

محافظت از کودکان و نوجوانان در برابر مخاطرات و آسیب‌های اجتماعی محیط دیجیتال: رهنمودهایی برای بهبود چارچوب‌های قانونی



بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

تاریخ انتشار:

۱۴۰۴/۲/۱۵

شماره مسلسل: ۲۰۶۸۷

کد موضوعی: ۲۱۰



مرکز پژوهش‌های
مجلس شورای اسلامی

عنوان گزارش:

محافظت از کودکان و نوجوانان در برابر مخاطرات و آسیب‌های اجتماعی محیط دیجیتال: رهنمودهایی برای بهبود چارچوب‌های قانونی

نوع گزارش: طرح و لایحه ☐، نظارتی ☐، راهبردی ☒، پیش‌نویس قانونی ☐

نام دفتر:

دفتر مطالعات اجتماعی (گروه آسیب‌های اجتماعی)

تهیه و تدوین:

فرشید خضری

اظهار نظر کنندگان:

مرتضی گنجی (دفتر مطالعات اجتماعی)، سکینه خانعلی پور و سید میثم عظیمی (دفتر مطالعات حقوقی)

ناظران علمی:

هادی افراسیابی، محمدرضا مالکی

ویراستار ادبی:

شیوا امین اسکندری

گرافیک و صفحه آرایی:

محمد دهقانی شهرابی

واژه‌های کلیدی:

۱. آسیب‌های اجتماعی و مخاطرات برخط

۲. کودکان و نوجوانان

۳. قانون جامع

۴. محیط دیجیتال

تاریخ شروع مطالعه:

۱۴۰۳/۰۶/۱۵



فهرست مطالب

چکیده.....	۶
خلاصه مدیریتی.....	۷
۱. مقدمه.....	۹
۲. پیشینه پژوهش.....	۱۱
۳. یافته‌ها.....	۱۴
۴. جمع‌بندی و پیشنهادها.....	۳۵
۵. پیوست.....	۳۷
منابع و مآخذ.....	۳۹

فهرست جداول

جدول ۱. تحلیل پیشینه پژوهشی.....	۱۱
جدول ۲. تحلیل پیشینه تقنینی.....	۱۲
جدول ۳. دسته‌بندی مخاطرات محیط دیجیتال برای کودکان.....	۱۵
جدول ۴. ابعاد و مولفه‌های بسته سیاستی محافظت از کودکان در برابر آسیب‌های محیط دیجیتال.....	۳۶
جدول ۱ پیوست. جدول اصلاحات و تعاریف آنها.....	۳۷

فهرست شکل‌ها

شکل ۱. ابعاد محافظت از کودکان در برابر مخاطرات و آسیب‌های محیط دیجیتال.....	۱۹
شکل ۲. هرم پیشگیری از آسیب‌های اجتماعی.....	۲۱
شکل ۳. زنجیره ارزش اینترنت.....	۲۴



محافظت از کودکان و نوجوانان در برابر مخاطرات و آسیب‌های اجتماعی محیط دیجیتال: رهنمودهایی برای بهبود چارچوب‌های قانونی

چکیده



دسترسی کودکان و نوجوانان به فناوری‌های اطلاعات و ارتباطات به صورت هم‌زمان فرصت‌ها، مخاطرات و آسیب‌های روانی-اجتماعی را برای آنان به همراه دارد. از این رو سیاست‌گذاری به منظور ارتقای فرصت‌ها و کاهش مخاطرات و آسیب‌های آن برای این قشر از جامعه به عنوان گروهی نیازمند حمایت ضروری است. بر این مبنا هدف این نوشتار احصای مخاطرات و آسیب‌های برخط برای کودکان و ارائه رهنمودهایی جهت بهبود چارچوب‌های قانونی در این حوزه است. یافته‌های این گزارش نشان می‌دهد مخاطرات و آسیب‌های این حوزه جدی هستند و کودکان در این محیط با طیف وسیعی از آنها مواجه‌اند. مخاطرات و آسیب‌های این حوزه در چارچوب محتوا-تماس-رفتار-قرارداد قابل دسته‌بندی است. همچنین گرچه در برخی از قوانین موادی به محافظت از کودکان در این زمینه اختصاص یافته است، اما همه ابعاد این موضوع مورد توجه نبوده است. یافته‌ها همچنین نشان می‌دهد که مقابله با مخاطرات و آسیب‌های محیط دیجیتال برای کودکان موضوعی چندبعدی است و باید مسئولیت بخش‌های مختلف و ابعاد این موضوع مورد توجه قرار گیرد. دولت در بخش‌های مختلف، کسب و کارها، جامعه مدنی و خانواده‌ها در این زمینه مسئولیت دارند و باید به ابعاد پیشگیری، درمان، حمایت از قربانیان، توان‌بخشی، ادغام مجدد و جبران خسارت، جرم‌انگاری و مجازات، تنظیم‌گری بین بخش‌های مختلف و همکاری‌های منطقه‌ای و بین‌المللی توجه داشته باشند.



بیان/شرح مسئله

دیجیتالی شدن جامعه پیامدهای زیادی را برای ساحت اجتماعی و اقشار مختلف از جمله کودکان به همراه داشته است. دسترسی کودکان به فناوری‌های اطلاعات و ارتباطات؛ ضمن تغییر دوران کودکی، فرصت‌ها و مخاطراتی را برای آنان ایجاد کرده است. به منظور استفاده بهتر کودکان از فرصت‌های این محیط و محافظت از آنان در برابر مخاطرات، باید سیاست‌گذاری لازم‌اندیشیده شود. لذا هدف این گزارش شناسایی مخاطرات محیط دیجیتال برای کودکان و ارائه رهنمودهای سیاستی برای بهبود چارچوب‌های قانونی است.

نقطه نظرات/یافته‌های کلیدی

مخاطرات و آسیب‌های محیط دیجیتال برای کودکان جدی هستند. مخاطرات این محیط در چارچوب محتوا-تماس-رفتار-قرارداد قابل دسته‌بندی هستند. به رغم وجود مخاطرات برخط متعدد برای کودکان، عمده نگرانی‌ها عبارت‌اند از قرار گرفتن کودکان در معرض محتوای آسیب‌رسان، سوءاستفاده جنسی و بهره‌کشی اقتصادی از آنها.

در مقیاس جهانی شاهد تغییر از عصر تنظیم‌گری ناکافی به عصر افزایش ابتکارات قانونی هستیم؛ این در حالی است که سیاست‌های دیجیتال ملی کنونی به‌ویژه قوانین، به‌اندازه کافی موضوعات کودکان از جمله محافظت از آنها در برابر مخاطرات را در نظر نمی‌گیرند. در مجموع، گرچه در لایه‌های قوانین برخی از مواد به محافظت از کودکان در برابر مخاطرات برخط پرداخته، اما هنوز فقدان قانونی جامع در این زمینه احساس می‌شود، چراکه قوانین موجود به همه ابعاد این موضوع از جمله پیشگیری، حمایت از قربانیان و جبران خسارت و تنظیم‌گری نپرداخته‌اند.

پیشنهاد راهکارهای تقنینی، نظارتی یا سیاستی

محافظت از کودکان در برابر آسیب‌های ناشی از محیط دیجیتال شامل ابعاد و مؤلفه‌های زیر است:

پیشگیری: عمده رهنمودها در این بعد عبارت‌اند از:

- احراز هویت و سن کاربران،
- فراهم کردن دسترسی متناسب با سن،
- ایجاد و تقویت ابزارهای کنترل والدین،
- راه‌اندازی کمپین‌ها، ارائه آموزش‌های همگانی، آموزش مهارت‌ها و سواد رسانه‌ای،
- شناسایی گروه‌ها و افراد در معرض مخاطره با طراحی ابزارهای مناسب و حمایت از آنها با فراهم کردن بسته‌های حمایتی و مداخلاتی مناسب،
- رتبه‌بندی و طبقه‌بندی محتوا، ارتباطات و اطلاعات برحسب سن و جنس و سایر ویژگی‌های فرهنگی و اجتماعی برای کودکان،
- حذف و مسدود کردن محتوای غیرقانونی یا نامتناسب با سن و مرحله رشد کودکان،
- وزارت آموزش و پرورش نیز می‌تواند به تناسب مقطع تحصیلی و جنسیت دانش‌آموزان آموزش‌های سواد رسانه‌ای را در محتوای کتاب‌های درسی بگنجانند و مقررات خاصی را برای استفاده از فضای دیجیتال در مدرسه تنظیم کند.
- مسئولیت کسب و کارها:** کسب و کارها به‌عنوان ارائه‌دهندگان خدمات، قدرت قابل توجهی در زمینه محافظت از کودکان از جمله با حذف محتوای نامناسب، شناسایی قربانیان و ردیابی مجرمان دارند. عمده وظایف آنها عبارت‌اند از:
- تلاش برای دسترسی عادلانه آحاد جامعه به‌ویژه خانوارها و کودکان در مناطق محروم به فناوری‌ها و خدمات دیجیتال،
- ادغام ملاحظات حقوق کودک در تمام سیاست‌ها و فرایندها،



■ اتخاذ سازوکارهای تضمین سن برای جلوگیری از دسترسی یا قرارگرفتن کودکان در معرض هرزه‌نگاری و سایر محتوای نامناسب،
■ ایجاد رویه‌های اطلاع و حذف، از جمله الزام به مسدودکردن یا حذف محتوای سوءاستفاده جنسی از کودکان،
■ شناسایی فعالانه محتوای سوءاستفاده جنسی از کودکان در محصولات یا خدمات در دسترس آنها به منظور مسدودکردن یا حذف
چنین محتوایی مشروط به حفظ حریم خصوصی کودکان،
■ گزارش محتوای برخاسته از سوءاستفاده جنسی از کودکان به مجری قانون یا سایر نهادهای تعیین شده در قانون،
■ حفظ حریم خصوصی کودکان به صورت پیش‌فرض در حداکثر میزان در طراحی پلتفرم‌ها و سایر ابزارهای کاربردی مورد استفاده
برای کودکان،

■ تهیه بسته‌های آموزش فناوری‌های ایمنی برخط به زبان کودکان،
■ جرم‌نگاری و تعیین مجازات برای اشخاص حقوقی یا کسب‌وکارهایی که علیه کودکان در محیط دیجیتال مرتکب جرم می‌شوند و
تعهدشان را برای محافظت از کودکان در برابر چنین آسیب‌هایی نقض می‌کنند و
■ منع و جرم‌نگاری پردازش داده‌های کودکان توسط کسب‌وکارها برای مقاصد اقتصادی به‌ویژه در مواردی که می‌تواند به آنها آسیب
برساند.

حمایت کیفری: عمده رهنمودها در این بعد عبارت‌اند از:

■ احصای همه جرائم برخاسته از سوءاستفاده جنسی از کودکان و ارائه تعریفی جامع از آنها،
■ می‌بایست اطمینان حاصل شود که قانون شامل جرائم خاص مرتبط با سوءاستفاده جنسی برخاسته از کودکان است. در این زمینه
می‌توان به جرائمی همچون تولید، تکثیر، عرضه، معامله، توزیع، واردات، صادرات، بارگذاری محتوا، ذخیره، تعامل، دسترسی و در
اختیار داشتن محتوای جنسی کودکان اشاره کرد،
■ باطل و بی‌اثر بودن رضایت مفروض کودک برای جرائمی همچون بهره‌کشی اقتصادی و سوءاستفاده جنسی،
■ جرم‌نگاری تلاش، همدستی و مشارکت به منظور ارتکاب جرم علیه کودکان به صورت برخط،
■ عملی که باعث می‌شود کودک، برای اهداف جنسی، شاهد سوءاستفاده جنسی یا فعالیت‌های جنسی از طریق فناوری‌های اطلاعاتی
و ارتباطی باشد، باید جرم‌نگاری شود،
■ تلاش، همدستی و مشارکت به منظور ارتکاب جرم علیه کودکان در فضای دیجیتال باید جرم‌نگاری شود،
■ معرفی صلاحیت قضایی جهانی برای مقابله با جرائم برخاسته از سوءاستفاده جنسی از کودکان،
■ تشدید مجازات در مواردی که شخص بزرگسال جرمی علیه کودکی مرتکب می‌شود،
■ رسیدگی به کودکان متهم یا محکوم به جرم در نظام قضایی جداگانه مطابق با اصول دوستدار کودک.
حمایت از قربانیان، توان‌بخشی، ادغام مجدد و جبران خسارت: وجود نظام حمایت قوی از قربانیان آسیب‌های برخاسته از عناصر
کلیدی در مقابله با پیامدهای آن است. عمده رهنمودها در این حوزه عبارت‌اند از:
■ تقویت نظام‌های موجود خدمات توان‌بخشی و ادغام مجدد به‌گونه‌ای که به نیازهای ویژه کودکان قربانی آسیب‌های برخاسته از کمک
کند،

■ ارائه آموزش‌های تخصصی به نیروی انسانی در زمینه مراقبت روانی و اجتماعی از کودکان قربانی،
■ ایجاد خطوط کمکی (خط کمکی و خط تماس ویژه) که اطلاعات و ارجاعات را به ارائه‌دهندگان خدمات مربوطه ارائه می‌دهند،
■ پیش‌بینی و ایجاد رویه‌های روشن برای حذف سریع محتوای سوءاستفاده جنسی از کودکان،
■ در نظر گرفتن سازوکارهای مختلف برای جبران آسیب/پرداخت غرامت به کودکان قربانی.
همکاری‌های منطقه‌ای و بین‌المللی: ماهیت جهانی اینترنت لزوم همکاری‌های منطقه‌ای و بین‌المللی را ضروری کرده است.

رهنمود عمده در این حوزه عبارت است از:

■ ایجاد زمینه همکاری‌های متقابل منطقه‌ای و جهانی مرتبط با محیط دیجیتال به منظور محافظت از کودکان.

تنظیم‌گری و نظارت مستقل: محافظت از کودکان در برابر آسیب‌های محیط دیجیتال موضوعی بین‌بخشی است که ذی‌نفعان مختلف درگیر آن هستند. به منظور ارتقای اثربخشی سیاست‌ها لازم است نهادی تنظیم‌گر، اقدام‌های این حوزه را همسو و بر روند اجرای موارد نام برده نظارت کند. رهنمود عمده این حوزه عبارت است از:

■ تعیین نهاد تنظیم‌گر و ناظر مستقل از میان نهادهای موجود با تأکید بر نهادهای حامی حقوق کودکان برای حفظ و ارتقای ایمنی برخط، از جمله محافظت از کودکان.

در نهایت، باید گفت گرچه همه موارد فوق به منظور محافظت از کودکان در برابر مخاطرات محیط دیجیتال مهم‌اند، اما به لحاظ ترتیب زمانی مواردی همچون قاعده‌گذاری برای نحوه استفاده از گوشی‌های هوشمند در مدارس، فراهم کردن دسترسی متناسب با سن، آموزش کودکان و والدین در بستر نظام مراقبت اجتماعی از دانش‌آموزان و رسانه‌ها و شناسایی فعالانه محتوای سوءاستفاده جنسی از کودکان و حذف آنها از اولویت برخوردار است.

۱. مقدمه

همانند پدیده‌هایی نظیر صنعتی شدن، شهرنشینی و گسترش سواد همگانی، «دیجیتالی شدن»^۱ نیز تأثیر ژرفی در تغییر جهان و زندگی ساکنان آن داشته است. استفاده از این فناوری‌ها به‌ویژه گوشی‌های هوشمند و شبکه‌های اجتماعی در زندگی روزمره، به امری اجتناب‌ناپذیر تبدیل شده است و بسیاری از افراد جامعه به دلایل و شیوه‌های مختلف از آنها استفاده می‌کنند. کودکان و نوجوانان نیز یکی از اقشار جامعه هستند که از این فناوری‌ها بهره می‌برند. شواهد در جهان نشان می‌دهد از هر سه کاربر اینترنت، یک نفر از آنها کودکان و نوجوانان زیر ۱۸ سال هستند [۱]. این میزان در ایران، یک کودک به‌ازای هر چهار نفر کاربر اینترنت است [۲]. در این میان، شیوع ویروس کووید ۱۹ و دیجیتالی شدن امر آموزش نیز هرچه بیشتر استفاده از این فناوری‌ها را تسریع بخشیده است. تأثیر این فناوری‌ها آن قدر زیاد بوده است که دوران کودکی و ماهیت تجربه این دوران را نسبت به نسل‌های قبل تغییر داده است. در ادبیات این حوزه اصطلاحاتی همچون «نسل زد»، «نسل مضطرب» یا «نسل آلفا» به این موضوعات اشاره دارد.

دسترسی به فناوری‌های اطلاعات و ارتباطات فرصت‌های بی‌سابقه‌ای را برای تحقق حقوق کودکان ایجاد کرده است. در این زمینه، می‌توان به مواردی نظیر بهبود آموزش و یادگیری، دسترسی به اطلاعات، سرگرمی و اظهارنظر درباره موضوعات اثرگذار بر زندگی آنان اشاره کرد. همچنین دسترسی به این فناوری‌ها و یادگیری نحوه کار کردن با آنها، کودکان را برای مشارکت در جامعه جدید و محیط کار آینده که تا حدود زیادی دیجیتالی شده است آماده می‌کند [۲].

به‌رغم ایجاد فرصت‌های گسترده، دسترسی به فناوری‌های اطلاعات و ارتباطات مخاطرات و آسیب‌هایی اجتماعی را نیز برای کودکان به‌همراه داشته است. باید گفت دسترسی به این فناوری‌ها، همراه با چالش‌های عمده‌ای برای سلامت روانی و اجتماعی آنان به‌صورت برخط-برون خط (آنلاین و آفلاین) بوده است. کودکان در محیط دیجیتال ممکن است در معرض محتوای نامناسب یا نامتناسب با سن و در معرض سوءاستفاده جنسی و بهره‌کشی اقتصادی قرار گیرند، با انتشار اطلاعات شخصی حساس یا نامناسب به اعتبار خود آسیب بزنند، چراکه ممکن است درک کاملی از پیامدهای بلندمدت اثر «ردپای دیجیتال»^۲ برای خود و دیگران نداشته باشند [۳].

1. Digitalization
2. Digital Footprint



همه اینها می‌تواند سایر عملکردهای آنها از جمله تحصیل را تحت تأثیر قرار دهد و به آسیب‌های دیگر منجر شود [۴]. این فناوری‌ها، ابعاد و شیوه‌های جدیدی در «وضعیت‌های مخاطره‌آمیز» برای کودکان ایجاد کرده‌اند. برای مثال، آنها قاچاق کودکان را تسهیل کرده یا مجرمان ممکن است با استفاده از آنها و گمنامی ناشی از این محیط به سوءاستفاده از کودکان بپردازند [۱]. همان‌طور که درباره «محتوای سوءاستفاده جنسی از کودکان»^۱ تأکید شده است، اینترنت نه تنها این شکل از خشونت را «آسان و ارزان»، بلکه آنها را «کم‌خطرتر، سودآورتر و بدون محدودیت مرزهای جغرافیایی» کرده است [۵]. همچنین ماهیت دائماً در حال تغییر فناوری دیجیتال نظیر فناوری‌های نوظهور (واقعیت تعمیم‌یافته^۲ و هوش مصنوعی) مخاطرات جدیدی را برای ایمنی کودکان ایجاد کرده است [۶].

یافته‌های جدید در مقیاس جهانی نشان‌دهنده افزایش گزارش‌های مختلف آسیب‌های اجتماعی و جرائم علیه کودکان در محیط دیجیتال است. نظرسنجی‌های ملی در کشورهای شرق و جنوب آفریقا و آسیای جنوب شرقی نشان می‌دهد ۲۰ درصد از کودکان در برخی کشورها در معرض بهره‌کشی و آزار جنسی قرار گرفته‌اند. یافته‌های مطالعه‌ای دیگر نشان داده است ۵۴ درصد از پاسخ‌دهندگان در دوره کودکی «آسیب‌های جنسی برخط» را تجربه کرده‌اند. منابع دیگر از این یافته حمایت می‌کنند که بهره‌کشی و سوءاستفاده جنسی از کودکان در محیط دیجیتال موضوع جهانی گسترده‌ای است که هیچ نشانه‌ای از کاهش آن دیده نمی‌شود [۷]. مصاحبه با کودکان در دوازده کشور در شرق آسیا و اقیانوسیه و شرق و جنوب آفریقا نشان می‌دهد که بین ۱ تا ۲۰ درصد از کودکان تجربه بهره‌کشی و سوءاستفاده جنسی برخط را داشته‌اند. البته، میزان واقعی آسیب‌های ناشی از محیط دیجیتال مشکلی ناشناخته است، بخشی از آن به دلیل موانع افشا از جمله ترس و حفظ آبرو گزارش و ثبت نمی‌شود [۸]. یافته‌های یک مطالعه ملی در ایران نیز نشان می‌دهد بخشی از کودکان در محیط دیجیتال رویدادهای مخاطره‌آمیز یا ناخوشایندی نظیر ارسال عکس شخصی به افراد غریبه، داشتن تجارب بد و ناراحت‌کننده، رفتار زنده یا مضر با دیگران، فریب خوردن و از دست دادن پول، استفاده زیاد از اینترنت و عملکرد تحصیلی ضعیف را تجربه کرده‌اند [۲].

وضعیت موجود در زمینه واقعیت‌های مربوط به زیست دیجیتال کودکان و نوجوانان در کشور، حاکی از آن است که به‌منظور استفاده مناسب‌تر این افشار از فرصت‌های محیط دیجیتال و محافظت از آنان در برابر خطرات و آسیب‌های این محیط، نیازمند سیاستگذاری است. گرچه برخی از کشورها قوانینی را در این زمینه تدوین و تصویب کرده‌اند، اما روی هم‌رفته سیاست‌های دیجیتال بین‌المللی و ملی کنونی اغلب به‌اندازه کافی مسائل کودکان از جمله محافظت از آنها در برابر آسیب‌ها را در نظر نمی‌گیرند [۹]. از سوی دیگر، چنانچه سیاستگذاری پای در شواهد نداشته باشد، می‌تواند کودکان را از فرصت‌های این حوزه محروم کند و حتی آنها را بیشتر در معرض مخاطره قرار دهد. در سطح ملی نیز سیاستگذاری در حوزه کودکان انسجام کافی را ندارد [۱۰] و درخصوص آسیب‌های ناشی از محیط دیجیتال برخی از اسناد و قوانین به‌صورت پراکنده به این موضوع پرداخته‌اند. در مجموع، قوانین به‌صورت جامع و منسجم و همگام با تحولات این حوزه، موضوع محافظت از کودکان و نوجوانان را در این محیط در دستور کار قرار نداده‌اند [۱۱].^۳ بر این مبنا هدف این گزارش:

شناسایی آسیب‌های محیط دیجیتال درباره کودکان و نوجوانان و ارائه بسته‌ای سیاستی برای بهبود چارچوب‌های قانونی در این زمینه است.

1. Child Sexual Abuse Material (CSAM)

2. eXtended Reality (XR)

واقعیت تعمیم‌یافته به استفاده از فناوری‌های فراگیر اشاره دارد که واقعیت را گسترش می‌دهند و دنیای فیزیکی و مجازی را ادغام می‌کنند. واقعیت تعمیم‌یافته اصطلاحی است که شامل واقعیت مجازی (VR)، واقعیت افزوده (AR) و واقعیت ترکیبی (MR) می‌شود.

۳. سند ملی صیانت از کودکان و نوجوانان در فضای مجازی (۱۴۰۰) مصوب شورای عالی فضای مجازی در این زمینه مستثنا است.



۲-۱. سوابق مطالعاتی

در سال‌های اخیر مطالعاتی درباره چالش‌ها و آسیب‌های محیط دیجیتال و راهکارهای مقابله با آن انجام شده است که بخشی از آنها معطوف به کودکان بوده است. در مرکز پژوهش‌های مجلس شورای اسلامی نیز مطالعاتی در این زمینه انجام شده است که اهم آنها در جدول زیر مرور شده است.

جدول ۱. تحلیل پیشینه پژوهشی

ردیف	عنوان گزارش	سال انتشار	شماره مسلسل	دفتر	توضیحات
۱	بررسی چالش‌های توسعه زیست‌بوم فضای مجازی در حوزه کودک و نوجوان و ارائه بسته سیاستی پیشنهادی	۱۴۰۱	۱۸۴۹۶	دفتر مطالعات آموزش و فرهنگ	مسئله اصلی گزارش فقدان خدمات و محتوای بومی زیست‌بوم فضای مجازی کودک و نوجوان است. نویسنده چالش‌های این حوزه را شناسایی و پیشنهادهای سیاستی ذیل سه گروه سیاستگذار، تنظیم‌گر / تسهیل‌گر و ارائه‌دهنده خدمت و محتوا را ارائه کرده است.
۲	پویایی‌شناسی مسائل و نابسامانی‌های فضای مجازی در ایران	۱۴۰۳	۱۹۸۸۵	دفتر مطالعات آموزش و فرهنگ	هدف این گزارش شناخت متغیرهای اصلی اثرگذار بر نابسامانی‌های فضای مجازی و روابط آنها است. با تحلیل پویایی‌شناسی نابسامانی‌ها چهار خوشه شناسایی شده است که عبارت‌اند از: ۱. فشار ناکارآمدی رسانه‌ای، ۲. فشار تولید محتوای نامناسب، ۳. فرصت بهره‌برداری از داده و ۴. فشار ناکارآمدی حکمرانی داده.
۳	هوش مصنوعی مولد: چالش‌ها و الزامات توسعه و پیاده‌سازی	۱۴۰۳	۱۹۸۷۹	دفتر مطالعات انرژی، صنعت و معدن	هدف گزارش شناسایی چالش‌های هوش مصنوعی مولد در ابعاد مختلف از جمله بعد اجتماعی و ارائه توصیه‌های سیاستی به‌منظور تنظیم‌گری آن است. برای مثال در بعد اجتماعی یکی از توصیه‌ها افزایش سواد دیجیتالی به‌منظور استفاده ایمن از این فناوری با تأکید بر افشار خاص نظیر کودکان است.

مأخذ: یافته‌های پژوهش.

۲-۲. سوابق تقنینی به‌همراه آسیب‌شناسی

در اسناد، قوانین و مقررات داخلی درخصوص محافظت از کودکان در برابر آسیب‌های برخط نیز احکامی آمده است. در جدول زیر مروری بر مهم‌ترین آنها شده است.

جدول ۲. تحلیل پیشینه تقنینی

ردیف	نام سند	مرجع تصویب	تاریخ تصویب	مواد	موضوع
۱	قانون اجازه الحاق دولت جمهوری اسلامی ایران به کنوانسیون حقوق کودک	مجلس شورای اسلامی	۱۳۷۲	(۱۹، ۱۶، ۳۵، ۳۴ و ۴۰)	احترام به حریم خصوصی کودک؛ تضمین حق دسترسی به اطلاعات از منابع گوناگون، حمایت از کودک در برابر کلیه اشکال بهره‌کشی و سوءاستفاده جنسی؛ جلوگیری از فروش و قاچاق کودکان؛ بازیابی سلامت و ادغام اجتماعی مجدد کودک قربانی و توجه به مصالح عالی به رسیدگی به امور کودک ناقض قوانین کیفری.
۲	قانون تجارت الکترونیکی	مجلس شورای اسلامی	۱۳۸۲	(۵۷-۵۰ و ۶۷)	توجه به قواعد تبلیغ همچون عدم فریب مخاطب در تبلیغ کالا و خدمات، عدم به خطر انداختن سلامت جامعه، ارائه اطلاعات دقیق، صبح و روشن مربوط به کالا و خدمات به مصرف‌کننده و توجه به موضوع تبلیغ و بازاریابی برای کودکان و نوجوانان زیر سن قانونی؛ جرم‌انگاری و تعیین مجازات برای کلاهبرداری کامپیوتری.
۳	قانون الحاق دولت جمهوری اسلامی ایران به پروتکل اختیاری کنوانسیون حقوق کودک در خصوص فروش، فحشا و هرزه‌نگاری کودکان	مجلس شورای اسلامی	۱۳۸۲	(۱۱-۱)	منع خرید و فروش، فحشا و هرزه‌نگاری کودکان؛ جرم‌انگاری و تعیین مجازات برای اقدام‌های هرزه‌نگاری؛ تعیین جرائم این حوزه به‌عنوان جرائم قابل‌استرداد؛ لزوم همکاری کشورها برای تحقیق، پیگرد جنایی و استرداد؛ ضبط و مصادره کالاهای مورد استفاده برای ارتکاب جرم، درآمدهای حاصله از ارتکاب جرم و انجام اقدام‌هایی برای تعطیلی موقت و دائم اماکنی که در آن جرم اتفاق افتاده است؛ اجرای قوانین، سیاست‌ها و برنامه پیشگیری از وقوع چنین جرائمی و تضمین کمک به قربانیان آنها به‌منظور بازگشت کامل به جامعه.
۴	قانون جرائم رایانه‌ای	مجلس شورای اسلامی	۱۳۸۸	(۱۳، ۱۴، ۱۵، ۱۶، ۱۷، ۱۸ و ۲۱)	جرم‌انگاری و تعیین مجازات برای کلاهبرداری مرتبط با رایانه، جرم‌انگاری جرائم علیه عفت و اخلاق عمومی نظیر انتشار، توزیع و معامله محتویات مستهجن، تحریک، ترغیب، تهدید یا تطمیع دیگران به‌منظور دستیابی افراد به محتویات مستهجن، ترغیب، تحریک، آموزش و یا تسهیل افراد به ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان‌گردان یا خودکشی یا انحرافات جنسی؛ جرم‌انگاری و تعیین مجازات برای هتک حیثیت و نشر اکاذیب نظیر تغییر یا تحریف و انتشار فیلم یا صوت یا تصویر دیگری و پالایش (فیلتر) محتوای ناشی از جرائم رایانه‌ای توسط ارائه‌دهندگان خدمات دسترسی.
۵	قانون آیین دادرسی کیفری	مجلس شورای اسلامی	۱۳۹۲	(۳۰۴ و ۶۶۴)	رسیدگی به همه جرائم افراد کمتر از هجده سال تمام شمسی در دادگاه اطفال و نوجوانان و صلاحیت رسیدگی به جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال توسط دادگاه‌های ایران.
۶	ضوابط میبانت از کودکان و نوجوانان در خدمات تلفن همراه باند پهن	کمیسیون تنظیم مقررات ارتباطات	۱۳۹۳	(۱ و ۲)	موظف شدن اپراتور به ارائه؛ سیم‌کارت کودک و نوجوان با قابلیت دسترسی به بسته‌های خدماتی جذاب تلفن همراه باند پهن متناسب با گروه‌های سنی کودک و نوجوان؛ بسته آموزشی استفاده صحیح از خدمات باند پهن تلفن همراه، شامل شیوه بهره‌برداری از فرصت‌ها و مقابله با تهدیدها و قابلیت اعمال برخی مدیریت‌ها برای استفاده کودک و نوجوان برای یک یا چند دسته از خدمات تلفن همراه؛ عدم مجاز بودن اپراتور به فروش هرگونه سیم‌کارت تلفن همراه به افراد کمتر از ۱۸ سال، الزام اپراتور به فراهم‌سازی تمهیدات فنی، اجرایی و مالی لازم برای اطلاع‌رسانی، آموزش و ایجاد آگاهی برای کودکان و نوجوانان و تعیین مسئولیت‌ها و تکالیف مشترکان نظیر حقوقی و مالی، اظهار یا ایجاد هویت جعلی یا غیرواقعی و نظارت فعال بر خدمات‌گیری کودک و نوجوان خود.

ردیف	نام سند	مرجع تصویب	تاریخ تصویب	مواد	موضوع
۷	قانون حمایت از اطفال و نوجوانان	مجلس شورای اسلامی	۱۳۹۹	(۲، ۵، ۶، ۹، ۱۰، ۱۱، ۱۲، ۱۴، ۱۵ و ۱۹)	تعیین بهره‌کشی از طفل و نوجوان به‌عنوان وضعیت مخاطره‌آمیز؛ شناسایی، پذیرش، حمایت، نگهداری و توانمندسازی اطفال و نوجوانان موضوع قانون؛ مجازات افرادی که: الف) مرتکب آزار یا سوءاستفاده جنسی از طفل یا نوجوان می‌شوند، ب) از طفل و نوجوان از طریق عرضه، در اختیار گرفتن، وادار یا اجیر کردن برای هرزه‌نگاری یا سوءاستفاده جنسی بهره‌کشی جنسی می‌کنند، ج) محتوا یا اثر مستهجن یا مبتذل را در دسترس طفل یا نوجوان قرار می‌دهند، د) از طفل و نوجوان برای تهیه، تولید، توزیع، تکثیر، نمایش، فروش و نگهداری آثار سمعی و بصری مستهجن یا مبتذل استفاده می‌کنند، ه) از اطفال و نوجوانان برای واردات، صادرات، تکثیر، انتشار، عرضه، معامله یا بارگذاری محتوا یا اثر مستهجن یا مبتذل که در آنها از اطفال و نوجوانان بهره‌گیری شده یا از آنها برای حمل و نگهداری این موارد استفاده می‌کنند، و) با طفل و نوجوان در فضای مجازی به‌منظور هرگونه آزار جنسی یا ارتباط جنسی نامشروع ارتباط برقرار می‌کنند. محکوم بودن معامله راجع به طفل یا نوجوان و تشدید مجازات چنانچه این رفتار با هدف فحشا و هرزه‌نگاری، بهره‌کشی اقتصادی، استفاده از طفل و نوجوان در فعالیت‌های مجرمانه باشد؛ مجازات کسانی که مرتکب قاچاق اطفال و نوجوانان می‌شوند؛ مجازات کسانی که موجب ارتکاب به خودکشی طفل یا نوجوان را فراهم می‌آورند یا آن را تسهیل می‌کنند یا در نتیجه این اقدام‌ها آسیب جسمی و روانی را برای آنان به‌همراه می‌آورند و مجازات کسانی که هویت یا اطلاعات و اسرار طفل یا نوجوان بزه‌دیده یا در وضعیت مخاطره‌آمیز را افشا می‌کنند.
۸	آیین‌نامه اجرایی ماده (۶) قانون حمایت از اطفال و نوجوانان	مجلس شورای اسلامی	۱۴۰۰	(۲، ۳ و ۴۴)	توجه به اصولی همچون حفظ حریم خصوصی طفل و نوجوان و پایش مستمر وضعیت تحصیلی و رفتاری دانش‌آموزان از طریق سامانه نماد.
۹	سند صیانت از کودکان و نوجوانان در فضای مجازی	شورای عالی فضای مجازی	۱۴۰۰	(۴-۱)	فراهم‌سازی فضای مجازی ویژه خردسالان، کودکان و نوجوانان در چارچوب فرهنگ اسلامی ایرانی برای استفاده مناسب از فضای مجازی و پیشگیری از آسیب‌های احتمالی آن از طریق ایجاد توسعه محیط‌های صیانت‌شده؛ آگاه‌سازی، هوشیارسازی و توانمندسازی، رده‌بندی همه محتوا و خدمات، تشویق، سامان‌دهی و مشارکت محوری بخش غیردولتی فعال در ارائه محتوا و خدمات سالم و مفید؛ تشدید مقابله قضایی و انتظامی کارآمد با بزه‌کاران، مجرمان و تهدیدکنندگان امنیت؛ ارتقای سواد فضای مجازی و مهارت‌افزایی؛ مراقبت روانی و اجتماعی؛ سامان‌دهی و مشارکت‌محوری بخش غیردولتی و استفاده از ظرفیت نوجوانان؛ توسعه همکاری‌های بین‌المللی و ایجاد سازوکار فنی و قانونی سلامت محتوا.

مأخذ: همان.

قوانین و مقرراتی که مرور شدند تنها بخشی از اسناد ملی حمایت از کودکان و نوجوانان در برابر مخاطرات و آسیب‌های اجتماعی محیط دیجیتال هستند. دامنه این اسناد بسیار بیشتر از این موارد است، برای مثال در این زمینه می‌توان به سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای (۱۳۷۷) و سیاست‌های کلی نظام در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات (افتا) (۱۳۸۹) و همچنین سایر مصوبات شوراهای عالی فضای مجازی و انقلاب فرهنگی اشاره کرد. لازم است در مطالعه‌ای دیگر تمامی اسناد بالادستی مرتبط با محافظت از کودکان در محیط دیجیتال احصا شده و ارزیابی دقیقی از آنها صورت گیرد.

درخصوص اسناد مرور شده می‌توان به چند موضوع عمده اشاره کرد: نخست، در زمینه مقابله با آسیب‌های ناشی از محیط دیجیتال دو دسته از قوانین وجود دارد. دسته نخست؛ نظیر قانون جرائم رایانه‌ای (۱۳۸۸)، قوانین کلی هستند که احاد جامعه را دربرمی‌گیرد و تنها معطوف به برخی از گروه‌های خاص نظیر کودکان نیست. برای مثال در بند «ب» ماده (۱۵) قانون جرائم رایانه‌ای (۱۳۸۸)، آموزش شیوه‌های ارتکاب یا استعمال مواد مخدر یا روان‌گردان و خودکشی جرم‌انگاری شده است. دسته دوم، اسنادی هستند که به‌صورت ویژه به محافظت از کودکان در برابر آسیب‌های برخط پرداخته‌اند. برای مثال برخی از مواد قانون حمایت از اطفال و نوجوانان



(۱۳۹۹) یا سند صیانت از کودکان و نوجوانان در فضای مجازی (۱۴۰۰) معطوف به محافظت از کودکان در برابر مخاطرات محیط دیجیتال است.

موضوع دیگر این است که گرچه در لایه‌های قوانین برخی از مواد به محافظت از کودکان در برابر مخاطرات و آسیب‌های اجتماعی ناشی از محیط دیجیتال پرداخته شده است و سند صیانت از کودکان و نوجوانان در فضای مجازی (۱۴۰۰) به صورت ویژه معطوف به کودکان است، اما نبود قانونی جامع در این زمینه قابل مشاهده است. برای مثال در قوانین موجود از جمله قانون حمایت از اطفال و نوجوانان (۱۳۹۹) از مخاطرات و آسیب‌های محیط دیجیتال به عنوان «وضعیت مخاطره‌آمیز» یاد نشده، همه آسیب‌ها و جرائم این حوزه احصا نشده، و به منظور پیشگیری از آنها راهبردهای مؤثر ارائه یا همه جرائم این حوزه جرم‌انگاری نشده است. همچنین اشاره‌ای به مسئولیت کسب‌وکارهای حوزه فناوری اطلاعات و ارتباطات برای پیشگیری از مخاطرات و آسیب‌ها یا کمک آنها به دولت برای شناسایی مجرمان نشده و به روش‌های تشخیص جرائم این حوزه نیز اشاره‌ای نشده است. در مجموع می‌توان گفت در قوانین موجود به همه ابعاد این موضوع شامل پیشگیری، تشخیص، شناسایی، درمان، حمایت از قربانیان، توان‌بخشی، ادغام مجدد و جبران خسارت، روش‌های تشخیص جرائم این حوزه، جرم‌انگاری و مجازات، تنظیم‌گری بین بخش‌های مختلف و غیره اشاره‌ای نشده است. این در حالی است که بسیاری از کشورها به دلیل ماهیت مخاطرات و آسیب‌های محیط دیجیتال و نیاز خاص کودکان به راهبردهای متفاوت برای بهره‌گیری از فرصت‌های این محیط و محافظت از آنان در برابر مخاطرات، قوانین ویژه‌ای را برای این قشر از جامعه تدوین و تصویب کرده‌اند [۱۲].

فقدان قانون جامع، می‌تواند انسجام نهادی و رویه‌ای به منظور مقابله با مخاطرات این حوزه را تضعیف و نظارت مؤثر از سوی نهادهای ناظر بر اقدام‌های انجام شده را محدود کند. گرچه سند صیانت از کودکان و نوجوانان در فضای مجازی (۱۴۰۰) یک سند ویژه این قشر از جامعه است، اما این سند نیز به تمامی ابعاد این موضوع به ویژه مسئولیت کسب‌وکارها و جرم‌انگاری اعمال مجرمانه علیه کودکان پرداخته است. روی هم رفته می‌توان گفت، در قوانین مربوطه نوع پرداختن به موضوع چندان متناسب با تغییر و تحولات این حوزه و حجم تهدیدها نیست، از بیان آسیب‌های این محیط به صورت موردی و ارائه راهکارهای متناسب با آنها غفلت ورزیده‌اند و در قوانین کشور الگوی قانونی منسجمی برای تحقق حقوق کودکان در محیط دیجیتال از جمله محافظت در برابر مخاطرات و آسیب‌ها در قوانین کشور دیده نمی‌شود. این مسئله ضرورت تدوین قانونی واحد و جامع را ایجاب می‌کند که به همه ابعاد موضوع بپردازد و متناسب با هدف و محیط مزبور باشد [۱۱، ۱۳، ۱۴].

۳. یافته‌های پژوهش



۳-۱. مخاطرات و آسیب‌های اجتماعی ناشی از محیط دیجیتال

با دیجیتالی شدن جامعه، بستر شکل‌گیری برخی از آسیب‌های اجتماعی سمت‌وسوی جدیدی به خود گرفته است. به لحاظ معرفت‌شناختی می‌توان سه نوع وضعیت نامطلوب را در این حوزه برشمرد: «مخاطره»، «آسیب» و «جرم». مخاطره به عنوان رابطه‌ای شناخته می‌شود که از تعامل پویا بین عاملیت کودک و عاملیت دیگران پدید می‌آید که در محیط دیجیتالی عمل می‌کند [۱۵]. مخاطرات برای کودکان با توجه به نوع ارتباط یا موقعیت آنها می‌تواند در رابطه با محتوا، تماس، رفتار و قرارداد رخ دهد. توضیح بیشتر این مخاطرات به شرح زیر است:

محتوا: کودک با محتوای بالقوه مضر درگیر می‌شود یا در معرض آن قرار می‌گیرد.

ارتباط: کودک ارتباط بالقوه مضر با بزرگسالان را تجربه می‌کند یا مورد هدف آنها قرار می‌گیرد.

رفتار: کودک شاهد رفتار بالقوه مضر همسالان است، در این رفتار مشارکت می‌کند و یا قربانی آن می‌شود.

قرارداد: کودک طرف قراردادی بالقوه مضر است یا توسط آن مورد بهره‌کشی قرار می‌گیرد [۱۵].

همچنین می‌توان به لحاظ ماهیت، بین مخاطرات چهارگانه تهاجمی، جنسی، ارزشی و متقاطع تمایز قائل شد. در این مورد آخر به مواردی نظیر نقض حریم خصوصی، ویژگی‌های فناوری پیشرفته مانند هوش مصنوعی و سلامت و رفاه کودکان اشاره کرد [۱۵]. بنابراین می‌توان مخاطرات محیط دیجیتال را براساس نوع رابطه و ماهیت آنها به شرح زیر دسته‌بندی کرد.

جدول ۳. دسته‌بندی مخاطرات محیط دیجیتال برای کودکان [۱۶، ۱۵، ۱]

نوع رابطه - ماهیت مخاطره	محتوی	ارتباط	رفتار	قرارداد
تهاجمی	اطلاعات و ارتباطات خشونت‌آمیز، حاوی خشونت، تزاوبرستانه، نفرت‌انگیز و افراطی مانند محتوای خود آسیب‌رسان، خودکشی و تبعیض	اذیت و آزار، پاییدن، ارتباط نفرت‌انگیز، نظارت ناخواسته یا بیش از حد، تضاد میان والدین و فرزندان و سوءاستفاده از داده‌های شخصی	قلدری، رفتار تنفرآمیز، خصمانه یا فعالیت همسالان نظیر رفتار توهین‌آمیز، طرد کردن و شرمسار کردن	انواع کلاهبرداری‌های اینترنتی نظیر طعمه‌گذاری، هک کردن، اخاذی، خطرات امنیتی و سرقت هویت
جنسی	هرزه‌نگاری، جنسی‌سازی فرهنگ، هنجار ستمگرانه به تصویر کشیدن بدن، قرار گرفتن در معرض محتوای جنسی یا ناخواسته مضر و تولید محتوای سوءاستفاده جنسی از کودکان.	درخواست جنسی، آزار و اذیت جنسی، اغفال جنسی، تولید و به اشتراک‌گذاری محتوای سوءاستفاده جنسی از کودکان	سوءاستفاده جنسی، ارسال پیام جنسی بدون رضایت، فشارهای جنسی نامطلوب، تولید و مصرف محتوای سوءاستفاده جنسی، تولید تصاویر ناشایست توسط کودک، به اشتراک گذاشتن تصاویر خصوصی و جنسی دیگران و ارتباطات غیراخلاقی.	بهره‌کشی جنسی، قاچاق برای مقاصد بهره‌کشی جنسی و جریانی‌سازی (پرداختن به) سوءاستفاده جنسی از کودکان.
ارزشی	اطلاعات نادرست، بازاریابی نامناسب با سن یا محتوای تولید شده توسط کاربر	اقتناع یا دستکاری ایدئولوژیک، افراط‌گرایی و عضوگیری افراد افراط‌گرا	اجتماعات کاربران بالقوه مضر نظیر اجتماعات آسیب‌رسان به خود، ضد واکسیناسیون و فشار نامطلوب همسالان	بازاریابی برخط کودکان، قماربازی، حساب‌های فیلتر ^۲ ، هدف‌گذاری خرد ^۳ و الگوهای تاریک شکل‌دهی به متقاعد کردن یا خرید ^۴ .
متقاطع	نقص حریم خصوصی (بین‌فردی، سازمانی و تجاری) مخاطرات سلامت جسمی و روانی (نظیر سبک زندگی کم‌تحرک، استفاده بیش از حد از صفحه نمایش، گوشه‌گیری و اضطراب). نابرابری‌ها و تبعیض (ادغام / طرد، بهره‌کشی از آسیب‌پذیری، سوگیری الگوریتم / تحلیل پیش‌بینی)			

همان‌گونه که جدول نشان می‌دهد چارچوب مخاطرات محتوا-تماس-رفتار-قرارداد^۵، همچنین می‌تواند راهی برای تفکر در مورد آسیب‌های واقعی فراهم کند که کودکان ممکن است به صورت برخط تجربه کنند. فراتر از موارد نام برده در جدول، مطالعات این حوزه اشکالی دیگر از مخاطرات و آسیب‌ها نظیر پریشانی روانی، افسردگی و انزوا، عدم حضور در مدرسه، اختلال در عملکرد تحصیلی، سوء مصرف مواد مخدر، روان‌گردان و الکل، پردازش داده‌های کودکان و سوءاستفاده از آنها، تبلیغات رفتاری و تجاری‌سازی دوره کودکی، آسیب‌های اخلاقی و ارزشی، شکاف نسلی، آسیب به شهرت یا اعتبار و غیره را مستند کرده‌اند [۱۶]. دسته‌ای دیگر از مطالعات از چهار

1. Oppressive Body Image Norm

2. Filter Bubbles

وضعیت یا چارچوب ایدئولوژیکی که در آن شخص تنها اخبار یا اطلاعاتی را دنبال می‌کند که حامی چیزی باشد که آن را دوست دارد یا به آن معتقد است. این می‌تواند ناشی از جستجوهای شخصی شده، سیستم‌های توصیه‌ای و تنظیم الگوریتمی باشد.

3. Micro Targeting

هدف‌گذاری خرد نوعی از تبلیغات هدفمند برخط است که داده‌های شخصی را تجزیه و تحلیل می‌کند تا علایق مخاطب یا فرد خاص را شناسایی کند و بر این اساس بر اقدام‌های آنها تأثیر گذارد. هدف‌گذاری خرد گاهی اوقات برای بازاریابی کالاها یا خدمات و بازاریابی سیاسی استفاده می‌شود.

۴. الگوهای تاریک الگوهای طراحی تعاملی هستند که از طریق فریب، حیل یا خصومت و با شیوه‌های طراحی مدنظر یا ناخواسته بر کاربران فناوری تأثیر می‌گذارند. این الگوها نشان‌دهنده برنامه‌های غیراخلاقی فناوری متقاعدکننده یا خرید است که زندگی کاربران را دشوار می‌سازد یا تأثیر منفی بر آن می‌گذارد. نمونه‌هایی از الگوهای تاریک عبارتند از: واداشتن مردم به خرید بیمه غیرضروری، قرار دادن کاربران در معرض محتوایی که باعث می‌شود آنها احساس بدی نسبت به خودشان داشته باشند تا بر رفتار آنها تأثیر گذارند و طراحی‌های محیطی که نسبت به گروه‌های خاصی خصمانه هستند [۴۸].

5. The Content-Contact-Conduct- Contract Risks Framework



زیان بنیادین محرومیت اجتماعی، محرومیت از خواب، پراکندگی توجه و اعتیاد ناشی از استفاده از محیط دیجیتال برای کودکان یاد کرده‌اند. این زیان‌ها نتیجه تغییرات عمیق در ماهیت دوران کودکی‌اند و از این جهت بنیادی هستند که بر توانایی‌های متعدد اجتماعی، هیجانی و شناختی کودکان تأثیر می‌گذارند [۴۹]. در مجموع زمینه‌های اصلی نگرانی از نظر آسیب عبارت‌اند از وب سایت‌های طرفدار محتوای آسیب‌رسان، نفرت‌انگیز و خودکشی، اذیت و آزار برخط، سوءاستفاده جنسی و بهره‌کشی اقتصادی برخط از کودکان [۱۷]. شکل دیگری از آسیب‌ها، محرومیت کودکان و نوجوانان از فناوری‌های اطلاعات و ارتباطات است. البته محرومیت لزوماً آسیب نیست بلکه می‌تواند زمینه به حاشیه رانده‌شدگی و آسیب را به‌همراه داشته باشد. باید گفت دسترسی به فناوری‌های دیجیتال به‌طور فزاینده‌ای یکی از عوامل تعیین‌کننده فرصت‌های برابر برای کودکان است و آنها را قادر می‌سازد از دسترسی به اطلاعات، دانش، فرصت‌های شغلی در آینده، مشارکت در اجتماع و درگیری فعال اجتماعی^۱ بهره‌مند شوند. زمانی که کودکان به‌ویژه در مناطق دورافتاده از دسترسی به این فناوری‌ها محروم می‌مانند، از فرصت‌های این حوزه نیز محروم می‌شوند و این به‌نوبه خود به عمیق شدن نابرابری‌ها و تقسیم‌بندهای اجتماعی-اقتصادی جدید و طرد و به حاشیه‌راندن این دسته از کودکان در آینده منجر می‌شود [۱].

حال پرسش این است که چه زمانی «مخاطره» به «آسیب» به‌ویژه از نوع اجتماعی آن تبدیل می‌شود؟ درک این موضوع به‌ویژه برای سیاستگذاران می‌تواند مهم باشد. از نظر مفهومی، مخاطره احتمال آسیب است، درحالی‌که آسیب شامل طیفی از پیامدهای منفی برای سلامت جسمی، روانی و اجتماعی است. اینکه آیا این مخاطرات به تجربیاتی تبدیل می‌شوند که به کودک آسیب می‌رسانند به عوامل مختلفی بستگی دارد که مهم‌ترین آنها طراحی، تنظیم و مدیریت محیط دیجیتال (نظیر تنظیمات حریم خصوصی)، ماهیت و/یا شدت مخاطره، شرایط فردی و اجتماعی و در دسترس بودن سازوکارهای حمایتی است [۹]. لذا وجود نظام حمایتی فراگیر و کارآمد برای مقابله با مخاطرات و آسیب‌های این حوزه عنصری کلیدی برای مقابله با پیامدهای کوتاه‌مدت و بلندمدت آنها است.

کودکانی که به‌صورت برون خط آسیب‌پذیر هستند در فضای برخط نیز بیشتر در معرض آسیب هستند. پیوند بین آسیب‌پذیری برخط و برون خط می‌تواند چالش‌های پیش روی برخی از آسیب‌پذیرترین و به حاشیه‌رفته‌ترین کودکان را عمیق‌تر کند. شواهد موجود نشان می‌دهد کودکانی که بیشترین آسیب‌پذیری را در برابر آسیب‌های برخط دارند شامل کودکان خانواده‌های فقیر، کودکان در جوامعی با درک محدودی از اشکال مختلف سوءاستفاده جنسی و بهره‌کشی از کودکان، کودکان با نیازهای آموزشی ویژه، کودکان خارج از مدرسه، کودکان دارای معلولیت و کودکان از گروه‌های به حاشیه رانده شده هستند. همچنین ناآگاهی والدین و کودکان از مخاطرات این حوزه می‌تواند آسیب‌ها را برای کودکان تشدید کند. جنسیت و سن نیز با این آسیب‌ها رابطه دارد. برای مثال پسران بیشتر در معرض اخاذی جنسی قرار دارند، درحالی‌که دختران بیشتر در معرض اغفال جنسی هستند یا اذیت و آزار جنسی دختران در محیط دیجیتال در حال تبدیل شدن به هنجار ثابت است. همچنین مطالعات نشان می‌دهد دختران نسبت به پسران بیشتر در معرض آسیب هستند. درنهایت، کودکان کم سن و سال‌تر بیشتر در معرض آسیب هستند و این نشان می‌دهد که باید بیشتر از این گروه‌ها محافظت کرد [۱، ۱۸، ۴۹].

چند رابطه بین آسیب‌های اجتماعی و استفاده از فناوری‌های دیجیتال را می‌توان شناسایی کرد. نخست، در برخی از موارد این فناوری‌ها به‌عنوان عامل یا عامل تسهیل و تسریع‌کننده آسیب‌های اجتماعی عمل می‌کنند. با استفاده از واژگان نظریه فعالیت‌های روزمره، این فناوری‌ها کودکان را به اهداف در دسترس برای مجرمان بالقوه تبدیل می‌کنند. به عبارت دقیق‌تر، این فناوری‌ها کنترل‌های سنتی (محافظ توانا) را تضعیف می‌کنند، با گسترش فعالیت، کاهش هزینه و توانا کردن مجرمان، دایره عمل آنها را گسترش می‌دهند (مجرم برانگیخته) و کودکان را به «هدف در دسترس» تبدیل می‌کنند. دوم، در موارد دیگر آسیب‌های اجتماعی می‌تواند پیامد ناخواسته استفاده از این فناوری‌ها باشد. برای مثال زمانی که کودک مورد سوءاستفاده جنسی واقع می‌شود، محتوای این سوءاستفاده در محیط دیجیتال به اشتراک گذاشته می‌شود و در معرض دید عموم قرار می‌گیرد؛ می‌تواند به احساس شرم، انزوا، افسردگی، خودآزاری و حتی خودکشی منجر شود (زنجیره به‌هم‌پیوسته آسیب‌ها). یا زمانی که کودک از این فناوری‌های بیش از اندازه استفاده می‌کند، به‌صورت ناخواسته سایر ابعاد زندگی او از جمله سلامت جسم و روان و عملکرد تحصیلی او تحت تأثیر قرار می‌گیرد. سوم،

سوءاستفاده از کودکان در محیط دیجیتال می‌تواند تأثیرات اضافی یا متفاوتی ایجاد کند. برای مثال تصاویر کودکان با فشار یک دکمه به صورت برخط در سطح جهانی به اشتراک گذاشته می‌شود و می‌تواند برای همیشه وجود داشته باشد. یا زمانی که محتوایی به اشتراک گذاشته می‌شود کنترل بر آن از دست می‌رود و این می‌تواند خطر قربانی شدن مجدد کودک را فراهم آورد [۱]. درنهایت، کودک می‌تواند از این فناوری‌ها برای آسیب رساندن به دیگران استفاده کند، نظیر زمانی که تصاویر جنسی دیگران را در اینترنت به اشتراک می‌گذارد یا علیه سایر همسالان قلدری می‌کند.

از سوی دیگر فناوری‌های اطلاعات و ارتباطات ماهیت و گستره آسیب‌های اجتماعی را نیز تغییر داده‌اند. آنها اشکال معمول آسیب‌ها را تسهیل و اشکال کاملاً جدیدی خلق کرده‌اند. برای مثال استفاده گسترده کودکان و نوجوانان از این فناوری‌ها جامعه هدف گسترده‌ای را برای مجرمان در جهان فراهم آورده است. همچنین مجرمان با استفاده از این فناوری‌ها، راحت‌تر می‌توانند قربانی‌شان را به دام اندازند. آنها با استفاده از انواع شگردها از این فناوری‌ها برای پنهان کردن هویت‌شان و سوءاستفاده از کودکان استفاده می‌کنند [۵]. ۱۹. زمانی که کودک یا هر شخص دیگر محتوای نامناسب از خود یا کودک دیگری را به اشتراک می‌گذارد، امکان کنترل بر محتوا از دست می‌رود و این وضعیت خطر قربانی شدن مجدد قربانیان را به همراه دارد [۶]. درنهایت باید گفت ماهیت دائماً در حال تحول این فناوری‌ها مقابله با مخاطرات این حوزه را به چالشی جدی تبدیل کرده است. شبکه‌های همتا به همتا، هوش مصنوعی و وب تاریک، به تسهیل تبادل محتوای سوءاستفاده جنسی از کودکان کمک کرده‌اند [۶]. افزایش استفاده از ارزهای دیجیتال، سیستم‌های پرداخت ناشناس و توسعه رمزگذاری‌های نرم‌افزاری جدید نیز به مجرمان و قاچاقچیان کمک کرده تا تراکنش‌های مربوط به سوءاستفاده و بهره‌کشی جنسی از کودکان را به صورت برخط و برون خط پنهان کنند. هنوز موارد بیشتری درباره آسیب‌های دیجیتال باقی مانده است که در زیر به صورت موردی به آنها پرداخته می‌شود:

جدی بودن میزان مخاطرات و آسیب‌های محیط دیجیتال: بدون اشاره به جزئیات، شواهد مطالعات در مقیاس جهانی نشان‌دهنده جدی بودن مخاطرات و آسیب‌های اجتماعی محیط دیجیتال و افزایش آنها طی سال‌های اخیر است. نتایج یک مطالعه نشان می‌دهد که ۵۴ درصد از پاسخ‌دهندگان در سراسر جهان آسیب جنسی برخط را در دوره کودکی تجربه کرده‌اند [۲۰].

توجه به پس‌زمینه‌های فرهنگی: گرچه برخی از آسیب‌های اجتماعی دیجیتال نظیر سوءاستفاده و بهره‌کشی جنسی برخط می‌توانند بین همه فرهنگ‌ها مشترک باشند، اما برخی از آنها در پس‌زمینه‌های فرهنگی خاص معنا می‌یابند. لذا مخاطرات و آسیب‌ها همیشه تابعی از خود رفتار نیستند، بلکه در برخی موارد بازتابی از نحوه درک جامعه از آن رفتار است. برای مثال تحت‌تأثیر فرایندهای جهانی شدن ارزش‌های برخی از کشورها، بیشتر در کشورهای دیگر اشاعه یافته است و به معضلاتی همچون تغییرات و شکاف ارزشی منجر شده است و مسائلی را در حوزه‌های مختلف اجتماعی و فرهنگی به وجود آورده است.

شکاف در شناخت و درک تجربه کودکان برخط و آسیب‌های اجتماعی ناشی از آن: شکاف قابل توجهی در درک ما درباره چرایی و نحوه اتصال کودکان، شرایطی که دسترسی آنها را تسهیل یا محدود / مسدود می‌کند، نحوه تجربه کودکان هنگام استفاده از فناوری دیجیتال، نحوه درک مخاطرات و آسیب‌های ناشی از آن و تأثیرات این فناوری‌ها وجود دارد. برای مثال، والدین ممکن است نگران مخاطرات ناشی از استفاده از فناوری‌های دیجیتال برای فرزندان‌شان باشند، درحالی‌که کودکان دخالت بیش از حد والدین را مسئله قلمداد کنند. در نظر گرفتن دیدگاه کودکان و نوجوانان درباره آسیب‌های اجتماعی و انجام مطالعات بیشتر به پر کردن این شکاف‌ها کمک می‌کند [۱].

ابهام در تمایز بین آسیب‌های اجتماعی برخط و برون خط: جدا کردن آسیب‌های برخط و برون خط مبهم است و در عالم واقع آنها دو روی یک سکه هستند [۲۱]. برای مثال اغفال جنسی از کودکان می‌تواند در محیط برخط شروع شود و به محیط برون خط کشیده شود یا اخاذی جنسی می‌تواند در محیط برون خط شروع و به محیط برخط کشیده شود، لذا نیاز است دوگانه برخط-برون خط کنار گذاشته شود.



تأثیر کسب‌وکارها: اگرچه کسب‌وکارها ممکن است مستقیماً در آسیب رساندن به کودکان نقش نداشته باشند اما آنها می‌توانند با طراحی و بهره‌برداری از خدمات دیجیتال باعث نقض حقوق کودکان شوند یا آن را تسهیل کنند. سازوکارهای ادغام کودکان در محیط دیجیتال نیز می‌تواند مخاطراتی را به همراه داشته باشد. برای مثال آنها می‌توانند مکان کودک را برای آزارگر احتمالی افشا کنند [۲۲].

۲-۳. رهنمودهای سیاستی محافظت از کودکان و نوجوانان در برابر آسیب‌های محیط دیجیتال

همان‌گونه که گفته شد تنظیم رفتارها، روابط و محتوا در محیط دیجیتال در ارتباط با محافظت از کودکان و تنظیم الگوی عمل ذی‌نفعان مرتبط با این محیط نیازمند قانونی جامع است. در این بخش تلاش می‌شود با مرور تجارب این حوزه در چند بخش، بسته‌ای سیاستی به منظور حمایت از کودکان و نوجوانان در برابر آسیب‌های محیط دیجیتال ارائه شود. قبل از ارائه این بسته لازم به ذکر است که هرگونه مقررگذاری در این زمینه نیازمند یک‌سری الزامات است که اهم آنها عبارت‌اند از:

جمع‌آوری داده‌های باکیفیت: همان‌گونه که گفته شد، شکاف بسیاری در شناخت ما از عوامل دستیابی / عدم دستیابی کودکان به فناوری‌های دیجیتال و نحوه تجربه و توجه آنها به فرصت‌ها و مخاطرات این محیط وجود دارد. در غیاب چنین شناختی، سیاستگذاری با چالش‌های متعددی از جمله ناتوانی در همگام شدن با سرعت سریع تغییرات فناوری و تأثیر آن بر زندگی کودکان مواجه است. همچنین محیط دیجیتال عمدتاً با این فرض که کاربران آن افراد بزرگسال هستند تنظیم شده است، درحالی‌که کودکان امروزه به اصطلاح «بومی دیجیتال»^۱ هستند [۱]. لذا لازم است داده‌های باکیفیت درباره موارد زیر به صورت دوره‌ای برای سیاستگذاری و بهبود قوانین موجود جمع‌آوری شود:

- میزان دسترسی / عدم دسترسی به فناوری‌های دیجیتال و اینترنت و عوامل مؤثر بر آنها،
 - مصرف رسانه‌ای در اشکال مختلف آن،
 - همه اشکال مخاطرات و آسیب‌های محیط دیجیتال با تأکید بر اشکال بهره‌کشی و سوءاستفاده جنسی از کودکان، چگونگی بروز آنها و اینکه چه کسانی بیشتر در معرض مخاطره هستند،
 - تعداد پرونده‌های گزارش شده، پیگرد قانونی، مجازات‌ها از جمله جبران خسارت ارائه شده به قربانیان،
 - ارزیابی واکنش فعلی نهادها،
 - بررسی پاسخ فعلی زیست‌بوم فناوری‌های اطلاعات و ارتباطات از جمله سازوکارهای گزارش‌دهی خطوط تلفن و تعامل آنها،
 - بررسی و ارزیابی فعالیت سایر ذی‌نفعان درگیر در این موضوع.
- جمع‌آوری چنین داده‌هایی قبل از تدوین یا اصلاح قانون به شفافیت در مورد موضوعات مورد بررسی، تعیین هدف قانون و اولویت‌های آن کمک می‌کند.

مشخص کردن نقطه شروع قانونگذاری: لازم است متناسب با تغییرات فناوری‌های دیجیتال و آسیب‌های ناشی از آنها برای کودکان، وضعیت قوانین به‌روز شوند. با توجه به وضعیت موجود هنگام فرایند اصلاح قانونگذاری، تعدادی احتمال وجود دارد: اصلاح قوانین موجود، تدوین قانون جدید یا ترکیبی از این دو. همان‌گونه که مرور شد در برخی از قوانین به صورت پراکنده به این موضوع پرداخته شده است و برخی از ابعاد این موضوع مغفول مانده است. از این رو آنچه که لازم است تدوین چارچوب قانونی واحد و جامع است که به همه ابعاد این موضوع بپردازد. همچنین لازم است ذی‌نفعان نحوه ورود به این موضوع را در نظر بگیرند. چند سناریو را در این زمینه می‌توان معرفی کرد. برای مثال می‌توان مقررات را در قانون جزایی، قانون جرائم سایبری یا امنیت سایبری، قانون حمایت از کودکان، قانون ایمنی برخط یا ترکیبی از آنها گنجانده [۸].

احترام به حقوق، آزادی‌های اساسی و فرصت‌ها برای کودکان: محافظت از کودکان در برابر آسیب‌های دیجیتال نباید به نقض

حقوق و آزادی‌های آنها نظیر دسترسی به اطلاعات و حق اظهار نظر منجر شود.

درخصوص مراقبت از کودکان در برابر مخاطرات و آسیب‌های محیط دیجیتال می‌توان مداخلات را به دو دسته اصلی تقسیم کرد: نخست، دسته‌ای از سیاست‌ها معطوف به زمینه‌های گسترده‌تر نظیر سیاست‌های بازی در مدارس و محلات، سیاست‌های حمایت از کودکان و نوجوانان محروم و غیره هستند. برای مثال هرچه زمینه‌ها برای بازی در مدارس و محلات فراهم باشد، کودکان و نوجوانان را از محیط دیجیتال و لذا آسیب‌های آن دور می‌کند. دوم، دسته‌ای دیگر از سیاست‌ها معطوف به محیط دیجیتال برای کودکان و نوجوانان و مراقبت از آنها در برابر مخاطرات این حوزه است. این دسته از سیاست‌ها بیشتر معطوف به این هستند که محیط دیجیتال و محتوای آن باید برای کودکان و نوجوانان چگونه باشد، چگونه از مخاطرات این محیط پیشگیری کرد و مداخلات حمایتی برای کودکان آسیب‌دیده باید چگونه باشد. رهنمودهای این گزارش بیشتر به دسته دوم از سیاست‌ها معطوف است. همچنین مقابله با مخاطرات، آسیب‌های اجتماعی و جرائم علیه کودکان در محیط دیجیتال موضوعی چندبعدی است و باید مسئولیت بخش‌های مختلف و ابعاد این موضوع مورد توجه قرار گیرد. دولت در بخش‌های مختلف، بخش خصوصی (کسب و کارها)، جامعه مدنی و خانواده‌ها در این زمینه مسئولیت دارد و ابعاد این موضوع شامل پیشگیری، درمان، حمایت از قربانیان، توان بخشی، ادغام مجدد و جبران خسارت، جرم‌انگاری و مجازات، تنظیم‌گری بین بخش‌های مختلف، همکاری‌های منطقه‌ای، بین‌المللی و غیره می‌شود. از این رو به فراخور مسئولیت و وظیفه بخش‌های مختلف و ابعاد موضوع رهنمودهای سیاستی به شرح زیر پیشنهاد می‌شود.

شکل ۱. ابعاد محافظت از کودکان در برابر مخاطرات و آسیب‌های محیط دیجیتال



مأخذ: همان.



۱-۲-۳. پیشگیری از مخاطرات و آسیب‌های ناشی از محیط دیجیتال برای کودکان

در یک تعریف کلی می‌توان گفت پیشگیری از آسیب‌های اجتماعی و بزهکاری نوعی رویکرد کنشی-پیشینی است که ماهیتی غیرقهرآمیز دارد و به دنبال کاهش یا از بین بردن عوامل فردی، اجتماعی، محیطی و وضعی مؤثر در وقوع آنها است [۲۳]. در این بخش با بهره‌گیری از رویکردهای رشدمدار، سلامت عمومی و وضعی راهبردهایی برای پیشگیری از آسیب‌های اجتماعی در محیط دیجیتال درخصوص مسئولیت دولت و خانواده‌ها پیشنهاد می‌شود. البته بخشی از پیشگیری ناظر بر مسئولیت کسب‌وکارها است که در بخش‌های بعد به آن پرداخته شده است.

■ **احراز هویت و سن کاربران در محیط دیجیتال و اجازه دسترسی پله‌ای برای استفاده از آن:** این پیشنهاد مبتنی بر ضوابط صیانت از کودکان و نوجوانان در خدمات تلفن همراه باند پهن (۱۳۹۳) است. بر این مبنا اپراتورها به ارائه سیم کارت کودک و نوجوان با قابلیت دسترسی به بسته‌های خدماتی جذاب تلفن همراه باند پهن متناسب با گروه‌های سنی کودک و نوجوان موظف شده‌اند. می‌توان گفت تعیین سن برای ایمنی دیجیتال از طریق طراحی و نحوه دسترسی به محیط دیجیتال مهم است، زیرا ارائه‌دهندگان خدمات تنها در صورتی می‌توانند از کودکان در برابر محتوا و رفتارهای ناامن محافظت کنند که بدانند کدامیک از کاربران‌شان کودک هستند. در این زمینه پیشنهاد می‌شود کودکان به صورت پله‌ای وارد محیط دیجیتال شوند و به‌هنگام وارد شدن باید هویت و سن‌شان احراز شود. در ابتدا لازم است تا سن مشخصی دسترسی به محیط دیجیتال برای آنها منع شود. در سنین بعد (برای مثال تا سن سیزده سالگی) استفاده از فناوری‌های دیجیتال و اینترنت می‌تواند برای کودکان با وجود یک‌سری از محدودیت‌ها نظیر عدم حضور در شبکه‌های اجتماعی و حضور با نظارت والدین مجاز باشد، و از سن سیزده سالگی به بعد با نظارت والدین و سایر مراقبان استفاده از اینترنت و شبکه‌های اجتماعی برای آنها مجاز قلمداد شود.^۱

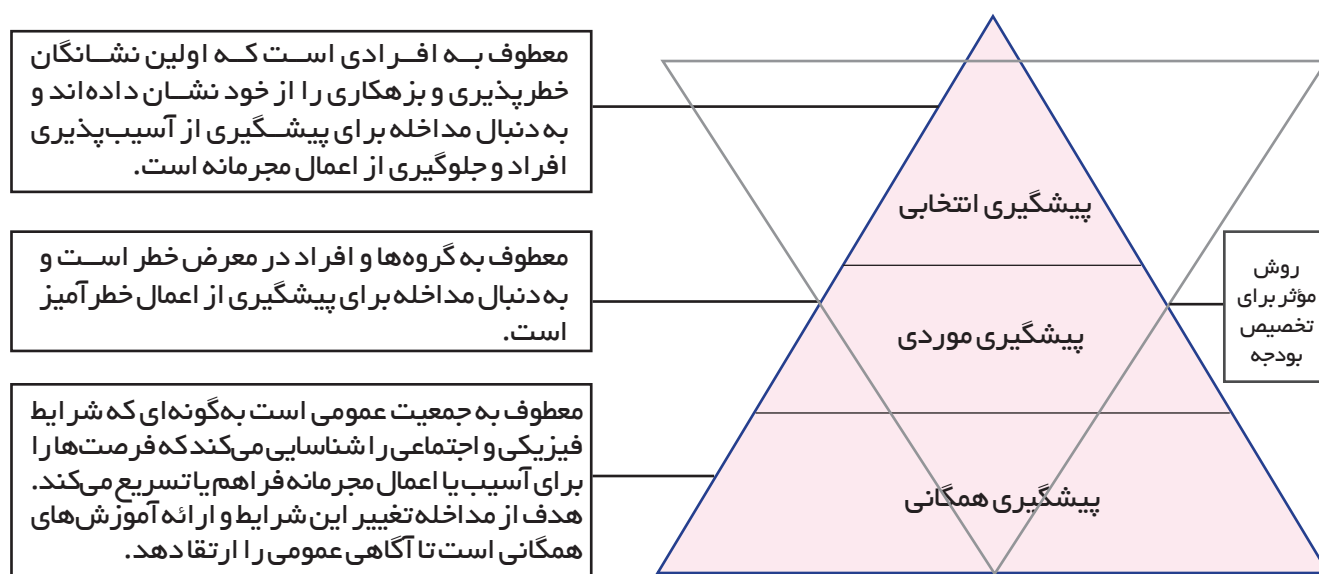
■ **استفاده از سازوکارهای تضمین سن^۲ یک گزینه در این زمینه است. بر مبنای این سازوکار:** ۱. اطمینان حاصل می‌شود که کودکان یا گروه‌های سنی خاصی از آنها نمی‌توانند به محتوای برخلاف یا خدمات دیجیتال بزرگسالان، مضر یا نامناسب دسترسی پیدا کنند و ۲. تأیید سن کاربر به گونه‌ای است که خدمات دیجیتالی باید بتواند براساس نیازهای آنها تنظیم شود و تدابیر حفاظتی متناسب با سن را اعمال کند. تضمین سن چندین شکل دارد، اما به صورت کلی به عنوان فناوری‌ها یا سازوکارهای تقسیم می‌شود که سن یا محدوده سنی کاربر را تخمین می‌زند («تخمین سنی») و آنهایی که سن واقعی کاربر را تأیید می‌کنند («تأیید سن»). سازوکار تضمین سن نباید تنها به خوداظهاری کاربران محدود شود و لازم است بسته به مواردی نظیر منابع تأییدکننده کارت شناسایی صادر شده که تاریخ تولد را نشان می‌دهد، داده‌های بیومتریک، مانند صدا یا ویژگی‌های چهره که می‌توانند برای تخمین سن کاربر استفاده شوند و بررسی سن توکن^۳ با استفاده از داده‌های بهداشتی یا آموزشی که در اختیار عموم قرار دارد نیز استفاده شود [۲۴].

■ **بهره‌گیری از رویکردهای پیشگیری متناسب با کودکان برای جلوگیری از آسیب‌پذیری:** رویکردهای سلامت عمومی و رشدمدار برای پیشگیری از مخاطرات و آسیب‌های اجتماعی به‌ویژه در دوره کودکی توصیه شده‌اند. رویکرد نخست، با توجه به درجه خطرپذیری گروه‌ها و افراد، مداخلات پیشگیری را به سه سطح همگانی، موردی و انتخابی تقسیم می‌کند. رویکرد رشدمدار به راهبردهایی توجه دارد که باعث کاهش عوامل خطر و تقویت عوامل محافظ در مراحل مختلف رشد می‌شوند. به عبارت دقیق‌تر برای هر دوره از رشد راهبردها و مداخلات متفاوتی را پیشنهاد می‌کند [۲۵]. ایجاد محدودیت سنی برای ایمنی دیجیتال که در بالا مرور شد نمونه‌ای از مداخلات رشدمدار است.

۱. هایت در این زمینه به موارد زیر اشاره دارد: ۱. دسترسی به تلفن‌های هوشمند باید تا قبل از دبیرستان ممنوع باشد، ۲. دسترسی به رسانه‌های اجتماعی باید تا قبل از ۱۶ سالگی ممنوع باشد، ۳. استفاده از تلفن باید در مدارس ممنوع باشد و ۴. استقلال دوران کودکی و بازی‌های عاری از نظارت باید بیشتر شوند [۴۹].

1. Age Assurance
3. Tokenised Age

شکل ۲. هرم پیشگیری از آسیب‌های اجتماعی [۷]



شکل بالا، سه سطح را برای پیشگیری معرفی می‌کند و بیان می‌دارد بیشترین میزان اعتبار باید به مداخلات پیشگیری در سطوح موردی و انتخابی تخصیص یابد. درخصوص آسیب‌های اجتماعی محیط دیجیتال اهم راهبردها برای پیشگیری به تفکیک سه سطح عبارت‌اند از:

پیشگیری همگانی

ابتکارات پیشگیری همگانی شامل موارد زیر می‌شود:

- ایجاد کمپین‌های آگاهی‌بخشی: حصول اطمینان از آگاهی کودکان و والدین آنها در مورد حقوق کودکان در محیط دیجیتال، آسیب‌های این حوزه و شیوه‌های مقابله با آنها ضروری است. لازم است اطلاعات مفید در این زمینه در اختیار کودکان و خانواده‌ها قرار گیرد. راه‌اندازی کمپین‌های آگاهی‌بخشی به‌ویژه برای کسانی که اقداماتشان تأثیر مستقیم یا غیرمستقیم بر کودکان دارد مفید است. همچنین این کمپین‌ها می‌توانند شامل توسعه برنامه‌های آموزشی درباره نحوه محافظت از حریم خصوصی، جلوگیری از قربانی شدن و شناسایی و پاسخ به کودک در معرض خطر در محیط دیجیتال برای کودکان و خانواده‌ها، افراد جامعه و تصمیم‌گیرندگان باشند. چنین محتوایی باید متناسب با سن و به شیوه‌های درخور و خلاق برای کودکان و خانواده‌ها ارائه شود [۲۲].
- تمرکز بر تغییر هنجارها، نگرش‌ها و رفتارهای اجتماعی در سطح جامعه با تولید محتوا و آموزش‌های همگانی،
- آموزش مهارت‌های زندگی، روابط سالم، تربیت جنسی براساس مبانی ایرانی-اسلامی، پیشگیری از قربانی سوءاستفاده جنسی و بهره‌کشی اقتصادی شدن در محیط دیجیتال، بهبود روابط بین والد-فرزند با ارائه آموزش‌های فرزندپروری و ...،
- آموزش مهارت‌ها و سواد رسانه‌ای به کودکان که متضمن مجموعه‌ای از شایستگی‌هاست و فراتر از مهارت‌های دیجیتال و فنی است و شامل توانایی جستجو، ارزیابی و مدیریت اطلاعات، تعامل، اشتراک‌گذاری و همکاری برخط؛ توسعه و ایجاد محتوا؛ استفاده از ویژگی‌های ایمنی و حفاظتی، حل مشکلات و خلاق بودن است [۱]. دانش و مهارت‌هایی که لازم است کودکان بیاموزند می‌تواند شامل موارد زیر باشد:
- **مهارت‌های ایمنی که اهم این مهارت‌ها عبارت‌اند از:** درک مخاطرات و محافظت از دستگاه‌ها و داده‌ها، حفظ حریم خصوصی، محافظت از داده‌های شخصی برخط و چگونگی محافظت از خود در برابر مخاطرات برخط نظیر قلدری و اخاذی جنسی، از دست دادن حریم خصوصی و مخاطرات ایجاد و اشتراک‌گذاری محتوا و داده‌ها،
- مهارت‌های درک، تفکر انتقادی و حل مسئله،



- مهارت‌های اجتماعی - ارتباط و تعامل مسئولانه،
- مهارت‌های پردازش اطلاعات: تولید محتوا و مشارکت،
- تقویت آموزش مدارا و همدلی در محیط دیجیتال و
- درک مسئولیت خود در قبال سایر کاربران.
- سایر اقدام‌هایی که باید در سطح کلان‌تر انجام شود، شامل موارد زیر است:
- حمایت از گنجاندن آموزش سواد دیجیتال در مدارس و برنامه‌های درسی آموزشی و در برنامه‌های آموزشی نظام مراقبت اجتماعی از دانش‌آموزان،
- حمایت ویژه از کودکان اجتماعات محروم و به حاشیه رانده شده،
- تربیت کادر متخصص برای ارائه این آموزش‌ها،
- توسعه مهارت‌ها و سواد دیجیتالی معلمان و والدین،
- ایجاد کتابخانه‌های برخط و سایر منابع آموزشی که در آن کودکان می‌توانند از راه دور و به‌صورت رایگان به آنها دسترسی داشته باشند و برگزاری برنامه‌های فوق‌العاده [۹، ۲۶].
- از آنجا که بخشی از کودکان از سنین خردسالی از فناوری‌های دیجیتال استفاده می‌کنند، لازم است آموزش‌ها و برنامه‌ها نیز از سنین پایین شروع شود تا علاوه بر ارتقای آگاهی همچنین آنان را برای سایر دوره‌های زندگی نیز آماده کنند.
- پیشگیری موردی:** این نوع از پیشگیری به دنبال حمایت و مراقبت از زیرگروه‌ها و افراد پرخطر نظیر کودکان در اجتماعات محروم و به حاشیه رانده شده، دانش‌آموزان دارای مشکلات تحصیلی و مواردی از این دست است. همچنین این نوع از پیشگیری معطوف به افرادی است که در معرض خطر جرم هستند و می‌تواند شامل برنامه‌هایی برای کمک به رسیدگی در رفتارهای مضر و اطمینان از درک افراد از پیامدهای احتمالی جرم باشد.
- پیشگیری انتخابی:** این سطح از پیشگیری معطوف به افرادی است که دارای اولین نشانگان اختلال یا رفتارهای پرخطر هستند. برای مثال کودکانی که به فناوری‌های دیجیتال وابسته هستند و خود و دیگران را به خطر می‌اندازند نمونه‌هایی از این دسته از کودکان هستند. لازمه دستیابی به اهداف پیشگیری انتخابی و موردی، طراحی بسته‌های متناسب با درجه خطرپذیری گروه‌ها و افراد است.
- **توسعه ابزارهای کنترل والدین:** یکی از راه‌های محافظت والدین از فرزندانشان در محیط دیجیتال نظارت بر آنها است. جزء «۲» بند «ب» ماده (۴) سند صیانت از کودکان و نوجوانان در فضای مجازی (۱۴۰۰) توصیه به استفاده از چنین ابزارهایی کرده است. به همین منظور ابزارهای مختلفی برای نظارت والدین بر استفاده فرزندانشان از محیط دیجیتال طراحی شده است. برخی از نمونه‌های داخلی آنها عبارت‌اند از: نرم‌افزارهای انارستان، درس‌آ، سانیار و سامانه مراقبت از خانواده در دنیای مجازی. لازم است این ابزارها با قابلیت‌های متنوع و متناسب با سن و مرحله رشد کودکان طراحی شود، نحوه استفاده از آنها به والدین آموزش داده شود و به‌صورت رایگان در اختیار خانواده‌ها قرار گیرد [۲۶، ۲۷].
- **رتبه‌بندی و طبقه‌بندی محتوا، ارتباطات و اطلاعات برحسب سن، جنسیت و سایر ویژگی‌های فرهنگی و اجتماعی برای کودکان و همچنین حذف و مسدود کردن محتوای غیرقانونی:** رتبه‌بندی و طبقه‌بندی محتوا، ارتباطات و اطلاعات برای کودکان و نوجوانان مبتنی بر بند «۳» ماده (۱) سند صیانت از کودکان و نوجوانان در فضای مجازی (۱۴۰۰) است. همچنین لازم است دولت به کمک اپراتورها و توسعه سازوکارهایی نظیر «اطلاع و حذف / برداشتن»^۱ و «خط تلفن اضطراری»^۲ محتوای غیرقانونی در بستر محیط دیجیتال را شناسایی کند و آنها را مسدود و حذف کند. در بخش مسئولیت کسب‌وکارها به‌صورت دقیق‌تر به برخی از سازوکارهای شناسایی و حذف محتوای غیرقانونی پرداخته شده است.

1. Notice and Takedown (NTD)
2. Hotline

برنامه‌های پیشگیری از آسیب‌پذیر شدن کودکان در محیط دیجیتال لازم است در نظام‌های پیشگیری موجود نظیر نظام مراقبت اجتماعی از دانش‌آموزان و برنامه‌های سازمان بهزیستی کشور ادغام شود. البته برخی از آنها نظیر ایجاد محدودیت سنی برای دسترسی به محیط دیجیتال، احراز هویت، سن و رتبه‌بندی و طبقه‌بندی محتوا، ارتباطات و اطلاعات معطوف به مسئولیت سایر دستگاه‌ها از جمله وزارت ارتباطات و فناوری اطلاعات است. بر مبنای آنچه که مرور شد توصیه‌های سیاستی زیر پیشنهاد می‌شود:

- احراز هویت و سن کاربران در محیط دیجیتال از طریق سازوکارهای تضمین سن و هویت و اجازه استفاده پله‌ای برای دسترسی به این محیط با استفاده از سازوکارهایی نظیر محدودیت استفاده تا سن مشخص (برای مثال تا سن هشت‌سالگی)، اعمال محدودیت جهت استفاده از این محیط نظیر عدم استفاده از شبکه‌های اجتماعی عمومی برای کودکان ۹ تا سیزده ساله و استفاده از این محیط با کنترل والدین از سنین چهارده تا هجده‌سالگی،
- پیشگیری از آسیب‌های محیط دیجیتال با راه‌اندازی کمپین‌ها، ارائه آموزش‌های همگانی، آموزش مهارت‌ها و سواد رسانه‌ای (دیجیتال)، شناسایی گروه‌ها و افراد در معرض خطر و طراحی بسته‌های حمایتی و مداخلاتی مناسب برای کاهش خطرپذیری آنها،
- ایجاد و تقویت ابزارهای کنترل والدین و در اختیار قرار دادن و آموزش رایگان آن برای خانواده‌ها،
- رتبه‌بندی و طبقه‌بندی محتوا، ارتباطات و اطلاعات بر حسب سن، جنسیت و سایر ویژگی‌های فرهنگی و اجتماعی برای کودکان و همچنین حذف و مسدود کردن محتوای غیرقانونی،
- وزارت آموزش و پرورش نیز می‌تواند به تناسب مقطع تحصیلی و جنسیت دانش‌آموزان آموزش‌های سواد رسانه‌ای را در محتوای کتاب‌های درسی بگنجانند و مقررات خاصی را برای استفاده از فضای دیجیتال در مدرسه تنظیم کند.

۲-۳. مسئولیت و وظایف کسب‌وکارها

کسب‌وکارها^۱ به‌ویژه کسب‌وکارهای حوزه دیجیتال از ذی‌نفعان کلیدی محافظت از کودکان در برابر آسیب‌های برخط هستند. آنها به‌عنوان ارائه‌دهندگان خدمات اینترنت، سرگرمی، محتوا، کالاهای دیجیتال و سایر کالاها و خدمات برخط، نقش زیادی در زندگی کودکان دارند. همچنین کسب‌وکارها به‌عنوان دروازه‌بان‌هایی که جریان اطلاعات را در سراسر شبکه‌ها کنترل می‌کنند، به حجم وسیعی از اطلاعات و داده‌های کودکان نیز دسترسی دارند. این نقش‌ها قدرت و نفوذ قابل‌توجهی به آنها داده است. از این‌رو کسب‌وکارها باید حمایت از حقوق کودکان را در مرکز سیاست‌ها و برنامه‌های خود قرار دهند و توجه ویژه‌ای به حفاظت از حریم خصوصی، داده‌های شخصی، تحقق حقوق از جمله حق آزادی بیان و مشارکت و ایجاد نظام‌هایی برای رسیدگی به نقض حقوق آنها در صورت وقوع داشته باشند [۲۸].

تنها صحبت کردن درباره مسئولیت شخصی کسب‌وکارها کافی نیست، آنها باید فعالانه به کودکان کمک کنند تا از حریم خصوصی خود و در برابر مخاطرات و آسیب‌ها محافظت کنند. به عبارت دقیق‌تر باید از قدرت و نفوذ کسب‌وکارها برای پیشبرد استانداردهای اخلاقی در سطح فناوری در مورد احقاق حقوق کودکان و همچنین محافظت از آنها در برابر مخاطرات برخط استفاده کرد. یونیسف پنج حوزه کلیدی را برای کسب‌وکارها جهت حمایت و محافظت از حقوق کودکان به‌هنگام استفاده از فناوری اطلاعات و ارتباطات و ترویج استفاده مثبت آنها برشمرده است که عبارت‌اند از:

۱. ادغام ملاحظات حقوق کودک در تمام سیاست‌ها و فرایندهای کسب‌وکارها؛
 ۲. توسعه فرایندهای استاندارد برای رسیدگی به محتوای سوءاستفاده جنسی از کودکان؛
 ۳. ایجاد محیط برخط امن‌تر و متناسب با رده سنی؛
 ۴. آموزش کودکان، والدین و معلمان در مورد ایمنی کودکان و استفاده مسئولانه از فناوری اطلاعات و ارتباطات و
 ۵. ترویج فناوری دیجیتال به‌عنوان روشی برای افزایش مشارکت مدنی [۳].
- البته مسئولیت کسب‌وکارهای دیجیتال تنها محدود به موارد بالا نمی‌شود و در اسناد بین‌المللی و ملی موارد بیشتری ذکر شده

۱. کسب‌وکارها می‌توانند خصوصی، دولتی یا ترکیبی از هر دو باشند.

است که در این بخش به آنها پرداخته شده است. روی هم رفته کسب و کارها نقشی حیاتی در **حذف محتوای سوءاستفاده جنسی از کودکان، شناسایی قربانیان و ردیابی مجرمان** دارند [۱]. اما قبل از هر چیزی به منظور تهیه پیش‌نویس قانون در این زمینه، داشتن درک صحیح از دسته‌های مختلف ذی‌نفعان کسب و کارها در امتداد آنچه که ممکن است به عنوان «زنجیره ارزش اینترنتی»^۱ نامیده شود و نقشی که آنها در محیط دیجیتال ایفا می‌کنند مهم است. باین حال، به طور فزاینده‌ای، کسب و کارها در سایر بخش‌ها نیز در حال توسعه یا به کارگیری فناوری‌های دیجیتال هستند، بنابراین مسائل مطرح شده در این بخش می‌تواند به کسب و کارهایی که به صورت دقیق در بخش دیجیتال نیستند نیز مرتبط باشد. کسب و کارها در زنجیره ارزش اینترنتی به پنج دسته ذی‌نفع تقسیم شده‌اند. شکل زیر نشان‌دهنده این پنج دسته است:

شکل ۳. زنجیره ارزش اینترنت [۲۹]



دارندگان حقوق محتوا: کسب و کارهای این بخش مالک انواع حقوق مختلف محتوا برای توزیع از طریق اینترنت هستند و در بیشتر موارد آنها را به دیگران می‌فروشند. حقوق محتوا شامل محتوای «ساخته شده برای محیط دیجیتال» است که جهت توزیع از طریق اینترنت تولید می‌شود. محتوا را می‌تواند کاربر مبتدی یا حرفه‌ای تولید کند. البته ممکن است محتوا شامل محتوای مضر برای کودکان باشد.

خدمات برخط: شامل طیف متنوعی از خدمات مصرف‌کننده و خدمات تجاری است که از طریق اینترنت یا به عبارت دیگر از طریق مرورگرها یا پلتفرم‌های کاربردی ارائه می‌شود. خدمات برخط را نیز می‌توان به پنج دسته تقسیم کرد، که هر یک ممکن است با متخلفان به عنوان وسیله‌ای برای سوءاستفاده از کودکان استفاده شود. این پنج دسته عبارت‌اند از: خدمات تجارت الکترونیک^۲، خدمات سرگرمی^۳، خدمات جستجو^۴، پلتفرم‌های جامعه‌ای و اجتماعی^۵، خدمات ابری^۶ و سایر خدمات الکترونیکی^۷.

فعال کردن فناوری و خدمات: گستره وسیعی از خدمات را پوشش می‌دهد که برای عملکرد کارآمد زیرساخت کلی اینترنت و وب‌سایت‌ها، سرورها، پلتفرم‌ها و استفاده از خدمات ضروری هستند. حضور فناوری و خدمات توانمند در این بخش در مبارزه با سوءاستفاده برخط از کودکان مهم است.

اتصال: به تأمین‌کنندگان خدماتی مانند خدمات دسترسی به اینترنت سریع اشاره دارد که کاربران نهایی را از طریق تلفن همراه یا دسترسی ثابت به اینترنت متصل می‌کند. ارائه‌کنندگان خدمات اینترنت ثابت و سیار نمونه‌ای از این تأمین‌کنندگان هستند.

واسطه‌های کاربر: واسطه‌های کاربر ممکن است به عنوان «ملموس‌ترین» بخش زنجیره ارزش اینترنت در نظر گرفته شوند چراکه شامل دستگاه‌ها، سیستم‌ها و نرم‌افزارهایی است که کاربران نهایی برای دسترسی به اینترنت و خدمات ذکر شده در بالا استفاده می‌کنند [۲۹]. حال استانداردهای توصیه شده برای کسب و کارها جهت محافظت از آنها در برابر آسیب‌های محیط دیجیتال عبارت‌اند از:

1. Internet Value Chain

۲. این خدمات شامل شرکت‌های خرده‌فروشی الکترونیکی است که کالاها و خدمات را به صورت برخط می‌فروشند و ممکن است به عنوان وسیله‌ای برای تولید، توزیع و فروش محتوای سوءاستفاده جنسی کودکان یا ارائه خدمات برای تسهیل بهره‌کشی و سوءاستفاده جنسی از آنها استفاده شوند.

۳. این خدمات شامل خدمات انتشاراتی، بازی، پلتفرم‌های ویدئویی و خدمات موسیقی است.

۴. این خدمات شامل موتورهای جستجوی برخط مانند گوگل و همچنین اطلاعات و خدمات مرجع مانند نقشه‌های گوگل و ویکی‌پدیا می‌شود. شرکت این خدمات برای مبارزه با سوءاستفاده از کودکان حیاتی است، به عنوان مثال، با جلوگیری از نمایش وب‌سایت‌هایی که میزبان محتوای سوءاستفاده جنسی از کودکان در نتایج جستجو هستند.

۵. شامل پلتفرم‌هایی مانند فیسبوک، توئیتر، اینستاگرام، اسنپ‌چت و لینکدین و سرویس‌های ارتباطی مانند واتساپ است که ممکن است توسط مجرمان برای سوءاستفاده از کودکان استفاده شود.

6. Cloud Services

۷. این خدمات شامل برنامه‌های پولی و سرویس‌های وب مبتنی بر تبلیغات و برنامه‌هایی است که ممکن است برای تبلیغ مطالب سوءاستفاده جنسی از کودکان استفاده شوند.

ارائه ضوابطی در قوانین مربوطه، جهت توانمند کردن کسب‌وکارها برای ایجاد دسترسی آحاد جامعه به‌ویژه خانواده‌ها و کودکان در مناطق محروم و به حاشیه رانده شده به فناوری‌ها و خدمات دیجیتال.

امروزه در زندگی استفاده از فناوری‌ها و خدمات دیجیتال در حوزه‌های مختلف، همچون آموزش، اقتصاد، سلامت، سرگرمی و غیره اجتناب‌ناپذیر شده است. در اقتصاد دیجیتالی نیز دسترسی به فناوری‌های دیجیتال همچون اینترنت و داشتن مهارت برای مشارکت اقتصادی ضروری است. فقدان دسترسی به این فناوری‌ها و خدمات باعث طرد و به حاشیه رانده شدن و لذا سایر آسیب‌ها می‌شود. تجربه کرونا و اجتماعات و افرادی که به این فناوری‌ها دسترسی نداشتند و از تحصیل و آموزش جا ماندند، یک مثال در این زمینه است. تلاش برای دسترسی آحاد جامعه به‌ویژه کودکان در مناطق محروم و به حاشیه رانده شده به فناوری‌ها و خدمات دیجیتال وظیفه دولت‌ها و مسئولیت کسب‌وکارها است. دولت‌ها می‌توانند با فراهم کردن حمایت‌ها و مشوق‌ها برای کسب‌وکارهای اینترنتی، دسترسی به فناوری‌ها و خدمات دیجیتال را توسعه دهند. کسب‌وکارها نیز می‌توانند با شرکای خود کار کنند تا زیرساخت‌های فناوری‌های دیجیتال را برای کودکان در مکان‌های دورافتاده ایجاد کنند [۱].

وظایف و مسئولیت‌های کسب‌وکارها باید با استفاده از رویکرد حقوق‌محور، در چارچوب گسترده‌تر حقوق بشر و اصول تجارت مورد بررسی قرار گیرد.

برخی نهادهای بین‌المللی حمایت از حقوق کودکان توصیه می‌کنند هنگام تدوین قانون در زمینه محافظت از کودکان در برابر آسیب‌های برخط، باید مسئولیت کسب‌وکارها در چارچوب گسترده‌تری نظیر اصول راهنمای سازمان ملل در تجارت و حقوق بشر را مورد توجه قرار داد. در این چارچوب کشورها تعهد به «احترام، محافظت و تحقق» حقوق کودکان را دارند که باید در محیط دیجیتال نیز اعمال شود. بر این مبنا لازم است دولت‌ها کسب‌وکارها را ملزم به رعایت حقوق کودکان کنند. این رویکرد شامل توسعه، نظارت، اجرا و ارزیابی «قوانین، مقررات و خط‌مشی‌ها» از سوی دولت‌ها است تا اطمینان حاصل شود که کسب‌وکارها تعهدات خود را برای تحقق حقوق کودکان و جلوگیری از سوءاستفاده از آنها به‌واسطه شبکه‌ها و خدمات برخط انجام دهند. دولت همچنین ملزم به محافظت از کودکان در برابر نقض حقوق آنها از سوی کسب‌وکارها است. علاوه بر موارد نامبرده در بالا این شامل بررسی و قضاوت در مورد جبران تخلفات در صورت وقوع نیز است. کمیته پیمان‌نامه حقوق کودک همچنین راهنمایی‌های خاصی را در مورد نقش کسب‌وکارها در حمایت از حقوق کودکان در محیط دیجیتال ارائه می‌دهد که شامل حق کودک برای محافظت در برابر بهره‌کشی و سوءاستفاده جنسی و همچنین طیف وسیعی از حقوق دیگر در پیمان‌نامه مانند حفظ حریم خصوصی، حق دسترسی به اطلاعات و آزادی بیان است [۲۲].

قانون تنظیم رفتار، خدمات و طراحی کسب‌وکارهای حوزه فناوری‌های دیجیتال، باید حقوق کودکان را در هسته اصلی قرار دهد. یکی از ابزارهای اولیه محافظت از کودکان در برابر آسیب‌های برخط، ایجاد محیط دیجیتالی امن، متناسب با سن، فراگیر و مشارکتی برای کودکان است [۳]. این موضوع براساس بند «۳» ماده (۱) [سند صیانت از کودکان و نوجوانان در فضای مجازی \(۱۴۰۰\)](#) است. در همین زمینه کمیته پیمان‌نامه حقوق کودک نیز به کشورهای عضو توصیه می‌کند تا کسب‌وکارها (کسب‌وکارهایی که بر حقوق کودکان در محیط دیجیتال اثر می‌گذارند) را ملزم کنند، چارچوب‌های نظارتی، کدهای صنعتی و شرایط خدماتی را پیاده‌سازی کنند که از بالاترین استانداردهای اخلاقی، حفظ حریم خصوصی و ایمنی در رابطه با طراحی، مهندسی، توسعه، بهره‌برداری، توزیع و بازاریابی محصولات و خدمات خود پیروی کنند. به‌صورت ویژه‌تر این براساس بند «۱» ماده (۳) کمیته پیمان‌نامه حقوق کودک است که پیشنهاد می‌کند مصالح عالی‌ه کودکان در همه اقدام‌ها از جمله اقدام‌های مربوط به کسب‌وکارهای بخش خصوصی باید از اهم ملاحظات باشد [۳۰]. لذا دولت باید اطمینان حاصل کند که مصالح عالی‌ه کودکان در قوانین و سیاست‌هایی که فعالیت‌ها و عملیات کسب‌وکارهای حوزه دیجیتال را شکل می‌دهند جاری باشد. این رویکرد مبتنی بر حقوق کودک برای تنظیم رفتار تجاری، خدمات و طراحی فناوری‌های دیجیتال است که به آن «حقوق به‌واسطه طراحی»^۱ نیز گفته می‌شود. به‌این‌ترتیب، حقوق به‌واسطه طراحی ملاحظات مربوط به حریم خصوصی و ایمنی طراحی را دربرمی‌گیرد که دولت باید از طریق خدمات و محصولات دیجیتال برای به

1. Rights-by-Design



حداقل رساندن خطر آسیب به کودکان از آن استفاده کند [۸].

الزام کسب‌وکارها به اتخاذ سازوکارهای تضمین سن، مطابق با الزامات حفاظت از داده‌ها و تدبیر حفاظتی^۱، برای جلوگیری از دسترسی یا قرار گرفتن کودکان در معرض هرزه‌نگاری و سایر محتوای جنسی غیرقانونی یا نامناسب.

باید سازوکارهای اندیشیده شود که دسترسی کودکان به محتوای غیرقانونی و نامناسب محدود یا از قرار گرفتن کودکان در معرض چنین محتوایی جلوگیری شود. این سازوکارها می‌تواند شامل ابزارهای کنترل والدین، ایجاد محتوای محافظت‌شده با رمز عبور برای سنین مختلف، فهرست‌های مسدود / مجاز، عملکردهای انصراف / خروج، فیلتر کردن، نظام‌های تأیید سن و غیره باشد [۲۲]. برای مثال دستورالعمل‌های شورای اروپا برای احترام، حفاظت و تحقق حقوق کودکان در محیط دیجیتال از کشورها می‌خواهد تا از سازوکارهای تأیید سن استفاده کنند [۲۸]. همچنین تأکید شده است که سازوکارهای تضمین سن نباید به صورت مجزا مورد استفاده قرار گیرد، بلکه باید به عنوان بخشی از رویکرد گسترده‌تر و چندوجهی برای محافظت از کودکان برخط استفاده شود. درنهایت، اتخاذ سازوکارهای کنترل تضمین سن و گنجاندن آن در قانون، موضوع پیچیده‌ای است که حداقل مستلزم در نظر گرفتن مواردی نظیر توجه به مراحل رشد و ظرفیت‌های کودک، عدم نقض حریم خصوصی و شواهدمحور بودن آن است [۹].

الزام کسب‌وکارها برای ایجاد رویه‌های اطلاع و حذف محتوای نامناسب، از جمله الزام به مسدود کردن یا حذف محتوای سوءاستفاده جنسی از کودکان با یک پرچم‌دار معتمد و به رسمیت شناخته شده که قانون تعیین کرده باشد.

اطلاع و حذف، فرایندی است که با کسب‌وکارها (میزبان‌های برخط) در پاسخ به دستورات دادگاه مبنی بر غیرقانونی بودن محتوا از جمله محتوای سوءاستفاده جنسی از کودکان در شبکه‌ها یا خدمات و برای جلوگیری از دسترسی و توزیع بیشتر انجام می‌شود. دلیل اطلاع و حذف این است که مطالب سوءاستفاده جنسی از کودکان می‌تواند به صورت نامحدود در محیط دیجیتال پخش شود، آسیب به کودکان قربانی را تداوم بخشد و باعث تقویت پنداشت «کودک به عنوان شیء جنسی»^۲ شود. بنابراین ضروری است که سازوکارهایی ایجاد شود تا کاربران، از جمله کودکان و عموم جامعه، بتوانند محتوای سوءاستفاده از کودکان را گزارش دهند تا آن محتوا به سرعت حذف یا مسدود شود [۸].

ارائه ضوابطی در قوانین مربوطه، جهت توانمند کردن کسب‌وکارها برای شناسایی فعالانه محتوای سوءاستفاده جنسی از کودکان که در محصولات یا خدمات در دسترس یا ذخیره شده آنها به منظور مسدود کردن یا حذف چنین محتوایی، مشروط بر اینکه قانون چنین اقدام‌هایی را مشروع، ضروری و متناسب و کم مزاحم‌ترین گزینه موجود، بدون خدشه‌دار کردن ماهیت حق حریم خصوصی افراد بداند.

مطالعه تجارب آسیب‌های برخط در دوران کودکی در سایر کشورها نشان می‌دهد که ۷۹ درصد از افراد مورد بررسی محتوای غیراخلاقی جنسی را در تلفن همراه خود دریافت کرده‌اند [۳۱]، از این رو شناسایی و حذف چنین محتوایی در محیط دیجیتال ضروری است. به همین منظور بسیاری از دولت‌ها و کسب‌وکارها در فناوری‌های جدید و هوش مصنوعی برای شناسایی فعالانه محتوای سوءاستفاده جنسی از کودکان و برخی دیگر از مخاطرات برخط سرمایه‌گذاری کرده‌اند تا پس از شناسایی این محتوا آنها را مسدود و حذف کنند یا آن را به مجری قانون گزارش دهند. ابزارهایی نظیر عکس دی‌ان‌ای و سالوس^۳ نمونه‌هایی از این موارد است. در شناسایی محتوای سوءاستفاده جنسی از کودکان، حفظ حریم خصوصی آنها مهم است. حفظ حریم خصوصی علاوه بر اینکه برای عاملیت و منزلت کودکان حیاتی است، برای ایمنی آنان نیز ضروری است. باین حال، حق حریم خصوصی افراد مطلق نیست و ممکن است در شرایط خاصی محدود شود. براساس استانداردها، هرگونه مداخله در حریم خصوصی افراد، از جمله در محیط دیجیتال، باید قانونی، ضروری، متناسب با مصالح عالیه کودک، کمترین مزاحم موجود بوده و نباید با مفاد، اهداف یا مقاصد پیمان‌نامه حقوق کودک مغایر باشد [۲۲].

1. Protection and Safeguarding

2. Child as a Sexual Object

3. Salus

سالوس برنامه ایمنی جدید است که روی دستگاه دیجیتال نظیر تلفن همراه قابل نصب است. تولیدکنندگان این برنامه بر این باورند که این ابزار می‌تواند برای پیشگیری پایدار و طولانی‌مدت از محتوای سوءاستفاده جنسی از کودکان و قربانی کردن مجدد بازماندگان حیاتی باشد.

کسب‌وکارها باید محتوای برخاسته از سوءاستفاده جنسی از کودکان را به مجری قانون یا سایر نهادهای تعیین شده در قانون گزارش دهند.

بررسی و شناسایی جرائم علیه کودکان در محیط دیجیتال به همکاری مؤثر بین بخش‌های مختلف از جمله بین صنعت فناوری و مجریان قانونی متکی است. این شامل کسب‌وکارهایی می‌شود که جرائم مربوط به محتوای سوءاستفاده جنسی از کودکان را به مجری قانون گزارش می‌دهند. بدون چنین همکاری‌ای شناسایی و بازداشت مجرمان و کسانی که به کودکان آسیب می‌زنند دشوار و در برخی موارد غیرممکن است [۱].

در نظر گرفتن طیف وسیعی از مجازات‌های کیفری، مدنی و اداری برای اشخاص حقوقی زمانی که علیه کودکان در فضای برخاسته مرتکب جرمی می‌شوند و تعهداتشان را برای محافظت از کودکان در برابر چنین آسیب‌هایی نقض می‌کنند.

جایی که کسب‌وکارها مرتکب جرائم برخاسته علیه کودکان می‌شوند، در آن مشارکت می‌کنند یا آن را تسهیل می‌کنند برای مثال محتوای سوءاستفاده جنسی از کودکان را به صورت برون‌خط یا برخاسته توزیع می‌کنند، دارای مسئولیت کیفری هستند. مسئولیت اشخاص حقوقی ممکن است کیفری، مدنی یا اداری باشد. اشخاص حقوقی باید مشمول مجازات یا اقدام‌های کیفری یا غیرکیفری مؤثر، متناسب و بازدارنده از جمله مجازات‌های مالی شوند [۲۲].

پردازش داده‌های کودکان برای مقاصد اقتصادی توسط کسب‌وکارها به‌ویژه در مواردی که می‌تواند به کودکان آسیب رساند می‌بایست منع و جرم‌انگاری شود.

هر بار که کودکان محتوایی را در رسانه به اشتراک می‌گذارند یا چیزی را جستجو می‌کنند، داده تولید می‌شود. این داده‌ها به نوبه خود وارد صنعتی می‌شوند که اطلاعات شخصی کودکان، از جمله هویت، مکان و ترجیحات آنها را پردازش می‌کند. کودکان ممکن است درک بسیار محدودی از مخاطرات این پردازش داشته باشند. پردازش داده‌ها از فعالیت‌های برخاسته بر همه به صورت مثبت یا منفی تأثیر می‌گذارد [۱]. کودکان همچنین در معرض خطر نقض یا سوءاستفاده از حقوق‌شان هستند. والدین نیز اغلب نمی‌دانند چه داده‌هایی و در چه موضوع‌هایی از فرزندانشان جمع‌آوری می‌شود [۳۲]. هنگامی که فناوری‌های دیجیتال کودک را برای مقاصد خود به تصویر می‌کشند، عدم آگاهی والدین نیز می‌تواند به رفاه کودکان آسیب رساند، زیرا ممکن است از سوی مجرمان مورد سوءاستفاده قرار گیرند. همچنین چنین تصویرسازی‌هایی می‌تواند در درازمدت با تداخل در توانایی‌های کودکان برای خودشناسایی، ایجاد هویت و یافتن شغل به رفاه آنان آسیب رساند [۱]. استفاده والدین از کودکان در صنعت تبلیغات مصداقی از این موضوع است [۳۳، ۳۴]. برای کسب‌وکارها، کودکان می‌توانند اهداف مهمی به عنوان منابع داده باشند، زیرا آنها بر تصمیمات مصرف‌کننده دوستان و خانواده‌ها تأثیر می‌گذارند. تبلیغات «رفتاری»، هدف قرار دادن تبلیغات برخاسته برای رفتارهای خاص، و همچنین سایر تکنیک‌های تبلیغاتی، می‌تواند به تجاری‌سازی روبه‌رشد دوران کودکی کمک کند [۳۵]. اما فراتر از هدف قرار گرفتن به عنوان مصرف‌کننده، وقتی کسب‌وکارها به آنچه که دیگران از جمله کودکان به صورت برخاسته انجام می‌دهند علاقه‌مند می‌شوند، کودکان در معرض خطر بیشتری قرار می‌گیرند: کل دنیای خصوصی آنها ممکن است روی ماشین بازاریابی گشوده شود که نه تنها کارهای کودک را تماشا و ضبط می‌کنند، بلکه محیط اجتماعی برخاسته را به گونه‌ای بازسازی و دستکاری می‌کنند که بر احساس خود و امنیت کودک تأثیر می‌گذارد [۳۶]. از این رو کسب‌وکارها نباید به دنبال کسب درآمد از اطلاعات شخصی کودکان مانند تبلیغات هدفمند باشند. آنها باید دستورالعمل اخلاقی را ایجاد کنند و نظارت و حفاظت بیشتری را برای طیف کامل داده‌های مربوط به کودکان، از جمله اطلاعات مربوط به موقعیت مکانی و عادات جستجوی کودکان به‌ویژه در مورد اطلاعات شخصی آنها، اجرا کنند [۱].

کسب‌وکارها در طراحی پلتفرم‌ها و سایر ابزارهای کاربردی مورد استفاده برای کودکان باید حریم خصوصی آنان را به صورت پیش‌فرض در حداکثر میزان تنظیم کنند.

حداکثر حفاظت از حریم خصوصی باید به صورت پیش‌فرض برای ابزارها و پلتفرم‌های دیجیتالی که از سوی کودکان استفاده می‌شود وجود داشته باشد و حفظ حریم خصوصی باید از همان ابتدا در طراحی تمام فناوری‌های جدید گنجانده شود. علاوه بر این، رسانه‌های اجتماعی و سایر شرکت‌های پلتفرم باید شرایط و ضوابط و خط‌مشی‌های حفظ حریم خصوصی خود را به زبانی ساده بنویسند که



کودکان بتوانند آن را درک کنند و راه‌های آسانی برای گزارش نقض حریم خصوصی یا سایر نگرانی‌ها در اختیار آنها قرار دهند. از این تکنیک تحت عنوان «ساده‌سازی قواعد» یاد شده است. به عبارت دقیق‌تر، صفحات قوانینی که بسیاری از ارائه‌دهندگان خدمات برخط از کاربران می‌خواهند آن را امضا کنند، می‌توانند کودک‌پسند^۱ شوند و در نتیجه به ایجاد سواد دیجیتالی کودکان کمک کنند [۱].^۲ در راستای مسئولیت اجتماعی، کسب‌وکارها باید بسته‌های آموزش فناوری‌های ایمنی برخط را به زبان کودکان تهیه کنند و در اختیار آنان قرار دهند.

یکی از محدودیت‌ها یا شکاف‌های ابزارهای دیجیتالی در زمینه هشدارها برای محافظت از خود، رفتارهای ایمن در محیط دیجیتالی، تنظیم حریم خصوصی، گزارش مخاطرات و غیره این است که زبان آنها اکثراً به زبان‌های خارجی نظیر زبان انگلیسی است. شواهد در این زمینه بر نیاز فوری به آموزش فناوری‌های ایمنی برخط و نحوه استفاده از آنها به زبان مادری کودکان تأکید دارد. برخی از کشورها نظیر ژاپن در این زمینه پیش رو بوده‌اند. از این رو کسب‌وکارها و حتی نهادهای دیگر همچون مدارس و سازمان‌های مردم‌نهاد می‌توانند برای کودکان بسته‌های آموزشی در زمینه چگونگی تنظیم حریم خصوصی، رفتار ایمن در محیط برخط، نحوه گزارش مخاطرات و غیره آماده کنند و به شیوه‌های مختلف آن را در اختیار کودکان قرار دهند. لذا کسب‌وکارهای اینترنتی باید با شرکای خود کار کنند تا زیرساخت‌های محلی و محتوای محلی‌تری به‌ویژه محتوا برای کودکانی که به زبان‌های اقلیت صحبت و در مکان‌های دورافتاده زندگی می‌کنند، تدوین و توزیع کنند [۱].

۳-۲-۳. حمایت کیفری^۳

اشخاصی هستند که با استفاده از فناوری‌های دیجیتالی به دنبال سوءاستفاده و آسیب رساندن به کودکان هستند، لازم است با جرم‌انگاری اعمال آنها و تعیین مجازات مناسب، از کودکان در برابر این اعمال حمایت کرد. حمایت کیفری از متداول‌ترین اشکال حمایت از کودکان بزه‌دیده است که نیازمند ضمانت اجرایی مشخص نیز است. در سیاست کیفری، حمایت کیفری از کودکان در قالب جرم‌انگاری رفتارهای مضر علیه آنها به‌عمل آمده است. همان‌گونه که در بخش سوابق تقنینی مرور شد گرچه در لایه‌های قوانین موجود به‌صورت پراکنده به محافظت از کودکان در برابر مخاطرات محیط دیجیتالی پرداخته شده است اما هنوز برخلاف نظم حقوقی برخی از کشورهای دیگر، الگوی قانونی منسجمی برای تحقق حقوق کودکان در محیط دیجیتالی از جمله محافظت در برابر مخاطرات و آسیب‌ها در قوانین کشور دیده نمی‌شود. یکی از بخش‌های محافظت از کودکان در برابر این مخاطرات، حمایت کیفری است. البته چگونگی حمایت کیفری از کودکان و نوجوانان در برابر آسیب‌ها و جرائم ناشی از محیط دیجیتالی نیازمند بررسی‌های دقیق حقوقی است که باید در مطالعات آتی در دستور کار قرار گیرد. در این بخش به‌صورت خلاصه با توجه به راهبردهای مطالعات موجود، موارد زیر به‌صورت کلی پیشنهاد می‌شود:

- می‌بایست همه جرائم علیه کودکان که با استفاده از فناوری‌های دیجیتالی تسهیل یا توسط آنها انجام می‌شود احصا و تعریف جامعی از آنها ارائه شود.

اهم جرائم این حوزه عبارت‌اند از: سوءاستفاده جنسی و بهره‌کشی برخط از کودکان، اغفال برخط کودکان، اخاذی برخط جنسی، آزار جنسی برخط، سرقت هویت، انواع کلاهبرداری‌های اینترنتی، هک کردن، جعل هویت، قاچاق برخط کودکان، انتشار ویروس، ارسال تصاویر برهنه به‌ویژه اندام جنسی از طریق اینترنت (فلش سایبری)^۴، تولید و به اشتراک‌گذاری محتوای سوءاستفاده جنسی از کودکان، پخش مستقیم آزار جنسی، نقض حریم خصوصی و غیره.^۵ در بخش ضمیمه، برخی از این جرائم احصا و تعریف شده‌اند. گفتنی است جرائم علیه کودکان که با استفاده از ابزارهای محیط دیجیتالی تسهیل می‌شوند اغلب با سایر مقررات در مورد جرائم علیه

1. Child Friendly

۲. برای مثال وکیل حریم خصوصی به‌منظور ساده‌سازی قواعد، متن طولانی از یک ارائه‌دهنده خدمت دیجیتالی که شامل ۱۱۲ کلمه بود را به‌صورت زیر بازنویسی کرد: «از حساب هیچ‌کس دیگر بدون اجازه او استفاده نکنید و سعی نکنید جزئیات ورود به سیستم آنها را پیدا کنید».

۳. اهم مباحث این بخش از منابع زیر برگرفته شده است: [۸، ۱۶].

4. cyber flashing

۵. بسیاری از جرائم این حوزه را می‌توان تحت دو اصطلاح سوءاستفاده جنسی و بهره‌کشی آنلاین از کودکان صورت‌بندی کرد. این دو اصطلاح از عمومیت کافی برخوردار است و می‌توان بسیاری از جرائم را ذیل آنها طبقه‌بندی کرد.

کودکان مرتبط هستند. برای مثال در بسیاری از قوانین بهره‌کشی و سوءاستفاده جنسی از کودکان جرم‌انگاری شده است، از این رو باید بررسی شود که آیا آنها مصادیق جزئی‌تر به‌ویژه آنهایی که با فناوری‌های دیجیتال تسهیل می‌شوند را دربرمی‌گیرد یا خیر. البته لازم به یادآوری است مرز بین جرائم برخط و برون خط اغلب در عمل مبهم است [۳۷]. تأکید شده است هنگام تهیه پیش‌نویس قانون جرائم برخط علیه کودکان، مهم است که اطمینان حاصل شود که اصطلاحات «در صورت امکان به روشی بی‌طرفانه از نظر فناوری فرمول‌بندی شده و فضایی را برای ظهور فناوری‌های جدید باقی گذارند» [۳۸]. لذا با توجه به ماهیت دائماً در حال تحول فناوری دیجیتال و اعمال مجرمانه در این حوزه، به‌صورت دوره‌ای جرائم این حوزه به‌روزرسانی شود.

می‌بایست اطمینان حاصل شود که قانون شامل جرائم خاص مرتبط با سوءاستفاده جنسی برخط از کودکان است. در این زمینه می‌توان به جرائمی همچون تولید، تکثیر (بازتولید)، عرضه، معامله، توزیع، واردات، صادرات، بارگذاری محتوا، ذخیره، تعامل، دسترسی و در اختیار داشتن محتوای جنسی کودکان از جمله برای تبلیغات اشاره کرد.

براساس توصیه‌های کمیته کنوانسیون حقوق کودک در مورد مبارزه با محتوای سوءاستفاده جنسی از کودکان، قانون باید اعمال زیر را جرم‌انگاری کند، به‌ویژه در مواردی که چنین اعمالی به‌صورت برخط انجام می‌شوند یا با استفاده از فناوری‌های اطلاعات و ارتباطات تسهیل می‌شوند:

- تولید محتوای آزار جنسی کودکان؛
- ارائه محتوای سوءاستفاده جنسی از کودکان؛
- توزیع یا انتشار محتوای سوءاستفاده جنسی از کودکان؛
- واردات یا صادرات محتوای آزار جنسی کودکان؛
- تعامل با محتوای آزار جنسی کودکان به‌صورت برخط، برای مثال، با اظهارنظر روی عکس‌ها، اشتراک‌گذاری نظرات با استفاده از عملکردهای چت یا «نظرات / کامنت‌ها»، و تشویق‌ها یا راهنمایی‌ها از راه دور؛
- دسترسی به محتوای سوءاستفاده جنسی از کودکان،
- در اختیار داشتن محتوای سوءاستفاده جنسی از کودکان فارغ از اینکه دارنده آن قصد توزیع آن را داشته باشد، مشروط به استثنائات مربوط بر الزامات حرفه‌ای مشروع، مانند اجرای قانون برای اهداف تحقیق و تعقیب جرائم؛ و
- تولید یا انتشار محتوایی که سوءاستفاده جنسی یا بهره‌کشی از کودکان را تبلیغ می‌کند یا به دیگران اطلاع می‌دهد که در کجا می‌توانند محتوای سوءاستفاده جنسی از کودکان را پیدا کنند [۵].

اطمینان حاصل شود که رضایت مفروض کودک برای جرائمی همچون بهره‌کشی اقتصادی و سوءاستفاده جنسی باطل و بی‌اثر است. هرگونه مقرراتی که رضایت کودک برای معافیت‌ها، توجیهات، یا دفاعیات مبتنی بر رضایت کودک برای بهره‌کشی و سوءاستفاده جنسی، چه با فناوری اطلاعات تسهیل شده باشد یا خیر را مفروض می‌گیرند، باید از قانون حذف شود. البته در نظر گرفتن رشد کودک در این موضوع باید در نظر گرفته شود.

■ عملی که باعث می‌شود کودک، برای اهداف جنسی، شاهد سوءاستفاده جنسی یا فعالیت‌های جنسی از طریق فناوری‌های اطلاعاتی و ارتباطی باشد، باید جرم‌انگاری شود.

قرار گرفتن در معرض محتوای جنسی می‌تواند به‌صورت جدی به کودکان آسیب رساند، به‌خصوص اگر در سنین پایین در معرض آن قرار گیرند. همچنین مجرمان با نمایش محتوای جنسی برای کودک ممکن است از فناوری اطلاعات و ارتباطات به‌عنوان بخشی از فرایند اغفال برای حساسیت‌زدایی از او نسبت به رفتار جنسی و فریب کودک برای به اشتراک گذاشتن تصاویر جنسی از خود استفاده کنند. لذا چنین اعمالی نیز باید جرم‌انگاری شود [۳۹].

■ تلاش، همدستی و مشارکت به‌منظور ارتکاب جرم علیه کودکان در فضای دیجیتال می‌بایست جرم‌انگاری شود.

در برخی موارد ممکن است افراد دیگری با مجرمان اصلی برای جرائم علیه کودکان در محیط دیجیتال تلاش، همدستی و مشارکت کنند، از این رو باید اعمال این دسته از افراد نیز جرم‌انگاری شود. برای مثال زمانی که فردی مسئولیت حفاظت از داده‌های کودکان را



به‌عهده دارد، اگر به هر دلیلی از آنها سوءاستفاده کنند یا آنها را در اختیار اشخاص ثالث به‌منظور سوءاستفاده از کودکان قرار دهند نمونه‌ای از همدستی و مشارکت است.

■ معرفی صلاحیت قضایی جهانی برای مقابله با جرائم برخط علیه کودکان، صرف‌نظر از اینکه چنین جرائمی با استفاده از فناوری‌های اطلاعات و ارتباطات تسهیل می‌شود یا خیر، و حذف هرگونه الزام برای «مجرمیت متقابل»^۱ جهت پیگرد چنین جرایمی.

برخی از جرائم علیه کودکان ازجمله قاچاق، بهره‌کشی اقتصادی و سوءاستفاده جنسی اغلب ماهیت فراملی دارد و می‌تواند با حوزه‌های قضایی متعدد ارتباط داشته باشد. فناوری‌های دیجیتال به ابعاد جهانی این جرائم دامن زده و لازم است در سطح جهانی سازوکارهایی برای مقابله با آنها اندیشیده شود. موضوع صلاحیت جهانی به این موضوع اشاره دارد و مفهومی است که در آن دادگاه ملی می‌تواند فردی را برای ارتکاب جرم براساس اینکه جرم به نظم بین‌المللی آسیب می‌زند، تحت تعقیب قرار دهد. برای کمک به حل این مشکل، قوانین ملی باید شامل بندهای صلاحیت قضایی جامع باشند که صلاحیت فراسرزمینی را فراهم کنند [۸]. براساس بند «ت» ماده (۶۶۴) قانون آیین دادرسی کیفری (۱۳۹۵) دادگاه‌های ایران می‌توانند به «جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از اینکه بزه‌دیده یا مرتکب ایرانی یا غیرایرانی باشد و مرتکب در ایران یافت شود» رسیدگی کند. درواقع قانونگذار، جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال را موضوع اصل صلاحیت جهانی قرار داده است [۱۶]. احکام دیگر در این زمینه شامل موارد زیر است:

■ تشدید مجازات در مواردی که شخص بزرگسال جرمی علیه کودکی مرتکب می‌شود.

در زمینه حمایت از بزه‌دیدگان آسیب‌پذیر و پیشگیری از چنین بزه‌هایی، ضرورت‌ها و منافع فردی و اجتماعی ایجاب می‌کند که مجازات مرتکبان علیه اشخاص آسیب‌پذیر در مقایسه با سایر افراد سنگین‌تر و شدیدتر باشد. چارچوب‌های بین‌المللی از کشورها می‌خواهند تا اقدام‌هایی را اتخاذ کنند که اطمینان حاصل شود تا جرائمی که علیه کودکان صورت می‌گیرد، به‌منظور نشان دادن جدیت مقابله با آنها با مجازات شدیدتر روبه‌رو هستند [۱۶].

■ می‌بایست اطمینان حاصل شود که با کودکانی که متهم یا محکوم به جرم هستند، به‌ویژه جرائمی که علیه دیگر کودکان مرتکب شده‌اند، در یک نظام قضایی جداگانه مطابق با اصول و رویه‌های عدالت دوستدار کودک، به جرم آنها رسیدگی می‌شود.

در برخی از موارد کودکان ممکن است به‌دلیل کنجکاوی مرتکب تخلفاتی نظیر تولید محتوای جنسی، ارسال «پیام جنسی»^۲، اذیت و آزار دیگران، به اشتراک‌گذاری محتوای جنسی و غیره شوند. به‌دلیل اینکه کودکان در حال رشد هستند و ظرفیت‌های شناختی و اخلاقی آنها هنوز به‌خوبی شکل نگرفته است رفتار آنها ماهیتاً نمی‌تواند جرم‌انگاری شود [۳۹، ۴۰]. در عوض دولت‌ها باید:

■ چارچوب‌های قانونی صریحی ایجاد کنند که از کودکان محافظت کند و

■ از طریق تلاش‌های پیشگیرانه، اطمینان حاصل کنند که کودکان در مورد اهمیت انتشار محتوا چه از خودشان و چه از دیگران آموزش می‌بینند و از آن آگاه هستند.

بحث و قانونگذاری در زمینه چگونگی مواجهه به تخلفات کودکان پیچیده است و استانداردهای بین‌المللی و منطقه‌ای بیان داشته‌اند می‌بایست قوانین بین ظرفیت‌های در حال رشد کودک و محافظت از آنها تعادل ایجاد کنند. به‌عنوان قاعده کلی، کودکان نباید به‌دلیل تخلفات تحت پیگرد قانونی قرار گیرند. بااین‌حال، در شرایطی خاص مانند زمانی که کودک، کودک دیگری را وادار به تولید محتوای جنسی می‌کند یا بدون اجازه و به‌منظور سوءاستفاده، محتوای تولید شده توسط دیگران را به اشتراک می‌گذارد ممکن است پیگرد قانونی البته مطابق با استانداردهای مربوط به نظام عدالت کودکان مجاز باشد [۸].

براساس آنچه که گفته شد این اعمال کودکان نمی‌تواند مصداق جرم تلقی شود، بلکه با کودکان متهم یا محکوم به جرم باید در یک نظام قضایی جداگانه مختص آنها مطابق با اصول و رویه‌های عدالت دوستدار کودک رسیدگی شود. این تعهد براساس بند «۳» ماده (۴۰) کنوانسیون حقوق کودک است که کشورهای عضو را ملزم می‌کند تا به‌دنبال ترویج ایجاد قوانین، رویه‌ها، مراجع و نهادهایی باشند که حداقل سنی را تعیین کنند که کودکان پایین‌تر از آن سن را نتوان دارای قابلیت نقض قوانین کیفری محسوب کرد (معمولاً

1. Double Criminality
2. Sexting

حداقل سن مسئولیت کیفری نامیده می‌شود) و در صورت مقتضی و مطلوب بودن تدابیری برای برخورد با این کودکان بدون توسل به دادرسی قضایی اعمال شود. در ماده (۳۰۴) قانون آیین دادرسی کیفری (۱۳۹۵) نیز اشاره شده است که «کلیه جرائم اطفال و افراد کمتر از هجده سال تمام شمسی در دادگاه اطفال و نوجوانان رسیدگی می‌شود». بنابراین اهم اقدام‌هایی که می‌توان انجام داد عبارت‌اند از:

- ارائه تدابیری در قانون برای برخورد با کودکانی که مرتکب جرم شده‌اند بدون مراجعه به دادگاه‌های کیفری. برای مثال می‌توان از طریق نظام‌های حمایتی و دادگاه‌های اطفال و نوجوانان به جرائم این دسته از کودکان رسیدگی کرد.
- معرفی مجموعه‌ای از اقدام‌های جایگزین برای مجازات حبس جهت اطمینان از اینکه با کودکان به شیوه‌ای متناسب با رفاه، شرایط و جرم آنها رفتار می‌شود (اقدام‌های جایگزین).
- برای جرائم مربوط به بهره‌کشی و سوءاستفاده جنسی برخاسته از کودکان دیگر، انحراف یا اقدام‌های جایگزین ممکن است شامل درمان‌های متناسب با رشد باشد که در صورت امکان شامل والدین نیز می‌شود [۸، ۴۲].

۳-۲-۴. همکاری‌های منطقه‌ای و بین‌المللی

ماهیت جهانی و به‌هم‌پیوسته اینترنت به این معنا است که محافظت از کودکان وضعیتی نیست که کشورها به‌تنهایی بتوانند آن را محقق کنند. به عبارت دیگر آسیب‌های برخاسته به‌عنوان تهدیدی جهانی، نیازمند تمهیدات منطقه‌ای و جهانی برای پاسخ به آنها است. از سوی دیگر در مقیاس جهانی، رویکردهای متفاوت برای مقابله با چنین تهدیدهایی می‌تواند به یک مانع در برابر محافظت از کودکان بدل شود [۷]. به همین منظور تلاش‌های منطقه‌ای و بین‌المللی مانند پیمان‌نامه شورای اروپا در مورد حمایت از کودکان در برابر بهره‌کشی جنسی و سوءاستفاده جنسی^۱، ابتکار حفاظت از کودکان برخط^۲، اتحاد جهانی وی‌پراتکت^۳ و شبکه جهانی تنظیم‌کننده ایمنی برخط^۴ برای پاسخ به این مسئله شکل گرفته است. تأمل درباره چگونگی همکاری دولت با چنین ابتکارانی نیازمند مطالعات جداگانه و ارزیابی منافع و مزایای آن است. از این‌رو لازم است در مطالعات آتی به‌صورت مستقل به این موضوع پرداخته شود. در هر حال با تأسی از قوانین پیشین در موضوع‌های فراملی از جمله بند «و» ماده (۴) سند صیانت از کودکان و نوجوانان در فضای مجازی (۱۴۰۰) می‌توان پیشنهادی زیر را توصیه کرد:

ایجاد زمینه همکاری‌های متقابل منطقه‌ای و جهانی مرتبط با محیط دیجیتال در جهت:

- تعامل مؤثر و هم‌افزا با کشورها، سرویس‌دهندگان خارجی و نهادهای بین‌المللی به‌منظور رعایت استانداردها و معیارهای جمهوری اسلامی ایران،
- مواجهه فعال و خلاقانه برای استفاده از فرصت‌های محیط دیجیتال و مقابله با تهدیدهای آن،
- مشارکت فعال در تصمیم‌سازی‌ها، تصمیم‌گیری‌ها و اقدام‌های مربوط،
- همسویی و سازگاری قوانین در تنظیم محیط دیجیتال،
- برنامه‌ریزی برای حضور در مجامع جهانی مرتبط با حقوق کودکان در محیط دیجیتال،
- فراهم کردن زمینه اقدام مشترک برای محافظت از کودکان در برابر مخاطرات و آسیب‌های اجتماعی برخط،
- بهره‌برداری از تجارب، امکانات و ظرفیت‌های کشورهای دیگر و سازمان‌های بین‌المللی در زمینه توسعه فناوریهای ایمن، توسعه زیرساخت‌ها و مقابله با مجرمین،
- توسعه قواعد و ابزارهای ایمنی برخط.

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

کشورها برای پیوستن به این پیمان‌نامه نیازی به عضویت در شورای اروپا ندارند، زیرا تونس در سال ۲۰۱۹ به آن ملحق شد

2. Child Online Protection (COP)

3. WeProtect Global Alliance (WPGA)

یک نهاد بین‌المللی مستقل است که در سال ۲۰۱۶ تأسیس شد. هدف آن پایان دادن به سوءاستفاده جنسی از کودکان به‌صورت برخط است. اقدام‌های این نهاد برای دستیابی به این هدف شامل ارزیابی تهدیدات جهانی و چارچوب‌های واکنش ملی و جهانی، تقویت صدای کودکان و بازماندگان سوءاستفاده و حمایت از همکاری بین‌المللی است. اعضای مؤسسه شامل ۹۹ کشور، چندین سازمان بزرگ بین‌المللی، ۵۹ کسب‌وکار بخش خصوصی و ۷۷ سازمان جامعه مدنی است.

4. The Global Online Safety Regulators Network



۵-۲-۳. حمایت از قربانیان، توان‌بخشی، ادغام مجدد و جبران خسارت

آسیب‌های اجتماعی برخط تأثیرات نامطلوبی بر سلامت و رشد جسمی، روانی و اجتماعی کودکان دارد. ماهیت آسیب‌های اجتماعی به‌گونه‌ای است که می‌تواند عملکرد فرد را تحت تأثیر قرار دهد و آسیب‌های بعدی را به‌همراه داشته باشد. زمانی که عنصر دیجیتال به این آسیب‌ها افزوده می‌شود، می‌تواند اثر بیشتر یا متفاوتی ایجاد کند. برای مثال برخی از پیامدهای سوءاستفاده جنسی و بهره‌کشی برخط عبارت‌اند از اختلال در عملکرد تحصیلی، انزوا و رفتارهای خود آسیب‌رسان همچون مصرف مواد مخدر و در موارد حادث خودکشی [۴۳]. بنابراین اگر خدمات حمایتی مناسب، توان‌بخشی و ادغام مجدد برای قربانیان در دسترس باشد نه‌تنها می‌تواند از آسیب‌های بعدی جلوگیری کند بلکه زمینه توانمندسازی و ادغام مجدد قربانیان را فراهم می‌آورد. وجود نظام حمایت قوی و در دسترس همراه با کارشناسان متخصص، عنصری کلیدی در مقابله با پیامدهای کوتاه‌مدت و بلندمدت آسیب‌های ناشی از محیط دیجیتال و درمان و ادغام مجدد افراد آسیب‌دیده اجتماعی است. اهم حمایت‌های این حوزه، جدا از حمایت‌های کیفری عبارت‌اند از حمایت مالی، حمایت اجتماعی و حمایت بالینی و پزشکی [۱۶]. در زیر به عمده رهنمودها در زمینه این حمایت‌ها پرداخته شده است.

■ تقویت نظام‌های موجود خدمات توان‌بخشی و ادغام مجدد به‌گونه‌ای که به نیازهای ویژه کودکان قربانی آسیب‌های برخط کمک کند.

برخی از ویژگی‌های آسیب‌های ناشی از محیط دیجیتال نظیر وابستگی غیرمعارف، تولید محتوای جنسی خودساخته و انتشار و لذا از کنترل خارج شدن آن بعد از انتشار، اغفال و اخاذی جنسی مستلزم راهکارهای جدید برای تشخیص سوءاستفاده و توان‌بخشی افراد آسیب‌دیده ناشی از آنها است. از این‌رو قربانیان دارای **نیازهای منحصر به فردی** هستند که باید نظام‌های موجود (نظیر نظام مراقبت اجتماعی از دانش‌آموزان و اورژانس اجتماعی) به‌منظور رسیدگی به آنها تقویت شود. این نظام‌ها می‌توانند با تجهیز بسته‌های حمایتی، آموزشی و خدمات مددکاری اجتماعی، روان‌شناسی، روان‌پزشکی و پزشکی و ایجاد سامانه‌های الکترونیک برای ارجاع الکترونیکی بین‌بخشی تقویت شوند.

نقش خانواده‌ها در حمایت از قربانیان نیز حائز اهمیت است، اما در بسیاری از موارد آنها دانش، مهارت و منابع کافی برای حمایت ندارند. همان‌گونه که نشان داده شده کودکان به حاشیه رانده شده بیش از همه در معرض مخاطره هستند و این نشان می‌دهد خانواده‌های این دسته از کودکان به حمایت نیاز دارند [۴۴]. همچنین این خطر وجود دارد که عوامل خطری که در ابتدا کودک را آسیب‌پذیر می‌کردند، همچنان حضور داشته باشند. چنین عوامل خطری شامل (اما نه محدود به) ارتباط نزدیک آزارگر با کودک یا خانواده او، پویایی خانواده قربانی و وضعیت مالی قربانی است [۴۵]. از این‌رو تجهیز و تقویت نظام موجود و حمایت از خانواده‌ها، می‌تواند به ادغام مجدد قربانی کمک کند.

ارائه آموزش‌های تخصصی به نیروی انسانی در زمینه مراقبت روانی و اجتماعی از کودکان قربانی آسیب‌های برخط. داشتن نیروی کار متخصص به این معنا است که آنها می‌توانند حمایت مناسبی را برای کودکان قربانی در حین انجام تحقیقات، مراحل قانونی، روند بهبودی و ادغام مجدد ارائه دهند. باید به نیروی کار موجود آموزش‌های مناسب در مورد چگونگی شناسایی و رسیدگی به پرونده‌ها در محیط دیجیتال ارائه شود. آموزش نیروی کار در مورد آسیب‌های محیط دیجیتال برای کودکان و همچنین قوانین، خدمات و رویه‌های موجود برای مقابله، آنها را قادر می‌سازد تا با اطمینان و به شیوه‌ای آگاهانه به چنین مواردی رسیدگی کنند. قانونگذار و دولت باید اطمینان حاصل کنند کسانی که به پرونده‌های آسیب‌ها رسیدگی می‌کنند (همچون مددکاران اجتماعی، متخصصان سلامت، مجریان قانون، دادستان‌ها و متخصصان حوزه فناوری اطلاعات) آموزش‌های تخصصی دریافت می‌کنند تا بتوانند با چنین مواردی به شیوه‌ای مناسب برخورد کنند. دستورالعمل‌ها توصیه می‌کنند که این آموزش باید شامل موارد زیر باشد:

■ هنجارها، استانداردها و اصول مربوط به حقوق کودکان؛

■ اصول و وظایف اخلاقی محل کار آنها درخصوص جامعه هدف به‌صورت خاص و جامعه به‌صورت عام؛

■ علائم و نشانه‌هایی که نشان‌دهنده جرم علیه کودکان است؛

- مهارت‌ها و تکنیک‌های ارزیابی بحران، به‌ویژه برای ارجاع، با تأکید بر نیاز به محرمانه بودن؛
 - آثار و پیامدهای جرائم علیه کودکان از جمله تأثیرات منفی جسمی و روانی؛
 - تدابیر و فنون ویژه برای کمک به کودکان قربانی و شاهدان در روند عدالت؛
 - مسائل بین فرهنگی و مرتبط با سن، زبان، مذهب، اجتماع و جنسیت؛
 - مهارت‌های ارتباطی مناسب بزرگسال و کودک؛
 - مهارت‌های برخورد با کودکان قربانی و شاهدان به شیوه‌ای حساس، قابل درک، سازنده و اطمینان‌بخش و
 - روش‌های حفاظت و ارائه شواهد و پرسش از شاهدان کودک [۴۶].
- منابع مالی تضمین‌شده سالیانه برای تخصیص به خدمات حمایت از قربانیان باید تدارک دیده شود. برنامه‌ها و نظام‌هایی که از قربانیان آسیب‌های برخط پشتیبانی می‌کنند، به‌ویژه خدمات پشتیبانی تخصصی که به کودکان ارائه می‌شوند، به اعتبارات کافی و پایدار نیاز دارند. بودجه تضمین‌شده؛ اجرای مداوم و پایدار برنامه‌ها و خدمات را تضمین می‌کند و ارائه‌دهندگان خدمات را قادر می‌سازد تا کارکنان حرفه‌ای را تربیت و حفظ کنند. ایجاد خطوط کمکی که اطلاعات و ارجاعات را به ارائه‌دهندگان خدمات مربوطه ارائه می‌دهند. خطوط کمکی سازوکار مفیدی برای ارائه اطلاعات یا ارجاع به ارائه‌دهنده خدمات بوده و لذا ضروری هستند. دو خط در این زمینه پیشنهاد شده است:
- الف) خط کمکی^۱:** این خط معمولاً بر ارائه خدمات پشتیبانی عمومی و ادغام مجدد، از جمله ارجاع به سرپناه‌ها، خدمات توان‌بخشی، مشاوره، پزشکی، حقوقی و اجتماعی تمرکز دارد. این خط باید برای همه اعضای جامعه در دسترس و خدمات آن رایگان باشد. با تقویت خطوط ۱۵۷۰ و ۱۲۳ می‌توان خدمات این خط را در آنها ادغام کرد.
- ب) خط تماس ویژه^۲:** این خط برای دریافت گزارش‌های مربوط به جرائم برخط علیه کودکان و حذف محتوای سوءاستفاده و بهره‌کشی از کودکان از اینترنت است. این خط باید ویژگی‌هایی داشته باشد که اهم آنها عبارت‌اند از:
- محرمانه و ناشناس بودن؛
 - دسترسی رایگان؛
 - قابل دسترسی در بیست‌وچهار ساعت در روز و هفت روز در هفته؛
 - علاوه بر تلفن از طریق وسایل دیگری مانند پیام‌های متنی، خدمات چت اینترنتی / پیام‌های اینترنتی، ایمیل و جلسات حضوری در دسترس باشد و
 - مشارکت بخش‌های مرتبط مانند امکانات آموزشی، بیمارستان‌ها، خدمات حمایتی، توان‌بخشی و سایر خدمات مرتبط با کودکان را به‌همراه داشته باشد.
- درنهایت ضروری است که کارکنان خطوط کمکی آموزش ببینند تا توانایی مقابله با مسائل مربوط به محیط دیجیتال و همچنین توانایی ارائه خدمات به شیوه‌ای حساس به کودکان را داشته باشند [۸].
- در نظر گرفتن ایجاد رویه‌های روشن برای حذف سریع محتوای سوءاستفاده جنسی از کودکان. حذف محتوای آسیب‌زا و غیرقانونی شکل مناسبی از جبران خسارت است. بنابراین، فراهم‌کنندگان خدمات اینترنتی باید رویه‌های قوی برای اطمینان از حذف به‌موقع محتوای آسیب‌رسان از کودکان به‌ویژه محتوای مرتبط با سوءاستفاده جنسی را ایجاد کنند. در بخش مسئولیت کسب‌وکارها مفصل‌تر به این موضوع پرداخته شد.
- لازم است سازوکارهای مختلفی برای جبران آسیب یا ضرر به کودکان قربانی فراهم و ارائه شود.
- در هر حوزه قضایی کودکان قربانی آسیب‌های برخط باید بدون تبعیض به فرایندهای جبران آسیب یا ضرر دسترسی داشته باشند.



تضمین دسترسی به این فرایندها به عهده دولت‌ها است. جبران می‌تواند به صورت استرداد، مجازات خاطی یا شخصی که علیه کودکان مرتکب جرم شده است، پرداخت مابه‌ازای ضرر و زیان، عذرخواهی و جلب رضایت، اصلاح یا حذف محتوای آسیب‌زا و غیرقانونی و دسترسی به خدمات بازتوانی روان‌شناختی یا اقدام‌های دیگر باشد [۴۳، ۴۱].

توافقی‌های خارج از دادگاه و روندهای قضایی یا به صورت «مصالحه» ممکن است در مواردی جذاب باشد، اما نباید تشویق شود. در این فرایند، مجرمان برای اجتناب از پیگرد قانونی، مبالغی را به کودک قربانی و خانواده او پرداخت می‌کنند. این موضوع می‌تواند برای کودکان و خانواده‌های فقیر جذاب باشد، اما چنین توافقی‌هایی به دلایل مختلف از جمله حمایت از قربانی و قربانیان احتمالی آینده باید منع شود. همچنین استفاده از نظام قضایی برای دریافت غرامت از سوی کودکان نباید طولانی، پیچیده، پرهزینه و همراه با آسیب‌های بالقوه بعدی باشد. این موارد باعث می‌شود کودک قربانی و خانواده او از تلاش برای دریافت غرامت اجتناب کند و انگیزه مجرمان برای تکرار جرم را تقویت کند.

۶-۲-۳. تنظیم‌گری و نظارت مستقل

همان‌گونه که مرور شد محافظت از کودکان در برابر آسیب‌های محیط دیجیتال موضوعی بین‌بخشی است که ذی‌نفعان مختلف درگیر آن هستند. به منظور ارتقای اثربخشی سیاست‌ها و برنامه‌ها لازم است یک نهاد تنظیم‌گر و ناظر مستقل، اقدام‌های این حوزه را همسو و بر روند اجرای موارد نام‌برده نظارت کند. همچنین نظارت مستقل بر حقوق کودکان در محیط دیجیتال، بخش مهمی از محافظت از کودکان در برابر آسیب‌های برخط است. تنظیم‌گری و نظارت مستقل بر حقوق کودکان در محیط دیجیتال از طریق نهاد ملی مرتبط با حقوق کودکان امکان‌پذیر است. از نظر ساختار نهادی، کمیته پیمان‌نامه حقوق کودک توصیه می‌کند **نهاد مسئول حقوق کودکان** مسئولیت این حوزه را به عهده داشته باشد. دلیل این امر، محدودیت منابع است، تا اطمینان حاصل شود که منابع موجود به بهترین نحو برای حمایت از حقوق کودکان از جمله محافظت در برابر مخاطرات برخط استفاده می‌شود [۲۲]. تعدد نهادهای متولی در این زمینه باعث موازی‌کاری، اثربخشی پایین برنامه‌ها و اقدام‌ها و هدر رفت منابع می‌شود. لذا بهره‌گیری از نهادهای حامی حقوق کودکان به عنوان نهاد تنظیم‌گر و ناظر، می‌تواند یک گزینه در این زمینه باشد. برخی از فعالیت‌های این نهاد در محیط دیجیتال شامل موارد زیر است:

- تدوین طرح‌ها و برنامه‌های ارتقای حقوق کودک در محیط دیجیتال با همکاری همه ذی‌نفعان؛
- ارائه نظرهای مشورتی در زمینه قوانین، مقررات، رویه‌ها و برنامه‌های مرتبط با حقوق کودک در محیط دیجیتال به همه ذی‌نفعان به‌ویژه به دستگاه‌های اجرایی و کسب‌وکارهای این حوزه؛
- تقسیم کار ملی و ایجاد هماهنگی و هم‌افزایی در زمینه مراقبت از کودکان در محیط دیجیتال در همه ابعاد اعم از فنی، حمایتی، آگاهی‌بخشی، علمی، محتوایی، کیفری و غیره و همچنین نظارت و کنترل مستمر بر عملکرد دستگاه‌ها در این زمینه؛
- نظارت بر کسب‌وکارها به منظور تحقق حقوق کودکان و جلوگیری از آسیب به کودکان در محیط دیجیتال با اقدام‌های نظارتی شفاف و سازنده؛
- همگام شدن با تغییرات عرصه فناوری‌های دیجیتال و تأثیر آن بر کودکان و اطمینان از اینکه سیاست‌ها و قوانین برای دستیابی به این هدف مناسب هستند و بر چالش‌های اجرایی غلبه می‌کنند؛
- پایش و ارزیابی تحقق حقوق کودکان در محیط دیجیتال؛
- برخورداری از قدرت دریافت، بررسی و رسیدگی به شکایات کودکان و نمایندگان آنها؛
- انجام تحقیقات در مورد نقض حقوق کودکان در محیط دیجیتال، پاسخ به شکایات فردی یا به ابتکار خود؛
- تهیه و انتشار نظرها، توصیه‌ها و گزارش‌ها، به درخواست مقامات ملی یا به ابتکار خود، در مورد مسائل مربوط به حمایت از حقوق کودکان در محیط دیجیتال؛
- نظارت بر کفایت و اثربخشی قوانین و رویه‌های مربوط به حقوق کودکان در محیط دیجیتال؛
- طراحی، سامان‌دهی و نظام‌مندسازی پالایش محتوای محیط دیجیتال برای کودکان و نظارت بر آن؛
- نیازسنجی و تعیین اولویت‌های فناوری‌های ایمن دیجیتال کودکان و همچنین زمینه‌سازی برای گسترش نوآوری‌های علمی و فناوری در این عرصه؛

■ تهیه گزارش‌های دوره‌ای ملی روند مخاطرات و آسیب‌های اجتماعی محیط دیجیتال برای کودکان و اقدام‌های انجام شده برای محافظت از کودکان. بر این مبنا توصیه زیر را در این زمینه می‌توان پیشنهاد کرد:

تعیین نهاد تنظیم‌گر و ناظر مستقل از میان نهادهای موجود با تأکید بر نهادهای حامی حقوق کودکان برای حفظ و ارتقای ایمنی برخط، از جمله محافظت از کودکان در برابر مخاطرات و آسیب‌های اجتماعی برخط.

با مروری در قوانین و اسناد بالادستی نهادهایی همچون دفتر حمایت از اطفال و نوجوانان قوه قضائیه، مرجع ملی کنوانسیون حقوق کودک (وزارت دادگستری) و شورای عالی فضای مجازی می‌توانند تنظیم‌گری و نظارت بر حقوق کودکان در محیط دیجیتال را به‌عهده گیرند. در ماده (۴) [قانون حمایت از اطفال و نوجوانان \(۱۳۹۹\)](#) «تشکیل دفتر حمایت از اطفال و نوجوانان قوه قضائیه به‌منظور ایجاد زمینه‌های همکاری با سایر نهادها، تهیه گزارش‌های موردی یا ادواری، انجام مطالعات و تحقیقات آماری و اطلاعاتی، پایش و ارزشیابی فعالیت‌ها» درخصوص اجرای قانون پیشنهاد شده است. در حال حاضر این دفتر در قوه قضائیه تشکیل شده است. همچنین در [آیین‌نامه مرجع ملی کنوانسیون حقوق کودک در جمهوری اسلامی ایران \(۱۳۹۱\)](#) وزارت دادگستری به‌عنوان مرجع ملی حقوق کودک معرفی شده است. با توجه به وظایفی که در ماده (۲) آیین‌نامه برای این مرجع در نظر گرفته شده است، این نهاد نیز می‌تواند گزینه مناسبی برای تنظیم‌گری و نظارت بر حقوق کودکان در محیط دیجیتال باشد. در آیین‌نامه اشاره شده است که «مرجع ملی حقوق کودک به‌عنوان نهادی سیاستگذار، هماهنگ‌کننده و ناظر به‌دنبال سامان‌بخشی به مسائل مختلف مربوط به کودکان در کشور می‌باشد» [۴۷].

همچنین نهادهای نظارتی مستقل حوزه محیط دیجیتال نظیر شورای عالی فضای مجازی و دبیرخانه این شورا هم می‌توانند تنظیم‌گر و ناظر این بخش باشند. برای مثال در بند «ت» ماده (۶۵) [قانون برنامه پنج‌ساله هفتم پیشرفت جمهوری اسلامی ایران \(۱۴۰۳\)](#) حکم شده است «شورای عالی فضای مجازی، مرجع سیاستگذاری، تصمیم‌گیری و هماهنگی در موضوعات مربوط به فضای مجازی است و حسب مورد مصوبات آن برای کلیه دستگاه‌های اجرایی لازم اجرا است». در ماده (۴) [سند صیانت از کودکان و نوجوانان در فضای مجازی \(۱۴۰۰\)](#) نیز «مدیریت کلان، راهبری و تدوین الگوی عملیاتی و مقررات عمومی صیانت از خردسالان، کودکان و نوجوانان در فضای مجازی» به کمیته‌ای زیر مجموعه مرکز ملی فضای مجازی سپرده شده است. در صورت تعیین این نهاد به‌عنوان تنظیم‌گر و ناظر، باید اطمینان حاصل شود که دستورات نهاد ملی حقوق کودکان و سایر نهادهای مستقل حمایت از حقوق کودکان ازسوی این تنظیم‌گر حوزه دیجیتال به‌کار گرفته شود و با این نهادها همکاری کامل را داشته باشد [۲۲].

۴. جمع‌بندی و پیشنهادها

دیجیتالی شدن جامعه در نتیجه گسترش فناوری‌های اطلاعات و ارتباطات به‌صورت هم‌زمان فرصت‌ها و مخاطراتی را به‌همراه داشته است. یکی از گروه‌های متأثر از این فرایند، کودکان و نوجوانان هستند. به‌دلیل ویژگی‌های خاص این دوره از زندگی، آنان ممکن است بیشتر تحت تأثیر مخاطرات باشند و احتمال آسیب‌دیدگی‌شان بیشتر است. مرور شواهد نشان داد خطرات و آسیب‌های این حوزه برای کودکان واقعی و جدی است و در چارچوب محتوا-تماس-رفتار-قرارداد قابل دسته‌بندی است.

به‌رغم آسیب‌های این حوزه، سیاست‌های دیجیتال ملی کنونی به‌اندازه کافی موضوعات کودکان از جمله محافظت از آنها در برابر خطرات و آسیب‌ها را در نظر نمی‌گیرند. بررسی قوانین و مقررات مصوب نشان می‌دهد دو دسته قوانین برای محافظت از آنان در برابر خطرات محیط دیجیتال وجود دارد. دسته نخست، قوانینی است که آحاد جامعه، بدون توجه به قشر خاصی از جمله کودکان را دربرمی‌گیرد. دسته دوم نیز، قوانینی است که به‌صورت ویژه به محافظت از کودکان در برابر آسیب‌های ناشی از محیط دیجیتال پرداخته است. درمجموع، گرچه در لایه‌لای قوانین برخی از مواد به محافظت از کودکان در برابر خطرات و آسیب‌های ناشی از محیط دیجیتال پرداخته، اما هنوز فاقد قانونی جامع در این زمینه است. قوانین موجود به همه ابعاد این موضوع از جمله پیشگیری، حمایت از قربانیان و جبران خسارت، جرم‌انگاری و تنظیم‌گری بین بخش‌های مختلف نپرداخته است.

به‌منظور محافظت از کودکان در برابر خطرات و آسیب‌های این حوزه به اصلاح و تقویت قوانین موجود یا تدوین قانونی جدید نیازمند است که به همه ابعاد این موضوع بپردازد. تجربه برخی از کشورهای دیگر نشان می‌دهد آنان چارچوب‌های حقوقی‌شان را متناسب با وضعیت جدید به‌روز و قوانین جدیدی را در این حوزه تدوین و تصویب کرده‌اند. در این گزارش نیز تلاش شد با مرور تجارب این حوزه، بسته‌ای سیاستی به‌منظور بهبود چارچوب‌های قانونی در این زمینه ارائه شود. این بسته شامل ابعاد پیشگیری، مسئولیت کسب‌وکارها، حمایت کیفری، حمایت از قربانیان، توان‌بخشی، ادغام مجدد و جبران خسارت، همکاری‌های منطقه‌ای و بین‌المللی و تنظیم‌گری و نظارت مستقل بود. ابعاد و مؤلفه‌های بسته سیاستی محافظت از کودکان و نوجوانان در برابر آسیب‌های محیط دیجیتال در جدول زیر ارائه شده است.

جدول ۴. ابعاد و مؤلفه‌های بسته سیاستی محافظت از کودکان در برابر آسیب‌های محیط دیجیتال

پیشگیری:

- احراز هویت و سن کاربران،
- ایجاد دسترسی متناسب با سن،
- ایجاد و تقویت ابزارهای کنترل والدین،
- راه‌اندازی کمپین‌ها، ارائه آموزش‌های همگانی، آموزش مهارت‌ها و سواد رسانه‌ای،
- شناسایی گروه‌ها و افراد در معرض خطر با ابزارهای مناسب و طراحی بسته‌های حمایتی و مداخلاتی مناسب برای کاهش خطرپذیری آنها،
- رتبه‌بندی و طبقه‌بندی محتوا، ارتباطات و اطلاعات برحسب سن، جنسیت و سایر ویژگی‌های فرهنگی و اجتماعی برای کودکان،
- حذف و مسدود کردن محتوای غیرقانونی یا نامتناسب با سن و مرحله رشد کودکان.
- وزارت آموزش و پرورش نیز می‌تواند به تناسب مقطع تحصیلی و جنسیت دانش‌آموزان آموزش‌های سواد رسانه‌ای را در محتوای کتاب‌های درسی بگنجاند و مقررات خاصی را برای استفاده از فضای دیجیتال در مدرسه تنظیم کند.

مسئولیت کسب‌وکارها:

- تلاش برای دسترسی آزاد جامعه به‌ویژه خانواده‌ها و کودکان در مناطق محروم و به حاشیه رانده شده به فناوری‌ها و خدمات دیجیتال،
- ادغام ملاحظات حقوق کودک در تمام سیاست‌ها و فرایندها،
- اتخاذ سازوکارهای تضمین سن برای جلوگیری از دسترسی یا قرار گرفتن کودکان در معرض هرزه‌نگاری و سایر محتوای جنسی غیرقانونی یا نامناسب،
- ایجاد رویه‌های اطلاع و حذف، از جمله الزام به مسدود کردن یا حذف محتوای سوءاستفاده جنسی از کودکان،
- شناسایی فعالانه محتوای سوءاستفاده جنسی از کودکان در محصولات یا خدمات در دسترس آنها به‌منظور مسدود کردن یا حذف چنین محتوای مشروط به حفظ حریم خصوصی کودکان،
- گزارش محتوای برخاسته از سوءاستفاده جنسی از کودکان به مجری قانون یا سایر نهادهای تعیین شده در قانون،
- حفظ حریم خصوصی کودکان به‌صورت پیش‌فرض در حداکثر میزان در طراحی پلتفرم‌ها و سایر ابزارهای کاربردی مورد استفاده برای کودکان،
- تهیه بسته‌های آموزش فناوری‌های ایمنی برخط به زبان کودکان،
- جرم‌انگاری و تعیین مجازات برای اشخاص حقوقی یا کسب‌وکارهایی که علیه کودکان در محیط دیجیتال مرتکب جرم می‌شوند و تعهداتشان را برای محافظت از کودکان در برابر چنین آسیب‌هایی نقض می‌کنند و
- منع و جرم‌انگاری پدازش داده‌های کودکان توسط کسب‌وکارها برای مقاصد اقتصادی به‌ویژه در مواردی که می‌تواند به آنها آسیب رساند.

حمایت کیفری:

- احصای همه جرائم علیه کودکان که با استفاده از فناوری‌های دیجیتال تسهیل یا توسط آنها انجام می‌شود و ارائه تعریفی جامع از آنها،
- باید اطمینان حاصل شود که قانون شامل جرائم خاص مرتبط با سوءاستفاده جنسی برخط از کودکان است. در این زمینه می‌توان به جرائمی همچون تولید، تکثیر (بازتولید)، عرضه، معامله، توزیع، واردات، صادرات، بارگذاری محتوا، ذخیره، تعامل، دسترسی و در اختیار داشتن محتوای جنسی کودکان از جمله برای تبلیغات اشاره کرد،
- باطل و بی‌اثر بودن رضایت مفروض کودک برای جرائمی همچون بهره‌کشی اقتصادی و سوءاستفاده جنسی،
- جرم‌انگاری عملی که باعث می‌شود کودک، برای اهداف جنسی، شاهد سوءاستفاده جنسی یا فعالیت‌های جنسی از طریق فناوری‌های اطلاعاتی و ارتباطی باشد،
- جرم‌انگاری تلاش، همدستی و مشارکت به‌منظور ارتکاب جرم علیه کودکان در فضای دیجیتال،
- معرفی صلاحیت قضایی جهانی برای مقابله با جرائم برخط علیه کودکان،
- تشدید مجازات در مواردی که شخص بزرگسال جرمی علیه کودکی مرتکب می‌شود،
- رسیدگی به کودکان متهم یا محکوم به جرم در یک نظام قضایی جداگانه مطابق با اصول و رویه‌های عدالت دوستدار کودک.

حمایت از قربانیان، توان‌بخشی، ادغام مجدد و جبران خسارت:

- تقویت نظام‌های موجود خدمات توان‌بخشی و ادغام مجدد به‌گونه‌ای که به نیازهای ویژه کودکان قربانی آسیب‌های برخط کمک کند،
- ارائه آموزش‌های تخصصی به نیروی انسانی در زمینه مراقبت روانی و اجتماعی از کودکان قربانی آسیب‌های برخط،
- تدارک منابع مالی تضمین شده سالیانه برای تخصیص به خدمات حمایت از قربانیان،
- ایجاد خطوط کمکی (خط کمکی و خط تماس ویژه) که اطلاعات و ارجاعات را به ارائه‌دهندگان خدمات مربوطه ارائه می‌دهند،
- ایجاد رویه‌های روشن برای حذف سریع محتوای سوءاستفاده جنسی از کودکان و
- در نظر گرفتن سازوکارهای مختلفی برای جبران آسیب / غرامت به کودکان قربانی.

همکاری‌های منطقه‌ای و بین‌المللی:

- تعامل مؤثر و هم‌افزا با سایر کشورها، سرویس‌دهندگان خارجی و نهادهای بین‌المللی به‌منظور رعایت استانداردها و معیارهای جمهوری اسلامی ایران،
- مواجهه فعال و خلاقانه برای استفاده از فرصت‌های محیط دیجیتال و مقابله با تهدیدهای آن،
- مشارکت فعال در تصمیم‌سازی‌ها، تصمیم‌گیری‌ها و اقدام‌های مربوط، همسویی و سازگاری قوانین،
- برنامه‌ریزی برای حضور در مجامع جهانی مرتبط با حقوق کودکان در محیط دیجیتال،
- فراهم کردن زمینه اقدام مشترک برای محافظت از کودکان در برابر مخاطرات و آسیب‌های برخط،
- بهره‌برداری از تجارب، امکانات و ظرفیت‌های کشورهای دیگر و سازمان‌های بین‌المللی در زمینه توسعه فناوری‌های ایمن، توسعه زیرساخت‌ها و مقابله با مجرمان و
- توسعه قواعد و ابزارهای ایمنی برخط.

تنظیم‌گری و نظارت مستقل:

- تعیین نهاد تنظیم‌گر و ناظر مستقل از میان نهادهای موجود با تأکید بر نهادهای حامی حقوق کودکان برای حفظ و ارتقای ایمنی برخط، از جمله محافظت از کودکان در برابر مخاطرات و آسیب‌های اجتماعی برخط.

مأخذ: یافته‌های پژوهش

با توجه به آنچه که مرور شد اتخاذ هرگونه رویکرد در این عرصه باید بین محافظت از کودکان به‌صورت برخط و احترام به حقوق و فرصت‌های آنان با توجه به دوره رشد تعادل ایجاد کند. همچنین سیاست‌گذاری دیجیتالی کودکان و نوجوانان موضوعی چندبخشی است و باید ابعاد دیگر آن از جمله فراهم کردن دسترسی مقرون‌به‌صرفه به منابع برخط با کیفیت، محافظت از حریم خصوصی کودکان، آموزش مهارت‌های دیجیتالی و غیره را نیز دربرگیرد. روی‌هم‌رفته سیاست‌گذاری دیجیتالی کودکان و نوجوانان حوزه‌ای نوپا است و کمتر به آن توجه شده است و سیاست‌های موجود هم عمده‌تاً با در نظر گرفتن کاربران بزرگسال تنظیم شده است. بنابراین باید بیشتر درباره این موضوع تأمل شود و مطالعات بیشتری در این زمینه با تأکید بر تجربه کودکان و نوجوانان، مخاطرات و آسیب‌های این حوزه با توجه به تحولات فناوری‌های دیجیتال و ابعاد سیاست‌گذاری دیجیتالی انجام شود.

۵. پیوست



در این بخش برخی از اصطلاحات درباره محیط دیجیتال و آسیب‌های ناشی از آنها مرور و تعریف شده است. البته گفتنی است دامنه این اصطلاحات بسیار وسیع‌تر از موارد نام‌برده است، اما به مهم‌ترین آنها (که با موضوع این گزارش مرتبط است) پرداخته شده است.

جدول ۱ پیوست، جدول اصطلاحات و تعاریف آنها [۳۷، ۲۲، ۸]

اصطلاح	تعریف
ارائه‌دهندگان خدمات اینترنت	سازمانی که خدمات دسترسی و استفاده از اینترنت را ارائه می‌دهد. ارائه‌دهنده‌ها ممکن است خدمات دیگری مانند خدمات ایمیل، ثبت دامنه، میزبانی وب، خدمات مرورگر و بسته‌های نرم‌افزاری را نیز ارائه دهند.
ارزیابی اثرات حقوق کودک ^۱	ابزاری است برای پیش‌بینی تأثیر هر نوع قانون، فناوری، سیاست یا تخصیص اعتبار پیشنهادی که بر کودکان و برخورداری آنان از حقوق‌شان تأثیر می‌گذارد.
استرداد	به فرایند رسمی اشاره دارد که طی آن یک دولت از دولت دیگر (دولتی که از او درخواست شده است) درخواست استرداد یک فرد متهم یا محکوم به جرم را برای محاکمه یا اجرای حکم در کشور درخواست‌کننده می‌کند.

اصطلاح	تعریف
اطلاع و حذف (برداشتن)	رویه کسب‌وکارها برای دریافت گزارش‌هایی که ممکن است از سوی مشتریان، کارمندان، مجریان قانون یا خطوط تماس مبنی بر کشف محتوای سوءاستفاده جنسی از کودکان در شبکه‌ها یا خدمات کسب‌وکار و برای جلوگیری از دسترسی و توزیع بیشتر ارسال شود.
اخاذی جنسی	عبارت است از اخاذی از یک شخص با کمک تصاویر ساخته‌شده به منظور مساعدت جنسی، پول یا سایر منافع با تهدید به اشتراک‌گذاری مطالب فراتر از رضایت شخص تصویر شده.
اغفال (برون‌خط / برخط) برای مقاصد جنسی	«اغفال / اغفال برخط» که به آن «درخواست از کودکان برای مقاصد جنسی» نیز گفته می‌شود، فرایند برقراری ارتباط با کودک به‌صورت حضوری یا از طریق استفاده از فناوری اطلاعات و ارتباطات برای تسهیل تماس جنسی برخط یا برون‌خط است. اغفال برخط شامل چهار عنصر به این شرح است: الف) ارتباط با کودک، ب) از طریق استفاده از فناوری اطلاعات و ارتباطات، ج) با قصد فریب یا تحریک کودک و د) برای درگیر کردن کودک در هر نوع فعالیت جنسی.
ایمنی به‌واسطه طراحی ^۱	عمل طراحی خدمات برخط با هدف اطمینان از ایمنی کاربران تا حد امکان. در این زمینه می‌توان به طراحی تنظیمات ایمن پیش‌فرض برای حساب کاربران زیر سن قانونی یا برای جلوگیری از تماس بزرگسالان با کاربران زیر سن قانونی اشاره کرد.
بازبینی محتوا ^۲	عمل نظارت و بازبینی محتوای تولید شده توسط کاربر براساس قوانین از پیش تعیین شده برای حذف محتوای غیرمجاز، چه به‌صورت خودکار یا با استفاده از ناظران انسانی.
بهره‌کشی جنسی از کودکان	شامل هر نوع سوءاستفاده واقعی یا تلاش ناشی از موقعیت آسیب‌پذیری، قدرت متمایز یا اعتماد، از جمله، اما نه محدود به سود مالی، اجتماعی و سیاسی ناشی از بهره‌کشی جنسی از دیگری است. آنچه بهره‌کشی جنسی از کودک را از سوءاستفاده جنسی متمایز می‌کند، مفهوم اساسی مبادله در بهره‌کشی است. همچنین لازم به گفتن است که هم‌پوشانی قابل‌توجهی بین این دو مفهوم وجود دارد، زیرا بهره‌کشی اغلب یکی از ویژگی‌های سوءاستفاده است و برعکس.
بهره‌کشی و سوءاستفاده جنسی از کودکان به‌صورت برخط	شامل تمام اعمال با ماهیت بهره‌کشی جنسی است که علیه کودک انجام می‌شود و در مرحله‌ای با محیط برخط ارتباط دارد، یا شامل هرگونه استفاده از فناوری اطلاعات و ارتباطات است که باعث بهره‌کشی جنسی از کودک یا به تولید، خرید، فروش، تملک، توزیع یا انتقال تصاویر یا سایر مطالب مستندکننده چنین بهره‌کشی جنسی منجر شود. بنابراین، این مفهوم می‌تواند شامل موارد زیر شود (اما لزوماً محدود به آنها نیست): ۱) بهره‌کشی جنسی در زمانی که قربانی برخط است (مانند اغواکردن / بازی‌دادن / تهدید کودک برای انجام اعمال جنسی در مقابل وب کم)، ۲) شناسایی و / یا اغفال کودکان قربانی بالقوه به‌صورت برخط با هدف بهره‌کشی جنسی از او (اعم از اینکه اعمال بعدی به‌صورت برخط یا برون‌خط انجام شوند)، ۳) توزیع، انتشار، واردات، صادرات، عرضه، فروش، در اختیار داشتن یا دسترسی آگاهانه به محتوای بهره‌کشی جنسی کودکان به‌صورت برخط (حتی اگر محتوا سوءاستفاده جنسی به‌صورت برون‌خط تهیه شده باشد).
پیام جنسی ^۴	محتوای جنسی خود تولید شده که از طریق پیام‌های متنی تلفن همراه یا سایر پیام‌های برخط برای دیگران ارسال می‌شود.
حریم خصوصی به‌واسطه طراحی ^۵	طراحی خدمات برخط با هدف حفظ حریم خصوصی کاربران تا حد امکان، به‌عنوان مثال با تنظیم حساب‌های کاربران زیر سن قانونی به‌صورت پیش‌فرض فرض خصوصی، جلوگیری از تماس بزرگسالان با کاربران زیر سن قانونی به‌صورت پیش‌فرض و به حداقل رساندن حجم داده‌های جمع‌آوری‌شده.
خطوط تلفن کمکی	خطوط کمکی که مشاوره مجرمانه را برای تماس‌گیرندگان فراهم می‌کند، و اغلب به‌عنوان نقاط ارجاع به سایر ارائه‌دهندگان خدمات عمل می‌کند.
دیجیتالی شدن ^۶	سازگاری محیط‌ها، شیوه‌ها، کسب‌وکارها و زندگی روزمره برای ادغام و بهره‌مندی از خدمات و زیرساخت‌های دیجیتال. همچنین به تبدیل اطلاعات به فرمت دیجیتال نیز اشاره دارد.
زیست‌بوم فناوری اطلاعات و ارتباطات	سیاست‌ها، راهبردها، فرایندها، اطلاعات، فناوری‌ها، برنامه‌های کاربردی و ذی‌نفعان که با هم یک محیط فناوری را برای یک کشور، دولت یا کسب و کار تشکیل می‌دهند.
سایبر فلشینگ ^۷	ارسال ناخواسته تصاویر یا فیلم از اندام تناسلی با استفاده از فناوری‌های دیجیتال.
سایت گزارش	صفحه وب سفارشی که در آن افراد می‌توانند محتوای مشکوک به سوءاستفاده جنسی از کودکان را گزارش کنند.
سوءاستفاده جنسی از کودک	درگیرکردن کودک در فعالیت‌های جنسی که به‌طور کامل آن را درک نمی‌کند، قادر به رضایت آگاهانه برای انجام آنها نیست، و یا کودک به‌لحاظ رشد برای انجام این فعالیت‌ها آماده نیست و نمی‌تواند رضایت دهد.
سوءاستفاده جنسی از کودکان به‌صورت برخط	این نوع از سوءاستفاده، می‌تواند هر شکلی از سوءاستفاده جنسی از کودکان باشد که پیوندی با محیط برخط دارد. بنابراین، سوءاستفاده جنسی برخط می‌تواند به‌شکل آزار جنسی از طریق رسانه‌های اجتماعی یا سایر کانال‌های برخط باشد.
سواد دیجیتالی	توانایی استفاده از فناوری اطلاعات و ارتباطات برای یافتن، ارزیابی، ایجاد و برقراری ارتباط.

1. Safety-by-Design
2. Content Moderation
3. Manipulating
4. Sexting
5. Privacy-by-Design
6. Digitization
7. Cyberflashing

اصطلاح	تعریف
سرقت هویت	جعل متقلبانه هویت فرد یا افراد دیگر، به منظور دسترسی به ثروت، آسیب‌رساندن به شهرت، دسترسی به مخاطبان برخط آنها یا کسب سود.
کنترل‌کننده داده	شخصی حقوقی یا حقیقی، یک آژانس، مقام دولتی یا هر ارگان دیگری که به‌تنهایی یا با کمک دیگران، اهداف هر نوع داده شخصی و ابزار پردازش آن را تعیین می‌کند.
کودک	اصطلاحی است که توافق نسبتاً جامعی درباره معنای آن وجود دارد و یا می‌توان بدون انگ زن یا آسیب‌زدن به کودک از آن استفاده کرد. در این متن به هر انسان زیر هجده سال اشاره دارد.
کودک در محیط دیجیتال	درک معنای اصطلاح «کودک» گاهی اوقات در حوزه برخط دشوارتر است زیرا ممکن است به دو موضوع مختلف مربوط به هم یعنی اعمال کودک برخط و نمایش کودک برخط اشاره داشته باشد. بر این اساس هر انسان زیر هجده سالی است که در محیط برخط یا برون‌خط فعالیت می‌کند.
فناوری اطلاعات و ارتباطات یا «ICT» / فناوری‌های دیجیتال	مجموعه متنوعی از ابزارها و منابع تکنولوژیکی که برای انتقال، ذخیره، ایجاد، اشتراک‌گذاری یا تبادل اطلاعات استفاده می‌شود. این ابزارها و منابع فناورانه شامل رایانه، اینترنت (وبسایت، وبلاگ و ایمیل)، فناوری‌های پخش زنده (رادیو، تلویزیون و پخش اینترنتی)، فناوری‌های پخش محتوای ضبط شده (پادکست، پخش‌کننده‌های صوتی و تصویری و دستگاه‌های ذخیره‌سازی) و تلفن (ثابت یا سیار، ماهواره، ویزیو / ویدئو کنفرانس و غیره) است.
محتوا	تمام محتوای چندرسانه‌ای موجود در پلتفرم‌های برخط مانند متن، تصویر، فایل‌های صوتی و تصویری و غیره.
محتوای سوءاستفاده جنسی از کودکان	اصطلاح «محتوای سوءاستفاده جنسی از کودکان» به‌طور فزاینده‌ای برای جایگزینی اصطلاح «هرزه‌نگاری کودکان» استفاده می‌شود. این تغییر بر این استدلال استوار است که مطالب جنسی که کودکان را به تصویر می‌کشد، درواقع بازنمایی و شکلی از سوءاستفاده جنسی از کودکان است و نباید به‌عنوان «هرزه‌نگاری» توصیف شود. لذا می‌توان گفت این اصطلاح به هرگونه تصویر بصری از رفتار جنسی صریح اشاره دارد که شامل کودک می‌شود.
محتوای جنسی خود تولید شده	کودکان و نوجوانان زیر هجده سال ممکن است از خود عکس‌ها یا فیلم‌های مخاطره‌آفرین بگیرند. درحالی‌که این رفتار به‌خودی‌خود لزوماً غیرقانونی نیست، اما این خطر وجود دارد که چنین محتوایی بتواند به‌صورت برخط یا برون‌خط برای آسیب‌رساندن به کودکان منتشر یا به‌عنوان مبثای برای اخاذی از آنها استفاده شود.
میزبانی وب	خدماتی که به سازمان‌ها و افراد اجازه می‌دهد تا وبسایت یا صفحه وب را در اینترنت ایجاد و منتشر کنند.
نشانی وب	شناسه‌ای منحصربه‌فرد یا آدرسی که در آن صفحه یا منبع خاصی را می‌توان در اینترنت یافت.
نت تاریک / وب تاریک	محتوای برخط رمزگذاری شده که با موتورهای جستجوی معمولی فهرست نشده‌اند و فقط با استفاده از مرورگرهای خاص قابل دسترسی است.
هرزه‌نگاری	تهیه و تولید هر اثری که محتوای آن بیانگر جذابیت جنسی طفل یا نوجوان مانند برهنگی، آمیزش، عمل جنسی یا اندام جنسی باشد.

[1] Keeley, B., & Little, C. (2017). The State of the World's Children 2017: Children in a Digital World. UNICEF. 3 United Nations Plaza, New York, NY 10017.

[۲] سلگی، محمد (۱۴۰۰). کودکان و اینترنت در ایران (فرصت‌ها و تهدیدها). پژوهشگاه فرهنگ، هنر و ارتباطات.

[3] UNICEF. (2015). Guidelines for industry on child online protection. UNICEF—Office of Research: Florence, Italy.

[4] Kowalski, R.M. and S.P. Limber, Psychological, physical, and academic correlates of cyberbullying and traditional bullying. Journal of adolescent health, 2013. 53(1): p. S13-S20.

[5] International Centre for Missing & Exploited Children. (2018). Child sexual abuse material: Model legislation and global review.

[6] The NetClean Report. (2016). 10 important insights into child sexual abuse crime', NetClean,

Gothenburg, Sweden.

[7] Alliance, W. G. (2023). Global Threat Assessment 2023: Assessing the scale and scope of child sexual exploitation and abuse online, to transform the response.

[8] UNICEF. (2022). Legislating for the digital age: Global guide on improving legislative frameworks to protect children from online sexual exploitation and abuse.

[9] Unicef. (2018). Policy Guide on Children and Digital Connectivity. New York: UNICEF.

[۱۰] تاج مزینانی، علی اکبر و یزدانی، فرشید (۱۴۰۲). سیاست‌گذاری در حوزه کودکان. در کودکی در دنیایی مدرن. تهران: دگر.

[۱۱] غنی‌زاده بافقی، مریم و رضوانی، سودابه (۱۴۰۲). راهبردهای حمایت از حقوق کودکان در محیط دیجیتال. فصلنامه تحقیقات حقوقی. ۴۹-۱۷۷: (۴) ۶۲.

[۱۲] قاسمی‌نژاد، عبدالرحیم (۱۴۰۱). بررسی چالش‌های توسعه زیست‌بوم فضای مجازی در حوزه کودک و نوجوان و ارائه بسته سیاستی. مرکز پژوهش‌های مجلس شورای اسلامی.

[۱۳] نیک‌بین، محسن و رئوفی، امین. (۱۴۰۲). حفاظت از حقوق کودک در فضای سایبر از منظر نظام ملل متحد و حقوق ایران. فصلنامه مطالعات حقوق عمومی: ۲۲-۱.

[۱۴] بادامی، محمدمهدی (۱۳۹۹). کودکان بر خط و حق آنان بر امنیت همه‌جانبه در فضای مجازی. تهران: مرکز مطبوعات و انتشارات قوه قضائیه.

[15] Livingstone, S., & Stoilova, M. (2021). The 4Cs: Classifying online risk to children.

[۱۶] کرامتی معز، هادی (۹۹۳۱). بزه‌دیده‌شناسی کودکان در شبکه‌های مجازی. تهران: دادگستر.

[17] Slavtcheva-Petkova, V., Nash, V. J., & Bulger, M. (2015). Evidence on the extent of harms experienced by children as a result of online risks: implications for policy and research. Information, Communication & Society, 18(1), 48-62.

[18] Mitchell, K. J., Ybarra, M. L., & Korchmaros, J. D. (2014). Sexual harassment among adolescents of different sexual orientations and gender identities. Child abuse & neglect, 38(2), 280-295.

[19] Koons Family Institute on International Law and Policy. (2017). Online grooming of children for sexual purposes: Model legislation & global review. International Centre for Missing and Exploited Children.

[20] Alliance, W. G. (2021). Estimates of childhood exposure to online sexual harms and their risk factors.

[21] Barber, C. S., & Bettez, S. C. (2021). Exposing patterns of adult solicitor behaviour: towards a theory of control within the cybersexual abuse of youth. European Journal of Information Systems, 30(6), 591-622.

[22] Unicef, General comment No. 25 (2021) on children's rights in relation to the digital environment.

[۲۳] بکاریا، سزار (۱۳۹۷). رساله جرائم و مجازات‌ها. ترجمه محمد علی اردبیلی، تهران: انتشارات میزان.

[24] OECD. (2024). Towards digital safety by design for children. OECD Digital Economy Papers, No. 363, OECD Publishing, Paris

[25] Siegel, L.J. and B.C. Welsh. (2005). Juvenile delinquency: Theory, practice, and law.

Cengage Learning.

- [۲۶] اصلانی بیشه، علی‌اکبر (۱۴۰۲). صیانت از کودکان و نوجوانان در فضای مجازی. تهران: جهاد دانشگاهی.
- [۲۷] وزارت ارتباطات و فناوری اطلاعات (۱۳۹۶). پیوست ۴ سند حمایتی و برنامه اقدام توسعه خدمات فضای مجازی کودک و نوجوان (ابزارهای کنترل والدین).
- [28] Livingstone, S., Lievens, E., & Carr, J. (2020). Handbook for policy makers on the rights of the child in the digital environment.
- [29] Page, M., Firth, C., & Rand, C. (2015). Internet value chain: A study on the economics of the Internet. Groupe Special Mobile association.
- [30] Unicef, Convention on the Rights of the Child. 1989.
- [31] Alliance, W.G and Economist Impact. (2023). Estimates of childhood exposure to online sexual harms and their risk factors.
- [32] Livingstone, S., Carr, J., & Byrne, J. (2015). One in three: Internet governance and children's rights.
- [۳۳] آقایی، عاطفه و رضانیان، زهرا (۱۳۹۸). مطالعه مفهوم «کودکان کار اینستاگرامی» در فضای مجازی ایران. فصلنامه حقوق کودک. ۱ (۳): ۱۶۱-۱۹۰.
- [۳۴] بیرانوند، فاطمه (۱۳۹۹). کار کودک در فضای مجازی و آسیب‌های آن. مطالعات فقه و حقوق رسانه. ۲۵-۵۲: (۱) ۲.
- [35] Palfrey, J. G., Gasser, U., & Boyd, D. (2010). Response to FCC notice of inquiry 09-94: Empowering parents and protecting children in an evolving media landscape. Berkman Center Research Publication, (2010-02), 10-19.
- [36] Brown, D. H., & Pecora, N. (2014). Online data privacy as a children's media right: Toward global policy principles. Journal of Children and Media, 8(2), 201-207.
- [37] Interagency Working Group. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse (Luxembourg Guidelines), ECPAT International and ECPAT Luxembourg.
- [38] COUNCIL, O. E. (2018). Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Recommendation CM/Rec, 7.
- [39] African Committee of Experts on the Rights and Welfare of the Child. (2021). General Comment No 7 on Article 27 of the Acrw (Sexual Exploitation).
- [40] Committee of the Parties to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Committee). (2019). Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children
- [41] United Nations. (2019). Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.
- [42] Unicef. (2020). Action to end child sexual abuse and exploitation: a review of the evidence 2020.



- [43] Rosli, N., Zubaidi, N. H. A., & Dusuki, F. N. (2019). Regulating the protection and rehabilitation of victims of internet child pornography in Malaysia. *International Journal of Academic Research in Business and Social Sciences*, 9(5), 450-469.
- [44] Von Weiler, J., Haardt-Becker, A., & Schulte, S. (2010). Care and treatment of child victims of child pornographic exploitation (CPE) in Germany. *Journal of Sexual Aggression*, 16(2), 211-222.
- [45] Dedase-Escoton, V., Walker, S., Shurter, D., Moreno, E., Diaz, N., & Silva, S. (2020). A study on online sexual exploitation of children for aftercare reintegration
- [46] Economic, U. N., & Council, S. (2005). Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, Resolution 2005/20. Note 8 (July 2005).

گزیده سیاستی

محیط دیجیتال برخی از مخاطرات و آسیب‌های اجتماعی گذشته را تسریع و اشکال جدیدی از آنها را به وجود آورده‌اند. یکی از گروه‌های در معرض خطر در برابر این آسیب‌ها کودکان و نوجوانان هستند. به منظور محافظت از آنها در این زمینه تدوین قانونی جامع ضروری است.



مرکز پژوهش‌های مجلس شورای اسلامی

تهران، خیابان پاسداران، روبروی پارک نیاوران (ضلع جنوبی، پلاک ۸۰۲)

تلفن: ۷۵۱۸۳۰۰۰ صندوق پستی: ۱۵۸۷۵-۵۸۵۵ پست الکترونیک: mrc@majles.ir

وبسایت: rc.majles.ir