

حمایت‌های قانونی در برابر مخاطره‌های پیش‌روی کودکان در فضای مجازی

فاطمه‌سادات حسینی ابراهیم‌آبادی^۱

زهرا حسین‌پور^۲

چکیده

محیط دیجیتال به بخش جدایی‌ناپذیری از زندگی روزمره و تعاملات کودکان تبدیل شده است. همراه با رشد فناوری و استفاده کودکان از محیط دیجیتال، مخاطره‌ها و مزایای مرتبط با آن نیز تکامل و گسترش می‌یابد. کودکان امروزی متناسب با زمانی که در فضای مجازی سپری می‌کنند، بیشتر با خطر نقض حریم خصوصی روبرو هستند، بیشتر در معرض محتوای نفرت‌انگیز، مضر یا توهین‌آمیز قرار دارند و احتمالاً بیش‌ازپیش مورد تبلیغات هدفمند تجاری قرار می‌گیرند. این مسائل سیاست‌گذاران را بر آن می‌دارد که با وضع قوانین و مقررات پاسخگوی نیازها و آسیب‌پذیری‌های خاص کودکان در این زمینه باشند. این مقاله تلاش نموده است با دسته‌بندی جامعی از مخاطره‌های پیش‌روی کودکان برخط و تطبیق قوانین و مقررات داخلی با مصادیق هر دسته ارائه نماید. همچنین با مروری اجمالی بر تجربه‌های بین‌المللی در این زمینه، توصیه‌هایی برای رفع خلأهای موجود در زمینه حمایت قانونی از کودکان در فضای مجازی ارائه نموده است.

واژه‌های کلیدی

کودکان برخط، فضای مجازی، حمایت‌های قانون.

sh_hoseinpour@outlook.com

۱- استادیار، دانشکده حقوق، دانشگاه غیرانتفاعی رفاه، تهران، ایران

۲- دانشجوی ارشد، رشته حقوق خانواده، دانشگاه غیرانتفاعی رفاه، تهران، ایران

مقدمه

در طول سه دهه گذشته، فناوری‌های اطلاعاتی و ارتباطی، شیوه تعامل و مشارکت کودکان با دنیای اطراف خود را عمیقاً تغییر داده است. گسترش نقاط دسترسی به اینترنت، فناوری تلفن همراه و روند رو به رشد دستگاه‌های مجهز به اینترنت، با گستره‌ای از منابع اطلاعات که در فضای مجازی یافت می‌شود، فرصت‌های بی‌سابقه‌ای را برای یادگیری، اشتراک‌گذاری و برقراری ارتباط فراهم می‌کند. استفاده از این فناوری کودکان را قادر می‌سازد تا از حقوق خود دفاع نموده و نظرهای خود را بیان کنند و راه‌های متعددی را برای ارتباط با خانواده و دوستان خود فراهم سازند. با این حال علی‌رغم مزایای فراوان این فناوری، کودکان در هنگام استفاده از آن با خطرهای متعددی نیز روبرو هستند. کودکان ممکن است در معرض محتوای نامناسب برای سن خود یا تماس نامناسب قرار گیرند.

آنها از آنجاکه نمی‌توانند به‌طور کامل پیامدهای بلندمدت «ردپای دیجیتالی» را درک کنند، ممکن است ناخواسته با انتشار اطلاعات شخصی حساس آسیبی به اعتبار برای خود و اطرافیانشان برسانند (ITU & UNICEF, 2015).

اگرچه در فضای حقوق کودک به‌صورت عام، کنوانسیون‌های بین‌المللی، قوانین و مقررات داخلی ازجمله کنوانسیون حقوق کودک (مجمع عمومی سازمان ملل متحد، ۱۹۸۹)، قانون الحاق دولت جمهوری اسلامی ایران به کنوانسیون حقوق کودک (مجلس شور، ۱۳۷۲)، قانون حمایت از کودکان و نوجوانان (مجلس شور، ۱۳۸۱) و قانون حمایت از اطفال و نوجوانان (مجلس شور، ۱۳۹۹) یا قوانین خاص مرتبط با فناوری اطلاعات از جمله قانون جرایم رایانه‌ای (مجلس شور، ۱۳۸۸)، قانون تجارت الکترونیکی (مجلس شور، ۱۳۸۲) و... در دسترس است، با این حال سرعت تحولات فناوری‌های اطلاعاتی و ارتباطی و تغییرهای بنیادین آن بر سبک زندگی از یک‌سو و ویژگی‌ها و اقتضائات کودکی و نوجوانی (محسنی، ۱۳۹۰) از سوی دیگر، جامعه را ملزم می‌سازد تا متناسب با تحولات این فناوری و اقتضائات جامعه، بستر تعامل کودکان با این فناوری را به‌صورت خاص در قالب چهارچوب‌های مدنی و قانونی، مورد بازبینی و تنظیم‌گری مجدد قرار دهد.

از این رو توصیه می‌شود کشورها در فواصل زمانی منظم، چهارچوب‌های قانونی را برای حمایت از تحقق کامل حقوق کودک در محیط دیجیتال به‌روزرسانی کنند. این امر نیز مستلزم آن است که اولاً کشورها مشخص کنند که کدام قوانین در حال حاضر وجود دارد، آیا شکاف‌ها یا همپوشانی‌هایی در آنها وجود دارد و کدام نهادها مسئولیت اجرای آن قوانین را بر عهده دارند (Livingstone et al., 2020). این پژوهش سعی نموده است با دسته‌بندی مخاطره‌های پیش‌روی کودکان در فضای مجازی، قوانین و مقررات مصوب کشور در این زمینه‌ها را در سرفصل‌های مخاطره‌ها دسته‌بندی نموده و شکاف‌ها و همپوشانی‌ها را شناسایی نماید. در ادامه نیز با الگوبرداری از مجموعه قوانین مرتبط در کشورهای توسعه‌یافته، توصیه‌ها و پیشنهادهایی برای رفع خلأهای موجود ارائه نموده است.

در زمینه حقوق کودک در فضای مجازی در منابع داخلی پژوهش‌های متعددی انجام شده است. با این حال با مرور پژوهش‌های انجام شده درمی‌یابیم که این پژوهش‌ها هر یک بر وجوه خاصی از حقوق کودکان برخط تمرکز نموده‌اند. در این میان تمرکز به حفظ حریم خصوصی کودک به عنوان یکی از وجوه حقوق کودکان برخط به تواتر مورد توجه پژوهشگران داخلی بوده است. فرامرزیانی و همکاران چهارچوب نسبتاً جامعی برای حمایت از حریم خصوصی کودکان برخط ارائه کرده و راهکارهایی نیز در زمینه حمایت‌های قانونی در این خصوص پیشنهاد نموده‌اند (فرامرزیانی و دیگران، ۱۴۰۰). علیزاده نیز موضوع حریم خصوصی کودک در فضای مجازی را از منظر حقوق ایران و کنوانسیون حقوق کودک را مورد بررسی قرار داده و مجموعه قوانین مرتبط با حریم خصوصی کودک در فضای مجازی را دسته‌بندی نموده است (علیزاده، ۱۳۹۹). همچنین شهریاری احمدی با الگوبرداری تطبیقی از اقدام‌های شورای اروپا در خصوص حمایت از حریم خصوصی کودک در فضای مجازی خلأهای موجود در قوانین داخلی را شناسایی نموده است (شهریاری احمدی، ۱۳۹۶). صادقی نیز راهکارهایی حقوقی برای صیانت از حریم خصوصی کودکان برخط با توجه قوانین موجود پیشنهاد نموده است (صادقی، ۱۳۹۹).

مرور مجموعه پژوهش‌های فوق مؤید آن است که مسئله صیانت حقوقی از حریم خصوصی بیش از هر جنبه دیگری از مخاطره‌هایی که کودکان برخط با آن مواجه‌اند،

مورد توجه بوده است.

کریمی، قدرتی و جواهری و همکاران مروری بر حمایت‌های قانونی در زمینه هرزه‌نگاری، پورنوگرافی و جرایم جنسی مرتبط با کودکان در فضای مجازی انجام داده‌اند (کریمی، ۱۳۹۷؛ قدرتی، ۱۳۹۸؛ جواهری و دیگران، ۱۳۹۹). همچنین پالاش و نیکبختی با انجام مطالعاتی تطبیقی بر روی قوانین بین‌المللی در زمینه هرزه‌نگاری کودکان در فضای مجازی، سعی در شناسایی خلأهای قوانین داخلی در این زمینه داشته‌اند (پالاش، ۱۳۹۴؛ نیکبختی، ۱۳۹۷).

همچنین گروهی از پژوهش‌ها نیز بر نقش قانونی بازیگران جامعه مدنی در زمینه حمایت از حقوق کودکان برخط تمرکز دارند. در این میان نقش والدین (رفاعی، ۱۳۹۸) از منظر سرپرست کودک و دولت (قاسمی نوروزآباد، ۱۳۹۷؛ حسینی، ۱۳۹۸) به‌عنوان تضمین‌کننده نهایی حقوق افراد در جامعه بیش از سایرین مورد توجه پژوهشگران قرار گرفته است. برخی از پژوهش‌ها مانند محسنی نیز از مصادیق حمایت از حقوق کودکان برخط عبور کرده و سعی نموده‌اند تا چهارچوبی کلی‌تر ارائه دهند (محسنی، ۱۳۹۰). بااین‌حال از آنجاکه این مطالعات یک مدل مرجع مخاطره‌های پیش‌روی کودکان برخط را مورد نظر قرار نداده‌اند، هریک از پژوهش‌های مورد اشاره تنها توانسته‌اند بخشی از فضای موضوع را ترسیم نموده و تصویری یکپارچه از موضوع ارائه ننموده‌اند؛ لذا برای رسیدن به تصویری جامع نیاز است پیش از هر چیز شناخت مناسبی از مخاطره‌های پیش‌روی کودکان برخط داشته باشیم.

۱- مخاطره‌های پیش‌روی کودکان برخط

با مروری بر مطالعات انجام پذیرفته در این زمینه، چهار دسته مخاطره قابل تمیز دادن هستند: (۱) مخاطره‌های محتوایی؛ (۲) مخاطره‌های رفتاری؛ (۳) مخاطره‌های تماسی و (۴) مخاطره‌های مصرف‌کننده.

۱-۱- مخاطره‌های محتوایی

مخاطره‌های محتوای شامل شرایطی شود که «کودک به‌طور منفعلانه محتوایی را که برای همه کاربران اینترنت در یک رابطه یک به چند در دسترس است، دریافت می‌کند یا در معرض آن قرار می‌گیرد». چهار صورت ریسک تحت عنوان ریسک‌های محتوایی تشخیص داده می‌شود. الف) محتوای نفرت‌انگیز؛ ب) محتوای مضر؛ ج) محتوای غیرقانونی و د) دروغ‌رسانی.

محتوای نفرت‌انگیز می‌تواند به شکل تصاویر، کلمه‌ها، فیلم‌ها، بازی‌ها، نمادها و حتی آهنگ‌ها باشد (Livingstone, 2019)؛ به‌طور مثال کودک ممکن است به‌دلیل دین، مذهب، نژاد، تمایل‌های جنسی، ناتوانی، جنسیت، ملیت، سن، هویت جنسی و وابستگی سیاسی (امامی و احمدی، ۱۳۹۷) قربانی چنین محتوایی شود. این‌گونه محتواها به‌صورت تصاعدی و اغلب غیرقابل کنترل در محیط دیجیتالی و پلتفرم‌ها تولید و پخش می‌گردند و ناشناس بودن و فاصله فیزیکی از قربانی نیز موجب تشدید آن شده است. اهمیت این خطر و رشدنمایی آن وقتی بیشتر مشخص می‌شود که بدانیم، بر اساس پژوهشی در بریتانیا، در سال ۲۰۱۰ تنها ۱۲ درصد از کودکان ۱۱ تا ۱۶ ساله گزارش دادند که در معرض محتوای نفرت‌انگیز برخط قرار گرفته‌اند، ولی تا سال ۲۰۲۱ این عدد به نیمی از کودکان ۱۲ تا ۱۵ سال رسیده است (Ofcom, 2021). جرایم ناشی از نفرت از دهه ۱۹۸۰ در ایالات متحده آمریکا و کشورهای دیگر رایج و وارد قلمرو مطالعاتی حقوق کیفری و جرم‌شناسی شده است. در سال‌های اخیر نیز مبارزه با محتوای نفرت‌انگیز خصوصاً در فضای مجازی در کشورهای فرانسه، آلمان (ایسنا، ۱۳۹۸) سوئیس (دیجیاتو، ۱۳۹۸) و سایر کشورهای توسعه‌یافته مورد قانون‌گذاری قرار گرفته است.

در حقوق ایران جرایمی تحت عنوان جرایم مبتنی بر نفرت در قوانین داخلی، به‌صورت جداگانه جرم‌انگاری و طبقه‌بندی نشده است (قورچی بیگی و رضائیان کوچی، ۱۳۹۹). به‌طور نمونه ازجمله قوانینی که به‌صورت محدودی که از مصادیق جرایم مبتنی بر نفرت را در ایران جرم‌انگاری کرده، قانون مجازات تبلیغ تبعیض نژادی (مجلس شورا، ۱۳۵۶) است که تبلیغ و نشر افکار مبتنی بر تبعیض بر اساس جنس و نژاد و نفرت نژادی و تحریک به آن

از طریق تبلیغ عمومی را به طور مستقل جرم‌انگاری کرده است. هر چند که این قانون قبل از انقلاب به تصویب رسیده، اما کماکان پابرجاست.

می‌توان سبب عدم توجه قانون‌گذاران داخلی به این موضوع را در عدم تنوع عقاید، مذاهب، نژاد و امثال آن در ایران و نیز این واقعیت دانست که کمتر جرم خاص و فراگیری اتفاق افتاده است که به جهت‌های نژادی و تعلق به یک گروه اعتقادی، قومی یا زبانی رخ داده باشد و به همین جهت در گذشته قانون‌گذار به این دلیل و عدم وجود چنین جرایمی در فقه لزومی بر جرم‌انگاری ندیده است (انصاری اصل و آرزومند، ۱۳۹۶). از طرفی نیز مقنن ایران نه تنها چنین جرایمی را جرم‌انگاری نکرده و ارتکاب جرم انتشار و پخش محتوای نفرت‌انگیز با انگیزه‌های نژادی، قومی، ملی و مذهبی هیچ تأثیری در میزان مجازات ندارد، حتی با وضع قوانین تبعیض‌آمیز بر پایه مذهب و جنسیت بزه‌کار و بزه‌دیده، موجب نوعی نفرت بالقوه در غیرمسلمانان، زنان و حتی کودکان و نیز موجب تجری مسلمانان و مردان شده است (امامی و احمدی، ۱۳۹۷). لذا با توجه به ساختار جمعیتی و ماهیت متکثر رو به تزاید جامعه ایرانی لازم است بر اساس اصول متعدد قانون اساسی از جمله اصول ۱۴، ۱۹، ۲۶ و ۲۹، با وضع قوانین خاص در این زمینه از گروه‌ها و قشرهای آسیب‌پذیر، خصوصاً کودکان حمایت بیشتری به عمل آید.

کودکان همچنین می‌توانند با طیف گسترده‌ای از محتوای مضر مانند تبلیغات پورنوگرافی، اخبار یا تصاویر ناخوشایند یا ترسناک دچار مشکل شوند (Byrne & Burton, 2017). محتوای خشونت‌آمیز و مستهجن می‌تواند باعث شوک و انزجار کودکان شود. مطالعه‌ای در سال ۲۰۲۰ نشان می‌دهد که در اتحادیه اروپا بیشترین محتوای مضر که کودکان (حداقل ماهانه) در معرض آن قرار می‌گیرند پیام‌های نفرت‌انگیز (متوسط ۱۷ درصد) و پس از آن تصاویر خشونت‌آمیز (متوسط ۱۳ درصد) بود. این گزارش همچنین نشان داد که قرار گرفتن در معرض انواع مختلف محتوای مضر به هم مرتبط است؛ به عنوان مثال، اگر کودکی یک نوع محتوای مضر را ببیند، احتمال بیشتری دارد که همان کودک انواع دیگری از محتوای مضر را نیز گزارش کند (Smahel et al., 2020).

در میان مخاطره‌های محتوایی، به خصوص در متون داخلی محتواهای مضر کمتر

مورد توجه قرار گرفته است. بخشی از این کم‌توجهی شاید به ماهیت این محتوا بازگردد. بر اساس تعریف مرکز اینترنت امنتر بریتانیا، محتوای مضر هر محتوایی است که باعث ناراحتی یا آسیب به شخص می‌شود. با این تعریف، مفهوم «محتوای مضر» می‌تواند حجم عظیمی از محتواها را دربرگیرد یا خیر. چرا که بسته به این خواهد بود که چه کسی درحال مشاهده آن است؟ آنچه ممکن است برای یک کودک مضر باشد الزاماً توسط یک بزرگسال ممکن است چنین نباشد.

قانون محافظت از کودکان در اینترنت (US Congress, 2003) در ایالات متحده از مدارس و کتابخانه‌ها می‌خواهد که برای محافظت از کودکان برابر محتوای برخلاف مضر از فیلترینگ استفاده کنند تا بتوانند از شرایط تأمین مالی فدرال بهره‌مند شوند. قانون فدرال «حمایت از کودکان در برابر اطلاعات مضر برای سلامتی و رشد آنها» در سال ۲۰۱۰ توسط دوماي روسیه تصویب و در سال ۲۰۲۰ اصلاح و بازنگری شده است. حمایت از کودکان در برابر محتواها نامناسب و زیان‌آور در رسانه‌های جمعی و شبکه‌های ارتباطی و اطلاعاتی به‌عنوان هدف این قانون عنوان شده است. سایر کشورها نیز به فراخور توسعه‌یافته موضوع در این زمینه قوانینی وضع نموده‌اند. همچنین مدتی است که اتحادیه اروپا در حال کار کردن روی قانون خدمات دیجیتالی (DSA) است. این قانون می‌تواند قدرتمندتر از همیشه جلوی انتشار محتواهای مضر در پلتفرم‌ها و تارنماهای مختلف را بگیرد (European Commission, 2022). حفاظت از کودکان در برابر محتوای مضر در ایران اخیراً در دستور کار دولت قرار گرفته است. در مصوبه شورای عالی فضای مجازی در خصوص صیانت از کودکان و نوجوانان در فضای مجازی، کلیه سکوها و ارائه‌دهندگان محتوا و خدمات فضای مجازی به نظارت، صیانت از داده‌ها، رده‌بندی و تفکیک محتوا و خدمات ویژه هر رده سنی از خدمات عمومی و در معرض دید قرار دادن تبلیغات، محتوا و خدمات مضر به این سنین و نیز جلوگیری از افشاء یا بهره‌برداری غیرمجاز از اطلاعات آنها ظرف مدت یک‌سال ملزم شده‌اند. با این حال مصوبه مذکور بیشتر ساختار یک توصیه‌نامه داشته و برای تبدیل شدن به یک قانون نیازمند تبیین ضمانت‌های اجرایی و تعیین مجازات و جرم‌انگاری موضوع می‌باشد.

محتوایی که انتشار آن غیرقانونی است می‌تواند کودکان را در معرض مفاهیمی قرار دهد که قادر به مدیریت و فهم درست آن نیستند. همچنین می‌تواند هنجارهای فرهنگی و اجتماعی را نقض کند؛ به‌عنوان مثال، تصاویر یا ویدیوهای سوءاستفاده جنسی از کودکان، محتوایی که از اقدام‌های تروریستی حمایت می‌کند، یا ترویج، راهنمایی یا تحریک جنایت یا خشونت در بسیاری از کشورها غیرقانونی است. با این حال واکنش قانونی به این نگرانی‌ها در حیطه قضایی کشورهای مختلف، متفاوت است؛ به‌عنوان مثال، در برخی از کشورهای اروپایی سخنان مشوق تنفر یا محتوای برخاسته از نژادپرستانه ممکن است غیرقانونی باشد، درحالی‌که سایر کشورها ممکن است واکنش متفاوتی برای مقابله با چنین مسائلی داشته باشند.

دروغ‌رسانی^۱ انتشار عامدانه و برنامه‌ریزی شده اطلاعات نادرست یا گمراه‌کننده برای فریب مخاطبان است. در فارسی به آن دروغ‌پراکنی و انتشار اخبار ساختگی هم گفته می‌شود. دروغ‌رسانی با غلط‌رسانی^۲ که ناشی از اشتباه و سهو است، تفاوت دارد. به بیان بهتر اطلاعات غلط زمانی که به‌صورت هدفمند و عمدتاً و به‌منظور فریب دادن منتشر شود، شکل دروغ‌رسانی به خود می‌گیرد (آیرتون و پوزتی، ۱۳۹۹).

اجماع فزاینده‌ای وجود دارد که کودکان باید در مورد دروغ‌رسانی آموزش ببینند تا بتوانند بین آنچه درست است را از آنچه نادرست است یا به شکل نادرست در محیط دیجیتال ارائه می‌شود، تمیز دهند. این یک مهارت کلیدی است؛ زیرا کودکان می‌توانند تفسیرهای متفاوتی از آنچه که یک رسانه خبری را معتبر می‌کند، داشته باشند و آنها بیشتر اخبار و اطلاعات را از رسانه‌های اجتماعی و پلتفرم‌هایی به‌دست می‌آورند که ممکن است غیرقابل اعتماد باشد (Babür, 2017). بر این اساس، کودکان به مهارت‌های سواد دیجیتال قوی نیاز دارند تا بتوانند محتوایی را که مصرف می‌کنند تحلیل انتقادی کنند و دروغ‌رسانی را تشخیص دهند (کاظم پوریان و عبلی، ۲۰۱۷).

در عین حال، مهم است که اطمینان حاصل شود که تمرکز بر حصول اطمینان از سواد دیجیتال قوی باعث نمی‌شود که مسئولیت کاهش این خطر مستقیماً بر دوش کودکان

1. disinformation
2. misinformation

گذاشته شود. کسانی که محتوا را ایجاد و میزبانی می‌کنند نقش حیاتی در مقابله با چنین اطلاعات نادرستی دارند. این امر در طول شیوع کرونا نیز مشهود بوده است. جایی که پلتفرم‌ها و شرکت‌های رسانه‌های اجتماعی خاص، تلاش‌های خود را برای حذف اطلاعات همراه‌کننده، نادرست و بالقوه مضر مرتبط با کرونا تقویت کرده‌اند. به‌طور خاص، فیس‌بوک، یوتیوب، گوگل، لینکدین، مایکروسافت، ردیت و توییتر بیانیه مشترکی در مورد همکاری خود با آژانس‌های بهداشتی دولتی برای جلوگیری از اطلاعات نادرست مرتبط با کرونا منتشر کرده‌اند (OECD, 2020). با این حال، با وجود این تلاش‌ها، کسب مهارت‌های سواد دیجیتال برای شناسایی دروغ‌رسانی همچنان می‌تواند برای کودکان چالش‌برانگیز باشد؛ به‌عنوان مثال، یک گزارش پارلمانی نشان داد که تنها دو درصد از کودکان و جوانان در بریتانیا مهارت‌های سواد دیجیتال لازم برای ارزیابی واقعی یا جعلی بودن یک خبر را دارند (National Literacy Trust, 2018).

علی‌رغم اهمیت روزافزون موضوع، حمایت قانونی از کودکان در مقابل دروغ‌رسانی در مراحل مقدماتی به‌سر می‌برد. توصیه‌هایی توسط نهادهای بین‌المللی فعال مانند یونیسف (Vosloo, 2021) و یا تلاش‌های مشترکی توسط برخی پلتفرم‌ها و شبکه‌های اجتماعی برای کاهش اثرهای سوء این پدیده خصوصاً در دوره شیوع کرونا به‌صورت داوطلبانه انجام پذیرفته است، ولی قوانین منسجمی در این زمینه در کشورهای پیشرو فناوری نیز تصویب و اجرا نشده است. به‌التبع در مقررات و قوانین داخلی نیز ردی از این موضوع مشاهده نمی‌شود.

در این زمینه قانون ممنوعیت تبلیغات و معرفی محصولات و خدمات غیرمجاز و آسیب‌رسان به سلامت در رسانه‌های ارتباط جمعی داخلی و بین‌المللی و فضاهای مجازی (مصوب ۱۳۹۷) تنها قانون داخلی است که به مفهوم دروغ‌رسانی، اطلاعات نادرست و خلاف واقع پرداخته ولی با تقلیل موضوع به محصولات، بالخصوص محصولات دارویی و خوراکی دامنه موضوع را به‌شدت محدود نموده است.

۱-۲- مخاطره‌های رفتاری

مفهوم «مخاطره رفتاری» وقتی رخ می‌دهد که کودک خود بازیگر یک تبادل اطلاعات یک

به یک بوده و به دلیل رفتار خود در معرض خطر باشد؛ به عنوان مثال با ارسال یک پیام یا برقراری یک تماس. کودکان باید از تأثیری که فعالیت برخط آنها بر روی خود و سایر افراد و ردپای دیجیتالی که در اینترنت ایجاد می کنند، آگاه باشند. ناشناس بودن در فضای برخط آسان است و مهم است که کودکان بدانند چه کسی می تواند اطلاعاتی را که ممکن است پست کرده باشد، مشاهده کند و احتمالاً به اشتراک بگذارد.

چهار صورت از ریسک های رفتاری نیز قابل تفکیک هستند. الف) رفتار نفرت آمیز؛ ب) رفتار مضر؛ ج) رفتار غیرقانونی و د) رفتار مشکل ساز کاربر. در بررسی حقوقی مشخص شده است ریسک رفتاری زمانی تشدید می شود که کودک به گونه ای رفتار کند که به انتشار محتوای دیجیتال یا تماس پرخطر کمک نماید (UNICEF, 2017).

رفتار نفرت انگیز می تواند ناشی از مذهب، نژاد، جنسیت، ناتوانی، گرایش جنسی، هویت جنسی قربانی باشد، یا حتی ویژگی های شخصی مانند لهجه، مهارت های زبانی، ظاهر شخصی، سرگرمی ها، سلیقه در موسیقی، مد و... هدف اصلی رفتار نفرت انگیز سوءاستفاده یا توهین به قربانی است. در مورد رفتار مضر، کودک یا کودکان می توانند از محیط دیجیتال برای تجاوز به کودک دیگر استفاده کنند که در بسیاری از موارد منجر به آزار و اذیت سایبری می شود.

عدم توافق بین بازیگران سیاست و تحقیقات در مورد آنچه که واقعاً مزاحمت سایبری را تشکیل می دهد، منجر به این شده است که کشورها به روش های مختلف به این نگرانی رسیدگی کنند که عمدتاً با وضع قوانین کیفری همراه بوده است. با این حال، در جایی که کودکان مرتکب این رفتار هستند، واکنش کیفری می تواند بسیار بحث برانگیز و نامتناسب باشد؛ زیرا می تواند منجر به جرم انگاری کودکانی شود که از تأثیر اعمال خود آگاه نیستند. ارسال و تبادل پیام های جنسی، نمونه ای از رفتار مشکل ساز کاربران است. این رفتار می تواند مشکلات متعددی (اعم از اجتماعی و حقوقی) ایجاد کند. به طور معمول چنین انگاشته می شود که ارسال پیام تنها در صورتی به عنوان یک ریسک بروز می کند که تصویری بدون رضایت سوژه به اشتراک گذاشته شود، اما در موضوع کودک چنین نیست. گاهی کودک با رضایت خودش پیامی را به اشتراک می گذارد و درواقع خود او

تولیدکننده محتواسـت. محتوای پورنوگرافی کودکان می‌توانند به سرعت پخش شوند و به‌طور دائم در محیط دیجیتال باقی بمانند. ارسال پیامک نه‌تنها بر حریم خصوصی، بلکه بر سلامت و رفاه کودک نیز تأثیر می‌گذارد، حتی این خطر وجود دارد که کودک در نتیجه تولید مطالب مستهجن توسط خودش مجرم محسوب شود.

۲-۳- مخاطره‌های تماسی

مخاطره‌های تماسی زمانی رخ می‌دهد که کودک در محیط دیجیتال تعامل داشته باشد. این ریسک به چند صورت بروز می‌کند: الف) کودک در معرض برخوردهای نفرت‌انگیز در محیط دیجیتال قرار می‌گیرد؛ ب) برخورد به قصد آسیب رساندن به کودک صورت می‌گیرد؛ ج) برخورد طبق قوانین کیفری قابل پیگرد قانونی است و د) برخورد مشکل‌ساز است، اما نمی‌توان آن را تحت سه دسته قبلی قرار داد.

درست مانند مخاطره‌های شناسایی شده قبلی، انگیزه‌های چنین تماس‌هایی می‌توانند همپوشانی داشته باشند و ممکن است برای مثال، همان اقدام‌هایی که منجر به ریسک رفتاری شده‌اند، منجر به ریسک تماسی نیز بشوند. تفاوت در اینجا این است که کودک در مقابل بازیگر، قربانی (یا گیرنده) چنین اعمالی است؛ به‌طورمثال، قربانی شدن کودک در یک آزار اینترنتی می‌تواند منجر به عواقب منفی برای رشد شخصی، ایمنی و رفاه قربانی شده و حتی گاه به خودکشی کودک منجر شود.

از نمونه‌های دیگر این ریسک می‌توان به اخاذی جنسی که نوعی استثمار است اشاره کرد، که به‌موجب آن کودک تهدید به افشا یا به‌اشتراک گذاشتن تصویری جنسی برای باجگیری با هدف انجام کاری مانند اشتراک‌گذاری تصاویر بیشتر، پرداخت پول یا شرکت در فعالیت جنسی شود.

علاوه‌براین، پدیده قاچاق جنسی^۱ و آراستگی سایبری^۲ کودکان، مخاطره‌های تماسی واضح و متأسفانه رو به افزایش هستند. در سال ۲۰۱۲، سازمان بین‌المللی کار گزارش

1. sex trafficking

2. cyber grooming

کرد ۹.۲۰ میلیون نفر مجبور به کار اجباری شده که از میان آنها ۲۲ درصد یعنی ۵.۴ میلیون نفر قربانی قاچاق جنسی هستند. این عدد در سال ۲۰۱۶ به ۵ میلیون قربانی قاچاق جنسی افزایش پیدا کرده است (ILO, 2017). با این حال، به دلیل پنهان بودن پدیده قاچاق جنسی به خصوص در میان کودکان، به دست آوردن آمار دقیق و قابل اعتماد برای محققان دشوار است.

نکته قابل تأمل آن است که اگرچه برخی از کشورها برای این گونه مخاطره‌ها در فضای مجازی قانون‌گذاری کرده‌اند، تعدادی نیز «آگاهانه» همچنان قوانین آزار و اذیت سنتی خود را در مورد جرایم آزار و اذیت سایبری اعمال می‌کنند؛ برای نمونه، بر اساس قوانین بریتانیا، قانون خاصی وجود ندارد که به صراحت آزار و اذیت سایبری را غیرقانونی کند، اگرچه طبق قوانین مختلف می‌تواند جرم محسوب شود. این امر از این جهت پیچیده است که از یک سو مستلزم وقوع عناصر تشکیل‌دهنده جرم آزار و اذیت سنتی در رفتار برخط است و از سوی دیگر مستلزم این است که جرم متناسب در میان قوانین متعدد شناسایی شود؛ به طور مثال، قانون حفاظت از آزار و اذیت بریتانیا (مصوب ۱۹۹۷) مشخص می‌کند که وقتی فردی رفتاری را دنبال کند که به آزار و اذیت دیگری ختم شود، چه مرتکب بداند یا نداند که آزار و اذیت انجام داده، مجرم است. این قانون همچنان می‌تواند برای ارسال ایمیل توهین‌آمیز به یک شخص به قصد ایجاد هشدار یا ناراحتی قابل استفاده باشد. با این حال، قانون ارتباطات مخرب (مصوب ۱۹۸۸)، قانون انتشارات زشت (مصوب ۱۹۵۹)، قانون نظم عمومی (مصوب ۱۹۸۶) و قانون سوءاستفاده از رایانه (مصوب ۱۹۹۰) نیز به طور بالقوه در این مورد قابل اجرا هستند. در سال ۲۰۱۴ یک کمیته مجلس اعیان بررسی کرد که آیا برای این موضوع یک قانون اختصاصی لازم است یا خیر؟ در نهایت، تصمیم گرفته شد که قوانین موجود «به طور کلی برای تعقیب جرایم مناسب است». با این حال، همچنان نگرانی فزاینده‌ای وجود داشت که قانون فعلی کاملاً مؤثر نیست؛ لذا در فوریه ۲۰۱۸، نخست‌وزیر دستور بررسی در مورد قانون مربوط به ارتباطات برخط توهین‌آمیز و زشت را اعلام کرد. این بررسی با هدف برجسته کردن هر گونه شکاف محتمل در قانون کیفری که ممکن است در برخورد با این

سوءاستفاده مشکل ایجاد کند، انجام شد. کمیسیون حقوقی در گزارش خود به این نتیجه رسید که اگرچه برخی ابهام‌ها و مسائل فنی در قانون وجود دارد، اما گستردگی جرایم ارتباطی فعلی برای ارتباطات برخط توهین‌آمیز و زشت به‌گونه‌ای است که در بیشتر موارد، جرایم کیفری موجود در قوانین برای چنین رفتارهایی به‌صورت برخط نیز پوشا هستند (El Asam & Samara, 2016).

در قوانین داخلی نیز تنها ماده ۶۰۸ قانون مجازات اسلامی در روابط افراد و ماده ۶۰۹ قانون مجازات اسلامی در ارتباط با مقامات فارغ از غیربرخط یا برخط بودن آن تنها توهین به افراد از قبیل فحاشی و استعمال الفاظ رکیک را جرم‌انگاری نموده است. همچنین در ماده ۱۶ قانون جرائم رایانه‌ای به‌نحوی موضوع هتک حیثیت فرد از طریق برخط جرم‌انگاری شده است. حال آنکه توهین در فضای مجازی قابل قیاس با توهین سنتی نمی‌باشد؛ زیرا در توهین سنتی ممکن است فرد در مقابل عده‌ای محدود مورد اهانت واقع شود، اما آسیب ناشی از توهین رایانه‌ای گستره بیشتری از توهین سنتی دارد. شاید بتوان در توهین سنتی اعاده حیثیت نمود، اما در توهین برخط که وسعتی به اندازه کل دنیا دارد، اعاده حیثیت بسیار مشکل و غالباً غیرممکن است و به‌همین جهت، نیاز به شدت عمل بیشتری دارد؛ لذا حتی توهین برخط که حداقل ریسک ارتباطی حتی برای بزرگسالان است نیز به‌صراحت در هیچ ماده‌ای از قوانین داخلی ذکر نشده و بدون مجازات ماندن آن مطمئناً بر ارتکاب روزافزون آن خواهد افزود. حال در خصوص کودکان بایستی موضوع به شکل خاص‌تری مورد وضع قرار گیرد.

۲-۴- مخاطره‌های مصرف‌کننده

کودکان همچنین می‌توانند به‌عنوان مصرف‌کننده در اقتصاد دیجیتال با مخاطره‌هایی روبرو شوند. کودک ممکن است در صورت دریافت پیام‌های بازاریابی برخط که برایش نامناسب است (مانند مشروبات الکلی) با ریسک مصرف‌کننده بازاریابی روبرو شود. همچنین کودکان می‌توانند در معرض پیام‌های تجاری‌ای قرار گیرند که به‌راحتی قابل

شناسایی نباشند (مانند تبلیغات نامحسوس^۱) یا پیام‌هایی که فقط برای بزرگسالان در نظر گرفته شده است (مانند خدمات دوست‌یابی). گاهی نیز باورپذیری و بی‌تجربه بودن کودک مورد سوءاستفاده قرار می‌گیرد و ریسک اقتصادی ایجاد می‌کند (مانند کلاهبرداری‌های برخط). از آنجایی که کودکان به واسطه سن، بلوغ و سایر شرایطشان بیشتر از بزرگسالان مستعد اقدام‌های گمراه‌کننده یا متقلبانه هستند، در محیط دیجیتال بیشتر هدف قرار می‌گیرند. درواقع، کودکان مخاطب مهمی برای بازاریابان هستند؛ زیرا احتمال زیادی وجود دارد که بر مخارج خانواده تأثیر بگذارند، ناخواسته در معاملات شرکت کنند و یا مصرف‌کنندگان آینده باشند (van der Hof, 2017).

چهار نوع ریسک را در ذیل مخاطره‌های مصرف‌کننده برای کودکان می‌توان شناسایی نمود: الف) مخاطره‌های بازاریابی؛ ب) مخاطره‌های پروفایل تجاری؛ ج) مخاطره‌های مالی و د) مخاطره‌های امنیتی. این مخاطره‌ها می‌تواند بر حریم خصوصی کودکان تأثیر بگذارد، به فشار تجاری تبدیل شود و کودکان را در معرض پیام‌ها یا محصولات نامناسب قرار دهد (Livingstone et al., 2016).

ریسک‌های بازاریابی شامل روش‌هایی است که می‌تواند کودکان را در معرض محصولات غیرقانونی و نامناسب سنی و راهبردهای بازاریابی بالقوه مضر مانند تبلیغات همسان^۲، بازاریابی غیرشفاف «تأثیرگذار» و «بازی‌های تبلیغاتی» قرار دهد. تمایز بین محتوای تجاری و غیرتجاری برای کودکان دشوار است (ICPEN, 2020).

کودکان ممکن است توانایی درک کامل اطلاعات ارائه شده در تراکنش‌های تجاری مانند افشای اطلاعات در مورد بازاریابی گزینه‌های منفی یا تله‌های اشتراک در برنامه‌ها و بازی‌های برخط را نداشته باشند؛ برای مثال، آنها ممکن است به‌طور کامل اطلاعات مربوط به «پرداخت‌های خرد» یا خرید «جعبه‌های شانس» درون بازی، را کاملاً درک نکنند. حتی ممکن است کودکان رابطه بین پول واقعی و پول درون بازی را به‌درستی درک نکنند (FTC, 2020).

1. Product Placement
2. native advertising

مخاطره‌های پروفایل تجاری ممکن است زمانی ایجاد شوند که تبلیغ‌کنندگان از داده‌های ایجاد شده از طریق استفاده کودکان از رسانه‌های اجتماعی و سایر موارد بهره‌برداری کنند. پلتفرم‌های دیجیتال بدون رضایت آگاهانه و گاهی حتی با نقض قوانین حفاظت از مصرف‌کننده یا داده‌ها چنین اقدامی را انجام می‌دهند. گاهی حتی در برخی کشورها دولت‌ها در مواجهه با شهروندان چنین مخاطره‌ای ایجاد می‌کنند. بسیاری از کودکان مهارت‌های سواد دیجیتالی کافی برای درک افشاگری‌هایی که در محیط دیجیتال ممکن است با آن مواجه شوند، ندارند، به‌ویژه در رابطه با استفاده از داده‌های شخصی خود.

در رابطه با پروفایل تجاری، در اتحادیه اروپا تحت بند ۷۱ مقررات عمومی حفاظت از داده‌ها (GDPR) (EU, 2016) الزام می‌کند که «چنین اقدام‌های پروفایل تجاری نباید درخصوص کودکان انجام شود». به‌غیر از مقررات اشاره شده، درحال حاضر هیچ قاعده جهانی پذیرفته شده‌ای برای تنظیم‌گری اقدام‌های پروفایل تجاری کودکان وجود ندارد (ICPEN, 2020).

شایان ذکر است که جدا از جنبه‌های تجاری آن، پروفایل می‌تواند برای اهداف گسترده دیگری نیز استفاده شود که گاه برای کودکان می‌تواند سودمند باشد. می‌توان از آن برای پیشنهاد محتوا مناسب به کودکان، تشویق آنها به رفتارهای خاص، تعیین مکان، زمان و تعداد دفعه‌های ارائه محتوا به کودک استفاده کرد. بالین حال، رشد هدایت محتوایی که به تدریج کودکان را از حوزه‌های اصلی مورد علاقه آنها دور و به محتوایی نامناسب رهنمون می‌سازد، نگرانی‌های بسیار مهمی ایجاد کرده است که علی‌رغم محاسن آن، نیاز به قانون‌گذاری در این زمینه را تشدید می‌نماید.

مخاطره‌های مالی برای کودکان یا والدین، مراقبان یا سرپرستان آنها زمانی ممکن است رخ دهد که شیوه‌های بازاریابی مورد بحث در بالا بر کودکان تأثیر بگذارد و ناآگاهانه محصولات را از طریق آنها سفارش دهند. دستیارهای دیجیتال، برای خدماتی که نیاز به پرداخت‌های مکرر دارند به کار بگیرند، یا بدون اطلاع یا رضایت والدین یا مراقبان، مبالغ زیادی را برای محصولات یا خدمات خرج کنند.

مخاطره‌های مصرف‌کننده همچنین شامل ریسک‌های امنیتی است. کودکان ممکن است در محیط دیجیتال به دام بازی‌های رایگان، آهنگ‌های زنگ، یا سایر دریافت‌هایی که حاوی

بداًفزار هستند، شبکه‌های اجتماعی که توسعه‌دهندگان آنها دسترسی غیرمجاز به اطلاعات شخصی و متن، پیست الکترونیک دارند یا پیام‌های «فیشینگ» که ممکن است سرقت اطلاعات هویتی را تسهیل کنند، بیفتند. در دنیای فیزیکی، شیوه‌ها و مقرراتی برای محافظت از کودکان در برابر مخاطره‌های مصرف‌کننده، از جمله تبلیغات نامناسب با سن وجود، و امثالهم وجود دارد ولی این شیوه‌ها و مقررات باید به‌طور دقیق در محیط دیجیتال نیز توسعه داده شوند (Livingstone et al., 2016). در پاسخ به نظرسنجی OECD، به استثنای برخی موارد، تنها چند کشور گزارش کردند که قوانین آنها به‌طور خاص به مخاطره‌های مصرف‌کننده برای کودکان می‌پردازد (OECD, 2021). البته تلاش‌هایی در قالب توصیه‌های اجرایی محدودکننده توسط برخی نهادهای بین‌المللی برای خریدهای غیرمجاز در بازی‌های برخط تدوین شده است که در پیشگیری و کاهش چنین مخاطره‌هایی برای والدین مؤثر است.

نتیجه‌گیری

با توجه به دسته‌بندی مخاطره‌های پیش‌روی کودکان در فضای مجازی و تطبیق آن با مجموعه قوانین و مقررات داخلی و بین‌المللی، درمی‌یابیم که اگرچه واکنش قانون‌گذاران در کشورهای توسعه‌یافته به مراتب گسترده‌تر از مراجع قانونگذار داخلی است، بااین‌حال حتی قوانین وضع شده بین‌المللی نیز در موارد محدودی از حقوق کودکان در فضای مجازی حمایت می‌نماید. شاید بیش از هر چیز، سرعت رشد این فناوری و ظهور مصادیق جدید این مخاطره‌ها عامل این عقب‌ماندگی نهادهای قانون‌گذار باشد. این چالش در مورد قوانین و مقررات داخلی از دو وجه شدت بیشتری دارد. از یک‌سو بسیاری از مخاطره‌های شناسایی شده مانند مخاطره‌های مصرف‌کننده، تماسی و ارتباطی که حتی تجربیات موفق بین‌المللی دارد نیز در مجموعه قوانین و مقررات ایران مغفول مانده و تمرکز قوانین بر بخشی از مصادیق مخاطره‌های محتوایی استوار است. این امر باعث شده که خانواده‌ها و سایر نقش‌های مرتبط با کودک از جمله دولت، نهاد قضایی و ضابطان قوانین موجود نیز رفتار منسجمی در مواجهه با مصادیق نقض حقوق کودک نداشته باشند. حتی قوانین و مقررات داخلی ناظر بر مخاطره‌های محتوایی نیز

عمدتاً مبتنی بر قواعد مشابه محیط غیربرخط وضع شده است. از این رو تناسب ماهوی با فضای مجازی و اثربخشی لازم را ندارند. مصادیق قانونی موجود یا نظیر «مقررات صیانت از کودکان و نوجوانان در فضای مجازی» (مصوب ۱۴۰۰) توصیه‌گونه‌اند و ضمانت‌های اجرایی و جرم‌انگاری در خصوص آن انجام نشده است، یا مانند قانون حمایت از اطفال و نوجوانان (مصوب ۱۳۹۹) و قانون حمایت از کودکان و نوجوانان (مصوب ۱۳۸۱) تنها بر جنبه‌های محیط غیربرخط تأکید دارند و به‌ندرت مستقلاً به مخاطره‌های نقض حقوق کودکان در فضای مجازی پرداخته‌اند. حتی قوانینی همچون قانون جرایم رایانه‌ای (مصوب ۱۳۸۸) نیز که انتظار می‌رود در جرم‌انگاری جرایم رایانه‌ای در این حوزه بتواند راهگشا باشد، مقوله کودک و مقتضیات آن را چه از منظر عامل و چه قربانی اساساً لحاظ نکرده است.

از سوی دیگر مسئولیت قانون‌گذاری، برآوردن نیازها و رسیدگی به این مخاطره‌ها به وزارتخانه‌ها یا بخش‌هایی واگذار شده است که مسئول اعمال مجرمانه مشابه در دنیای واقعی هستند. این منجر به آن خواهد شد که مقتضیات فضای مجازی به‌عنوان یک فناوری بنیادین نادیده گرفته شود و این مفهوم که این فضایی است که از مرزهای قانونی سنتی عبور می‌کند، به‌درستی درک نگردد.

فهم صحیح «بدون مرز بودن فناوری اطلاعات و فضای مجازی» در قانون‌گذاری و اجرای قوانین این حوزه بسیار حائز اهمیت است. این انتظار که در فضای متکثر اعتقادات و باورهای مذهبی و اجتماعی دنیای دیجیتال، بتوان تنها بر اساس قوانین و مقرراتی که صرفاً منبعث از عقاید مذهبی و ملی باشند اقدام نمود، دشوار می‌نماید. همچنین عدم پیوستگی ساختار سیاسی حاکم بر ایران با نظام‌های بین‌المللی، تشدیدکننده این موضوع در بهره‌مندی از تجربه‌ها و قوانین جاری بین‌المللی در زمینه حمایت از حقوق کودکان است. عمده پلتفرم‌ها و شبکه‌های اجتماعی به شکل فراملی و تحت قوانین بین‌المللی فعالند. صرف حضور یک کاربر در دایره مجموعه‌ای از قوانین خاص غیرمتصل با بخش عمده‌ای از قوانین بین‌المللی ناظر بر این پلتفرم‌ها، تنها موجب می‌گردد که نه قوانین ملی حاکم بر کاربر اثربخش باشد و نه کاربر بتواند از ضمانت‌های قوانین بین‌المللی بهره‌مند

گردد. نتیجه آنکه کاربران به خصوص کودکان در فضای پلتفرم‌ها و شبکه‌های بین‌المللی حمایت قانونی خاصی ندارند.

بایستی توجه داشت که فناوری اطلاعات یک فناوری دوران‌ساز است. برخی محققان دوران تحول بشر را به عصر کشاورزی، صنعتی، اطلاعات و در ادامه مجازی تقسیم می‌کنند؛ لذا نمی‌توان انتظار داشت که قانون‌گذاری در چنین موضوعی که نیاز به دانش فرارشته‌ای، مطالعات چندتخصصی و مشارکت گسترده دارد، در بستر قانون‌گذاری عام حال حاضر تحقق یابد. تجربه‌های بین‌المللی نیز مؤید آن است که در این زمینه مجامع بین‌المللی مشترک و نهادهای تخصصی در بسیاری کشورها به صورت گسترده فعالند و مستمراً در خصوص تدوین و بازنگری قوانین، مقررات و آیین‌نامه‌های اجرایی اهتمام دارند. شکل‌گیری نهادهای تخصصی ملی تحت عنوان «مراکز اینترنت امنتر» در کشورهای همچون فرانسه، اتریش، فنلاند، دانمارک، کرواسی و ... عمدتاً با چنین دیدگاهی بوده است. همچنین می‌توان به نمونه‌هایی از همکاری‌های مشترک بین‌المللی در زمینه حمایت از حقوق کودکان برخط مانند حمایت برخط از کودکان اتحادیه بین‌المللی مخابرات (ITU) و ائتلاف ایمنی برخط کودکان در چهارچوب انجمن حاکمیت اینترنت (IGF) اشاره نمود.

منابع و مآخذ

- آی‌رتون، شریلین و پوزتی، جولی (۱۳۹۹)، *روزنامه‌نگاری، «اخبار جعلی» و دروغ‌رسانی: کتاب راهنمای آموزش روزنامه‌نگاری*، بی‌جا: انتشارات یونسکو.
- امامی، امید و احمدی، حدیث (۱۳۹۷)، *جرایم مبتنی بر نفرت. در اولین همایش بزرگ مطالعات و پژوهش‌های علمی علوم انسانی، مؤسسه قانون یار با حمایت معنوی دانشگاه آزاد اسلامی واحد کرمانشاه.*
- انصاری اصل، محمد و آرزومند، بهنام (۱۳۹۶)، *رویکرد سیاست کیفری ایران نسبت به جرایم مبتنی بر نفرت، کنفرانس پژوهش‌های نوین ایران و جهان در روان‌شناسی و علوم تربیتی حقوق و علوم اجتماعی.*
- ایسنا (۱۳۹۸، ۱۹ تیر)، *تصویب لایحه مبارزه با محتوای نفرت‌انگیز فضای مجازی در فرانسه؛*

<https://www.isna.ir/news/98041910260>

پالاش، افسانه (۱۳۹۴)، *مطالعه تطبیقی پدیده هرزه‌نگاری کودکان و نوجوانان در فضای مجازی (حقوق ایران و اسناد بین‌المللی)*، پایان‌نامه کارشناسی ارشد، دانشکده دانشگاه علامه طباطبائی، دانشکده حقوق و علوم سیاسی.

جواهری، غلامرضا؛ اسماعیلی، مهدی؛ حاجی‌تبار، فیروز و جائی، حسن (۱۳۹۹)، *هرزه‌نگاری سایبری: از مبانی نظری تا الگوهای واکنش کیفری، فصلنامه پژوهش حقوق کیفری*، ۱(۳۰)، ۱۷۳-۲۰۰.

حسینی، محمدرضا (۱۳۹۸)، *مسئولیت دولت‌ها و سازوکارهای صیانت از حقوق کودک در فضای مجازی. حقوق کودک*، ۴(۱)، ۳۳-۵۹.

دیجیاتو (۱۳۹۸)، ۲ اسفند، *لایک کردن محتوای نفرت‌انگیز یا افتراآمیز از این پس در سوئیس جرم محسوب می‌شود*.

<https://digiato.com/article/2020/02/21>

رفاعی، غزاله (۱۳۹۸)، *تبیین قلمرو نظارت دولت بر حقوق و تکالیف والدین کودک در نظام حقوقی ایران*، پایان‌نامه کارشناسی ارشد، دانشکده رفاه، دانشگاه گروه حقوق.

شهریاری احمدی، مرجان (۱۳۹۶)، *حمایت از حریم خصوصی کودک در فضای سایبر با تأکید بر اقدامات شورای اروپا*، پایان‌نامه کارشناسی ارشد، دانشکده دانشگاه علامه طباطبائی، دانشکده حقوق و علوم سیاسی.

صادقی، امین (۱۳۹۹)، *راهکارهای حقوقی صیانت از حریم خصوصی کودکان و نوجوانان در فضای مجازی با تأکید بر چالش‌های حقوقی*، پایان‌نامه کارشناسی ارشد، دانشکده دانشگاه آزاد اسلامی واحد اردبیل، دانشکده علوم انسانی.

علیزاده، مصطفی (۱۳۹۹)، *حریم خصوصی کودک از منظر حقوق ایران و کنوانسیون حقوق کودک*، پایان‌نامه کارشناسی ارشد، دانشکده دانشگاه علوم قضایی و خدمات اداری، دانشکده حقوق قضایی.

فرامرزیانی، پروانه؛ انصاری، باقر؛ سلطانی‌فر، محمد و مظفری، افسانه (۱۴۰۰)، *طراحی الگوی راهکارهای حمایت از حریم خصوصی کودکان در فضای مجازی، پژوهش‌های ارتباطی*، ۲۸(۱۰۶)، ۹-۳۰.

قاسمی نوروزآباد، ظریفه (۱۳۹۷)، *دولت و امنیت اخلاقی کودکان در فضای مجازی*، پایان‌نامه کارشناسی ارشد، دانشکده دانشگاه تهران، دانشکده حقوق و علوم سیاسی.

قدرتی، صادق (۱۳۹۸)، *حمایت کیفری از صغار با تأکید بر جرایم جنسی در فضای مجازی*، پایان‌نامه کارشناسی ارشد، دانشکده دانشگاه مازندران، دانشکده حقوق و علوم سیاسی.

قورچی بیگی، مجید و رضائیان کوچی، محمدرضا (۱۳۹۹)، *تحلیلی بر بایسته‌های سیاست کیفری بزه‌دیده‌مدار در جرایم ناشی از نفرت*، فصلنامه پژوهش حقوق کیفری، ۹ (۳۲)، صص. ۲۱۳-۲۴۴.

کاظم پوریان، سعید و عبدلی، سمانه (۲۰۱۷)، *سواد دیجیتال: راهکاری برای پوشش شکاف دیجیتال و پرورش شهروند دیجیتال*، سیاست‌نامه علم و فناوری، ۶ (۴)، صص. ۵۳-۶۴.

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

مجلس شورا (۱۳۷۲)، *قانون اجازه الحاق دولت جمهوری اسلامی ایران به کنوانسیون حقوق کودک*، بی‌جا: بی‌نا.

مجلس شورا (۱۳۸۲)، *قانون تجارت الکترونیکی*.

مجلس شورا (۱۳۸۸)، *قانون جرایم رایانه‌ای*.

مجلس شورا (۱۳۹۹)، *قانون حمایت از اطفال و نوجوانان*.

مجلس شورا (۱۳۸۱)، *قانون حمایت از کودکان و نوجوانان*.

مجلس شورا (۱۳۵۶)، *قانون مجازات تبلیغ تبیض نژادی*.

مجمع عمومی سازمان ملل متحد (۱۹۸۹)، *کنوانسیون حقوق کودک*.

محسنی، فرید (۱۳۹۰)، *سهم کودکان و نوجوانان از حمایت کیفری در فضای مجازی و*

حقیقی، آموزه‌های حقوق کیفری، ۱ (۱)، صص. ۱۳۷-۱۷۰.

نیکبختی، جواد (۱۳۹۷)، *بررسی مطابقت حقوق کیفری ایران با پروتکل حقوق کودک در مورد فروش، روسپیکری و هرزه‌نگاری کودکان*، پایان‌نامه کارشناسی ارشد، دانشکده دانشگاه دامغان، دانشکده علوم انسانی.

- Babür, Oset (2017, March 27), We've Heard All about Fake News—Now What? Retrieved July 21, 2022, from <https://www.harvardmagazine.com/2017/03/fake-news-solutions-berkman-klein>
- Byrne, Jasmina; & Burton, Patrick (2017), Children as Internet users: how can evidence better inform policy debate? *Journal of Cyber Policy*, 2(1), 39-52. <https://doi.org/10.1080/23738871.2017.1291698>
- El Asam, Aiman; & Samara, Muthanna (2016), Cyberbullying and the law: A review of psychological and legal challenges. *Computers in Human Behavior*, 65, 127-141. <https://doi.org/10.1016/j.chb.2016.08.012>
- EU. General Data Protection Regulation (2016).
- European Commission (2022, April 23), DSA: Commission welcomes political agreement. Retrieved July 21, 2022, from https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545
- FTC (2020, August), Staff Perspective Paper on Loot Box Workshop. Retrieved July 21, 2022, from <http://www.ftc.gov/reports/staff-perspective-paper-loot-box-workshop>
- ICPEN (2020), *Best Practice Principles for Marketing Practices directed towards Children Online*. International Consumer Protection Enforcement Network.
- ILO (2017, September 19), 40 million in modern slavery and 152 million in child labour around the world. Retrieved July 21, 2022, from http://www.ilo.org/global/about-the-ilo/newsroom/news/WCMS_574717/lang--en/index.htm
- ITU; & UNICEF (2015), *Guidelines for Industry on Child Online Protection*. International Telecommunication Union (ITU) and United Nations Children's Fund (UNICEF).
- Livingstone, Sonia (2019, June 27), Revenge pornography and online hate content: the evidence underpinning calls for regulating online harms in the UK.
- Livingstone, Sonia; Byrne, Jasmina; & Carr, John. (2016). *One in Three: Internet Governance and Children's Rights* (p. 37). UNICEF Office of Research - Innocenti.
- Livingstone, Sonia; Lievens, Eva; & Carr, John (2020), *Handbook for policy makers on the rights of the child in the digital environment*. Council of Europe.
- National Literacy Trust (2018), *Fake news and critical literacy The final report of the Commission on Fake News and the Teaching of Critical Literacy in Schools*. National Literacy Trust.
- OECD (2020), *Combating COVID-19 disinformation on online platforms*.
- OECD (2021), *Children in the digital environment: Revised typology of risks*.
- Ofcom (2021, July 13), Children and parents: media use and attitudes report 2020/21. Retrieved July 21, 2022, from <https://www.ofcom.org.uk/research-and-data/media-literacy-research/childrens/children-and-parents-media-use-and-attitudes-report-2021>.

- Smahel, David; MacHackova, Hana; Mascheroni, Giovanna; Dedkova, Lenka; Staksrud, Elisabeth; Olafsson, Kjartan; Livingstone, Sonia; & Hasebrink, Uwe (2020), *EU Kids Online 2020: survey results from 19 countries*. London School of Economics and Political Science.
- UNICEF (ed.) (2017), *Children in a digital world*. UNICEF.
- US Congress. Children's Internet Protection Act (2003).
- van der Hof, Simone (2017), I Agree... Or Do I? A Rights-Based Analysis of the Law on Children's Consent in the Digital World. *Wisconsin International Law Journal*, 34(2), 409-445.
- Vosloo, Steven (2021, August 24), Digital misinformation / disinformation and children | UNICEF Office of Global Insight & Policy. Retrieved July 21, 2022, from <https://www.unicef.org/globalinsight/stories/digital-misinformation-disinformation-and-children>.