پیش‌کنترلی تعبیه‌شده در این سیستم، امکان نظارت پیشینی بر محتوای دریافتی و درخواست مراودات را فراهم ساخته و از طریق خنثی‌سازی تعامل با عوامل تهدیدزا، به‌طور معناداری فرصت‌های ارتکاب جرائمی نظیر سوءاستفاده‌های سایبری و اغفال جنسی آنلاین را کاهش می‌دهد. این راهکار پیشرفته با بهره‌گیری از مکانیسم‌های نظارت جامع ارتباطی، کلیه تعاملات تلفنی ورودی و خروجی و همچنین پیام‌های متنی مرتبط با سیم‌کارت را به‌طور سیستماتیک و فراتر از حافظه‌ی محلی دستگاه، در زیرساخت ابری خود بایگانی می‌نماید. دسترسی یکپارچه به این مخزن داده‌ها از طریق پورتال اختصاصی والدین میسر گردیده که امکان پایش مستمر و جامع را حتی بر ارتباطاتی که ظاهراً حذف شده‌اند فراهم می‌سازد. کاربران مجهز به قابلیت مسدودسازی پویا می‌باشند که امکان ممانعت فوری از تماس‌ها و پیامک‌های نامطلوب را صرفاً با یک عملیات ساده مهیا می‌کند. افزون بر این، دسترسی به شبکه‌های داده‌ی اینترنتی از طریق سوئیچ گزینشی فعال/غیرفعال قابل اعمال توسط والدین بوده؛ هم‌زمان الگوی ارتباطی بی‌هزینه با شماره‌های

---

[1] Frag FINN
[2] https: www.fragfinn.de
[3] White list
[4] https: international.eco.de
[5] https: ecsa.lucyfaithfull.org

داخلی منزل به‌عنوان یکی از ارکان تقویت امنیت روان‌شناختی کاربران جوان عمل می‌نماید. چارچوب حکمرانی زمانی هوشمند با اعمال محدودیت‌های دوره‌ای مبتنی بر رویداد (نظیر ساعات خواب یا زمان‌بندی آموزشی) تعاملات ارتباطی را در بازه‌های مشخص به‌صورت خودکار معلق می‌سازد. پارامترهای امنیتی این سامانه از الگویی توسعه‌پذیر مبتنی بر سن تبعیت می‌کند که متناسب با پیشرفت شناختی-اجتماعی فرزند در طول زمان، سطوح اختیارات ارتباطی را به‌صورت تدریجی و افزایشی تنظیم می‌نماید. قابل تأکید است که رویکرد این سامانه عاری از الگوهای ترغیب مصرف یا تبلیغات تجاری بوده و هیچ‌گونه محتوای تشویقی جهت هزینه‌کرد بیشتر ارائه نمی‌دهد. در نهایت، سیاست تخصیص پویای داده‌های سیار روزانه با بهینه‌سازی کارآمد توزیع پهنای‌باند، تداوم بی‌وقفه‌ی دسترسی به خدمات داده‌ای را در سراسر چرخه‌ی صورت حساب ماهیانه تضمین می‌نماید.[1] کشورهای متعددی فناوری سیمکارت های مخصوص کودکان با قابلیت های کنترل والدین و امنیت ارتباطات را توسعه داده و عرضه میکنند. این سرویس ها معمولاً شامل محدودیت تماس/پیامک، فیلتر محتوای نامناسب، عدم ردیابی موقعیت جغرافیایی، تنظیم محدودیت زمانی استفاده و مدیریت برنامه ها هستند.

۳. اقدامات آموزشی و تربیتی کلان

پیشگیری اجتماعی، به‌مثابه شکلی از پیشگیری غیرکیفری، با اتخاذ مداخلات بنیادین درصدد تقلیل نرخ جرائم و متعاقباً کاهش بزه‌دیدگی از طریق سازوکارهایی نظیر فرهنگ‌سازی، ارتقای سواد و ظرفیت‌های آموزشی است.[2] ماهیت این رویکرد ذیل اقدامات تربیتی-آموزشی تعریف می‌شود که نقشی محوری در فرآیند جامعه‌پذیری ایفا می‌نماید. بر پایه دیدگاه‌های تخصصی، این پیشگیری به دو گونه متمایز تقسیم‌پذیر است: پیشگیری جامعه‌مدار (محیط‌محور) که معطوف به تعدیل شرایط محیطی پیرامون کنشگران اجتماعی است، و پیشگیری رشدمدار[3] که ناظر بر اعمال تدابیر پیشگیرانه در مراحل تحول روانی-اجتماعی کودکان و نوجوانان می‌باشد(نجفی ابرندآبادی،۱۳۸۳: ۵۲). غایت نهایی این استراتژی، مقابله نظام‌مند با عوامل جرم‌زای محیطی محسوب می‌شود که نمونه‌های شاخص آن شامل تدابیر آموزشی، پرورشی و برنامه‌های جامعه‌پذیرکننده است. بر این مبنا، بخش مرتبط این قسمت از پژوهش از تحلیل اقدامات آموزشی و تربیتی ـ که کارآمدترین مؤلفه نظام پیشگیری تلقی می‌شوند ـ آغاز می‌گردد. تدابیر آموزشی در حوزه پیشگیری اجتماعی، متضمن کلیه اقدامات نظام‌مندی است که با محوریت ارتقای سواد پیشگیرانه، افزایش دانش فنی درباره مکانیسم‌های ارتکاب جرم، روش‌های مقابله با آن، و آگاهی‌بخشی پیرامون الگوهای بزه‌دیدگی و مخاطرات جرم طراحی می‌شوند. این برنامه‌ها عمدتاً با تمرکز بر بزه‌دیدگان احتمالی و بدون محدودیت‌های سنی، از طریق سازوکارهای آموزشی همگانی به تحقق

---

[1] https: parentshield.co.uk

[2] برای مطالعه بیشتر بنگرید به:

- ابراهیمی، شهرام(۱۴۰۱). ***جرم شناسی پیشگیری***. جلد اول، چاپ ششم، تهران: انتشارات میزان، صص.۶۰-۸۳.

- سی ولش براندون و دیوید پی فارینگتون(۱۳۹۴). ***دانشنامه پیشگیری از جرم آکسفورد (ترجمه: گروهی از پژوهشگران حقوق کیفری و جرم شناسی به کوشش حمیدرضا نیکوکار)***. با دیباچه علی حسین نجفی ابرندآبادی، تهران: انتشارات میزان، صص.۲۰۶-۳۷۱.

[3] برای مطالعه بیشتر بنگرید به:

- مهدوی، محمود(۱۴۰۳). ***پیشگیری از جرم(پیشگیری رشدمدار)***. چاپ پنجم، تهران: انتشارات سمت.

- حیدری، سیدعلی(۱۴۰۱). ***پیشگیری از بزهکاری کودکان و نوجوانان. پیشگیری رشدمدار***. با دیباچه محمود مهدوی، تهران: انتشارات میزان.

کاهش نرخ جرائم می‌انجامند. ماهیت این تدابیر در دو سطح متمایز تجلی می‌یابد: نخست در قالب برنامه‌های سوادافزایی پایه‌ای که به انتقال دانش می‌پردازند، و دوم از رهگذر مداخلات هشدارمحور که با هدف افزایش حساسیت جامعه نسبت به تهدیدات جرمی و پیامدهای بزه‌دیدگی ساماندهی می‌گردند(سلیمی،۱۳۹۷: ۷۳). اقدامات آموزشی و آگاهی‌بخش مرتبط با این حوزه در چارچوبی سلسله‌مراتبی و مبتنی بر سطح‌بندی مداخلات (خانواده، مدرسه، رسانه) به کودکان انتقال می‌یابد. این پروتکل‌های تربیتی عمدتاً در دو محور کلان متمرکز است؛ نخست آموزش سواد سایبری با تأکید بر کاربست مسئولانه‌ی فضای مجازی به‌ویژه شبکه‌های اجتماعی، و دوم توانمندسازی پیشگیرانه در مواجهه با پدیده‌های جنسی ناشناخته و مکانیسم‌های بزه‌دیدگی جنسی (با محوریت شناسایی و مقابله با اغفال و اغوای سایبری). این نظام آموزشی چندلایه، با هدف ایجاد مصونیت شناختی–رفتاری در برابر اشکال نوین بزهکاری (به‌طور خاص اغفال جنسی سایبری کودکان و نوجوانان) طراحی می‌گردد.

خانواده به عنوان اصلی‌ترین نهاد آموزشی و پرورشی، نقش بنیادینی در شکل‌گیری شناخت و رفتار فرد ایفا می‌کند. این نهاد، نخستین و مؤثرترین عامل در فرآیند رشد کودک به شمار می‌رود و کارکرد آن به‌عنوان یک سیستم کلیدی، در معماری فکری و کنشی افراد تعیین‌کننده است. خانواده از طریق تعاملات دوسویه‌ی خود، همزمان هم بسترساز تشکیل سرمایه‌ی روانی–اجتماعی است و هم کانون اصلی بازتولید یا کاهش عوامل خطرزایی که می‌توانند به رفتارهای ناهنجار منجر شوند. یافته‌های تحقیقاتی نشان می‌دهند که ضعف در عملکرد خانواده، ارتباط مستقیمی با سه عامل آسیب‌زای اصلی دارد: کمبود نظارت والدین، اختلال در ارتباط بین والدین و فرزند و کاستی در انتقال هنجارهای بازدارنده(حسینعلی‌خانی،۱۴۰۱: ۹۰). در این شرایط، برنامه‌های پیشگیرانه با هدف تقویت توانایی والدین شکل می‌گیرد که بر سه محور اصلی استوار است: آموزش مدیریت خانواده با بهره‌گیری از روش‌های رفتاری–شناختی، به کارگیری تکنیک‌های گفت‌وگوی هدفمند برای ایجاد فضای ارتباطی بدون قضاوت، و آموزش نظارت مؤثر بر فعالیت‌های دیجیتال فرزندان در عین حفظ حریم خصوصی آنان. در کنار این اقدامات، بازسازی روابط درون خانواده نیز از طریق استقرار مکانیسم‌های نظام‌مند برای حل اختلافات، طراحی برنامه‌های مشترک برای افزایش تاب‌آوری، و ایجاد چارچوب‌های روشن برای تعریف نقش‌ها و حدود هر یک از اعضا انجام می‌شود.(Mowen & Boman,2022:60). این روند با پشتیبانی یک سیستم نهادی یکپارچه کامل می‌شود که شامل شبکه‌های حمایتی محلی، سامانه‌های اخطار اولیه و برنامه‌های بازدید از منزل است. مکانیسم‌های اثرگذاری این مداخلات در تقویت توانمندی والدین، تحکیم پیوندهای عاطفی ایمن و نهادینه کردن تاب‌آوری جمعی در خانواده تجلی می‌یابد که نتیجه آن کاهش قابل توجه موقعیت های خطر است. بر این اساس، خانواده به عنوان خط مقدم پیشگیری اجتماعی، از یک طرف با کاهش آسیب‌پذیری در برابر کجروی‌ها و از طرف دیگر با تقویت مکانیزم‌های محافظتی درونی، نقش بی‌همتای خود در نظام پیشگیری رشدمحور را احیا می‌کند.

سطح دوم مداخلات پیشگیرانه، نظام آموزشی را به عنوان نهاد میانی در فرآیند رشد فرد مورد توجه قرار می‌دهد. این نظام که پس از خانواده نقش کلیدی در اجتماعی‌سازی ثانویه افراد ایفا می‌کند، در عمل عمدتاً بر جنبه‌های آموزشی متمرکز شده و به شکلی نظام‌مند از پرورش شایستگی‌های چندبعدی (شامل توانمندی‌های فردی اجتماعی و عاطفی–فرهنگی) غفلت ورزیده است. در حالی

که یافته‌های پژوهشی نشان می‌دهد توجه به این شایستگی‌ها نه تنها در پیشگیری از کجروی‌های اجتماعی مؤثر است، بلکه به صورت همزمان موجب ارتقای ظرفیت‌های شناختی، اجتماعی و هیجانی دانش‌آموزان نیز می‌شود(مهدوی و حیدری،۱٤۰۳: ٥٦۱).

مدارس موفق با ایجاد فضایی پویا و مبتنی بر مشارکت جمعی و همچنین به کارگیری نیروهای متخصص و متعهد، به نتایج قابل توجهی در کاهش آسیب‌پذیری‌های روانی و اجتماعی دانش‌آموزان دست یافته‌اند. این محیط‌های آموزشی با فراهم آوردن بسترهایی برای تعامل سازنده و تقویت حس تعلق، نقش مهمی در ارتقای تاب‌آوری و سلامت روانی دانش‌آموزان ایفا می‌کنند. چنین رویکردی نه تنها از بروز بسیاری از مشکلات رفتاری جلوگیری می‌کند، بلکه زمینه را برای پرورش نسلی مسئولیت‌پذیر و توانمند فراهم می‌سازد(Amodei& Scott,2022:526). این اثربخشی در پرتو دو ویژگی ساختاری تشدید می‌شود: نخست طول مدت تماس (حداقل ۱۲ سال حضور مستمر) و دوم نفوذپذیری چندلایه (تأثیرپذیری مستقیم/غیرمستقیم) که مدرسه را به‌عنوان محلی برای شکل‌دهی شخصیت تثبیت می‌کند. کارکرد ویژه آموزشی پیشگیرانه در این فضا، متوجه ابعاد چندگانه‌ای از انتقال اطلاعات واقع‌انگارانه و افزایش آگاهی از پیامدهای اجتماعی سوءرفتارها تا تقویت قابلیت‌های تشخیص موقعیت‌های مخاطره‌آمیز، پاسخ‌دهی سازگارانه به تهدیدات، درک پلورالیسم ارزشی–فکری و تکوین شخصیت اخلاقی یکپارچه است.

آموزش رسانه‌ای، سومین سطح از مدل پیشگیری مبتنی بر آموزش و پرورش را تشکیل می‌دهد. امروزه کارکردهای بنیادین رسانه‌ها در تنظیم فرآیندهای توسعه (در ابعاد فرهنگی، اجتماعی، اقتصادی و علمی) و نیز تدوین راهبردهای پیشگیری، به حدی حیاتی است که چشم‌پوشی از قابلیت‌های راهبردی آنها، تحقق اهداف توسعهای و خط‌مشی‌های مقابله با جرم را غیرممکن می‌کند(عباسی،۱۳۹٦: ۷۰) در این میان، فضای مجازی و شبکه‌های اجتماعی به‌واسطه‌ی ماهیت چندوجهی و قابلیت پاسخگویی هم‌زمان به نیازهای ارتباطی، اطلاعاتی و تعاملی بشر، جایگاه محوری‌تری یافته‌اند.

دو محور راهبردی توانمندسازی سایبری (شامل سواد سایبری و کاربری فضای مجازی) و آموزش محافظت جنسیتی (شامل مداخلات جامعه‌پذیرکننده در برابر پدیده‌های نوظهور جنسی) در مداخلات پیشگیرانه دارای جایگاه بی‌بدیلی هستند. در تدوین چارچوب مفهومی، سواد سایبری در رویکرد گسترده‌نگر به عنوان ترکیبی از توانش‌های شناختی (مانند تحلیل انتقادی) و مهارت‌های عملیاتی تعریف می‌شود که هدف آن بهره‌مندی حداکثری از رسانه و کاهش مخاطرات است. در مقابل، رویکرد محدودنگر صرفاً بر دسترسی فنی و فهم بنیادین محتوا تأکید دارد که به دلیل فقدان توانش تفسیری، می‌تواند به انحرافات ادراکی و پیامدهای نامطلوب بینجامد(حسینی،۱۳۹۷: ٦۷).

پژوهش‌های متأخر در حوزه پیشگیری از آسیب‌های جنسیِ اطفال، آموزش نظام‌مند ابعاد پنهان هویت جنسی را به‌عنوان محور دوم راهبردهای مداخله‌ای معرفی می‌نمایند که کارکرد آن کاهش بزه‌دیدگی جنسی کودکان از طریق شفاف‌سازی مفاهیم است. یافته‌های تحولی حاکی از آن است که اکثریت والدین در مواجهه با پرسش‌های طبیعی ناشی از گذار نوجوانی، با چالش‌های پاسخ‌دهی سازنده مواجه می‌گردند(Stone et al,2013:240). در این چارچوب، دو مؤلفه آموزش جنسیِ رشدمدار در مراحل اولیه تحول شناختی و استقرار گفتمان امنِ دوسویه به‌مثابه سازوکارهای کلیدی، سهم تعیین‌کننده‌ای در تقلیل آسیب‌پذیری جنسی و ارتقای تاب‌آوری روانی و اجتماعی ایفا می‌نمایند(قربانی و زمانی،۱۳۹٤: ۲۰۱).

بر پایه انگاره‌های جامعه‌پذیری جنسی، پاسخ‌دهی هدفمند به کنجکاوی‌های جنسی جزئی جدایی‌ناپذیر از فرآیند تربیت جنسی محسوب می‌شود که تحقق نظام‌مند آن منوط به رعایت سه اصل بنیادینِ جامعیت محتوایی، تدریج‌گرایی رشدی و عقلانیت زمینه‌مند است. شواهد سنجش‌پذیر نشان می‌دهد التزام به این اصول، زمینه‌ساز تکوین سازه‌های شناختی-هیجانی پایدار در مواجهه با بحران‌های بهداشتی-اجتماعی می‌گردد. در نهایت، تدارک اطلاعات دقیق درباره روابط جنسی به‌عنوان پیش‌نیاز تصمیم‌گیری‌های مبتنی بر خودکارآمدی جنسی، تحقق بهزیستی چندبعدی در چرخه حیات را تسهیل می‌نماید(Brissette et al,2013:762).

در سطح خانواده، آموزش سواد سایبری مستلزم برگزاری کارگاه‌های دیجیتال والدگری با محوریت نظارت هوشمند بر الگوهای مصرف رسانه‌ای و تشخیص نشانگان تعاملات پرخطر است. تکمیل این فرآیند از طریق استقرار پروتکل امنیت سایبری خانگی محقق می‌شود که شامل نصب توافقی ابزارهای کنترلی و شفاف‌سازی حریم خصوصی دیجیتال می‌باشد. در محور آموزش مسائل جنسیتی، گفتمان‌سازی مبتنی بر آگاهی جنسیتی با تأکید بر مرزبندی فیزیکی-دیجیتال و شبیه‌سازی موقعیت‌های پرخطر برای تمرین پاسخ‌های مقاومتی ضروری است.

در سطح مدرسه، آموزش سواد سایبری نیازمند تدوین برنامه درسی پلکانی است که پایه‌های سوم تا پنجم را با شناخت داده‌های شخصی، پایه‌های ششم تا نهم را با تحلیل تکنیک‌های مهندسی اجتماعی، و پایه‌های دهم تا دوازدهم را با آموزش حقوق سایبری پوشش می‌دهد. در بُعد آموزش مسائل جنسیتی، بسته‌های تربیت جنسی رشدمحور شامل آشنایی دوره ابتدایی با ارتباطات غیرمجاز مجازی و آموزش دوره متوسطه درباره تحلیل روابط مجازی، به‌همراه تمرین‌های ایفای نقش برای مواجهه با فشارهای جنسی سایبری پیشنهاد می‌گردد. در سطح رسانه، محور سواد سایبری از طریق طراحی سکوهای تعاملی ایمن شامل بازی‌های شبیه‌ساز خطر و استقرار سیستم رتبه‌بندی محتوای تعاملی محقق می‌شود. در حوزه آموزش مسائل جنسیتی، راه‌اندازی پویش‌های رسانه‌ای چندسکویی با روایت‌های قربانیان واقعی و توسعه سامانه‌های خودارزیابی خطر با ارائه بازخورد اختصاصی می‌تواند آسیب‌پذیری کاربران کودک و نوجوان را کاهش دهد.

سطح دوم: راهکارهای خانواده محور

راهکارهای خانواده محور به اقدامات پیشگیرانه‌ای اشاره دارد که با مسئولیت مستقیم والدین و در محیط خانواده اجرا می‌شوند. این راهبردها بر سه محور نظارت و کنترل، ایمن‌سازی فنی و آموزش ارتباطی استوارند و شامل مواردی چون مدیریت دسترسی، استفاده از نرم‌افزارهای کنترلی، تنظیم حریم خصوصی، به‌روزرسانی امنیتی، گفت‌وگوی آموزشی مستمر و تقویت هوش سایبری کودکان می‌شوند. هدف نهایی این راهبردها، ایجاد ایمنی فعال از طریق ترکیب نظارت هوشمند و توانمندسازی کودک است که در ذیل سه قسمت توضیح داده خواهد شد.

۱. راهبردهای نظارتی و کنترلی

در کانون راهبردهای پیشگیری وضعی معطوف به صیانت سایبری از کودکان، اجرای نظام‌های محدودیت‌ساز دسترسی به‌مثابه سنگ بنایی حیاتی تلقی می‌گردد که بر پایه‌ی پارادایم پالایش و فیلترینگ ساختاریافته‌ی محیط‌های تعاملی استوار گشته است؛[1] این

[1] نگاه کنید به:

چارچوب راهبردی با به‌کارگیری سامانه‌های فنی و تخصصی متشکل از نرم‌افزارهای کنترلی پیشرفته و سخت‌افزارهای مدیریت شبکه‌ای یکپارچه، بر گره‌های حیاتی زیرساخت‌های ارتباطی شامل پایانه‌های کاربری، مسیریاب‌های هسته‌ای شبکه‌های توزیع‌شده، و سکوهای ارائه‌دهندگان خدمات اینترنتی در مقیاس سازمانی پیاده‌سازی می‌شود تا از رهگذر اعمال مکانیسم‌های سلب دسترسی گزینشی مبتنی بر تحلیل پویای ریسک، تبادل داده‌های غیرمجاز یا محتوا و تعاملات غیرقانونی را در سطوح پیشگیرانه و با اتکا بر پروتکل‌های واکنش زنجیره‌ای مسدود نماید. چارچوب‌های فنی غالب در این عرصه که در ذیل رده‌بندی کلان فناوری‌های تعدیل‌کننده‌ی دسترسی قرار می‌گیرند، عمدتاً در سه گونه‌ی متمایز قابل تفکیک هستند: «دیواره‌های آتشین» [1]پیشرفته که به‌مثابه سدهای امنیتی لایه‌بندی شده‌ی تطبیق‌پذیر عمل می‌نمایند و قادر به رصد فعال ترافیک شبکه در سطوح پروتکلی عمیق‌اند، سامانه‌های فیلترینگ پویای مبتنی بر پایگاه‌های داده‌ی سیاهه‌دار به‌روزرسانی شونده‌ی ابری که از الگوریتم‌های یادگیری عمیق برای شناسایی الگوهای رفتاری مخاطره‌آمیز استفاده می‌کنند، و «پراکسی»[2]های هوشمند میانجی‌گر چندپروتکلی با قابلیت بازپیکربندی پویای مسیرهای ارتباطی که امکان اعمال سیاست‌های امنیتی مبتنی بر زمینه‌ی تعاملی را فراهم می‌سازند. این ابزارها با اتکا بر بانک‌های اطلاعاتی سلسله‌مراتبی از محتوای مجاز و غیرمجاز که در قالب الگوهای چندبعدی طبقه‌بندی شده‌اند، فرآیندهای غربالگری هوشمند را از طریق ترکیب الگوریتم‌های تطبیق الگوی نیمه‌ساختاریافته و یادگیری ماشینی نظارت‌شده‌ی تقویتی به اجرا می‌گذارند و به‌طور مستمر از طریق مکانیسم‌های بازخورد انطباقی، پایگاه دانش خود را ارتقاء می‌بخشند(عوضیان دره،۱٤۰۱: ۳۹).

از دیدگاه عملکردی و با توجه به معماری نظارتی، دو گونه متمایز از سیستم‌های نظارتی قابل شناسایی است: سامانه‌های یک‌سویه غیرفعال که صرفاً بر نظارت بر جریان‌های داده‌ای ورودی متمرکز بوده و عمدتاً در قالب فیلترهای محتوایی پایه با الگوی لیست سفید و سیاه عمل می‌کنند، و راهکارهای دوسویه فعال پیشرفته که با نظارت همزمان بر ترافیک ورودی و خروجی در لایه‌های انتقال و کاربرد، مکانیسم‌های بازدارندگی جامع چندبعدی را از طریق تحلیل رفتاری بلادرنگ ایجاد می‌نمایند(حیدری نژاد،۱۳۹۷: ۳۳).

این سیستم‌های پیشرفته با بهره‌گیری از فناوری‌های هوشمند، قادر به شناسایی الگوهای رفتاری غیرعادی، تشخیص ناهنجاری‌ها و پیش‌بینی تهدیدات بالقوه هستند که امکان پاسخگویی فعال و انعطاف‌پذیر به چالش‌های امنیتی در محیط‌های دیجیتال پیچیده را فراهم می‌آورد. در عصر کنونی، به کارگیری این تمهیدات در قالب راهبردهای چندلایه‌ای کاهش تهدیدات سایبری متبلور می‌شود که در چهارچوب الگوهای امنیتی نسل نوین قابل درک بوده و نمونه‌های عینی آن شامل اجرای سیاست‌های مسدودسازی آی‌پی مبتنی بر ارزیابی پویای ریسک برای مقابله هدفمند با منابع داخلی و خارجی شناخته‌شده آسیب‌زا، پیاده‌سازی فناوری‌های رمزنگاری پیشرفته نقطه پایانی با استفاده از الگوریتم‌های خارجی به منظور کاهش آسیب‌پذیری‌های زیرساختی در مقابل حملات پیچیده

– خانعلی پور واجارگاه، سکینه(۱٤۰۰). ***پیشگیری فنی از جرم***. چاپ دوم، تهران: انتشارات میزان.

[1] «**Firewall**» یک تدبیر نرم افزاری بوده که داده های وارد یا خارج شده از وب سایت ها و نرم افزار های تحت وب را مانیتور، فیلتر گذاری یا مسدود می نماید.

[2] «**Proxy**»پراکسی را می‌توان سروری دانست که امکان ایجاد فیلترهای خاص به جهت افزایش امنیت در شبکه مورد نظر را فراهم می‌کند. به طور کلی پراکسی امکانات و قابلیت‌های زیادی دارد که از آن جمله می‌توان به افزایش ذخیره‌سازی و سرعت دستیابی به اطلاعات اشاره کرد. این سرور به همراه سیستم‌های تصدیق هویت می‌تواند ضامنی برای **امنیت در شبکه** باشد.

مستمر، و استقرار معماری‌های امنیتی انعطاف‌پذیر شناختی که با پایش مستمر محیط تهدید و تحلیل پیش‌بینانه نقاط ضعف، پارامترهای کنترلی را به صورت خودکار و مبتنی بر سنجش ریسک بلادرنگ بازتنظیم می‌نمایند، می‌باشد. چنین مکانیسم‌هایی نه تنها ضریب ایمنی شبکه‌ها و ارتباطات کاربران را به صورت تصاعدی و از طریق ایجاد لایه‌های دفاعی عمیق افزایش می‌دهند، بلکه با ایجاد موانع ساختاری پیشگیرانه پویا در چارچوب نظریه انتخاب عقلانی، هزینه‌های ارتکاب جرائم سایبری علیه گروه‌های آسیب‌پذیر مانند کودکان را تا سطح مطلوبی افزایش داده و از طریق بالابردن شاخص‌های تلاش مورد نیاز و کاهش بازده مورد انتظار برای مجرمان، به بازتعریف معادلات سود و زیان فعالیت‌های مجرمانه در فضای سایبری می‌پردازند.[1]

۲. راهبردهای ایمن سازی فنی

ارتقای سطح ایمنی و تضمین امنیت کاربران در فضای مجازی، همراه با فراهم‌آوری بستری امن برای تعاملات آنلاین، به‌عنوان ضرورتی اجتناب‌ناپذیر در راستای تحقق امنیت سایبری قلمداد می‌شود. جهان دیجیتالِ امروز، مستلزم اتخاذ راهبردهای امنیتی پویا و تطبیق‌پذیر است تا بتواند همگام با تحولات فزاینده و پرشتاب شبکه‌های اینترنتی، پاسخگوی چالش‌های نوظهور باشد(داوری دولت آبادی،۱۴۰۰: ۹۶). از آنجا که بسیاری از تعاملات خطرناک از طریق حساب‌های کاربری آنلاین صورت می‌گیرد، ایمن‌سازی این حساب‌ها یکی از گام های مهم در پیشگیری از بزه‌دیدگی کودکان محسوب میشود(Ojagverdiyeva,2018:89). برای افزایش ایمنی کودکان در فضای دیجیتال، می‌توان با تنظیم حساب‌های کاربری در «حالت خصوصی»[2]، دسترسی را صرفاً به مخاطبین تأییدشده محدود نموده و از تعامل با کاربران ناشناس پیشگیری کرد. همچنین با غیرفعال سازی امکان دریافت پیام از افراد ناشناس در شبکه‌های اجتماعی و پلتفرم‌های ارتباطی، سطح محافظت را ارتقاء داد. از سوی دیگر، بهره‌گیری از ابزارهای کنترلی و نظارتی والدین همچون اعمال محدودیت‌های سنی می‌تواند از بروز چالش در سطوح مختلف ارتباطات آنلاین کودکان جلوگیری به عمل آورد(Hernandez,2024:776). برای ارتقای امنیت سایبری و جلوگیری از دسترسی های غیرمجاز به کودکان در شبکه های اجتماعی، فعال‌سازی احراز هویت دو مرحله ای به عنوان لایه حفاظتی مضاعف توصیه میشود. این مکانیزم امنیتی با نیاز به تایید دومرحله ای، احتمال نفوذ به حساب های کاربری را به حداقل میرساند. در کنار این روش، آموزش و ترغیب کاربران به ویژه کودکان به استفاده از رمزهای عبور پیچیده متشکل از ترکیبی منحصر به فرد از حروف بزرگ و کوچک، اعداد و نمادهای خاص ضروری است. همچنین بروزرسانی منظم نرم افزارها و اپلیکیشن ها نیز از دیگر اقدامات حیاتی محسوب میشود، چرا که آخرین نسخه های منتشر شده معمولاً شامل اصلاح آسیب پذیری های امنیتی کشف شده هستند. در حوزه ارتباطات و مراودات آنلاین، نظارت و در صورت

---

[1] برای مطالعه بیشتر در مورد دیدگاه مخالف بنگرید به:

-Jesse, M., & Jannach, D (2021). **Digital nudging with recommender systems: Survey and future directions**. *Computers in Human Behavior Reports*, *3*, 100052.

-Maier, M., Bartoš, F., Stanley, T. D., Shanks, D. R., Harris, A. J., & Wagenmakers, E. J (2022). **No evidence for nudging after adjusting for publication bias**. *Proceedings of the National Academy of Sciences*, *119*(31), pp:1-20.

-Masur, P. K., DiFranzo, D., & Bazarova, N. N (2021**). Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure**. *Plos one*, *16*(7), pp:187-202.

-Taylor, S. H., DiFranzo, D., Choi, Y. H., Sannon, S., & Bazarova, N. N (2019). **Accountability and empathy by design: Encouraging bystander intervention to cyberbullying on social media.** *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), pp:1-26.

[2] Private mood

نیاز مسدودسازی «برنامه های گفت و گوی ناشناس»[1] در بستر پلتفرم های عمومی گفت و گو محور و برخی پلتفرم های بازی آنلاین که امکان تعامل با افراد ناشناس را فراهم میکنند، از اهمیت ویژه ای برخوردار است. به عنوان جایگزین امن تر، میتوان از پیام رسان های طراحی شده مخصوص کودکان که مجهز به سیستم کنترل والدین است استفاده کرد. این برنامه ها ضمن حفظ قابلیت های ارتباطی، محیطی کنترل شده و ایمن را برای کاربران خردسال فراهم می آورند. ترکیب این راهکارها سطح حفاظتی مناسبی در برابر تهدیدات سایبری ایجاد میکند و فضای دیجیتال امنتری برای کودکان و نوجوانان مهیا میسازد. این راهکارها در کنار مدیریت زمان استفاده از دستگاه‌های هوشمند از طریق تعیین بازه‌های زمانی مجاز، به صورت جامع از مواجهه با تهدیدات سایبری پیشگیری کرده و امنیت دیجیتال کودکان را تقویت می‌نماید.

۳. راهبردهای ارتباطی- تربیتی

در چارچوب مکانیسم‌های پیشگیرانه برای حفاظت از کودکان و نوجوانان در برابر مخاطرات فضای مجازی، برنامه‌های آموزشی والدین به عنوان مداخله‌ای راهبردی از جایگاه محوری برخوردار است. این برنامه‌ها با هدف دوگانه پیشگیری از بزه‌دیدگی سایبری و کاهش آسیب‌پذیری‌های دیجیتال طراحی شده‌اند. والدین به عنوان اولین نهاد تربیتی و ناظران اصلی، نقشی دیالکتیکی در اکوسیستم رشدی کودک ایفا می‌کنند که کیفیت تعاملات آنها می‌تواند همزمان به عنوان عامل محافظتی یا عامل تهدیدکننده عمل نماید.

شواهد نشان می‌دهد که کمبود سواد دیجیتال و ضعف در مهارت‌های تربیتی مؤثر در برخی والدین، منجر به دو پدیده آسیب‌زای فقدان نظارت فعال بر رفتارهای سایبری و اعمال کنترل‌های انضباطی نامتناسب می‌شود که در موارد شدید، غفلت را به عاملی تسهیل‌کننده برای قربانی‌شدن تبدیل می‌کند(قادری،۱٤۰٤: ۸۷). این مداخلات آموزشی با اتخاذ رویکردی نظام‌مند و مبتنی بر شواهد، سه محور اصلی را پوشش می‌دهند: نخست، آموزش روش‌های انضباطی سازنده مانند تکنیک‌های تنبیهی غیرخشونت‌آمیز و تقویت مثبت رفتاری که به ایجاد مرزهای اخلاقی واضح منجر می‌شود. دوم، توسعه راهبردهای مدیریت نظارتی شامل پایش هوشمندانه محتوای مصرفی، تنظیم حریم خصوصی و شناسایی نشانه‌های خطر از طریق مکانیزم‌هایی مانند نظارت مشارکتی. سوم، آموزش ایجاد محدودیت‌های اثربخش شامل طراحی قواعد متناسب با سن، توافق بر برنامه زمان‌بندی استفاده و بهکارگیری فیلترینگ پویا که چارچوب‌های حمایتی انعطاف‌پذیری ایجاد می‌نماید.

پیامدهای این مداخلات فراتر از ایمنی سایبری، شامل استحکام دلبستگی ایمن در روابط والد–فرزندی، تقویت کارکردهای اجرایی کودک از طریق الگوسازی، پایه‌ریزی گفت‌وگوی انتقادی درباره مخاطرات دیجیتال، و تبدیل خانواده به نظام حمایتی اولیه است.

علی‌رغم اثربخشی مستند این برنامه‌ها، چالش‌هایی چون شکاف دیجیتالی نسلی، موانع اقتصادی–اجتماعی دسترسی، و نبود پشتیبانی نهادی پایدار، اجرای بهینه آن‌ها را محدود ساخته است. جهت غلبه بر این موانع، ضروری است توسعه آتی مداخلات با رویکردی میان‌رشته‌ای و از طریق تلفیق ظرفیت‌های نهادهای مدنی، آموزشی و قضایی به سمت الگوهای جامعه‌محور سوق یابد. در تحلیل نهایی، توانمندسازی والدین به مثابه کارگزاران فعال ایمنی سایبری در گرو تلفیق سه‌گانه آموزش مهارت‌های پرورشی، ارتقای سواد

[1] Private chat

رسانه‌ای و طراحی سیاست‌های کلان حمایتی است که نه تنها سپری در برابر تهدیدات مجازی ایجاد می‌کند، بلکه زیرساختی برای رشد تاب‌آورانه در زیست‌جهان دیجیتال فراهم می‌آورد.

در چارچوب راهبردهای پیشگیری از بزه‌دیدگی اطفال در فضای مجازی، برنامه‌های مبتنی بر ملاقات‌های خانوادگی به‌عنوان مداخلاتی زودهنگام و ساختاریافته از جایگاهی ممتاز برخوردارند. نمونه‌ی برجسته‌ی این رویکرد، «برنامه المیرا»[1] است که از دهه‌ی ۱۹۷۰ میلادی در نیویورک آمریکا به‌صورت علمی اجرا شد و با تمرکز بر خانواده‌های پرخطر، الگویی پیشرو در مداخلات والدمحور ارائه داد(روبرو،۱۳۸٤: ۳۰٤) هسته‌ی این برنامه مبتنی بر ملاقات‌های منظم در محیط خانه بود که آموزش‌های تخصصی فرزندپروری، بهبود تعاملات خانوادگی و مدیریت محیط رشد را از سنین پایین آغاز می‌کرد. برنامه المیرا با اتخاذ رویکردی چندسطحی، فراتر از آموزش مستقیم، از طریق حمایت‌های اجتماعی نظام‌مند شامل شبکه‌سازی با خویشاوندان، یکپارچه‌سازی خدمات بهداشتی–رفاهی و پیوند زدن خانواده‌ها با نهادهای محلی، به توانمندسازی ساختاری خانواده به‌مثابه یک سیستم منسجم می‌پرداخت. تطبیق این الگو در حوزه‌ی ایمنی سایبری کودکان، با بازتعریف محتوای آموزشی، اثربخشی قابل‌توجهی در ارتقای سواد دیجیتال والدین دارد. در این بازطراحی، ملاقات‌های خانوادگی می‌توانند به انتقال مهارت‌های نظارتی ویژه‌ی فضای مجازی (شامل رصد رفتارهای آنلاین و تشخیص نشانگان سوءاستفاده‌ی دیجیتال، آموزش مهندسی محدودیت‌های سن‌محور (تنظیم حریم‌خصوصی و مدیریت زمان استفاده)، بنیان‌گذاری گفت‌وگوهای انتقادی والد–فرزندی درباره‌ی مخاطرات آنلاین، و ایجاد پل‌های حمایتی با نهادهای تخصصی (مراکز گزارش‌گیری جرایم سایبری و مشاوران رسانه‌ای) تبدیل شوند. تجربه‌ی المیرا نشان می‌دهد که تلفیق آموزش چهره‌به‌چهره با پشتیبانی نهادی نه‌تنها دانش نظری والدین را افزایش می‌دهد، بلکه پایداری رفتاری را از طریق ایجاد سیستم‌های حمایتی ملموس تضمین می‌کند. در حوزه‌ی فضای مجازی، این رویکرد قادر است شکاف دیجیتالی نسلی را با آموزش‌های عملیاتی در بستر طبیعی خانواده کاهش دهد و از کمبود پیگیری– به‌عنوان نقطه‌ضعف برنامه‌های مرسوم– جلوگیری نماید. بنابراین، بازآفرینی برنامه‌های ملاقات خانوادگی با محتوای سایبری، نه‌تنها مکمل مداخلات آموزشی موجود، بلکه چارچوبی تحول‌آفرین در پیشگیری اولیه از بزه‌دیدگی دیجیتالی محسوب می‌شود که با تقویت تاب‌آوری خانواده‌ها، زیرساختی برای رشد ایمن در زیست‌جهان پیچیده‌ی دیجیتال فراهم می‌آورد.

نتیجه‌گیری

شواهد پژوهشی گواه آن است که توسعه روزافزون فناوری اطلاعات و ارتباطات، به صورت مستقیم و غیرمستقیم، در تسهیل و تشدید رفتارهای مجرمانه نقش داشته است. این پدیده منجر به تبدیل فضای سایبری به بستری آسیب‌زا و مستعد برای ارتکاب طیف وسیعی از جرائم شده است. جذابیت‌های ساختاری این عرصه، از قبیل فراملی بودن، ناشناس‌مانی، قابلیت دسترسی بالا و کاهش هزینه‌های ارتکاب جرم، انگیزه‌های قدرتمندی برای کوچ بزهکاران از عرصه حقیقی به حوزه مجازی فراهم آورده است. در این میان، اگرچه هیچ گروه سنی مصون از تهدیدات همه‌جانبه این فضا نیست، لیکن کودکان و نوجوانان به دلایل آسیب‌پذیری‌های ذاتی

[1] Elmira Program

ناشی از مراحل رشدی، از جمله فقدان بلوغ شناختی، اعتماد نامتعارف، کنجکاوی بی‌محابا و درک محدود از عواقب، در صدر گروه‌های در معرض خطر و مستعد بزه‌دیدگی قرار می‌گیرند. در کانون این طیف از آسیب‌پذیری‌ها، پدیده «اغفال جنسی سایبری» قرار دارد که به مثابه یکی از شاخص‌ترین و هولناک‌ترین مصادیق بزه‌دیدگی کودکان در عصر دیجیتال قلمداد می‌گردد. این جرم نوظهور که ذاتاً در گفتمان قدرت و سوءاستفاده میان یک بزرگسال و یک کودک تعریف می‌شود، از طریق ایجاد رابطهٔ مبتنی بر فریب و اعتمادسازی کاذب در بستر پلتفرم های دیجیتال و خارج از چارچوب‌های نظارتی والدین و نهادهای قانونی محقق می‌گردد. این پدیده را می‌توان به مثابه گونهٔ خاص و مدرنی از «بهره‌کشی جنسی از کودکان» طبقه‌بندی نمود که در آن، فناوری به عنوان یک تسهیل‌گر قاطع عمل می‌کند. ماهیت تهاجمی و عمیقاً آسیب‌زای این بزهکاری، آن را به‌طرزی معنادار خطرناک‌تر از بسیاری دیگر از اشکال بزه‌دیدگی سایبری متمایز می‌سازد. بی‌تردید، گامی اساسی در راستای صیانت از کودکان در قلمرو سایبری، معطوف به اتخاذ راهبردهای مؤثر در پیشگیری از وقوع جرم است؛ امری که توجیهات عقلانی، جامعه‌شناختی و روان‌شناختی آن در ادبیات پژوهشی به تفصیل مورد واکاوی قرار گرفته است. اگرچه مطالعات ارزشمندی در حوزهٔ کلی پیشگیری از بزه‌دیدگی اطفال در فضای مجازی به انجام رسیده، با این حال، مقالهٔ حاضر عمدتاً درصدد است تا با تمرکز بر جرم خاص مراودات با هدف اغوا و اغفال جنسی کودکان، راهکارهای پیشگیرانهٔ اختصاصی و هدفمندی را برای این نوع خاص از بزهکاری ارائه نماید. بدین ترتیب، دامنهٔ پژوهش حاضر از مباحث کلی‌تر فراتر رفته و با انحصار توجه بر مکانیسم‌ها و راه‌کارهای مقابله با این جرم نوپدید، در جهت پر کردن خلأ موجود در ادبیات تخصصی این حوزهٔ خاص گام برمی‌دارد.

یافته‌های این پژوهش نشان می‌دهد که مقابله با پدیده اغفال جنسی سایبری کودکان مستلزم اتخاذ رویکردی چندسطحی و جامع است که در سطح کلان، راهبردهای نهادی و سیاستی را دربرمی‌گیرد. در این راستا، آموزش ساختاریافته سواد سایبری و مسائل جنسی متناسب با سن از طریق گنجاندن در برنامه درسی مدارس، اجرای برنامه‌های خانواده‌محور و کمپین‌های رسانه‌ای ملی به عنوان امری ضروری شناسایی شده است. همچنین، بازنگری و اصلاح قوانین موجود و پیش‌بینی قوانین پیشگیرانه خاص با محوریت حمایت از بزه‌دیدگان، همراه با تأسیس و توسعه پلتفرم‌ها و فضای مجازی امن و ایزوله مخصوص کودکان (بر اساس الگوهای موفق بین‌المللی همچون فرگ فین در آلمان) و نیز تخصصی‌سازی نهادهای نظارتی از طریق ایجاد دایره‌های ویژه در پلیس فتا متشکل از نیروهای متبحر در روانشناسی کودک و جرائم سایبری، از دیگر اقدامات بنیادین محسوب می‌گردند. در سطح خرد و خانوادگی، کاربست مداخلات والدمحور از طریق برگزاری جلسات آموزشی و خانوادگی منظم به منظور ارتقای نظارت و کیفیت ارتباط، همراه با اعمال محدودیت‌های فنی نظیر ایجاد محدودیت‌های سنی، احراز هویت دو مرحله‌ای، انسداد دریافت پیام از کاربران ناشناس و بهره‌گیری از سیم‌کارت‌های مخصوص کودکان به عنوان یک پایگاه نظارتی، می‌تواند سهم به‌سزایی در کاهش آسیب‌پذیری ایفا نماید. در نهایت، به‌کارگیری همزمان و ترکیبی این راهکارها در هر دو سطح، به‌منزله یک استراتژی جامع، برای صیانت مؤثر از کودکان در فضای سایبری اجتناب‌ناپذیر است.

منابع فارسی

۱. ابراهیمی، شهرام(۱۴۰۱). ***جرم شناسی پیشگیری***. جلد اول، چاپ ششم، تهران: انتشارات میزان.

۲. ابوذری، مهرنوش(۱٤۰۱). **تاثیر هوش مصنوعی در کیفیت تحقیقات جنایی**. *حقوق فناوری های نوین*، ۳(٦)، صص.۱-۱۳.

۳. ایقانی و دیگران (۱٤۰۱). **علت شناسی و ارائه راهکارهای پیشگیری غیرکیفری از پدیده بزه‌دیدگی اطفال در فضای مجازی**. *مطالعات پیشگیری از جرم*،۱۷(٦٦)،صص.۱۰۰۷-۱۰۲٦.

٤. ایقانی، مصطفی و زهروی، رضا و میری، حسین و اسماعیلی، علی اکبر(۱٤۰۰). **پیشگیری وضعی و اجتماعی از بزه دیدگی اطفال در فضای مجازی**. *جامعه شناسی سیاسی ایران*، ۱٦،صص.۱۰۰۷-۱۰۲٦. 10.30510/psi.2022.293706.1948

۵. حسینعلی خانی، زهرا (۱٤۰۱). **پیشگیری رشد مدار از خشونت اطفال و نوجوانان تحت تاثیر فضای مجازی**. {پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، تهران: دانشگاه تهران}.

٦. حسینی، سید هادی (۱۳۹۷). **آسیب های فضای مجازی در بین خانواده ها**. *نشریه معارف اسلامی و تبلیغ و ارتباطات*،٦(۱۲)، صص۵۷-٦۹.

۷. حیدری نژاد، نصرالله (۱۳۹۷). **پیشگیری وضعی در جرایم سایبری از منظر حقوق کیفری ایران و جهان**. *نشریه علمی قانون یار*،٦(۲)، صص.۲۹-٤٤.

۸. حیدری، سیدعلی(۱٤۰۱). ***پیشگیری از بزهکاری کودکان و نوجوانان پیشگیری رشدمدار***. با دیباچه محمود مهدوی، تهران: انتشارات میزان.

۹. خانعلی پور واجارگاه، سکینه (۱٤۰۰). ***پیشگیری فنی از جرم***. چاپ دوم، تهران: انتشارات میزان.

۱۰. خواجه نوری یاسمن و امیرحسین نیازپور(۱٤۰۳). **کنشگری پیشگیرانه پلیس در قانون حمایت از اطفال و نوجوانان ۱۳۹۹**. *دو فصلنامه تحقیق و توسعه در حقوق کیفری و جرم شناسی*، ۱(۲)،صص. ۱۵۱-۱۸٤. 10.22034/jclc.2025.2048674.1132

۱۱. داوری دولت آبادی، بهاره (۱٤۰۰). **راهکارهای پیشگیری وضعی از جرایم سایبری علیه خانواده متاثر از اینستاگرام**{ پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی، اصفهان: دانشگاه شهید اشرفی اصفهانی}.

۱۲. سی ولش براندون و دیوید پی فارینگتون(۱۳۹٤). ***دانشنامه پیشگیری از جرم آکسفورد (ترجمه: گروهی از پژوهشگران حقوق کیفری و جرم شناسی به کوشش حمیدرضا نیکوکار)***. با دیباچه علی حسین نجفی ابرندآبادی، تهران: انتشارات میزان.

۱۳. شاهپوری تهمینه و تهمورث بشیریه.(۱٤۰٤). **بررسی پیش‌بینی‌های بزه دیدگی جنسی از منظر مدل تلفیقی**. *دو فصلنامه تحقیق و توسعه در حقوق کیفری و جرم شناسی*، ۲(۳)،صص ۲۷۸-۳۰۷ . 10.22034/jclc.2025.2047336.1128

۱٤. عباسی، مریم(۱۳۹٦). **تاثیر استفاده از فضای مجازی و ماهواره بر نوجوانان**. *نشریه زندگی پاک*،۵(۱٦)، صص.٦۵-۷۸.

۱۵. عوضیان دره، ماندانا(۱٤۰۱). **پیشگیری وضعی از جرایم سایبری در بوته آسیب شناسی حاکم بر آن**{پایان نامه کارشناسی ارشد، اصفهان: دانشگاه شهید اشرفی اصفهانی}.

۱٦. قادری، علیرضا(۱٤۰٤). **تحلیل جرم شناختی اغفال کودکان و نوجوانان در فضای سایبر**{پایان نامه کارشناسی ارشد، تهران: دانشگاه تهران}.

۱۷. قربانی، مهسا و زمانی علویجه فرشته(۱۳۹٤). **آموزش و ارتقای سلامت جنسی کودکان: شناخت کنجکاوی های جنسی کودکانه: مقدمه ای بر آموزش و ارتقای سلامت جنسی آنان**. آموزش بهداشت و سلامت و ارتقاء سلامت ایران،۳(۳)،صص.۱۹۸-۲۱۰

۱۸. کاریو، روبر(۱۳۸٤). **مداخله روان شناختی- اجتماعی زودرس در پیشگیری از رفتارهای مجرمانه(ترجمه علی حسین نجفی ابرندآبادی)**. فصلنامه تحقیقات حقوقی،۵(۳۵)،صص.۲٦۷-۳۰٤.

۱۹. گل محمدی خامنه، علی(۱۳۸۵). ***مدیریت پیشگیری از جرایم***. تهران: انتشارات دانشگاه علوم انتظامی امین.

۲۰. مهدوی، محمود و حیدری، سید علی(۱٤۰۳). ***پیشگیری از جرم(پیشگیری رشدمدار)***. چاپ دوم، تهران: انتشارات میزان.

۲۱. مهدوی، محمود(۱٤۰۳). ***پیشگیری از جرم(پیشگیری رشدمدار)***. چاپ پنجم، تهران: انتشارات سمت.

۲۲. نجفی ابرندآبادی، علی حسین(۱۳۸۳). ***پیشگیری عادلانه از جرم، علوم جنایی، مجموعه مقالات در تجلیل از دکتر محمد آشوری***. تهران: انتشارات سمت

References

1. Abbasi, Maryam. (2017). **The Impact of Using Cyberspace and Satellite TV on Adolescents**. *Pakzendegi Journal*, 5(16), 65-78. (In Persian)

2. Abuzari, Mehrmoush. (2022). **The Impact of Artificial Intelligence on the Quality of Criminal Investigations**. *Journal of Modern Technology Law*, 3(6), 1-13. (In Persian)

3. Amodei, N., & Scott, A. A (2002). **Psychologists' contribution to the prevention of youth violence**. *The Social Science Journal*, *39*(4), pp:511-526.

4. Avaziyan Dareh, Mandana. (2022). **Situational Prevention of Cybercrimes: A Pathology of its Governing Challenges** [Master's thesis]. Isfahan: Shahid Ashrafi Esfahani University. (In Persian)

5. Brissette, I., Wales, K., & O'Connell, M (2013). **valuating the Wellness School Assessment Tool for use in public health practice to improve school nutrition and physical education policies in New York**. *Journal of school health*, *83*(11), pp:757-762.

6. Cario, Robert. (2005). **Early Psycho-Social Intervention in the Prevention of Criminal Behavior** (Translated by Ali Hossein Najafi Abrand abadi). Legal Research Quarterly, 5(35), 267-304. (Original work published earlier) (In Persian)
7. Dandurand, Y (2014). **Criminal justice reform and the system's efficiency**. *Criminal Law Forum*, 25(3).
8. Davari dowlatabadi Bahareh. (2021). **Situational Prevention Strategies for Cybercrimes Against Families Affected by Instagram** [Master's thesis in Criminal Law and Criminology]. Isfahan: Shahid Ashrafi Esfahani University. (In Persian)
9. Ebrahimi, Shahram. (2022). ***Preventive Criminology*** (Vol. 1, 6th ed.). Tehran: Mizan Publications. (In Persian)
9. Eighani, Mostafa, et al. (2022). **Etiology and Presenting Non-Criminal Prevention Strategies for the Victimization of Children in Cyberspace**. *Criminology Studies*, 17(66), 1007-1026. (In Persian)
10. Eighani, Mostafa, Zehrovi, Reza, Miri, Hossein, & Esmaeili, Ali Akbar. (2021**). Situational and Social Prevention of Child Victimization in Cyberspace.** *Iranian Political Sociology Journal*, 16, 1007-1026. (In Persian)
11. Ghaderi, Alireza. (2025). **Criminological Analysis of the Entrapment of Children and Adolescents in Cyberspace** [Master's thesis]. Tehran: University of Tehran. (In Persian)
12. Ghorbani, Mahsa, & Zamani Alavijeh, Fatemeh. (2015). **Education and Promotion of Children's Sexual Health: Recognizing Children's Sexual Curiosity: An Introduction to Educating and Promoting Their Sexual Health**. *Iranian Journal of Health Education and Health Promotion*, 3(3), 198-210. (In Persian)
13. Golmohammadi Khameneh, Ali. (2006). ***Crime Prevention Management***. Tehran: Amin Police University Press. (In Persian)
14. Heidari Nejad, Nasrollah. (2018). **Situational Prevention in Cybercrimes from the Perspective of Iranian and International Criminal Law**. *Scientific Journal of Ghanoon Yar*, 6(2), 29-44. (In Persian)
15. Heidari, Seyed Ali. (2022). ***Prevention of Child and Juvenile Delinquency: Developmental Prevention.*** With a preface by Mahmoud Mahdavi. Tehran: Mizan Publications. (In Persian)
16. Hernandez, J. M., Ben-Joseph, E. P., Reich, S., & Charmaraman, L (2024). **Parental monitoring of early adolescent social technology uses in the US: a mixed-method study**. *Journal of Child and Family Studies*, *33*(3), pp:759-776.
17. Hosseinali Khani, Zahra. (2022). **Developmental Prevention of Violence in Children and Adolescents Affected by Cyberspace** [Master's thesis in Criminal Law and Criminology]. Tehran: University of Tehran. (In Persian)
18. Hosseini, Seyed Hadi. (2018). **The Damages of Cyberspace Among Families.** *Journal of Islamic Education and Communication*, 6(12), 57-69. (In Persian)
19. Jesse, M., & Jannach, D (2021). **Digital nudging with recommender systems: Survey and future directions**. *Computers in Human Behavior Reports*, *3*, 100052.
20. Kaylor, L. E., Winters, G. M., Jeglic, E. L., & Cilli, J (2023). **An analysis of child sexual grooming legislation in the United States.** ***Psychology***, *Crime & Law*, *29*(9), pp:982-1000.
21. Kesuma, D. A (2024). **Criminal Law Reform to Increase the Effectiveness of the Justice System in Overcoming Crime**. *International Journal of Science and Society*, *6*(1).
22. Khajeh Nouri Yasaman & Niazpour, Amirhossein. (2024). **The Preventive Role of the Police in the 2020 Law on the Protection of Children and Adolescents**. *Journal of Research and Development in Criminal Law and Criminology*, 1(2), 151-184. 10.22034/jclc.2025.2048674.1132 (In Persian)
23. Khanalipour Vajargah, Sakineh. (2021). ***Technical Crime Prevention*** (2nd ed.). Tehran: Mizan Publications. (In Persian)
24. Mahdavi, Mahmoud, & Heidari, Seyed Ali. (2024). Crime Prevention (Developmental Prevention) (2nd ed.). Tehran: Mizan Publications. (In Persian)
25. Mahdavi, Mahmoud. (2024). ***Crime Prevention*** (Developmental Prevention) (5th ed.). Tehran: SAMT Publications. (In Persian)
26. Maier, M., Bartoš, F., Stanley, T. D., Shanks, D. R., Harris, A. J., & Wagenmakers, E. J (2022). **No evidence for nudging after adjusting for publication bias**. *Proceedings of the National Academy of Sciences*, *119*(31), pp:1-20.
27. Masur, P. K., DiFranzo, D., & Bazarova, N. N (2021**). Behavioral contagion on social media: Effects of social norms, design interventions, and critical media literacy on self-disclosure**. *Plos one*, *16*(7), pp:187-202.
28. Mowen, T. J., & Boman IV, J. H (2022). **Recognizing the multidimensional roles of family and peers on crime**. *Sociology compass*, *14*(3), pp:44-60.
29. Najafi Abrand abadi, Ali Hossein. (2004). **Just Crime Prevention. In Criminal Sciences**: A Collection of Articles in Honor of Dr. Mohammad Ashouri (pp. [Page numbers would be needed]). Tehran: SAMT Publications. (In Persian)
30. Ojagverdiyeva, S (2018). **Ensuring child safety in internet environment**. *Problems of information society*, *9*(1).
31. Shahpouri, tahmineh, & Bashiriyeh, Tahmoores. (2025). **Predicting Sexual Victimization from the Perspective of an Integrated Model**. *Journal of Research and Development in Criminal Law and Criminology*, 2(3), 278-307. 10.22034/jclc.2025.2047336.1128 (In Persian)
32. Stone, N., Ingham, R., & Gibbins, K (2013). **Where do babies come from? 'Barriers to early sexuality communication between parents and young children**. *Sex Education*, *13*(2), pp:228-240.
33. tarov, K. A., Maksimov, S. V., Beisembayeva, A. O., & Alshurazova, R. A (2023). **OPTIMIZATION OF CRIMINAL LEGISLATION: REFORMING CRIMINAL PROCEDURAL AND PENAL LAWS**. *Journal of Actual Problems of Jurisprudence/Habaršy. Zaṇ Seriâsy*, *108*(4).
34. Taylor, S. H., DiFranzo, D., Choi, Y. H., Sannon, S., & Bazarova, N. N (2019). **Accountability and empathy by design: Encouraging bystander intervention to cyberbullying on social media.** *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), pp:1-26.

35. Welsh, Brandon C., & Farrington, David P. (2015). ***The Oxford Handbook of Crime Prevention*** (Translated by: A group of criminal law and criminology researchers compiled by Hamidreza Nikookar). With a preface by Ali Hossein Najafi Abrandabadi. Tehran: Mizan Publications. (Original work published 2014) (In Persian)

منابع اینترنتی

https: www.fragfinn.de
https: international.eco.de
https: ecsa.lucyfaithfull.org
https: parentshield.co.uk