Comparative Studies in Jurisprudence, Law, and Politics

International, Regional, and Local Activities Regarding the Fight Against Child Abuse in Cyberspace

1. Mostafa Abbasi: Department of Law, La.C., Islamic Azad University, Lahijan, Iran
2. Abbas Taghvaei*: Department of Islamic Studies, La.C., Islamic Azad University, Lahijan, Iran.
Email: taghvaee.abbas@iau.ac.ir (Corresponding Author)
3. Tayyebeh Ghodrati Siahmezgi: Department of Law, La.C., Islamic Azad University, Lahijan, Iran
4. Amirreza Mahmoudi: Department of Law, La.C., Islamic Azad University, Lahijan, Iran

ABSTRACT

The rapid expansion of cyberspace and social media platforms has created unprecedented opportunities for human interaction, knowledge exchange, and the development of communication skills. Nevertheless, this environment has simultaneously generated a vulnerable setting for specific groups—particularly children—exposing them to various forms of online child abuse. This phenomenon encompasses sexual exploitation, psychological harassment, exposure to harmful content, and even the economic exploitation of minors. Given that such abuses produce long-term and sometimes irreversible psychological and social consequences for victims, they require heightened attention from the international community as well as national policymakers. Addressing this issue is essential because cyber child abuse not only contributes to behavioral and psychological disorders among children but also poses a broader threat to social security, family cohesion, and the mental well-being of future generations. The primary objective of this article is to provide a comprehensive analysis of international, regional, and national activities aimed at preventing and combating online child abuse and to evaluate the effectiveness of multilevel approaches in protecting children. The research adopts a descriptive–analytical methodology based on the review of legal documents, official reports issued by international organizations such as UNICEF and INTERPOL, and case studies of countries that have successfully implemented preventive and protective programs in this field. The findings indicate that existing legal frameworks and policy initiatives at the international and regional levels have taken significant steps toward addressing digital child abuse by establishing common definitions, developing shared protocols, and strengthening judicial and law-enforcement cooperation among states. However, numerous challenges—including enforcement limitations, cultural differences, unequal levels of technological development among countries, and the transnational mobility of offenders in cyberspace—continue to reduce the effectiveness of these measures. Furthermore, insufficient parental awareness, inadequate supervision of social media platforms, and the absence of efficient support infrastructures have complicated efforts to confront this phenomenon. The study concludes that integrating international, regional, and national approaches, alongside cooperation among governmental institutions, the private sector, and civil society, can substantially enhance prevention capacities and child protection mechanisms. The findings highlight the necessity of coordinated policymaking, strengthening institutional capacities, continuous education of users—particularly parents and teachers—and the development of monitoring and protective technologies. Adopting a comprehensive and multilevel strategy not only enables the mitigation of current harms but also contributes, in the long term, to the creation of a safer and healthier digital environment for children.

Keywords: *Online child abuse; Cyberspace; Child protection; International policies; Multilevel approaches.*

How to cite: Abbasi, M., Taghvaei, A., Ghodrati Siahmezgi, T., & Mahmoudi, A. (2026). International, Regional, and Local Activities Regarding the Fight Against Child Abuse in Cyberspace. *Comparative Studies in Jurisprudence, Law, and Politics*, *8*(3), 1-18.

© 2026 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Submit Date: 27 October 2025
Revise Date: 17 February 2026
Accept Date: 23 February 2026
Publish Date: 23 August 2026

پژوهش‌های تطبیقی فقه،
حقوق و سیاست

فعالیت های بین المللی، منطقه ای و محلی راجع به مبارزه با کودک‌آزاری در فضای مجازی

۱. مصطفی عباسی: گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران
۲. عباس تقوائی*: گروه معارف اسلامی، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران.
پست الکترونیک: taghvaee.abbas@iau.ac.ir (نویسنده مسئول)
۳. طیبه قدرتی سیاهمزگی: گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران
۴. امیررضا محمودی: گروه حقوق، واحد لاهیجان، دانشگاه آزاد اسلامی، لاهیجان، ایران

چکیده

گسترش روزافزون فضای مجازی و شبکه‌های اجتماعی، فرصت‌های بی‌سابقه‌ای برای تعاملات انسانی، تبادل دانش و توسعه مهارت‌های ارتباطی فراهم آورده است. با این حال، همین فضا بستری آسیب‌پذیر برای گروه‌های خاص به‌ویژه کودکان ایجاد کرده است که می‌تواند به اشکال مختلف کودک‌آزاری آنلاین منجر شود. این پدیده شامل سوءاستفاده جنسی، آزار روانی، دسترسی به محتوای مضر و حتی استثمار اقتصادی کودکان است و از آنجا که آثار روانی و اجتماعی بلندمدت و بعضاً جبران‌ناپذیر بر قربانیان بر جای می‌گذارد، توجه ویژه جامعه جهانی و سیاست‌گذاران ملی را می‌طلبد. پرداختن به این موضوع ضروری است، زیرا کودک‌آزاری سایبری نه تنها موجب بروز اختلالات رفتاری و روان‌شناختی در کودکان می‌شود، بلکه تهدیدی برای امنیت اجتماعی، انسجام خانواده و سلامت روانی نسل آینده محسوب می‌شود.هدف اصلی این مقاله، تحلیل جامع فعالیت‌های بین‌المللی، منطقه‌ای و ملی در زمینه پیشگیری و مقابله با کودک‌آزاری آنلاین و ارزیابی میزان اثربخشی رویکردهای چندسطحی در حمایت از کودکان است. روش تحقیق مقاله به‌صورت توصیفی-تحلیلی انتخاب شده و بر اساس مرور اسناد حقوقی، گزارش‌های رسمی سازمان‌های بین‌المللی مانند یونیسف و اینترپل، و همچنین مطالعات موردی کشورهایی که برنامه‌های موفقی در این زمینه اجرا کرده‌اند، تدوین گردیده است.یافته‌های تحقیق نشان می‌دهد که چارچوب‌های قانونی و سیاست‌های موجود در سطح بین‌المللی و منطقه‌ای، گام‌های مهمی در مسیر مقابله با کودک‌آزاری دیجیتال برداشته‌اند و به ایجاد تعاریف واحد، تدوین پروتکل‌های مشترک و تقویت همکاری‌های قضایی و پلیسی بین کشورها منجر شده‌اند. با این وجود، چالش‌های متعددی همچون محدودیت‌های اجرایی، تفاوت‌های فرهنگی، سطح متفاوت توسعه فناوری در کشورها و تحرک بزهکاران در فضای مجازی باعث کاهش اثربخشی این اقدامات می‌شود. علاوه بر این، کمبود آگاهی والدین، ضعف نظارت بر پلتفرم‌های اجتماعی و فقدان زیرساخت‌های حمایتی کارآمد، مقابله با این پدیده را دشوارتر کرده است.نتیجه این بررسی نشان می‌دهد که ترکیب رویکردهای بین‌المللی، منطقه‌ای و ملی، در کنار همکاری نهادهای دولتی، بخش خصوصی و جامعه مدنی، می‌تواند شانس پیشگیری و حمایت مؤثر از کودکان را به‌طور چشمگیری افزایش دهد. این مطالعه اهمیت تدوین سیاست‌های هماهنگ، تقویت ظرفیت‌های نهادی، آموزش مستمر کاربران و به‌ویژه والدین و معلمان، و توسعه فناوری‌های نظارتی و حفاظتی را برجسته می‌سازد. اتخاذ رویکردی جامع و چندسطحی نه تنها امکان کاهش آسیب‌های فعلی را فراهم می‌کند بلکه در بلندمدت به ایجاد محیطی ایمن‌تر و سالم‌تر برای حضور کودکان در فضای مجازی کمک خواهد کرد.

واژگان کلیدی: *کودک‌آزاری آنلاین، فضای مجازی، حمایت از کودکان، سیاست‌های بین‌المللی، رویکردهای چندسطحی.*

نحوه استناددهی: عباسی، مصطفی.، تقوائی، عباس.، قدرتی سیاهمزگی، طیبه.، و محمودی، امیررضا. (۱۴۰۵). فعالیت های بین المللی، منطقه ای و محلی راجع به مبارزه با کودک‌آزاری در فضای مجازی. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۸(۳)، ۱۸-۱.

© ۱۴۰۵ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

تاریخ ارسال: ۵ آبان ۱۴۰۴
تاریخ بازنگری: ۲۸ بهمن ۱۴۰۴
تاریخ پذیرش: ۴ اسفند ۱۴۰۴
تاریخ چاپ: ۱ شهریور ۱۴۰۵

مقدمه

حفاظت از کرامت و رفاه کودکان در سطح بین‌المللی دارای اهمیتی بی‌بدیل است. این اهمیت از طریق تصویب کنوانسیون حقوق کودک توسط تقریباً تمامی کشورهای عضو سازمان ملل به رسمیت شناخته شده است. کودک‌آزاری، فارغ از نوع آن، مخالف اصول مندرج در این کنوانسیون است و سلامت روانی و رشد اجتماعی کودک را تهدید می‌کند. با ظهور فضای مجازی و شبکه‌های اجتماعی، این جرائم فراتر از مرزهای ملی رخ می‌دهند و نیاز به اقدامات بین‌المللی هماهنگ و همکاری میان‌دولتی را بیش از پیش ضروری می‌سازند.در سطح بین‌المللی، تصویب کنوانسیون شورای اروپا در مورد حمایت از کودکان در برابر استثمار جنسی و سوءاستفاده جنسی و همچنین کنوانسیون جرایم سایبری، پاسخ به نیاز تنظیم فعالیت‌های کودک‌آزاری در فضای مجازی محسوب می‌شوند. در سطح منطقه‌ای، همکاری‌های میان کشورها و تدوین سیاست‌ها و چارچوب‌های منطقه‌ای به کاهش سوءاستفاده‌های دیجیتال کمک می‌کند، و در سطح ملی، قوانین کیفری مسئول تنظیم و مقابله با این جرائم هستند.کودک‌آزاری می‌تواند فیزیکی، جنسی، روانی یا عاطفی باشد. در حالی که سوءاستفاده فیزیکی مستلزم آسیب بدنی است و نمی‌تواند از طریق فضای مجازی رخ دهد، سوءاستفاده روانی و جنسی به طور فزاینده‌ای از بستر دیجیتال بهره می‌گیرد. یکی از اشکال رایج سوءاستفاده روانی، قلدری سایبری است که طی آن کودکان یا نوجوانان توسط همسالان خود از طریق پیامک، ایمیل، پیام‌رسان یا سایر فناوری‌های دیجیتال مورد آزار، تهدید یا تحقیر قرار می‌گیرند. این نوع سوءاستفاده می‌تواند حتی آسیب‌زننده‌تر از قلدری سنتی باشد، زیرا قربانیان در فضای خصوصی خانه خود نیز از آن مصون نیستند و عاملان قادرند هویت خود را مخفی کنند.در دنیای امروز، صفحات شبکه‌های اجتماعی مانند فیس‌بوک و توییتر بخشی از هویت فردی را شکل می‌دهند و تهدید به اعتبار دیجیتال می‌تواند تأثیر مستقیم بر زندگی واقعی کودک داشته باشد. انتشار محتواهای نامناسب یا مخاطره‌آمیز ممکن است منجر به باج‌گیری، تحقیر یا تهدید روانی کودک شود و وی را در معرض محیطی ناسالم قرار دهد که با رفاه او سازگار نیست. ماندگاری محتوا در اینترنت نیز می‌تواند آثار طولانی‌مدت و آسیب‌های روانی پایدار ایجاد کند، به طوری که موارد خودکشی کودکان در اثر قلدری سایبری گزارش شده است.سوءاستفاده جنسی نیز یکی از اشکال گسترده کودک‌آزاری در فضای مجازی است که شامل مالکیت و توزیع محتوای پورنوگرافی کودکان، چشم‌چرانی و درخواست انجام اعمال جنسی از کودکان می‌شود. اگرچه تماس فیزیکی در فضای مجازی ممکن نیست، اقدامات گرومینگ یا درخواست از کودکان برای اهداف جنسی یکی از جدی‌ترین اشکال سوءاستفاده آنلاین است. این اشکال سوءاستفاده می‌تواند به اقدامات فیزیکی نیز منجر شود و آمار گزارش‌شده نشان می‌دهد روند گرومینگ کودکان رو به افزایش است.

در بخش‌های بعدی، فعالیت‌ها و سیاست‌های بین‌المللی، منطقه‌ای و ملی در مقابله با کودک‌آزاری در فضای مجازی تحلیل شده و اثربخشی آن‌ها مورد بررسی قرار می‌گیرد. همچنین، راهکارهای پیشگیرانه و اقدامات عملی برای کاهش این جرائم و حمایت از کودکان در محیط دیجیتال ارائه خواهد شد.

۱. ابزارهای بین‌المللی مبارزه با کودک آزاری

ابزارهای اصلی بین‌المللی فعلی که به سوءاستفاده از کودکان می‌پردازند عبارتند از: کنوانسیون حقوق کودک سازمان ملل متحد ۱۹۸۹ و پروتکل اختیاری آن در مورد فروش کودکان، فحشای کودکان و پورنوگرافی کودکان ۲۰۰۰. ذذدو

کنوانسیون حقوق کودک سازمان ملل متحد

ماده ۳۴ این کنوانسیون به طور خاص به سوءاستفاده جنسی و بهره‌کشی از کودکان می‌پردازد. مواد ۳۵ و ۳۶ بعدی به ربودن و قاچاق کودکان و هر شکل دیگری از بهره‌کشی که برای کودکان مضر است، می‌پردازند (United Nations, 1989).عبارت "*تمام اشکال بهره‌کشی جنسی و سوءاستفاده جنسی*" در ماده ۳۴ نشان می‌دهد که سازمان ملل تعریف گسترده‌ای از آنچه سوءاستفاده جنسی از کودک را تشکیل می‌دهد، پذیرفته است. چنین رویکردی می‌تواند مورد انتقاد قرار گیرد زیرا در واقع هیچ تعریف ملموسی ارائه نمی‌دهد و بنابراین به دولت‌ها اختیار زیادی در نظر گرفتن اینکه چه چیزی سوءاستفاده محسوب می‌شود، می‌دهد. با این حال، باید درک کرد که با عدم ارائه فهرست جامع، کنوانسیون کاربرد اصطلاح سوءاستفاده جنسی را محدود نمی‌کند. این مهم است زیرا با توجه به تحول مداوم در پیشرفت‌های فناوری، این رویکرد کلی طیف وسیع‌تری از تفسیر را برای مقامات فراهم می‌کند. بنابراین، اشکال جدید شیوه‌های عملیاتی همچنان می‌توانند سوءاستفاده از کودک محسوب شوند. علاوه بر این، از آنجا که سوءاستفاده از کودکان از طریق فضای مجازی چالشی برای مرزهای قضایی ایجاد می‌کند، تفسیر گسترده از آنچه سوءاستفاده جنسی را تشکیل می‌دهد، اصل حقوقی "*بدون قانون جرمی وجود ندارد*" را که باید در روند استرداد رعایت شود، برآورده می‌کند.

با این حال، ماده ۳۴ کنوانسیون تنها وظیفه حفاظت از کودکان در برابر سوءاستفاده جنسی را بر دولت‌ها تحمیل نمی‌کند. همچنین تعهد مثبتی را بر دولت‌ها برای اتخاذ اقدامات لازم جهت پیشگیری از سوءاستفاده ایجاد می‌کند. در اینجاست که این ماده نوع رفتاری را که دولت‌ها قصد جلوگیری از آن را دارند، فهرست می‌کند. چنین رفتارهایی شامل اجبار کودکان به شرکت در فعالیت‌های جنسی غیرقانونی، فحشا و پورنوگرافی است. اینها همه اشکالی از سوءاستفاده هستند که ممکن است از طریق فضای مجازی ارتکاب یا تسهیل شوند. بنابراین، دولت‌ها موظفند حتی در وب، محیطی امن برای کودکان ایجاد کنند.

تدوین‌کنندگان کنوانسیون رویکرد مشابهی را هنگام تدوین مواد ۳۵ و ۳۶ اتخاذ کردند. در این مواد، استفاده از کلمه "هر" مجدداً خواستار تفسیر گسترده‌ای است و شامل فعالیت‌های انجام شده از طریق فضای مجازی می‌شود. جالب است توجه کنیم که ماده ۳۶ به خودی خود یک مقرره چتری است که "*تمام اشکال دیگر بهره‌کشی که برای هر جنبه‌ای از رفاه کودک مضر است*" را محکوم می‌کند. بنابراین، تمام اشکال سوءاستفاده که قبلاً توصیف شده‌اند از طریق این مقرره مورد توجه قرار می‌گیرند زیرا همه آنها شکلی از رفتار تحقیرآمیز مضر برای رفاه کودکان را تشکیل می‌دهند.

باید به تعهد مثبت دیگری که توسط کنوانسیون در ماده ۳۹ اعلام شده است، اشاره کرد. این ماده وظیفه ارائه درمان لازم برای بازتوانی کودکان قربانی را بر دولت‌ها تحمیل می‌کند. این یک مقرره ضروری است زیرا به کودک به صورت کل‌نگر می‌نگرد. علاوه بر این، مهم است توجه داشته باشیم که این بهبودی ضروری است، زیرا اگر کودک در نتیجه تروما نسبت به فناوری بی‌اعتماد شود، این امر احتمالاً هم برای رشد آموزشی و هم اجتماعی کودک مضر خواهد بود. از آنجا که فناوری و اینترنت ابزارهای مهمی برای اهداف آموزشی و اجتماعی هستند، مهم است که یک قربانی اعتماد به چنین ابزارهایی را که به خودی خود مضر نیستند بلکه سوء استفاده از آنها آنها را خطرناک می‌کند، بازیابد.

پروتکل اختیاری کنوانسیون حقوق کودک در مورد فروش کودکان، فحشای کودکان و پورنوگرافی کودکان

این پروتکل اختیاری در ۱۸ ژانویه ۲۰۰۲ لازم‌الاجرا شده است. همانطور که در مقدمه این پروتکل بیان شده، این سند به منظور دستیابی بیشتر به اهداف تعیین شده در کنوانسیون حقوق کودک سازمان ملل متحد، از جمله اهداف مندرج در مواد ۳۴، ۳۵ و ۳۶ تدوین شده است. (پروتکل

اختیاری، پاراگراف ۱ مقدمه) مقدمه به طور خاص بیان می‌کند که تدوین این سند قانونی از جمله به دلیل "*نگرانی [دولت‌های عضو] درباره افزایش دسترسی به پورنوگرافی کودکان در اینترنت و سایر فناوری‌های در حال تکامل*" صورت گرفته است.

تعهد دولت‌ها در اطمینان از رسیدگی به هر شکل از سوءاستفاده از کودکان را می‌توان در ماده ۲ پروتکل مشاهده کرد. در رابطه با پورنوگرافی کودکان، بند ج مقرر می‌دارد که پورنوگرافی کودکان باید "*هر گونه نمایش، به هر وسیله‌ای، از یک کودک درگیر در فعالیت‌های جنسی صریح واقعی یا شبیه‌سازی شده*" تلقی شود. چنین تعریفی در زمینه سوءاستفاده از کودکان از طریق فضای مجازی ضروری است. زیرا شامل دسترسی از طریق طیف گسترده‌ای از دستگاه‌ها مانند رایانه‌های شخصی، لپ‌تاپ‌ها، تلفن‌های هوشمند، تبلت‌ها و هر دستگاه فناوری که هنوز اختراع نشده و از طریق آن چنین موادی قابل دسترسی خواهد بود، می‌شود. همچنین هر نوع نرم‌افزار و فرمت فایلی را که این اطلاعات ممکن است در آن ذخیره شود، پوشش می‌دهد.

اشاره به مواد واقعی و شبیه‌سازی شده نیز در این زمینه ضروری است. این به دلیل نرم‌افزارهای مختلف ویرایش عکس در گردش امروزی است که در آن ویرایش موادی که شبیه‌سازی یک عمل جنسی را نشان می‌دهد، به راحتی قابل ساخت است. در پرتو این ماده، حتی نوع اخیر مواد یا حتی فقط ژست گرفتن و نه واقعاً درگیر شدن در یک عمل جنسی نیز به عنوان سوءاستفاده در نظر گرفته می‌شود.

ماده ۳ پروتکل تعهداتی را بر دولت‌ها برای ارائه مقررات کیفری لازم جهت حفاظت از کودکان در برابر اشکال سوءاستفاده و بهره‌کشی تعریف شده در ماده ۲ ایجاد می‌کند. طیف گسترده‌ای از اقدامات به عنوان جرم پورنوگرافی کودکان در نظر گرفته می‌شود. این اقدامات شامل: تولید، توزیع، انتشار، واردات، صادرات، عرضه، فروش یا حتی صرفاً در اختیار داشتن مواد توصیف شده در بالا می‌شود. برای تحمیل مجرمیت، معامله اقتصادی یا ثروت‌اندوزی لازم نیست. علاوه بر این، بند ۳ شامل تلاش، همدستی یا مشارکت در چنین جرایمی به عنوان فعالیت‌هایی است که باید توسط دولت‌ها جرم‌انگاری شوند. علاوه بر این، ماده ۳ بند ۴ مقرر می‌دارد که مسئولیت برای این جرایم باید برای اشخاص حقوقی، از جمله شرکت‌های تجاری، تعیین شود.

ماده ۴ به مسئله صلاحیت قضایی می‌پردازد و سعی دارد اطمینان حاصل کند که تحت هر شرایطی مرتکبین چنین جرایمی تحت پیگرد قرار می‌گیرند. این بدان معناست که چه متهم تبعه یک کشور باشد یا صرفاً در قلمرو آن اقامت داشته باشد، یک دولت موظف به پیگرد قانونی است. چنین تعهدی در مواردی که شخص درخواست شده تبعه آن کشور است نیز اعمال می‌شود. بنابراین، این ماده اصل "*یا استرداد کن یا محاکمه کن*" را برقرار می‌کند که حفاظت از حقوق کودکان در فضای مجازی را در مرزهای مختلف افزایش می‌دهد. جالب توجه است که اعلام اصول شخصیت فعال و منفعل در این پروتکل ابزار ضروری در هماهنگ‌سازی صلاحیت‌های قضایی است که اصول حقوقی متفاوتی را اعمال می‌کنند. چنین هماهنگی مهم است زیرا همکاری متقابل و به اشتراک گذاشتن ارزش‌ها و اصول حقوقی یکسان در مبارزه با سوءاستفاده از کودکان در فضای مجازی لازم است. در واقع، ماده ۴ باید در ارتباط با ماده ۵ خوانده شود. ماده اخیر به طور خاص به مسئله استرداد می‌پردازد. چنین ماده‌ای هنگام پرداختن به جنبه بین‌المللی سوءاستفاده از کودکان در فضای مجازی به دو دلیل اصلی مهم است:

- مقرر می‌دارد که جرایم تعیین شده در پروتکل باید حتی زمانی که قبلاً توافقنامه استرداد بین دولت‌ها وجود دارد، توسط دولت‌ها قابل استرداد در نظر گرفته شوند.
- همچنین به پروتکل وضعیت یک معاهده استرداد بین دولت‌ها را می‌دهد زمانی که درخواستی مربوط به چنین جرایمی بین دولت‌هایی که قبلاً با معاهده استرداد ملزم نبوده‌اند، انجام می‌شود.

علاوه بر این، ماده ۶ مقرر می‌دارد که دولت‌های عضو باید در تحقیقات مربوط به چنین جرایمی به یکدیگر کمک کنند. این باز هم عنصر مهم دیگری در مبارزه با سوءاستفاده از کودکان در فضای مجازی است زیرا در جرایم سایبری ممکن است شواهد در صلاحیت‌های قضایی مختلف یافت شود. از طریق چنین ماده‌ای، دولت‌ها موظفند داده‌های جمع‌آوری شده از ارائه‌دهندگان خدمات اینترنتی و نهادهای اجرای قانون که در حوزه صلاحیت آنها یافت می‌شود را در اختیار یکدیگر قرار دهند. این مفهوم همکاری بین‌المللی مجدداً در ماده ۱۰ پروتکل مطرح شده است. این ماده تعهدی را بر دولت‌ها تحمیل می‌کند تا اقدامات لازم برای پیگرد، پیشگیری و همچنین افزایش آگاهی درباره چنین جرایمی را با یکدیگر هماهنگ کنند.

۲. ابزارهای منطقه‌ای اروپایی

با توجه به اینکه بیش از ٪۷۵ کودکان و نوجوانان اروپایی کاربران آنلاین هستند (Livingstone & Haddon, 2009). کشورهای اروپایی نیز به خطراتی که کودکان در فضای مجازی با آن مواجه هستند از طریق قانون‌گذاری پرداخته‌اند. در سطح شورای اروپا[1] می‌توان به موارد زیر اشاره کرد: "*کنوانسیون حمایت از کودکان در برابر استثمار جنسی و سوءاستفاده جنسی*" و "*کنوانسیون جرایم سایبری شورای اروپا*".

در سطح اتحادیه اروپا نیز موارد زیر را می‌یابیم: تصمیم شورای اتحادیه اروپا در مه ۲۰۰۰ برای مبارزه با پورنوگرافی کودکان در اینترنت، دستورالعمل اروپایی در مورد تجارت الکترونیک، و دستورالعمل ۹۲/۲۰۱۱ EU/مورخ ۱۳ دسامبر ۲۰۱۱ در مورد "*مبارزه با سوءاستفاده جنسی و استثمار جنسی کودکان و پورنوگرافی کودکان*".

اسناد شورای اروپا

کنوانسیون لانزاروته سند رسمی شورای اروپا است که به دنبال مبارزه با سوءاستفاده از کودکان است. در مقدمه آن به وضوح بیان شده است که این سند در پاسخ به مشاهده دولت‌ها تدوین شده است "که استثمار جنسی و سوءاستفاده جنسی از کودکان در سطح ملی و بین‌المللی به ابعاد نگران‌کننده‌ای رسیده است، به ویژه در رابطه با افزایش استفاده از فناوری‌های اطلاعات و ارتباطات[2] توسط کودکان و مرتکبین".

مقدمه، کنوانسیون حقوق کودک سازمان ملل متحد و پروتکل‌های اختیاری آن، همراه با ابزارهای اتحادیه اروپا را به عنوان الهام‌بخش این سند به رسمیت می‌شناسد. پیرو رویکرد اتخاذ شده توسط این ابزارها، مقدمه همچنین بیان می‌کند که این کنوانسیون به عنوان یک سند جامع در نظر گرفته شده است که بر پیشگیری، حمایت و ایجاد مکانیسم‌های لازم برای پیگرد قانونی تمرکز دارد. اولین ماده کنوانسیون بیان می‌کند که علاوه بر مبارزه با سوءاستفاده از کودکان، هدف کنوانسیون پیشگیری از آن است. علاوه بر این، از طریق بند ۲، یک "*سازوکار نظارتی خاص ایجاد می‌شود*". این ماده را می‌توان همراه با ماده ۴ کنوانسیون خواند که تعهد رسمی دولت‌ها را برای اتخاذ اقدامات لازم جهت پیشگیری از سوءاستفاده جنسی اعلام می‌کند.

مواد ۵ تا ۸ به وظیفه دولت‌ها برای افزایش آگاهی و اجرای برنامه‌ها، هم برای اهداف آموزشی و هم پیشگیرانه در سطوح مختلف می‌پردازند. این سطوح از افرادی که در تماس نزدیک با کودکان کار می‌کنند، خود کودکان و عموم مردم را شامل می‌شود. ماده ۹ بند ۲ به ویژه برای موضوع مورد بحث مرتبط است. این به این دلیل است که تعهد مثبتی را بر دولت‌ها ایجاد می‌کند تا اطمینان حاصل کنند که بخش خصوصی، که شامل بخش فناوری اطلاعات و ارتباطات می‌شود، نقش فعالی در "تدوین و اجرای سیاست‌هایی برای پیشگیری از استثمار جنسی و سوءاستفاده جنسی از کودکان و اجرای هنجارهای داخلی از طریق خود تنظیمی یا تنظیم مشترک" دارد.

[1] CoE
[2] ICT

مفهوم خود تنظیمی ابزار کلیدی دیگری در مبارزه با جرایم سایبری است. به دلیل ماهیت انعطاف‌پذیر آن، برای قانون‌گذاران ملی دشوار است که با پویایی همیشه در حال تغییر فضای مجازی همگام شوند. با این حال، بخش فناوری ارتباطات و اطلاعات، که شامل ارائه‌دهندگان خدمات اینترنتی، شرکت‌های طراحی وب‌سایت و شرکت‌های ارائه‌دهنده دامنه‌های وب‌سایت می‌شود، به طور مناسب‌تری مجهز هستند تا به تهدیدات مختلف ناشی از استفاده از چنین فناوری‌هایی رسیدگی کنند. بنابراین، اگر این بخش‌ها قوانین لازم را برای تنظیم خود وضع کنند، این امر از نظر زمانی کارآمدتر و مستقیماً متوجه منبع تهدید خواهد بود. با این حال، مهم است توجه داشته باشیم که این نهادها نباید نظر انحصاری در مورد نحوه تنظیم بخش خود داشته باشند. اقتدار نهایی همیشه در دولت به عنوان محافظ نهایی، سرپرست و مدافع رفاه کودکان قرار دارد.

فصل ششم کنوانسیون شامل مواد حقوق کیفری ماهوی است. ماده ۱۸ به سوءاستفاده جنسی می‌پردازد. اگرچه به طور خاص بیان نمی‌کند که سوءاستفاده از کودک چیست، بخش ۱ بند الف به نظر می‌رسد اشاره دارد که سوءاستفاده از کودک شامل فعالیت جنسی با شخصی است که هنوز به سن قانونی برای انجام فعالیت‌های جنسی مطابق با قانون یک کشور خاص نرسیده است. منظور از "*فعالیت جنسی*" طیف گسترده‌ای از اعمال است، اما اختیار زیادی به دولت‌ها در تعریف آنچه باید به عنوان سن رضایت در نظر گرفته شود، داده شده است. (کنوانسیون لانزاروته، ۲۰۰۷، ماده ۱۸ بند ۲) در واقع، در سراسر اروپا، حوزه‌های قضایی مختلف سنین رضایت متفاوتی را تعیین کرده‌اند. این سنین از ۱۳ سال در اسپانیا تا ۱۸ سال در ترکیه و مالت متغیر است (Gil, 2025). این ناسازگاری بین حوزه‌های قضایی مختلف می‌تواند منجر به دشواری‌هایی در نظر گرفتن یک عمل جنسی به عنوان شکلی از سوءاستفاده از کودک شود، به ویژه در مواردی که طرفین درگیر از ملیت‌های مختلف باشند و حوزه‌های قضایی مختلف درگیر باشند.

ماده ۱۹ به جرایم مربوط به فحشای کودکان می‌پردازد. این ماده استخدام کودکان برای اهداف فحشا را به عنوان بخشی از جرم در نظر می‌گیرد. بنابراین، اگر از فضای مجازی برای استخدام کودکان برای قاچاق و فحشا استفاده شود، این اقدام نیز توسط این کنوانسیون پوشش داده می‌شود. ماده ۲۰ به پورنوگرافی کودکان می‌پردازد. مشابه کنوانسیون حقوق کودک سازمان ملل و پروتکل آن، تولید، توزیع و در اختیار داشتن مواد پورنوگرافی را به عنوان رفتاری که باید توسط دولت‌ها جرم‌انگاری شود، در بر می‌گیرد. در رابطه با اقدامات انتشار، واردات، صادرات، ارائه و فروش مواد پورنوگرافی، به نظر می‌رسد این اقدامات در سند شورای اروپا تحت عناوین ارائه یا در دسترس قرار دادن و تهیه مواد پورنوگرافی یکپارچه شده‌اند. بنابراین، صرف در دسترس بودن مواد خاص در اینترنت به منزله جرم خواهد بود. علاوه بر این، به نظر می‌رسد این ابزار یک گام فراتر از ابزارهای سازمان ملل رفته است، زیرا اقدام "*آگاهانه دسترسی به پورنوگرافی کودکان از طریق فناوری‌های اطلاعات و ارتباطات*" جرم اضافی دیگری است که توسط کنوانسیون لانزاروته ایجاد شده است.

نظر اضافی باید درباره ماده ۲۰ بند ۳ ارائه شود. این ماده اخیر مقرر می‌دارد که دولت‌ها اختیار دارند که ماده ۲۰ را در مواردی که تصاویر مورد نظر نمایش‌های شبیه‌سازی شده یا تصویر یک کودک غیرواقعی باشد، اعمال کنند یا نکنند. به نظر این یک مقرره خطرناک است به ویژه از آنجا که فناوری می‌تواند به راحتی برای تولید تصاویر شبیه‌سازی شده استفاده شود. این امر باعث نمی‌شود که مواد کمتر واقع‌گرایانه یا از نظر جنسی کمتر جذاب برای یک فرد پدوفیل باشد. علاوه بر این، اگرچه هیچ کودک واقعی هدف قرار نمی‌گیرد، این همچنان یک شیء‌انگاری کودک و حمله به کرامت کودکان به طور کلی محسوب می‌شود. بنابراین، این امر با روح پیشگیری و حمایت اعلام شده در مقدمه در تضاد خواهد بود. همچنین، بند ۳ بیان می‌کند که اگر مواد شامل کودکانی باشد که به سن رضایت رسیده‌اند و فقط برای استفاده خصوصی خودشان باشد، دولت‌های عضو باز هم آزاد هستند که این ماده را اعمال نکنند. با این حال، به نظر این نویسنده این نیز رویکردی خطرناک است. رسیدن

به سن رضایت به معنای داشتن بلوغ لازم برای تشخیص اثرات کامل اعمال خود نیست. علاوه بر این، سؤالی در مورد اینکه چگونه عبارت "*استفاده خصوصی*" در پرتو به اشتراک گذاشتن مواد خود در رسانه‌های اجتماعی در نظر گرفته می‌شود، مطرح می‌شود.

ماده ۲۱ به استخدام و اجبار کودکان در نمایش‌های پورنوگرافی و همچنین حضور در نمایش‌های پورنوگرافی شامل کودکان می‌پردازد. مهم است توجه داشته باشیم که تمام این اعمال ممکن است از طریق فضای مجازی به وسیله انجمن‌ها و چت‌های ویدئویی انجام شود، بنابراین اینها نیز به عنوان جرایم تحت این کنوانسیون گنجانده می‌شوند.

ماده ۲۲ به "*فساد کودکان*" می‌پردازد و بنابراین در معرض قرار دادن کودکان به سوءاستفاده جنسی یا فعالیت‌های جنسی را جرم‌انگاری می‌کند. با توجه به حجم زیاد موادی که سوءاستفاده یا فعالیت جنسی را در فضای مجازی نشان می‌دهد، این موضع مهمی است که توسط شورای اروپا اتخاذ شده است. در واقع، مطالعات نشان داده‌اند که "دیدن پورنوگرافی آنلاین دومین خطر رایج در حدود ۴ نفر از هر ۱۰ نوجوان در سراسر اروپا است" (Livingstone & Haddon, 2009). مطالعات همچنین نشان می‌دهند که ملاقات با فردی که آنلاین ملاقات شده در یک موقعیت آفلاین، کمترین شکل رایج از تمام اشکال سوءاستفاده از طریق فضای مجازی است (Livingstone & Haddon, 2009).

با این حال، با آگاهی از اینکه این یکی از خطرناک‌ترین اشکال سوءاستفاده از طریق فضای مجازی است، کنوانسیون به این جرم درخواست از کودکان برای اهداف جنسی نیز پرداخته است. (کنوانسیون لانزاروته، ۲۰۰۷، ماده ۲۳)

مشابه ابزار سازمان ملل متحد، کنوانسیون لانزاروته تلاش برای ارتکاب جرایم مندرج در آن را جرم‌انگاری می‌کند. با این حال، به همدستی و مشارکت اشاره نمی‌کند، بلکه از عبارت "*کمک و مساعدت*" استفاده می‌کند. (کنوانسیون لانزاروته، ۲۰۰۷، ماده ۲۴) اگرچه به نظر می‌رسد این امر همان تفسیر را نشان می‌دهد، در واقعیت طیف گسترده‌تری از اقدامات را شامل می‌شود. همدستی نوعی قصد مشترک خاص در مشارکت در سوءاستفاده را نشان می‌دهد. با این حال، در مورد کمک یا مساعدت، صرفاً فراهم کردن یک خروجی یا وسیله‌ای که از طریق آن اعمال خاصی که جرم را تشکیل می‌دهند ممکن است انجام شود، کافی خواهد بود. اگرچه قصد همچنان عنصر مهمی در جرم است، به نظر می‌رسد که این قصد مشارکت در جرم نیست که در نظر گرفته می‌شود، بلکه قصد تسهیل ارتکاب جرم است.

مشابه ابزار سازمان ملل متحد، کنوانسیون لانزاروته تلاش برای ارتکاب جرایم مندرج در آن را جرم‌انگاری می‌کند. با این حال، به همدستی و مشارکت اشاره نمی‌کند، بلکه از عبارت "*کمک و مساعدت*" استفاده می‌کند. (کنوانسیون لانزاروته، ۲۰۰۷، ماده ۲۴) اگرچه به نظر می‌رسد این امر همان تفسیر را نشان می‌دهد، در واقعیت طیف گسترده‌تری از اقدامات را شامل می‌شود. همدستی نوعی قصد مشترک خاص در مشارکت در سوءاستفاده را نشان می‌دهد. با این حال، در مورد کمک یا مساعدت، صرفاً فراهم کردن یک خروجی یا وسیله‌ای که از طریق آن اعمال خاصی که جرم را تشکیل می‌دهند ممکن است انجام شود، کافی خواهد بود. اگرچه قصد همچنان عنصر مهمی در جرم است، به نظر می‌رسد که این قصد مشارکت در جرم نیست که در نظر گرفته می‌شود، بلکه قصد تسهیل ارتکاب جرم است.

شورای اروپا هنگام پرداختن به صلاحیت قضایی نیز رویکردی مشابه سازمان ملل متحد اتخاذ کرده است. ماده ۲۵ مقرر می‌دارد که دولت‌ها می‌توانند صلاحیت قضایی را در موارد زیر اعمال کنند:

- زمانی که جرم در قلمرو آن ارتکاب یابد (شامل کشتی‌های حامل پرچم آن و هواپیماهای ثبت شده تحت قوانین آن)؛
- توسط یکی از اتباع آن؛
- توسط شخصی که معمولاً در قلمرو آن اقامت دارد؛ یا

- زمانی که قربانی تبعه آن یا ساکن معمولی در قلمرو آن باشد.

با این حال، همانطور که در بند ۳ ماده ۲۵ اعلام شده، ممکن است از صلاحیت قضایی بر ساکنان معمولی غیرتبعه صرف‌نظر شود. با توجه به آزادی تردد اشخاص، این ممکن است منجر به معافیت برخی افراد از پیگرد قانونی شود. با این حال، این موضوع در بندهای بعدی مورد توجه قرار گرفته است که در آن مقرر شده دولت‌ها نباید خود را از اعمال صلاحیت قضایی در مواردی که شخصی به دلیل تابعیت مسترد نمی‌شود، محدود کنند. علاوه بر این، ماده ۲۵ بند ۴ استثنای بسیار مهمی را برای اصل دوگانگی که معمولاً در روند استرداد دنبال می‌شود، ایجاد می‌کند. این بخش مقرر می‌دارد که دولت‌ها نباید صلاحیت قضایی خود را بر اساس اینکه دولت دیگر چنین اعمالی را جرم‌انگاری نمی‌کند، محدود کنند. همچنین، در بند ۶، کنوانسیون بیان می‌کند که اعمال صلاحیت قضایی نباید با الزام قربانی به ثبت گزارش یا دولتی که در آن جرم ارتکاب یافته به اعلام جرم محدود شود. بنابراین، اصل زیربنایی همچنان به نظر می‌رسد این است که دولت‌ها تعهد دارند متهم ادعایی یافت شده در حوزه صلاحیت خود را تحت پیگرد قرار دهند.

همانطور که می‌توان متوجه شد، این کنوانسیون تنها به سوءاستفاده جنسی می‌پردازد، بنابراین قلدری سایبری مورد توجه قرار نگرفته است. با این حال، کنوانسیون اصل جالبی را به ویژه در رابطه با مبارزه با سوءاستفاده از کودکان در فضای مجازی معرفی می‌کند. با توجه به اینکه پورنوگرافی کودکان یکی از صنایع با سریع‌ترین رشد در وب است و شرکت‌ها و اشخاص حقوقی کاملی پشت آن هستند، این امر به تضمین چارچوب گسترده‌تری از حمایت از کودکان کمک خواهد کرد. در نهایت، کنوانسیون لانزاروته تأکید مداوم بر اهمیت همکاری بین دولت‌های عضو در طول تحقیقات و رسیدگی‌های بعدی دارد.

دومین ابزار شورای اروپا مرتبط با این بحث، کنوانسیون جرایم سایبری است که بخشی از آن نیز از کنوانسیون حقوق کودک سازمان ملل الهام گرفته شده است. با این حال، تنها در ماده ۹، که پورنوگرافی کودکان را تنظیم می‌کند، به طور خاص به سوءاستفاده از کودکان می‌پردازد. تحت این ماده، همان تعریف از آنچه پورنوگرافی را تشکیل می‌دهد که توسط کنوانسیون لانزاروته پذیرفته شده، استفاده می‌شود. همچنین مشابه کنوانسیون اخیر، هر تصویر واقع‌گرایانه‌ای که نشان‌دهنده افراد صغیر درگیر در "*رفتار جنسی صریح*" باشد را نیز پورنوگرافیک تلقی می‌کند. بنابراین، این کنوانسیون باید همراه با کنوانسیون لانزاروته خوانده شود. در واقع، در رابطه با پیگرد قانونی و جمع‌آوری شواهد، کنوانسیون جرایم سایبری مواد خاص‌تری را ارائه می‌دهد که به فناوری‌های اطلاعات و ارتباطات می‌پردازد. مواد ۱۶ تا ۲۱ مسائلی مانند حفظ، جستجو و توقیف داده‌های رایانه‌ای و ترافیک اینترنت، تولید چنین داده‌هایی و جمع‌آوری داده‌های ترافیک در زمان واقعی را تنظیم می‌کند. چنین مقرراتی در مبارزه با جرایم سایبری مهم هستند زیرا همچنین تعهدی را بر دولت‌ها تحمیل می‌کنند تا قوانین و مکانیسم‌های لازم را برای تنظیم نحوه برخورد با داده‌ها توسط ارائه‌دهندگان خدمات اینترنتی و سایر نهادهای مربوطه ایجاد کنند. علاوه بر این، این کنوانسیون برای اهداف همکاری بین دولت‌ها در مبارزه با سوءاستفاده از کودکان در فضای مجازی بسیار مهم است، زیرا برخلاف کنوانسیون لانزاروته، کنوانسیون جرایم سایبری توسط دولت‌های غیر اروپایی نیز به رسمیت شناخته شده است. در واقع، این کنوانسیون توسط کانادا و آفریقای جنوبی امضا شده و توسط استرالیا، ژاپن و ایالات متحده تصویب شده است (Council of Europe, 2001).

۳. اسناد در سطح محلی

قانون جزای مالت رویکردی بسیار گسترده در نظر گرفتن آنچه که سوءاستفاده تلقی می‌شود، اتخاذ کرده است. به نظر می‌رسد قلدری سایبری در محدوده ماده ۲۵۱ الف که به آزار و اذیت می‌پردازد، قرار می‌گیرد (Ghio, 2010). اشاره خاص به استفاده از فناوری‌ها در ارتکاب جرم

در ماده ۲۰۴ د که به فعالیت‌های جنسی غیرقانونی می‌پردازد، ماده ۲۰۸ الف که به مالکیت و تولید مواد غیراخلاقی تصویرکننده افراد صغیر اشاره دارد و ماده ۲۰۸ الف الف که درخواست از کودکان برای اهداف جنسی (آماده‌سازی کودکان) را جرم‌انگاری می‌کند، صورت گرفته است. تمام این مقررات بازتاب مواردی است که در اسناد بین‌المللی پیش‌تر مورد بحث قرار گرفت. علاوه بر این، مطابق با مقررات کنوانسیون لانزاروت، نه تنها شهروندان مالتی بلکه ساکنان دائمی نیز مسئول چنین جرایمی هستند.

علاوه بر مقررات مندرج در قانون جزا، در فوریه ۲۰۰۳ واحد جرایم سایبری مالت تأسیس شد. این واحد شاهد افزایش پرونده‌هایی بوده که به صورت روزانه با آن‌ها سروکار دارد، به طوری که در سال ۲۰۰۳ به یک مورد در هفته می‌رسید، در حالی که در سال ۲۰۱۱ با ۲ مورد در روز مواجه بود. اگرچه همه این جرایم شامل سوءاستفاده از کودکان نمی‌شود، واحد جرایم سایبری تأکید ویژه‌ای بر اهمیت گزارش سوءاستفاده از کودکان دارد. در واقع، این واحد همچنین یک پورتال اینترنتی ایجاد کرده است که از طریق آن می‌توان موارد سوءاستفاده آنلاین را گزارش کرد.از تحلیل فوق می‌توان استدلال کرد که در سطح قانونگذاری و اجرا، به نظر می‌رسد مالت به تعهدات بین‌المللی خود پایبند است و حمایت از کودکان را از طریق قانون جزای خود تضمین می‌کند. با این حال، همانطور که در پیش‌نویس سیاست ملی کودکان برجسته شده است، این کافی نیست. همین سیاست استدلال می‌کند که به نظر می‌رسد مالت در سایر تعهدات خود برای ایجاد کمپین‌های آگاهی‌بخشی مناسب کوتاهی می‌کند. در واقع، گزارش اخیر معرفی کمپین‌های آموزشی بیشتر با هدف قرار دادن هم کودکان و هم والدین را توصیه می‌کند. علاوه بر این، این گزارش از معرفی مجازات‌های سخت‌تر برای ارتکاب جرایم مورد بحث و اتخاذ مکانیسم‌های مؤثرتر مانند "*بستن وب‌سایت‌های سوءاستفاده از کودکان برای جلوگیری از قربانی شدن مجدد [و نه] صرفاً مسدود کردن وب‌سایت‌های ناقض چنین اعمالی*" حمایت می‌کند ("Draft National Children's Policy," 2011).

۴. چارچوب‌های حقوقی مقابله با کودک‌آزاری آنلاین در اسناد بین‌المللی و قوانین ملی

نقش چارچوب‌های بین‌المللی و اسناد حقوق بشری

چارچوب‌های بین‌المللی و اسناد حقوق بشری، سنگ بنای اصلی در ایجاد یک نظام حمایتگرانه برای مقابله با کودک‌آزاری آنلاین محسوب می‌شوند و نقش تعیین‌کننده‌ای در تضمین حقوق بنیادین کودکان در فضای مجازی دارند. در رأس این اسناد، کنوانسیون حقوق کودک سازمان ملل متحد (CRC) قرار دارد که تقریباً به‌طور جهانی به تصویب رسیده و دولت‌های عضو را ملزم می‌کند تا با اتخاذ قوانین، سیاست‌ها و اقدامات اجرایی، حقوق کودکان را در تمامی محیط‌ها از جمله فضای دیجیتال تضمین کنند. این کنوانسیون با تأکید بر اصل منافع عالیه کودک و حق دسترسی ایمن به فناوری‌های اطلاعاتی، کشورها را متعهد می‌سازد تا به پیشگیری از هرگونه بهره‌کشی یا آزار آنلاین بپردازند و سازوکارهای حمایتی و قضایی لازم را فراهم آورند (Gil, 2025).

نقش شورای اروپا و همکاری فراملی

شورای اروپا با اسناد راهبردی و کنوانسیون‌هایی همچون کنوانسیون بوداپست در مورد جرایم سایبری و دستورالعمل‌های حمایتی از حقوق دیجیتال کودکان، چارچوبی هماهنگ برای کشورها ایجاد کرده است تا با همکاری فراملی، جرایم مرتبط با آزار آنلاین کودکان را رصد، پیگیری و مجازات کنند. این اسناد نه تنها بر تقویت همکاری‌های قضایی و پلیسی بین‌المللی تأکید دارند بلکه کشورها را به ایجاد نظام‌های ردیابی محتوا، آموزش والدین و توسعه پلتفرم‌های امن تشویق می‌کنند (Hosseini Akbarnejad & Javaheri Arasteh, 2020).

قوانین نمونه در ایالات متحده

اجرای عملی این چارچوب‌ها در سطح ملی از طریق قوانین خاص صورت می‌گیرد. در ایالات متحده، قانون حفاظت از حریم خصوصی کودکان از جمله مهم‌ترین نمونه‌ها است که گردآوری، استفاده و افشای اطلاعات شخصی کودکان زیر ۱۳ سال را منوط به رضایت والدین کرده و شرکت‌های فناوری را مکلف به رعایت استانداردهای سختگیرانه نموده است. همچنین قانونCIPA ، مدارس و کتابخانه‌های عمومی را ملزم به استفاده از نرم‌افزارهای فیلترکننده محتوای مضر برای کودکان کرده تا دسترسی به وب‌سایت‌های نامناسب به حداقل برسد (Gil, 2025).

رویکرد کشورهای اروپایی

کشورهای اروپایی مانند آلمان و انگلیس، مقررات سختگیرانه‌ای برای کنترل محتوای آنلاین وضع کرده‌اند. به عنوان مثال، آلمان با تصویب قانونNetzDG ، پلتفرم‌های اجتماعی را ملزم به حذف محتوای مجرمانه در مدت زمان کوتاه کرده است. اتحادیه اروپا نیز در مقررات عمومی حفاظت از داده‌ها(GDPR) ، برای پردازش داده‌های کودکان زیر ۱۶ سال، الزام به کسب رضایت والدین را مقرر کرده و بدین ترتیب امنیت داده‌های شخصی کودکان را تضمین نموده است (Hosseini Akbarnejad & Javaheri Arasteh, 2020). مجموعه اسناد بین‌المللی و قوانین ملی، با یکدیگر چارچوبی جامع برای مقابله با کودک‌آزاری آنلاین تشکیل می‌دهند. این رویکرد نه‌تنها به کاهش وقوع این جرایم کمک می‌کند بلکه امکان حمایت حقوقی از قربانیان، پیگیری قضایی مرتکبان و ایجاد یک محیط دیجیتال امن و سالم برای رشد و شکوفایی کودکان را فراهم می‌آورد (Gil, 2025).

۵. نقش نهادهای بین‌المللی در حمایت از کودکان در فضای مجازی

نقش نهادها و سازمان‌های بین‌المللی در حمایت از کودکان در فضای مجازی بسیار حیاتی و گسترده است. سازمان ملل متحد از طریق «پیمان‌نامه حقوق کودک» مصوب ۱۹۸۹، چارچوبی الزام‌آور برای حمایت از کودکان در شرایط مختلف از جمله فضای دیجیتال ایجاد کرده است. «کمیته حقوق کودک سازمان ملل» در تفسیر عمومی شماره ۲۵ (۲۰۲۱) درباره حقوق کودکان در فضای دیجیتال، دولت‌ها را موظف می‌سازد تا امنیت کودکان، حفظ حریم خصوصی آن‌ها و پیشگیری از سوءاستفاده‌های آنلاین را تضمین کنند (Faramarziyani et al., 2025). این تفسیر علاوه بر حمایت‌های قانونی، بر آموزش، آگاهی‌بخشی و توسعه ابزارهای محافظتی برای کودکان و والدین تأکید می‌کند (همان، ۷).

شورای اروپا نیز با تصویب «کنوانسیون بوداپست» درباره جرائم سایبری و «کنوانسیون لانزاروت» درباره حمایت از کودکان در برابر سوءاستفاده جنسی، مجموعه‌ای از تعهدات را برای دولت‌ها مقرر کرده است. این اسناد بر جرم‌انگاری تولید و انتشار محتوای سوءاستفاده جنسی از کودکان و ایجاد سازوکار همکاری بین‌المللی در تعقیب مجرمان تأکید دارند. افزون بر این، شورا با انتشار راهنماهای عملی از شرکت‌های فناوری می‌خواهد امکان گزارش‌دهی سریع محتوای آسیب‌زا را فراهم کنند (Mahdizadeh Langroudi, 2022). یونیسف نیز در گزارش‌های سالانه خود تأکید می‌کند که ارتقای سواد دیجیتال کودکان و والدین و همکاری دولت‌ها با بخش خصوصی برای ایجاد محیطی ایمن، کلید کاهش خطرات فضای آنلاین است. این سازمان با تدوین دستورالعمل‌های سیاستگذاری و برنامه‌های آموزشی، به کشورها کمک می‌کند تا در برابر تهدیدات سایبری علیه کودکان آماده‌تر باشند (محمدکریمی، ۱۳۹۷، ۵۲).در سطح عملیاتی نیز نهادهایی مانند کارگروه جنایات اینترنتی علیه کودکان (ICAC) در ایالات متحده با ایجاد شبکه‌ای از همکاری‌های قضایی و پلیسی، به شناسایی و تعقیب مجرمان جنسی آنلاین کمک

می‌کنند (Taghizadegan, 2023). این مدل همکاری در بسیاری از کشورها به عنوان الگو برای آموزش پلیس، توسعه نرم‌افزارهای حفاظتی و ارتقای آگاهی خانواده‌ها مورد استفاده قرار می‌گیرد (Sadeghi & Panabad, 2017)

۶. حمایت از کودکان در فضای مجازی؛ چارچوب‌های بین‌المللی و ملی

حمایت از کودکان در فضای مجازی یکی از مهم‌ترین موضوعات حقوق بشر در عصر دیجیتال است. کنوانسیون حقوق کودک سازمان ملل که در سال ۱۹۸۹ تصویب شد، برای نخستین‌بار اصولی کلی درباره حق دسترسی ایمن کودکان به اطلاعات و حفاظت از آنان در برابر خشونت و سوءاستفاده ارائه کرد (United Nations, 1989). در ادامه، کمیته حقوق کودک در تفسیر عمومی شماره ۲۵ تصریح نمود که دولت‌ها باید راهکارهای مشخصی برای حفاظت از داده‌های شخصی کودکان، نظارت بر محتوای دیجیتال و تضمین محیطی امن در فضای آنلاین ایجاد کنند.

در سطح منطقه‌ای، شورای اروپا با تصویب کنوانسیون بوداپست درباره جرایم سایبری، بستر حقوقی لازم برای مقابله با جرایم آنلاین علیه کودکان را فراهم ساخته و همکاری میان دولت‌ها را در زمینه تعقیب مجرمان تسهیل کرده است (Council of Europe, 2001). این شورا همچنین در کنوانسیون لانزاروت بر ضرورت پیشگیری از استثمار جنسی کودکان در فضای مجازی و توسعه سازوکارهای گزارش‌دهی سریع تأکید کرده است (Council of Europe, 2007). از منظر آموزشی، ارتقای سواد رسانه‌ای خانواده‌ها و آموزش‌های پیشگیرانه در مدارس یکی از مؤثرترین روش‌ها برای کاهش آسیب‌های فضای مجازی به شمار می‌رود. پژوهش‌ها نشان داده‌اند که ترکیب سیاست‌های آموزشی با فناوری‌هایی مانند فیلترینگ هوشمند و سامانه‌های نظارت والدین می‌تواند نقش مهمی در محافظت از کودکان ایفا کند (Rashidi, 2019). علاوه بر این، سازمان یونیسف در گزارش‌های سالانه خود بر آموزش والدین و کودکان درباره خطرات فضای مجازی و ضرورت همکاری دولت‌ها برای توسعه ابزارهای حمایتی تأکید کرده است. این سازمان همچنین برنامه‌هایی برای آموزش سواد دیجیتال در کشورهای در حال توسعه اجرا کرده است تا والدین توانایی بیشتری در کنترل محتوای نامناسب داشته. در حقوق ایران نیز پژوهش‌های اخیر نشان می‌دهند که رویکرد قانون‌گذار عمدتاً بر جرم‌انگاری رفتارهای مجرمانه علیه کودکان متمرکز بوده و در حوزه پیشگیری نیازمند تقویت مقررات است (Faramarziyani et al., 2025). پیشنهاد شده است که نظام حقوقی ایران با بهره‌گیری از اسناد بین‌المللی و تجربه سایر کشورها، راهبردی جامع برای پیشگیری، حمایت و آموزش تدوین کند (Taghizadegan, 2023). به‌طور کلی، همگرایی میان اسناد بین‌المللی، سیاست‌های ملی و اقدامات خانواده‌ها ضروری است تا کودکان بتوانند با امنیت و اعتماد بیشتری از فرصت‌های فضای دیجیتال بهره‌مند شوند (Gil, 2025; Taghizadegan, 2023).

۷. حفاظت از کودکان در فضای مجازی: چارچوب‌های بین‌المللی، همکاری‌های منطقه‌ای و نقش قوانین ملی

حمایت از کودکان در فضای مجازی به یکی از اولویت‌های حیاتی نظام‌های حقوقی و سیاست‌گذاری بین‌المللی تبدیل شده است، چرا که رشد سریع فناوری‌های دیجیتال و دسترسی گسترده کودکان به اینترنت، خطر سوءاستفاده و آزار آنلاین را افزایش داده است. اتحادیه اروپا با تدوین چارچوب‌های قانونی جامع تلاش کرده است محیط‌های دیجیتال را برای کودکان امن کند؛ این چارچوب‌ها شرکت‌های فناوری را ملزم به شناسایی و حذف محتوای سوءاستفاده جنسی از کودکان می‌سازد و با ایجاد مراکز تخصصی، هماهنگی حقوقی و اجرایی در سطح منطقه‌ای را تقویت می‌کند، به‌گونه‌ای که شفافیت و مسئولیت‌پذیری در عملکرد پلتفرم‌ها افزایش یابد و محیطی ایمن برای کودکان فراهم شود (Ragbar Moghadam et al., 2019). در سطح بین‌المللی، ائتلاف‌هایی با تبادل داده‌ها، توسعه فناوری‌های نوین و ارائه آموزش‌های عمومی، ظرفیت

جهانی مقابله با سوءاستفاده‌های آنلاین از کودکان را ارتقا داده و تجارب موفق کشورها را در اختیار دیگر دولت‌ها قرار می‌دهند تا اقدامات پیشگیرانه و واکنش‌های قانونی مؤثرتر شکل گیرد (فرجی، ابوبیه و بهنیافر، ۱۴۰۳، ۳۲).نمونه موفق همکاری منطقه‌ای در بالکان غربی مشاهده می‌شود، جایی که شبکه‌ای از مراکز اینترنت امن برای کودکان ایجاد شده است تا با آموزش والدین و کودکان، فراهم آوردن سامانه‌های گزارش‌دهی سریع و پشتیبانی از قربانیان، ظرفیت‌های ملی و هماهنگی اقدامات پیشگیرانه را تقویت کند و محیط دیجیتال را ایمن‌تر سازد (Hosseini Akbarnejad & Javaheri Arasteh, 2020). این رویکرد نشان می‌دهد که حفاظت از کودکان در فضای مجازی بدون ترکیب چارچوب‌های حقوقی، آموزش‌های گسترده و فناوری‌های حفاظتی مؤثر امکان‌پذیر نیست و همکاری‌های منطقه‌ای و بین‌المللی نقش محوری در افزایش اثربخشی این اقدامات دارند. به طور کلی، سیاست‌ها و همکاری‌های بین‌المللی، تلفیق قوانین سخت‌گیرانه، برنامه‌های آموزشی و فناوری‌های پیشگیرانه، محیطی ایمن و چارچوبی جامع برای حمایت از کودکان در فضای دیجیتال فراهم می‌آورند و تضمین می‌کنند که کودکان هم از حفاظت داده‌ها بهره‌مند شوند، هم از محتواهای مضر مصون بمانند و هم فرهنگ استفاده ایمن از اینترنت در میان آنان ترویج یابد (Hosseini Akbarnejad & Javaheri Arasteh, 2020).

۸. چالش‌ها و موانع اجرای اقدامات بین‌المللی، منطقه‌ای و محلی در مقابله با کودک‌آزاری سایبری

اجرای اقدامات بین‌المللی، منطقه‌ای و محلی برای مقابله با کودک‌آزاری در فضای سایبری با مجموعه‌ای از چالش‌ها و موانع متعدد مواجه است که در زمینه‌های حقوقی، فنی، فرهنگی و سازمانی نمود پیدا می‌کند. از نظر حقوقی، تفاوت‌ها و ناهماهنگی‌های قوانین ملی با استانداردهای بین‌المللی، نبود ضمانت اجرای مؤثر و پیچیدگی شناسایی عاملان بزه در فضای سایبری، اجرای کامل و مؤثر قوانین را با مشکل مواجه می‌سازد (Ghanizadeh Bafghi & Sareshki, 2023). در زمینه فرهنگی و اجتماعی، پایین بودن سطح آگاهی خانواده‌ها و جامعه نسبت به خطرات فضای مجازی و حقوق کودکان، آموزش ناکافی والدین و مربیان و مقاومت در پذیرش مسائل مرتبط با فضای سایبری، مقابله مؤثر با کودک‌آزاری را محدود می‌کند. همچنین کودکان به دلیل سن پایین و کمبود مهارت‌های تشخیص خطر، آسیب‌پذیرتر هستند. در حوزه فناوری، توسعه سریع ابزارها و فناوری‌های نوین، به‌ویژه فناوری‌های رمزنگاری، فعالیت‌های مجرمانه آنلاین را دشوارتر برای ردیابی کرده و نبود زیرساخت‌های فنی مناسب و ظرفیت محدود سیستم‌های امنیتی و پلیسی کشورهای مختلف، هماهنگی و اجرای اقدامات مقابله‌ای را با چالش مواجه می‌کند (Ghanizadeh Bafghi & Sareshki, 2023). علاوه بر این، عدم هماهنگی میان نهادها و سازمان‌های محلی، ملی و بین‌المللی در جمع‌آوری اطلاعات و تبادل تجربیات، نبود ساختارهای منسجم و پایدار همکاری و محدودیت‌های اطلاعاتی ناشی از حفاظت از حریم خصوصی، پیشرفت در مقابله با کودک‌آزاری سایبری را محدود می‌کند (Ghanizadeh Bafghi & Sareshki, 2023). با توجه به این چالش‌ها، تدوین راهکارهای جامع، آموزش مستمر والدین و کودکان، ارتقای فناوری‌های امنیتی و تقویت همکاری‌های بین‌المللی و بین‌بخشی برای اجرای مؤثر قوانین و حمایت از کودکان در فضای مجازی ضروری است.

نتیجه‌گیری

تحلیل‌های ارائه‌شده نشان می‌دهد که کشورهای مختلف از طریق قانون‌گذاری و اجرای مقررات توانسته‌اند گام‌های مهمی در مقابله با سوءاستفاده از کودکان در فضای مجازی بردارند. ایجاد چارچوب‌های قانونی، تصویب کنوانسیون‌ها و تدوین سیاست‌های ملی، پایه‌های مهمی برای حمایت از کودکان فراهم کرده است. با این حال، این چارچوب‌ها هنوز با چالش‌های قابل توجهی مواجه‌اند و کارآمدی کامل آن‌ها بدون همکاری بین‌المللی و هماهنگی میان نهادهای مختلف قابل تحقق نیست.

یکی از مهم‌ترین نکات روشن‌شده از این تحلیل، نیاز به تصویب گسترده‌تر اسناد و کنوانسیون‌های بین‌المللی و ترویج همکاری‌های چندسطحی میان کشورها است. این اقدامات می‌تواند تبادل اطلاعات، هماهنگی در اجرای قوانین و مقابله مؤثر با جرایم سایبری را تقویت کند. افزون بر آن، تحلیل‌ها نشان می‌دهد که قوانین به تنهایی کافی نیستند و پیشگیری از جرایم کودک‌آزاری دیجیتال مستلزم اقدامات آموزشی و ارتقای آگاهی عمومی نیز هست. آموزش کاربران، والدین، معلمان و کودکان درباره مخاطرات فضای مجازی، مسئولیت‌های اخلاقی استفاده از فناوری و پیامدهای احتمالی رفتارهای آنلاین، یکی از مهم‌ترین ابزارهای پیشگیرانه است که می‌تواند به کاهش قربانیان کمک کند.همچنین، تجربه‌های جهانی نشان می‌دهد که برخورد با کودک‌آزاری آنلاین نیازمند ترکیبی از اقدامات قانونی، فرهنگی و تکنولوژیک است. ایجاد فرهنگ مسئولانه در استفاده از اینترنت، ترویج اخلاق دیجیتال و توسعه مهارت‌های مقابله با تهدیدات آنلاین، می‌تواند محیطی امن‌تر و حمایتی‌تر برای کودکان فراهم کند. همکاری میان دولت‌ها، نهادهای قضایی و اداری، سازمان‌های اجرای قانون، ارائه‌دهندگان خدمات دیجیتال و خود کاربران، کلید موفقیت در این مسیر است.در نهایت، مبارزه با سوءاستفاده از کودکان در فضای مجازی یک نبرد از دست‌رفته نیست؛ بلکه نیازمند رویکردی جامع، چندسطحی و پایدار است که تمام ذینفعان در آن نقش فعال داشته باشند. تنها از طریق ترکیب سیاست‌های پیشگیرانه، اقدامات قانونی مؤثر و فرهنگ‌سازی مسئولانه می‌توان امنیت و رفاه کودکان را در محیط دیجیتال تضمین کرد و اثرات مخرب این نوع جرایم را به حداقل رساند. این نتیجه‌گیری بر اهمیت استمرار تلاش‌های بین‌المللی و ملی، ارتقای ظرفیت‌های نهادی و آموزش مستمر کاربران فضای مجازی تأکید دارد و نشان می‌دهد که آینده‌ای امن برای کودکان در فضای دیجیتال قابل دستیابی است، مشروط بر آن که همه بازیگران در این عرصه نقش فعال و هماهنگ ایفا کنند.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

The rapid digital transformation of contemporary societies has fundamentally reshaped patterns of communication, socialization, and access to information, creating unprecedented opportunities for children's participation in educational, cultural, and social environments while simultaneously exposing them to new forms of vulnerability and risk. The emergence of cyberspace has extended traditional forms of child abuse into transnational digital environments where geographical borders no longer limit criminal behavior, thereby requiring coordinated international legal responses grounded in human rights principles. The recognition of children's dignity and welfare as a universal concern is reflected in the near-universal ratification of the Convention on the Rights of the Child, which establishes a comprehensive framework obligating states to protect children against exploitation, abuse, and harmful digital exposure. Within this framework, online child abuse encompasses diverse manifestations including psychological harassment, cyberbullying, sexual exploitation, grooming, exposure to harmful content, and economic manipulation, all of which produce long-term psychological and social consequences affecting individual development and collective social security. The digital persistence of harmful content intensifies trauma because

abusive materials can remain accessible indefinitely, amplifying reputational harm and emotional distress. Consequently, contemporary legal scholarship emphasizes that combating online child abuse requires a shift from reactive criminal justice responses toward preventive, cooperative, and technologically informed governance mechanisms. International instruments emphasize broad interpretative approaches allowing emerging technological practices to be addressed without constant legislative revision, thereby enabling adaptability to evolving digital threats. The United Nations Convention on the Rights of the Child articulates obligations requiring states not only to prohibit sexual exploitation but also to adopt preventive and rehabilitative measures ensuring holistic protection of victims (United Nations, 1989). Subsequent legal developments—including optional protocols addressing child pornography and exploitation—expanded definitional clarity to encompass both real and simulated materials accessible through digital devices, reflecting awareness of technological manipulation and virtual reproduction risks. The conceptual expansion of abuse definitions is particularly significant in cyberspace because anonymity, remote access, and rapid data circulation facilitate offender mobility and complicate jurisdictional accountability. As digital technologies increasingly shape children's identities and social interactions, threats to online reputation and psychological security directly influence real-world well-being, highlighting the necessity of integrated legal, educational, and technological responses capable of safeguarding children within evolving digital ecosystems.

At the regional level, European legal frameworks represent one of the most advanced attempts to translate international child-protection norms into operational regulatory systems. With more than seventy-five percent of European minors actively engaged in online environments, regional institutions have recognized cyberspace as both a developmental opportunity and a domain of heightened risk requiring coordinated governance (Livingstone & Haddon, 2009). The Council of Europe's Lanzarote Convention introduced a comprehensive preventive model combining criminalization, awareness-raising, victim protection, and monitoring mechanisms designed to address sexual exploitation facilitated by information and communication technologies. This convention emphasizes not only prosecution but also prevention through education, professional training, and public awareness campaigns, thereby reflecting a shift toward proactive child-protection strategies. Importantly, it assigns responsibilities to private technology actors, encouraging self-regulation and co-regulation approaches that complement governmental oversight. Such collaboration recognizes that digital platforms and internet service providers possess technical capacities enabling rapid identification and removal of harmful content. Regional instruments further address jurisdictional challenges by expanding prosecutorial authority based on nationality, residence, or victim status, ensuring offenders cannot evade accountability through cross-border mobility. Differences among national legal systems—such as varying ages of sexual consent across European jurisdictions—demonstrate the complexity of harmonizing legal standards while preserving national sovereignty (Gil, 2025). Complementing the Lanzarote Convention, the Budapest Convention on Cybercrime provides detailed procedural mechanisms governing data preservation, digital evidence collection, and international cooperation, thereby strengthening investigative capabilities against technologically sophisticated crimes (Council of Europe, 2001). Together, these regional instruments illustrate how layered governance structures enhance enforcement capacity by integrating substantive criminal law with procedural and technological cooperation frameworks. Empirical findings concerning online risks—such as widespread exposure of adolescents to online pornography and digital harassment—reinforce the urgency of such coordinated regulatory approaches (Livingstone & Haddon, 2009).

National legal systems operationalize international and regional standards through domestic legislation, institutional development, and enforcement mechanisms tailored to local contexts. Comparative analysis demonstrates that effective child protection requires not only criminalization of harmful conduct but also institutional specialization and accessible reporting systems. The Maltese legal framework, for instance, adopts a broad understanding of abuse encompassing harassment, grooming, and possession of illicit digital material, reflecting alignment with international obligations (Ghio, 2010). The establishment of dedicated cybercrime units and online reporting portals illustrates the importance of institutional capacity in translating legal commitments into practical protection mechanisms. Nevertheless, policy evaluations reveal that legislative compliance alone does not guarantee effective prevention; public awareness campaigns, educational initiatives, and parental guidance remain essential components of comprehensive strategies. Similar patterns appear in broader comparative analyses showing that legal frameworks must be accompanied by preventive education and technological safeguards to reduce victimization risks. International human rights instruments serve as foundational normative references guiding domestic policy reform, encouraging states to adopt coordinated legislative, judicial, and educational responses protecting children's digital rights (Gil, 2025). Regional cooperation initiatives further demonstrate that harmonized approaches—such as coordinated monitoring systems and data-sharing arrangements—enhance the capacity of states to track transnational offenders and respond rapidly to emerging threats (Hosseini Akbarnejad & Javaheri Arasteh, 2020). The convergence of international norms and domestic implementation highlights an evolving paradigm in which child protection is viewed as a shared global responsibility requiring continuous adaptation to technological change and social transformation.

International organizations play a central role in operationalizing child protection norms by providing policy guidance, educational resources, and coordination mechanisms supporting national implementation. The United Nations Committee on the Rights of the Child has clarified state obligations in digital environments through interpretative guidance emphasizing privacy protection, digital literacy, and preventive education (Faramarziyani et al., 2025). These interpretations underscore that safeguarding children online extends beyond criminal prosecution to encompass empowerment through education and awareness. The Council of Europe reinforces this approach by encouraging rapid reporting systems and collaboration between governments and technology companies to identify harmful content efficiently (Mahdizadeh Langroudi, 2022). International organizations such as UNICEF contribute through capacity-building programs promoting digital literacy among children, parents, and educators, thereby addressing vulnerabilities arising from insufficient awareness and supervision. Operational models such as Internet Crimes Against Children (ICAC) task forces demonstrate how cross-agency collaboration strengthens investigative effectiveness and supports victim assistance mechanisms (Taghizadegan, 2023). Research also highlights the importance of combining educational initiatives with technological tools such as parental monitoring systems and intelligent filtering technologies to reduce exposure to harmful content (Rashidi, 2019). The integration of educational, legal, and technological strategies reflects a holistic understanding of child protection that recognizes prevention, enforcement, and rehabilitation as mutually reinforcing components. Emerging international coalitions facilitate data exchange, technological innovation, and dissemination of best practices, enabling states with limited resources to benefit from shared expertise and collective learning processes (Ragbar Moghadam et al., 2019). These collaborative networks demonstrate that global governance structures increasingly

function as dynamic ecosystems linking legal norms, institutional practices, and technological innovation in pursuit of safer digital environments for children.

Despite significant progress, the implementation of international, regional, and national measures encounters substantial legal, technological, cultural, and organizational challenges that limit overall effectiveness. Jurisdictional fragmentation remains a major obstacle because disparities among national laws complicate prosecution of cross-border cybercrimes and create enforcement gaps exploitable by offenders. Rapid technological innovation—including encryption technologies and anonymization tools—further complicates investigative processes and evidence collection. Cultural factors also influence implementation outcomes, as variations in societal attitudes toward digital risks and limited parental awareness reduce preventive capacity. Children's developmental characteristics, including limited risk perception and digital literacy, increase vulnerability to manipulation and exploitation. Additionally, insufficient coordination among governmental institutions, law-enforcement agencies, and international partners hampers information sharing and delays responses to emerging threats. Structural limitations such as inadequate technical infrastructure and resource disparities among states exacerbate enforcement challenges, highlighting global inequalities in cybersecurity capacity. Scholars emphasize that effective responses require comprehensive strategies integrating legal harmonization, technological innovation, continuous training of professionals, and sustained international cooperation (Ghanizadeh Bafghi & Sareshki, 2023). Privacy concerns also present complex dilemmas, as enhanced monitoring measures must balance child protection with fundamental rights to data protection and freedom of expression. These multifaceted challenges illustrate that combating online child abuse is not solely a legal issue but a multidimensional governance problem requiring coordinated action across legal, technological, educational, and cultural domains.

The analysis ultimately demonstrates that combating child abuse in cyberspace depends on the integration of international norms, regional cooperation mechanisms, national legislation, institutional capacity, technological innovation, and public awareness initiatives within a coherent multilevel governance framework. Sustainable child protection requires the simultaneous strengthening of preventive education, victim support systems, cross-border investigative cooperation, and accountability mechanisms for digital platforms. Long-term effectiveness lies not only in criminalization but also in cultivating digital ethics, promoting responsible internet use, and empowering children and families with knowledge and skills necessary to navigate online environments safely. Building resilient digital ecosystems demands collaboration among governments, international organizations, private technology companies, educators, families, and civil society actors. Through coordinated policymaking, continuous institutional learning, and adaptive regulatory strategies, societies can transform cyberspace into an environment that preserves innovation and connectivity while ensuring the safety, dignity, and well-being of children.

References

Council of Europe. (2001). Convention on Cybercrime (CETS No. 185).

Council of Europe. (2007). Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

Draft National Children's Policy. (2011).

Faramarziyani, M., Nikbin, M., & Raoufi, A. (2025). Protection of Children's Rights in Cyberspace from the Perspective of the United Nations System and Iranian Law. *Comparative Law Quarterly*, *55*(1), 697-718.

Ghanizadeh Bafghi, M., & Sareshki, A. H. (2023). Cyber Grooming and Entrapment of Children; Challenges and Solutions. *Cyberspace Law*.

Ghio, A. (2010). The Rise of the Cyber Bully. *ICT Law Malta*. http://ictlawmalta.blogspot.com/2010/09/rise-of-cyber-bully.html

Gil, E. (2025). *Helping Abused and Traumatized Children*. Arjmand Publications.
Hosseini Akbarnejad, H., & Javaheri Arasteh, M. (2020). Criminal Protection of Children Against Abuse in Cyberspace in Iranian and English Laws and International Documents. *Legal Research*, *19*(44), 107-132.
Livingstone, S., & Haddon, L. (2009). *EU Kids Online: Final Report*. https://doi.org/10.46692/9781847427342
Mahdizadeh Langroudi, H. (2022). Criminological Study of the Crime of Psychological Child Abuse in Cyberspace with a Study of the Opinions of Imami Jurists. 4th International Conference on Jurisprudence, Law, Psychology and Educational Sciences,
Ragbar Moghadam, R., Roshan, M., & Jamalianzadeh, S. B. (2019). Cyberspace and its Effects on Children and Adolescents. 2nd International Conference on Psychology, Educational Sciences and Social Studies,
Rashidi, M. (2019). *The Harms of the Internet and Cyberspace on Children and Adolescents*. Zarrin Andishmand Publishing.
Sadeghi, A., & Panabad, S. (2017). *Child Abuse*. Pazhuheshgar Bartar.
Taghizadegan, M. (2023). Children and Cyberspace. *Cultural and Communication Studies*, 55-60.
United Nations. (1989). Convention on the Rights of the Child.