سن دیجیتال و قوانین کیفری در مواجهه با سوءاستفاده‌های سایبری از کودکان و نوجوانان

وحید کیومرثی
مدرس دانشگاه، گروه حقوق جزا و جرم‌شناسی، دانشگاه آزاد اسلامی تهران، تهران، ایران.
vahid.kiomarsi@iau.ac.ir

چکیده

در دنیای امروز، ورود سریع کودکان و نوجوانان به فضای مجازی فرصت‌های آموزشی و اجتماعی فراوانی ایجاد کرده اما تهدیدهای جدی نیز به همراه داشته است. این تهدیدها شامل آزار و بهره‌کشی جنسی آنلاین، سوءاستفاده تجاری، تشویق به رفتارهای پرخطر و آزار سایبری است. این شرایط، ضرورت نقش‌آفرینی نظام حقوق کیفری را در حفاظت از این گروه سنی دوچندان کرده است. پژوهش حاضر به بررسی توان نظام کیفری ایران در مقابله با سوءاستفاده‌های سایبری از کودکان و نوجوانان می‌پردازد و سعی دارد میزان انطباق آن را با چالش‌های عصر دیجیتال ارزیابی کند. با استفاده از روش توصیفی-تحلیلی و منابعی چون قوانین داخلی، اسناد بین‌المللی و رویه قضایی، این تحقیق نشان می‌دهد که با وجود قوانینی مانند قانون جرایم رایانه‌ای و قانون حمایت از اطفال و نوجوانان، هنوز نقایص جدی در حیطه جرم‌انگاری، نظارت بر پلتفرم‌های اینترنتی و برخورد با پیچیدگی‌های فنی فضای دیجیتال وجود دارد. از یافته‌های کلیدی این پژوهش ضرورت اصلاح قوانین، تدوین دستورالعمل‌های روشن قضایی، ارتقای مسئولیت‌پذیری نهادهای نظارتی و تقویت آگاهی حقوقی دیجیتال است. در مجموع، پژوهش تاکید می‌کند که حمایت کیفری مؤثر از کودکان در فضای مجازی نیازمند بازنگری همه‌جانبه و هماهنگی بین ساختارهای قانونی و فناوری‌های نوین است.

کلید واژه: سن دیجیتال، سوءاستفاده از کودکان، حقوق کیفری، قانون جرایم رایانه‌ای، جرایم سایبری.

مقدمه

گسترش فناوری‌های نوین ارتباطی و دسترسی آسان به ابزارهای دیجیتال، چهره‌ی زندگی بشر در قرن بیست‌ویکم را به‌گونه‌ای بنیادین دگرگون ساخته است. در این میان، کودکان و نوجوانان به عنوان بخشی از جمعیت دیجیتال‌زاده، بیش از هر گروه دیگری در معرض تحولات فضای مجازی قرار گرفته‌اند. ورود زودهنگام به دنیای آنلاین، گرچه فرصت‌هایی بی‌نظیر برای یادگیری، خلاقیت و ارتباط فراهم کرده، اما هم‌زمان آنان را در معرض طیف گسترده‌ای از تهدیدها و آسیب‌های نوظهور قرار داده است؛ از جمله آزار جنسی آنلاین، سوءاستفاده از تصاویر و اطلاعات شخصی، بهره‌کشی تجاری، ترغیب به رفتارهای خطرناک، و مشارکت ناخواسته در فعالیت‌های مجرمانه.

در چنین فضایی، ضرورت بازاندیشی در نقش نظام حقوق کیفری در حمایت از کودکان و نوجوانان در برابر جرایم سایبری بیش از پیش احساس می‌شود. قوانین سنتی، اغلب مبتنی بر جرایم عینی و فیزیکی طراحی شده‌اند، در حالی که در دنیای دیجیتال، مرز میان قربانی و فضا، میان کنش و پیام، و میان واقعیت و توهم، به‌شدت کمرنگ شده است. این پرسش اصلی مطرح می‌شود که آیا نظام کیفری ایران قادر است در قالب قواعد موجود، پاسخ مؤثر و متناسبی به تهدیدهای نوین علیه کودکان در فضای سایبری بدهد یا نیازمند بازسازی تقنینی و ساختاری است؟

هدف از این مقاله، بررسی تطبیقی و انتقادی قوانین کیفری مرتبط با سوءاستفاده‌های سایبری از کودکان و نوجوانان در نظام حقوقی ایران، شناسایی کاستی‌ها و چالش‌ها، و ارائه پیشنهادهایی برای ارتقاء سطح حمایت کیفری در برابر این جرایم است. برای دستیابی به این هدف، مقاله در چهار بخش تنظیم شده است: در بخش نخست، مفاهیم کلیدی چون «سوءاستفاده سایبری»، «سن دیجیتال» و ویژگی‌های قربانی‌شونده کودکان تبیین می‌شود. در بخش دوم، انواع جرایم سایبری علیه کودکان با تمرکز بر بسترهای وقوع آن تحلیل می‌گردد. بخش سوم به بررسی وضعیت قوانین کیفری ایران اختصاص دارد و در نهایت، در بخش چهارم، پیشنهادهایی برای اصلاح و تکمیل چارچوب کیفری موجود ارائه می‌شود. نتایج اولیه پژوهش نشان می‌دهد که علی‌رغم وجود برخی مقررات حمایتی نظیر قانون حمایت از اطفال و نوجوانان (۱۳۹۹) و قانون جرایم رایانه‌ای (۱۳۸۸)، چارچوب کیفری ایران در حوزه سوءاستفاده‌های سایبری از کودکان با خلأهایی نظیر نبود جرم‌انگاری خاص در برخی مصادیق، ضعف در پیش‌بینی ابزارهای پیشگیری، و فقدان سازوکارهای نظارتی بر پلتفرم‌ها مواجه است. همچنین برخی موانع اجرایی و فرهنگی موجب می‌شود که در عمل، حمایت کیفری از این قشر آسیب‌پذیر با دشواری‌هایی روبه‌رو گردد. نوآوری پژوهش حاضر در آن است که با تلفیق رویکرد حقوق جزای سنتی و مسائل نوظهور فضای دیجیتال، به‌صورت خاص بر گروه سنی کودکان و نوجوانان تمرکز کرده و با نگاهی انتقادی، خلأها و نارسایی‌های تقنینی موجود را در سطح جزئی و مصداقی شناسایی و تحلیل می‌کند. همچنین با بهره‌گیری از تجربه نظام‌های حقوقی پیشرو، چارچوبی پیشنهادی برای به‌روزرسانی پاسخ کیفری ایران ارائه می‌دهد.

۱- مفهوم سن دیجیتال

با گسترش فناوری‌های ارتباطی، مفهومی نو به‌نام «سن دیجیتال» وارد ادبیات اجتماعی و حقوقی شده که به نسل کودک و نوجوانی اشاره دارد که از بدو تولد با ابزارهای دیجیتال رشد یافته و بخش مهمی از زیست روزمره خود را در فضای مجازی تجربه می‌کند. در این مبحث، نخست تعاریف حقوقی مرتبط با مفاهیم «سن دیجیتال» و «کودک/نوجوان» مورد واکاوی قرار می‌گیرد و سپس به تبیین مفهوم «سوءاستفاده سایبری» از منظر حقوق جزا پرداخته می‌شود، تا بستر مفهومی مناسبی برای تحلیل‌های بعدی فراهم گردد.

۱-۱- تعریف «سن دیجیتال» و «کودک/نوجوان» از منظر حقوقی

اصطلاح «سن دیجیتال[۱] » مفهومی نوپدید و میان‌رشته‌ای است که در اسناد حقوقی هنوز به‌صورت رسمی تعریف نشده، اما در ادبیات حقوق فناوری و مطالعات تطبیقی، به دوره‌ای از رشد فرد اشاره دارد که در آن تعامل مستمر و عمیق با فناوری‌های

---

[۱] Digital Age

دیجیتال، به‌ویژه اینترنت و رسانه‌های اجتماعی، نقش بنیادینی در شکل‌گیری هویت، روابط اجتماعی، سواد رسانه‌ای و حتی حقوق و تکالیف فرد ایفا می‌کند. این مفهوم بیش از آن‌که سن تقویمی خاصی را دربر گیرد، به ویژگی‌های نسلی، دسترسی زودهنگام به فضای سایبر و استفاده فراگیر از فناوری اشاره دارد.[۲]

از سوی دیگر، تعاریف «کودک» و «نوجوان» در منابع حقوقی داخلی و بین‌المللی دارای مرزهای مشخص‌تری هستند. در نظام حقوقی ایران، بر اساس قانون حمایت از اطفال و نوجوانان (مصوب ۱۳۹۹)، کودک به فرد زیر ۱۸ سال اطلاق می‌شود و اصطلاح «نوجوان» بدون تعریف مستقل، غالباً در بازه سنی ۱۵ تا ۱۸ سال مورد استفاده قرار می‌گیرد. این تعریف با ماده ۱ کنوانسیون حقوق کودک سازمان ملل متحد (CRC) نیز هماهنگ است که کودک را فرد زیر ۱۸ سال معرفی می‌کند، مگر اینکه قانون ملی سن پایین‌تری برای بلوغ قانونی تعیین کرده باشد.[۳]

با توجه به این موارد، در این مقاله منظور از «کودک/نوجوان در سن دیجیتال»، افرادی زیر ۱۸ سال هستند که بخش قابل‌توجهی از تعاملات فردی، آموزشی، تفریحی و هویتی آنان در بستر فناوری‌های دیجیتال و فضای مجازی شکل می‌گیرد. این گروه نه‌تنها از نظر سنی در زمره افراد آسیب‌پذیر قرار دارند، بلکه در محیطی زندگی می‌کنند که تهدیدها و فرصت‌های دیجیتال، رفتارها و مخاطرات خاص خود را برای آن‌ها ایجاد کرده است؛ امری که مستقیماً ضرورت توجه نظام کیفری به ویژگی‌های خاص این نسل را مطرح می‌کند.

۱-۲- تبیین «سوءاستفاده سایبری» در بستر حقوق جزا

«سوءاستفاده سایبری» در بستر حقوق جزا، مفهومی است که به بهره‌برداری غیرقانونی، مکارانه یا فریب‌کارانه از امکانات و ساختارهای فضای سایبری علیه حقوق فردی یا حیثیت انسانی اشخاص، با توسل به وسایل الکترونیکی یا فناوری‌های دیجیتال اطلاق می‌شود؛ به‌گونه‌ای که این رفتار در چارچوب عنصر قانونی جرم قرار گیرد و موجب مسئولیت کیفری فاعل گردد.

در این تعریف، سه عنصر اصلی قابل شناسایی است: نخست، رفتار مداخله‌گرانه مرتکب که با قصد بهره‌برداری از آسیب‌پذیری دیجیتالی قربانی صورت می‌گیرد؛ دوم، بهره‌برداری با سوءنیت که ممکن است جنبه مالی، جنسی، روانی یا حیثیتی داشته باشد؛ و سوم، بهره‌برداری از بستر سایبری، به این معنا که جرم نه در فضای فیزیکی بلکه از طریق فناوری‌های متصل به شبکه، مانند اینترنت، پلتفرم‌های ارتباطی یا نرم‌افزارهای دیجیتال، واقع می‌شود.[۴]

سوءاستفاده سایبری زمانی قابلیت تعقیب کیفری می‌یابد که رفتار ارتکابی واجد وصف مجرمانه باشد، یعنی قانون‌گذار به‌طور مشخص آن را جرم‌انگاری کرده باشد و عناصر سه‌گانه جرم (قانونی، مادی و معنوی) در آن جمع باشد. این مفهوم در مقام یک رفتار کیفری، نه‌فقط به نقض قوانین ارتباطات الکترونیکی، بلکه به نقض حق قانونی اشخاص برای حفظ تمامیت جسمی، روانی، حیثیتی یا اطلاعاتی در فضای مجازی بازمی‌گردد و دقیقاً در همین نقطه است که مرز میان تخلف دیجیتال و جرم سایبری ترسیم می‌شود.[۵] از نظر نگارنده، سوءاستفاده سایبری در حقوق جزا، نه صرف هرگونه استفاده از فضای دیجیتال، بلکه استفاده‌ای است که بر بستر نقض آگاهانه حقوق غیر در چارچوب ابزارهای سایبری و با تحقق ارکان قانونی جرم، صورت می‌پذیرد.

۲- انواع جرایم سایبری علیه کودکان و نوجوانان

در جهان دیجیتال امروز، کودکان و نوجوانان به‌عنوان کاربران فعال فضای مجازی، در معرض انواع آسیب‌ها و تهدیدات سایبری قرار دارند که برخی از آن‌ها واجد وصف کیفری و قابل تعقیب در نظام حقوق جزا هستند. جرایم سایبری علیه این گروه‌های

---

[2] Frame, Alexander, Interculturalities in the Digital Age, (EPISTÉMÈ, 2025), 33:1, 15-21.

[۳] السان، مصطفی، حقوق فضای مجازی، (تهران: انتشارات شهر دانش، ۱۴۰۲)، ۶۷.

[۴] Wall, David S, "Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime." Information, Communication & Society, (2008) 11.6, 861.

[۵] Sabillon, Regner, et al., "Cybercrime and cybercriminals: A comprehensive study." (International Journal of Computer Networks and Communications Security,2016), 4 (6), 297.

سنی، از آنجا که متوجه حیثیت، امنیت روانی، سلامت جسمی یا آزادی‌های فردی آنان است، دارای ویژگی‌هایی متمایز از جرایم مشابه علیه بزرگسالان‌اند. در این مبحث، تلاش می‌شود با تکیه بر اسناد ملی و بین‌المللی، مهم‌ترین انواع جرایم سایبری ارتکابی علیه کودکان و نوجوانان شناسایی و طبقه‌بندی شده، و ویژگی‌های کیفری هر دسته مورد تحلیل قرار گیرد. این تحلیل، گامی اساسی در جهت شناسایی خلأهای تقنینی و تقویت حمایت‌های کیفری ویژه از آسیب‌پذیرترین اقشار جامعه در بستر دیجیتال محسوب می‌شود.

۲-۱- جرایم جنسی آنلاین

جرایم جنسی آنلاین[۶] علیه کودکان و نوجوانان، یکی از پیچیده‌ترین و خطرناک‌ترین اشکال سوءاستفاده سایبری محسوب می‌شوند که ماهیتاً ترکیبی از رفتارهای سنتی مجرمانه با ابزارها و بسترهای فناوری نوین‌اند. این جرایم در بستر فضای دیجیتال رخ می‌دهند و به طور خاص متوجه تعرض به سلامت جنسی، حیثیت و کرامت انسانی کودک یا نوجوان‌اند؛ افرادی که به‌واسطه سن و وضعیت رشد ذهنی، از حمایت‌های ویژه کیفری برخوردارند.

در این دسته از جرایم، عنصر مادی معمولاً از طریق رفتارهایی مانند ارسال، تولید، توزیع یا نگهداری تصاویر و محتوای جنسی مرتبط با کودکان، برقراری ارتباط آنلاین با انگیزه تحریک یا اغوای جنسی کودک، فریب دیجیتالی برای کسب رضایت ظاهری کودک به ارتکاب اعمال جنسی، یا حتی تشویق به رفتارهای خودآزارانه با زمینه جنسی تحقق می‌یابد. پلتفرم‌های ارتباطی نظیر شبکه‌های اجتماعی، برنامه‌های پیام‌رسان رمزگذاری‌شده، اتاق‌های گفت‌وگوی خصوصی، یا بازی‌های آنلاین تعاملی به عنوان ابزارهای ارتکاب این جرایم مورد استفاده قرار می‌گیرند و با توجه به ماهیت غیرحضوری این فضا، مرتکب اغلب با بهره‌گیری از ناشناسی یا جعل هویت، به جذب قربانی اقدام می‌کند.[۷]

عنصر معنوی این جرایم مبتنی بر قصد مجرمانه آگاهانه و مشخص نسبت به تعرض به حریم جنسی کودک است؛ به این معنا که مرتکب، ضمن اشراف به سن قربانی، به‌عمد در پی ارضای امیال جنسی یا کنترل روانی قربانی از طریق بهره‌برداری جنسی است. حتی در مواردی که اعمال ارتکابی به ظاهر فاقد تماس فیزیکی هستند، نظیر ارسال درخواست‌های نامتعارف، تشویق به ارسال تصاویر خصوصی یا تحریک کلامی مستمر، عنصر معنوی جرم همچنان محقق بوده و نظام کیفری، به‌ویژه در اسناد بین‌المللی مانند «کنوانسیون بوداپست» و «پروتکل اختیاری حقوق کودک درباره فروش، فحشا و پورنوگرافی کودکان»، این افعال را در زمره رفتارهای کیفری قابل پیگرد طبقه‌بندی می‌کند.[۸]

۲-۲- آزار سایبری[۹]

آزار سایبری به‌عنوان یکی از مصادیق بارز خشونت روانی در فضای دیجیتال، مفهومی است که به رفتارهای عمدی، تکرارشونده و خصمانه‌ای اطلاق می‌شود که با بهره‌گیری از ابزارهای ارتباطی آنلاین، علیه یک فرد، به‌ویژه کودکان و نوجوانان، صورت می‌گیرد و هدف آن تحقیر، تهدید، توهین، بی‌آبرو کردن، طرد اجتماعی یا آسیب روانی به قربانی است. این پدیده در تقاطع فناوری، روابط انسانی و حقوق کیفری قرار دارد و از آن‌رو که عموماً در محیط‌های غیرقابل کنترل مانند شبکه‌های اجتماعی، گروه‌های پیام‌رسان یا حتی بسترهای آموزشی آنلاین رخ می‌دهد، شناسایی و مقابله حقوقی با آن با دشواری‌های خاصی همراه است.[۱۰]

از نظر نگارنده، عنصر مادی آزار سایبری می‌تواند اشکال مختلفی به خود بگیرد؛ از انتشار عمدی اطلاعات دروغ یا تحقیرآمیز، ساختن پروفایل جعلی برای تمسخر، تهدید به افشای تصاویر خصوصی، ارسال مکرر پیام‌های توهین‌آمیز یا تهدیدآمیز، تا تشویق

---

[6] Online Child Sexual Abuse/Exploitation

[7] Wijakusumariasih, I. P. N, "Legal Protection For Children Against Online Sexual Exploitation and Abuse of Children." Jurnal Magister Hukum Udayana (Udayana Master Law Journal) (2003), 8, 4.

[8] Ibd, 11.

[۹] Cyberbullying

[۱۰] مشیراحمدی، علیرضا، "تحلیل جرم‌شناختی جرایم سایبری." دوفصل نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)، ۸، ۱(۱۳۹۸)، ۵۲.

به انزوای اجتماعی قربانی در فضای مجازی. آنچه این رفتارها را از سایر اشکال ناسازگاری در فضای آنلاین متمایز می‌سازد، عنصر تکرار و استمرار آن‌ها، و همچنین قصد مشخص مرتکب در تحقیر یا آسیب رساندن به شخصیت یا سلامت روانی قربانی است. این رفتارها ممکن است در نگاه نخست جنبه فیزیکی یا ملموسی نداشته باشند، اما اثرات آن‌ها اغلب عمیق‌تر از خشونت فیزیکی و در بسیاری موارد، منجر به افسردگی، اضطراب شدید، فرار از خانه، خودزنی یا حتی خودکشی در میان کودکان و نوجوانان می‌شود.

آزار سایبری واجد ویژگی‌های خاصی است که آن را از سایر جرایم افتراقی می‌سازد. نخست، عنصر مکان وقوع که در بستر فضای مجازی است و از لحاظ صلاحیت قضایی، تعقیب کیفری را با پیچیدگی‌هایی مواجه می‌سازد. دوم، چالش در احراز هویت مرتکب به دلیل امکان استفاده از حساب‌های جعلی یا بسترهای رمزنگاری‌شده. سوم، صدمه‌ای که غالباً ماهیت روانی دارد و اثبات آن در چارچوب قواعد سنتی اثبات جرم با دشواری‌هایی همراه است.[۱۱]

در اسناد بین‌المللی، مانند «راهنمای مبارزه با خشونت علیه کودکان در فضای مجازی» منتشر شده توسط یونیسف، آزار سایبری به‌عنوان شکلی نوین از خشونت علیه اطفال به رسمیت شناخته شده و توصیه‌هایی برای جرم‌انگاری مستقل آن ارائه شده است. در حقوق داخلی ایران، اگرچه آزار سایبری به‌صورت مستقل جرم‌انگاری نشده، اما با استفاده از مقررات عمومی‌تر مانند ماده ۱۷ قانون جرایم رایانه‌ای (مصوب ۱۳۸۸) در خصوص انتشار محتوای توهین‌آمیز یا هتاکانه، یا مواد مربوط به تهدید، توهین، افترا و نشر اکاذیب در قانون مجازات اسلامی، امکان تعقیب کیفری برخی مصادیق آن وجود دارد. با این حال، فقدان تعریف قانونی صریح، نبود سازوکار حمایتی مؤثر برای قربانیان خردسال و ناتوانی ساختار قضایی در پاسخ‌گویی سریع به این دسته از جرایم، موجب شده است که آزار سایبری، به‌رغم آثار ویرانگرش، در بسیاری موارد بدون پاسخ کیفری مؤثر باقی بماند.[۱۲] به همین سبب، ضرورت شناسایی آن به‌عنوان جرم مستقل با تعریف دقیق، تعیین ضمانت اجراهای خاص و پیش‌بینی نهادهای حمایتی، به‌ویژه در قبال کودکان و نوجوانان، در حقوق کیفری نوین به شدت احساس می‌شود.

۲-۳- جنبه کیفری توهین، تهدید، نشر اکاذیب در فضای مجازی

در فضای حقوق کیفری، وقوع جرایمی مانند توهین، تهدید و نشر اکاذیب در محیط مجازی، واجد همان ارکان کلاسیک جرم (عنصر قانونی، مادی و معنوی) است؛ اما شکل و شدت آن‌ها، به واسطه ماهیت خاص بستر سایبری، دچار تحول مفهومی و عملیاتی شده‌اند. ویژگی‌هایی چون ناشناسی[۱۳]، گستره دسترسی عمومی، سرعت انتشار و دشواری در شناسایی فاعل، نه‌تنها کشف جرم را پیچیده‌تر می‌سازد، بلکه آثار مجرمانه را تشدید کرده و از منظر جرم‌شناختی، نیازمند واکنش کیفری خاص می‌گردد. توهین سایبری: زمانی محقق می‌شود که شخصی با استفاده از ابزارهای دیجیتال (نظیر پیام‌رسان‌ها، شبکه‌های اجتماعی، وب‌سایت‌ها و یا حتی ایمیل‌ها) الفاظ یا تصاویری منتشر کند که واجد بار توهین‌آمیز علیه حیثیت و آبروی شخص دیگری باشد. برخلاف فضای فیزیکی که توهین در حضور مخاطب رخ می‌دهد، در فضای سایبری، توهین می‌تواند از طریق انتشار عمومی در بستری غیرحضوری صورت گیرد.[۱۴] همین امر باعث می‌شود عنصر علنی بودن - که در قانون مجازات اسلامی برای برخی مصادیق موجب تشدید مجازات است - با شدت بیشتری محقق شود. همچنین، ظهور مفاهیمی همچون «میم‌های تحقیرآمیز»، «هشتگ‌های توهین‌آمیز» و «تگ کردن قربانی در محتوای مجرمانه»، مصادیق نوینی از توهین را به وجود آورده‌اند که از دید قانون‌گذار سنتی مغفول مانده‌اند.

---

[۱۱] عطازاده، سعید و همکاران، هرزه‌نگاری سایبری علیه کودکان در سیاست جنایی تقنینی ایران با نگاهی به حقوق انگلستان. پژوهش های اطلاعاتی و جنایی, ۱۶/۶۳ (۱۴۰۰)، ۱۲۴.

[۱۲] زمانی جباری، افسانه و پژوهش جهرمی، امین، "مبانی جرم‌انگاری جرایم سایبری مجازی." دوفصل نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)، ۷، ۲(۱۳۹۸)، ۹.

[13] Anonymity

[14]Brenner, Susan W, Cybercrime: criminal threats from cyberspace, (Bloomsbury Publishing USA, 2010), 16-18.

تهدید سایبری: در قالب تهدید به ارتکاب جرم علیه جان، مال، حیثیت یا آبروی مخاطب یا بستگان وی، زمانی در فضای مجازی تحقق می‌یابد که این تهدید از طریق پیام‌رسان‌ها، ایمیل یا سایر ابزارهای دیجیتال انجام شود و قابلیت ایجاد خوف یا نگرانی واقعی در مخاطب را داشته باشد. در این فضا، تهدیدکننده می‌تواند از هویت‌های مجازی استفاده کند، از داده‌های شخصی قربانی سوءاستفاده کرده یا حتی با ابزارهایی چون فتوشاپ، تصاویر ساختگی تهیه و تهدید به انتشار آن‌ها کند. تهدید سایبری گاه در قالب جرایم ترکیبی همچون «باج‌گیری دیجیتال»[۱۵] یا «اخاذی اینترنتی» رخ می‌دهد و با توجه به آسیب روانی مستمر وارد بر قربانی، می‌تواند در زمره جرایم مستمر و پیچیده قرار گیرد.[۱۶]

نشر اکاذیب در فضای مجازی: به معنای انتشار عمدی اطلاعات دروغ و بی‌اساس درباره‌ی شخص حقیقی یا حقوقی با هدف اضرار به آبرو یا حیثیت اجتماعی وی است. این جرم ممکن است در قالب انتشار پست‌های دروغین در شبکه‌های اجتماعی، ارسال پیام‌های ساختگی یا تهیه محتوای جعلی در رسانه‌های دیجیتال تحقق یابد. در این فضا، ساختن اکانت‌های جعلی، تولید محتواهای جعلی و گسترش اطلاعات بی‌پایه از طریق الگوریتم‌های پلتفرم‌ها، ابعاد تازه‌ای از جرم را شکل می‌دهد که قابلیت کنترل آن از سوی قانون‌گذار سنتی دشوار است. تفاوت فضای دیجیتال با فضای سنتی در این است که در اولی، نشر اکاذیب ممکن است در عرض چند ثانیه به دست هزاران نفر برسد و آثار آن به شکل غیرقابل جبرانی گسترده شود.[۱۷] در تمام این موارد، ارکان قانونی از طریق مواد قانون مجازات اسلامی و قانون جرایم رایانه‌ای قابل پیگیری هستند؛ اما چالش‌های موجود در عنصر مادی (نحوه ارتکاب در بستر غیرحضوری، ابزارهای فنی و دیجیتال) و عنصر روانی (احراز سوء نیت عام و خاص در محیطی که شفافیت ارتباط محدود است)، بررسی‌های دقیق فنی، قضایی و جرم‌شناختی را ضروری می‌سازد.

۲-۴- بهره‌برداری مالی یا تجاری

بهره‌برداری مالی یا تجاری از کودکان در فضای سایبری، یکی از اشکال پیچیده و در حال گسترش سوءاستفاده سایبری است که با استفاده از خلأهای قانونی و عدم رعایت الزامات سن دیجیتال صورت می‌گیرد. این نوع سوءاستفاده عمدتاً از طریق پلتفرم‌های دیجیتال و شبکه‌های اجتماعی انجام می‌شود و هدف اصلی آن تحصیل منافع مالی از طریق نمایش، تبلیغ، یا بهره‌کشی مستقیم یا غیرمستقیم از تصویر، صدای کودک، یا حتی فعالیت‌های او در فضای مجازی است. در اغلب موارد، این بهره‌برداری بدون رضایت آگاهانه و معتبر کودک یا والدین او انجام می‌شود، یا رضایتی ارائه می‌شود که از نظر حقوقی فاقد اعتبار است، زیرا کودک به علت سن و عدم بلوغ فکری و حقوقی قادر به تشخیص و ارزیابی پیامدهای تصمیم خود نیست.[۱۸]

این رفتارها ممکن است مصداق جرایمی چون «سوءاستفاده از طفل برای منافع اقتصادی»، «تهیه و انتشار محتوای زیان‌بار از کودک»، یا «نقض حق تصویر و حیثیت کودک» قرار گیرند. در برخی موارد نیز اگر بهره‌برداری با اجبار، اغوا یا فریب صورت گرفته باشد، می‌تواند مشمول عنوان مجرمانه «استثمار» یا حتی «سازمان‌یافتگی مجرمانه در فضای سایبر» شود. افزون بر این، مسئولیت کیفری شرکت‌های دیجیتال، پلتفرم‌های تبلیغاتی و والدینی که آگاهانه یا به‌صورت غفلت‌آمیز زمینه بهره‌برداری تجاری از فرزندان خود را فراهم می‌کنند، قابل طرح است.[۱۹]

به نظر نگارنده، نبود تعریف دقیق و الزام‌آور از «سن دیجیتال» و اختلاف آن با «سن بلوغ حقوقی» سبب می‌شود که کودکان بدون احراز کفایت سنی و عقلانی، در بسترهای تجاری یا تبلیغاتی ثبت‌نام کرده و تحت قراردادهایی قرار گیرند که از نظر اصول حمایت از کودک، فاقد مشروعیت و عدالت‌اند. این وضعیت، نقض صریح اصول کنوانسیون حقوق کودک سازمان ملل متحد و

---

[15] Cyber Blackmail

[16] Moore, Robert, Cybercrime: Investigating high-technology computer crime, (Routledge, 2014), 154.

[۱۷] استادي، سمیه و میری، حسین، "بررسی جرم نشر اکاذیب در فضای سایبر." مطالعات حقوق، ۸، ۳۴ (۱۴۰۲)، ۱۰۸.

[18]Lubis, A. R. (2024), The Kidfluencer Phenomenon and Modern Slavery: A Critical Analysis of Indonesia's Legal Framework in Protecting Children from Digital Exploitation. Arkus, 11, 1(2024), 772.

[19] Verdoodt, Valerie (2019), The Role of Children's Rights in Regulating Digital Advertising, publication in the International Journal of Children's Rights, 27, 3(2019), 10.

همچنین قواعد بنیادین سیاست کیفری حمایتی در قبال اطفال محسوب می‌شود. در نتیجه، توسعه قوانین کیفری که بهره‌برداری تجاری از کودک در فضای دیجیتال را جرم‌انگاری کند، از ضرورت‌های انکارناپذیر دوران معاصر است

۲-۵- جرایم مشارکتی یا ترغیبی

در عصر دیجیتال، یکی از پیچیده‌ترین اشکال جرایم سایبری علیه کودکان و نوجوانان، آن دسته از جرایمی است که به‌صورت غیرمستقیم و با تکیه بر نفوذ روانی، قربانی را به مشارکت در عمل مجرمانه یا آسیب‌رسانی به خود یا دیگران سوق می‌دهد. این دسته از جرایم که می‌توان آن‌ها را تحت عنوان «جرایم مشارکتی یا ترغیبی» طبقه‌بندی کرد، از منظر حقوق کیفری با چالش‌های عمیقی مواجه است؛ زیرا عنصر «تحریک» یا «اقناع» در آن، جایگزین اجبار و تهدید فیزیکی شده و بزه‌دیده به ظاهر، به اختیار خویش وارد فرآیند بزه می‌شود.

در این نوع از جرایم، رفتار مرتکب معمولاً مبتنی بر طراحی سناریوهای روانی دقیق، بهره‌گیری از الگوریتم‌های پلتفرمی، سوءاستفاده از الگوسازی اجتماعی، میل به پذیرش در گروه، و نیاز نوجوان به دیده‌شدن یا تعلق داشتن است. تأثیرگذاری روانی به نحوی انجام می‌شود که کودک یا نوجوان احساس می‌کند در برابر یک خواسته جمعی، الزامی برای پیروی دارد یا در نتیجه محرک‌های پیاپی، قدرت تمییز بین درست و غلط را از دست می‌دهد. اینجا، مفاهیمی چون «اراده» و «رضایت» در چارچوب حقوق کیفری نیازمند بازنگری هستند، زیرا در بسیاری از این موارد، قربانی از لحاظ فنی رضایت داده اما از منظر روانی و حقوقی، درک و آزادی لازم برای تصمیم‌گیری نداشته است.[۲۰]

یکی از نمونه‌های بارز این پدیده، چالش نهنگ آبی[۲۱] است که مراحل آن با اقداماتی ساده آغاز می‌شود؛ مانند بیدار ماندن تا نیمه‌شب، تماشای فیلم‌های ترسناک یا کشیدن تصاویر خاص، و در ادامه با خودزنی، بریدن بدن با تیغ، و نهایتاً اقدام به خودکشی به پایان می‌رسد. در طول این فرایند، قربانی به‌گونه‌ای برنامه‌ریزی‌شده تحت تأثیر قرار می‌گیرد که تصور می‌کند در یک بازی تعهدآور شرکت دارد و اگر مأموریت‌ها را انجام ندهد، با پیامدهایی از قبیل افشای اطلاعات شخصی، تنبیه مجازی یا طرد شدن از گروه مواجه خواهد شد. رفتار مرتکب در این سناریو نه با اجبار بلکه با «هدایت روانی» همراه است و پرسش اصلی این است که آیا این تأثیرگذاری، می‌تواند جایگزین عنصر «اکراه» یا «تحریک مستقیم» باشد؟ این پرسش در نظام‌های مختلف کیفری، پاسخ‌های متفاوتی دارد. برخی کشورها، رفتار تحریک‌کننده دیجیتال را در قالب «تحریک به خودکشی» یا «تشویق به ارتکاب جرم» تحت پیگرد قرار داده‌اند، اما این مسئله همچنان در حوزه دادرسی با چالش‌هایی چون اثبات رابطه سببیت بین رفتار ترغیبی و نتیجه مجرمانه روبه‌روست.[۲۲]

علاوه بر چالش نهنگ آبی، بازی‌ها و چالش‌هایی مانند «مومو»، «چالش اره»، یا موارد مشابه نیز در این چارچوب قرار می‌گیرند؛ جایی که از ابزارهای دیجیتال برای به‌راه انداختن زنجیره‌ای از رفتارهای پرخطر استفاده می‌شود، بدون اینکه تماس مستقیمی بین مرتکب و قربانی برقرار باشد. حتی در مواردی، فاعل جرم به‌صورت ناشناس عمل می‌کند و از پراکندگی جغرافیایی فضای سایبر بهره می‌برد تا قابل شناسایی نباشد. باید توجه داشت که ارتکاب چنین اعمالی بدون نیاز به تماس فیزیکی، بدون اجبار کلاسیک، و تنها از طریق ترغیب تدریجی و برنامه‌ریزی‌شده، نوعی مسئولیت کیفری مبتنی بر روان‌فریبی و تحریک مخرب ایجاد می‌کند. بنابراین، توسعه مفهومی در عناصر «عنصر معنوی» جرم، تعریف موسع از «سببیت روانی»، و تدوین قواعد خاص برای «مسئولیت کیفری در فضای مجازی» ضروری است تا این‌گونه رفتارها از خلأهای قانونی خارج شوند.[۲۳]

۳- تحلیل حقوق جزای ایران در مقابله با این جرایم

---

[20] Guinchard, Audrey (2008), "Cybercrime: The Transformation of Crime in the Information Age." Information, Communication & Society, 11, 7(2008), 1032.

[21] Blue Whale Challenge

[۲۲] حسینی، سجاد و رایجیان اصلی، مهرداد (۱۴۰۲)، "یادگیری رفتار مجرمانه در فضای سایبر،" مجلس و راهبرد، ۳۰، ۱۱۴(۱۴۰۲)، ۲۸۳.

[۲۳] Dannhauser, Thomas, Digitally Engineered Attention and Energy Theft via Psychological Manipulation, IEEE Technology and Society Magazine, 41, 2(2022), 68.

در این مبحث تمرکز بر واکاوی سازوکارهای تقنینی موجود در نظام کیفری ایران در قبال سوءاستفاده‌های دیجیتال از کودکان و نوجوانان خواهد بود. در این بخش، نخست به شناسایی مواد قانونی پراکنده و موجود در قوانین کیفری عام و خاص نظیر قانون مجازات اسلامی، قانون جرایم رایانه‌ای و قانون حمایت از کودکان و نوجوانان پرداخته می‌شود. سپس، نقاط قوت مقررات مزبور همچون جرم‌انگاری کلی پدیده کودک‌آزاری، حتی در بستر مجازی، و نیز شناسایی مصادیق نوپدید کودک‌آزاری آنلاین مورد تحلیل قرار می‌گیرد. در نهایت، خلأهای قانونی، از جمله فقدان تعریف دقیق از سوءاستفاده سایبری، عدم تطبیق برخی مقررات با تحولات فناوری، و نبود ضمانت اجراهای متناسب با سن و آسیب‌پذیری کودک، بررسی خواهد شد. این مبحث زمینه‌ای فراهم می‌کند برای ارزیابی کارآمدی ساختار کیفری ایران در برخورد با تهدیدات روبه‌گسترش عصر دیجیتال علیه حقوق کودکان.

۳-۱- بررسی مواد قانونی مرتبط

در حقوق کیفری ایران، مقابله با جرایم سایبری علیه کودکان و نوجوانان به‌واسطه وجود قوانین متعدد و پراکنده، هم فرصتی برای حمایت گسترده‌تر فراهم کرده و هم موجب چالش‌های جدی در تفسیر و اعمال مواد قانونی شده است. از منظر تحلیل مواد قانونی، می‌توان نقاط قوت و ضعف این نظام حقوقی را به تفصیل بررسی کرد.

قانون حمایت از اطفال و نوجوانان (۱۳۹۹) نقطه عطفی در نظام حقوقی ایران محسوب می‌شود، زیرا نخستین بار به‌طور خاص به حفاظت از کودکان در فضای مجازی توجه کرده است. ماده ۱ بند (ث) این قانون به‌صراحت «بهره‌کشی و سوءاستفاده از کودک در فضای مجازی» را جرم‌انگاری نموده است. این ماده نشان‌دهنده پیشرفت قابل توجهی نسبت به قوانین پیشین است و بر اهمیت توجه ویژه به فضای سایبری و مخاطرات آن برای کودکان تاکید دارد. با این حال، ابهاماتی در تعریف دقیق «سوءاستفاده در فضای مجازی» و محدوده شمول آن باقی است که می‌تواند منجر به تفسیرهای متفاوت و محدود شود.[۲۴]

در قانون جرایم رایانه‌ای (۱۳۸۸)، مواد متعددی به‌طور مستقیم یا غیرمستقیم با سوءاستفاده‌های سایبری علیه کودکان مرتبط هستند. به‌عنوان مثال، ماده ۱۴ که مربوط به «تولید، انتشار و ذخیره‌سازی محتوای مستهجن» است و همچنین ماده ۱۰ قانون حمایت از اطفال و نوجوانان، با توجه به تاکید تبصره آن بر محتوای مربوط به کودکان، یکی از ابزارهای مهم مقابله با جرایم جنسی آنلاین علیه کودکان به شمار می‌رود. این ماده نشان‌دهنده جرم‌انگاری صریح این نوع رفتارهاست، اما محدودیت‌هایی از حیث اثبات و دسترسی به مرتکبین در فضای بین‌المللی، چالش اصلی است. همچنین، ماده ۱۵ قانون مذکور که «تحریک یا ترغیب به ارتکاب جرم» را جرم‌انگاری کرده، قابلیت گسترده‌ای برای برخورد با چالش‌هایی مانند نهنگ آبی دارد؛ هرچند، در عمل اثبات رابطه سببیت میان تحریک و اقدام زیان‌بار کودک دشوار است و نیازمند تفسیر قضایی دقیق‌تر است.

قانون مجازات اسلامی (۱۳۹۲) مواد متعددی دارد که می‌تواند در موارد سوءاستفاده سایبری علیه کودکان به کار رود. ماده ۶۳۹ که به «تشکیل محفل فساد و فحشا» اشاره دارد، در موارد شبکه‌های سازمان‌یافته سوءاستفاده جنسی از کودکان، قابل استناد است. با این وجود، این ماده عمدتاً برای جرایم فیزیکی طراحی شده و در مواجهه با جرایم دیجیتال، تطبیق آن نیازمند توسعه قضایی است. مواد ۵۶۸ تا ۵۷۰ درباره نقض حریم خصوصی، در مواجهه با نشر تصاویر یا اطلاعات شخصی کودکان در فضای مجازی بسیار کاربردی‌اند؛ اما مجازات‌ها و ضمانت‌اجراهای آن‌ها اغلب بازدارندگی کافی ندارند.[۲۵]

نکته مهمی که در تحلیل این قوانین مشخص می‌شود، پراکندگی و عدم انسجام در تعاریف و مصادیق جرم است. فقدان تعریف دقیق و یکپارچه از مفاهیمی مانند «سوءاستفاده سایبری» و «سن دیجیتال» باعث می‌شود که برخورد قضایی دچار ناهماهنگی شود. علاوه بر این، خلأهای تقنینی در زمینه همکاری‌های بین‌المللی و امکانات فنی شناسایی مرتکبان فضای سایبر، اجرای

---

[۲۴] کلانتری، کیومرث و نصرالهی، ابوذر، "سیاست جنایی تقنینی ایران در قبال جرایم جنسی علیه کودکان و نوجوانان." نشریه: حقوق و سیاست، ۹، ۲۲(۱۳۸۶)، ۷۴.

[۲۵] اکبری، مسعود و قناد، فاطمه، "سیاست کیفری ایران در قبال اطفال و نوجوانان بزهدیده گردشگری جنسی." فصلنامه پژوهش حقوق کیفری، ۲، ۵(۱۳۹۲)، ۱۳۷.

قوانین را با مشکلات جدی مواجه کرده است. به‌علاوه، مقررات موجود، در برخورد با ویژگی‌های خاص کودکان و نوجوانان به‌عنوان گروه‌های آسیب‌پذیر و نیازمند حمایت ویژه، کمبودهایی دارد که می‌تواند منجر به ناکافی بودن حمایت کیفری شود.
با وجود وجود مواد قانونی متعدد که می‌توانند علیه سوءاستفاده‌های سایبری از کودکان به کار گرفته شوند، نیازمند اصلاحات اساسی، تدوین مقررات جامع‌تر و بروزتر، و تفسیر قضایی تخصصی‌تر برای پاسخگویی به چالش‌های نوین این حوزه هستیم. این امر مستلزم همکاری میان‌دستگاهی، استفاده از فناوری‌های نوین و تقویت ظرفیت‌های حقوقی و قضایی است تا حمایت مؤثر و مستمر از کودکان در فضای دیجیتال تحقق یابد.

۳-۲- تحلیل نقاط قوت

در نظام حقوق کیفری ایران، یکی از نقاط قوت مهم در مقابله با سوءاستفاده‌های سایبری از کودکان، جرم‌انگاری کلی و جامع سوءاستفاده از کودکان و همچنین شناسایی کودک‌آزاری در بستر آنلاین است. این نقطه قوت، به ویژه در پرتو تصویب قانون حمایت از اطفال و نوجوانان (۱۳۹۹) و اصلاحات مرتبط در قانون مجازات اسلامی و قانون جرایم رایانه‌ای نمود یافته است.
جرم‌انگاری کلی سوءاستفاده از کودکان در حقوق ایران: به معنای این است که هر گونه بهره‌کشی، آزار، تحقیر، تهدید، یا سوءاستفاده جنسی، مالی یا روانی از کودک به عنوان یک جرم مستقل و قابل تعقیب شناخته می‌شود، بدون آنکه لزوماً نیاز به تفصیل تمام مصادیق خاص وجود داشته باشد. این رویکرد کلی، امکان انطباق با انواع مختلف سوءاستفاده، حتی آن‌هایی که در فضای سایبری رخ می‌دهند، را فراهم می‌آورد. به طور خاص، ماده ۱۰ بند (پ) قانون حمایت از اطفال و نوجوانان، ضمن جرم‌انگاری صریح «سوءاستفاده از کودک در فضای مجازی و شبکه‌های اجتماعی»، محدوده گسترده‌ای برای شمول جرایم نوپدید دیجیتال ایجاد کرده است. این موضوع موجب می‌شود که حتی رفتارهای جدید و پیچیده سایبری، که در قوانین قدیمی‌تر به صورت مشخص نیامده‌اند، تحت پوشش قانون قرار گیرند.[۲۶]
شناسایی کودک‌آزاری آنلاین: به عنوان یک نوع خاص از کودک‌آزاری، از دیگر دستاوردهای مهم حقوق کیفری ایران است. ماده ۳ قانون حمایت از اطفال و نوجوانان، کودک‌آزاری را شامل هرگونه رفتار مخل به سلامت جسمی، روانی و اخلاقی کودک دانسته که شامل آزار و اذیت روانی، تهدید، تحقیر، و تحمیل رفتارهای پرخطر می‌شود. این تعریف، به رغم جامعیت در متون قانونی، به صورت ضمنی شامل کودک‌آزاری در فضای سایبری نیز می‌شود. در واقع، با توجه به رشد فناوری و گسترش استفاده کودکان از اینترنت و شبکه‌های اجتماعی، رویکرد قانونگذار ایران در این ماده، امکان انطباق مفاهیم سنتی کودک‌آزاری با شرایط دیجیتال را فراهم ساخته است.[۲۷]
یکی از نکات قوت این رویکرد کلی و جامع، قابلیت انعطاف آن در برابر پیشرفت‌های فناوری و ظهور جرایم نوظهور است. برخلاف قوانین محدود به مصادیق مشخص، جرم‌انگاری کلی امکان می‌دهد که با ظهور رفتارهای مجرمانه جدید در فضای سایبری، قانون‌گذار یا قاضی بتواند بدون نیاز به اصلاحات فوری، برخورد کیفری مناسب را اعمال نماید. به این ترتیب، خلأهای قانونی کمتری در حوزه حفاظت از کودکان در فضای مجازی ایجاد می‌شود. جرم‌انگاری کلی سوءاستفاده از کودکان و شناسایی کودک‌آزاری آنلاین موجب تسهیل تعقیب کیفری مرتکبان می‌گردد، چرا که نیازی به اثبات همه جزئیات دقیق رفتار مجرمانه خاص نیست و می‌توان به کلیت رفتار و آثار آن استناد کرد. این امر در دادگاه‌ها به ویژه در پرونده‌های فضای سایبری که اثبات جزئیات فنی و محتوایی دشوار است، می‌تواند تسهیل‌کننده باشد.[۲۸] در عین حال، این نقطه قوت مستلزم وجود تفسیر قضایی دقیق و استانداردهای کارشناسی علمی برای تعریف مرزهای سوءاستفاده و کودک‌آزاری در فضای مجازی است تا از تفسیرهای

---

[۲۶] عارفی ، مرتضی، شرح جامع قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹، (تهران: شرکت سهامی انتشار ۱۴۰۲)، ۳۵.
[۲۷] همان، ۴۸.
[۲۸] زینالی حمزه، "نوآوری های قانون «حمایت از کودکان و نوجوانان» و چالش های فراروی آن." نشریه: رفاه اجتماعی، ۲، ۷(۱۳۸۲)، ۶۴.

وسیع یا نامناسب جلوگیری شود. افزون بر این، حمایت‌های کیفری باید با حمایت‌های اجتماعی و روانشناسی همراه باشد تا اثربخشی کامل در پیشگیری و مقابله با آسیب‌های وارده حاصل گردد.

۳-۳- خلأها و چالش‌ها

در نظام حقوق کیفری ایران، علی‌رغم پیشرفت‌های قابل توجه در جرم‌انگاری سوءاستفاده‌های سایبری از کودکان و نوجوانان، خلأها و چالش‌های جدی متعددی وجود دارد که مانع تحقق کامل حمایت قانونی مؤثر از این گروه آسیب‌پذیر در فضای دیجیتال می‌شود. این خلأها را می‌توان در چند محور اصلی بررسی کرد:

اولین خلأ مهم، فقدان تعریف دقیق و منسجم از مفاهیم کلیدی مانند «سن دیجیتال»، «سوءاستفاده سایبری» و «کودک‌آزاری آنلاین» در متون قانونی است. در حالی که قانون حمایت از اطفال و نوجوانان (۱۳۹۹) و قانون جرایم رایانه‌ای (۱۳۸۸) به صورت کلی به سوءاستفاده و جرایم سایبری اشاره دارند، اما تعاریف مشخص و منسجمی که بتواند دامنه شمول قوانین را با توجه به پیچیدگی‌های فضای دیجیتال تعیین کند، وجود ندارد. این مسئله منجر به ابهام در تفسیر قضایی و اختلاف نظر میان کارشناسان و مجریان قانون می‌شود که از نظر کارایی حقوقی، نقطه ضعف مهمی به شمار می‌آید.

دومین چالش، پراکندگی و تشتت قوانین مرتبط است. قوانین متعددی از جمله قانون حمایت از اطفال و نوجوانان، قانون جرایم رایانه‌ای، قانون مجازات اسلامی و حتی برخی آیین‌نامه‌ها و مقررات جزئی، به موضوع سوءاستفاده‌های سایبری از کودکان پرداخته‌اند. این پراکندگی باعث می‌شود که در عمل، همکارهای بین‌دستگاهی و قضایی دچار سردرگمی و ناهماهنگی شود و پیگیری پرونده‌ها با مشکلات جدی مواجه گردد. نبود یک قانون جامع و یکپارچه در این زمینه، کارایی نظام کیفری را کاهش می‌دهد و باعث می‌شود مرتکبان جرایم سایبری از خلأهای قانونی بهره‌مند شوند.[۲۹]

سومین خلأ، ضعف ضمانت‌های اجرایی و ابزارهای فنی مقابله با جرایم سایبری است. گرچه مواد قانونی نسبتاً جامعی برای جرم‌انگاری سوءاستفاده از کودکان وجود دارد، اما اجرای مؤثر این مواد مستلزم فناوری‌های پیشرفته شناسایی و ردیابی مجرمان سایبری است که در ایران هنوز به اندازه کافی توسعه نیافته است. همچنین، کمبود تخصص فنی در مراجع قضایی و نیروهای انتظامی، روند تعقیب کیفری را کند و ناکارآمد می‌کند.[۳۰]

چهارمین مورد، ضعف در همکاری‌های بین‌المللی است. با توجه به ماهیت فرامرزی جرایم سایبری، همکاری بین‌المللی برای شناسایی و تعقیب مجرمان حیاتی است، اما مقررات و سازوکارهای عملیاتی برای این همکاری در حقوق ایران به اندازه کافی پیشرفته و کارآمد نیست. این امر موجب می‌شود بسیاری از جرایم سایبری علیه کودکان که از خارج کشور انجام می‌شود، بی‌پاسخ بماند.[۳۱]

به نظر نگارنده، نبود رویکردهای حمایتی تکمیلی و پیشگیرانه، مانند آموزش حقوقی و دیجیتال به کودکان، خانواده‌ها و معلمان، و نیز فقدان نظام حمایتی روانی و اجتماعی برای کودکان قربانی، باعث می‌شود حتی پس از وقوع جرم، آثار سوء آن کاهش نیابد. قوانین کیفری به تنهایی قادر به مقابله کامل با آسیب‌های این جرایم نیستند و باید در کنار آن‌ها سیاست‌های اجتماعی و فرهنگی تقویت شود. خلأها و چالش‌های موجود در قوانین ایران درباره سوءاستفاده‌های سایبری از کودکان، ضرورت اصلاحات ساختاری، تدوین قوانین جامع‌تر، افزایش ظرفیت‌های فنی و تخصصی و توسعه همکاری‌های بین‌المللی را به شدت برجسته می‌کند تا بتوان از حقوق کودکان در عصر دیجیتال به‌طور کامل و مؤثر حفاظت کرد.

---

[۲۹] صبح خیز، رضا، "چالش های حقوقی جرایم سایبری در نظام حقوق بین الملل و نظام حقوقی ایران." نشریه: پژوهش های اطلاعاتی و جنایی، ۱۰، ۳(۱۳۹۴)، ۱۲۴.

[۳۰] طهماسبی، جواد و شاهمرادی، خیرالله، چالش‌ها و خلأهای موجود در فرایند رسیدگی به جرایم سایبری، حقوقی دادگستری، ۸۲، ۱۰۴(۱۳۹۷)، ۹۹.

[۳۱] فرهادی آلاشتی، زهرا، برساخت قضائی کنترل جرایم سایبری کودکان و نوجوانان: به‌سوی ارائهٔ نظریه‌ای داده‌بنیاد، نشریه مطالعات حقوق کیفری و جرم شناسی، ۵۲، ۲(۱۴۰۱)، ۲۸۶.

۴- مسئولیت کیفری پلتفرم‌ها و اشخاص ثالث

در این مبحث به بررسی نقش و مسئولیت قانونی بازیگران کلیدی غیرمستقیم در وقوع و تداوم جرایم علیه کودکان و نوجوانان می‌پردازد. این موضوع اهمیت ویژه‌ای دارد، زیرا پلتفرم‌های دیجیتال مانند شبکه‌های اجتماعی، پیام‌رسان‌ها و سرویس‌های آنلاین به عنوان بستری برای ارتکاب سوءاستفاده‌های سایبری شناخته می‌شوند. همچنین، نقش اشخاص ثالث مانند ارائه‌دهندگان خدمات اینترنتی و شرکت‌های فناوری در پیشگیری، شناسایی و مقابله با این جرایم، محور اصلی تحلیل این مبحث است. در این بخش، به تحلیل چارچوب‌های حقوقی موجود، ظرفیت‌ها و محدودیت‌های مسئولیت کیفری این نهادها پرداخته می‌شود تا جایگاه قانونی آن‌ها در محافظت از حقوق کودکان در فضای دیجیتال روشن‌تر گردد.

۴-۱- جایگاه مسئولیت کیفری در فضای مجازی

مسئولیت کیفری در فضای مجازی به‌مثابه یکی از مباحث نوپدید حقوق کیفری، در پی پاسخ به این پرسش اساسی است که در بستر دیجیتال، چه زمانی و تحت چه شرایطی می‌توان فاعلان مستقیم و غیرمستقیم یک رفتار مجرمانه را مورد مؤاخذه قرار داد. این مفهوم متکی بر اصول کلاسیک حقوق جزا، از جمله اصل فردی بودن مسئولیت کیفری، اصل قانونی بودن جرم و مجازات و اصل ضرورت تقصیر است، اما در بستر مجازی به‌واسطه پیچیدگی‌های فناورانه، تعاملات چندلایه کاربران، و نقش میانجی‌گرانه پلتفرم‌ها، دستخوش تحولاتی مفهومی و اجرایی شده است.[۳۲]

در فضای مجازی، رفتارهای مجرمانه غالباً از طریق ساختارهای فنی پیچیده‌ای مانند رمزنگاری، هویت‌های ناشناس، و بسترهای فرامرزی رخ می‌دهند و در نتیجه، شناسایی عنصر مادی و عنصر روانی جرم، با دشواری‌های مضاعفی روبه‌رو است. این وضعیت، جایگاه مسئولیت کیفری را به چالش می‌کشد؛ چراکه هم‌زمان با بروز رفتار زیان‌بار، امکان تعقیب و شناسایی فاعل یا مباشر جرم به‌دلیل ماهیت غیرمادی فضای مجازی ممکن است محدود باشد. افزون بر آن، مسئولیت کیفری در فضای مجازی باید میان مسئولیت فردی کاربران، مسئولیت نهادهای تسهیل‌گر مانند پلتفرم‌ها، و نقش اشخاص ثالثی نظیر ارائه‌دهندگان خدمات اینترنتی یا میزبان‌های داده، تفکیک قائل شود.

به همین ترتیب، یکی از چالش‌های مهم، تعریف حدود و ثغور مسئولیت کیفری نهادهای غیرشخصی در فضای مجازی است. به‌رغم آن‌که اشخاص حقوقی نیز طبق قانون می‌توانند تحت شرایطی مسئولیت کیفری داشته باشند، اما تطبیق این مفهوم با پلتفرم‌های دیجیتال و تعیین مصادیق ترک فعل مؤثر یا تسهیل غیرمستقیم ارتکاب جرم، به ملاحظات حقوقی ویژه‌ای نیاز دارد. در چنین شرایطی، نظام کیفری با لزوم تدوین استانداردهایی مواجه است که هم مقتضیات حمایت از بزه‌دیدگان - به‌ویژه کودکان و نوجوانان - را تأمین کند و هم اصول بنیادین حقوق جزا نظیر شخصی بودن مسئولیت را مخدوش نسازد. بدین ترتیب، جایگاه مسئولیت کیفری در فضای مجازی، نیازمند تبیین‌هایی متناسب با تحولات فناورانه و با حفظ وفاداری به اصول حقوق کیفری است.[۳۳]

۴-۲- مسئولیت ارائه‌دهندگان خدمات اینترنتی و سوشال مدیا

ارائه‌دهندگان خدمات اینترنتی و سوشال مدیا، به دلیل نقش محوری خود در فراهم‌سازی بسترهای دیجیتال که کودکان و نوجوانان به‌طور گسترده از آن استفاده می‌کنند، مسئولیت‌های حقوقی و اخلاقی ویژه‌ای در قبال این گروه سنی و رعایت محدودیت‌های سنی دیجیتال دارند. این مسئولیت‌ها در چارچوب‌های حقوقی بین‌المللی، منطقه‌ای و ملی تعریف شده و بر حفاظت از حقوق کودکان، تضمین ایمنی آنها در فضای آنلاین و اجرای دقیق قوانین مربوط به سن دیجیتال متمرکز است. در ادامه، این مسئولیت‌ها با تأکید بر جنبه‌های حقوقی و بدون کلی‌گویی تشریح می‌شود.

---

[۳۲] رضوی فرد، بهزاد و موسوی، سید نعمت الله، مسئولیت کیفری در فضای سایبر در حقوق ایران، فصانامه پژوهش حقوق کیفری دانشگاه علامه طباطبایی، ۵، ۱۶(۱۳۹۵)، ۳۳-۳۴.

[۳۳] ایمانقلی، مریم، جرایم فضای سایبری در حقوق ایران، سومین کنفرانس ملی حقوق در چشم انداز ۱۴۰۴، رشت، (۱۳۹۹)، https://civilica.com/doc/1152558

یکی از مهم‌ترین مسئولیت‌های این ارائه‌دهندگان، رعایت محدودیت‌های سنی دیجیتال است که در بسیاری از حوزه‌های قضایی برای استفاده از خدمات آنلاین تعیین شده است. به‌عنوان مثال، در اتحادیه اروپا، GDPR سن دیجیتال را ۱۶ سال تعیین کرده، مگر اینکه کشورهای عضو سن پایین‌تری (حداقل ۱۳ سال) را انتخاب کنند. پلتفرم‌ها موظف‌اند فرآیندهای تأیید سن را پیاده‌سازی کنند تا اطمینان حاصل شود که کاربران زیر سن مجاز بدون رضایت والدین یا قیم قانونی به خدمات دسترسی ندارند. این فرآیندها باید به‌گونه‌ای طراحی شوند که هم دقیق باشند و هم حریم خصوصی کاربران را نقض نکنند. عدم اجرای مؤثر این محدودیت‌ها می‌تواند به جریمه‌های سنگین، مانند آنچه تحت GDPR اعمال می‌شود، منجر شود.[۳۴]

حفاظت از داده‌های شخصی کودکان و نوجوانان از دیگر وظایف کلیدی است. ارائه‌دهندگان خدمات باید اطمینان حاصل کنند که داده‌های جمع‌آوری‌شده از کاربران خردسال، مانند اطلاعات هویتی، موقعیت مکانی یا الگوهای رفتاری، تنها با رضایت صریح والدین یا قیم قانونی جمع‌آوری و پردازش می‌شود. این داده‌ها باید با بالاترین استانداردهای امنیتی ذخیره شوند و از دسترسی غیرمجاز یا استفاده تجاری بدون مجوز محافظت شوند. نقض این تعهدات، مانند فروش داده‌های کودکان به اشخاص ثالث، می‌تواند مسئولیت مدنی و کیفری به همراه داشته باشد. همچنین موظف‌اند در برابر آزار و اذیت سایبری، سوءاستفاده آنلاین و شکارگری دیجیتال[۳۵] از کودکان و نوجوانان محافظت کنند. این شامل طراحی سیستم‌های گزارش‌دهی ساده و قابل دسترس برای کاربران خردسال و والدین آنها، و همچنین واکنش سریع به گزارش‌های مربوط به رفتارهای سوءاستفاده‌گرانه است. علاوه بر این، ارائه‌دهندگان باید آموزش‌ها و منابع اطلاعاتی را برای کاربران خردسال و والدین فراهم کنند تا آگاهی آنها از خطرات آنلاین و راه‌های مقابله با آن افزایش یابد. در برخی نظام‌های حقوقی، مانند قانون خدمات دیجیتال (DSA) در اتحادیه اروپا، پلتفرم‌ها ملزم به انتشار گزارش‌های شفافیت در مورد اقدامات خود برای حفاظت از کاربران خردسال هستند.[۳۶]

به نظر نگارنده، همکاری با نهادهای قضایی و سازمان‌های حمایت از کودکان بخش دیگری از مسئولیت‌های این ارائه‌دهندگان است. آنها باید در صورت وقوع جرائم مرتبط با کودکان، مانند انتشار محتوای غیرقانونی یا سوءاستفاده جنسی آنلاین، با مقامات همکاری کنند و اطلاعات لازم را در چارچوب قوانین ارائه دهند. این همکاری باید با رعایت اصول حریم خصوصی انجام شود تا از افشای غیرضروری داده‌های کاربران جلوگیری شود. در نهایت، ارائه‌دهندگان خدمات باید سیاست‌های شفافی در مورد نحوه مدیریت کاربران خردسال و رعایت محدودیت‌های سنی دیجیتال منتشر کنند. این سیاست‌ها باید برای والدین و کاربران قابل فهم باشند و شامل اطلاعاتی در مورد نحوه جمع‌آوری داده‌ها، فرآیندهای تأیید سن و اقدامات حفاظتی باشند. عدم شفافیت در این زمینه می‌تواند به کاهش اعتماد عمومی و مسئولیت‌های حقوقی منجر شود.

۴-۳- مسئولیت والدین در پرتو بی‌توجهی یا ترک فعل

والدین در مقام قیم و ولی قهری، بر اساس قواعد عمومی حقوق مدنی و خانوادگی، موظف‌اند ایمنی جسمی و روانی فرزندان خود را تضمین کنند و نظارت مستمر بر فعالیت‌های آنها در محیط‌های حقیقی و مجازی را به‌عمل آورند. این الزام از ماده ۱۱۸۰ قانون مدنی ناشی می‌شود که پدر و جد پدری را ولی قهری می‌داند و در ادامه، در مواد ۱۱۸۳ و ۱۱۸۴ وظایف قیم مشخص شده است.[۳۷] به موجب این مواد، ولی قهری باید «شخصاً مراقبت‌های لازم را به‌عمل آورد و امور مربوط به تربیت و اداره اموال طفل را عهده‌دار شود»، امری که بی‌توجهی به نظارت بر دسترسی و مصرف محتوای دیجیتال را نیز دربر می‌گیرد.

---

[۳۴] Livingstone, Sonia, and Brian O’Neill, "Children’s rights online: Challenges, dilemmas and emerging directions." Minding minors wandering the web: Regulating online child safety, (2014), 27-28.

[۳۵] Online Predation

[۳۶] Sorensen, Shannon, "Protecting children's right to privacy in the digital age: Parents as trustees of children's rights." Child. Legal Rts. J. 36, (2016), 156.

[۳۷] صفایی، سید حسین، اشخاص و محجورین، (تهران: انتشارات سمت، ۱۴۰۳)، ۲۳۱.

در عرصه حقوق کیفری، ترک فعل ولی نسبت به نظارت بر فعالیت‌های فرزند موجب مسئولیت می‌شود، هرگاه مخاطرات محتمل فضای سایبری، مانند دسترسی به محتوای خشونت‌آمیز یا مستهجن، یا ارتباط با افراد زیان‌بار، سبب ورود آسیب روانی یا جسمی به کودک گردد. مطابق ماده ۲۹۵ قانون مجازات اسلامی (تعزیرات)، هرگاه کسی بر اثر ترک فعل خود موجب صدمه بدنی یا روانی دیگری شود، به حبس یا جزای نقدی محکوم خواهد شد. در این معنا، ترک فعل ولی در نظارت بر فرزند می‌تواند مصداق «غفلت منجر به آسیب» محسوب شود.

در حوزه مسئولیت مدنی نیز، بر اساس اصول «مقصر بودن قیم» و ماده ۱۲۳۸ قانون مسئولیت مدنی، قیم در برابر خسارات وارده بر طفل یا خساراتی که طفل به دیگری وارد می‌کند، مسئول شناخته می‌شود، مگر آن‌که در اثبات بی‌تقصیری خود موفق گردد. اگر کودک به دلیل فقدان نظارت والدین مرتکب عملی زیان‌آور در فضای مجازی شود یا خود مورد سوءاستفاده قرار گیرد، ولی علاوه بر مسئولیت مدنی به جبران خسارت، ممکن است در مقام ایذاء و ترک فعل مقصر هم تلقی گردد و با محکومیت کیفری همراه شود.

قاعده کلی «توقع مراقبت معقول» از فرزندان در فضای دیجیتال اقتضا می‌کند که والدین ابزارهایی چون فیلتر نرم‌افزاری، تعیین حدود سنی برای ثبت‌نام در پلتفرم‌ها و آموزش سواد رسانه‌ای را پیاده کنند. عدم به‌کارگیری این اقدامات با توجه به امکان پیش‌بینی آسیب‌های سایبری، مغایر با استانداردهای رفتار قیمانه دانسته می‌شود و در صورت وقوع رخدادهای زیان‌بار، ترک فعل تلقی می‌گردد. ترک فعل در قبال کودکان نه تنها یک تخلف اخلاقی، بلکه مصداق حقیقی «جریحه‌دار کردن سلامت جسمی و روانی طفل» است که نظام جزا موظف به مقابله با آن است. [۳۸] به این ترتیب، شناسایی ترک فعل ولی در نظارت بر استفاده فرزندان از فضای مجازی، مبنای محکمه‌پسندی برای اعمال مسئولیت کیفری و مدنی قرار می‌گیرد و ضرورت تدوین دستورالعمل قضایی و الزام قانونی والدین به اتخاذ تمهیدات نظارتی دیجیتال را نمایان می‌سازد.

۴-۴- مقایسه با نظام‌های پیشرفته

در نظام حقوق ایالات متحده، COPPA[۳۹] چارچوبی دقیق برای تعیین ظرفیت قانونی کودکان در فضای دیجیتال ترسیم می‌کند و تنها به وب‌سایت‌ها یا خدمات آنلاین «مستقیماً متوجه افراد زیر ۱۳ سال» یا آنهایی که «عمداً اطلاعات شخصی کودک زیر ۱۳ سال» را جمع‌آوری می‌کنند، اجازه می‌دهد در صورت کسب «رضایت قابل‌تأیید والدین» اقدام نمایند. این رضایت، سازوکارهای سخت‌گیرانه‌ای دارد: ارائه‌دهنده باید سیاست حفظ حریم خصوصی کودک را به‌وضوح منتشر کند، پیش از هرگونه جمع‌آوری داده از والدین اطلاع بگیرد و مستندسازی کند، امکان مرور و حذف اطلاعات جمع‌آوری‌شده را برای والدین فراهم آورد و داده‌ها را تنها تا زمان لازم برای هدف مشخص نگه دارد. با این روش سن دیجیتال را معیار تعیین «کودک» قرار داده و به‌صراحت ظرفیت قانونی تصمیم‌گیری را تا ۱۳ سالگی منتفی می‌داند.[۴۰]

در مقابل، در حقوق اتحادیه اروپا، بخشی از GDPR (ماده ۸ و راغبت ۳۸) به‌عنوان «GDPR-K» از «خدمات جامعه اطلاعاتی» که به‌طور مستقیم به کودکان ارائه می‌شود، می‌خواهد پیش از پردازش داده‌های شخصی افراد زیر ۱۶ سال (یا سن پایین‌ترِ اعلامی توسط هر دولت‌عضو تا حداقل ۱۳ سال) از «رضایت والدین یا قیم قانونی» بهره‌مند گردد. در این نظام، علاوه بر الزام به اخذ رضایت، اصل «حداقل‌سازی داده» و «حق فراموش‌شدن» تأکید شده و محدودیت‌هایی بر تبلیغات هدفمند علیه کودکان وضع شده که بر مبنای درک ناقص آنها از مخاطرات داده‌محور است.[۴۱]

---

[۳۸] محمدی، شهرام و همکاران، "نقش خانواده، مدرسه و رسانه در پیشگیری از وقوع جرم با تأکید بر معیارهای بین‌المللی حاکم بر تعهد دولت‌ها در آموزش افراد." تدریس پژوهی، ۶، ۴(۱۳۹۷)، ۲۴۱.

[۳۹] Children's Online Privacy Protection Rule

[۴۰] Chaturvedi, Ashish, "Enforcement and Compliance of the Children's Online Privacy Protection Act (COPPA): Evaluating the Impact of FTC Settlements on Corporate Practices." Issue 3 Int'l JL Mgmt. & Human. 6 (2023), 3329.

[۴۱] Goddard, Michelle (2017), "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact." International Journal of Market Research 59.6 (2017), 703-705.

به نظر نگارنده، هر دو نظام با اتکا به مفهوم سن دیجیتال، ظرفیت قانونی خردسال را تا دوره‌ای محدود دانسته و برای غلبه بر ناتوانی آنها در ارزیابی مخاطرات داده، آن را به رضایت والدین پیوند زده‌اند. تفاوت عمده در اصول فنی و دامنه اعمال است: COPPA صرفاً وب‌سایت‌ها و اپلیکیشن‌های آمریکایی را دربر می‌گیرد و تمرکز اصلی‌اش بر حریم خصوصی کودک است، اما GDPR-K دامنه وسیع‌تری از «خدمات جامعه اطلاعاتی» را زیر چتر می‌گیرد[۴۲]، حق‌های گسترده‌تری چون دسترسی، تصحیح و حذف داده را به کودک می‌دهد و مقررات آن جنبه پیشگیرانه و محافظت گسترده‌تری دارد. ضرورت «سن دیجیتال» در هر دو سامانه، مبنای قانونی اثربخشی سازوکارهای حمایت از کودکان در فضای مجازی است؛ به این معنا که تا پیش از بلوغ فکری و حقوقی کودک، سرپرست وظیفه هدایت و نظارت بر تعامل آنلاین او را بر عهده دارد. این رویکرد ترکیبی از اصول حمایت از کودک و حقوق دیجیتال، امکان اعمال سیاست‌های حفاظتی متناسب با تفاوت‌های رشد شناختی کودکان را در برابر خطرات سایبری فراهم می‌آورد.

نتیجه

نظام کیفری ایران گام‌های اولیه‌ای در جهت مقابله با سوءاستفاده‌های سایبری از کودکان و نوجوانان برداشته است؛ به‌ویژه از طریق جرم‌انگاری عمومی بهره‌کشی از اطفال در قانون حمایت از اطفال و نوجوانان و به‌کارگیری مواد قانون جرایم رایانه‌ای برای مواجهه با محتوای جنسی یا تهدیدآمیز دیجیتال. با این حال، فقدان معیار مشخص «سن دیجیتال» به‌منظور تعیین ظرفیت قانونی تصمیم‌گیری در فضای مجازی، موجب شده که کودکان بدون هیچ محدودیتی در معرض خطرات جدی قرار گیرند؛ از سوی دیگر، تکالیف اختیاری واسطه‌های فنی در شناسایی و مسدودسازی خودکار محتوای مضر، عملاً بی‌اثر مانده و خلأ اجرای دستورالعمل‌های قضایی ویژه کودکان قربانی، حاکمیت حمایت قانونی را مخدوش کرده است.

افزون بر این، پراکندگی مقررات کیفری و ناتوانی در احراز هویت کاربران خردسال، مراجع قضایی را در رسیدگی به پرونده‌های سایبری با دشواری فنی و اجرایی مواجه ساخته است. تجربه‌های موفق بین‌المللی، به‌ویژه لزوم کسب «رضایت قابل‌تأیید والدین» پیش از دسترسی کودک به خدمات دیجیتال و پیش‌بینی سازوکارهای نظارت مداوم بر پلتفرم‌ها، نشان می‌دهد که یک تعریف قانونی شفاف از سن دیجیتال و اعمال آن در حوزه کیفری و مدنی، به همراه الزامات فنی احراز سن و گزارش‌گیری آنلاین، می‌تواند نقش مؤثری در پیشگیری از جرایم سایبری بازی کند. برای تضمین حمایت مؤثر از نسل دیجیتال، ضروری است که قانون‌گذار با یکپارچه‌سازی مقررات، تدوین آئین‌نامه‌های اجرایی دقیق و ایجاد دستورالعمل قضایی تخصصی برای دادرسی ویژه کودکان، اقدام نماید؛ همچنین فراهم‌سازی ابزارهای فنی مطمئن برای تشخیص محتوای مضر و پاسخ به ترک فعل والدین و پلتفرم‌ها، تکمیل‌کننده ساختاری خواهد بود که بتواند سایه تهدید سایبری را از حقوق کودکان و نوجوانان برطرف سازد.

پیشنهادها

۱- ضرورت‌های تقنینی و سیاست‌گذاری کیفری: با توجه به افزایش روزافزون و پیچیده تهدیدهای سایبری علیه کودکان و نوجوانان، بازنگری و ساماندهی تقنین کیفری در این حوزه امری اجتناب‌ناپذیر است. فقدان مقررات جامع و یکپارچه، موجب پراکندگی واکنش‌های کیفری و کاهش کارآمدی حمایت‌های قانونی می‌شود. ازاین‌رو، تدوین سیاست جنایی پیشگیرانه و حمایتی، به‌عنوان زیربنای تضمین حق مصونیت نسل جوان در فضای دیجیتال، باید در اولویت قانون‌گذاری قرار گیرد.

۲- ایجاد سامانه‌های گزارش‌گیری آنلاین و حفاظت پیشگیرانه: سامانه‌های گزارش‌گیری آنلاین باید با رعایت اصل دسترسی آسان، سرعت و صداقت اطلاعات طراحی شوند تا کودکان، والدین و نهادهای آموزشی بتوانند در تمام ساعات شبانه‌روز موارد آزار، تهدید یا سوءاستفاده سایبری را ثبت و پیگیری کنند. این سامانه‌ها لازم است از طریق وب‌سایت‌ها و اپلیکیشن‌های رسمی قوه قضائیه یا نهادهای متولی حمایت از کودکان ارائه شوند و واجد ویژگی‌هایی نظیر رمزگذاری ارتباطات، حفظ محرمانگی اطلاعات شاکی و امکان ارسال گزارش به‌صورت ناشناس باشند. ارجاع خودکار گزارش‌ها به پلیس فتا یا مرجع قضایی صالح،

---

[۴۲] Choi, Bryan H, "A Prospect Theory of Privacy." (Idaho L. Rev. 5, 2014), 623.

امکان پیگیری وضعیت پرونده، دریافت پاسخ و اطلاع از زمان‌بندی اقدامات آتی، و نیز بهره‌گیری از فرم‌های استاندارد حقوقی و دسته‌بندی دقیق جرایم سایبری، از الزامات این سامانه‌هاست. این سازوکار علاوه بر تسهیل دسترسی به عدالت، امکان تحلیل آماری و شناسایی نقاط بحرانی را برای سیاست‌گذاران فراهم می‌آورد.

۳- لزوم تدوین دستورالعمل قضایی ویژه جرایم سایبری علیه کودکان: برای تضمین عدالت کیفری و ترمیمی مؤثر، تدوین دستورالعمل قضایی ویژه جرایم سایبری علیه کودکان ضروری است. این دستورالعمل باید ضابطان و قضات را ملزم سازد تا در تمامی مراحل دادرسی—از پذیرش شکایت و تحقیق مقدماتی تا صدور و اجرای حکم—ملاحظات سنی، روانی و اجتماعی کودک بزه‌دیده را رعایت کنند. نحوه اخذ اظهارات کودک، استفاده از ادله دیجیتال، تضمین محرمانگی، جلوگیری از بازبزه‌دیدگی و تسهیل دسترسی به خدمات حمایتی و مشاوره‌ای، باید به‌صورت دقیق و الزام‌آور در این دستورالعمل پیش‌بینی شود.

۴- پیشنویس ماده قانونی پیشنهادی: در راستای تحقق موارد فوق، پیشنهاد می‌شود ماده‌ای با مضمون زیر به قوانین مرتبط با جرایم رایانه‌ای یا قانون حمایت از اطفال و نوجوانان الحاق شود:

هرگونه آزار، تهدید، سوءاستفاده جنسی، مالی یا روانی از اطفال و نوجوانان در فضای سایبری، جرم محسوب شده و مرتکب حسب مورد به مجازات مقرر در این قانون محکوم می‌گردد.

مراجع قضایی و ضابطان دادگستری مکلف‌اند در رسیدگی به این جرایم، اصول حمایت ویژه از کودک، از جمله حفظ محرمانگی هویت بزه‌دیده، اخذ اظهارات متناسب با سن و وضعیت روانی وی، و بهره‌گیری از سامانه‌های گزارش‌گیری الکترونیکی امن را رعایت نمایند.

آیین‌نامه اجرایی این ماده، مشتمل بر نحوه گزارش‌دهی، رسیدگی تخصصی و ارائه خدمات حمایتی، ظرف شش ماه از تاریخ لازم‌الاجرا شدن این قانون، توسط قوه قضائیه با همکاری نهادهای ذی‌ربط تهیه و تصویب می‌شود.

منابع

الف) فارسی:

کتاب‌ها

۱. السان، مصطفی، حقوق فضای مجازی، تهران: انتشارات شهر دانش، ۱۴۰۲.

۲. صفایی، سید حسین، اشخاص و محجورین، تهران: انتشارات سمت، ۱۴۰۳.

۳. عارفی ، مرتضی، شرح جامع قانون حمایت از اطفال و نوجوانان مصوب ۱۳۹۹، تهران: شرکت سهامی انتشار ۱۴۰۲.

مقالات

۴. اکبری، مسعود و قناد، فاطمه، "سیاست کیفری ایران در قبال اطفال و نوجوانان بزهدیده گردشگری جنسی." فصلنامه پژوهش حقوق کیفری، ۲، ۵(۱۳۹۲)، ۱۳۷.

۵. استادي، سمیه و میری، حسین (۱۴۰۲)، "بررسی جرم نشر اکاذیب در فضای سایبر." مطالعات حقوق، ۸، ۳۴(۱۴۰۲)، ۱۰۸.

۶. ایمانقلی، مریم، جرایم فضای سایبری در حقوق ایران، سومین کنفرانس ملی حقوق در چشم انداز ۱۴۰۴، رشت، (۱۳۹۹)، https://civilica.com/doc/1152558

۷. رضوی فرد، بهزاد و موسوی، سید نعمت الله، مسئولیت کیفری در فضای سایبر در حقوق ایران، فصانامه پژوهش حقوق کیفری دانشگاه علامه طباطبایی، ۵، ۱۶(۱۳۹۵)، ۳۳-۳۴.https://doi.org/10.22054/jclr.2016.6753

۸. زمانی جباری، افسانه و پژوهش جهرمی، امین، "مبانی جرم‌انگاری جرایم سایبری مجازی." دوفصل نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)، ۷، ۲(۱۳۹۸)، ۹.http://monadi.isc.org.ir/article-1-105-fa.html

۹. زینالی حمزه، "نوآوری های قانون «حمایت از کودکان و نوجوانان» و چالش های فراروی آن." نشریه: رفاه اجتماعی، ۲، ۷(۱۳۸۲)، ۶۴. Available from: https://sid.ir/paper/56886/fa

۱۰. حسینی، سجاد و رایجیان اصلی، مهرداد، "یادگیری رفتار مجرمانه در فضای سایبر،" مجلس و راهبرد، ۳۰، ۱۱۴(۱۴۰۲)، ۲۸۳.

۱۱. صبح خیز، رضا، "چالش های حقوقی جرایم سایبری در نظام حقوق بین الملل و نظام حقوقی ایران." نشریه: پژوهش های اطلاعاتی و جنایی، ۱۰، ۳(۱۳۹۴)، ۱۲۴. Available from: https://sid.ir/paper/249181/fa

۱۲. طهماسبی، جواد و شاهمرادی، خیرالله، چالش‌ها و خلأهای موجود در فرایند رسیدگی به جرایم سایبری، حقوقی دادگستری، ۸۲، ۱۰۴(۱۳۹۷)، ۹۹. Available from: https://sid.ir/paper/137883/fa

۱۳. عطازاده، سعید و همکاران، هرزه‌نگاری سایبری علیه کودکان در سیاست جنایی تقنینی ایران با نگاهی به حقوق انگلستان. پژوهش های اطلاعاتی و جنایی, ۱۶/۶۳ (۱۴۰۰)، ۱۲۴. https://doi.org/10.1080/13691180802158557

۱۴. فرهادی آلاشتی، زهرا، برساخت قضائی کنترل جرایم سایبری کودکان و نوجوانان: به‌سوی ارائهٔ نظریه‌ای داده‌بنیاد، نشریه مطالعات حقوق کیفری و جرم شناسی، ۵۲، ۲(۱۴۰۱)، ۲۸۶. 10.22059/jqclcs.2023.359958.1849

۱۵. کلانتری، کیومرث و نصرالهی، ابوذر، "سیاست جنایی تقنینی ایران در قبال جرایم جنسی علیه کودکان و نوجوانان." نشریه: حقوق و سیاست، ۹، ۲۲(۱۳۸۶)، ۷۴. Available from: https://sid.ir/paper/98074/fa

۱۶. محمدی، شهرام و همکاران، "نقش خانواده، مدرسه و رسانه در پیشگیری از وقوع جرم با تأکید بر معیارهای بین‌المللی حاکم بر تعهد دولت‌ها در آموزش افراد." تدریس پژوهی، ۶، ۴(۱۳۹۷)، ۲۴۱. doi 20.1001.1.24765686.1397.6.4.12.9

۱۷. مشیراحمدی، علیرضا، "تحلیل جرم‌شناختی جرایم سایبری." دوفصل نامه علمی منادی امنیت فضای تولید و تبادل اطلاعات (افتا)، ۸، ۱(۱۳۹۸)، ۵۲. http://monadi.isc.org.ir/article-1-117-fa.html

لاتین:

1. Brenner, Susan W, Cybercrime: criminal threats from cyberspace, Bloomsbury Publishing USA, 2010.

2. Chaturvedi, Ashish, "Enforcement and Compliance of the Children's Online Privacy Protection Act (COPPA): Evaluating the Impact of FTC Settlements on Corporate Practices." Issue 3 Int'l JL Mgmt. & Human. 6, 2023.

3. Choi, Bryan H, "A Prospect Theory of Privacy." Idaho L. Rev. 5, 2014.

4. Dannhauser, Thomas, Digitally Engineered Attention and Energy Theft via Psychological Manipulation, IEEE Technology and Society Magazine, 41, 2(2022),.

5. Frame, Alexander, Interculturalities in the Digital Age, EPISTÉMÈ, 33:1, 2025.

6. Goddard, Michelle, "The EU General Data Protection Regulation (GDPR): European regulation that has a global impact." International Journal of Market Research 59.6 (2017), 703-705. https://doi.org/10.2501/IJMR-2017-050

7. Guinchard, Audrey, "Cybercrime: The Transformation of Crime in the Information Age." Information, Communication & Society, 11, 7(2008), 1032. https://doi.org/10.1080/13691180802158557

8. Livingstone, Sonia, and Brian O'Neill, "Children's rights online: Challenges, dilemmas and emerging directions." Minding minors wandering the web: Regulating online child safety, 2014.

9. Lubis, A. R, The Kidfluencer Phenomenon and Modern Slavery: A Critical Analysis of Indonesia's Legal Framework in Protecting Children from Digital Exploitation. Arkus, 11(1), 2024.

10. Moore, Robert, Cybercrime: Investigating high-technology computer crime. Routledge, 2014.

11. Sabillon, Regner et al., "Cybercrime and cybercriminals: A comprehensive study." International Journal of Computer Networks and Communications Security, 4 (6), 2016.

12. Sorensen, Shannon, "Protecting children's right to privacy in the digital age: Parents as trustees of children's rights." Child. Legal Rts. J. 36, 2016.

13. Verdoodt, Valerie, The Role of Children's Rights in Regulating Digital Advertising, publication in the International Journal of Children's Rights, Volume 27: Issue 3, 2019.

14. Wall, David S, "Cybercrime and the culture of fear: Social science fiction (s) and the production of knowledge about cybercrime." Information, Communication & Society 11.6 (2008), 861. https://doi.org/10.1080/13691180802007788

15. Wijakusumariasih, I. P. N, "Legal Protection For Children Against Online Sexual Exploitation and Abuse of Children." Jurnal Magister Hukum Udayana (Udayana Master Law Journal, 8 2003), 4-11.

The digital age and criminal laws in the face of cyber abuse of children and adolescents

Abstract
In today's world, the rapid entry of children and adolescents into cyberspace has created many educational and social opportunities, but it has also brought serious threats. These threats include online sexual abuse and exploitation, commercial exploitation, encouragement of risky behaviors, and cyberbullying. These conditions have doubled the necessity of the role of the criminal justice system in protecting this age group. The present study examines the ability of Iran's criminal justice system to deal with cyber abuse of children and adolescents and tries to assess its compatibility with the challenges of the digital age. Using a descriptive-analytical method and sources such as domestic laws, international documents, and judicial procedure, this research shows that despite laws such as the Computer Crimes Law and the Law on the Protection of Children and Adolescents, there are still serious shortcomings in the field of criminalization, monitoring of Internet platforms, and dealing with the technical complexities of the digital space. Among the key findings of this research is the necessity of amending laws, developing clear judicial guidelines, promoting the accountability of supervisory institutions, and strengthening digital legal awareness. In total, the research emphasizes that effective criminal protection of children in cyberspace requires a comprehensive review and coordination between legal structures and new technologies.

Keywords: Digital age, child abuse, criminal law, Computer Crimes Law, cybercrime