بسم الله الرحمن الرحیم

عصر فضای مجازی

گزارش شماره ۸۴

مهر ۱۴۰۰

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

دستورالعمل‌هایی برای سیاست‌گذاران حفاظت از کودکان در فضای مجازی (۲۰۲۰)

محتوای انتشار یافته در این اثر
الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست

تهیه شده در پژوهشگاه فضای مجازی
(گروه علوم و فناوری‌های نوین)

تهیه‌کنندگان: محمد مهدی رضاپور
حمیده قراخانی‌بنی (کارشناسی ارشد مهندسی کامپیوتر دانشگاه اصفهان)

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶ غربی، پلاک ۲۰
تلفن: ۰۲۱-۸۶۱۵۱۰۶۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

بخش سوم

بخش چهارم

بخش پنجم

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

چکیده

در دنیایی که اینترنت تقریباً به هر جنبه‌ای از زندگی مدرن رخنه کرده است، حفظ امنیت کاربران کم‌سن در فضای آنلاین به یک مسئله‌ی اضطراری برای همه کشورها تبدیل شده است. هرچند اینترنت به منبعی غنی برای بازی و یادگیری کودکان تبدیل شده است، برای حضور بدون همراه، فضایی خطرناک است. کودکان امروز با خطرات زیادی از جمله مسائل مربوط به حریم خصوصی، محتوای خشن و نامناسب، کلاه‌برداران اینترنتی و سوءاستفاده و بهره‌برداری جنسی مواجه هستند. خطرات در حال افزایش هستند و مجرمان هم‌زمان در چندین حوزه فعالیت می‌کنند و کارایی واکنش‌ها و اصلاحات کشورها را کاهش می‌دهند. بعلاوه، همه‌گیری جهانی کووید ۱۹ نیز باعث افزایش حضور کودکان در فضای مجازی برای پیگیری درس‌ها و تعاملات اجتماعی شده است. محدودیت‌هایی که این ویروس بر زندگی ما اعمال کرده است باعث شده تا کودکان بسیار زودتر از آنچه که والدینشان برنامه‌ریزی کرده بودند وارد فضای مجازی شوند. همچنین گرفتاری کاری والدین نیز مانع نظارت مناسب بر فعالیت آنلاین کودکان شده است که خطر دسترسی آن‌ها به محتوای نامناسب

یا هدف قرار گرفتن از سوی مجرمان برای سوءاستفاده‌های مختلف را افزایش داده است. امروز بیش از هر زمان دیگری، حفظ امنیت کودکان در فضای مجازی به یک واکنش هماهنگ و مشارکتی از سوی بخش‌های مختلف جامعه نیاز دارد . ذینفعان زیادی از حوزه صنعت مانند پلتفرم‌های بخش خصوصی، ارائه‌دهندگان خدمات و اپراتورهای شبکه گرفته تا دولت و جامعه مدنی باید وارد عمل شوند و از این برنامه پشتیبانی کنند.

گزارش حاضر سندی تحت عنوان « دستورالعمل‌هایی برای سیاست‌گذاران حفاظت از کودکان در فضای مجازی(۲۰۲۰)» را ارائه می‌کند که در سال ۲۰۲۰ توسط اتحادیه بین‌المللی مخابرات(ITU) جهت بهره‌مندی سیاست‌گذاران مربوطه ارائه شده است. نسخه قبلی این سند در سال ۲۰۱۸ ارائه شده بوده است که با یک بازنگری، بازنویسی و بازطراحی اساسی و اعمال تغییرات عمده در چشم‌انداز دیجیتالی که کودکان در آن در حال فعالیت هستند، نسخه حاضر ارائه شده است. علاوه بر واکنش به تغییرات جدید در فناوری‌ها و پلتفرم‌های دیجیتال، نسخه جدید به کودکان دارای معلولیت توجه ویژه‌ای داشته است. دنیای آنلاین برای این کودکان فضایی کاملاً مناسب فراهم می‌آورد تا بتوانند مشارکت اجتماعی خود را تحقق بخشند. نیازهای خاص کودکان مهاجر و دیگر گروه‌های آسیب‌پذیر نیز در این نسخه جدید در نظر گرفته‌شده‌اند.

مباحث مطرح شده در مجموعه دستورالعمل‌های این سند می‌توانند در راستای تدوین اسناد و استراتژی‌های ملی حفاظت از کودکان در فضای مجازی، به سیاست‌گذاران نهادهای ذیربط کشور

کمک شایانی نماید.

واژگان کلیدی: سیاست‌گذاری محافظت از کودکان در فضای مجازی، ITU، دستورالعمل‌های حفاظت از کودکان، فضای مجازی و کودکان

مقدمه

مقدمه

سی سال پیش، تقریباً تمامی دولت‌ها متعهد به احترام به حقوق کودکان، محافظت و ارتقای آن شدند. کنوانسیون حقوق کودک سازمان ملل تنها قرارداد بین‌المللی در حوزه حقوق بشر است که بیشترین پذیرش را در کشورهای مختلف به همراه داشته است. بااینکه پیشرفت‌های قابل‌توجهی در سه دهه گذشته حاصل شده است، چالش‌های مهم هنوز پابرجا هستند و خطرات جدید برای کودکان ظاهر شده‌اند.

در سال ۲۰۱۵، تمامی کشورها تعهد خود را به کودکان در برنامه ۲۰۳۰ و ۱۷ هدف توسعه پایدار جهانی تکرار کردند. به‌عنوان مثال هدف ۲،۱۶ خواستار پایان سوءاستفاده، بهره‌کشی و هر نوع از خشونت و آزار کودکان تا سال ۲۰۳۰ شده است. اما حفاظت از کودکان بحث اصلی ۱۱ هدف از ۱۷ هدف توسعه پایدار است. طبق شکل ۱، یونیسف کودکان را در مرکز برنامه کاری ۲۰۳۰ قرار داده است.

شکل ۱. کودکان، فناوری‌های ارتباطات و اطلاعات و اهداف توسعه پایدار

برنامه کاری ۲۰۳۰ برای توسعه پایدار تصدیق می‌کند که فناوری‌های ارتباطات و اطلاعات می‌توانند نقش اساسی در دستیابی به اهداف توسعه پایدار داشته باشند. گسترش فناوری ارتباطات و اطلاعات و اتصال جهانی می‌تواند پیشرفت انسانی را سرعت بخشد، شکاف‌های دیجیتال را پر کند و جوامع دانش‌محور را توسعه دهد. این برنامه اهداف خاصی را برای استفاده از فناوری‌های ارتباطات و اطلاعات برای توسعه پایدار در آموزش (هدف ۴)، برابری جنسیتی (هدف ۵)، زیرساخت (هدف ۹ - دسترسی ارزان و مقرون‌به‌صرفه به اینترنت) و شراکت و ابزار پیاده‌سازی (هدف ۱۷) تعریف می‌کند. فناوری ارتباطات و اطلاعات با کمک به تحقق هرکدام از این ۱۷ هدف، می‌تواند اقتصاد را دچار تحول عمیق کند. فناوری ارتباطات و اطلاعات حرکت خود را آغاز کرده و به میلیاردها انسان در سرتاسر جهان دسترسی به منابع آموزشی و خدمات سلامت و خدماتی مانند دولت الکترونیک و رسانه‌های اجتماعی و بسیاری خدمات دیگر را ارائه داده است.

بدین وسیله، انفجار فناوری ارتباطات و اطلاعات فرصت‌های بی‌سابقه‌ای

را برای کودکان و نوجوانان فراهم آورده است تا ارتباط و تماس برقرار کنند، به اشتراک بگذارند، یاد بگیرند، به اطلاعات دسترسی یابند و عقاید خود را درباره مسائلی که بر زندگی و جوامع آن‌ها اثر می‌گذارند ابراز کنند.

اما دسترسی وسیع‌تر و راحت‌تر به اینترنت و فناوری موبایل چالش‌های مهمی را برای امنیت و رفاه آفلاین و آنلاین کودکان به همراه داشته است.

برای کاهش خطرات دنیای دیجیتال و هم‌زمان توانمندسازی کودکان و نوجوانان برای برخورداری از مزایای آن، دولت‌ها، جامعه مدنی، جوامع محلی، سازمان‌های بین‌المللی و صنعت باید حول یک هدف مشترک گرد هم‌آیند. سیاست‌گذاران به‌ویژه باید در رسیدن به این هدف بین‌المللی یعنی حفظ امنیت کودکان در فضای آنلاین کمک کنند.

برای پاسخ به چالش‌هایی که توسعه سریع فناوری ارتباطات و اطلاعات ایجاد کرده و همچنین چالش‌هایی که در حوزه محافظت از کودکان وجود دارد، اقدام محافظت آنلاین کودکان به‌عنوان یک اقدام چند ذینفعی از سوی اتحادیه بین‌المللی مخابرات در نوامبر ۲۰۰۸ معرفی شد. هدف این اقدام جمع‌کردن شرکا از تمامی بخش‌های جامعه جهانی است تا تجربه‌ای امن و توانمند ساز برای کودکان در تمامی جهان در فضای آنلاین فراهم آورند.

بعلاوه، کنفرانس اتحادیه بین‌المللی مخابرات که در سال ۲۰۱۸ در دبی برگزار شد بر اهمیت اقدام محافظت آنلاین کودکان تأکید کرده و آن را به‌عنوان پلتفرمی برای افزایش آگاهی، به اشتراک‌گذاری

تجربیات موفق و ارائه کمک و پشتیبانی به دولت‌های عضو به‌ویژه کشورهای در حال توسعه در توسعه و اجرای نقشه‌های راه محافظت آنلاین کودکان معرفی کرد. این کنفرانس همچنین بر اهمیت محافظت کودکان در فضای آنلاین در چارچوب کنوانسیون حقوق کودک سازمان ملل و دیگر قراردادهای حقوق بشری تأکید کرده و همکاری بین تمامی فعالان در محافظت آنلاین کودکان را خواستار شد.

کنفرانس، برنامه کاری ۲۰۳۰ برای توسعه پایدار را به رسمیت شناخته و به چندین جنبه از محافظت آنلاین کودکان در اهداف توسعه پایدار به‌ویژه اهداف ۱، ۳، ۴، ۵، ۹، ۱۰ و ۱۶ پرداخت. همچنین قطعنامه ۱۷۵ (بازبینی شده، دوبی، ۲۰۱۸) در مورد دسترسی معلولان و افراد با نیازهای خاص به فناوری ارتباطات و اطلاعات و قطعنامه ۶۷ (بازبینی شده، بوینس آیرس، ۲۰۱۷) متعلق به کنفرانس جهانی توسعه مخابرات در مورد نقش بخش توسعه مخابراتی اتحادیه بین‌المللی مخابرات در محافظت آنلاین کودکان را به رسمیت شناخت.

در اواخر سال ۲۰۱۹، کمیسیون پهنای باند اتحادیه بین‌المللی مخابرات/یونسکو برای توسعه پایدار، گزارش امنیت آنلاین کودکان را منتشر کرد که توصیه‌هایی عملی در مورد ایمن‌سازی اینترنت برای کودکان ارائه می‌داد.

در سال ۲۰۰۹، اتحادیه بین‌المللی مخابرات اولین مجموعه دستورالعمل‌های مربوط به محافظت آنلاین کودکان را در قالب اقدام محافظت آنلاین کودکان منتشر کرد. در طول یک دهه اخیر، دستورالعمل‌های محافظت آنلاین کودکان به چندین زبان ترجمه شده و بسیاری از کشورهای جهان آن را به‌عنوان مرجعی برای نقشه

راه و استراتژی‌های ملی مرتبط با محافظت آنلاین کودکان به کار بسته‌اند. این دستورالعمل‌ها به شرکت‌های دولتی، سازمان‌های مدنی، مؤسسات مراقبت از کودکان، صنعت و بسیاری فعالان در جهت محافظت آنلاین از کودکان یاری رسانده‌اند.

به‌ویژه، دستورالعمل‌ها برای تدوین، توسعه و اجرای استراتژی‌های محافظت آنلاین از کودکان در بسیاری از کشورهای عضو مانند کامرون، گابن، گامبیا، غنا، کنیا، سیرالئون، اوگاندا و زامبیا و قاره آفریقا، بحرین و عمان در منطقه عرب، برونئی، کامبوج، کروباس، اندونزی، مالزی، میانمار و وانواتو در منطقه آسیا اقتیانوسیه و بوسنی، گرجستان، مولدووا، مونته نگرو، لهستان و اوکراین در اروپا به کار رفته است.

بعلاوه، این دستورالعمل‌ها اساس رویدادهای منطقه‌ای مانند کنفرانس محافظت آنلاین کودکان، توانمندسازی شهروندان دیجیتال آینده در کامپالا، اوگاندا (۲۰۱۴) و کنفرانس محافظت آنلاین کودکان منطقه‌ای آسه آن در بانکوک تایلند (۲۰۲۰) بوده است.

بر اساس قطعنامه ۱۷۹ (بازبینی شده، دوبی، ۲۰۱۸) اتحادیه بین‌المللی مخابرات با همکاری شرکای اقدام محافظت آنلاین کودکان، چهار دستورالعمل، از جمله دستورالعمل مربوط به کودکان معلول و دارای نیازهای خاص را به‌روزرسانی کردند و توسعه فناوری در صنعت مخابرات را مدنظر قرار دادند.

درنتیجه‌ی این فرایند، متخصصان و ذینفعان مرتبط این دستورالعمل‌ها را بررسی و به‌روزرسانی کرده و توصیه‌هایی برای حفظ امنیت کودکان در دنیای دیجیتال تدوین کردند. این توصیه‌ها نتیجه همکاری ذینفعان مختلف است که از دانش، تجربه و تخصص سازمان‌ها

و افراد بسیاری در سرتاسر جهان در حوزه محافظت آنلاین کودکان بهره‌مند شده است. هدف آن‌ها نهادن اساس دنیای آنلاین امن و ایمن برای نسل‌های آینده است. این توصیه‌ها به‌عنوان نقشه راه عمل می‌کند که می‌توان آن‌ها را بر اساس عرف و قوانین کشورهای مختلف تغییر داد. بعلاوه، این دستورالعمل‌ها مسائل مربوط به تمامی کودکان زیر ۱۸ سال در شرایط زندگی مختلف و کودکان با معلولیت و نیازهای خاص را هدف قرار می‌دهد. این دستورالعمل‌ها همچنین وسعت محافظت آنلاین کودکان را افزایش داده، تمامی خطرات، تهدیدها و آسیب‌هایی که کودکان ممکن است در فضای آنلاین تجربه کنند را در برمی‌گیرد.

امید است که این دستورالعمل‌ها نه‌تنها پیشگام ساخت یک جامعه دانش‌محور جامع باشند، بلکه دولت‌های عضو اتحادیه بین‌المللی مخابرات را یاری رسانند تا وظایف خود در جهت محافظت و تحقق حقوق کودکان که در کنوانسیون حقوق کودک در قطعنامه نشست عمومی سازمان ملل ۲۵/۴۴ در ۲۰ نوامبر ۱۹۸۹ و سند نشست نتایج جامعه اطلاعات بیان شده است را انجام دهند.

با انتشار این دستورالعمل‌ها، اقدام محافظت آنلاین کودکان از تمامی ذینفعان می‌خواهد تا سیاست‌ها و راهبردهایی را اجرا کنند که کودکان را در فضای آنلاین محافظت می‌کنند و دسترسی امن‌تر آن‌ها به تمامی فرصت‌های خارق‌العاده منابع آنلاین را فراهم آورند.

بخش اول

مروری کلی بر سند

بخش اول

مروری کلی بر سند

۱-۱- هدف

دولت‌ها وظیفه دارند تا در دنیای مجازی و واقعی امنیت کودکان را تأمین کنند. امروزه فناوری‌های جدید آن‌چنان در جنبه‌های مهمی از زندگی بسیاری از کودکان و نوجوانان وارد شده است که نمی‌توان بین وقایع دنیای واقعی و مجازی تمایزی مشخص قائل شد. این دو دنیا درهم‌تنیده و به هم وابسته شده‌اند.

سیاست‌گذاران[1] و دیگر ذینفعان مرتبط نیز نقش مهمی ایفا می‌کنند. سرعت تکامل فناوری به این معنی است که بسیاری از روش‌های سنتی سیاست‌گذاری دیگر برای این هدف مناسب نیست. سیاست‌گذاران باید یک چارچوب قانونی تطبیق‌پذیر، جامع و مناسب برای عصر متغیر دیجیتال تدوین کنند تا کودکان را در فضای آنلاین محافظت کنند.

هدف این دستورالعمل‌ها ارائه یک چارچوب منعطف و کاربرپسند به دولت‌های عضو اتحادیه بین‌المللی مخابرات است تا وظایف قانونی خود را درک و اجرا کرده و کودکان را در دنیای حقیقی و مجازی محافظت کنند.

۱. اصطلاح سیاست‌گذار به تمامی افرادی اطلاق می‌شود که مسئول تدوین و اجرای سیاست‌ها به‌ویژه در حوزه حاکمیت هستند.

این دستورالعمل‌ها پرسش‌های زیر را برای سیاست‌گذاران پاسخ می‌دهند:

۱) محافظت آنلاین کودکان به چه معناست؟

۲) چرا من به‌عنوان سیاست‌گذار باید به محافظت کودکان در فضای آنلاین اهمیت دهم؟

۳) شرایط قانونی، اجتماعی-سیاسی و توسعه‌ای کشور من چگونه است؟

۴) سیاست‌گذاران چگونه باید سیاست مؤثر و پایداری را برای محافظت آنلاین کودکان در کشورهای خود تدوین کنند؟

در انجام این کار، دستورالعمل‌ها با استفاده از مدل‌ها، چارچوب‌ها و منابع موجود، تجربیات مؤثر در سرتاسر جهان را به تصویر می‌کشند.

۱-۲- گستره

گستره محافظت آنلاین کودکان هرگونه آسیبی که کودکان در فضای آنلاین در معرض آن هستند را در برمی‌گیرد. این گستره طیف وسیعی از خطراتی است که امنیت و رفاه کودکان را تهدید می‌کند. این چالشی پیچیده است که باید از زوایای مختلف ازجمله قانونی، حکومتی، آموزشی، سیاسی و اجتماعی بررسی شود.

بعلاوه، محافظت آنلاین کودکان باید بر اساس درکی از خطرات، تهدیدها و آسیب‌های عمومی و خاص هر جامعه در دنیای دیجیتال باشد. این امر نیازمند تعاریف دقیق و تعیین پارامترهای شفاف برای مداخله است که شامل و متمایزکننده افعال مجرمانه و اعمالی است که غیرقانونی نیستند اما رفاه کودک را به خطر می‌اندازند.

بدین منظور، این دستورالعمل‌ها مروری بر خطرات و تهدیدهای کنونی پیش روی کودکان در محیط‌های دیجیتال را ارائه می‌دهد. سرعت تحول فناوری و آسیب‌ها و تهدیدات مربوط به آن به این معناست که روش‌های سنتی سیاست‌گذاری نمی‌توانند با این سرعت همراه شوند. سیاست‌گذاران در عصر دیجیتال باید چارچوب‌های قانونی و سیاسی‌ای را بنا نهند که به اندازه کافی جامع و تطبیق‌پذیر باشند تا بتوانند با چالش‌های موجود مبارزه کنند و تا حد امکان چالش‌های جدید را پیش‌بینی کنند. انجام این کار نیازمند همکاری با تک‌تک ذینفعان از جمله صنعت فناوری ارتباطات و اطلاعات، جامعه تحقیقاتی، جامعه مدنی، عموم و خود کودکان است. با در نظر گرفتن تمامی اصول جامع در محافظت آنلاین کودکان می‌توان از این فرایند پشتیبانی کرد.

۱-۳- اصول جامع

یازده اصل جامع در اینجا مطرح می‌شود که با هم می‌توانند در تدوین یک استراتژی ملی، جامع و آینده‌نگر برای محافظت آنلاین کودکان به کار روند.

ترتیب این اصول نشان دهنده ترتیب منطقی است و نه ترتیب اهمیت.

استراتژی محافظت آنلاین کودکان باید:

۱. بر اساس دیدی جامع، دربرگیرنده دولت، صنعت و جامعه باشد؛

۲. ناشی از درک جامع و تحلیل کل فضای دیجیتال اما مناسب اولویت‌ها و شرایط خاص هر کشور باشد؛

۳. بـه حقـوق اساسـی کـودکان در کنوانسـیون حقـوق کـودک سـازمان ملـل و دیگـر کنوانسـیون‌ها و قوانیـن بین‌المللـی احتـرام گذاشـته و در راسـتای آن باشـد؛

۴. در راسـتای اسـتراتژی‌ها و قوانیـن داخلـی مرتبـط و مشـابه موجـود ماننـد قوانیـن سوءاسـتفاده از کـودکان و اسـتراتژی‌های امنیـت کـودکان باشـد و از آن‌هـا پیـروی کنـد؛

۵. بـه آزادی‌هـا و حقـوق کـودکان کـه نبایـد قربانـی محافظـت شـوند احتـرام بگـذارد؛

۶. بـا مشـارکت فعـال تمامـی ذینفعـان مرتبـط از جملـه خـود کـودکان، تدویـن شـود. تمامـی نیازهـا و مسـئولیت‌ها را دربرگیـرد و نیازهـای اقلیت‌هـا و گروه‌هـای حاشـیه‌ای را درنظرگیـرد؛

۷. در راسـتای برنامه‌هـای کلی‌تـر دولـت بـرای رفـاه اقتصـادی و اجتماعـی باشـد و نقـش فنـاوری ارتباطـات و اطلاعـات را بـرای توسـعه پایـدار و شـمول اجتماعـی بـه حداکثـر برسـاند؛

۸. از مناسـب‌ترین ابزارهـای سیاسـی در دسـترس اسـتفاده کنـد تـا بـا در نظـر گرفتـن شـرایط کشـور هـدف خـود را محقـق سـازد؛

۹. در بالاتریـن سـطح دولـت تدویـن شـده باشـد، کـه مسـئول تخصیص نقش‌هـا و مسـئولیت‌ها و منابـع مالـی و انسـانی کافـی اسـت؛

۱۰. بـه سـاخت محیـط دیجیتالـی کمـک کنـد کـه کـودکان، والدیـن/ مراقبـان و ذینفعـان بتواننـد بـه آن اعتمـاد کننـد؛

۱۱. تلاش‌هـای ذینفعـان در جهـت توانمندسـازی و آمـوزش کـودکان در مـورد سـواد دیجیتـال بـرای محافظـت خـود در فضـای آنلایـن را هدایـت کنـد.

۱-۴- کاربرد این دستورالعمل‌ها

این دستورالعمل‌ها تحقیقات مرتبط، مدل‌های موجود و منابع را در نظر گرفته و توصیه‌های شفافی برای تدوین یک استراتژی ملی محافظت آنلاین از کودکان را ارائه می‌دهد.

- بخش ۲ محافظت آنلاین کودکان را معرفی کرده و اطلاعاتی از تحقیقات اخیر در مورد فناوری‌های جدید، تهدیدها و آسیب‌های مهم پیش روی کودکان ارائه می‌دهد.
- بخش ۳ بیان می‌کند که چگونه می‌توان برای یک استراتژی محافظت آنلاین کودکان آمادگی کسب کرد، و تمامی ذینفعان مرتبط را دخیل کرد. همچنین نمونه‌های موجود از واکنش‌ها به آسیب‌ها و تهدیدات آنلاین و مزایای داشتن یک استراتژی آنلاین را ذکر می‌کند.
- بخش ۴ توصیه‌هایی برای چارچوب‌ها و اجرا ارائه می‌دهد.
- بخش ۵ چک‌لیست‌های ملی برای تدوین استراتژی ملی محافظت آنلاین کودکان ارائه می‌دهد.
- بخش ۶ منابع مفید را ارائه می‌دهد.

بخش دوم

مقدمه

بخش دوم

مقدمه

در سال ۲۰۱۹، بیش از نیمی از جمعیت جهان از اینترنت استفاده می‌کردند. بزرگ‌ترین گروه کاربران افراد زیر ۴۴ سال هستند، که در میان آن‌ها، افراد ۱۶ تا ۲۴ سال و ۳۵ تا ۴۴ سال بیشترین استفاده از اینترنت را داشتند. در سطح جهانی، از هر سه کودک (۰ تا ۱۸ سال) یک نفر از اینترنت استفاده می‌کند. در کشورهای در حال توسعه، کودکان و نوجوانان بیشترین استفاده از اینترنت را دارند و تخمین زده می‌شود که در پنج سال آینده، این جمعیت دو برابر شود. نسل‌های جدید با اینترنت بزرگ می‌شوند و اکثر آن‌ها، به‌ویژه در کشورهای در حال توسعه، به فناوری شبکه موبایل متصل هستند.

هرچند دسترسی به اینترنت در تحقق حقوق کودکان نقشی اساسی دارد، همچنان تفاوت‌های برجسته منطقه‌ای، ملی، جنسیتی و غیره در دسترسی وجود دارد که فرصت‌ها را برای دختران، کودکان معلول، کودکان متعلق به اقلیت‌ها و دیگر گروه‌های آسیب‌پذیر محدود می‌سازد. از لحاظ تقسیم جنسیتی دیجیتال، تحقیقات نشان می‌دهد که در هر منطقه، به‌جز ایالات متحده آمریکا، کاربران اینترنت مذکر از کاربران مؤنث بیشتر هستند. در بسیاری کشورها، دختران فرصت‌های

دسترسی مشابه پسران ندارند. حتی زمانی که این فرصت‌ها فراهم است، دختران نه‌تنها در هنگام استفاده از اینترنت محدود و نظارت می‌شوند بلکه امنیت خود را در هنگام استفاده از اینترنت در خطر بیشتری می‌بینند. مشخص است که کودکان و نوجوانانی که مهارت‌های دیجیتال ندارند یا به زبان‌های اقلیت صحبت می‌کنند نمی‌توانند به‌راحتی محتوای آنلاین مرتبط را پیدا کنند. همچنین، کودکان از مناطق روستایی مهارت‌های دیجیتال کمتری دارند، زمان بیشتری را در فضای آنلاین سپری می‌کنند (به‌ویژه با بازی کردن) و نظارت و مداخله کمتری از سوی والدین دریافت می‌کنند.

اما هر گفتگویی در مورد خطرات و تهدیدات باید ماهیت مفید و توانمندساز فناوری دیجیتال را نیز تأیید کند. اینترنت و فناوری‌های دیجیتال در حال دگرگون ساختن نحوه زندگی ما هستند و راه‌های جدیدی را برای برقراری ارتباط، بازی کردن، لذت بردن از موسیقی و انجام فعالیت‌های فرهنگی، آموزشی و مهارت‌سازی برای ما گشوده‌اند. اینترنت می‌تواند دسترسی کلیدی به خدمات سلامت و آموزشی و اطلاعات در مورد موضوعاتی ارائه دهد که برای نوجوانان مهم هستند اما ممکن است در جوامع آن‌ها ممنوع باشند.

کودکان و نوجوانان در خط مقدم پذیرش و استفاده از فرصت‌های جدید ارائه‌شده از سوی اینترنت هستند. اما به همان میزان در معرض مشکلات امنیتی و سلامتی هستند که جامعه باید آن‌ها را تصدیق کرده و با آن‌ها مبارزه کند. باید این خطرات را که در پیش روی کودکان و نوجوانان در فضای آنلاین است با شفافیت به بحث کشید. بحث‌ها می‌توانند پلتفرمی را بگشایند که از طریق آن کودکان و

نوجوانان بتوانند بیاموزند که چگونه خطرات را شناسایی کنند، از آسیب‌ها جلوگیری کنند و با آن‌ها مبارزه کنند. این بحث‌ها هم‌زمان باید مزایا و فرصت‌های اینترنت را برشمارند.

در بسیاری از مناطق جهان، افراد کم‌سن درک خوبی از برخی از خطرات آنلاین دارند. تحقیقات نشان داده است که به‌عنوان مثال اکثریت کودکان و نوجوانان می‌توانند زورگویی آنلاین را از تمسخر و آزار آنلاین متمایز سازند. آن‌ها می‌دانند که زورگویی آنلاین آسیب‌رسان است اما برقراری تعادل بین فرصت‌ها و خطرات آنلاین برای کودکان هنوز یک چالش است.

برای دولت‌های عضو اتحادیه بین‌المللی مخابرات، محافظت از کودکان و نوجوانان در فضای آنلاین همچنان یک اولویت است که باید در تعادل با تلاش‌ها در جهت افزایش فرصت‌های آنلاین برای کودکان باشد. این کار باید به‌گونه‌ای انجام شود که بر دسترسی آن‌ها یا عموم بر اطلاعات، یا برخورداری از آزادی بیان و ارتباطات تأثیر نگذارد.

بین کودکان و بزرگسالان شکاف دیجیتالی وجود دارد که راهنمایی را از جانب والدین، معلمان و سرپرستان محدود می‌کند. به همین دلیل سرمایه‌گذاری و راه‌حل‌های خلاقانه برای برطرف کردن خطرات پیش روی کودکان در فضای آنلاین مورد نیاز است. وقتی کودکان بزرگ می‌شوند و به والدین و اعضای فعال جامعه تبدیل می‌شوند، برای آن‌ها فرصتی پیش می‌آید تا شکاف دیجیتال را کاهش دهند.

در این راستا، اعتمادسازی در اینترنت باید اولویت سیاست

عمومی باشد. دولت‌ها و جامعه باید با کودکان و نوجوانان کار کنند تا نظرات آن‌ها را درک کنند و بحث‌های عمومی صریح در مورد خطرات و فرصت‌ها راه بیندازند. حمایت از کودکان و نوجوانان برای مدیریت خطرات آنلاین می‌تواند مؤثر باشد اما دولت‌ها باید اطمینان حاصل کنند که خدمات حمایتی مناسب برای افرادی که آسیب‌های آنلاین را تجربه می‌کنند وجود دارد و اینکه کودکان می‌دانند چگونه به این خدمات دسترسی یابند.

برخی کشورها در تخصیص منابع کافی برای ارتقای سواد دیجیتال و امنیت آنلاین کودکان مشکل دارند. اما کودکان عقیده دارند که والدین، معلمان، شرکت‌های فناوری و دولت‌ها بازیگران مهمی در تدوین راه‌حل‌ها برای حمایت از امنیت آنلاین آن‌ها هستند. دولت‌های عضو اتحادیه بین‌المللی مخابرات نیز اذعان کرده‌اند که از تلاش‌های هماهنگ و به اشتراک‌گذاری اطلاعات برای حفظ امنیت آنلاین تعداد بیشتری از کودکان حمایت می‌کنند.

فضای دیجیتال برای کودکان روزبه‌روز پیچیده‌تر می‌شود و استفاده از هوش مصنوعی برای یادگیری ماشینی، تحلیل کلان‌داده، رباتیک، واقعیت افزوده و مجازی و اینترنت اشیا فعالیت‌های رسانه‌ای کودکان را متحول می‌کند. این کار نیازمند سیاست‌گذاری و سرمایه‌گذاری برای کودکان، والدین و جوامع آینده و امروزی است.

۲-۱- محافظت آنلاین کودکان چیست؟

فناوری‌های آنلاین فرصت‌های زیادی را برای برقراری ارتباط، یادگیری مهارت‌های جدید، افزایش خلاقیت و ساخت جامعه‌ای بهتر پیش

روی کودکان قرار می‌دهد. اما این فناوری‌ها می‌توانند خطراتی نیز برای آن‌ها به همراه داشته باشند. مشکلاتی از قبیل حریم خصوصی، محتوای غیرقانونی، مزاحمت، زورگویی آنلاین، سوءاستفاده از داده‌های شخصی یا آماده‌سازی برای اهداف جنسی و حتی سوءاستفاده جنسی از کودکان، از جمله این خطرات هستند.

این دستورالعمل‌ها رویکردی جامع ایجاد می‌کنند تا به‌تمامی خطرات و آسیب‌های احتمالی پیش روی کودکان در هنگام کسب سواد دیجیتال بپردازند. طبق این دستورالعمل‌ها، تمامی ذینفعان مرتبط در انعطاف‌پذیری، رفاه و محافظت آنلاین کودکان نقش دارند و هم‌زمان کودکان از فرصت‌هایی که اینترنت ارائه می‌دهد برخوردار می‌شوند.

محافظت از کودکان یک مسئولیت اشتراکی است و بر عهده تمامی ذینفعان است تا آینده‌ای پایدار برای همگان رقم زنند. به این منظور، سیاست‌گذاران، صنعت، والدین، سرپرستان، آموزگاران و دیگر ذینفعان باید مطمئن شوند که کودکان و نوجوانان می‌توانند ظرفیت‌های آنلاین و آفلاین خود را تحقق بخشند.

هرچند هیچ تعریف جهانی برای محافظت آنلاین کودکان وجود ندارد، هدف جامع آن ایجاد فضای دیجیتال امن، مناسب سن، همه‌شمول و مشارکتی برای کودکان و نوجوانان است، که ویژگی‌های آن شامل موارد زیر می‌شود:

- پاسخ، حمایت و کمک به خود در مقابله با تهدیدها؛
- پیشگیری از آسیب؛
- تعادل پویا بین محافظت و ارائه فرصت برای کودکان و تبدیل

1. accountability

شدن به شهروندان دیجیتال؛

• حمایت از حقوق و مسئولیت‌های کودکان و جامعه.

بعلاوه، به دلیل پیشرفت‌های سریع در فناوری و جامعه و ماهیت بدون مرز اینترنت، محافظت آنلاین کودکان باید سریع و تطبیق‌پذیر باشد تا بتواند اثربخش باشد. این دستورالعمل‌ها بینش‌هایی را در مورد تهدیدهای پیش روی کودکان در فضای آنلاین ارائه می‌دهد که شامل محتوای غیرقانونی و آسیب‌زا، آزار، زورگویی آنلاین، سوءاستفاده از داده‌های شخصی، یا آماده‌سازی برای اهداف جنسی و سوءاستفاده و بهره‌کشی جنسی است. با این وجود، چالش‌های جدید با نوآوری‌های فناوری جدید ظاهر می‌شوند که از منطقه‌ای به منطقه دیگر متفاوت هستند. اما چالش‌های جدید را می‌توان با همکاری در سطح جهانی به بهترین شکل برطرف کرد چون برای این چالش‌ها باید راه‌حل‌های جدید یافت شود.

۲-۲- کودکان در دنیای دیجیتال

اینترنت نحوه زندگی ما را دگرگون کرده است و وارد تمامی جنبه‌های زندگی کودکان شده است. امروزه نمی‌توان دنیای فیزیکی و دیجیتال را جدای از هم تصور کرد. یک‌سوم تمامی کاربران اینترنت کودکان و نوجوانان هستند و یونیسف تخمین می‌زند که ۷۱ درصد نوجوانان در فضای آنلاین حضور دارند.

این حجم از اتصال به اینترنت قدرت زیادی را به کودکان و نوجوانان می‌دهد. دنیای آنلاین به کودکان امکان می‌دهد تا بر نابرابری‌ها و معلولیت چیره شوند و حوزه‌های جدیدی از سرگرمی، آموزش،

مشارکت و برقراری روابط بیابند. پلتفرم‌های دیجیتال امروزه برای فعالیت‌های زیادی به کار می‌روند و اغلب تجربیات چندرسانه‌ای ارائه می‌دهند.

دسترسی به آموزش استفاده از این فناوری برای رشد کودکان اهمیت حیاتی دارد و اغلب نیز در سنین پایین رخ می‌دهد. سیاست‌گذاران باید درک کنند که کودکان و نوجوانان اغلب استفاده از این پلتفرم‌ها و خدمات را قبل از رسیدن به حداقل سن مجاز آغاز می‌کنند بنابراین آموزش نیز باید زودتر شروع شود.

کودکان و نوجوانان می‌خواهند که در گفتگوها دخیل باشند و به‌عنوان افرادی که در عصر دیجیتال متولد شده‌اند تخصصی دارند که می‌توانند به اشتراک بگذارند. سیاست‌گذاران و فعالان باید در مورد محیط‌های آنلاین با کودکان و نوجوانان بحث‌های پیوسته داشته باشند تا از حقوق آن‌ها دفاع کنند.

دسترسی به اینترنت

در سال ۲۰۱۹، بیش از نیمی از جمعیت جهان از اینترنت استفاده می‌کردند (۶,۵۳ درصد) که به‌طور تخمینی معادل ۱,۴ میلیارد نفر بود. در سطح جهانی، از هر سه کاربر اینترنت یک نفر کودک زیر ۱۸ سال است. در برخی کشورهای کم‌درآمد، این نسبت یک به دو است و در کشورهای پردرآمدتر، این نسبت یک به پنج است. بر اساس آمار یونیسف، ۷۱ درصد نوجوانان در سطح جهان به فضای آنلاین دسترسی دارند. در نتیجه کودکان و نوجوانان حضوری اساسی، دائمی و ثابت در اینترنت دارند. اینترنت اهداف اجتماعی، اقتصادی و سیاسی

دیگری را برآورده می‌کند و به یک کالا یا خدمت خانوادگی یا مصرفی تبدیل شده است که نقش اساسی در زندگی خانواده‌ها و کودکان دارد.

در سال ۲۰۱۷، دسترسی کودکان و نوجوانان به اینترنت ارتباط بالایی با سطح درآمد داشت. کشورهای کم درآمد نسبت به کشورهای پردرآمد تعداد کاربران کودک کمتری داشتند.

کودکان و نوجوانان در بیشتر کشورها در آخر هفته نسبت به روزهای هفته زمان بیشتری را در اینترنت می‌گذرانند. نوجوانان (۱۵ تا ۱۷ سال) بیشترین زمان را در اینترنت صرف می‌کنند که بسته به کشور به‌طور متوسط بین ۵٫۲ تا ۳٫۵ ساعت در هفته است.

استفاده از اینترنت

در میان کودکان و نوجوانان، محبوب‌ترین وسیله برای دسترسی به اینترنت گوشی موبایل است و پس از آن کامپیوتر دسکتاپ و لپ‌تاپ. کودکان و نوجوانان به‌طور متوسط دو ساعت در روز در طول هفته و چهار ساعت در روز در آخر هفته را در اینترنت صرف می‌کنند. برخی از آن‌ها به‌طور دائم به اینترنت وصل هستند. اما بسیاری دیگر هنوز به اینترنت خانگی دسترسی ندارند.

در عمل، اکثر کودکان و جوانانی که از اینترنت استفاده می‌کنند از طریق بیش از یک دستگاه به آن متصل می‌شوند. کودکان و جوانانی که هر هفته به اینترنت وصل می‌شوند، از حداکثر سه دستگاه مختلف برای این کار استفاده می‌کنند. کودکان با سن بالاتر یا ساکن کشورهای ثروتمندتر از دستگاه‌های بیشتری استفاده می‌کنند و در تمام کشورهای مورد بررسی، پسران نسبت به دختران از دستگاه‌های

بیشتری استفاده می‌کنند.

محبوب‌ترین فعالیت (در میان دختران و پسران) تماشای کلیپ‌های ویدیویی است. بیش از سه چهارم کودکان و نوجوانان کاربر اینترنت اعلام کرده‌اند که حداقل هفته‌ای یک بار ویدیوهای آنلاین تماشا می‌کنند که یا به‌تنهایی است و یا به همراه خانواده. بسیاری از کودکان و جوانان را می‌توان کاربران فعال رسانه‌های اجتماعی مانند فیسبوک، توییتر، تیک‌تاک یا اینستاگرام دانست.

کودکان و نوجوانان همچنین در مسائل سیاسی آنلاین وارد می‌شوند و از طریق نوشتن بلاگ عقاید خود را بیان می‌کنند.

سطح کلی مشارکت در بازی‌های آنلاین در کشورهای مختلف متفاوت است که در راستای دسترسی کودکان و نوجوانان به اینترنت است. ۱۰ تا ۳۰ درصد کودکان و نوجوانان کاربر اینترنت هر هفته در فعالیت‌های خلاقانه آنلاین شرکت می‌کنند.

برای مقاصد آموزشی، بسیاری از کودکان و نوجوانان از تمامی سنین هر هفته برای انجام تکالیف و یا حتی رسیدن به کلاس پس از غیبت در رده‌ها یا کسب اطلاعات در مورد سلامتی از اینترنت استفاده می‌کنند. به نظر می‌رسد که کودکان با سنین بالاتر اشتیاق بیشتری برای اطلاعات دارند تا کودکان کم‌سن‌تر.

۲-۳- اثر فناوری بر تجربیات دیجیتال کودکان

اینترنت و فناوری دیجیتال می‌توانند فرصت‌ها و تهدیدهایی برای کودکان به همراه داشته باشند. به‌عنوان مثال، زمانی که کودکان از رسانه‌های اجتماعی استفاده می‌کنند، فرصت‌های زیادی در اختیار دارند

تا یاد بگیرند، کشف کنند، ارتباط برقرار کنند و مهارت‌های جدید کسب کنند. به‌عنوان مثال، شبکه‌های اجتماعی برای کودکان پلتفرم‌هایی هستند که به آن‌ها امکان می‌دهند تا هویت شخصی خود را در یک فضای امن کشف کنند. داشتن مهارت‌های مناسب و دانستن چگونگی مبارزه با مشکلات مربوط به حریم شخصی و شهرت برای کودکان ضروری است.

«من می‌دانم که هر چیزی که در اینترنت منتشر می‌شود تا ابد در آنجا باقی می‌ماند و می‌تواند زندگی شما را در آینده تحت تأثیر قرار دهد.» پسر ۱۴ ساله از شیلی

اما مشاوره‌ها نشان می‌دهند که اکثر کودکان قبل از سن حداقلی ۱۳ سال از رسانه‌های اجتماعی استفاده می‌کنند و خدمات اعتبارسنجی سن نیز اکثراً ضعیف و ناقص هستند. در این شرایط خطرات پیش روی کودکان می‌تواند بیشتر شود. هرچند کودکان می‌خواهند مهارت‌های دیجیتال را فرا بگیرند و به شهروندان دیجیتال تبدیل شوند و به‌ویژه به حریم خصوصی خود اهمیت می‌دهند، حریم خصوصی را در رابطه با دوستان و آشنایان خود در نظر می‌گیرند: «دوستانم چه چیزی را می‌توانند ببینند؟» و کمتر به غریبه‌ها و اشخاص ثالث فکر می‌کنند. این امر، به همراه کنجکاوی طبیعی کودکان و آستانه‌ی پایین‌تر آن‌ها در برابر ریسک، آن‌ها را در معرض بهره‌کشی، زورگویی یا دیگر محتوا و تماس‌های آسیب‌زا قرار می‌دهد.

محبوبیت گسترده به اشتراک‌گذاری تصاویر و ویدیو از طریق اپ‌های موبایل و به‌ویژه استفاده کودکان از پلتفرم‌های پخش آنلاین، خطرات و

مشکلات مربوط به حریم شخصی را افزایش داده است. برخی کودکان تصاویر جنسی از خود تولید می‌کنند و دوستان و خواهر و برادرهای آن‌ها این تصاویر را در فضای آنلاین به اشتراک می‌گذارند. برای برخی، به‌ویژه کودکان در سنین بالاتر، این امر می‌تواند فرایند طبیعی اکتشاف جنسیت و هویت جنسی باشد. اما برای برخی دیگر، به‌ویژه در سنین پایین‌تر، اغلب زورگویی از سوی یک بزرگسال یا کودک دیگر دخیل است. دلیل هر چه که باشد، محتوای تولیدی در بسیاری از کشورها غیرقانونی است و می‌تواند کودکان را در معرض تعقیب قانونی قرار دهد یا می‌تواند برای بهره‌کشی بیشتر از کودک به کار رود.

به همین ترتیب، بازی‌های آنلاین به کودکان امکان می‌دهند که حق اساسی خود برای بازی کردن را تحقق بخشند، شبکه روابط بسازند، با دوستان خود وقت بگذرانند، دوستان جدید پیدا کنند و مهارت‌های مهم فراگیرند. این تأثیر می‌تواند بسیار مثبت باشد. اما شواهد زیادی وجود دارد مبنی بر اینکه اگر بزرگسالان بر این پلتفرم‌های بازی آنلاین نظارت نداشته باشند، می‌توانند خطراتی برای کودکان به همراه داشته باشند، از اختلالات بازی، خطرات مالی، جمع‌آوری و کسب درآمد از داده‌های شخصی کودکان گرفته تا زورگویی آنلاین، سخنان ناشی از نفرت، خشونت و قرار گرفتن در معرض محتوای نامناسب و آماده‌سازی برای سوءاستفاده جنسی. این کارها با استفاده از تصاویر واقعی، کامپیوتری یا حتی واقعیت مجازی و ویدیوهایی انجام می‌شود که سوءاستفاده و بهره‌برداری جنسی از کودکان را به تصویر کشیده و عادی‌سازی می‌کنند.

بعلاوه، توسعه فناوری منجر به ظهور اینترنت اشیا شده است که در آن تعداد روزافزونی از وسایل به اینترنت وصل می‌شوند و از طریق آن ارتباط برقرار می‌کنند. این دستگاه‌ها شامل اسباب‌بازی‌ها، دستگاه‌های نظارت بر نوزادان، و دستگاه‌هایی است که با هوش مصنوعی کار می‌کنند و می‌توانند خطراتی از لحاظ حریم خصوصی و محتوای ناخواسته به همراه داشته باشند.

۲-۴- خطرات اصلی فضای آنلاین برای کودکان

بزرگسالان و کودکان در فضای آنلاین در معرض خطرات و تهدیداتی هستند. اما کودکان آسیب‌پذیرتر هستند. برخی کودکان از کودکان دیگر آسیب‌پذیرتر هستند، مانند کودکان دارای معلولیت یا کودکان مهاجر. سیاست‌گذاران باید تضمین کنند که تمامی کودکان در فضای دیجیتال امن رشد کرده و آموزش ببینند. آسیب‌پذیر بودن کودکان و لزوم محافظت از آن‌ها در مقابل تمامی شکل‌های سوءاستفاده در کنوانسیون حقوق کودک سازمان ملل ذکر شده است.

حوزه‌های مختلف محیط آنلاین فرصت‌های مناسبی در اختیار کودکان قرار می‌دهند اما ممکن است هم‌زمان خطراتی را برای آن‌ها داشته باشند که به آن‌ها آسیب عمیق بزنند و سلامت آن‌ها را تضعیف کنند. بزرگسالان و کودکان به یک‌میزان در معرض حمله به حریم خصوصی، دریافت اطلاعات نادرست، و حتی بدتر، دسترسی به پورنوگرافی، قرار دارند.

در اینجا تمایز بین ریسک و آسیب برای کودکان حیاتی است. هر فعالیتی که ممکن است عناصری از ریسک به همراه داشته باشد

مخاطره‌آمیز نیست و هر ریسکی لزوماً برای کودکان آسیب‌زا نیست. به‌عنوان مثال، ارسال پیام‌های جنسی، که برای نوجوانان راهی است برای کشف جنسیت و روابط، ممکن است لزوماً آسیب‌زا نباشد.

	محتوا کودک به‌عنوان دریافت‌کننده (تولیدات انبوه)	تماس کودک به‌عنوان شرکت‌کننده (فعالیتی که بزرگ‌سال تشویق کرده است)	رفتار کودک به‌عنوان عمل‌کننده (مجرم/قربانی)
خشن	محتوای خشونت‌آمیز / ناخوشایند	آزار، تعقیب	زورگویی، فعالیت خصمانه همسالان
جنسی	محتوای پورنوگرافیک	آماده‌سازی، سوءاستفاده جنسی در ملاقات با غریبه‌ها	آزار جنسی، پیامک جنسی
ارزش‌ها	محتوای نژادپرستانه / نفرت‌انگیز	متقاعدسازی ایدئولوژیک	محتوای تولیدی کاربران بالقوه آسیب‌زا
تجاری	تبلیغات، بازاریابی نهفته	سوءاستفاده از داده‌های شخصی	قمار، تخلف از کپی‌رایت

شکل ۲. طبقه‌بندی تهدیدات آنلاین برای کودکان

ظهور عصر دیجیتال چالش‌های جدیدی را برای محافظت از کودکان به همراه داشته است. کودکان باید توانمند شوند تا در امنیت در دنیای آنلاین فعالیت کنند و از مزایای آن بهره‌مند شوند.

سیاست‌گذاران باید اطمینان حاصل کنند که قوانین مرتبط، ابزارها و محافظت‌های مناسب برای یادگیری و رشد امن کودکان تهیه می‌شوند. کودکان باید مهارت‌های لازم را کسب کنند تا تهدیدات را شناسایی کرده و عواقب و جزییات رفتارهای آنلاین خود را به‌طور کامل درک کنند.

کودکان در فضای آنلاین با خطرات زیادی از سوی سازمان‌ها،

بزرگ‌سالان و همسالان خود مواجه می‌شوند.

۲-۴-۱- محتوا و دست‌کاری

• قرار گرفتن در معرض محتوای نامناسب و حتی مجرمانه می‌تواند کودکان را به کارهای افراطی مانند آسیب زدن به خود و رفتارهای خشن و تخریب‌گر سوق دهد. چنین محتوایی می‌تواند به گرایش به افکار رادیکال، نژادپرستانه یا تبعیض‌آمیز منجر شود. بسیاری از کودکان از محدودیت‌های سنی وبسایت‌ها تبعیت نمی‌کنند.

• اطلاعات نادرست یا ناکامل درک کودکان از دنیای پیرامون را محدود می‌کند. شخصی‌سازی محتوا بر اساس رفتارهای کاربر می‌تواند به «حباب فیلتر» منجر شود که کودکان را از رشد و دریافت طیف وسیعی از محتوا محروم کند.

• محتوایی که الگوریتم‌ها فیلتر کرده‌اند می‌تواند بر رشد، عقاید، ارزش‌ها و عادات کودک تأثیر بگذارد. قرار دادن کودکان در «اتاق‌های پژواک» یا «حباب‌های فیلتر» آن‌ها را از دسترسی به عقاید و افکار متنوع بازمی‌دارد.

۲-۴-۲- تماس از جانب بزرگ‌سالان یا همسالان

کودکان می‌توانند در معرض تهدیدهای تماسی مختلفی از جانب همسالان یا بزرگ‌سالان قرار گیرند.

• زورگویی آنلاین می‌تواند نسبت به زورگویی آفلاین بسیار وسیع‌تر و سریع‌تر گسترش یابد. می‌تواند در هر زمانی از روز یا شب رخ دهد و در نتیجه فضاهایی که قبلاً امن بودند را مورد تهاجم

قرار دهد. همچنین می‌تواند از سوی منبعی بی‌نام باشد.

• کودکانی که در فضای آفلاین قربانی می‌شوند می‌توانند در فضای آنلاین هم قربانی شوند. این امر کودکان دارای معلولیت را در معرض ریسک‌های آنلاین بیشتری قرار می‌دهد چون طبق تحقیقات، کودکان معلول بیشتر هرگونه سوءاستفاده را تجربه می‌کنند و به‌ویژه در معرض آزار جنسی بیشتر هستند. این آزارها می‌تواند شامل زورگویی، اذیت، طرد شدن و تبعیض بر اساس معلولیت واقعی یا درک شده کودک و یا بر اساس جنبه‌هایی از معلولیت مانند نحوه رفتار یا گفتار یا تجهیزات و خدمات مورد استفاده او باشد.

• آسیب به آبرو و حیثیت: تصاویر و ویدیوها می‌توانند تغییر داده شوند و در دسترس میلیاردها نفر قرار گیرند. نظرات منفی می‌توانند تا دهه‌ها در دسترس و معرض دید همگان باشند.

• مجرمان می‌توانند از طریق اینترنت کودکان را هدف قرار دهند، برای مقاصد جنسی آماده سازند و مورد سوءاستفاده قرار دهند. این اقدامات می‌تواند در سطح محلی یا در نقطه‌ای دیگر از جهان انجام شود، و فرد مجرم اغلب در مورد هویت خود دروغ می‌گوید. این کار می‌تواند به شکل‌های مختلفی انجام شود مانند تحمیل عقاید رادیکال یا متقاعدسازی به ارسال محتوای جنسی از خود.

• تحمیل فشار، فریب یا متقاعدسازی برای خرید آنلاین بدون اجازه پرداخت‌کننده

• تبلیغات ناخواسته مسائلی از قبیل رضایت یا فروش داده‌ها را به همراه دارد.

۲-۴-۳-رفتار کودک می‌تواند به پیامدهایی منجر شود

• زورگویی آنلاین می‌تواند آزاردهنده و آسیب‌رسان باشد چون می‌تواند در سطح وسیع‌تری گسترش یابد، عمومیت بیشتری یابد و محتوایی که به‌صورت الکترونیک منتشر می‌شود می‌تواند هرزمانی بازیابی شود. درنتیجه، قربانی زورگویی سخت‌تر می‌تواند از حادثه بهبود یابد؛ زورگویی می‌تواند شامل تصاویر آسیب‌رسان یا حرف‌های آزاردهنده باشد. محتوا ۲۴ ساعت روز در دسترس است؛ زورگویی الکترونیک می‌تواند ۲۴ ساعته و هفت روز هفته رخ دهد بنابراین می‌تواند حریم شخصی قربانی را مورد تجاوز قرار دهد، حتی در مکان‌هایی امن مانند خانه. و اطلاعات شخصی می‌تواند دست‌کاری شود، عکس‌ها تغییر داده شوند، و در دسترس دیگران قرار گیرند. بعلاوه، این کار می‌تواند به‌صورت بی‌نام انجام شود. افشای اطلاعات شخصی منجر به آسیب فیزیکی، مواجهه واقعی با آشنایان آنلاین، و امکان سوءاستفاده فیزیکی و یا جنسی می‌شود.

• تخلف از حقوق خود یا دیگران از طریق سرقت ادبی و بارگذاری محتوا بدون اجازه، شامل دریافت و بارگذاری عکس‌های نامناسب بدون اجازه.

• تخلف از حقوق کپی‌رایت مانند دانلود موسیقی، فیلم یا برنامه‌های تلویزیونی که باید برای آن‌ها هزینه پرداخت شود می‌تواند برای قربانی دزدی آسیب‌زا باشد.

• استفاده بیش‌ازحد یا اعتیادگونه از اینترنت و یا بازی‌های آنلاین، به‌گونه‌ای که به فعالیت‌های اجتماعی یا بیرونی مهم برای

سلامتی، اعتمادبه‌نفس، رشد اجتماعی و رفاه عمومی آسیب بزند.

• تلاش برای آسیب زدن، آزار رساندن یا زورگویی به فردی دیگر، خود را جای فرد دیگر (اغلب کودکی دیگر) جا زدن.

• رفتاری که در میان کودکان امروزی در حال افزایش است، ارسال پیامک‌های جنسی است (ارسال تصاویر یا پیام‌های جنسی از طریق گوشی موبایل). این تصاویر و پیام‌ها اغلب بین شرکای رابطه یا شرکای احتمالی ردوبدل می‌شوند اما گاهی اوقات در دسترس مخاطبان بیشتری قرار می‌گیرند. کودکان و نوجوانان درک مناسبی از پیامدهای این رفتارها و ریسک‌های احتمالی آن‌ها ندارند.

۲-۵- آسیب‌های کلیدی برای کودکان در فضای آنلاین

بخش قبلی به تهدیداتی پرداخت که کودکان در فضای آنلاین تجربه می‌کنند. در این بخش به آسیب‌های ناشی از این تهدیدات می‌پردازیم.

آسیب‌ها

بر اساس مطالعات یونیسف در مورد کاربرد اینترنت، موارد زیر شامل ریسک‌ها و آسیب‌ها می‌شوند:

- آسیب به خود و سوءاستفاده از خود:
  - محتوای خودکشی
  - تبعیض
- قرار گرفتن در معرض محتوای نامناسب
  - قرار گرفتن در معرض محتوای خشن/ افراطی/ ناخوشایند
  - بازاریابی نهفته

• قمار آنلاین

- در حدود ۲۰ درصد کودکان شرکت‌کننده در نظرسنجی اعلام کردند که در یک سال گذشته وب‌سایت‌ها یا بحث‌های آنلاینی دیده‌اند که در مورد افرادی بوده است که به خود آسیب جسمی رسانده‌اند.

- رادیکال سازی:

• متقاعدسازی ایدئولوژیک

• سخنان نفرت پراکن

- کودکان بیشتر گزارش می‌دهند که از محتوای جنسی یا سخنان نفرت پراکن آنلاین، دیدن رفتارهای منفی آنلاین یا آفلاین، یا ملاقات فیزیکی با فردی که در ابتدا به‌صورت آنلاین با او آشنا شده بودند، ناراحت شده‌اند.

- سوءاستفاده و بهره‌کشی جنسی

• محتوایی که توسط کودک تولیدشده است

• آماده‌سازی جنسی

• مطالب سوءاستفاده جنسی از کودکان

• قاچاق

• بهره‌کشی جنسی از کودکان در سفر و توریسم

مطالعه‌ای که در سال ۲۰۱۷ روی کودکان در دانمارک، مجارستان و انگلستان انجام شد نشان داد که ۶ درصد کودکان تصاویر جنسی از خود دارند که بدون اجازه آن‌ها به اشتراک گذاشته‌شده است.

در سال ۲۰۱۹، بنیاد دیده‌بان اینترنت[1] بیش از ۱۳۲۰۰۰ صفحه وب را شناسایی کرد که تصاویر و ویدیوهایی از سوءاستفاده جنسی

1. Internet Watch Foundation

از کودکان داشتند. هر صفحه وب می‌تواند حاوی یک تا هزاران تصویر از این دست باشد.

ریسک‌های مربوط به خشونت آنلاین، مانند انتشار تصاویر برهنه بدون رضایت و زورگویی آنلاین جنسی در میان دختران و پسران متفاوت است. دختران بیشتر تحت فشار برای انجام رفتارهای جنسی قرار می‌گیرند و پیامدهای منفی و آسیب‌زای بیشتری را تجربه می‌کنند.

- سوءاستفاده از داده‌های شخصی
  - هک
  - کلاه‌برداری و سرقت

بسیاری از مردم با کلاه‌برداری و هک آشنا هستند اما تجاوز به حریم شخصی در رابطه با فعالیت‌های آنلاین کودکان یک نوع دیگر تخلف محسوب می‌شود. بزرگسالان اغلب با بررسی موبایل‌ها و رصد فعالیت‌های آنلاین کودکان، به آن‌ها صدمه می‌زنند. به‌عنوان‌مثال، گزارش‌هایی از برزیل نشان می‌دهد که پسران و دختران از گروه‌های مختلف سنی، فکر می‌کنند که والدین بیشتر بر استفاده دختران از اینترنت کنترل دارند. برای توضیح این پدیده گفته می‌شود که دختران ممکن است در شرایط مشابه به دلیل ساختارهای اجتماعی که در آن زندگی می‌کنند، به‌ویژه ازلحاظ امنیت، در فضایی که مرز بین تعاملات آنلاین و آفلاین محو شده است، در معرض آسیب بیشتری هستند.

- زورگویی آنلاین، تعقیب و آزار: فعالیت خصمانه یا خشن از سوی همسالان

اتاق‌های گفتگوی آنلاین و شبکه‌های اجتماعی می‌توانند درها را برای خشونت و زورگویی بگشایند چون کاربران گمنام، از جمله کودکان، وارد ارتباط خشن یا سوءاستفاده‌گر می‌شوند. در هفت کشور اروپایی (بلژیک، دانمارک، ایرلند، ایتالیا، پرتغال، رومانی و انگلستان) لیوینگستون، ماشرونی، اولافسون و هادون[1] دریافتند که به‌طور متوسط در سال ۲۰۱۰، ۸ درصد کودکان زورگویی آنلاین را تجربه کرده بودند، در حالی که این رقم در سال ۲۰۱۴ به ۱۲ درصد رسید.

باید در نظر گرفت که کودکان آسیب‌پذیر اغلب با خطر بیشتری برای زورگویی آنلاین مواجه هستند.

۲-۵-۱- بحث: تقویت نابرابری‌ها

در سال ۲۰۱۷، حدود ۶۰ درصد کودکان در منطقه آفریقا به اینترنت دسترسی نداشتند، که این رقم در اروپا تنها ۴ درصد بود. کاربران مذکر اینترنت در تمامی مناطق جهان از کاربران مؤنث بیشتر هستند و دختران در استفاده از اینترنت بیشتر نظارت و محدود می‌شوند. با گسترش پهنای باند به مناطقی از جهان که به اینترنت دسترسی ندارند، این نابرابری با افزایش شدید مواجه خواهد شد.

کودکانی که به‌جای کامپیوتر از گوشی موبایل استفاده می‌کنند، تجربه ضعیف‌تری در اینترنت دارند. کودکانی که به زبان‌های اقلیت صحبت می‌کنند، اغلب نمی‌توانند محتوای مناسب را در فضای آنلاین پیدا کنند، و کودکان از مناطق روستایی بیشتر در معرض سرقت پسورد یا پول هستند.

1. Livingstone, Mascheroni, Ólafsson, and Haddon1

تحقیقات نشان می‌دهند که بسیاری از نوجوانان در سرتاسر جهان باید از موانع زیادی عبور کنند تا به مشارکت آنلاین برسند. برای بسیاری، چالش‌های مربوط به دسترسی، اتصال ضعیف، هزینه‌های بالای اینترنت و دستگاه‌ها، و نداشتن تجهیزات مناسب، از موانع اصلی هستند.

با گسترش پهنای باند ارزان در کشورهای درحال‌توسعه، نیاز ضروری برای کاهش ریسک و خطرات پیش روی کودکان وجود دارد که هم‌زمان آن‌ها را قادر سازد بر روی تمامی مزایای دنیای دیجیتال سرمایه‌گذاری کنند.

۲-۵-۲-بحث: محتوای سوءاستفاده جنسی از کودکان

مقیاس مسئله

اینترنت، مقیاس و ماهیت تولید، توزیع و دسترسی به مطالب سوءاستفاده جنسی از کودکان را تغییر داده است. در سال ۲۰۱۸، شرکت‌های فناوری در آمریکا بیش از ۴۵ میلیون عکس و فیلم آنلاین را گزارش کردند که مشکوک به سوءاستفاده جنسی از کودکان در سرتاسر جهان بودند. این یک صنعت جهانی است و مقیاس و شدت سوءاستفاده، علیرغم تلاش‌ها برای توقف آن، در حال افزایش است.

در گذشته، در دنیای آفلاین، مجرمان برای یافتن محتوای سوءاستفاده جنسی از کودکان باید خطرات و هزینه‌های بزرگی را متحمل می‌شدند. با ظهور اینترنت، مجرمان می‌توانند به‌سادگی به این نوع محتوا دسترسی یابند و رفتارهای پرخطر انجام دهند. دوربین‌ها کوچک‌تر شده‌اند، وارد همه جنبه‌های زندگی ما شده‌اند و فرایند تولید محتوای سوءاستفاده جنسی از کودکان و دسترسی به محتوا از

سوءاستفاده غیرتماسی راحت‌تر از قبل شده است.

نمی‌توان مشخص کرد که این فعالیت‌های غیرقانونی و مخفی به چه شکل و اندازه هستند. اما مشخص است که تعداد تصاویر غیرقانونی که اکنون در دسترس است به میلیون‌ها می‌رسد. تقریباً تمامی این تصاویر از کودکان تکثیرشده‌اند. در سال ۲۰۱۸، طبق پیگیری بنیاد دیده‌بان اینترنت، تصاویر کودکی که در سال ۲۰۱۳ نجات داده شده بود، چند بار دیده شده بود؟ در طول سه ماه، تحلیلگران بنیاد دیده‌بان اینترنت تصاویر را ۳۴۷ بار رهگیری کردند: پنج بار در هر روز کاری.

چشم‌انداز کنونی

هر بار که تصویری از یک کودک در حال سوءاستفاده در فضای آنلاین ظاهر می‌شود، یا به دست یک مجرم دانلود می‌شود، این کودک دوباره مورد سوءاستفاده قرار می‌گیرد. این تصاویر به‌طور دائمی در فضای اینترنت وجود دارد و منتشر می‌شود و قربانیان مجبورند با این موضوع برای همیشه زندگی کنند.

به‌محض اینکه محتوا یا وب‌سایتی کشف می‌شود که سوءاستفاده کودکان را به تصویر می‌کشد، باید به‌سرعت حذف و مسدود شود. ماهیت جهانی اینترنت این کار را دشوار می‌سازد: مجرمان می‌توانند محتوا را در یک کشور تولید کنند، میزبان سایت را در کشوری دیگر قرار دهند و آن را در کشوری سوم در دسترس مصرف‌کنندگان قرار دهند. بدون مشارکت گسترده جهانی، نمی‌توان آگهی‌ها و حکم‌ها را در سطح ملی اجرا کرد.

سرعت نوآوری در دنیای دیجیتال به این معنی است که چشم‌انداز برای مجرمان دائماً در حال تغییر است. خطرات اصلی که اخیراً ظاهر شده‌اند شامل موارد زیر است:

- ظهور پیام‌های کدگذاری شده به مجرمان امکان می‌دهد که محتوای مجرمانه را با کانال‌های مخفی به اشتراک بگذارند در حالیکه کشف و اعمال قوانین به همین اندازه سخت‌تر است.
- تالارهای گفتگو مخصوص آماده‌سازی کودکان در گوشه‌های مخفی اینترنت، این رفتار را نرمال‌سازی و تشویق می‌کنند. در چنین محیط‌هایی کودکان اغلب نیاز به ارائه‌ی «محتوای جدید» دارند تا اجازه ورود یابند.
- گسترش سریع اینترنت به کاربران امکان می‌دهد تا در مناطقی به اینترنت متصل شوند که هنوز استراتژی‌های پیشگیرانه جامع یا زیرساخت‌های مربوطه را ندارند.
- کودکان از سنین کم از دستگاه‌هایی استفاده می‌کنند که تحت نظارت والدین نیستند. رفتار جنسی در فضای آنلاین نرمال‌سازی شده است. تعداد تصاویری که کودکان از خود تهیه‌کرده‌اند هر سال افزایش می‌یابد.

۲-۵-۳- بحث: محتوای تولید شده به دست کودک

کودکان و نوجوانان ممکن است تصاویر نامناسبی از خود تهیه کنند. این رفتار لزوماً غیرقانونی نیست و می‌تواند به‌عنوان بخشی از رشد جنسی سالم و نرمال انجام شود. اما خطراتی وجود دارد مبنی بر اینکه این محتوا در فضای آنلاین و آفلاین منتشر شود و کودکان

را در معرض آسیب قرار دهد یا به‌عنوان وسیله‌ای برای باج‌گیری به کار رود. هرچند برخی از کودکان ممکن است برای به اشتراک گذاشتن این تصاویر تحت فشار قرار گیرند، دیگران (به‌ویژه نوجوانان) ممکن است خودخواسته این محتوای جنسی را تولید کنند. این به معنای رضایت یا مسئولیت در قبال انتشار یا استفاده سوء یا بهره‌برداری از این تصاویر نیست.

ارسال پیام‌های جنسی به‌عنوان «تولید تصاویر جنسی توسط خود کاربر» یا «تبادل پیام‌ها و تصاویر جنسی» و «ایجاد، به اشتراک‌گذاری و ارسال تصاویر برهنه یا نیمه برهنه از طریق موبایل و اینترنت» تعریف شده است. پیام‌های جنسی نوعی محتوای جنسی تولید شده توسط کاربر است که «از لحاظ موقعیت، معنا و قصد، بسیار متنوع است.»

هرچند ارسال پیام‌های جنسی معمول‌ترین نوع محتوای جنسی تولید شده توسط کاربر است که کودکان انجام می‌دهند، و اغلب به دست نوجوانانی انجام می‌شود که از این تجربه رضایت دارند و لذت می‌برند، بسیاری از انواع پیام‌های جنسی ناخواسته نیز وجود دارد. این نمونه‌ها شامل جنبه‌های بدون رضایت فعالیت می‌شود مانند ارسال یا دریافت ناخواسته عکس، ویدیو، یا پیام جنسی از سوی فردی شناخته یا ناشناخته که تلاش می‌کند با کودک ارتباط برقرار کند، یا او را تحت فشار قرار دهد. ارسال پیام‌های جنسی می‌تواند نوعی زورگویی جنسی باشد که در آن کودک تحت فشار قرار می‌گیرد تا به دوست دختر/دوست پسر/ هم‌سال خود عکسی ارسال کند و او نیز بدون رضایت کودک، محتوا را برای دیگر

همسالان ارسال می‌کند.

۲-۵-۴-بحث: زورگویی آنلاین

هرچند زورگویی پدیده‌ای است که به قبل از اینترنت برمی‌گردد، مقیاس، وسعت و دوام زورگویی آنلاین بسیار بیشتر است که می‌تواند آنچه که برای قربانیان آزاردهنده و آسیب‌زا است را شدت بخشد. زورگویی آنلاین به‌عنوان آزار مکرر و عمدی از طریق استفاده از کامپیوتر، گوشی همراه، و دیگر لوازم الکترونیک تعریف شده است. زورگویی آنلاین اغلب در کنار زورگویی آفلاین در مدرسه یا جایی دیگر رخ می‌دهد و می‌تواند ابعاد نژادپرستانه، مذهبی یا جنسی قوی‌تری داشته باشد. همچنین می‌تواند در ادامه آزار آفلاین باشد مثلاً از طریق هک حساب فردی، انتشار عکس‌ها و ویدیوهای آنلاین و محتوا و پیام‌های آزاردهنده‌ای که به‌طور دائمی در دسترس هستند. به‌طور کلی، به‌عنوان یک مشکل اجتماعی و نه مجرمانه، سیاست‌ها برای مقابله با زورگویی آنلاین نیاز به یک رویکرد جامع دارد که شامل مدارس، خانواده‌ها و خود کودکان باشد.

۲-۵-۵- بحث: آماده‌سازی و اخاذی آنلاین

با پیشرفت‌های سریع فناوری و افزایش دسترسی به اینترنت و ارتباطات دیجیتال در مهروموم‌های اخیر، ریسک فعالیت‌های مجرمانه در مقابل کودکان نیز افزایش یافته است. آماده‌سازی آنلاین و اخاذی جنسی کودکان شکل‌های نوظهور سوءاستفاده جنسی آنلاین هستند. آماده‌سازی آنلاین به‌طورکلی به این معناست که یک بزرگسال با کودک

دوست می‌شود و از طریق اینترنت و دیگر فناوری‌های دیجیتال بر او اثر می‌گذارد تا با او تعامل جنسی تماسی و غیرتماسی برقرار کند. از طریق فرایند آماده‌سازی، مجرم کودک را مجبور به حفظ رازداری می‌کند تا از کشف و تنبیه جلوگیری کند. این نوع سوءاستفاده در میان همسالان نیز وجود دارد.

اینترپل گزارش می‌دهد که اینترنت به دلیل ارائه اهداف در دسترس و جذب کودک به دست مجرم، آماده‌سازی آنلاین را تسهیل کرده است. مجرمان جنسی کودک آنلاین با استفاده از فریب، متقاعدسازی و اغوا، کودکان را وادار به انجام فعالیت‌های جنسی می‌کنند. فرد آماده‌ساز از فرایند عمدی شناسایی قربانی آسیب‌پذیر احتمالی، جمع‌آوری اطلاعات در مورد حمایت خانوادگی کودک، و استفاده از فشار یا شرم/ترس برای سوءاستفاده جنسی از کودک استفاده می‌کند. آماده‌سازی ممکن است از محتوای پورنوگرافی بزرگسالان و سوءاستفاده از کودکان استفاده کند تا اهداف احتمالی خود را آماده سازند و فعالیت جنسی کودکان را نرمال و طبیعی جلوه دهند. اینترنت نحوه تعامل مردم را تغییر داده و مفهوم «دوست» را بازتعریف کرده است. فرد آماده‌ساز می‌تواند با کودک از طریق اینترنت راحت و سریع رابطه دوستی برقرار کند. این امر ارزیابی دوباره پیام‌های آموزشی «غریبه - خطر» را واجب می‌سازد.

آماده‌سازی آنلاین ابتدا در یک سند قانونی بین‌المللی در سال ۲۰۰۷ از سوی شورای اروپایی کنوانسیون محافظت از کودکان در مقابل سوءاستفاده جنسی و بهره‌کشی جنسی (کنوانسیون لانزاروتی)[1] به‌طور رسمی به رسمیت شناخته شد. بند ۲۳ «نزدیک شدن به کودکان

1.Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)

بـا اهـداف جنسـی» را جـرم می‌دانـد کـه شـامل پیشـنهاد عمـدی بـرای ملاقـات بـا کـودک بـا هـدف انجـام جـرم جنسـی و پـس‌ازآن «اعمـال فیزیکـی منجـر بـه چنیـن ملاقاتـی» اسـت. در بسـیاری از مـوارد آماده‌سـازی، کـودکان در فضـای آنلایـن مـورد سوءاسـتفاده و بهره‌کشـی قـرار می‌گیرنـد. «ملاقاتـی» کـه کنوانسـیون لانزاروتـی و بسـیاری قوانیـن ملـی موجـود ذکـر می‌کننـد کامـلاً مجـازی اسـت امـا بـه همـان انـدازه ملاقـات فیزیکـی بـرای کـودک آسـیب‌زا اسـت.

اخـاذی جنسـی به‌عنـوان بخشـی از آماده‌سـازی آنلایـن یـا به‌عنـوان یـک جـرم مسـتقل انجـام می‌شـود. هرچنـد اخـاذی جنسـی می‌توانـد بـدون آماده‌سـازی آنلایـن انجـام شـود، در برخـی مـوارد آماده‌سـازی آنلایـن می‌توانـد بـه اخـاذی جنسـی منجـر شـود. فـرد آماده‌سـاز در طـول فراینـد آماده‌سـازی از طریـق تهدیـد، تـرس و متقاعدسـازی کـودک را فریـب می‌دهـد و بـر او اثـر می‌گـذارد تـا تصاویـر جنسـی از خـود ارسـال کننـد (محتـوای تولیدشـده توسـط کـودک). اگـر قربانـی نتوانـد ایـن درخواسـت‌ها را انجـام دهـد، تصاویـر خصوصـی، پـول یـا مزایـای بیشـتری در اختیـار او قـرار داده می‌شـود. یـا اینکـه تصاویـر او در فضـای آنلایـن منتشـر می‌شـوند تـا بـا تحقیـر و تـرس کـودک را مجبـور بـه ارائـه محتـوای جنسـی بیشـتر کننـد.

اخـاذی جنسـی، بـه دلیـل اثـرات روانـی و عاطفـی مشـابهی کـه بـر قربانیـان دارد، به‌عنـوان «تجـاوز جنسـی مجـازی» نامیـده شـده اسـت. در برخـی مـوارد، سوءاسـتفاده آن‌چنـان ضربـه‌ای بـه شـخص وارد می‌کنـد کـه قربانیـان تـلاش می‌کننـد بـه خـود آسـیب برسـانند یـا خودکشـی کننـد تـا از سوءاسـتفاده فـرار کننـد.

یوروپل[1] اعلام کرده است که جمع‌آوری اطلاعات برای ارزیابی وسعت اخاذی جنسی کودکان دشوار است و ممکن است موارد زیادی از آن گزارش نشده باشد. بعلاوه، نبود اصطلاحات و تعاریف مشترک برای آماده‌سازی آنلاین و اخاذی جنسی مانع جمع‌آوری داده‌های دقیق و درک وسعت واقعی مسائل در سطح جهانی است.

۲-۶- کودکان آسیب‌پذیر

کودکان و نوجوانان می‌توانند به دلایل مختلفی آسیب‌پذیر باشند. تحقیقاتی که در سال ۲۰۱۹ انجام شد نشان داده است که «زندگی دیجیتال کودکان آسیب‌پذیر، به‌ندرت آن توجه دقیق و حساسی را دریافت می‌کند که سختی‌های زندگی واقعی آن‌ها جلب می‌کند.» بعلاوه، گزارش می‌گوید که «این کودکان در بهترین حالت همان توصیه‌های کلی امنیت آنلاین را دریافت می‌کنند که در دسترس همه کودکان است، در حالی که مداخله تخصصی لازم دارند.»

سه نمونه از آسیب‌پذیری‌های خاص شامل کودکان مهاجر، کودکان با طیف اوتیسم و کودکان معلول هستند. اما مسلماً موارد بسیار زیادی وجود دارند.

۲-۶-۱- کودکان مهاجر

کودکان و نوجوانان مهاجر اغلب به کشوری مهاجرت می‌کنند که تجربیات و انتظارات اجتماعی-فرهنگی خاصی دارند. هرچند فناوری معمولاً تسهیل‌کننده ارتباط و مشارکت است، ریسک‌ها و فرصت‌های آنلاین می‌توانند در موقعیت‌های مختلف متفاوت باشند. بعلاوه، یافته‌های

1. Europol

تجربی نشان می‌دهند که رسانه‌های دیجیتال نقش حیاتی دارند. این رسانه‌ها

- نقش مهمی در سازگاری دارند (در هنگام مهاجرت به یک کشور جدید).
- نقش مهمی در آشنایی با جامعه و فرهنگ کشور مقصد دارند.
- رسانه‌های اجتماعی می‌توانند نقش مهمی در برقراری ارتباط با خانواده و همسالان و دسترسی به اطلاعات عمومی داشته باشند.

علاوه بر بسیاری از جنبه‌های مثبت، رسانه‌های دیجیتال می‌توانند چالش‌هایی را برای مهاجران به همراه داشته باشند:

- زیرساخت: باید در مورد فضاهای امن آنلاین فکر کرد تا کودکان مهاجر بتوانند از حریم خصوصی و امنیت بهره ببرند.
- منابع: مهاجران بیشتر پول خود را صرف کارت‌های تلفن اعتباری می‌کنند.
- یکپارچه‌سازی: در کنار دسترسی به فناوری، کودکان مهاجر نیز باید آموزش دیجیتال خوبی دریافت کنند.

۲-۶-۲- کودکان با اختلال طیف اوتیسم

طیف اوتیسم دو ویژگی اصلی را در فرایند تشخیص رفتاری DSM-5 دارد:

- رفتار تکراری و محدود (نیاز به شباهت)
- مشکل در رفتارهای ارتباطی و اجتماعی
- موارد مکرر ناتوانی فکری، مشکلات زبانی و غیره.

فنـاوری و اینترنـت فرصت‌هـای بیشـماری بـرای یادگیـری، برقـراری ارتبـاط و بـازی در اختیـار کـودکان قـرار می‌دهنـد. امـا در کنـار ایـن مزایـا، خطراتـی نیـز وجـود دارد کـه کـودکان مبتـلا بـه اوتیسـم بیشـتر در مقابـل آن‌هـا آسـیب‌پذیر هسـتند:

- اینترنـت می‌توانـد بـه کـودکان دارای اوتیسـم فرصت‌هایـی بـرای برقـراری روابـط اجتماعـی و پرداختـن بـه علایـق خـود بدهـد کـه در فضـای آفلایـن از آن محـروم هسـتند.
- چالش‌هـای خـاص ماننـد دشـواری در درک مقاصـد دیگـران می‌توانـد ایـن گـروه را نسـبت بـه «دوسـتان» بـا مقاصـد بد آسـیب‌پذیر سـازد.
- چالش‌هـای آنلایـن اغلـب بـا ویژگی‌هـای اصلـی اوتیسـم مرتبـط هسـتند: راهنمایـی خـاص و ملمـوس می‌توانـد تجربیـات آنلایـن افـراد را بهبـود بخشـد امـا چالش‌هـای اصلـی باقـی می‌ماننـد.

۲-۶-۳-کودکان دارای معلولیت

خطراتـی کـه کودکان معلـول در فضای آنلاین تجربه می‌کنند در بسـیاری مـوارد ماننـد خطراتـی اسـت کـه کـودکان غیرمعلـول تجربـه می‌کننـد امـا ممکـن اسـت ریسـک‌هایی را نیـز تجربـه کننـد کـه مختـص معلولیـت آن‌هـا باشـد. کـودکان دارای معلولیـت اغلـب طردشـدگی، محرومیـت، موانع (فیزیکـی، اقتصـادی، اجتماعـی و خلقـی) را در مقابـل مشـارکت در جوامـع خـود تجربـه می‌کننـد. ایـن تجربیـات می‌تواننـد کـودک معلـول را بـه سـمت دوسـتی و تعامـلات اجتماعـی در فضـای آنلایـن سـوق دهنـد، کـه می‌توانـد مثبـت بـوده، عـزت نفـس بـه او بدهـد و شـبکه‌های حمایتـی بـرای او ایجـاد کنـد. امـا، ایـن امـر می‌توانـد آن‌هـا را در خطـر بزرگ‌تـری

از لحاظ آماده‌سازی، آزار جنسی و ارتباطات آنلاین قرار دهد. تحقیقات نشان داده است که کودکانی که در فضای آفلاین با مشکل مواجه هستند و کودکانی که مشکلات روان‌شناختی دارند بیشتر در خطر این تجربیات هستند.

به‌طورکلی، کودکانی که در فضای آفلاین قربانی می‌شوند، با احتمال بیشتری در فضای آنلاین قربانی می‌شوند. این امر کودکان معلول را در خطر آنلاین بالاتری قرار می‌دهد. از طرفی آن‌ها نسبت به سایر کودکان نیاز بیشتری برای حضور آنلاین دارند. طبق تحقیقات، کودکان معلول بیشتر در معرض هرگونه سوءاستفاده هستند و به‌ویژه آزار جنسی را بیشتر تجربه می‌کنند. آزار می‌تواند شامل زورگویی، محرومیت، تبعیض و اذیت بر اساس معلولیت واقعی یا درک شده کودک باشد یا بر اساس جنبه‌هایی از معلولیت مانند نحوه صحبت یا رفتار یا تجهیزات و خدماتی که استفاده می‌کنند باشد.

مجرمان آماده‌سازی، ارتباطات غیرمجاز آنلاین، و آزار جنسی کودکان معلول نه‌تنها می‌توانند کودکان را هدف قرار دهند، بلکه کودکان معلول را نیز هدف قرار می‌دهند. چنین مجرمانی ممکن است شامل «دوستدارها» باشند- افراد غیرمعلول که به افراد معلول گرایش جنسی دارند برخی از آن‌ها وانمود می‌کنند که خود نیز معلول هستند. این افراد ممکن است عکس‌ها و ویدیوهای کودکان معلول را دانلود کنند یا در تالارهای گفتگوی مخصوص یا حساب‌های رسانه‌های اجتماعی به اشتراک بگذارند. ابزارهای گزارش‌دهی در این تالارهای گفتگو و رسانه‌های اجتماعی اغلب مسیر مناسب یا هدفمندی برای برخورد با این اعمال ندارند.

نگرانی‌هایی مبنی بر اینکه به‌اشتراک‌گذاری عکس‌های کودکان به دست والدین در فضای آنلاین می‌تواند نقض حریم خصوصی کودک باشد، به زورگویی منجر شود، باعث خجالت کودک شود، یا در سال‌های بعد برای او پیامدهای منفی داشته باشد وجود دارد. والدین کودکان معلول ممکن است چنین اطلاعاتی را برای دریافت حمایت یا توصیه به اشتراک بگذارند و کودکان معلول را در ریسک بالاتری از لحاظ پیامدهای منفی قرار دهند.

برخی کودکان معلول ممکن است مشکلاتی را در استفاده و حتی محرومیت از محیط‌های آنلاین به دلیل طراحی غیرقابل‌دسترس (مانند اپ‌هایی که اجازه بزرگ شدن اندازه متن را نمی‌دهند)، نداشتن امکانات مورد نیاز(مانند نرم‌افزار خوانش صفحه یا کنترل‌های کامپیوتری قابل تطبیق)، یا نیاز به حمایت مناسب (مانند آموزش نحوه استفاده از تجهیزات، حمایت فردی در تعاملات اجتماعی) را تجربه کنند.

در رابطه با خطرات مربوط به قرارداد یا شرایط و ضوابط، کودکان معلول در خطر بالاتری برای پذیرش شرایط بلندمدت قرار دارند که گاهی مواقع حتی بزرگسالان هم نمی‌توانند درک کنند.

۲-۷- درک کودکان از ریسک‌های آنلاین

دسترسی به محتوا، کالاها و خدمات نامناسب، قرار گرفتن در معرض خشونت در سطح جهانی، نگرانی‌ها در مورد استفاده بیش از حد، مشکلات مربوط به محافظت از داده‌ها و حریم شخصی ریسک‌هایی هستند که کودکان در معرض آن قرار دارند.

نوجوانان طیفی از نگرانی‌ها را در مورد استفاده از فناوری‌های دیجیتال گزارش می‌کنند. این نگرانی‌ها شامل موارد معمول آنلاین می‌شود، مانند ترس از تعامل با غریبه‌ها در فضای آنلاین، دسترسی به محتوای نامناسب یا قرار گرفتن در معرض ویروس و بدافزار. دیگر نگرانی‌ها شامل قابل‌اعتماد بودن دسترسی به فناوری، مزاحمت والدین در زندگی خصوص آنلاین آن‌ها و مهارت‌های سواد دیجیتالی آن‌ها می‌شود.

تحقیقات آنلاین کودکان اتحادیه اروپا نشان می‌دهند که محتوای خشن و پورنوگرافی بالاترین نگرانی‌ها در مورد فعالیت آنلاین کودکان در اروپا هستند. به‌طورکلی، پسران بیشتر تحت تأثیر خشونت و دختران بیشتر نگران خطرات مربوط به تماس هستند. نگرانی در مورد خطرات در کشورهای «مصرف بالا، خطر بالا» بیشتر است.

در آمریکای لاتین، مشاوره‌های کودکان نشان داده است که از دست دادن حریم شخصی، خشونت و آزار از مهم‌ترین نگرانی‌ها هستند. کودکان گزارش می‌کنند که، به‌ویژه هنگام بازی‌های آنلاین، افرادی با آن‌ها تماس می‌گیرند که نمی‌شناسند. در چنین مواردی، به نظر می‌رسد که استراتژی اصلی وارد نشدن به ارتباط یا بلاک کردن فرد باشد. دختران در رسانه‌های اجتماعی از سنین پایین با آزار مواجه می‌شوند. آن‌ها می‌توانند با بلاک کردن فرد یا تغییر تنظیمات حریم شخصی، این نوع از خشونت را به‌تنهایی مدیریت کنند. آزار از سوی کاربرانی انجام می‌شود که گاهی اوقات اسپانیایی صحبت نمی‌کنند اما می‌توانند برای آن‌ها عکس ارسال کنند، درخواست دوستی بدهند، و در مورد پست‌های آن‌ها نظر بگذارند. برخی پسران نیز

گزارش کرده‌اند که چنین درخواست‌هایی را دریافت کرده‌اند.

در بسیاری از مناطق دنیا، کودکان درک خوبی از برخی ریسک‌های آنلاین دارند. تحقیقات نشان داده است که اکثر کودکان می‌توانند بین زورگویی آنلاین و تمسخر یا شوخی آنلاین تمایز قائل شوند و می‌دانند که زورگویی آنلاین ابعاد اجتماعی دارد و به‌منظور آسیب رساندن انجام می‌شود.

بخش سوم

آمادگی برای یک استراتژی ملی حمایت از کودکان آنلاین

بخش سوم

آمادگی برای یک استراتژی ملی حمایت از کودکان آنلاین

در تدوین استراتژی ملی حمایت از کودکان آنلاین برای ارتقا امنیت آنلاین کودکان و نوجوانان، دولت‌های ملی و نهادهای سیاست‌گذار باید بهترین روش‌ها را شناسایی کرده و ذینفعان اصلی را دخیل کنند. بخش‌های زیر بازیگران و ذینفعان معمولی را به همراه خلاصه‌ای از نقش و مسئولیت‌های بالقوه آن‌ها در رابطه با محافظت آنلاین از کودکان ترسیم می‌کنند.

۳-۱- بازیگران و ذینفعان

سیاست‌گذاران می‌توانند افراد، گروه‌ها و سازمان‌های مناسب را در حوزه قضایی خود شناسایی کنند که نماینده این بازیگران و ذینفعان باشند. درک همه فعالیت‌های فعلی، برنامه‌ریزی‌شده و بالقوه آن‌ها در هرگونه هماهنگی ملی و تنظیم استراتژی‌های حفاظت آنلاین کودکان مهم است.

۳-۱-۱- کودکان و جوانان

در سراسر جهان کودکان و نوجوانان نشان داده‌اند که می‌توانند با سهولت

بسیار با فناوری‌های جدید سازگار شوند و از آن‌ها استفاده کنند. اینترنت در مدارس و به‌عنوان عرصه‌ای که کودکان می‌توانند در آن کار، بازی و ارتباط برقرار کنند ، اهمیت بیشتری پیدا می‌کند.

طبق آخرین گزارش ائتلاف صندوق کودکان[1] ، فقط ۱,۱۸ درصد از کودکان مصاحبه شده فکر می‌کنند مسئولان حکومتی برای محافظت از آن‌ها عمل می‌کنند. سیاست‌گذاران باید در این زمینه کودکان را دخیل کنند ، و حق آن‌ها را برای شنیده شدن به رسمیت بشناسند (ماده ۱۲ CRC).

سیاست‌گذاران برای محافظت از کودکان باید تعریف استانداردی از کودک در تمام اسناد قانونی ارائه کنند. کودک باید به‌عنوان هر فرد زیر ۱۸ سال تعریف شود. این با ماده ۱ کنوانسیون حقوق کودک سازمان ملل متحد[2] (UNCRC) مطابقت دارد که می‌گوید «منظور از کودک هر انسانی زیر ۱۸ سال است» . شرکت‌ها نباید اجازه داشته باشند هر فردی که زیر ۱۸ سال است اما می‌تواند ازلحاظ قانونی با پردازش داده‌ها موافقت کند را بزرگ‌سال در نظر بگیرند. این حقوق کودکان را تضعیف می‌کند و امنیت آن‌ها را تهدید می‌کند.

در حالی که ممکن است بسیاری از کودکان در استفاده از فناوری اعتماد به نفس داشته باشند، بسیاری از آن‌ها در فضای آنلاین احساس ناامنی دارند و نگرانی‌های زیادی در مورد اینترنت دارند.

کمبود تجربه کودکان و جوانان در دنیا می‌تواند آن‌ها را در معرض خطرات مختلفی قرار دهد. آن‌ها حق دارند انتظار کمک و حمایت داشته باشند. همچنین لازم به یادآوری است که همه کودکان و جوانان اینترنت یا فناوری‌های جدید را به یک روش تجربه نخواهند

1. ChildFund Alliance
2. UN Convention on the Rights of the Child

کـرد. برخـی از کـودکان بـا نیازهـای ویـژه ناشـی از ناتوانی‌هـای جسـمی یـا سـایر معلولیت‌هـا ممکـن اسـت به‌ویـژه در یـک محیـط آنلایـن آسـیب‌پذیر باشـند و بـه حمایـت بیشـتری نیـاز داشـته باشـند.

بررسـی‌ها به‌طـور مکـرر نشـان داده اسـت کـه آنچـه بزرگ‌سـالان فکـر می‌کننـد کـودکان و جوانـان به‌صـورت آنلایـن انجـام می‌دهنـد و آنچـه درواقـع اتفـاق می‌افتـد می‌توانـد بسـیار متفـاوت باشـد. نیمـی از کـودکان مـورد بررسـی گفتنـد کـه در کشورشـان بزرگ‌سـالان بـه نظـر آن‌هـا در مـورد موضوعاتـی کـه بـرای آن‌هـا مهـم اسـت گـوش نمی‌دهنـد. بـه همیـن دلیـل، بایـد اطمینـان حاصـل کـرد کـه در تمامـی برنامه‌ریزی‌هـا در سـطح ملـی و سیاسـت‌گذاری در ایـن زمینـه، سـازوکارهای مناسـب وجـود داشـته باشـد تـا صـدای کـودکان شـنیده شـود و تجربیـات عینـی آن‌هـا در اسـتفاده از فنـاوری در نظـر گرفتـه شـود.

۳-۱-۲- والدین، سرپرستان، مربیان

والدیـن ، سرپرسـتان و مربیـان بیشـترین وقـت را با کـودکان می‌گذرانند. آن‌هـا بایـد سـواد دیجیتـال داشـته باشـند تـا محیـط آنلایـن را درک کننـد و بتواننـد از کـودکان محافظـت کننـد و بـه آن‌هـا بیاموزنـد کـه چگونـه از خـود محافظـت کنند.

وظیفـه ویـژه مؤسسـات آموزشـی ایـن اسـت کـه بـه کـودکان بیاموزنـد چگونـه در اینترنـت ، چـه از اینترنـت در مدرسـه، در خانـه و یـا هـر جـای دیگـر کـه از اینترنـت اسـتفاده می‌کننـد، امنیـت خـود را حفـظ کننـد. سیاسـت‌گذاران بایـد از سـنین پاییـن (۳ تـا ۱۸ سـال) سـواد دیجیتـال را در برنامه‌هـای درسـی ملـی قـرار دهنـد. بدین‌وسـیله کـودکان می‌تواننـد

از خود محافظت کنند، از حقوق خود آگاه شوند و بنابراین از اینترنت به‌عنوان وسیله‌ای برای کسب دانش استفاده کنند.

سیاست‌گذاران باید بدانند که والدین و سرپرستان تقریباً همیشه اولین، آخرین و بهترین خط دفاعی و حمایت از فرزندان خود خواهند بود. با این حال، والدین ممکن است در فضای اینترنت سردرگم شوند. در اینجا نیز مدارس می‌توانند به‌عنوان یک کانال مهم برای ارتباط با والدین و سرپرستان عمل کنند تا آن‌ها را از خطرات و بسیاری از امکانات مثبت فناوری‌های جدید آگاه سازند. با این حال، مدارس نباید تنها مسیری باشند که برای تماس با والدین و سرپرستان استفاده می‌شود. استفاده از کانال‌های مختلف بسیار مهم است تا امکان دسترسی به بیشترین تعداد ممکن از والدین و سرپرستان فراهم شود. صنعت در اینجا نقش مهمی در حمایت از کاربران یا مشتریان آن‌ها دارد. والدین و سرپرستان ممکن است تصمیم بگیرند که فعالیت آنلاین و دسترسی کودک خود را مدیریت کنند، با او در مورد رفتار صحیح و استفاده از فناوری صحبت کنند، رفتارهای کودک در فضای آنلاین را درک کنند، تا گفتگوی خانوادگی بتواند تجارب آنلاین و آفلاین را یکپارچه سازد.

والدین و سرپرستان نیز باید الگوی خوبی در مورد نحوه استفاده از وسایل و رفتارهای مناسب در اینترنت برای فرزندانشان باشند. سیاست‌گذاران باید بدانند که والدین و مراقبین برای دستیابی به دیدگاه‌ها، تجربیات و درک صحیح محافظت آنلاین از کودکان به مشاوره نیاز دارند.

درنهایت، سیاست‌گذاران به همراه سایر نهادهای عمومی می‌توانند

کمپین‌های آگاهی عمومی، از جمله برای والدین، مراقبان و مربیان را ترتیب دهند. کتابخانه‌های عمومی، مراکز بهداشتی، حتی مراکز خرید و سایر مراکز عمده تجاری می‌توانند مکان‌های قابل دسترسی برای ارائه اطلاعات ایمنی الکترونیکی و مهارت‌های دیجیتال باشند. در انجام این کار، دولت‌ها باید اطمینان حاصل کنند که در توصیه‌های ارائه‌شده ، بدون هیچ‌گونه منفعت شخصی و بی‌طرف عمل کرده و موضوعات متنوعی را در فضای دیجیتال پوشش دهند.

۳-۱-۳- صنعت

صنعت یکی از ذینفعان اصلی در اکوسیستم است زیرا این بخش دارای دانش فناوری است که سیاست‌گذاران برای توسعه چارچوب قانونی باید به آن بپردازند و آن را درک کنند.

همچنین، صنعت باید تشویق شود تا هنگام توسعه فناوری جدید امنیت را در کسب‌وکار خود تلفیق کند. شرکت‌هایی که محصولات و خدمات با فناوری جدید را تولید یا ارائه می‌کنند باید به کاربران خود کمک کنند تا نحوه کار و نحوه استفاده ایمن و مناسب از آن‌ها را فرابگیرند.

مسئولیت مهم صنعت این است که آگاهی در مورد فضای آنلاین و امنیت را به‌ویژه برای کودکان و والدین و سرپرستان آن‌ها و همچنین کل جامعه ارتقا دهند. ذینفعان صنعت به این روش در مورد نگرانی‌های دیگر ذینفعان و ریسک‌ها و آسیب‌های پیش روی کاربران نهایی اطلاعات بیشتری کسب می‌کنند. با این اطلاعات، صنعت می‌تواند کالاها و خدمات موجود را اصلاح کرده و خطرات را در طراحی شناسایی کند.

پیشرفت‌های اخیر در هوش مصنوعی به صنعت امکان می‌دهند تا برای شناسایی کاربر و فراهم آوردن فضایی مفید برای رفتار آنلاین مثبت، اقدامات کنترلی مناسبی انجام دهد. این پیشرفت‌ها می‌توانند ریسک‌هایی برای کودکان نیز به همراه داشته باشند.

در برخی کشورها، اینترنت تحت یک چارچوب خودمقرراتی و هم‌مقرراتی مدیریت می‌شود. اما برخی کشورها چارچوب‌های قانونی و مقرراتی مانند اجبار شرکت‌ها به شناسایی، مسدود، و حذف آسیب علیه کودکان از پلتفرم‌ها و خدمات و ارائه مسیرهای گزارش‌دهی شفاف و دسترسی به حمایت را اجرا کرده‌اند.

۳-۱-۴- جامعه تحقیقاتی و سازمان‌های غیردولتی

در دانشگاه‌ها و جامعه پژوهشی، به احتمال زیاد طیف وسیعی از دانشگاهیان و دانش‌پژوهان هستند که علاقه حرفه‌ای و شناخت دقیقی از تأثیرات اجتماعی و فنی اینترنت دارند. آن‌ها از منظر کمک به دولت‌ها و سیاست‌گذاران ملی در تدوین استراتژی‌های مبتنی بر حقایق عملی و شواهد درست، یک منبع بسیار ارزشمند هستند.

به همین ترتیب، درون جامعه سازمان‌های غیردولتی، طیفی از تخصص و اطلاعات وجود دارد که می‌تواند منبع ارزشمندی برای تماس با کودکان، والدین، سرپرستان و مربیان آن‌ها و ارائه خدمات به آن‌ها در جهت افزایش امنیت آنلاین و دفاع از منافع عموم باشند.

۳-۱-۵- اجرای قانون

متأسفانه با وجود تمام شگفتی‌های فناوری، توجه مجرمان و افراد

ضد اجتماع نیز به آن جلب شده است. اینترنت انتشار مطالب سوءاستفاده جنسی از کودکان و دیگر آسیب‌ها را افزایش داده است. مجرمان جنسی با استفاده از اینترنت با کودکان تماس برقرار می‌کنند و آن‌ها را فریب می‌دهند تا شکل‌های خطرناک تماس آنلاین و آفلاین را برقرار کنند. زورگویی و دیگر اشکال آزار می‌توانند آسیب زیادی به زندگی کودکان بزنند و اینترنت مسیر جدیدی برای این کار خلق کرده است.

به همین دلایل، ضروری است که مسئولان اجرای قانون به دنبال یک استراتژی کلی برای کمک به امنیت بیشتر اینترنت برای کودکان و نوجوانان باشند. برای انجام تحقیقات در مورد جرائم مربوط به اینترنت علیه کودکان و نوجوانان، مسئولان اجرای قانون باید به‌درستی آموزش ببینند. آن‌ها به دانش و دسترسی کافی به امکانات جرم‌شناختی نیاز دارند تا بتوانند داده‌ها را در کمترین زمان ممکن از اینترنت و کامپیوترها جمع‌آوری و تفسیر کنند.

علاوه بر این ، بسیار مهم است که بخش اجرای قانون سازوکارهای روشنی را ایجاد کند تا از طریق آن کودکان و جوانان یا افراد دیگر بتوانند هرگونه حوادث یا نگرانی‌هایی را که ممکن است در مورد امنیت آنلاین کودک یا یک جوان داشته باشند، گزارش دهند. به‌عنوان مثال، بسیاری از کشورها برای تسهیل گزارش محتوای سوءاستفاده جنسی از کودکان، خطوط تلفنی مستقر کرده‌اند و سازوکارهای مشابهی هم برای گزارش‌دهی دیگر انواع مشکلات مانند زورگویی دارند. سیاست‌گذاران باید با انجمن بین‌المللی خطوط تلفن اینترنتی[1] همکاری و آن‌ها را در ارزیابی و پردازش گزارش‌های مطالب

1. INHOPE

سوءاستفاده جنسی از کودکان حمایت کنند و در مکان‌هایی که خطوط تلفنی وجود ندارد از انجمن بین‌المللی خطوط تلفن اینترنتی کمک بگیرند. سیاست‌گذاران باید اطمینان حاصل کنند که کانال‌های ارتباطی بازبین اجرای قانون و سایر ذینفعان وجود دارد. نهادهای اجرای قانون منبع اصلی توقیف محتوای سوءاستفاده جنسی درون مرزهای ملی هستند. برای بررسی اینکه آیا قربانیان محلی قابل شناسایی هستند یا خیر، باید فرایندی برای بررسی این مطالب در نظر گرفته شود. در صورت عدم امکان ، مطالب باید به اینترپل منتقل شوند تا در بانک اطلاعاتی بین‌المللی سوءاستفاده جنسی از کودکان[1] قرار گیرند. از آنجا که این یک تهدید جهانی است، سیاست‌گذاران باید از همکاری بین‌المللی بین نهادهای اجرای قانون در سراسر جهان اطمینان حاصل کنند. این امر باعث کاهش زمان انجام فرایندهای رسمی و پاسخگویی سریع‌تر از سوی مأموران می‌شود.

۳-۱-۶- خدمات اجتماعی

زمانی که کودکان یا جوانان در فضای آنلاین مورد سوءاستفاده یا آزار قرار گرفته‌اند، مثلاً تصویری نامناسب یا غیرقانونی از آن‌ها منتشر شده است، به حمایت یا مشاوره طولانی و تخصصی نیاز خواهند داشت. ممکن است اقدامات اصلاحی و خدماتی برای مجرم نیز نیاز باشد، به‌ویژه برای مجرمان جوان که خود قربانی سوءاستفاده آنلاین یا آفلاین بوده‌اند. افراد حرفه‌ای که در خدمات اجتماعی کار می‌کنند باید به‌درستی آموزش ببینند تا بتوانند این نوع از حمایت را ارائه دهند. این حمایت باید از طریق کانال‌های آنلاین و آفلاین ارائه شود.

1. ICSE

۳-۱-۷- خدمات مراقبت و سلامتی

خدمات مراقبتی مورد نیاز برای هرگونه خشونت در مقابل کودکان باید تحت پوشش بیمه ملی باشد. نهادهای سلامت باید گزارش سوءاستفاده را اجباری کنند. افراد شاغل در عرصه سلامت باید به‌طور مناسب مجهز و آگاه باشند تا بتوانند کودکان را در این زمینه حمایت کنند. خدمات سلامت باید گسترش یابند تا کودکان را در زمینه رفاه و سلامت روانی حمایت کنند.

۳-۱-۸- وزارت‌خانه‌ها

سیاست محافظت از کودکان در فضای آنلاین در حوزه وظایف چند وزارت خانه مختلف قرار می‌گیرد و باید تمامی آن‌ها را در یک استراتژی و برنامه عملی موفق ملی تلفیق کرد. این وزارتخانه‌ها شامل وزارت کشور، بهداشت، آموزش، دادگستری، اطلاعات و دیجیتال، و قانون‌گذاران می‌شوند. قانون‌گذاران بهترین موقعیت را برای کنترل و بررسی در همکاری با نهادهای دولتی دارند. این نهادها می‌توانند شامل نهادهای مقرراتی رسانه و محافظت اطلاعات باشند.

۳-۱-۹- اپراتورهای شبکه وای فای، موبایل و پهنای باند

اپراتورها می‌توانند درون شبکه خود محتوای غیرقانونی را کشف، مسدود و گزارش کنند و به خانواده‌ها ابزارهایی بدهند تا والدین نحوه دسترسی فرزندان خود به اینترنت را مدیریت کنند. این اپراتورها باید اطمینان حاصل کنند که آزادی‌های مدنی و حریم خصوصی هردو به یک اندازه اعمال می‌شوند.

۳-۱-۱۰- حقوق کودکان

نهادهای حقوق بشری مستقل برای کودکان می‌توانند نقش حیاتی در محافظت کودکان در فضای آنلاین ایفا کنند. هرچند وظایف آن‌ها مختلف است، این نهادها می‌توانند:

- بر تأثیر قانون، سیاست و عملکرد در حمایت از حقوق کودکان نظارت کنند؛
- اجرای استانداردهای حقوق بشری بین‌المللی را در سطح ملی ارتقا دهند؛
- نقض حقوق کودکان را بازرسی کنند؛
- در دادگاه‌های حقوق کودک، خدمات تخصصی ارائه دهند؛
- اطمینان حاصل کنند که صدای کودکان در موارد مربوط به حقوق انسانی شنیده می‌شود، از جمله در تدوین قوانین و سیاست‌های مرتبط؛
- درک و آگاهی از حقوق کودکان را افزایش دهند؛ و
- اقدامات آموزشی حقوق بشری انجام دهند.

طبق ماده ۱۲ کنوانسیون حقوق کودک سازمان ملل، مشاوره مستقیم با کودکان جزو حقوق آن‌ها محسوب می‌شود. بنابراین باید این نوع مشاوره را در دستور کار قرار داد. کارکردهای مشاوره‌ای، بازرسی، آگاهی‌بخشی و آموزشی نهادهای حقوق بشری مستقل همگی برای پیشگیری و واکنش به آسیب‌های آنلاین کودکان مناسب هستند. این نهادها باید در مرکز تدوین استراتژی‌های جامع و مبتنی بر حقوق باشند تا چارچوب‌های قانونی، مقرراتی و سیاسی محافظت آنلاین کودکان را تقویت کنند، از جمله مشاوره مستقیم با کودکان

به‌عنوان بخشی از حقوق آن‌ها تحت ماده ۱۲ کنوانسیون حقوق کودک سازمان ملل.

اخیراً در برخی مناطق، آژانس‌های دولتی وظیفه یافته‌اند تا از حقوق آنلاین کودکان محافظت کنند و آن‌ها را در برابر آسیب یا خشونت حمایت کنند. این آژانس‌های دولتی باید محافظت از حقوق کودکان در سطح ملی را نیز تقویت کنند.

۱.۱ واکنش‌های موجود به محافظت آنلاین از کودکان

اقدامات زیادی در سطح ملی و بین‌المللی انجام شده‌اند که با خطرات فناوری اطلاعات و ارتباطات در زندگی کودکان مقابله می‌کنند.

۳-۱-۱۱- مدل‌های ملی

در سطح ملی، قوانین زیادی به جنبه‌های مهم چارچوب جامع محافظت آنلاین کودکان می‌پردازند. برخی از این قوانین شامل موارد زیر می‌شود:

- دستورالعمل خدمات رسانه‌ای و صمعی بصری (بازنگری شده ۲۰۱۸، اتحادیه اروپا)
- مقررات عمومی محافظت از اطلاعات (۲۰۱۸، اتحادیه اروپا)

اقدامات نهادی و مقرراتی دولت‌های عضو برای مقابله با تهدیدات امنیتی و رفاهی کودکان در فضای آنلاین بسیار نوآورانه بوده‌اند. برای مقابله با مطالب سوءاستفاده جنسی از کودکان، زورگویی و دیگر آسیب‌های آنلاین راه‌های زیادی در دسترس است و در سال‌های اخیر رویکردهای جدیدی در این زمینه اتخاذ شده است:

۳-۱-۱۲- قانون طراحی متناسب با سن (۲۰۱۹، انگلستان)

در اوایل سال ۲۰۱۹، اداره سرپرستان اطلاعات، در جهت افزایش محافظت آنلاین از کودکان، پیشنهادهایی را برای قانون طراحی متناسب با سن ارائه کرد. این قانون پیشنهادی منافع کودکان را که کنوانسیون حقوق کودک سازمان ملل اعلام کرده است در نظر می‌گیرد و وظایفی را برای صنعت برمی‌شمرد. این وظایف شامل اقدامات قدرتمند در جهت اعتبارسنجی سن، خاموش بودن خدمات مکانی برای کودکان به‌صورت پیش‌فرض، جمع‌آوری کمترین میزان داده در مورد کودکان از سوی صنعت، طراحی امن محصولات و توضیحات متناسب با سن و قابل دسترسی برای کودکان است.

۳-۱-۱۳- قانون ارتباطات دیجیتال آسیب‌رسان (بازنگری شده ۲۰۱۷، نیوزیلند)

قانون مربوط به سال ۲۰۱۵ سوءاستفاده آنلاین را جرم قلمداد کرده و بر طیف وسیعی از آسیب‌ها از زورگویی آنلاین تا پورن انتقامی را در بر می‌گرفت. به‌منظور شناسایی، پیشگیری و کاهش ارتباطات مضر دیجیتال، برقراری ارتباط دیجیتال با هدف آسیب عاطفی به فردی دیگر جرم شناخته شد و ۱۰ اصل ارتباطی دیگر نیز تدوین شد. این قانون به کاربران امکان می‌دهد تا اگر این اصول نقض شوند، به یک سازمان مستقل شکایت کنند و در صورت عدم حل مشکل، فرد ایجاد کننده یا میزبان ارتباط مورد نظر را به دادگاه ببرند.

۳-۱-۱۴- هیئت امنیت الکترونیک (۲۰۱۵، استرالیا)

هیئت امنیت الکترونیک اولین آژانس دولتی دنیا است که به‌طور تخصصی به امنیت آنلاین می‌پردازد. این هیئت که در سال ۲۰۱۵ تأسیس شد، رهبری، آموزش، هماهنگی و مشاوره در مورد مسائل مربوط به امنیت آنلاین را بر عهده دارد تا تمامی مردم استرالیا تجربیات آنلاین امن، مثبت و تواناساز داشته باشند. امنیت الکترونیک طرح‌های بازرسی‌ای انجام می‌دهد که بر طیفی از آسیب‌ها تمرکز دارند، از زورگویی آنلاین کودکان گرفته تا سوءاستفاده از تصاویر و محتوای ممنوعه. این هیئت قدرت کافی در اختیار دارد تا برای رسیدگی به شکایات و گزارش‌ها مربوط به این آسیب‌ها بازرسی و اقدام کند. مثلاً در برخی موارد می‌تواند به افراد هشدار داده و خدمات آنلاین را وادار به حذف مطالب خود کنند. امنیت الکترونیک در کنار قدرت بازرسی، از اقدامات و مداخلات اجتماعی، فرهنگی و فناوری نیز برخوردار است. تلاش‌های پیشگیرانه، محافظتی و فعالانه این هیئت رویکردی جامع برای امنیت آنلاین ارائه می‌دهند.

۳-۱-۱۵- مدل‌های بین‌المللی

ذینفع‌های متفاوتی استانداردها و توصیه‌های بین‌المللی را منتشر کرده‌اند. این دستورالعمل‌ها بر اساس تلاش‌های زیر بنا شده‌اند:

- دستورالعمل‌های اجرای پروتکل اختیاری کنوانسیون حقوق کودک در مورد فروش کودکان، روسپیگری کودکان و پورنوگرافی کودکان.
- دستورالعمل‌های شورای اروپا برای محافظت و برآورده کردن حقوق کودک در دنیای دیجیتال.

این دستورالعمل‌ها برای تمامی دولت‌های عضو شورای اروپا ارسال شده‌اند تا به آن‌ها و ذینفعان دیگر کمک شود رویکردی جامع و استراتژیک در محافظت از حقوق کودکان در فضای آنلاین اتخاذ کنند. در میان موضوعات بسیاری که مطرح شده‌اند، محافظت از داده‌های فردی، ارائه محتوای مناسب کودک و متناسب با رشد توانایی‌های آن‌ها، خطوط تلفنی امدادی، آسیب‌پذیری و بهبودی، و نقش و مسئولیت شرکت‌های تجاری وجود دارند. بعلاوه، دستورالعمل‌ها از دولت‌ها می‌خواهد تا در فرایندهای تصمیم‌گیری کودکان را دخیل کنند تا مطمئن شوند که سیاست‌های ملی به‌طور مناسب تغییرات فضای دیجیتال را در نظر می‌گیرند. دستورالعمل‌ها در حال حاضر به ۱۹ زبان در دسترس هستند. در کنار آن‌ها، یک نسخه کودک‌پسند و راهنمای سیاست‌گذاران نیز قرار دارد که راهنمایی ملموس در جهت اجرای این دستورالعمل‌ها ارائه می‌دهد.

۳-۱-۱۶- کنوانسیون شورای اروپا-لانزاروتی

کنوانسیون شورای اروپا در مورد حفاظت از کودکان در مقابل بهره‌کشی و سوءاستفاده جنسی (کنوانسیون لانزاروتی) دولت‌ها را ملزم می‌کند واکنشی جامع به خشونت جنسی علیه کودکان از طریق پیشگیری، محافظت، تعقیب و ارتقای مشارکت ملی و بین‌المللی نشان دهند. کمیته احزاب کنوانسیون محافظت کودکان در مقابل سوءاستفاده و بهره‌کشی جنسی (کمیته لانزاروتی) عملکرد کنوانسیون در رابطه با محیط دیجیتال را از طریق چند سند شفاف‌سازی می‌کند. این سندها شامل: نظر در مورد ویدیوها و یا تصاویر جنسی کودکان

تولید و منتشر شده به دست کودکان (۶ ژوئن ۲۰۱۹)؛ نظر تفسیری در مورد کاربرد کنوانسیون لانزاروتی برای جرائم جنسی علیه کودکان تسهیل شده با فناوری‌های ارتباطی و اطلاعاتی (۱۲ مه ۲۰۱۷)؛ اعلامیه آدرس‌های وب تبلیغ‌کننده محتوا و تصاویر سوءاستفاده جنسی کودکان یا هرگونه جرم در راستای تعاریف کنوانسیون لانزاروتی (۱۶ ژوئن ۲۰۱۶)؛ و نظر در مورد ماده ۲۳ کنوانسیون لانزاروتی (ارتباط با کودکان با اهداف جنسی از طریق فناوری‌های ارتباطی و اطلاعاتی). کمیته لانزاروتی بر اجرای کنوانسیون نظارت دارد. دومین دور نظارت موضوعی کمیته بر محافظت کودکان در مقابل سوءاستفاده و بهره‌کشی جنسی از طریق فناوری‌های ارتباطی و اطلاعاتی متمرکز بود. گزارشی در مورد این دور نظارت در سال ۲۰۲۰ منتشر می‌شود. از سال ۲۰۱۹، ۴۶ حزب دولتی در کنوانسیون حضور دارند، از جمله تونس، اولین دولت غیر عضو کنوانسیون.

۳-۱-۱۷- دستورالعمل‌های دیگر شورای اروپا

ابزارها و استانداردهای دیگر شورای اروپا به رسیدن به یک چارچوب جامع برای تمامی ذینفعان کمک می‌کنند. کنوانسیون جرائم سایبری شورای اروپا شامل الزام اعضا به جرم‌انگاری بزه‌های مختلف مرتبط با مطالب سوءاستفاده جنسی کودکان است. در حال حاضر ۶۴ دولت آن را به رسمیت می‌شناسند. هدف شورای اروپا این است که کودکان و اطرافیان آن‌ها توانمند شوند تا با امنیت از فضای دیجیتال استفاده کنند. این کار به‌وسیله ابزارهای آموزشی انجام می‌شود مانند راهنمای سواد اینترنتی[1] کاملاً بازبینی شده (۲۰۱۷)،

1. Internet Literacy Handbook

راهنمـای آمـوزش شـهروندی دیجیتـال[1] (۲۰۱۹) و راهنماهایـی بـرای والدیـن: والدگـری در عصـر دیجیتـال، راهنمـای والدیـن بـرای محافظـت آنلایـن کـودکان از سوءاسـتفاده و بهره‌کشـی جنسـی (۲۰۱۷)؛ شـهروندی دیجیتـال... و کـودک، آنچـه کـه هـر والـدی بایـد بدانـد و انجـام دهـد (۲۰۱۹). در نهایـت، شـورای اروپـا تحقیقـات مشـاوره‌ای بـا کـودکان در رابطـه بـا حقوقشـان در فضـای دیجیتـال را انجـام می‌دهـد: «ایـن دنیـای مـا اسـت: نظـرات کـودکان در مـورد چگونگـی محافظـت از حقوقشـان در دنیـای دیجیتـال (۲۰۱۷)». همچنیـن ایـن شـورا تحقیقـات مشـاوره‌ای در رابطـه بـا تجربیـات کـودکان معلـول در فضـای دیجیتـال انجـام داده اسـت: «دو کلیـک بـه جلـو یـک کلیـک بـه عقـب: گـزارش در مـورد کـودکان معلـول در فضـای دیجیتـال (۲۰۱۹)».

۳-۱-۱۸- گزارش امنیت آنلاین کودک

- امنیت آنلاین کودک: به حداقل رسـاندن ریسـک خشـونت، سوءاستفاده و بهره‌کشـی آنلاین و اعلامیه جهانی امنیت آنلاین کودک
- توصیه‌هـای بهره‌کشـی آنلایـن جنسـی کـودکان در مـورد محافظـت آنلایـن کـودکان (۲۰۱۲، بازبینـی ۲۰۱۹-۲۰۲۰). دیگـر اقدامـات ملـی و بین‌المللـی نیـز بایسـتی بـرای حمایـت از مشـارکت بین‌المللـی و تلاش‌هـای ملـی بـرای تدویـن اسـتراتژی‌های محافظـت آنلایـن کـودکان ذکـر شـوند، ماننـد:

1. Digital Citizenship Education Handbook

۳-۱-۱۹- پایگاه داده‌های بین‌المللی تصاویر بهره‌کشی جنسی کودکان

پایگاه داده‌های بین‌المللی تصاویر بهره‌کشی جنسی کودکان که تحت مدیریت اینترپل است، یک ابزار قدرتمند اطلاعاتی و بازرسی است که از طریق آن بازرسان می‌توانند داده‌ها را با همکاران خود در سرتاسر جهان به اشتراک بگذارند. این پایگاه داده‌ها که در سیستم امن ارتباطی پلیس جهانی اینترپل در دسترس است (با نام I-247)، با استفاده از نرم‌افزار پیشرفته مقایسه تصاویر، بین قربانیان، مجرمان و مکان‌ها ارتباط ایجاد می‌کند. این پایگاه داده به کاربران ثبت شده در کشورهای عضو امکان می‌دهد به‌صورت آنی به بانک اطلاعاتی دسترسی یابند، از مظنونان بازجویی کنند، داده‌های جدید آپلود کنند، مطالب را مرتب و رده‌بندی کنند، تجزیه‌وتحلیل انجام دهند و برای تحقیقات خود در مورد بهره‌کشی جنسی کودکان، با دیگر متخصصان در سرتاسر جهان ارتباط برقرار کنند.

۳-۱-۲۰- اتحاد جهانی وی‌پروتکت[1]

اتحاد جهانی وی‌پروتکت یک جنبش جهانی است که نفوذ، تخصص و منابع مورد نیاز برای مدیریت بهره‌کشی جنسی کودکان در سرتاسر جهان را گرد هم می‌آورد. این جنبش یک شراکت بین دولت‌ها، شرکت‌های جهانی فناوری و سازمان‌های مدنی است. ماهیت چند ذینفعی آن در این حوزه منحصربه‌فرد است. هدف این اتحاد شناسایی و محافظت از قربانیان بیشتر، دستگیری مجرمان بیشتر و پایان بخشیدن به بهره‌کشی آنلاین کودکان است.

1. WePROTECT

اتحادیه جهانی وی‌پروتکت شامل مؤلفه‌های متعددی به‌ویژه مدل واکنش ملی و واکنش استراتژیک جهانی است. جزییات بیشتر در پیوست ۳ در دسترس است.

۳-۱-۲۱- شاخص امنیت آنلاین کودک ۲۰۲۰

شاخص امنیت آنلاین کودک ۲۰۰۲ متعلق به موسسه دی‌کیو[1] اولین پلتفرم آنی تحلیلی جهان است که به ملت‌ها کمک می‌کند وضعیت امنیت آنلاین کودکان خود را نظارت کنند.

این شاخص بر شش ستون بنا شده است که چارچوب آن را تشکیل می‌دهند. ستون‌های یک و دو، ریسک سایبری و کاربرد دیجیتال کنترل شده، به کاربرد عاقلانه فناوری دیجیتال مرتبط می‌شوند. ستون‌های سه و چهار، قدرت دیجیتال و راهنمایی و آموزش، به توانمندسازی مرتبط می‌شوند. دو ستون آخر به زیرساخت مربوط می‌شوند که ستون‌های زیرساخت اجتماعی و اتصال هستند.

۳-۲- نمونه‌هایی از واکنش به آسیب‌های آنلاین

در پیوست ۴ نمونه‌هایی از واکنش به آسیب‌های آنلاین ذکر شده است. این نمونه‌ها واکنش‌های آموزشی، قانونی و شناسایی آسیب‌های آنلاین را شامل می‌شوند.

۳-۳- مزایای استراتژی ملی محافظت آنلاین کودکان

۳-۳-۱- هماهنگ‌سازی قوانین

برای رسیدن به امنیت سایبری جهانی، تمام کشورها باید قوانین مناسب

1. DQ Institute

را برای مقابله با سوءاستفاده از فناوری‌های ارتباطی و اطلاعاتی برای اهداف مجرمانه تدوین کنند. از آنجا که تهدیدات می‌توانند از هر جایی در دنیا باشند، چالش‌ها بین‌المللی هستند و به مشارکت، کمک تحقیقاتی و مواد قانونی اساسی و آیین‌نامه‌ای مشترک نیاز دارند. بنابراین، کشورها باید چارچوب‌های قانونی خود را با هم هماهنگ کنند تا با جرائم سایبری مقابله کنند، از کودکان در فضای آنلاین محافظت کنند و همکاری بین‌المللی را تسهیل نمایند.

تدوین قوانین ملی مناسب، وجود چارچوب قانونی مرتبط با جرائم اینترنتی، و هماهنگی بین‌المللی گام‌های کلیدی در جهت هرگونه استراتژی ملی برای محافظت آنلاین کودکان هستند. این امر نیازمند ارائه قوانین کیفری مناسب است تا کارهایی مانند کلاه‌برداری کامپیوتری، دسترسی غیرقانونی، مداخله اطلاعاتی، نقض کپی‌رایت و انتشار مطالب سوءاستفاده جنسی کودکان را جرم‌انگاری کنند و هم‌زمان مراقب باشند که کودکان بی‌دلیل مجرم شناخته نشوند. وجود مواد قانونی در قانون کیفری که به جرائم مشابه در دنیای واقعی می‌پردازند به این معنا نیست که برای جرائم اینترنتی هم مناسب هستند. بنابراین، تحلیل جامع قوانین ملی کنونی برای شناسایی هرگونه شکاف اهمیت اساسی دارد. گام بعدی شناسایی و تعریف زبان قانونی و مرجع‌هایی است که می‌توانند در تدوین قوانین هماهنگ جرائم سایبری و قوانین آیین‌نامه‌ای به کشورها کمک کنند. این ابزارهای عملی می‌توانند برای بهبود چارچوب قانونی امنیت سایبری و قوانین مرتبط به کار روند. اتحادیه بین‌المللی مخابرات با کشورهای عضو و ذینفعان مرتبط در این زمینه همکاری کرده است و به

هماهنگ‌سازی جهانی قوانین جرائم سایبری کمک می‌کند.

با توجه به‌سرعت بالای نوآوری فناوری، خودمقرراتی و هم‌مقرراتی به‌عنوان راه‌حل‌هایی برای منسوخ شدن مقررات کنونی و فرایندهای قانونی طولانی پیشنهاد شده‌اند. با این وجود، برای اثربخش بودن، قانون‌گذاران و سیاست‌گذاران باید اهداف و چالش‌های محافظت آنلاین کودکان را به روشنی تعریف کنند، فرایند ارزیابی شفافی برای بررسی اثربخشی خودمقرراتی و هم‌مقرراتی تدوین کنند، و اگر خودمقرراتی و هم‌مقرراتی نتوانستند چالش‌ها را برطرف کنند، یک فرایند رسمی قانون‌گذاری آغاز کنند تا این چالش‌ها را برطرف کنند. همچنین، اقدامات موفقیت‌آمیز خودمقرراتی می‌توانند به‌تدریج وارد قانون رسمی و فرایندهای قانون‌گذاری شوند تا به یک پشتیبان قانونی تبدیل شوند و از نقض قوانین خودمقرراتی جلوگیری کنند.

۳-۳-۲- هماهنگی

در میان بازیگران و ذینفعان مختلف امکان دارد که برخی فعالیت‌ها در جهت محافظت آنلاین کودکان انجام شده باشد. اما این اقدامات به‌صورت منفرد انجام گرفته‌اند. درک این موضوع در تدوین استراتژی ملی محافظت آنلاین کودکان اهمیت اساسی دارد. این استراتژی تمامی تلاش‌های موجود و جدید را با یکدیگر هماهنگ می‌کند.

بخش چهارم

توصیه‌هایی برای چارچوب‌ها و اجرا

بخش چهارم

توصیه‌هایی برای چارچوب‌ها و اجرا

دولت‌ها باید تمامی شکل‌های خشونت در مقابل کودکان در محیط آنلاین را در نظر بگیرند. اما اقدامات انجام شده در جهت محافظت آنلاین کودکان نباید بی‌دلیل حقوق دیگر مانند حق آزادی بیان، دسترسی به اطلاعات یا آزادی انجمن را نقض کند. به‌جای محدود کردن کنجکاوی و حس نوآوری ذاتی کودکان به دلیل ترس از مواجهه با خطرات آنلاین، باید از فکر خود کودکان استفاده کرد و هم‌زمان با کشف ظرفیت‌های دنیای دیجیتال، انعطاف‌پذیری آن‌ها را تقویت کرد.

در بسیاری از موارد، اعمال خشونت‌آمیز علیه کودکان به دست دیگر کودکان انجام می‌شود. در چنین مواردی، دولت‌ها باید تا آنجا که می‌توانند رویکردهای احیایی اتخاذ کنند تا آسیب انجام شده را ترمیم کند و هم‌زمان از مجرم‌انگاری کودکان جلوگیری کنند. دولت‌ها باید استفاده از فناوری‌های ارتباطی و اطلاعاتی مانند توسعه فناوری‌ها و منابع برای دسترسی کودکان به اطلاعات، مسدود کردن مطالب مضر و گزارش دادن موارد خشونت را در پیشگیری و مقابله با خشونت ارتقا بخشند.

برای مقابله با مشکل امنیت آنلاین کودکان، دولت‌ها باید ارتباط بین نهادهای مرتبط را تسهیل کرده و با هم مشارکت کنند تا آسیب آنلاین برای کودکان را از بین ببرند.

۴-۱- چارچوب‌های پیشنهادی

۴-۱-۱- چارچوب قانونی

دولت‌ها باید برای حمایت از تحقق کامل حقوق کودک در محیط دیجیتال، چارچوب قانونی خود را بررسی و به‌روز کنند. یک چارچوب حقوقی جامع باید به اقدامات پیشگیرانه بپردازد، انواع خشونت علیه کودکان در محیط دیجیتال ممنوع شود، راهکارهای درمانی مؤثر، بازیابی و ادغام مجدد برای رسیدگی به موارد نقض حقوق کودکان ارائه شود، سازوکارهای مشاوره ایجاد شوند، گزارش‌دهی و شکایت مخصوص کودک امکان‌پذیر شود و سازوکار پاسخگویی برای مبارزه با مصونیت از مجازات ایجاد شود.

هرجا که امکان‌پذیر باشد، قانون‌گذاری باید نسبت به فناوری خنثی باشد تا پیشرفت‌های آینده فناوری کاربردپذیری آن را از بین نبرد.

اجرای مؤثر قانون‌گذاری دولت‌ها را ملزم می‌کند اقدامات مکمل از جمله آگاهی‌بخشی و بسیج اجتماعی، تلاش‌ها و برنامه‌های آموزشی و ظرفیت‌سازی متخصصانی که با کودکان کار می‌کنند را انجام دهند.

در تدوین قانون مناسب، باید در نظر داشت که کودکان گروه همگنی نیستند. برای کودکان از گروه‌های سنی مختلف و همچنین کودکانی که نیازهای خاصی دارند یا در معرض خطر آسیب‌دیدگی در محیط دیجیتال

هستند، ممکن است واکنش‌های متفاوتی مورد نیاز باشد.

دولت‌ها باید فضای قانونی و مقرراتی روشن و قابل پیش‌بینی ایجاد کنند که از مشاغل و سایر اشخاص ثالث پشتیبانی کند تا به مسئولیت‌های خود برای حفظ حقوق کودکان در طول فعالیت‌های خود، در داخل و خارج از کشور عمل کنند.

جنبه‌های زیر برای سیاست‌گذاران در بررسی دامنه هر چارچوب قانونی و ارائه موارد زیر مفید خواهد بود:

- آماده‌سازی یا سایر اشکال تحریک از راه دور، اخاذی یا اجبار کودکان به تماس جنسی یا فعالیت جنسی نامناسب؛
- اطمینان از در اختیار داشتن، تولید و توزیع مطالب سوءاستفاده جنسی کودکان، صرف نظر از قصد توزیع؛
- آزار، زورگویی، سوءاستفاده یا سخنان نفرت پراکن در فضای آنلاین؛
- مطالب مربوط به تروریسم آنلاین؛
- امنیت سایبری؛
- آنچه در فضای آفلاین غیرقانونی است در فضای آنلاین هم به همان اندازه غیرقانونی است.

۴-۱-۲- چارچوب‌های نهادی و سیاستی

دولت‌ها برای تضمین تحقق حقوق کودکان در محیط دیجیتال باید هم‌زمان مزایای استفاده کودکان از فناوری‌های ارتباطی و اطلاعاتی را به حداکثر رسانده و خطرات مرتبط با آن‌ها را به حداقل برسانند. . برای این کار باید تدابیری برای محافظت آنلاین از کودکان در برنامه‌های

ملـی پهن‌بانـد در نظـر گرفتـه و یـک اسـتراتژی جداگانـه چندجنبـه‌ای حفاظـت آنلایـن از کـودکان اتخـاذ شـود. چنیـن برنامـه‌ای بایـد کامـلاً بـا هـر چارچـوب سیاسـتی موجـود مربـوط بـه حقـوق کـودکان یـا حمایـت از کـودکان هماهنـگ باشـد. همچنیـن بایـد بـا ارائـه چارچوبـی خـاص بـرای همـه خطـرات و آسـیب‌های احتمالـی بـرای کـودکان بـا هـدف ایجـاد یـک فضـای دیجیتالـی امـن، فراگیـر و توانمنـد، سیاسـت‌های ملـی حمایـت از کـودکان را تکمیـل کنـد.

دولت‌هـا بایـد یـک چارچـوب هماهنـگ ملـی بـا وظایـف مشـخص و اختیـار کافـی بـرای هماهنگـی کلیـه فعالیت‌هـای مربـوط بـه حقـوق کـودکان و رسـانه‌های دیجیتـال و فناوری‌هـای ارتباطـی اطلاعاتـی در سـطوح بیـن بخشـی، ملـی ، منطقـه‌ای و محلـی ایجـاد کننـد. دولت‌هـا بایـد اهـداف محـدود و فرآیندهـای شـفاف بـرای ارزیابـی و نظـارت بـر پیشـرفت داشـته باشـند و بایـد اطمینـان حاصـل کننـد کـه منابـع انسـانی، فنـی و مالـی لازم بـرای عملکـرد مؤثـر ایـن چارچـوب در دسـترس اسـت.

دولت‌هـا بایـد بـرای هدایـت توسـعه، اجـرا و نظـارت بـر برنامـه ملـی دیجیتـال بـرای کـودکان، یـک پلتفـرم چندذی‌نفعـی ایجـاد کننـد. چنیـن پلتفرمـی بایـد نماینـدگان مهم‌تریـن گروه‌هـای ذینفـع را گـرد هـم آورد، از جملـه کـودکان و نوجوانـان، انجمـن والدیـن/ مراقبـان، بخش‌هـای مربوطـه در دولـت، بخش‌هـای آمـوزش، عدالـت، بهداشـت و مراقبت‌هـای اجتماعـی، نهادهـای ملـی حقـوق بشـر و نهادهـای نظارتـی مربوطـه، جامعه مدنـی، صنعـت، دانشـگاهیان و انجمن‌هـای تخصصـی مربوطـه.

دولت‌هـا مسـئول نقـض حقـوق کـودکان بـه دسـت شـرکت‌های تجـاری هسـتند. بـه ایـن دلیـل کـه دولت‌هـا اقدامـات لازم، مناسـب و معقـول بـرای

جلوگیری و اصلاح چنین نقض‌هایی انجام نمی‌دهند یا در موارد دیگر با تخلفات همکاری کرده یا آن‌ها را تحمل می‌کنند.

اصول راهنمای کسب‌وکار و حقوق بشر پیش‌بینی کرده است که شرکت‌ها باید سازوکارهای اصلاحی و رسیدگی به شکایات قانونی، قابل دسترسی، قابل پیش‌بینی، عادلانه، سازگار با حقوق، شفاف، مبتنی بر گفتگو و تعامل و منبع یادگیری مستمر را ارائه دهند. مکانیسم‌های رسیدگی به شکایات توسط شرکت‌های تجاری می‌توانند راه‌حل‌های جایگزین انعطاف‌پذیر و به‌موقع ارائه دهند. در بعضی مواقع ممکن است به نفع کودک باشد که نگرانی‌های ایجاد شده در مورد رفتار یک شرکت از طریق خود شرکت برطرف شود. در همه موارد، دادگاه یا رسیدگی قضایی به اصلاحات اجرایی و سایر روش‌ها باید در دسترس باشد. باید سازوکارهایی در نظر گرفته شود که خدمات ایمن و متناسب با سن را برای کودکان ایجاد کنند تا نگرانی‌های خود را گزارش دهند.

علیرغم وجود سازوکارهای داخلی رسیدگی به شکایات، دولت‌ها باید مکانیسم‌های نظارتی را برای بازرسی و جبران نقض حقوق کودکان، با هدف بهبود پاسخگویی فناوری‌های ارتباطی و اطلاعاتی، و همچنین افزایش مسئولیت آژانس‌های نظارتی برای تدوین استانداردهای مربوط به حقوق کودکان و فناوری را در دستور کار خود قرار دهند. این امر به‌ویژه از این جهت مهم است که سایر راه‌های درمانی که برای افراد آسیب دیده از عملکرد شرکت‌ها در نظر گرفته شده است (مانند دادرسی مدنی و سایر جبران‌های قضایی) اغلب دست‌وپاگیر و گران است.

کمیته حقوق کودک سازمان ملل متحد با ترسیم نقش نهادهای ملی حقوق بشری در دریافت، تحقیق و میانجیگری در شکایت‌های مربوط به تخلفات نهادهای صنعتی، انجام تحقیقات عمومی در مورد سوءاستفاده‌های گسترده و انجام بررسی‌های قانونی برای اطمینان از انطباق با کنوانسیون حقوق کودک، نقش بالقوه این نهادها را در این زمینه نشان داده است. این کمیته اعلام کرده است که، در صورت لزوم «دولت‌ها باید الزامات قانونی نهادهای ملی حقوق بشر را برای تطبیق با حقوق و موارد مربوط به کودکان افزایش دهند». هر مکانیسم شکایتی حتماً باید به کودک حساس باشد، از حریم خصوصی و محافظت از قربانیان اطمینان حاصل کند و فعالیت‌های نظارتی، پیگیری و راستی‌آزمایی برای کودکان قربانی را انجام دهد.

یک نمونه از مواردی که در آن یک نهاد ملی حقوق بشر یا نهاد نظارتی دیگر می‌تواند درمان مؤثری برای کودکان ارائه دهد در موارد زورگویی اینترنتی است. سازوکارهای داخلی جبران و رسیدگی به شکایات در بعضی مواقع در چنین مواردی ناکارآمد هستند زیرا، اگرچه محتوا ناراحت‌کننده و آسیب‌رسان است، اغلب قوانین ملی به آن نپرداخته و هیچ دلیل روشنی برای درخواست حذف آن به دست میزبان محتوا وجود ندارد. برای محافظت از کودکان، باید یک مسئول عمومی قدرت داشته باشد تا شکایات در مورد موارد مزاحمت اینترنتی را دریافت کرده و میزبان محتوا را ملزم به حذف آن کند. به این طریق، واکنش سریع انجام می‌شود (که در موارد زورگویی آنلاین بسیار مهم است) و همچنین اساس حقوقی شفاف برای حذف مطلب آزاردهنده فراهم می‌شود.

دولت‌ها در تلاش برای تدوین استراتژی حقوقی در مورد محیط دیجیتال، باید از اثر این قوانین بر حقوق بشر از جمله آزادی بیان آگاه باشند.

دولت‌ها باید مشاغل را ملزم به انجام مراقبت‌های لازم درباره حقوق کودکان کنند. به این طریق، کسب‌وکارها اثر منفی خود را بر حقوق کودکان در روابط تجاری و عملیات جهانی خود، شناسایی، پیشگیری و به حداقل می‌رسانند.

بعلاوه، دولت‌ها باید اقدامات مکمل را نیز انجام دهند. مثلاً اطمینان حاصل کنند که شرکت‌های صنعتی که فعالیت‌های آن‌ها بر حقوق کودکان در فضای دیجیتال اثر می‌گذارد از بالاترین استانداردها پیروی کنند و از نقض حقوق کودکان جلوگیری کنند تا واجد صلاحیت دریافت بودجه یا بستن قرارداد شوند.

۴-۲- توصیه‌هایی برای اجرا

دولت‌ها باید اطمینان حاصل کنند که قربانیان نقض حقوق کودک به درمان‌های مؤثر دسترسی دارند. این درمان‌ها شامل کمک به دریافت سریع اصلاح آسیب در زمان مناسب است. دولت‌ها همچنین باید به کودکان قربانی تخلفات مربوط به رسانه‌های دیجیتال و فناوری‌های ارتباطی و اطلاعاتی پشتیبانی و کمک کافی ارائه دهند به‌طور مثال ارائه‌ی خدمات جامع برای اطمینان از بهبودی کامل و بازگشت کودک، و جلوگیری از آسیب دوباره کودکان قربانی.

قانون باید مکانیسم‌های مشاوره، گزارش‌دهی و شکایات ایمن و به‌راحتی در دسترس کودک، مانند خطوط تلفن راهنما، را ایجاد

کنـد و بایـد بخشـی از سیسـتم ملـی حمایـت از کـودک باشـد. ایـن خدمات بایـد بـه سـرویس‌های نظارتـی متصـل باشـند تـا تعامـلات کـودک بـا نهادهـای اجتماعـی در هنـگام بـروز مشـکل تسـهیل شـود. خطـوط تلفـن راهنمـا در موضوعـات بسـیار حسـاس، ماننـد سوءاسـتفاده جنسـی، کـه ممکـن اسـت بحـث در مـورد آن بـا همسـالان، والدیـن، مراقبـان یـا معلمان دشـوار باشـد بسـیار بـاارزش هسـتند. خطـوط تلفـن راهنمـا همچنیـن در هدایـت کـودکان بـه سـمت خدماتـی ماننـد خدمـات حقوقـی، خانه‌هـای امـن، اجـرای قانـون یـا توان‌بخشـی نقشـی اساسـی دارنـد.

همچنیـن، دولت‌هـا بایـد رفتـار متخلفـان را شناسـایی و پیگیـری کننـد تـا نـرخ شناسـایی مجرمـان را افزایـش داده و خطـر متهمـان را بـرای ارتـکاب مجـدد جـرم کاهـش دهنـد. خطـوط تلفـن راهنمـا بـا ارائه مشـاوره و پشـتیبانی رایـگان و ناشـناس تلفنـی یـا چـت برای افـرادی که احساسـات یـا افـکار علاقـه جنسـی در کـودکان دارنـد، یعنـی بزهـکاران احتمالـی، باید ایجـاد شـود. کمـک بـه بزهـکاران در تغییـر رفتـار خـود خطـر جـرم مجـدد را بـه حداقـل می‌رسـاند.

سـازوکارهای کیفـری رسـیدگی بـه شـکایات نیـز بخـش مهمـی از چارچـوب بـرای اقدامـات قضایـی مؤثـر را تشـکیل می‌دهـد.

نهادهـای نظارتـی بایـد اقدامـات و مطالعـات مسـتقل انجـام دهنـد تـا ارزیابـی کننـد کـه پلتفرم‌هـا چگونـه بـا موضوعـات مربـوط بـه حمایـت از کـودک روبـرو می‌شـوند. فنـاوری نظـارت بـر پلتفرم‌هـا در دسـترس ناظـران اسـت تـا به‌طـور مسـتقل ایـن پلتفرم‌هـا را نظـارت کننـد. بخـش صنعـت بایـد حمایـت شـوند تـا گزارش‌هـای شـفاف را منتشـر کننـد.

دولت‌هـا در کنـار صنعـت و جامعه بین‌المللی باید معیارهای جهانی تدوین

کنند تا ذینفعان با استفاده از آن تمامی جنبه‌های مرتبط با امنیت آنلاین کودکان را اندازه‌گیری کنند.

۴-۲-۱- بهره‌کشی جنسی

سیاست‌گذاران معیارهای عینی در اختیار دارند تا تهدیدهای پیش روی کودکان، به‌ویژه مطالب سوءاستفاده جنسی کودکان، محتوای تولید شده توسط کاربر، آماده‌سازی و اخاذی جنسی و دیگر خطرات آنلاین را بررسی کنند. این معیارها شامل موارد زیر می‌شود:

- گام‌هایی در جهت ایجاد اختلال یا کاهش ترافیک در مطالب سوءاستفاده جنسی کودکان، به‌عنوان مثال ایجاد یک خط تلفن مستقیم برای استفاده در موارد اضطراری یا یک پورتال گزارش بنیاد دیده‌بان اینترنت، و استفاده از اقداماتی که دسترسی به محتوای آنلاین حاوی مطالب مربوط به سوءاستفاده جنسی کودکان را قطع می‌کند.
- ایجاد فرآیندهای ملی برای اطمینان از اینکه مطالب سوءاستفاده جنسی کودکان موجود در یک کشور به سمت یک منبع ملی و متمرکز هدایت می‌شود که دارای اختیارات قانونی برای الزام شرکت‌ها به حذف محتوا است.
- راهکارهایی برای رسیدگی به تقاضای مطالب سوءاستفاده جنسی کودکان به‌ویژه در میان کسانی که برای چنین جرائمی محکوم شده‌اند. باید همگان را آگاه کرد که این یک جرم بدون قربانی نیست. کودکان برای تولید مطالب مورد سوءاستفاده قرار می‌گیرند و با مشاهده یا بارگیری عمدی مطالب سوءاستفاده جنسی کودکان،

افراد مستقیماً در سوء استفاده از کودک به تصویر کشیده شده نقش دارند و همچنین سوءاستفاده از کودکان بیشتر برای تولید تصاویر بیشتر را تشویق می‌کنند.

• باید همگان آگاه شوند که کودکان هرگز نمی‌توانند رضایت دهند که مورد آزار جنسی قرار بگیرند، چه برای تولید مطالب سوءاستفاده جنسی کودکان و چه به روش دیگر. افرادی که از مطالب سوءاستفاده جنسی کودکان استفاده می‌کنند را تشویق کنید کمک حرفه‌ای دریافت کنند، درعین‌حال، آن‌ها را آگاه کنید که مسئولیت کیفری فعالیت غیرقانونی خود را عهده‌دار خواهند بود.

• استراتژی‌های دیگر برای رسیدگی به تقاضای مطالب سوءاستفاده جنسی کودکان. به‌عنوان مثال، بعضی از کشورها لیستی از مجرمان جنسی دارند. دادگاه‌ها دستورات قضایی صادر کرده‌اند که این‌گونه مجرمان را از استفاده کامل از اینترنت یا استفاده از قسمت‌هایی از اینترنت که مورد استفاده کودکان و نوجوانان است منع می‌کند. مشکل این دستورات تاکنون اجرای قانون بوده است. بااین‌حال، در برخی از کشورها، لیست مجرمان جنسی شناخته‌شده وارد یک لیست سیاه شده است که از بازدید یا پیوستن افراد آن لیست به وب‌سایت‌های خاص جلوگیری می‌کند، به‌عنوان مثال وبسایت‌هایی که کودکان و نوجوانان از آن‌ها استفاده می‌کنند. مطمئناً، اگر مجرم با استفاده از نام دیگری یا ورود به سیستم جعلی به وب‌سایتی بپیوندد، تأثیر چنین اقداماتی تا حد زیادی کاهش می‌یابد اما با جرم‌انگاری این رفتار، بازدارندگی بیشتری ایجاد می‌شود.

• ارائه پشتیبانی مناسب طولانی‌مدت از قربانیان. زمانی که کودکان یا نوجوانان به‌صورت آنلاین قربانی شده‌اند، به‌عنوان مثال تصویر غیرقانونی از آن‌ها در اینترنت منتشر شده است، آن‌ها به‌طور طبیعی از اینکه چه کسی ممکن است آن را دیده باشد و اینکه این امر چه تأثیری بر آن‌ها خواهد داشت، بسیار نگران خواهند بود. این امر می‌تواند باعث شود کودک یا نوجوان در برابر زورگویی یا سوءاستفاده و آزار بیشتر جنسی آسیب‌پذیر باشد. در این شرایط، وجود خدمات برای پشتیبانی حرفه‌ای حمایت از کودکان و نوجوانانی که خود را در این شرایط می‌بینند، مهم خواهد بود. چنین حمایتی ممکن است به‌صورت طولانی‌مدت لازم باشد.

• ایجاد مکانیسم و گسترش آن برای ارائه ابزاری سریع و قابل درک برای گزارش کردن محتوای غیرقانونی یا رفتار غیرقانونی یا نگران‌کننده آنلاین. به‌عنوان مثال، سیستمی شبیه به همان چیزی که گروه ضربت این‌هوپ[1] ایجاد کرده است. استفاده از سیستم ۲۴ ساعته و هفت روز هفته اینترپل نیز باید تشویق شود.

• اطمینان از اینکه تعداد کافی از مقامات انتظامی در زمینه تحقیقات در اینترنت و جرائم مبتنی بر رایانه به‌طور مناسب آموزش دیده‌اند و به امکانات جرم‌شناسی مناسب دسترسی دارند تا بتوانند داده‌های دیجیتالی مربوطه را استخراج و تفسیر کنند.

• سرمایه‌گذاری در آموزش مقامات انتظامی، دادستانی و قضایی در مورد روش‌هایی که مجرمان آنلاین برای ارتکاب این جنایات استفاده می‌کنند. همچنین برای به دست آوردن و حفظ امکانات

1. INHOPE

لازم بـرای دریافـت و تفسـیر شـواهد پزشـکی قانونـی از دسـتگاه‌های دیجیتـال، سـرمایه‌گذاری لازم خواهـد بـود. عـلاوه بـر ایـن، ایجـاد همـکاری و تبـادل اطلاعـات دوجانبـه و چندجانبـه بـا مقامـات مربوطـه انتظامـی و نهادهـای تحقیقاتـی در کشـورهای دیگـر مهـم خواهـد بـود.

۴-۲-۲- آموزش

بـه کـودکان در زمینـه سـواد دیجیتـال به‌عنـوان بخشـی از یـک اسـتراتژی آمـوزش دهیـد تـا بتواننـد از فنـاوری بـدون آسـیب اسـتفاده کننـد. ایـن امـر باعـث می‌شـود کـه کـودکان مهارت‌هـای تفکـر انتقـادی را پیـدا کننـد کـه بـه آن‌هـا کمـک می‌کنـد جنبه‌هـای خـوب و بدرفتـار خـود را در فضـای دیجیتـال شناسـایی و درک کننـد. هرچنـد نشـان دادن آسـیب‌های آنلایـن بـه کـودکان بسـیار مهـم اسـت، ایـن تنهـا در صورتـی مؤثـر اسـت کـه به‌عنـوان بخشـی از یـک برنامـه سـواد دیجیتـال گسـترده‌تر باشـد کـه مناسـب سـن بـوده و بـر مهارت‌هـا و شایسـتگی‌ها متمرکـز اسـت. وارد کـردن مفاهیـم یادگیـری اجتماعـی و عاطفـی در آمـوزش امنیـت آنلایـن بسـیار مهـم اسـت زیـرا ایـن مـوارد بـه درک و مدیریـت دانش‌آمـوزان بـرای داشـتن روابـط سـالم و احترام‌آمیـز، چـه به‌صـورت آنلایـن و چـه به‌صـورت آفلایـن کمـک می‌کننـد.

کـودکان بایـد از ابـزار مناسـب برخـوردار باشـند و دانـش اسـتفاده از اینترنـت یکـی از بهتریـن راه‌هـا بـرای حفـظ امنیـت آن‌هـا اسـت. معرفـی سـواد دیجیتـال در برنامـه درسـی مـدارس یـک راه اسـت. راه دیگـر ایجـاد منابـع آموزشـی خـارج از برنامـه درسـی مدرسـه اسـت. افـرادی کـه بـا کـودکان کار می‌کننـد بایـد دانـش و مهـارت مناسـبی داشـته باشـند

تا در پاسخگویی و حل مسائل مربوط به حمایت آنلاین کودکان و همچنین ارائه مهارت‌های دیجیتالی لازم به کودکان برای استفاده‌ی بدون آسیب آن‌ها از فناوری حمایت کنند.

۴-۲-۳-صنعت

بازیگران ملی و بین‌المللی صنعت باید در جهت افزایش آگاهی از مسائل مربوط به امنیت آنلاین کودک و کمک به همه بزرگسالانی که مسئولیت رفاه کودک را دارند (از جمله والدین و مراقبان، مدارس، سازمان‌ها و جوامع در خدمت نوجوانان) تلاش کنند تا با افزایش دانش و مهارت مورد نیاز به حفظ امنیت کودکان کمک کنند. صنعت باید امنیت را در طراحی محصولات، خدمات و پلتفرم‌های خود افزایش دهد و آن را به‌عنوان یک هدف اصلی بداند.

- ابزارهای خانواده‌پسند و مناسب سن ارائه کنند تا به کاربران خود کمک کنند از خانواده خود در فضای آنلاین محافظت کنند.
- سازوکارهای گزارش‌دهی مناسبی را برای گزارش مشکلات و نگرانی‌های کاربران خود فراهم آورند. کاربران باید منتظر پاسخ به‌موقع این گزارش‌ها به‌همراه اطلاعاتی درباره اقدامات انجام شده باشند. کاربران می‌توانند در صورت لزوم پشتیبانی بیشتری دریافت کنند.
- به‌صورت مستمر گزارش سوءاستفاده علیه کودکان را برای کشف و رسیدگی به هر نوع سوءاستفاده (طبقه‌بندی‌شده به‌عنوان فعالیت مجرمانه) علیه کودکان ارائه دهند. این روش نشان داده است که اگر همه ذینفعان در شناسایی، مسدود و گزارش کردن

مشارکت داشته باشند، می‌توانیم به داشتن یک اینترنت تمیزتر و امن‌تر برای همه فکر کنیم. صنعت باید تمامی ابزارهای مرتبط را در نظر بگیرد تا پلفترم‌های صنعتی مانند خدمات بنیاد دیده‌بان اینترنت مورد سوءاستفاده قرار نگیرند.

همه بازیگران مرتبط در اکوسیستم باید از خطرات و آسیب‌های آنلاین آگاه باشند تا بتوانند از قرار گرفتن کودکان در معرض خطرات غیرضروری جلوگیری کنند.

معیارهای مشترکی برای ایمنی آنلاین کودکان با هدف سنجش تمام جنبه‌های مربوط به موضوع تهیه کنید. استانداردها و معیارهای مشترک تنها راه برای نظارت بر پیشرفت کشورها و تعیین موفقیت پروژه‌ها و فعالیت‌های اجرا شده برای از بین بردن هرگونه خشونت علیه کودکان و تأیید قدرت اکوسیستم امنیت آنلاین کودکان است.

بخش پنجم

چک لیست ملی

بخش پنجم
چک‌لیست ملی

۵-۱- چک‌لیست ملی

برای تدوین یک استراتژی ملی برای امنیت آنلاین کودکان، سیاست‌گذاران باید طیفی از استراتژی‌ها را در نظر بگیرند. جدول ۱ حوزه‌های اصلی مدنظر را نشان می‌دهد.

		حوزه‌های اصلی مدنظر	جزییات بیشتر
چارچوب قانونی	۱	چارچوب قانونی موجود را بررسی کنید تا مشخص شود که تمامی قدرت‌های قانونی برای اجرای قانونی وجود دارند و دیگر آژانس‌های مرتبط می‌توانند کودکان را در فضای آنلاین و در تمامی پلتفرم‌های اینترنتی محافظت کنند.	به‌طورکلی به قوانینی نیاز است که مشخص کند هرگونه جرمی که در دنیای واقعی علیه کودکان انجام می‌شود می‌تواند در اینترنت یا هر شبکه الکترونیک دیگر نیز رخ دهد. همچنین ممکن است لازم باشد که قوانین جدید تدوین شود یا قوانین موجود اصلاح شوند تا برخی رفتارها که تنها در اینترنت رخ می‌دهند نیز غیرقانونی شوند. به‌عنوان مثال، فریب کودکان برای انجام یا تماشای

جدول ۱: حوزه‌های اصلی مدنظر

		حوزه‌های اصلی مدنظر	جزییات بیشتر
			اعمال جنسی یا آماده سازی کودکان برای ملاقات در دنیای واقعی برای یک منظور جنسی. همچنین باید چارچوبی قانونی وجود داشته باشد که سوءاستفاده از کامپیوتر برای اهداف مجرمانه، هک و دیگر کاربردهای منفی یا بدون رضایت کامپیوتر را غیرقانونی اعلام کند و مشخص کند که اینترنت مکانی است که می‌تواند در آن جرم صورت گیرد.
	۲	تعیین کنید که هر عملی علیه یک کودک در دنیای واقعی که جرم محسوب می‌شود در دنیای آنلاین نیز جرم است و قوانین مربوط به حریم خصوصی و محافظت داده‌ها برای کودکان نیز کاربرد دارند.	
چارچوب مقرراتی	۳	سیا ست مقرراتی را تدوین کنید. این سیاست می‌توا ند در چارچوب خودمقرراتی یا هم‌مقرراتی یا یک چارچوب کامل مقرراتی باشد. مدل خود یا هم‌مقرراتی می‌تواند شامل تدوین و انتشار قواعد رفتار خوب یا انتظارات اساسی امنیت آنلاین باشد، هم از لحاظ کمک به هماهنگی و تنظیم و نگهداری حضور تمامی ذینفعان و هم از لحاظ تسریع واکنش های مناسب به تغییرات فناوری. مدل مقرراتی می‌توا ند انتظارات و وظایف ذینفعان مختلف را شرح دهد و در یک موقعیت قانونی بگنجد. مجازات برای نقض سیاست‌ها نیز می‌تواند تعریف شود.	برخی کشورها مدل‌های خودمقرراتی یا هم‌مقرراتی تنظیم کرده‌ا ند که ا قدا مات مناسب را برای محافظت آنلاین کودکان شرح می‌دهند. به‌عنوان مثال، در اتحادیه اروپا که قوانین برای شبکه‌های اجتماعی و شبکه‌های موبایل در رابطه با ارائه محتوا و خدمات به کودکان از طریق این شبکه‌ها منتشر شده‌اند. خود و هم‌مقرراتی می‌توانند برای افزایش سرعت واکنش به تغییرات فناوری مؤثرتر باشند. به‌تازگی چند کشور چارچوب‌های مقرراتی را تدوین یا اجرا کرده‌اند. در این نمونه‌ها، چارچوب مقرراتی از مدل‌های خود یا هم‌مقرراتی حاصل شده و الزا مات و انتظارات از ذینفعان به‌ویژه بخش صنعت را بیان می‌کند تا از کاربران خود بهتر محافظت کنند.

		حوزه‌های اصلی مدنظر	جزییات بیشتر
گزارش محتوای غیرقانونی	۴	اطمینان از اینکه سازوکاری مناسب به‌طور گسترده استفاده می‌شود تا ابزاری ساده برای گزارش دادن محتوای غیر قانونی در اینترنت ارائه دهد. به‌عنوان مثال، یک خط تلفن ملی که بتواند سریعاً پاسخگو باشد و مطالب غیرقانونی را حذف و غیرقابل‌دسترس سازد. صنعت نیز باید سازوکارهایی برای شناسایی، مسدود کردن و حذف مطالب غیرقانونی داشته باشد و تمامی سرویس‌های مرتبط با سازمان‌های صنعتی را پوشش دهد.	سازوکارهایی برای گزارش سوءاستفاده سرویس‌های آنلاین یا گزارش رفتارهای نامناسب و غیرقانونی آنلاین. به‌عنوان مثال یک خط تلفن ملی باید در سطح وسیع در اینترنت و دیگر رسانه‌ها تبلیغ و اطلاع‌رسانی شود. اگر خط تلفن ملی در دسترس نیست، بنیاد دیده‌بان اینترنت پرتال‌های گزارش‌دهی را پیشنهاد می‌دهد. در تمامی وب‌سایت‌هایی که کاربران محتوا منتشر می‌کنند، باید لینک‌های گزارش محتوای نامناسب وجود داشته باشد. همچنین افرادی که به هر روشی احساس خطر می‌کنند یا شاهد فعالیت‌های نگران‌کننده در اینترنت بوده‌اند باید بتوانند در اسرع وقت به نهادهای اجرای قانون گزارش دهند. این نهادها هم باید آموزش ببینند تا به‌درستی پاسخ دهند. Virtual Global Taskforce یک نهاد اجرای قانون است که سازوکاری ۲۴ ساعته و ۷ روز هفته دارد تا گزارش‌های مربوط به رفتارها و محتوای غیرقانونی را از آمریکا، کانادا، استرالیا و ایتالیا دریافت کند. کشورهای دیگر هم به‌زودی به آن افزوده می‌شوند.به www.virtualglobaltaskforce.com و INHOPE مراجعه کنید.
گزارش نگرانی‌های کاربران	۵	صنعت باید فرصت گزارش نگرانی‌ها و مشکلات را به کاربران بدهد و به‌درستی به آن‌ها پاسخ دهد.	تأمین‌کنندگان باید ملزم شوند سازوکاری در اختیار کاربران خود قرار دهند که به‌راحتی مسائل و نگرانی‌های خود را در سرویس های آن ها گزارش کنند. این سازوکارها باید کودک‌پسند و به‌راحتی در دسترس باشد.
بازیگران و ذینفعان	۶	تمامی ذینفعانی که در محافظت آنلاین کودکان منافعی دارند دخیل کنید، به‌ویژه: • آژانس‌های دولتی	در چند کشور، تمامی ذینفعان و بازیگران مرتبط در کنار هم جمع شده‌اند تا اقدامی ملی در جهت افزایش امنیت آنلاین

		حوزه‌های اصلی مدنظر	جزییات بیشتر
		• نهادهای اجرای قانون • سازمان های خدمات اجتماعی • ارائه‌دهندگان سرویس‌های اینترنت (ISP) و دیگر ارائه‌دهندگان سرویس‌های الکترونیک (ESP) • اپراتور های شبکه های موبایل • اپراتورهای وای فای • دیگر شرکت‌های فناوری پیشرفته مرتبط • سازمان‌های معلمان • سازمان‌های والدین • کودکان و جوانان • سازمان‌های محافظت از کودکان و دیگر سازمان های غیردولتی مرتبط • جامعه دانشگاهی و تحقیقاتی • صاحبان کافی‌نت‌ها و دیگر ارائه‌دهندگان خدمات عمومی مانند کتابخانه‌ها، مراکز مخابراتی و مراکز بازی‌های آنلاین	کودکان انجام شود و آگاهی در مورد این مسئله و نحوه مواجهه با آن افزایش یابد. در این استراتژی باید درک کرد که بسیاری از افراد در سطح جهان و به‌طور پیوسته از طریق وسایل مختلف به اینترنت متصل می‌شوند. اپراتورهای پهن‌باند، موبایل و وای‌فای نیز باید دخیل شوند. بعلاوه، در بسیاری از کشورها شبکه‌های کتابخانه‌های عمومی، مراکز مخابراتی و کافی‌نت‌ها نیز منابع مهمی برای ارائه دسترسی اینترنت به‌ویژه به کودکان و نوجوانان هستند.
تحقیقات	۷	در مورد بازیگران و ذینفعان ملی تحقیق کنید تا عقاید، تجربیات، نگرانی‌ها و فرصت‌های آن‌ها در رابطه با محافظت آنلاین کودکان را دریابید. مسئولیت‌ها و فعالیت‌های موجود یا برنامه‌ریزی‌شده برای محافظت آنلاین کودکان باید تعیین شود.	
آموزش سواد دیجیتال	۸	امکانات سواد دیجیتال را به‌عنوان بخشی از برنامه درسی ملی به‌گونه‌ای	مدارس و سیستم آموزشی به‌طورکلی به‌عنوان بخش اساسی آموزش و سواد

		حوزه‌های اصلی مدنظر	جزییات بیشتر
		متناسب با سن و کاربردی برای تمامی کودکان تدوین کنید.	دیجیتال استراتژی محافظت آنلاین کودکان عمل می‌کنند. تمام برنامه‌های درسی مدارس ملی باید شامل جنبه‌های محافظت آنلاین کودکان باشند و به تمامی کودکان در تمامی سنین مهارت‌های متناسب با سن را آموزش دهند تا از فناوری به‌درستی استفاده کنند. همچنین باید به خطرات و آسیب‌ها حساس باشند تا از آن‌ها دوری کنند. رفتارهای سازنده و مثبت آنلاین باید تشویق شوند. در هر برنامه افزایش آگاهی و آموزش، باید لحن مناسب گنجانده شود. پیام‌های مبتنی بر ترس نباید ارسال شود و باید بر جنبه‌های مثبت و تفریحی فناوری تأکید شود. اینترنت ابزار مناسبی برای توانمندسازی کودکان برای کشف دنیاهای جدید است. آموزش رفتارهای مثبت و مسئولانه آنلاین هدف اصلی برنامه‌های آموزشی و آگاهی بخشی آنلاین است. افرادی که با کودکان کار می‌کنند، به‌ویژه معلمان، باید به‌درستی آموزش و تجهیز شوند تا این مهارت‌ها را به‌خوبی به کودکان آموزش دهند. آن ها باید آسیب ها و تهدیدات آنلاین را بشناسند، با اطمینان نشانه‌های سوءاستفاده و آسیب را شناسایی کنند، آن‌ها را گزارش کنند و به‌درستی به آن ها واکنش نشان دهند تا از کودکان محافظت کنند.
منابع آموزشی	۹	از دانش و تجربه همه ذینفعان استفاده کنید و پیام‌ها و مطالب مربوط به امنیت آنلاین تهیه کنید که با قوانین و هنجارهای فرهنگی محلی همخوانی داشته باشند و آن‌ها را به‌خوبی در میان تمامی مخاطبان اصلی توزیع کنید. از رسانه‌های جمعی برای انتشار این پیام‌ها استفاده کنید.	در هنگام تدوین مطالب آموزشی، به خاطر داشته باشید که بسیاری از افرادی که به‌تازگی با فناوری آشنا شده‌اند نمی‌توانند به‌راحتی از آن استفاده کنند. به همین دلیل مطالب مورد نظر باید به شکل کتبی و از طریق دیگر رسانه های مورد استفاده تازه‌واردان نیز در دسترس قرار گیرند.

		حوزه‌های اصلی مدنظر	جزییات بیشتر
		بر جنبه های مثبت و توانمندساز اینترنت برای کودکان تأکید کنید و از پیام‌های مبتنی بر ترس خوددرای کنید. رفتارهای مثبت و مسئولانه آنلاین را تشویق کنید. منابعی تدوین کنید تا والدین بتوانند امنیت آنلاین کودکان خود را ارزیابی کنند و یاد بگیرند چگونه ریسک‌ها را به حداقل برسانند و ظرفیت‌ها را برای خانواده خود به حداکثر برسانند.	بسیاری از شرکت‌های اینترنتی بزرگ وب‌سایت‌هایی دارند که اطلاعات زیادی در مورد مشکلات آنلاین کودکان ارائه می‌دهند. اما بسیاری مواقع، این مطالب تنها به زبان انگلیسی و یا زبان های محدودی در دسترس هستند. بنابراین این مطالب باید در سطح محلی تولید شوند که قوانین و هنجارهای فرهنگی محلی را منعکس کنند. این امر برای هر برنامه امنیت اینترنت یا هر مطلب آموزشی اهمیت فراوانی دارد.
محافظت از کودکان	۱۰	سازوکارهای جهانی و سیستماتیک محافظت آنلاین از کودکان باید ایجاد شوند تا تمامی افرادی که با کودکان کار می‌کنند (مراقبت اجتماعی، سلامت، مدارس و غیره) موارد سوءاستفاده و آسیب آنلاین را شناسایی و گزارش کنند و به‌درستی به آن واکنش نشان دهند.	یک سیستم جهانی محافظت کودکان باید ایجاد شود و تمامی افرادی که با کودکان کار می‌کنند باید ملزم شوند که از آن استفاده کنند. آن ها باید آسیب یا سوءاستفاده از کودکان را گزارش دهند تا این موارد مورد بررسی قرار گرفته و حل شوند.
آگاهی ملی	۱۱	برنامه‌های آگاهی ملی ترتیب دهید تا مسائل مربوط به محافظت آنلاین کودکان برجسته شوند. می‌توان از برنامه‌های بین‌المللی مانند روز اینترنت امن برای ایجاد این کمپین‌ها استفاده کرد.	والدین، سرپرستان و افراد شاغل مانند معلمان نقشی اساسی در کمک به حفظ امنیت آنلاین کودکان دارند. برنامه های حمایتی باید تدوین شوند تا در مورد این مسائل آگاهی سازی شود و استراتژی‌هایی برای مقابله با آن‌ها ارائه شود. باید از رسانه‌های جمعی در انتشار پیام‌ها و کمپین‌های اطلاع‌رسانی استفاده شود. فرصت‌هایی مانند روز اینترنت امن برای تشویق و تحریک گفتگوی ملی در مورد محافظت آنلاین کودکان مفید هستند. بسیاری از کشورها کمپین‌های آگاهی ملی در روز اینترنت امن راه‌اندازی کرده‌اند. همه ذینفعان و بازیگران در این کمپین‌ها پیام‌های جهانی را در رسانه‌های جمعی و اجتماعی منتشر می‌کنند.

		حوزه‌های اصلی مدنظر	جزییات بیشتر
ابزارها، خدمات و تنظیمات	۱۲	نقش تنظیمات دستگاه‌ها، ابزارهای فنی (مانند برنامه‌های فیلتر کننده) و اپ های محافظت کودکان نیز مهم است. کاربران را تشویق کنید تا سیستم‌عامل دستگاه‌های خود را به‌روزرسانی کنند و از اپ‌ها و نرم‌افزارهای امنیتی مناسب استفاده کنند.	سرویس های مختلفی می‌توانند مطالب ناخواسته را حذف کنند یا تماس های ناخواسته را مسدود کنند. برخی از این برنامه های امنیت کودکان و فیلترینگ رایگان هستند چون بخشی از سیستم‌عامل کامپیوتر هستند یا به‌عنوان بسته اینترنتی اپراتور ارائه می‌شوند. سازندگان برخی کنسول‌های بازی نیز ابزارهای مشابهی ارائه می‌دهند اگر دستگاه به اینترنت وصل شود. این برنامه‌ها محافظت صد درصد ارائه نمی‌دهند اما سطح مناسبی از پشتیبانی ارائه می‌دهند به‌ویژه به خانواده هایی که کودک کم‌سال دارند. اکثر دستگاه ها تنظیماتی دارند که از کودکان محافظت می‌کنند و میزان استفاده سالم را تشویق می‌کنند. سازوکارهایی وجود دارند که والدین از طریق آن‌ها می‌توانند میزان استفاده کودک از دستگاه را محدود و مدیریت کنند. اپلیکیشن هایی وجود دارند که خریدها را مدیریت می‌کنند. اخیراً تنظیماتی طراحی‌شده‌اند که میزان دسترسی و استفاده کودکان را مدیریت می‌کنند. این ابزارهای فنی باید در کنار دیگر ابزارها استفاده شوند. دخالت والدین یا سرپرستان بسیار مهم است. وقتی کودکان بزرگ‌تر می‌شوند به دنبال حریم خصوصی بیشتری هستند و می‌خواهند که به‌تنهایی دنیا را کشف کنند. بعلاوه، فروشندگانی که کالاها و خدمات یا مطالب با محدودیت سنی به فروش می‌رسانند باید به‌درستی سن خریداران خود را تأیید کنند. وقتی رابطه خریدار و فروشنده نباشد، استفاده از فناوری تأیید سنی ممکن است مشکل‌ساز باشد یا در بسیاری کشورها به دلیل کمبود منابع داده‌های قابل اعتماد امکان‌پذیر نباشد.

۵-۲- نمونه سؤالات

با شناسایی بازیگران و ذینفعان ملی، پرسش‌های زیر را می‌توان در اختیار آن‌ها قرار داد و از آن‌ها دعوت کرد تا به آن‌ها پاسخ دهند. پاسخ‌های آن‌ها کمک می‌کند که گستره پوشش سیاست‌ها، نقاط قوت و حوزه‌هایی که باید در چک‌لیست ملی به آن‌ها پرداخت را شناسایی کرد.

- امنیت و حقوق آنلاین کودکان تا چه میزان در حوزه مسئولیت شما است؟
- جایگاه امنیت و حقوق آنلاین کودکان در خط‌مشی‌ها و فرایندهای شما چیست؟
- امنیت آنلاین تا چه میزان در قوانین موجود گنجانده شده است؟
- اولویت‌های شما در زمینه امنیت آنلاین چیست؟
- برای حمایت از امنیت آنلاین چه کارهایی باید انجام دهید؟
- برای بهبود امنیت آنلاین با کدام آژانس‌ها و سازمان‌ها همکاری می‌کنید؟
- آیا کودکان و والدین می‌توانند مشکلات مربوط به امنیت آنلاین را به شما گزارش دهند؟
- سه چالش کلیدی شما در دنیای آنلاین چیست؟
- سه فرصت کلیدی شما در فضای آنلاین چیست؟

همچنین می‌توان تحقیقاتی انجام داد و درک و تجربه کودکان و والدین از محافظت آنلاین کودکان را بررسی کرد.

csri.majazi.ir