Applied Criminology Research
پژوهش های جرم شناسی کاربردی
دوره ۲ / شماره ۴/ تابستان ۱۴۰۳
تاریخ دریافت: ۱۴۰۳/۰۲/۱۱
تاریخ پذیرش: ۱۴۰۳/۰۴/۲۷
صفحه: ۱ الی ۲۴

Volume 2, Issue 4, Summer 2024
Received: 2024/04/30
Date of Acceptance: 2024/07/17
Pages: 1-24

Article Type: **Research**
نوع مقاله: پژوهشی

System: qacr.ir doi: 10.22034/ AQCR.2025.2049110.1047

Cybersecurity of children and adolescents in cyberspace (Case study: citizens over 18 years of age in Tehran)

Maryam Vali Zadeh[1]

Abstract

Field and Aims: The cyber space is more of a threat to children and adolescents than an opportunity for development and progress. Accordingly, studying the cybersecurity of children and adolescents in cyberspace; pathology and neutralization of risks is an important necessity and study goal.

Method: The research method is a survey type and the statistical population of the research includes all citizens over 18 years of age in Tehran, who, based on the estimation of sample size tables and Cochran's formula, 384 people were selected as the sample size in a multi-stage cluster in Tehran only. The research hypotheses were tested in the form of a structural equation model using Amos Graphics software. The sample size is citizens over 18 years of age in Tehran.

Findings and Conclusions: Documentary findings are a support for developing the model, and in the tested model, the results show that neutralizing cyberspace risks with a coefficient of (-0.72) has a negative effect on cyberspace pathology, and also that neutralizing cyberspace risks has a positive and significant effect on cybersecurity with a coefficient of (0.77), and the greater the neutralization of space risks, the greater the level of cybersecurity of children and adolescents.

Keyword: Cybersecurity, Neutralizing Risks, Cyberspace, Children and Adolescents.

❋Citation (APA): Vali Zadeh, M. (2024). Cybersecurity of children and adolescents in cyberspace (Case study: citizens over 18 years of age in Tehran). *Applied criminology research*, 2(4), 1-24.
https://qacr.ir/article_720757.html?lang=en

1. Researcher Candidate in Criminal Law and Criminology, Karaj Branch, Islamic Azad University, Karaj, Iran. Email: vlizade.mrym@gmail.com

دوره ۲ / شماره ۴/ تابستان ۱۴۰۳
تاریخ دریافت: ۱۴۰۳/۰۲/۱۱
تاریخ پذیرش: ۱۴۰۳/۰۴/۲۷
صفحه: ۱ الی ۲۴

پژوهش های جرم شناسی کاربردی
Applied Criminology Research

Volume 2, Issue 4, Summer 2024
Received: 2024/04/30
Date of Acceptance: 2024/07/17
Pages: 1-24

نوع مقاله: پژوهشی
Article Type: **Research**

سامانه: qacr.ir doi: 10.22034/ AQCR.2025.2049110.1047

امنیت سایبری اطفال و نوجوانان در فضای مجازی
(مورد مطالعه: شهروندان بالای ۱۸ سال در شهر تهران)

مریم ولی زاده[۱]

چکیده

زمینه و هدف: فضای مجازی بیش از آنکه برای اطفال و نوجوانان فرصتی برای تحول و پیشرفت باشد، تهدیدی برای به‌انحراف‌کشیده‌شدن آنها است. بر همین اساس، مطالعه امنیت سایبری اطفال و نوجوانان در فضای مجازی، آسیب‌شناسی و خنثی‌سازی مخاطرات یک ضرورت و هدف مطالعاتی مهم است.

روش: روش پژوهش از نوع پیمایشی بوده و جامعه آماری پژوهش شامل همه شهروندان بالای ۱۸ سال در شهر تهران هستند که بر اساس برآورد جداول حجم نمونه و فرمول کوکران، تعداد ۳۸٤ نفر به صورت خوشه‌ای چندمرحله‌ای فقط در شهر تهران، به عنوان حجم نمونه، انتخاب شده‌اند. فرضیات پژوهش در قالب مدل معادله ساختاری با استفاده از نرم‌افزار Amos Graphics آزمون‌شده از شهروندان بالای ۱۸ سال در شهر تهران است.

یافته‌ها و نتایج: یافته‌های اسنادی پشتوانه‌ای برای تدوین مدل بوده و در مدل آزمون‌شده نیز نتایج نشان داده خنثی‌سازی خطرات فضای مجازی با ضریب (۰/۷۲-) اثر معکوسی بر آسیب‌شناسی فضای مجازی دارد و همچنین، خنثی‌سازی خطرات فضای مجازی اثرش بر امنیت سایبری با توجه به ضریب (۰/۷۷)، مثبت و معنادار است و هرچقدر خنثی‌سازی خطرات فضای بیشتر باشد، میزان امنیت سایبری اطفال و نوجوانان نیز بیشتر خواهد شد.

کلیدواژه‌ها: امنیت سایبری، خنثی‌سازی خطرات، فضای مجازی، اطفال و نوجوانان.

❋ استناددهی (APA): ولی زاده، مریم. (۱٤۰۳). امنیت سایبری اطفال و نوجوانان در فضای مجازی (مورد مطالعه: شهروندان بالای ۱۸ سال در شهر تهران). *پژوهش‌های جرم‌شناسی کاربردی*، ۲(٤)، ۲٤-۱.
https://qacr.ir/article_720757.html

۱. پژوهشگر دکتری حقوق جزا و جرم‌شناسی، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران.
رایانامه: vlizade.mrym@gmail.com

مقدمه

تحولات عمده در حوزه فناوری، انقلاب در زندگی اطفال و نوجوانان نیز تأثیر زیادی بر جا گذاشته است. والدین امروزی به جهت درگیری در فعالیت‌های متنوع اجتماعی، گاهی امکان کنترل فعالیت های فرزندان خود را ندارند و کودکان زمان قابل‌توجهی را در تعامل با فضای مجازی[1] صرف می کنند. زمانی که صحبت از فضای مجازی به میان می آید، مردم اغلب به موبایل و رایانه‌ای فکر می‌کنند که به اینترنت متصل است؛ در حالی که این فقط بخش بسیار کوچکی از فضای مزبور را تشکیل می‌دهد. فضای مجازی، فضایی است که از اتصال رایانه هایی پدید آمده است که تمامی انسان ها، ماشین ها و منابع اطلاعاتی در جهان را به هم متصل کرده است (اسپادا[2]، ۲۰۱٤: ۲۰۸) و در چنین وضعیتی، یک ضرورت مهم، ایجاد امنیت سایبری در این فضا است. همه کاربران، صرف‌نظر از سن، هنگام گذراندن زمان قابل‌توجهی در اینترنت در معرض خطرات امنیتی مختلفی قرار دارند. برای پرداختن به این خطراتی که کاربران اینترنت در زندگی روزمره خود با آن مواجه می‌شوند، از اصطلاحات مختلفی استفاده می‌شود. امنیت سایبری، امنیت آنلاین، امنیت آنلاین و امنیت اینترنت به‌جای یکدیگر در ادبیات برای رسیدگی به نگرانی‌های امنیتی در دنیای دیجیتال استفاده می‌شوند. امنیت سایبری یک اصطلاح پرکاربرد با دیدگاه‌های مختلف است. امنیت فضای مجازی برای کودکان به دلیل افزایش دسترسی به اینترنت و شبکه‌های اجتماعی مجازی برای کودکان و در نتیجه، قرارگرفتن آنها در معرض خطرات مختلف آنلاین بسیار مورد توجه قرار گرفته و به موضوعی به سرعت در حال رشد تبدیل شده است (قیوم، کروز و ژاکری[3]، ۲۰۲۱: ۲).

فضای مجازی در زندگی کودکان از نحوه بازی کودکان تا استفاده برای آموزش و تحصیل، حضور پررنگی دارد و مساله محافظت از اطلاعات آنها در این فضا یکی از ضروریات مهم در ارتباط با آنها است. همچنین، ارتباط کودکی با اینترنت و فضای مجازی همچنان تجربهٔ جدیدی است که در این فضا همان‌گونه که قابلیت‌های آموزش و یادگیری را در سطح بسیار بالایی برای کودکان و نوجوانان فراهم می کند، به همان میزان دارای ظرفیت ورود آسیب‌ها و

---

۱. «فضای سایبر» با «فضای مجازی» متفاوت است؛ گرچه در ادبیات سیاست‌گذاری، بعضاً این دو واژه، یکی انگاشته شده و فضای مجازی در معنا و به‌جای فضای سایبر بکار رفته است؛ ولی فضای سایبر با وجود اشتراک زیادی با فضای مجازی، دقیقاً معادل آن نیست؛ چرا که فضای سایبر، فضای مجازی و غیرواقعی نیست، بلکه محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و توسط رایانه‌های متصل به‌هم به صورت شبکه‌ای، نظیر شبکه اینترنت، در آن روی می‌دهد (کرامتی، ۱۳۹۹: ۲۱).

2. Spada
3. Quayyum, Cruzes & Jaccheri

ناملایماتی برای کودکان نیز هست. قلدری، سوءاستفادهٔ جنسی از کودکان، بردگی جنسی، قاچاق کودکان و خیلی از موارد نقض قانون در صورت عدم کنترل این فضا وجود داشته و در آینده نیز خواهد داشت و در صورت عدم اتخاذ تمهیدات مناسب، می‌تواند در آینده روند رو به افزایشی داشته باشد (فینکلور، والش، جونز، میشل و کولیر[1]، ۲۰۲۱: ۱۲۳۳)؛ چرا که حتی رفتارهایی را که در دنیای واقعی حقیقی خود، حتی به ذهن او خطور نکند، در دنیای سایبری مرتکب می‌شود (نجفی ابرندآبادی، ۱۴۰۲: ۱۱۸). بر این مبنا، فضای مجازی این ظرفیت را دارد که بسیاری از جنبه‌های زندگی اطفال و نوجوانان را تغییر دهد و در حالی که می‌تواند اثرات مثبتی داشته باشد، به همان اندازه خطراتی را متوجه آنها کند. مهم‌ترین تهدیدهایی که اطفال و نوجوانان در مواجه با فضای مجازی ممکن است درک کنند، نقض حریم خصوصی، امنیت داده‌های آنها، درک تبعیض و سوءاستفاده از اخلاق دیجیتال خواهد بود. لذا، ایجاد مکانیسم‌های مؤثر حفاظت از حریم خصوصی اطفال و نوجوانان به منظور حفظ امنیت اطفال و نوجوانان در فضای مجازی اولین اقدام ضروری است که مستلزم آسیب‌شناسی و خنثی‌سازی خطرات احتمالی در این حوزه است. علاوه بر این، ایمنی داده‌های کودکان و امنیت سایبری به ویژه در زمینه استفاده از فضای مجازی باید به عنوان راهبردی پیشگیرانه از مخاطرات مطرح شود. بنابراین، این پژوهش با هدف ایجاد امنیت سایبری اطفال و نوجوانان در فضای مجازی به شناسایی و آزمون خنثی‌سازی مخاطرات می‌پردازد.

ادبیات مفهومی و نظری پژوهش

امروزه، فن‌آوری اطلاعات و ارتباطات به خصوصی‌ترین لایه‌های زندگی بشر نفوذ کرده و دایره شمول آن، هر روز بیشتر از دیروز می‌شود. با اذعان به فواید این تکنولوژی، شواهد موجود مؤیّد این مسئله است که اگر در بهره‌مندی از آن، استانداردهای لازم رعایت نشود، آثار زیانبار و غیرقابل‌جبرانی به بار خواهد آورد. این فن آوری بر تمامی اقشار سِنّی جامعه اثر مستقیم و غیرمستقیم دارد، اما به نظر می‌رسد کودکان با توجه به ویژگی‌های خود مهمترین قربانی مضرات این پدیده باشند؛ چرا که از توانایی‌های لازم برای بهره‌مندی سالم و مثبت از این تکنولوژی برخوردار نیستند (بادامی، مقدادی و پیله‌ور، ۱۴۰۱: ۴۵۷). از طرفی هم گسترش حضور اقشار مختلف جامعه در فضای مجازی، با وجود تمام محاسن آن، نگرانی‌هایی را بر خانواده‌ها تحمیل کرده و موضوعی است که در میان معضلات امروزی، بسیار خودنمایی می‌کند. استفادهٔ فزایندهٔ اطفال و نوجوانان از ابزارهای جذاب محیط‌های مجازی باعث شده

1. Finkelhor, Walsh, Jones, Mitchell, & Collier

است که یک محیط خصوصی در داخل خانه و مدرسه برای فرزندان ایجاد شود و آن‌ها بدون نظارت قابل‌توجهی، به دنیای رنگارنگ مدرن وارد شوند. تنها در صورتی می‌توان از این محیط به‌عنوان محیط مناسب آموزشی برای اطفال و نوجوانان بهره‌برداری کرد که جذابیت‌های آن کاهش نیابد، زیرا در آن صورت کودک و نوجوان به آموزش‌های این محیط تعلق خاطر دارند و بدون اصرار والدین، به تربیت صحیح خو می‌گیرند (اسپادا، ۲۰۱٤: ۲۰۸). بنابراین، امنیت سایبری در سه حوزه کلی نیاز است برقرار باشد و این حوزه‌ها به ترتیب شامل امنیت شبکه و سیستم‌ها، امنیت اطلاعات و داده‌ها و امنیت اطلاعات شخصی است که برای کودکان و حتی بزرگسالان حفظ این امنیت لازم و ضروری است. بر پایه ادبیات نظری موجود و با توجه به موضوع پژوهش، ادبیات نظری مرتبط با امنیت سایبری اطفال در فضای مجازی در دو حوزه کلی قابل‌بررسی است. در اولین گام، نیاز به آسیب‌شناسی امنیت سایبری و در گام دوم، لازم است راهبردهای خنثی‌سازی مخاطرات شناسایی شوند.

۱. آسیب‌شناسی فضای مجازی برای اطفال

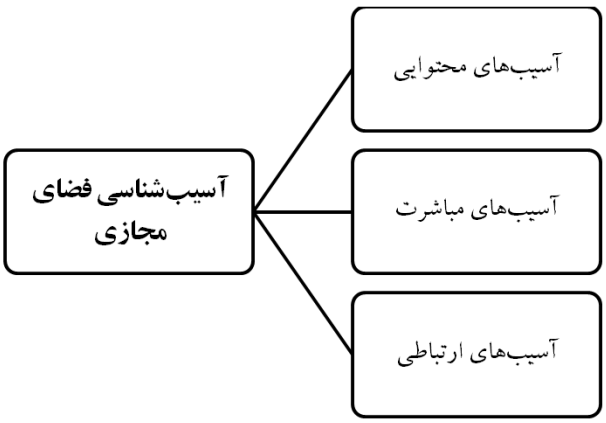
در عصر کنونی، افزایش دسترسی به اینترنت و استفاده گسترده از تلفن‌های هوشمند توسط اطفال و نوجوانان، در فضای مجازی و رسانه‌ای که شاید یکی از مدرن‌ترین محیط‌های مؤثر در تربیت به شمار می‌آید، تبدیل به یک منبع نگران‌کننده شده است و تربیت و پرورش فضائل اخلاقی در این طیف را در فضای مجازی به موضوع روز نهادهای علمی و فرهنگی تبدیل نموده است. چنین رفتارهایی به وسیله رسانه‌های ارتباطی همچون برنامه‌های تلفن همراه نظیر شبکه‌های اجتماعی مجازی، ایمیل، اتاق‌های گفتگو (چت آنلاین) و... با محتویات تهدیدات اینترنتی، اشاعه ناهنجاری‌های اخلاقی، سوءاستفاده جنسی، استثمار آنلاین، مزاحمت‌های سایبری، آموزش ناهنجاری‌ها و... در حال گسترش است و موجب تضییع حق تربیت کودکان معصوم شده است. این پدیده فراتر از محدودیت‌ها و مرزهای جغرافیایی، نژادی، طبقاتی، مذهبی و فرهنگی علیه کودک دیده می‌شود و فراگیری آن به حدی است که تمام ابعاد زندگی وی را دربرمی‌گیرد. به تعبیری، قاره ششم یا فضای مجازی بیشترین مکان و جمعیت جهان، به ویژه کودکان، را به خود اختصاص داده است (بادامی، مقدادی و پیله‌ور، ۱٤۰۱: ٤۵۸). کودکان و نوجوانان که پیش از این به عنوان یکی از مهمترین و در عین حال، آسیب‌پذیرترین اقشار جامعه همواره به نحو جدی در معرض انواع بزه‌دیدگی و صدمات جبران‌ناپذیر جسمی، روانی، اجتماعی و... قرار داشته‌اند، به لحاظ شرایط ویژه و کاربرد وسیع فناوریهای نوین اطلاعات و ارتباطات در عصر حاضر، بیش از هر زمان دیگر در معرض خطر قرار گرفته‌اند. نتیجهٔ این امر،

تأیید و تأکید نظامهای حقوقی و اجتماعی مختلف، اعم از داخلی و بین‌المللی، بر اصل لزوم حمایت ویژه از کودکان و نوجوانان می‌باشد (محسنی، ۱۳۹۰: ۱۳۷).

همچنین، کودکان اغلب در فضای مجازی به‌علت هیجانی که از اظهار هویت خود دارند، بیشتر از بزرگسالان در معرض فاش‌کردن اسرار و حریم شخصی خود هستند؛ چرا که کودکان به جهت عدم آگاهی نسبت به حریم شخصی و خصوصی خود بیشتر از بزرگسالان در نقض حریم خصوصی خود نقش فعال ایجاد می‌کنند. از نظر خطرات امنیتی اطلاعات شخصی و درز اطلاعات خصوصی کاربران اینترنت، خردسالان توانایی تشخیص بدافزارها و جاسوس‌افزارها را ندارند و در فضای اینترنت از خدمات آنلاین با خطرپذیری بالاتری مانند نرم‌افزارهای مخرب استفاده می کنند؛ برای مثال، جرائم آنلاین مانند آلوده‌کردن رایانهٔ خانواده که والدین از آن برای خدمات بانکی برخط استفاده می‌کنند، در کمین کودکان قرار دارد. جاسوس‌افزار تجاری، در وب گاه‌های کودکان قرار داده می‌شود و در دستگاه کاربر ذخیره می‌شود تا رفتار آنلاین او را نظارت کنند و این نظارت ممکن است برای اهداف دیگر، به‌عنوان بازاریابی آنلاین اطلاعات استفاده شود. بنابراین، باید راهکارهای لازم برای تضمین امنیت کودکان در اینترنت پیش‌بینی و به‌موقع اجرا گذارده شود (لاگینووا و فورنالووا[1]، ۲۰۱۸: ۷۸). سند «امنیت و سلامت کودکان آنلاین»[2] به انجام تلاش‌های گسترده‌ای در انگلستان منجر شده است. بر اساس مفاد این سند، از تولیدکنندگان محصولات تجاری در فضای مجازی، معلمان و سایر متصدیان برخورد و تعامل با کودکان خواسته شده تا توصیه‌های سند را در ارتباط با کودکان جدی بگیرند. به طور کلی در این سند، خطرات آنلاینی که کودکان را تهدید می‌کند، به سه دستهٔ مهم خطر محتوایی، خطر مباشرت و خطر ارتباطی تقسیم شده است. خطر محتوایی باعث می‌شود که در محیط اینترنت، کودکان محتوای نامناسبی را دریافت کنند؛ از جملهٔ این محتواها می توان به پورنوگرافی، خشونت زیاد یا محتواهایی شامل سخنان تنفرآمیز (تبعیض‌آمیز) یا افراطی اشاره کرد. در خطر مباشرت نیز کودکان ممکن است در فضای اینترنت در یک‌سری فعالیت های مضر به حال خود، درگیر شوند. این فعالیت ها شامل قلدری، فعالیت‌های جنسی، تجاوز، رفتار تهاجمی یا چشم چرانی، رفتار وحشیانه یا رفتارهایی شوند که به خود کودک آسیب شدید وارد می‌کند؛ علاوه بر این، فعالیت‌هایی نظیر خودکشی، پرخوری افراطی، کم‌اشتهایی یا کم‌خوری افراطی، سوءمصرف الکل و مواد مخدر نیز در این فضا به کودکان آموزش داده می‌شود. در خطر ارتباطی نیز در اثر ارتباط با افراد خطرناک در اینترنت ممکن

1. Lagíňová & Fornálová
2. Children's Online Safety and Health

است خطرات و عواقب وخیمی دامن گیر اطفال شود؛ مثلاً، آدرس‌دادن به افراد خطرناک یا ارائه اطلاعاتی نظیر مساعدت عبور و مرور از مدرسه به خانه یا فاش‌کردن مواقع تنهایی در خانه، همگی می‌تواند برای کودکان خطرآفرین باشد (بنیاد واچ اینترنت[1]، ۲۰۲۱: ۳). البته، این در حالی است که برخی از پیامدهای ناامنی در فضای سایبری ممکن است آسیب و صدمه‌ای جدی در پی نداشته باشند، اما این فعالیت‌ها منجر به یک فعالیت غیرقانونی می‌شوند؛ که در آینده می‌توانند زمینه انحرافات جدی در کودکان را فراهم آورد. همچنین، برخی از فعالیت‌های آنلاین مانند استثمار جنسی، عکس‌های برهنه گرفتن و پخش‌کردن آن‌ها، قاچاق آنلاین کودکان، سوءاستفادهٔ فیزیکی یا روانی از بچه‌ها، خریدوفروش مواد مخدر، پورنوگرافی و بسیاری از انحرافات مشابه فقط مختص به کودکان نیست، ولی به جهت اثرپذیری کودکان، آن‌ها احتمالاً راحت‌تر درگیر این اعمال انحرافی می‌شوند (لاگینووا و فورنالووا[2]، ۲۰۱۸: ۷۸). برای فهم بهتر این رویکرد نظری، ابعاد آسیب‌شناسی امنیت سایبری اطفال و نوجوانان به تصویر کشیده شده است.



نمودار ۱- ابعاد آسیب‌شناسی امنیت سایبری اطفال و نوجوانان در فضای مجازی

۲. خنثی‌سازی مخاطرات فضای مجازی برای اطفال و نوجوانان

در کشور انگلستان، بیش از سایر کشورها راهبردهای خنثی‌سازی مخاطرات سایبری مورد توجه قرار گرفته است. در همین ارتباط، سند راهگشایی برای تضمین امنیت کودکان آنلاین در انگلستان توسط شورای سلامت اینترنت کودکان انگلستان به نام «امنیت و سلامت کودکان

1. Internet Watch Foundation
2. Lagíňová & Fornálová

آنلاین» درخصوص سرویس‌های اینترنتی و شبکه‌های اجتماعی صادر شده است. در این سند، محتوای فضای آنلاین، راهبردهای مقابله‌ای با سوءرفتار آنلاین، مقابله با سوءاستفاده از کودکان یا برخوردهای قانونی، حفظ حریم خصوصی و هوشیاری (آگاهی‌دادن) و آموزش همگی برای تضمین امنیت کودکان در فضای مجازی مورد تاکید قرار گرفته‌اند. با توجه به اینکه بزهکاری اطفال و نوجوانان از دیرباز در این کشور در صدر توجهات سیاستمداران قرار داشته است و رسانه‌های گروهی نیز در انگلستان بر مسأله افزایش نرخ جرم در میان اطفال و نوجوانان تمرکز دارند، تلاش های صورت‌گرفته در این کشور برای مقابله با مخاطرات فضای مجازی در قلمرو اطفال و نوجوانان می‌تواند مفید باشد (فینکلور، والش، جونز، میشل و کولیر[1]، ۲۰۲۱: ۱۲۳۳). علاوه بر این، در سند مذکور رهنمودهای عملی، مثال‌های کاربردی و توصیه‌هایی در جهت تضمین امنیت کودکان در فضای مجازی وجود دارد. همچنین، امروزه کودکان زمان قابل‌توجهی را به صورت آنلاین صرف اهداف آموزشی یا سرگرمی می کنند. اینترنت فرصت‌های زیادی را ارائه می‌دهد و خطرات متعددی را به همراه دارد. با توجه به سن اطفال و نوجوانان، ارزیابی فرصت‌ها و خطرات استفاده از اینترنت و سیستم‌های دیجیتال برای آنها دشوار است، حتی با توجه به اینکه بیشتر و بیشتر زندگی آنها به صورت دیجیتالی ثبت می شود و به طور بالقوه، اثرات بلندمدتی بر حریم خصوصی آنها ایجاد می کند که اغلب اوقات، خانواده‌ها متوجه خطرات آن نمی‌شوند؛ بنابراین، آن‌ها به راحتی می‌توانند قربانی سوءاستفاده های آنلاین شوند. همراه با اقدامات متقابل فنی، آگاهی و اقدامات امنیتی می تواند به کاربران کمک کند تا از خطرات عدم امنیت سایبری جلوگیری کرده یا آن را کاهش دهند. در حالی که شیوه‌های امنیتی به عوامل متعددی متکی هستند، یک عامل میزان آگاهی و (آموزش) توانمندسازی افراد برای ارزیابی خطر و به‌کارگیری دانش برای کاهش تهدیدها و خنثی‌سازی آنها است (جرتسن، جیره، بارتنز و فلورس[2]، ۲۰۱۷: ٦٠). در بیشتر کشورهای دنیا، قوانینی در قالب سند و یا دستورالعمل‌هایی برای حفاظت از کودکان در فضای مجازی وجود دارد. این اسناد و دستورالعمل‌ها تولیدکنندگان محتواهای فضای مجازی را مورد خطاب قرار می‌دهند که آن‌ها باید با توجه به آموزش‌ها و آگاهی‌های ضروری که کسب می‌کنند، به کاربران کودک و نوجوان، والدین آن ها و مدارس کمک کنند که مبانی اساسی جهت تضمین امنیت اینترنت و فضای مجازی را یاد بگیرند (قیوم، کروز و ژاکری[3]، ۲۰۲۱: ۳). علاوه بر این، تقویت

1. Finkelhor, Walsh, Jones, Mitchell & Collier
2. Gjertsen, Gjære, Bartnes & Flores
3. Quayyum, Cruzes & Jaccheri

ظرفیت‌های جامعه نیز می‌تواند در این زمینه مفید باشد. به طور کلی، طراحان شبکه‌های اجتماعی مجازی باید مرکز امنیت اینترنت را برای همهٔ افراد قابل‌دستیابی سازند و نه اینکه فقط برای کاربران، این منشورها و مراکز امن در دسترس قرار گیرد. بدین طریق، والدین اطفال و نوجوانان می توانند قبل از اینکه اجازهٔ دسترسی فرزندانشان به این سایت ها را بدهند، از منشورها و امنیت سایت‌ها و صفحات اجتماعی مجازی اطمینان حاصل کنند. به طور کلی، راهبردهای زیر برای خنثی‌سازی مخاطرات عدم امنیت سایبری مورد توجه هستند.

۱. خنثی‌سازی مخاطرات از طریق آگاهی‌دادن

قرارگرفتن در معرض محتوای نامناسب یکی از نگرانی های رایج برای اطفال و نوجوانان است. بنابراین، آگاهی از امنیت سایبری به عنوان روشی برای آموزش کاربران اینترنت به منظور حساس‌بودن به تهدیدات سایبری مختلف و آسیب‌پذیری رایانه‌ها و داده‌ها در برابر این تهدیدات تعریف شده است. همچنین، آگاهی از امنیت سایبری به عنوان درجه درک کاربران در مورد اهمیت امنیت اطلاعات و مسئولیت‌های آنها برای اعمال سطوح کافی از کنترل اطلاعات برای محافظت از داده‌ها و شبکه‌های سازمان تعریف شده است و بر اساس این تعاریف، آگاهی از امنیت سایبری دو هدف اصلی دارد: هدف اول، هشداردادن به کاربران اینترنت در مورد خطرات امنیت سایبری و هدف دوم، افزایش درک کاربران اینترنت از خطرات امنیت سایبری تا به اندازه کافی متعهد به پذیرش امنیت در هنگام استفاده از اینترنت باشند (جیاناکاس، پاپاسالوروس، کامبوراکیس و گریتزالیس[1]، ۲۰۱۹: ۸۳). قوانین محافظت از کودکان در مقابل فضای مجازی در اغلب کشورها به تولیدکنندگان محتوای فضای مجازی خاطر نشان می‌کنند که الگوهایی برای آگاه‌سازی والدین و خود اطفال و نوجوانان به‌منظور حفظ امنیت فضای مجازی در نظر گیرند. آن‌ها اغلب منشورها و دستورالعمل‌هایی را طراحی کرده‌اند که به نحو بسیار آسان، آگاهی‌های لازم را به والدین و کودکان ارائه می‌دهند. این آگاه‌سازی حاوی نکات راهبردی و مرحله‌به‌مرحله هستند که در گام اول، اطلاعات و آگاهی‌های به‌روز درخصوص استفادهٔ امن از سرویس‌های خاص ارائه می‌شود. در گام دوم، باید یک مرکز امن در هر صفحهٔ اجتماعی طراحی شود و کاربران به راحتی بتوانند به آن دسترسی پیدا کنند. در گام سوم، باید برای کاربران کودک، قوانین ارتباطی صحیح توضیح و به آن‌ها هشدار داده شود و توجه آن‌ها به این هشدارها جلب شود. در نهایت، در آخرین گام، راه‌های پذیرش (اکسپت)، مسدودکردن (بلاک‌کردن) و قفل‌کردن ارتباطات با افراد مختلف به

1. Giannakas, Papasalouros, Kambourakis & Gritzalis

نحو ساده و روشن در صفحات اجتماعی (شبکه‌های اجتماعی مجازی) به کودکان توضیح داده شود (بنیاد واچ اینترنت[1]، ۲۰۲۱: ۵). به طور کلی، فنّاوری امروز با وجود تمام محاسن و خدمات گسترده، استعدادی سرشار در تأثیرگذاری منفی بر زندگی اطفال و نوجوانان دارد. فضای سایبری موجب اجتماعی‌شدن اطفال و نوجوانان شده، ولی در عین حال ویژگی کنجکاوی و ریسک‌پذیری، فضایی مستعد برای ارتکاب بزه و به‌طور مشخص، جرائم رایانه‌ای شده است. البته، با آموزش صحیح و ابزارهای نظارتی امن می‌توان دانش‌آموزان را آگاه و مصون کرد (رضازاده، آقاصرام، میزانیان و مصطفوی، ۱۳۹۸: ۲۷).

۲. خنثی‌سازی مخاطرات از طریق آموزش و توانمندسازی

امنیت سایبری به موضوع مهمی برای اکثر کشورها تبدیل شده است که نیازمند جستجو برای روش‌های جدید آموزش است و یکی از بهترین راه‌های آموزشی خنثی‌سازی مخاطرات در حوزه امنیت سایبری اطفال و نوجوانان، استفاده از انیمیشن‌های آموزشی و نمایش عروسکی و برنامه‌های کاربردی در این حوزه است. مسئولان ذی‌ربط در این حوزه با استفاده از نظرات کارشناسی، راهکارهای مقابله با این تهدیدات و فرهنگ استفادهٔ صحیح از فضای مجازی را تشریح می‌کنند و به واسطه رسانه‌های جمعی، این آموزش‌ها به اطفال و والدین منتقل می‌شود. به طور کلی، این ابزارها می‌تواند باعث افزایش و ارتقای فرهنگ امنیت در فضای مجازی باشد؛ چرا که از نظر آموزشی، این مدل یادگیری، هم‌افزایی از آموزش با سرگرمی و بازی را نشان می‌دهد که ممکن است تجربیات یادگیری کودکان را به طور کلی افزایش دهد (چادویک[2]، ۲۰۱۶: ۱). از طرفی هم کودکان در حال حاضر، کاربران مکرر اینترنت هستند و به طور فزاینده‌ای، دستگاه‌های آنلاین خود را دارند. آن‌ها می‌توانند خیلی سریع با وسایل الکترونیکی آشنا شوند. بنابراین، محبوبیت اینترنت و شبکه‌های اجتماعی مجازی در میان این گروه سنی به طور فزاینده‌ای افزایش یافته است. بر همین اساس، برنامه آموزش و توانمندسازی در کشور انگلستان یکی از راهبردهای مهم برای خنثی‌سازی خطرات اینترنتی برای همه شهروندان است و دولت بریتانیا شهروندان خود را موظف می‌کند که از امنیت سایبری خود مراقبت کنند. سیاست‌گذاران این کشور توصیه‌های گسترده‌ای در قالب برنامه‌های آموزشی ارائه می‌دهند تا از این طریق از کودکان در مقابل جرائم سایبری محافظت کنند. در این راستا، والدین بریتانیایی، به عنوان بخشی از سیستم آموزشی، مسئولیت آموزش فرزندان

1. Internet Watch Foundation
2. Chadwick

خود در مورد امنیت سایبری را برعهده دارند. با وجود اینکه والدین بریتانیایی احساس می‌کنند که مسئولیت آموزش امنیت سایبری به فرزندانشان درست و مناسب است، با این حال، آن‌ها از مشاوره‌های مربوط به امنیت سایبری ارائه‌شده توسط دولت انگلستان بهره می‌برند (پایر و رنود[1]، ۲۰۲٤: ۷۸). در قسمت بسیار مهمی از سند «امنیت و سلامت کودکان آنلاین»،[2] تمرکز بر مسئلهٔ آموزش و آگاهی مورد توجه قرار گرفته است. در این سند عنوان شده است که مسئلهٔ بسیار مهم این است که باید برای اطفال و نوجوانان فرصت‌هایی فراهم شود که خودشان به سمت محتواهای مضر و منحرف گرایش پیدا نکنند. اگر آن‌ها را با روشی درست آموزش بدهیم و حق انتخاب را برای خودشان قائل شویم، آنها هم از مزایای عصر دیجیتال بهره می‌برند و با آگاهی مراقب خود و همسالانشان خواهند بود و جامعه‌ای عاری از خطرات و تهدیدهای دنیای مجازی خواهند ساخت (بنیاد واچ اینترنت[3]، ۲۰۲۱: ٤).

با ایجاد بسترهای مناسب در برخورد با امکانات و آسیب‌های فضای مجازی و تبدیل این محیط به یک محیط آموزشی مناسب، می‌توان ضمن رعایت حقوق و آزادی‌های کودکان و نوجوانان، از ابزار پیشگیری جامعه‌مدار برای اجرای اهداف خود، یعنی عدم گرایش اطفال و نوجوانان کشورمان به بزهکاری، بهترین استفاده را برد (ملکوتی و محسنی، ۱٤۰۲: ۲۰۷).

در چند سال اخیر، برنامه‌های تحقیقاتی و آموزشی درباره امنیت سایبری برای کودکان توجه قابل‌توجهی را هم از سوی صنعت و هم از سوی محققان جلب کرده است و مطالعات زیادی خطرات بالقوه امنیت سایبری را برای کودکان مورد بررسی قرار داده‌اند. بر اساس این مطالعات، توانمندسازی کودکان در برای حفاظت از رمز عبورها، حریم خصوصی آنلاین و فیشینگ به پلتفرم‌های آموزشی زیادی برای کودکان در مورد خطرات امنیت سایبری و موضوعات مرتبط نیاز دارد (دزیمپلز، هاندرز و واندسومپل[4]، ۲۰۲۰: ۲). یکی از مصادیق توانمندسازی در انگلستان برای سهولت گزارش آنلاین از طریق کودکان با قراردادن آیکونی خاص به نام (ClickCEOP) در سایت‌های خود این امکان را برای کودکان فراهم نموده‌اند که با فشردن این آیکون سریعاً، گزارشی مبنی بر اعمال خشونت آنلاین برای سازمانی مشخص در این زمینه ارسال می‌گردد و سریعاً، از این طریق می‌توانند فرد مجرم را مورد شناسایی قرار دهند (آندرو، آلثور و چتی[5]، ۲۰۲۰: ۱۲۵).

1. Prior & Renaud
2. Children's Online Safety and Health
3. Internet Watch Foundation
4. Desimpelaere, Hudders & Van de Sompel
5. Andrews, Alathur & Chetty

۳. خنثی‌سازی مخاطرات از طریق تقویت ظرفیت‌های جامعه

در کنار توسعهٔ خدمات فضای مجازی برای اطفال و نوجوانان باید به فکر بهبود فرهنگ استفاده از اینترنت در میان گروه سنی مذکور نیز بود. به همین منظور و در راستای نهادینه‌کردن فرهنگ استفادهٔ صحیح اطفال و نوجوانان از فضای مجازی، نهادهایی مانند سازمان فناوری اطلاعات، وزارت آموزش‌وپرورش، پلیس و... در زمینه فرهنگ‌سازی و آموزش اطفال و نوجوانان سهیم خواهند بود. بسیاری از کشورها پروژه‌های کلانی با عنوان «کودک و اینترنت» با هدف آشنایی اطفال و نوجوانان با آسیب‌ها و تهدیدات فضای مجازی و ارائهٔ آموزش‌ها و نحوهٔ مقابله با چالش‌های فضای مجازی انجام داده‌اند و در نتیجه، این پروژه‌ها با برگزاری کارگاه‌های آموزشی باعث آشنایی کودکان و والدین ایشان با فرصت‌ها و تهدیدهای مهم فضای مجازی بوده است (اسپادا، ۲۰۱٤: ۲۲۰). همچنین، یکی از مهمترین تدابیری که نقش بسزایی در کاهش بزه‌دیدگی اطفال و نوجوانان در شبکه‌های اجتماعی مجازی دارد، تدابیر پیشگیرانه در قالب کنترل و نظارت است؛ شورای عالی فضای مجازی و پلیس فتا دو نهاد مهم سیاست‌گذار و اجرایی هستند که در زمینه پیشگیری از بزه‌دیدگی کودکان در فضای مجازی نقش‌آفرینی کلیدی دارند و می‌توانند از طریق ایجاد محدودیت‌های دسترسی به شبکه‌های اجتماعی و همچنین، با اعمال نظارت و کنترل در این فضا، هدف پیشگیری از بزه‌دیدگی کودکان در شبکه‌های اجتماعی را بیش‌ازپیش تأمین کنند (منصورآبادی، میرخلیلی و کرامتی‌معز، ۱٤۰۰: ۳۰).

در عرصه‌های بین‌المللی نیز نهادهای بین‌المللی با مکانیزم‌های مختلفی حمایت و حفاظت از کودکان در برابر خطرات احتمالی فضای مجازی را مورد توجه قرار داده‌اند. به طور کلی، فکر ایجاد شورای عالی فضای مجازی به عنوان نهادی مستقل و فراقوایی دورنمای بسیار جالبی دارد، اما تا زمانی که اختیارات لازم به آن داده نشود و در هر قوه یا وزارتخانه متولی مستقلی برای حوزه فضای مجازی وجود داشته باشد، این شورا نمی‌تواند رسالت خود را پیش ببرد. همچنین، شورای عالی فضای مجازی توامان هم وظیفه تنظیم مقررات و هم وظیفه نظارت در فضای مجازی، به ویژه صیانت از حقوق بزه‌دیدگان آسیب‌پذیر، را داراست.

پلیس فتا نیز این قابلیت بالقوه را دارد که با استفاده از زیرساخت‌های سخت‌افزاری و نرم‌افزاری خود، دائماً این فضا را تحت نظارت و کنترل خود داشته باشد و در شبکه‌های اجتماعی مجازی، نقش نظارتی خود را در قبال پیشگیری از بزه‌دیدگی کودکان ایفا کند. به منظور یکسان‌سازی مقررات و نظارت بر مراجع و نهادهای کثیری که بر فضای اینترنت

قاعده‌انگاری و در این زمینه فعالیت می‌کنند، باید طراحی «نظام حقوق فضای مجازی»، ازجمله: سیاست‌گذاری، قانون‌گذاری و هماهنگی در اداره این فضا، به شورای عالی فضای مجازی واگذار شود. پیش‌بینی می‌شود در پرتو طراحی علمی این نظام بتوان وضعیت بهتری را در فضای مجازی شاهد بود و با بزهکاری و بزه‌دیدگی کمتری در این فضا روبه‌رو شد. پلیس فتا نیز با توجه به رشد تکنولوژی و به موازات آن، افزایش بی‌رویه جرم و الکترونیکی‌شدن ارتکاب آن در فضای مجازی، می‌تواند با بهره‌گیری از آموزه‌های جرم‌شناسی، از یک سو و استفاده از نرم‌افزارهای تخصصی پلیسی، از سوی دیگر، نقش موثری در این زمینه ایفا کند (منصورآبادی و همکاران، ۱٤۰۰: ۳۰). به طور کلی، همه کشورهای جهان به واسطه نیروهای امنیتی یا نیروهای پلیس اقدامات پیشگیرانه‌ای را برای حفاظت از اطفال در دستور کار قرار داده و در حوزه عمل نیز از شناسایی و ردیابی مجرمان اینترنتی و کشف جرائم مربوط به آنها به عنوان وظیفه اصلی این نیروها تعریف و مشخص شده است و تمام فعالیت‌های آنها بر همین حفاظت و پیشگیری متمرکز است. بنابراین، موضوع حفاظت از اطفال و نوجوانان در فضای مجازی مقوله نیازمند تعامل و همکاری لازم بین نهادهای مختلف جامعه و خانواده است. در سایه چنین تعاملی می‌توان از نتیجه‌دادن تلاش‌ها و موفقیت اقدامات و سیاستگذاری‌های مرتبط با امنیت سایبری اطفال اطمینان حاصل کرد (کیانی، حیدری و شادمان‌فر، ۱٤۰۳: ۵۳).

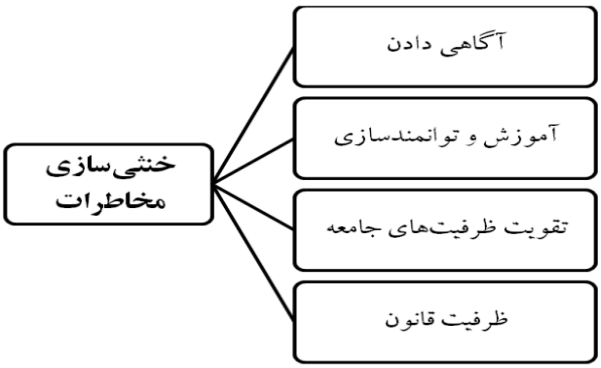
٤. خنثی‌سازی مخاطرات از طریق ظرفیت قانون

حفاظت از کودکان در اینترنت یک حوزه نگرانی نسبتاً جدید برای بسیاری از کشورها است که نیاز به ارزیابی مجدد سیاست‌های حقوقی موجود دولت و توسعه پاسخ‌های سیاست قانونی جدید دارد. در زمینه اهمیت این موضوع، تصور کنید پسر ده‌ساله شما در حال صحبت در خیابان با یک غریبه باشد. حداقل سعی خواهید کرد بفهمید این شخص کیست و با پسر شما چه موضوعات مشترکی برای گفتگو دارند. چه احساسی خواهید داشت وقتی کودک بگوید این دوست اوست، آن‌ها هر روز با هم ارتباط برقرار می‌کنند، آن‌ها در پارک با هم ملاقات می‌کنند و کودک نمی‌داند این مرد واقعاً چه کسی است و کجا کار می‌کند؛ این مثال قطعاً ترسناک است. با این حال، از نظر شیوع، احتمالاً در عمل به اندازه آشنایی‌های مشکوک در فضای اینترنت رایج نیست. مشکل محافظت از اطفال و نوجوانان در برابر چنین افراد مشکوک و بالقوه خطرناک در فضای اینترنت نگران‌کننده است. این موضوع به دلیل این واقعیت است

که «رشد اولیه اینترنت» با ظرفیت قانونی افراد زیر سن قانونی ناسازگار است (اروکینا و لتوتا[1]، ۲۰۲۰: ۶۰۷). خردسالان، قبل از رسیدن به بلوغ اجتماعی، در حال حاضر به طرز ماهرانه‌ای بر فناوری‌های مدرن تسلط دارند و کار طولانی خود را در رایانه با نیاز به تکمیل تکالیف خود توضیح می‌دهند. تقریباً ۹۲ درصد از خردسالان می‌توانند اقدامات بالقوه خطرناک فعال در فضای مجازی را از والدین خود پنهان کنند. این شامل تماشای محتوای نامناسب بر اساس سن، برقراری ارتباط با غریبه‌های خطرناک یا شرکت در قلدری آنلاین است. از سوی دیگر، فناوری‌های مدرن فرصت‌های گسترده‌ای را برای ارتباط و تحقق علایق می‌گشایند. سفر به فروشگاه با خرید از راه دور جایگزین می‌شود، مطالعه در سالن‌های کتابخانه با دسترسی آنلاین به وجوه آن و امکان دسترسی به کتابخانه جایگزین می‌شود. بر همین اساس، می‌توان انواع تهدیدات سایبری را برای اطفال و نوجوانان برجسته کرد. یکی از این تهدیدات، افشای اسرار شخصی و خانوادگی است که بر فعالیت‌های حرفه‌ای اطفال و اعضای خانواده‌اش تأثیر منفی دارد. علاوه بر این، برخی سرگرمی‌های ناهنجار مانند بازی در کازینوهای آنلاین می‌تواند خانواده یک طفل را در شرایط سخت مالی قرار دهد و به سلامت روان همه اعضای خانواده آسیب برساند. همچنین، اطفال و نوجوانان نیز ممکن است در معرض هرزه‌نگاری یا نژادپرستی و خشونت آنلاین قرار بگیرند (نارتیجاروی[2]، ۲۰۱۸: ۱۰۲۰). همان طور که بارها اشاره شد، محیط دیجیتال جدید، اطفال و نوجوانان را در معرض تهدیدات مختلف امنیت سایبری، از جمله سوءاستفاده از داده‌های آنها برای مقاصد سوء قرار می‌دهد. بر همین اساس، نیاز مبرم به قواعد حقوقی در حفاظت از داده‌های اطفال و نوجوانان در برابر تهدیدات امنیت سایبری برای جلوگیری از سوءاستفاده از کودکان ضرورت عصر حاضر شده و برای محافظت از امنیت آنلاین اطفال و نوجوانان، معاهدات بین‌المللی، مقررات منطقه‌ای و قوانین ملی در سطوح مختلف وارد عمل شده‌اند و همه این قواعد و قوانین بر حفظ حریم خصوصی آنان تأکید می‌کنند (گوپتا، کوماری و ساگاند[3]، ۲۰۲۳: ۱). بدون شک، به دلیل مشغله‌های کاری، والدین همیشه قادر به نمایندگی و حفظ منافع فرزندان و منافع خانواده در فضای اینترنت نیستند. امنیت سایبری شامل اقداماتی است که می‌تواند برای محافظت از یک دامنه سایبری، در مناطق عمومی، دولتی، نظامی و خانوادگی، در برابر تهدیداتی که می‌تواند به شبکه‌ها و زیرساخت‌های اطلاعاتی وابسته به هم آسیب یا ضرر برساند، مورد استفاده قرار گیرد. به طور

1. Erokhina & Letuta
2. Naarttijärvi
3. Gupta, Kumari & Sugandh

مستقیم یا غیرمستقیم، مسائل حمایت از اطفال و نوجوانان در اینترنت و یافتن بهترین ابزار برای چنین حمایتی در ادبیات حقوقی و سایر متون خاص مورد توجه قرار گرفته است (اروکینا و لتوتا[1]، ۲۰۲۰: ۶۰۸). بر همین اساس، از نظر بسیاری از محققان، ارزیابی رابطه بین حفاظت از داده‌های شخصی و لزوم نظارت بر پیام‌ها و رعایت اصول قانونی برای جوامع مهم و حیاتی است. به طور خلاصه، قواعد حقوقی می‌توانند از آسیب مجرمان سایبری در اینترنت به اطفال و نوجوانان جلوگیری کنند. برای همین منظور، اهمیت برنامه‌های آموزشی، از جمله پشتیبانی اطلاعاتی از برنامه برای محافظت از اطفال و نوجوانان در برابر جرائم سایبری مورد تاکید قرار گرفته است (نارتیجاروی[2]، ۲۰۱۸: ۱۰۲۰). بعضی کشورها به طور مشخص مانند آمریکا، ژاپن، استرالیا و روسیه استراتژی امنیت دیجیتال را به عنوان یک قانون برای حفاظت از حریم خصوصی آنلاین کودکان تدوین کرده‌اند. به طور کلی، تضمین امنیت سایبری افراد زیر سن قانونی توسط قوانین حقوقی نظارتی مختلف و برخی قوانین بین‌المللی تنظیم می‌شود؛ در این راستا، اعلامیه حقوق بشر کنوانسیون حمایت از حقوق بشر و آزادی‌های اساسی، کنوانسیون سازمان ملل متحد در مورد حقوق کودک و اخیراً، قانون «حمایت از کودکان در برابر اطلاعات مضر برای سلامت و رشد آنها» مصوب سال ۲۰۰۸، ایمنی و حریم خصوصی کودکان در اینترنت را مورد حفاظت قرار می‌دهد (روی، روی و سینا[3]، ۲۰۱۷: ۲۸۱).



نمودار ۲- ابعاد خنثی‌سازی مخاطرات ناامنی سایبری اطفال و نوجوانان در فضای مجازی

فرضیات پژوهش

1. Erokhina & Letuta
2. Naarttijärvi
3. Roy, Roy & Sinha

فرضیه اول: خنثی‌سازی مخاطرات فضای مجازی بر امنیت سایبری اطفال و نوجوانان اثر دارد.

فرضیه دوم: خنثی‌سازی مخاطرات فضای مجازی بر آسیب‌شناسی فضای مجازی اطفال و نوجوانان اثر دارد.

فرضیه سوم: آسیب‌شناسی فضای مجازی بر امنیت سایبری اطفال و نوجوانان اثر دارد.

روش

روش این پژوهش کمی از نوع پیمایشی بوده و بر مبنای هدف اصلی پژوهش که مطالعه امنیت سایبری اطفال و نوجوانان، آسیب‌شناسی و خنثی‌سازی مخاطرات بوده است، بعد از بررسی اسنادی نظریات موجود در این حوزه اطلاعات آماری برای آزمون فرضیات در بین شهروندان ۱۸ سال به بالای شهر تهران گردآوری شده است که بر اساس برآورد جداول حجم نمونه و فرمول کوکران، تعداد ۳۸٤ نفر حجم نمونه این پژوهش بوده‌اند. شیوه نمونه‌گیری به روش خوشه‌ای چندمرحله‌ای انجام شده است. انتخاب خوشه‌ها بر اساس پهنه جغرافیایی از کل مناطق ۱۱گانه شهر تهران، چهار منطقه (خوشه) به صورت تصادفی ساده به تناسب جمعیتی انتخاب شدند. سپس، داده‌ها، توسط نرم‌افزارهای Spss و Amos Graphics مورد تجزیه و تحلیل قرار گرفت. ابزار اندازه‌گیری در این پژوهش، پرسشنامه محقق‌ساخته است که با استفاده از برخی نظریات موجود مفاهیم و مولفه‌های آسیب‌شناسی امنیت سایبری اطفال و نوجوانان و خنثی‌سازی مخاطرات شاخص‌سازی شده‌اند. تحلیل داده‌ها نیز با استفاده از مدلسازی معادله ساختاری انجام شده است.

یافته‌های کمّی

آزمون فرضیات

فرضیه اول: خنثی‌سازی مخاطرات فضای مجازی بر امنیت سایبری اطفال و نوجوانان اثر دارد.

جدول ۱- آزمون همبستگی و تحلیل رگرسیون اثر خنثی‌سازی مخاطرات فضای مجازی بر امنیت سایبری اطفال

نام متغیر	R	R^2	B	Beta	T	F	Sig
خنثی‌سازی مخاطرات	۰/۷۲٤	۰/۵۲٤	٤/۰۳۵	۰/۷۲٤	۱۰/٦۵۳	۱۱۳/٤۸۲	۰/۰۰۰

بر اساس نتایج حاصله، همبستگی (R=۰/۷۲٤) مثبتی بین میزان خنثی‌سازی مخاطرات فضای مجازی و امنیت سایبری اطفال وجود دارد و بر همین اساس، مقدار R^2=۰/۵۲٤ نشان می‌دهد

که متغیر میزان خنثی‌سازی مخاطرات فضای مجازی توانسته است ۵۲ درصد از واریانس متغیر وابسته (امنیت سایبری اطفال) را تبیین نماید. با توجه به مقادیر T=۱۰/٦۵۳، F=۱۱۳/٤۸۲ و Sig =۰/۰۰۰، رابطه مشاهده‌شده بین دو متغیر در سطح ۹۹ درصد معنی‌دار است؛ لذا، فرضیه فوق تأیید می‌شود.

فرضیه دوم: خنثی‌سازی مخاطرات فضای مجازی بر آسیب‌شناسی فضای مجازی اطفال و نوجوانان اثر دارد.

جدول ۲- آزمون همبستگی و تحلیل رگرسیون اثر خنثی‌سازی مخاطرات فضای مجازی بر آسیب‌شناسی فضای مجازی

نام متغیر	R	R^2	B	Beta	T	F	Sig
خنثی‌سازی مخاطرات	-۰/٦۳۱	۰/۳۹۸	۱۲/۵۹۳	-۰/٦۳۱	-٦/۰۷۸	٦۸/۰۷٤	۰/۰۰۰

بر اساس نتایج حاصله، همبستگی (R=۰-/٦۳۱) معکوسی بین میزان خنثی‌سازی مخاطرات فضای مجازی و آسیب‌شناسی فضای مجازی اطفال وجود دارد و بر همین اساس، مقدار R^2=۰/۳۹۸ نشان می‌دهد که متغیر میزان خنثی‌سازی مخاطرات فضای مجازی توانسته است ٤۰ درصد از واریانس متغیر وابسته (آسیب‌شناسی فضای مجازی اطفال) را تبیین نماید. با توجه به مقادیر T=-٦/۰۷۸، F=٦۸/۰۷٤ و Sig =۰/۰۰۰، رابطه مشاهده‌شده بین دو متغیر در سطح ۹۹ درصد معنی‌دار است؛ لذا، فرضیه فوق تأیید می‌شود.

فرضیه سوم: آسیب‌شناسی فضای مجازی بر امنیت سایبری اطفال و نوجوانان اثر دارد.

جدول ۹- آزمون همبستگی و تحلیل رگرسیون اثر سیاستگذاری‌های شهرداری تهران (نمایشگاه‌های کتاب شهر) در سبک زندگی مطالعه‌محور

نام متغیر	R	R^2	B	Beta	T	F	Sig
آسیب‌شناسی فضای مجازی	-۰/٤۸۰	۰/۲۳۰	۳/۳٤۰	-۰/٤۸۰	-۵/۵۵۱	۳۰/۸۱٤	۰/۰۰۰

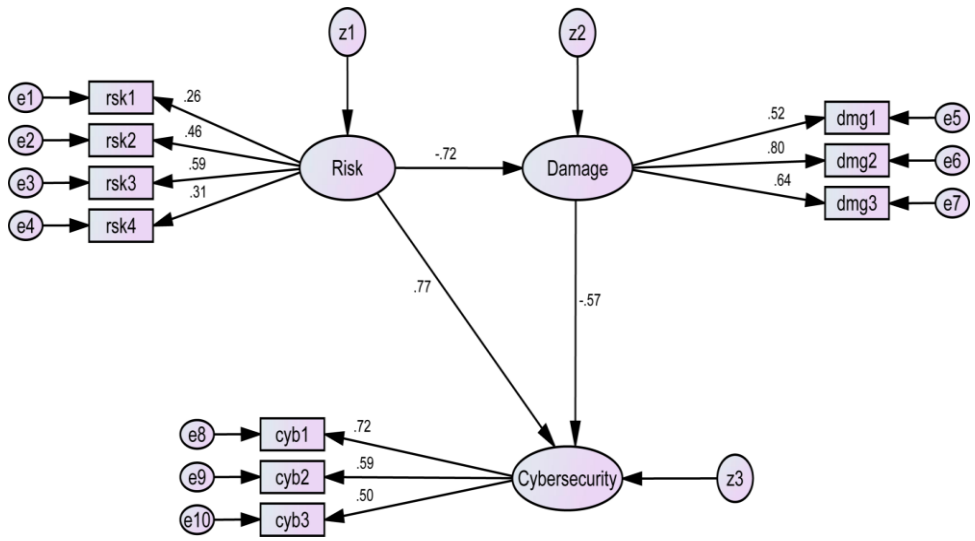
بر اساس نتایج حاصله، همبستگی (R=۰-/٤۸۰) معکوسی بین میزان آسیب‌شناسی فضای مجازی اطفال و امنیت سایبری اطفال وجود دارد و بر همین اساس، مقدار R^2=۰/۲۳۰ نشان می‌دهد که متغیر میزان آسیب‌شناسی فضای مجازی توانسته است ۲۳ درصد از واریانس متغیر وابسته (امنیت سایبری اطفال) را تبیین نماید. با توجه به مقادیر T=-۵/۵۵۱، F=۳۰/۸۱٤ و

Sig =۰/۰۰۰، رابطه مشاهده‌شده بین دو متغیر در سطح ۹۹ درصد معنی‌دار است؛ لذا، فرضیه فوق تأیید می‌شود.

در راستای آزمون فرضیات، مدلسازی معادله ساختاری نیز انجام شده است.

آزمون مدل معادله ساختاری پژوهش

در راستای آزمون اثرگذاری خنثی‌سازی مخاطرات بر آسیب‌شناسی امنیت سایبری اطفال، محقق از یک مدل معادله ساختاری استفاده کرده است که نحوه سنجش روابط در مدل را با علائم برداری نشان داده است. متغیرها و روابط موجود در مدل بر پایه پشتوانه نظری موجود تدوین شده‌اند و بر اساس منطق حاکم بر مدلسازی معادله ساختاری، کلیت و جزییات مدل مورد تأیید قرار گرفته است. برای تبیین بهتر، نتایج مدل در ادامه تحلیل شده است.



شکل ۲- مدل معادله ساختاری برای تبیین امنیت سایبری اطفال (Cybersecurity)

در ساختار این مدل، تعدادی متغیر مشاهده‌شده وجود دارند که هر کدام دارای شاخص‌های تعریفی مختلفی بوده‌اند. این متغیرهای آشکار یا مشاهده‌شده در مدل ده مورد است؛ برای مثال، در شاخص‌سازی متغیر اصلی خنثی‌سازی خطرات فضای مجازی برای اطفال (Risk)، چهار مؤلفه اصلی: خنثی‌سازی از طریق آگاهی‌دادن، خنثی‌سازی از طریق آموزش و توانمندسازی، خنثی‌سازی از طریق تقویت ظرفیت‌های جامعه و خنثی‌سازی از طریق ظرفیت قانون وجود

دارند که هر کدام با چندین گویه تعریف شده‌اند. از میان این چهار شاخص، «خنثی‌سازی از طریق تقویت ظرفیت‌های جامعه» با ضریب (۰/۵۹) بیشترین توان تبیین خنثی‌سازی خطرات فضای مجازی را دارد. بقیه ضرایب نیز با توجه به بالابودن و مثبت‌بودن قابل‌قبول هستند و توان تبیین بالایی برای خنثی‌سازی خطرات فضای مجازی دارند. در مورد سایر متغیرهای اصلی و میانجی نیز اوضاع به همین ترتیب است و هر دو متغیر آسیب‌شناسی فضای مجازی و امنیت سایبری دارای شاخص‌ها یا معرف‌های مناسبی به لحاظ آماری هستند. در تبیین روابط ساختاری نیز خنثی‌سازی خطرات فضای مجازی با تأثیر معکوسی بر آسیب‌شناسی فضای مجازی و امنیت سایبری نشان داده که هرچقدر خنثی‌سازی خطرات فضای مجازی بیشتر باشد، به تبع آن، آسیب‌شناسی فضای مجازی نیز کمتر می‌شود. این ضریب (۰/۷۲-) شده است و به منزله مقدار بتای منفی برای تبیین اثرگذاری خنثی‌سازی خطرات فضای مجازی بر آسیب‌شناسی فضای مجازی بوده است. با توجه به ضریب (۰/۵۷-) برای تبیین اثرگذاری آسیب‌شناسی فضای مجازی بر امنیت سایبری باید گفت هرچقدر حجم آسیب‌های فضای مجازی بیشتر باشد، به تبع آن، امنیت سایبری کاهش خواهد یافت. در نهایت، اثرگذاری خنثی‌سازی خطرات فضای مجازی بر امنیت سایبری اطفال با توجه به ضریب (۰/۷۷)، مثبت و معنادار است و هرچقدر خنثی‌سازی خطرات فضای مجازی بیشتر باشد، میزان امنیت سایبری اطفال نیز بیشتر خواهد شد.

جدول ۱- برآورد وزن‌های رگرسیونی متغیرهای موجود در مدل

			Estimate	S.E.	C.R.	P	Label
Damage	<---	Risk	1.073	.300	3.582	***	
Cybersecurity	<---	Damage	-.700				
Cybersecurity	<---	Risk	3.163	.825	3.836	***	
rsk1	<---	Risk	1.293	.371	3.479	***	
rsk2	<---	Risk	1.019	.388	2.630	***	
rsk3	<---	Risk	1.594	.399	3.997	***	
rsk4	<---	Risk	1.000				
dmg1	<---	Damage	1.000				
dmg2	<---	Damage	1.672	.255	6.552	***	
dmg3	<---	Damage	1.175	.184	6.394	***	
cyb1	<---	Cybersecurity	1.000				
cyb2	<---	Cybersecurity	1.401	.227	6.178	***	
cyb3	<---	Cybersecurity	1.226	.181	6.768	***	

در اطلاعات و خروجی‌های به‌دست‌آمده از جدول فوق، مقادیر برآورده‌شده و مقایسه آنها برای اعتباربخشی آزمون‌ها به مقدار خطای برآورده‌شده بستگی دارد. بر اساس قواعد آماری مورد پذیرش در ساختار آزمون‌های آماری، پذیرش خطای معیار تا ۵ درصد مورد قبول است و با توجه به مقادیر (P Value) در جدول فوق، در همه موارد، خطای محاسبه‌شده بررسی روابط تبیین متغیرهای کمتر از صفر است و در این شرایط، همه روابط موجود در مدل با اطمینان بالایی مورد تأیید قرار گرفته است.

بحث و نتیجه‌گیری

در ایران نیز مانند بسیاری از کشورهای جهان، اسنادی برای حفاظت از اطفال و نوجوانان در فضای مجازی تدوین شده است. این سند که با عنوان «مصوبه شورای عالی فضای مجازی در خصوص صیانت از کودکان و نوجوانان در فضای مجازی» شناخته می‌شود، در سال ۱۳۹۹ در اجرای ماده ۱۱ آیین‌نامه داخلی شورای عالی فضای مجازی، به پیوست سند «صیانت از کودکان و نوجوانان در فضای مجازی» مصوب جلسات شماره شصت و نه مورخ ۲۸/۱۱/۱۳۹۹، شماره هفتاد مورخ ۲۶/۱۲/۱۳۹۹ و شماره هفتاد و یک مورخ ۱۷/۳/۱۴۰۰ شورای عالی فضای مجازی که طی نامه شماره ۱۰۲۱۲۰ مورخ ٦/٤/١٤٠٠ به استحضار مقام معظم رهبری (مدظله العالی) رسیده است، برای اجرا ابلاغ شده است. این سند مهم قانونی در اولین اصل خود صیانت و حفاظت از اطفال و نوجوانان را در فضای مجازی ملاک قرار داده و برای نیل به این هدف مهم و دستیابی به سایر اهداف مرتبط با سند، بر موضوع‌های مهمی مانند آموزش، تربیت فنی و حقوقی تمرکز کرده و در مسائل آموزشی به آموزش کودکان اکتفا نکرده و آموزش والدین را نیز در دستور کار قرار داده است. علاوه بر این، در یک اقدام مهم، از مساله تولید محتوا در اینترنت غافل نبوده و برنامه‌های نظارتی مهمی برای مدیریت محتوا در فضای مجازی مورد توجه قرار داده و اقدامات مورد نیاز را برای آن پیش‌بینی کرده است. در اقدامات تکمیلی‌تری، راهبردهای مشاوره‌ای برای شرایط خاص مورد توجه قرار گرفته و با خدماتی مشاوره‌ای، پشتیبانی از سیاست‌ها و اقدامات پیش‌بینی و مورد توجه قرار گرفته است. بر اساس این سند، فراهم‌سازی فضای مجازی ویژه خردسالان، کودکان و نوجوانان در چارچوب فرهنگ اسلامی- ایرانی برای استفاده مناسب از فضای مجازی و پیشگیری از آسیب‌های احتمالی آن به پنج اقدام اساسی نیاز دارد. این اقدامات شامل مدیریت و راهبری، ایجاد محیط صیانت‌شده، توسعه محتوا و خدمات رده‌بندی‌شده، حمایت و مراقبت و نهایتاً، فرهنگ‌سازی و ارتقای سواد فضای مجازی است. باید اذعان داشت که در ایران اغلب

خنثی‌سازی مخاطرات از مجاری آموزشی تحقق می‌یابد. یکی دیگر از اسناد مدونی که در حوزهٔ ایجاد محیط آموزشی مناسب در فضای مجازی برای کودکان است، سند برنامهٔ اقدام توسعهٔ خدمات فضای مجازی کودک است که توسط پژوهشگاه ارتباطات و فناوری اطلاعات (مرکز تحقیقات مخابرات ایران) تهیه شده است. این سند دارای قسمت های مختلف در خصوص متولیان ایجاد فضای آموزشی مناسب برای اطفال در فضای مجازی است. در قسمتی از این سند، از مخاطبان خدمات فضای مجازی کودک، چهار دستهٔ کودک، والدین، معلمان و اشخاص حقیقی و حقوقی دولتی و غیردولتی مرتبط نام برده شده، ولی تأکید شده که مخاطب اصلی سند، کودک است. در این سند آمده است که در دوره کودکی، لازم است اطلاعاتی در خصوص کودک به پدر و مادر ارائه شود و ایشان بر رفتار کودک خود در خدمات فضای مجازی کودک، مدیریت و نظارت کنند. مخاطب دیگر طرح، معلم است که بخش مهمی از آموزش و تربیت کودک، مدیریت و نظارت رفتار درسی کودک برعهدهٔ ایشان است. در نهایت، دیگر مخاطبان، اشخاص حقیقی و حقوقی دولتی و غیردولتی هستند که از یک سو، بر رفتار کودک تأثیر می‌گذارند و از سوی دیگر، کنترل رفتار کودک در این فضا را برعهده دارند. بنا بر نظر پژوهشگران حوزهٔ فضای مجازی کودک، بهره‌بردای و استفاده نادرست از این فضا در دو بُعد مهم برای اطفال و نوجوانان جلوه‌گری می‌کند. در یک شکل آن، استفاده بی‌حدواندازه و خارج از کنترل منجر به شکلی از اعتیاد به اینترنت و فضای مجازی می‌شود و در شکل دوم، این خارج‌شدن از قاعده دلیل گسست اطفال و نوجوانان از بسیاری برنامه‌های مطلوب تربیتی و فراغتی می‌شود، به گونه‌ای که برخی رفتارهای مطلوب فراغتی مانند ورزش و فعالیت‌های جسمانی مفید به کلی از زندگی فرد حذف می‌شوند. علاوه بر این، انجام تکالیف تحصیلی و ارتباطات مؤثر و تغییر عادات منظم خوردن و خوابیدن دچار مشکل می‌شود.

به طور کلی، در اقدامی راهبری ایجاد محیطی صیانت‌شده برای اطفال و نوجوانان در فضای مجازی باید به ایجاد زیرساخت و خدماتی کنترل‌شده و نظارت‌شده از لحاظ هویت‌های حضوریافته در این فضا، نوع دسترسی به اطلاعات، شیوه‌های نظارتی و روش‌های پرداخت آنلاین منجر شود. در حوزه توسعه محتوا و خدمات رده‌بندی‌شده نیز تأمین پایداری کسب‌وکار محتوا و خدمات مورد نیاز در محیط صیانت‌شده و تدوین ضوابط و نصاب‌های اعتبارسنجی، ممیزی و نشان‌دارکردن محتوا و خدمات مورد اطمینان، پشتیبانی از همه ابعاد سخت و نرم‌اپ‌های بومی و تولید داخل و مجبورکردن همه سکوهای تولید محتوا اطفال در فضای مجازی با درنظرگرفتن اصل صیانت از کودکان لازم و ضروری است. در حمایت و مراقبت نیز

توسعه نظام خدمات مشاوره و مددکاری به خانواده‌ها و راه‌اندازی خط تماس مشاوره آنلاین، راه‌اندازی خط تماس اضطراری، حمایت قانونی از اطفال و نوجوانان و صیانت از داده‌ها، رده‌بندی و تفکیک محتوا لازم است. در نهایت، در زمینه فرهنگ‌سازی و ارتقای سواد فضای مجازی باید اطلاع‌رسانی، آموزش سواد فضای مجازی و ترویج محتوا و خدمات موجود در محیط مجازی صیانت‌شده و نحوه استفاده از امکانات تعبیه‌شده در این محیط توسط سازمان صداوسیما و وزارت آموزش‌وپرورش با همکاری وزارت ارتباطات و فناوری اطلاعات انجام شود.

منابع

- بادامی، محمدعلی؛ مقدادی، محمد مهدی؛ پیله‌ور، مرضیه. (۱٤۰۱). جایگاه حمایت‌های حقوقی از کودکان در فضای مجازی با تأکید بر حق تربیت دینی. *پژوهش‌های حقوقی*، ۲۱(۵۰)، ۵۷-٤۹٤.
doi: 10.48300/jlr.2021.279730.1619
- رضازاده، فرید؛ آقاصرام، مهدی؛ میزانیان، کیارش؛ مصطفوی، سیداکبر. (۱۳۹۸). چالش‌ها و بایسته‌های پیشگیری از بزه سایبری در مدارس، *نوآوری‌های فناوری اطلاعات و ارتباطات کاربردی*، ۱ (۲)، ۲۷-۳۹.
- شورای عالی فضای مجازی. (۱٤۰۰). مصوبه شورای عالی فضای مجازی در خصوص صیانت از کودکان و نوجوانان در فضای مجازی، مرکز پژوهش‌های مجلس شورای اسلامی.
https://rc.majlis.ir/fa/law/show/1681090
- کرامتی معز، هادی. (۱۳۹۹). *بزه‌دیده‌شناسی کودکان در شبکه‌های اجتماعی*. چاپ اول. دادگستر.
- کیانی، نیکفر؛ حیدری، مسعود؛ شادمان‌فر، محمدرضا. (۱٤۰۳). پیشگیری از بزه‌دیدگی اطفال در جرائم جنسی در فضای سایبر. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ٦(۳)، ٤۵-۵۹.
https://csjlp.org/index.php/csjlp/article/view/187
- محسنی، فرید. (۱۳۹۰). سهم کودکان و نوجوانان از حمایت کیفری در فضای مجازی و حقیقی، *آموزه‌های حقوق کیفری*، ۸(۱): ۱۷۰-۱۳۷.
https://cld.razavi.ac.ir/article_847.html
- ملکوتی، نصیر؛ محسنی، فرید. (۱٤۰۲). پیشگیری جامعه‌مدار از بزهکاری اطفال و نوجوانان در محیط های آموزشی مجازی (با تأکید بر یافته های جرم‌شناسی). *دیدگاه‌های حقوق قضائی*، ۲۸(۱۰۲)، ۲۰۷-۲۳٤.
doi: 10.22034/jlvi.2024.1998625.0
- منصورآبادی، عباس؛ میرخلیلی، سیدمحمود؛ کرامتی‌معز، هادی. (۱٤۰۰). پیشگیری از بزه‌دیدگی کودکان در شبکه‌های اجتماعی مجازی با تاکید بر نقش نظارتی شورای عالی فضای مجازی و پلیس فتا. *مطالعات بین‌المللی پلیس*، ۱۲(٤٦)، ۳۰-۵۲.
http://interpol.jrl.police.ir/article_95912.html
- نادری، نیلوفر؛ تدین، عباس و عبدالهی، سامان. (۱٤۰۲). عوامل مؤثر بر پیشگیری از بزه‌دیدگی اطفال و نوجوانان در فضای مجازی- مورد مطالعه استان تهران. *انتظام اجتماعی*، ۱۵(۱)، ۵۷-۲٤.
http://sopra.jrl.police.ir/article_100618.html
- نجفی‌ابرندآبادی، علی حسین. (۱٤۰۲). *تقریرات جرم‌شناسی (کلیات جرم‌شناسی)*. به کوشش محمد کاظم تقدیر. ویرایش: سید پوریا حسینی تحت نظارت شهرام ابراهیمی. دانشکده حقوق دانشگاه شهید بهشتی.

- Andrews, D., Alathur, S., & Chetty, N. (2020). International efforts for children online safety: A survey. *International Journal of Web Based Communities*, 16(2), 123-133.

-Chadwick, D. (2016). Defining a formal model of edutainment that enhances the learning of cyber security subjects by higher education students. *PhD thesis*, University of Greenwich.
-Desimpelaere, L., Hudders, L., & Van de Sompel, D. (2020). Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behavior. *Computers in human behavior*, 110, 106382.
-Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A. (2021). Youth internet safety education: Aligning programs with the evidence base. *Trauma, violence, & abuse*, 22(5), 1233-1247.
-Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. *Information Security Journal: A Global Perspective*, 28(3), 81-106.
-Gjertsen, E.; Gjære, E.; Bartnes, M. & Flores, W. (2017). Gamification of Information Security Awareness and Training. *In Proceedings of the 3rd International Conference on Information Systems Security and Privacy- ICISSP*; SciTePress, pages 59-70.
DOI: 10.5220/0006128500590070
-Gupta, S., Kumari, S., & Sugandh, U. (2023). Protecting Children's Data from Cybersecurity Attacks to Prevent Child Sexual Abuse: A Techno-Legal Approach. *In 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI)* (pp. 1-7). IEEE**.**
-Internet Watch Foundation. (2021). Children's Online Safety and Health, *UK Safer Internet Centre*, 1-193.
https://annualreport2022.iwf.org.uk/?gad_source
-Lagíňová, D., & Fornálová, T. (2018). *Net children go Mobile. Media Literacy and Academic Research*, 1(1), 77-79.
-Naarttijärvi, M. (2018). Balancing data protection and privacy–The case of information security sensor systems. *Computer law & security review*, 34(5), 1019-1038.
-Prior, S., & Renaud, K. (2024). Are UK parents empowered to act on their cybersecurity education responsibilities?. In International Conference on Human-Computer Interaction (pp. 77-96). *Cham: Springer Nature Switzerland*.
-Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343.
-Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. *International Journal of Child-Computer Interaction*, 30, 100343.
-Roy, S., Roy, U., & Sinha, D. D. (2017). ACO-random forest approach to protect the kids from internet threats through keystroke. *Int. J. Eng. Technol*, 9(35), 279-285.
-Spada, M. M. (2014). *An overview of problematic internet use, Addictive behaviors*, No. 39 (1). 208-224.