Iran's penal policy towards providing security for children in cyberspace

Seyed Abbas Khalilpour Chalkiasari [1]

Abstract

The astonishing advancement of information technology in the early years of the twenty-first century has brought about countless changes in the various fields and opened another door to the new world so that all human economic, social, political, cultural and scientific activities are fundamentally changed. Law is also a branch of the humanities that regulates human relations in the context of collective life. It has developed laws to prevent children from unsecured entering the virtual world and legal measures to protect them. Adopting a distinct approach to the substantive criminal law of cybercrime can minimize harm to children and adolescents by prevention. In the meantime, questions and doubts have been raised about the limits of freedom of use of the Internet for children, the limits of free flow of information against child users, protection of child privacy in cyberspace and finally the role of legal regulations to protect this vulnerable group that easily can be exploited in this boundless world. In this research, through data collection tools and using library and internet resources with rational analysis of the content to study the legislative policy of criminal law on criminal security for children in cyberspace, in comparison with the iranian legal system and international documents, in order to better confront and prevent these crimes, the issues and problems and the strengths and weaknesses of the enacted laws are presented and suggestions and solutions for solving these problems are discussed.

Keywords

Cyberspace, Children, Security, Criminal Law, Legislative Policy

---

1. PhD in Criminal Law and Criminology, Islamic Azad University of Lahijan, Department of Criminal Law and Criminology, Lahijan, Iran.
Email: syedabbaskhalilpour@gmail.com

Original Article Received: 17 Aug 2019 Accepted: 15 Dec 2019

Please cite this article as: Khalilpour Chalkiasari A. Iran's penal policy towards providing security for children in cyberspace. Child Rights J 2020; 2(5): 161-187.

سیاست تقنینی کیفری ایران در قبال تأمین امنیت کودکان در فضای مجازی

سیدعباس خلیل پورچالکیاسری [۱]

چکیده

پیشرفت خیره‌کننده فناوری اطلاعات در سال‌های آغازین سده بیست ویکم، دگرگونی‌های بیشماری را در زمینه‌های مختلف بوجود آورده و دروازه دیگری را به جهان نوین گشوده است؛ به گونه‌ای که تمام فعالیت‌های اقتصادی، اجتماعی، سیاسی، فرهنگی و علمی بشر را به طور بنیادین دستخوش تغییر و تحول قرار داده است. علم حقوق نیز به عنوان شاخه ای از علوم انسانی که تنظیم روابط انسان‌ها را در چارچوب حیات جمعی به عهده داشته، با امعان نظر به دنیای مجازی و دسترسی آسان و ساده کودکان به اینترنت و وجود خطرات اجتناب‌ناپذیر در این پهنه گسترده، پرسش‌هایی را در خصوص اقدامات حقوقی در این عرصه پیش رو نهاده و برای جلوگیری از ورود غیرایمن کودکان در دنیای مجازی و اقدامات قانونی لازم برای حفاظت از آن‌ها، ابزارهایی را مطرح داشته است. اتخاذ رویکرد متمایز در حقوق کیفری ماهوی جرایم رایانه‌ای می‌تواند با اِعمال پیشگیری، آسیب‌ها نسبت به کودکان و نوجوانان را به حداقل ممکن کاهش دهد. در این میان، پرسش ها و تردیدهایی در زمینه حدود آزادی استفاده از اینترنت برای کودکان، حدود گردش آزاد اطلاعات در مقابل کاربران کودک، حفاظت از حریم خصوصی کودک در فضای مجازی و نهایتاً نقش مقررات حقوقی برای حفاظت و حمایت از این گروه آسیب پذیر که به سهولت می توانند در این دنیای بی حد و مرز در معرض سوء استفاده قرارگیرند، مطرح می‌شود. در این پژوهش، با استفاده از منابع کتابخانه ای و اینترنتی و تحلیل عقلی مطالب، به بررسی سیاست تقنینی نظام حقوق کیفری در حیطه تامین امنیت کودکان در

---

۱. دوره دکتری حقوق جزا وجرم شناسی، دانشگاه آزاد اسلامی لاهیجان، گروه حقوق جزا و جرم‌شناسی، لاهیجان، ایران. Email: syedabbaskhalilpour@gmail.com

نوع مقاله: مروری **تاریخ دریافت مقاله:** ۱۳۹۸/۵/۲۶ **تاریخ پذیرش مقاله:** ۱۳۹۸/۹/۲۴

فضای مجازی ضمن مطالعه مقایسه‌ای نظام حقوقی ایران و اسناد بین المللی، با هدف ارزیابی چگونگی مقابله و پیشگیری نسبت به جرایم ارتکابی در این زمینه و بیان مسائل و مشکلات و نقاط قوت و ضعف قوانین مصوب و همچنین ارائه پیشنهادات و راهکارهایی جهت حل مشکلات کنونی پرداخته شد.

واژگان کلیدی

فضای مجازی، کودکان، امنیت، حقوق کیفری، سیاست تقنینی

مقدمه

توسعه پدیده جهانی فناوری اطلاعات و ارتباطات، دگرگونی شگرفی در ابعاد مختلف حیات اقتصادی، اجتماعی، فرهنگی، امنیتی و سیاسی ایجاد نموده است؛ انقلاب الکترونیک، تبدیل به مهمترین پدیده تعیین‌کننده معاصر شده است. فناوری اطلاعات و ارتباطات نه تنها صنعت، اقتصاد، تجارت و دیگر عرصه ها را تحت تأثیر قرار داده، بلکه حقوق هم از این تحولات بی‌بهره نبوده است. به فراخور این تغییرات بنیادین، طبعاً حقوقدانان نیز همانند متخصصین دیگر رشته‌ها باید برای هماهنگی با این فناوری و عقب نماندن از آن، به ارائه ضوابط، اصول و قواعد حقوقی جهت پیشگیری یا حل و فصل اختلافات ناشی از این تغییرات، اقدام نمایند. فضای اینترنت، چالش‌هایی در ساحت روابط اجتماعی به عنوان خاستگاه قواعد حقوقی، ایجاد نموده است. کودکان و نوجوانان هنگامی که به عرصه جهان اینترنت، وارد می‌شود و به گشت وگذار در فضای مجازی می‌پردازند؛ و به انبوهی از داده‌های متنی و تصویری از طریق اینترنت دسترسی پیدا می‌کنند و به تعاملات برخط روی می‌آورند؛ پیوند های اجتماعی معقول و نامعقولی برقرار می کنند، و از منظری، در معرض خطر عناصری از اجتماع قرار می گیرند که در جهان واقعی از آنان پرهیز می‌شود.

به دلیل وجود محرک‌های پر جاذبه و مسحورکننده در اینترنت، کودکان و نوجوانان به عنوان سریع‌ترین کاربران در حال رشد، بیشتر در معرض آسیب جنبه‌های منفی آن قرار می‌گیرند. آنان اغلب اوقات از طریق آی پاد، سایت‌های ویدیویی، سایت‌های شبکه-های اجتماعی، اتاق‌های چت، سایت‌هایی با چند بازیکن در بازی‌های تعاملی و بعلاوه دوربین های وب کم و گوشی‌های هوشمند، عملاً در دسترس رسانه‌ها قرار می‌گیرند. کودکان با ورود به اینترنت با دنیای جدید مواجه می‌شوند که در آنجا می‌توانند هم مجهولات زیادی کشف کنند و هم مطالب زیادی بیاموزند. وجود اطلاعات متعدد در اینترنت مزایای پرشماری برای نوجوانان فراهم می‌کند، اما تهدیدات جدی را نیز با خود با ارمغان می‌آورد؛ مانند: قرار گرفتن در معرض آزار و اذیت جنسی، دسترسی به مواد مضر و غیرقانونی مخدر، الکل، سیگار، قمار و بسیاری از مواد پرخطر دیگر.

آسیب‌ها و خطرات بالقوه موجود برای کودکان در سراسر جهان را می‌توان در سه دسته کلی هدف‌گیری تجاری و تبلیغاتی، بهره‌برداری و استثمار جنسی کودکان و نقض حریم خصوصی آن‌ها تقسیم کرد. کودکان در اینترنت بخش قابل توجهی از اطلاعات شخصی خود را در محیط‌هایی چون اتاق‌های گفت و گوی شبکه‌های اجتماعی، سایت-های بازی آنلاین و نظایر آن افشا می‌کنند که جمع آوری داده‌های غیرقانونی آن‌ها تهدیدی جدی برای حریم خصوصی آنان به شمار می‌آید چرا که هرگز مشخص نیست که این اطلاعات بدست چه کسانی می‌افتد و چگونه مورد استفاده قرار می‌گیرند. چنین وضعیتی می‌تواند کودکان را در معرض استفاده‌های تجاری از اطلاعات آن‌ها با هدف-گیری تبلیغاتی قرار دهد. در دهه اخیر پدیده سوء استفاده جنسی و هرزه‌نگاری کودکان که عمدتاً از طریق فریب و جمع‌آوری اطلاعات کودک در فضای وب صورت می‌گیرد، نگرانی جدی در جامعه ایجاد کرده است. حال باید دید که حقوق کیفری برای جلوگیری از طعمه قرارگرفتن کودکان چه راهکارهای را پیش‌بینی کرده است.

به دلایل روشنی نمی‌توان از کودکان و نوجوانان خواست تا وارد محیط اینترنت نشوند. منع کامل استفاده از اینترنت و رایانه، برای آنان نه مفید است و نه امکان پذیر! اگر از کودکان پاسداری نکنیم زندگی‌شان در جهان پر از تباهیِ بزهکارانِ فضای اینترنت به شدت به خطر می‌افتد. فضای اینترنت فضایی پر از چالش است. به نظر پژوهشگر، یکی از وجوه تمایز واکنش به جرایم رایانه‌ای، در قالب کیفیت تعریف جرایم، تعریف و توسعه مسئولیت کیفری و تعیین مجازات در قوانین کیفری ظاهر می‌شود؛ به گونه ای که بتواند قابلیت اجرایی، ارعابی و بازدارندگی بیشتری به واکنش‌های کیفری ببخشد.

فضای مجازی

فضای مجازی اشاره دارد به مجموعهٔ ارتباطات درونی میان انسان‌ها از طریق رایانه و وسایل مخابراتی بدون ملاحظه جغرافیای فیزیکی. به بیان دیگر، فضای مجازی، فضایی است که در آن فعالیت‌های مختلف در ابعاد داده ورزی و اطلاع رسانی، ارتباطات

و ارائه خدمات، مدیریت و کنترل از طریق ساز و کارهای الکترونیکی و مجازی صورت می پذیرد. مهمترین مختصات و ویژگی‌های فضای مجازی عبارت‌اند از: ۱- هزینه پایین ورود، ۲-گمنامی (۱)؛ ۳- نامتقارن بودن در آسیب پذیری (۲)؛ ۴- جهانی و فرامرزی بودن؛ ۵- دسترسی دائم و آسان به آخرین اطلاعات؛ ۶- جذابیت و تنوع؛ ۷- عدم وابستگی به زمان و مکان خاص؛ ۸- چند رسانه‌ای بودن (۳)؛ ۹- سهولت تعامل و تبادل اطلاعات با دیگران؛ و ۱۰- سرعت بالای تبادل اطلاعات و امکانات قابل توجه اینترنت برای افراد جامعه (۱).

سابقه جرایم رایانه‌ای

مطابق گزارش‌ها، نخستین جرم رایانه‌ای در ایران به تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست و پس از این تاریخ بود که گروه های هکر، جرم های دیگری را نیز مرتکب شدند. بر اساس آمارهای موجود در سال ۱۳۸۴، ۵۳ مورد پرونده مربوط به جرم اینترنتی و رایانه ای در کشور تشکیل شده است. از مهمترین موارد جرایم رایانه ای در طی یک سال، برای مثال، ۳۲ مورد سوء استفاده از کارت های اعتباری، ۱۱ مورد کلاهبرداری اینترنتی ، ۷ مورد ایجاد مزاحمت از طریق اینترنت، ۳ مورد کپی رایت و ۲ مورد نشر اکاذیب و ۵ مورد نیز موضوعات متفرقه، بیان شده است. رفته رفته با افزایش نفوذ رایانه و گسترش مقیاس فضای مجازی و تکاثر کاربران، آمار جرایم رایانه‌ای نیز رو به تزاید نهاده است.

تعریف جرایم رایانه‌ای

جرایم رایانه‌ای را می‌توان اینگونه تعریف نمود: «هر جرمی که قانونگذار به صراحت رایانه را به منزله موضوع یا وسیله جرم، جزء رکن مادی آن اعلام کرده باشد، یا عملاً رایانه به منزله موضوع یا وسیله ارتکاب یا وسیله ذخیره یا پردازش یا انتقال دلایل جرم، در آن نقش داشته باشد» (۴).

ویژگی جرایم رایانه‌ای

۱- سرعت

در زمان حاضر، مفهوم متعارف زمان و مکان در دنیای مجازی دچار تحول شده است. یکی از فاکتورهای کندی وقوع پدیده بزهکارانه در جهان واقعی بعد مکانی میان سه ضلع بزهکاری، یعنی بزهکار، آماج بزه و مکان ارتکاب بزه است. ساختار فضای مجازی به گونه ای است که در آن قرابت مکان میان سه عنصر فوق ضرورتی ندارد. این وضعیت موجب صرفه جویی شگرفی از بعد زمان و هزینه برای بزهکاران گردیده و آنها را قادر ساخته است تا بدون وجود مانعی به نام مکان، جرایم متعددی را در سریع‌ترین زمان مرتکب شوند.

۲- ناشناختگی

عنصر ناشناختگی از اصول حاکم بر جرایم مجازی است (۵). از یک سو اساساً شناسایی کاربران ماشین متصل به شبکه امری پیچیده و پرهزینه است و از سویی دیگر استفاده از شیوه های سرقت مشخصات دیگر ماشین ها، استتار آنلاین و سایر مخفی-کاری‌های موجود، امر شناسایی مرتکبین را به صورت معمول سخت و بعضاً ناممکن می‌نماید. این جرایم عمدتاً قبل از اطلاع نهادهای قانونی و حتی خود قربانی، رخ داده و آثار جرایم و نرم افزارهای مورد استفاده، پس از ارتکاب جرم توسط بزهکار، سریعاً نابود می‌شوند و یا به صورت اتوماتیک از بین می‌روند.

۳- مقیاس وسیع و ارزان‌بودن جرایم

مقیاس بزه‌های ارتکابی در فضای سایبر بسیار وسیع است و به علت امکانات موجود و نبود محدودیت ها، بزهکار از الگوی سریالی و شبکه ای استفاده می‌کند. لذا قربانی-کردن هزاران نفر طی اقدامی واحد، فرضی واقعی در فضای رایانه ای است. این امر باعث می شود که حجم و آمار بزه در دنیای مجازی با دنیای واقعی قابل قیاس نباشد. آمار جنایی با توجه به زمینه های مذکور قابلیت رشد تصاعدی دارند. مهم‌ترین وسیله ارتکاب بزه در فضای سایبر وجود یک دستگاه رایانه و خط تلفن برای اتصال به اینترنت

است. ارزان بودن جرم، محدودیت منابع مالی و انسانی را برای سیستم عدالت کیفری تشدید می کند (۶).

۴- روش قانون گذاری بین المللی

روش قانونگذاری بین المللی با توجه به یکپارچگی اینترنت و مشکلات ناشی از قانونگذاری ملی مطرح شد (۷). این شیوه در بهترین شکل با انعقاد معاهدات بین‌المللی محقق می‌گردد. به طور مثال، ماده ۳ پروتکل الحاقی به کنوانسیون حقوق کودک، مورخ ۲۰۰۰ در خصوص فروش، فحشا و هرزه نگاری کودکان به صراحت بر نقش اینترنت در توزیع هرزه نگاری کودکان اشاره دارد و از کشورها می‌خواهد که اینگونه افعال را جرم انگاری کنند. همچنین یکی از مهمترین کنوانسیون های مربوط به فضای سایبر، کنوانسیون بوداپست در خصوص جرایم سایبری است. با این حال، این کنوانسیون نمی‌تواند به عنوان معاهده‌ای جامع تلقی شود، چه آنکه اولاً، تمام جرایم سایبری را دربرنمی‌گیرد و ثانیاً، این کنوانسیون صرفاً برای کشورهای اروپایی لازم الاجراست. در هر صورت، معاهدات منطقه ای و دوجانبه، پاسخگوی حل مشکلات نبوده و معاهده اینترنتی در سطح بین المللی مورد نیاز است (۷).

برخی از قواعد آمره، نظیر ممنوعیت دزدی دریایی، برده‌داری و نسل‌زدایی در فضای سایبر نیز قابل اعمال است (۸). سازمان های بین المللی نیز در فرایند بین‌المللی‌سازی قانونگذاری در فضای سایبر، نقش قابل توجهی داشته اند. پیش از همه، آنسیترال با تصویب قانون نمونه آنسیترال در خصوص تجارت الکترونیکی در سال ۱۹۹۶ (۹) نقش چشمگیری در هماهنگ‌سازی قوانین ملی کشورها درباره مسائل مربوط به تجارت الکترونیک داشته است. گروه هشت نیز در اولین اقدام خود در سال ۱۹۹۷ کمیته فرعی جرایم رایانه ای را برای مقابله با جرایم سایبری تأسیس، و متعاقباً یک برنامه اقدام ده اصلی را در این رابطه تصویب کرد (۱۰). مجمع عمومی سازمان ملل متحد در سالهای ۲۰۰۰ و ۲۰۰۳ تلاش هایی برای تنظیم امنیت اطلاعاتی و سایبری انجام داد. پس از تلاش اتحادیه اروپا برای تصویب کنوانسیون جرایم سایبری، اتحادیه عرب به پیشنهاد ایالات متحده عربی یک مدل قانونی در خصوص همسان‌سازی قوانین ملی کشورهای

عربی را در سال ۲۰۰۳ پذیرفت. شورای همکاری خلیج فارس نیز در کنفرانس ۲۰۰۷ به دولت ها توصیه کرد که رویکردی متحدانه را در خصوص مواجهه با موضوعات سایبری اتخاذ کنند. سازمان کشورهای امریکایی، سازمان همکاری و توسعه اقتصادی، سازمان همکاری و اقتصادی آسیا اقیانوسیه و سازمان کشورهای مشترک المنافع نیز در یکسان‌سازی قواعد بین المللی تلاش هایی داشته اند. اما شاید مهمترین تلاش، اجلاس جهانی جامعه اطلاعات در سال ۲۰۰۳ باشد که در آن تشکیل سازمان بین المللی اینترنت و انعقاد معاهده‌ای اینترنتی پیشنهاد شد. اتحادیه بین المللی مخابرات در می ۲۰۰۷ آژانس جهانی جرائم سایبری و متعاقباً گروه کارشناسان ارشد را با هدف ارائه پیشنهادهایی برای جرم انگاری سایبری بنیانگذاری کرد (۱۱). بالاخره سند اصلاحی مقررات اتحادیه بین المللی مخابرات با اعطای وجهه حقوقی بین المللی به قانونگذاری در فضای اینترنت با رأی اکثریت کشورها به تصویب رسید.

باید توجه داشت که فناوری محوری فضای سایبر موجب می‌شود که سهم کشورهای مختلف در تنظیم نظام حقوقی حاکم بر فضای سایبر متفاوت باشد. به همین دلیل، یکی از مدل های پیشنهادی در قانونگذاری بین المللی در فضای سایبر، تقسیم وظایف و امتیازات بر مبنای مؤلفه هایی مانند قدرت، ثروت و تخصص است. این روش که از آن تحت عنوان (هندسه متغیر) یاد می‌شود، در ساختار شورای امنیت، صندوق بین المللی پول و سازمان تجارت جهانی اعمال شده است. این راهکار در ماده ۴۹ اعلامیه اجلاس جهانی جامعه اطلاعاتی نیز مندرج است که مسیر مشارکت همه ذی نفع ها (اعم از عمومی و خصوصی) را در مدیریت فضای سایبر هموار می سازد. در این روش به عنوان مثال می‌توان برای دولت ها و سازمان های فنی، حق رأی بیشتر و برای نمایندگان جامعه مدنی، حق رأی کمتری اختصاص داد. مشکل محتمل در استفاده از روش هندسهٔ متغیر این است که ایجاد چنین نظامی نیازمند مذاکراتی طولانی و جزیی برای جلب منافع همه گروه ها است.

۵- روش خودانتظامی

از نظر برخی حقوقدانان، به جهت ماهیت یکپارچه و فرامرزی فضای سایبر، قواعد سنتی صلاحیت، مناسب بافت اینترنت نیست و باید برای اینترنت، حاکمیتی جداگانه به رسمیت شناخت (۱۲). نتیجه این نگرش، شیوه خودانتظامی در قانونگذاری در فضای سایبر خواهد بود. در روش خودانتظامی به جای دولت ها، شرکت‌های سایبری یا مالکان تارنما ملزم به ایجاد محدودیت در فضای سایبر هستند. مهمترین دلیل خودانتظامی فضای سایبر این است که فضای سایبر برخلاف دولت‌ها غیرمتمرکز و جهانی است(۱۳). همچنین این روش، علاوه بر اینکه کارایی قانونگذاری ملی را داراست، به مراتب، ساده‌تر و ارزان‌تر بوده (۱۴) و به دلیل نقش پیشگیرانه این روش از آمار جرایم در فضای سایبر نیز کاسته خواهد شد. روش خودانتظامی در عمل با مشکلاتی روبه روست. اولاً، به دلیل حذف نهاد دولت به عنوان رکنی فرادستی، موجب هرج و مرج در فضای سایبر خواهد شد(۱۵). ثانیاً، از نظر حامیان (مشترکات ابتکاری)، الزام تأمین‌کنندگان خدمات اینترنتی به خودسانسوری، خلاقیت در محیط دیجیتال را تحت الشعاع قرار می‌دهد. همچنین لازمه اقدام نهادهای فنی و صاحبان تارنماها، داشتن پشتوانه قانونی توسط دولت هاست، درحالیکه دولت ها در حال حاضر از این نظر حمایت نمی‌کنند(۸).

۶- روش مختلط

این اعتقاد وجود دارد که نباید مدیریت اینترنت را به قانونگذاری ملی یا قانونگذاری بین‌المللی یا شیوه خودانتظامی واگذار کرد. هر یک از سه شیوه قانونگذاری در خصوص مشروعیت یا اجرا، اشکالاتی دارد. برخلاف قانونگذاری بین المللی که از بالاترین سطح اجرا و پایین‌ترین سطح مشروعیت برخوردار است، خودانتظامی دارای بالاترین سطح مشروعیت و پایین‌ترین سطح اجراست. همچنین قانونگذاری ملی، حالتی بینابین بوده و همواره با ضعف نسبی در اجرا و مشروعیت مواجه است. لذا انتخاب روشی مختلط، زمینه را برای حل معضلات ناشی از مشروعیت و اجرا و همچنین نیل به تفاهم میان همه بازیگران فعال در فضای سایبر باز خواهد کرد. خصیصه برخی جنبه های اینترنت مانند جرایم و تجارت اینترنتی به گونه ای است که نیازمند قانونگذاری است، درحالیکه مناسب است جنبه های زیربنایی فضای سایبر با توجه به تخصصی‌بودن در اختیار

نهادهای غیردولتی حفظ شود. همچنین همکاری بین المللی برای یکسان‌سازی حقوقی لازم است. در این راستا، کنوانسیون بوداپست به شیوه مختلط توجه داشته و در ماده ۳۲ به همکاری بین المللی و در ماده ۱۱ به قانون‌گذاری متقابل توجه کرده است.

صلاحیت تقنینی در فضای سایبر

۱- صلاحیت سرزمینی

لازمه توسل به صلاحیت سرزمینی در فضای سایبر، وجود مرزهای دقیق است تا مقررات دولتی در حیطه آن عینیت یابد (۱۶). عدم امکان اجرای قواعد سنتی بر فضای بی‌انتهای سایبر از ویژگی‌ها و پیچیدگی‌های این فضاست. یکی دیگر از معضلات صلاحیت سرزمینی در فضای سایبر، ناپیدابودن محل ارتکاب جرم در این فضاست. اغلب نمی‌توان محل وقوع جرم را شناسایی کرد. حتی اگر تارنماها با کد کشوری به عنوان محل وقوع جرم ملاک گرفته شود، این اشکال درمورد تارنماهای با کد عمومی باقی می ماند. به رغم اینکه برخی کشورها معیارهایی مانند محل وقوع سامانه های رایانه‌ای، داده‌های رایانه‌ای و ذخیره اطلاعات را به عنوان ملاک تعیین سرزمین در نظر گرفته‌اند، لیکن، قانونگذاری های متعارض موجب می شود یک عمل در آن واحد در صلاحیت سرزمینی چند کشور قرار گیرد.

۲- صلاحیت شخصی

اعمال صلاحیت شخصی در فضای سایبر، مستلزم احراز تابعیت مجرم یا بزه دیده است. شناسایی مجرم در این فضا منوط به تعیین شناسهٔ اوست؛ درحالیکه فرد به راحتی با استفاده از برنامه های رایانه ای، قادر به جعل شناسهٔ خود می‌باشد. ثانیاً، لازمه اعمال صلاحیت شخصی منفعل در این فضا، انجام تحقیقات در رایانه‌های واقع در خارج از کشور (ولو از راه دور) است که موجب نقض حاکمیت سرزمینی کشور محل اطلاعات خواهد شد (۱۰). علاوه بر این، اعمال موسع صلاحیت شخصی در فضای سایبر به روند تجارت الکترونیک در فضای سایبر، لطمه خواهد زد (۱۳).

۳- صلاحیت واقعی

بکارگیری صلاحیت واقعی نیز با این اشکال روبه روست که ضابطه دقیقی برای توسل به آن وجود ندارد. البته دست دولت ها برای اعمال صلاحیت واقعی کاملاً باز نیست و باید از اعمال موسع صلاحیت واقعی امتناع کرد. لذا در این زمینه لازم است میان اعمال صلاحیت واقعی و اصل آزادی اینترنت، موازنه ای عادلانه برقرار شود که در نتیجهٔ آن، اعمال صلاحیت واقعی در فضای سایبر در چارچوب موازین حقوق بشری صورت پذیرد (۱۷). دادگاه آلمان در قضیه توبن در رابطه با انکار هولوکاست توسط یک استرالیایی در تارنمایی در استرالیا، صلاحیت واقعی را اعمال کرد (۱۸). دادگاه فرانسه نیز در رابطه با ارائه یادبودهای نازی ها در یک سرور مستقر در ایالات متحده معتقد بود که حقوق کیفری فرانسه نقض گردیده است. همچنین طبق قانون میهن دوستی امریکا، اداره تحقیقات فدرال مجاز است با قرار قضایی به پیامهای پستهای صوتی افراد، دسترسی داشته باشد یا مقامات مجاز بدون رعایت الزامات قانون شنود، اطلاعات رایانه-ای افراد را رهگیری کنند.

۴- صلاحیت جهانی

صلاحیت جهانی، یکی دیگر از مبانی قانونگذاری در فضای سایبر است. باید توجه داشت که برخی اقدامات در برخی مناطق، مورد ادعای صلاحیت هیچ دولتی نیست و لذا اعمال صلاحیت در خصوص آنها نه تنها مداخله در حاکمیت دیگر دولت ها نیست، بلکه برای جلوگیری از تبدیل شدن (سرزمین بی قانون) (۱۹) آن منطقه به پناهگاه امن متخلفین و پرهیز از شکل‌گیری، لازم است. دزدی دریایی در آبهای آزاد در گذشته و اقدامات مجرمانه در اینترنت در زمان حاضر از نمونه های این وضعیت است. ماده ۲۲ کنوانسیون جرایم سایبری شورای اروپا (کنوانسیون بوداپست) جایگاه صلاحیت جهانی در فضای سایبر را تأیید می‌کند. مبانی صلاحیت جهانی برای برخی جرایم سایبری مانند تحریک به نسل کشی در معاهدات بین المللی موجود است و قوانین داخلی دولت‌ها، برخی جرایم سایبری را مانند هرزه نگاری کودکان، مشمول صلاحیت جهانی

قرار داده اند. در مجموع، قانونگذاری ملی، مشکلاتی برای دولت‌ها و کاربران ایجاد خواهد کرد. این شیوه موجب اعمال فراسرزمینی قوانین خواهد شد که تعارض قوانین میان دولت‌ها را به دنبال خواهد داشت و همچنین موجب اعمال همزمان چند نظام حقوقی بر کاربران فضای سایبر و متعاقباً سردرگمی کاربران خواهد شد. لذا کاربران، خود به خود ملزم به رعایت قوانین متعدد و حتی متناقض خواهند بود، درحالیکه ممکن است از محتوای آن قوانین بی خبر باشند (۲۰). در این شیوه همچنین خطر چند کیفری وجود دارد؛ خصوصاً آنکه افراد نمی‌دانند کدام قانون را باید پاس بدارند و در نهایت مجبور خواهند بود مضیق‌ترین قانون را رعایت کنند (۲۱). در واقع، ماهیت جهان شمولی موجب می شود افراد بر اساس معیارهای مختلف صلاحیتی، تحت شمول قوانین چند کشور قرار گیرند (۲۲). با این حال، موافقت نامه های معاضدت قضایی و تعهدات حقوق بشر می‌توانند این معضل را کاهش دهند.

صلاحیت قانونگذاری در فضای سایبر در حقوق ایران

صلاحیت قانونگذاری با اتکا بر اقسام صلاحیت، شامل صلاحیت سرزمینی، شخصی، واقعی و جهانی، امکانپذیر است. ماده ۳ قانون مجازات اسلامی، مصوب ۱۳۹۲ و قوانین مرتبط با فضای سایبر، از جمله قانون تجارت الکترونیکی، مصوب ۱۳۸۲ ، قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه ای، مصوب ۱۳۷۹، قانون جرایم رایانه ای، مصوب ۱۳۸۸ و مقررات اصلاحی آن، مندرج در آیین دادرسی کیفری ۱۳۹۲ اصل را بر صلاحیت سرزمینی قرار داده‌اند. تقریباً در تمام مواد قانون جرایم رایانه ای و مواد مرتبط در قانون آیین دارسی کیفری، عبارت (هر کس) بدون توجه به تابعیت مرتکب به کار رفته است. هرچند معیار صلاحیت سرزمینی در جرایم گوناگون سایبری متفاوت است، معیار صلاحیت سرزمینی در ماده ۱ (دسترسی غیرمجاز)، ماده ۲ (شنود غیرمجاز) و ماده ۳ (جاسوسی رایانه‌ای) قانون جرایم رایانه ای، وقوع (سامانه های رایانه‌ای) در قلمرو ایران است. معیار صلاحیت سرزمینی در مواد ۶ و ۷ قانون جرایم

رایانه ای نیز وقوع (داده های رایانه ای) در قلمرو ایران است. بند (الف) ماده ۶۶۴ قانون آیین دادرسی کیفری، معیار دیگری اضافه می‌کند و (ذخیره اطلاعات) در قلمرو ایران را نیز مشمول صلاحیت سرزمینی ایران قرار می‌دهد. به علاوه بند (ب) این ماده، تارنماهای دارای دامنه مرتبه بالای کد کشوری ایران (ir) را در حکم خاک ایران قلمداد کرده و جرایم ارتکابی در این تارنماها را به مانند جرایم ارتکابی در قلمرو ایران می‌داند. صلاحیت شخصی فعال در ماده ۷ قانون مجازات اسلامی به طور موسع آمده است و تمامی جرایم از جمله جرایم رایانه ای را در بر می‌گیرد. ماده ۸ قانون مجازات اسلامی نیز به صلاحیت شخصی منفعل، اختصاص یافته است، هرچند اعمال آن، مشروط به جرم انگاری متقابل شده است. اغلب جرایم ارتکابی در فضای سایبر از سوی بارگذاران ارتکاب می یابد. لذا قانون جرایم رایانه ای در اغلب موارد، همانند ارتکاب هتک حیثیت و نشر اکاذیب در مواد ۱۶ و ۱۷ بارگذار را مجرم تلقی کرده است و لذا او مشمول صلاحیت قانونی ایران می‌شود. با اینحال، ماده ۱۴ در باب انتشار، توزیع، معامله، تولید، ذخیره یا نگهداری محتویات مستهجن، علاوه بر بارگذار، پیاده ساز را نیز مشمول مجازات دانسته است. صلاحیت واقعی در ماده ۵ قانون مجازات اسلامی آمده است و صراحتاً اقدام علیه امنیت داخلی یا خارجی را در حیطه صلاحیت ایران می‌داند. همچنین مطابق بند (پ) ماده ۶۶۴ قانون آیین دادرسی کیفری، ارتکاب جرم در خارج از ایران علیه سامانه‌ها یا تارنماهای مورد استفاده قوای سه گانه، نهاد رهبری، نمایندگی‌های رسمی دولت، نهادهای ارائه کننده خدمات عمومی و علاوه بر این، حمله گسترده به تارنماهای مرتبه بالای کد کشوری را در شمول صلاحیت محاکم ایران قرار داده است. بنابراین، رویکرد ایران در صلاحیت قانونگذاری در فضای سایبر، دربردارنده طیف متنوعی از صلاحیت های قانونگذاری سرزمینی، شخصی، واقعی و جهانی است.

رویکرد ایران در قانونگذاری فضای سایبر

رویکرد ایران در حیطه مدیریت داخلی اینترنت، مبتنی بر قانونگذاری ملی است. پیرو ابلاغ «سیاست‌های کلی شبکه‌های اطلاع رسانی رایانه ای» از سوی مقام رهبری،

شورای عالی انقلاب فرهنگی، «مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه ای» را در سال ۱۳۸۰ تصویب کرد. طبق این قانون به موازات حق دسترسی آزاد به اطلاعات، بر رعایت حقوق داخلی در موضوعات اجتماعی، فرهنگی و فنی کشور تأکید گردید. نخستین قانون جامع و متمرکز در ایران با رویکرد حقوق داخلی ایران، بر روش قانونگذاری ملی تکیه داشته و بر این مبنا، قانون جرایم رایانه ای، مصوب ۱۳۸۸ و قوانین اصلاحی آن، مندرج در قانون آیین دادرسی کیفری ۱۳۹۲، تدوین شده است.

مولفه‌های موثر بر قانونگذاری در جرایم رایانه ای و اینترنتی در جهان

در کشورهای گوناگون برای مدیریت جرایم رایانه‌ای، راهکارهای متفاوتی به کار گرفته می‌شود. بیشتر کشورها سعی دارند تا با تصویب قوانین و مقررات، آسیب های ناشی از جرایم رایانه ای را به کمترین میزان برسانند. اما علاوه بر این قوانین بازدارنده، باید مراجعی نیز وجود داشته باشند تا با شناسایی ریسک‌های فضای مجازی به خصوص در مورد کودکان، نرخ وقوع بزه را در این زمینه کاهش بدهند. در ادامه به چند نمونه از این ریسک ها پرداخته می شود.

۱- ریسک‌های فناوری اینترنت

ریسک‌های فناوری اینترنت مشتمل بر دو گروه اصلی است:

۱) ریسک های محتوا (کودک، در معرض نمایش محتوای در دسترس همه کاربران اینترنت در روابط یک به چند است).

۲) ریسک های تماس (کودک، به طور فعال، درگیر یک رابطه شخصی یا تعامل، دو جانبه یا چند جانبه، می باشد).

۱-۱- ریسک محتوا

ریسک محتوا، شامل سه زیر مجموعه اصلی است:

- محتوای غیرقانونی؛
- محتوای نامناسب سن یا محتوای زیان آور؛

- آگاهی و مشاوره زیان آور؛

عواقب احتمالی، متأثر از نوع ریسک و عوامل دیگر نظیر سن کودک و انعطاف-پذیری، متفاوت خواهند بود.

۱-۱-۱- محتوای غیرقانونی

محتوای غیرقانونی آنطور که از نام آن بر می‌آید، محتوایی است که انتشار آن، خلاف قانون است. مثلا ترویج جنبش نژادی، نژادپرستی، سخن گفتن از نفرت و دیگر اشکال تبعیض که در بعضی از کشورها ممکن است غیرقانونی باشند. خاصه، در جایی که ممکن است تحت دسته بندی محتوای نامناسب سن نیز قرار بگیرد. محتوای مرتبط با استثمار جنسی کودکان در بسیاری از کشورها غیر قانونی است و احتمال برخورد کودکان با این نوع محتوا، خیلی کم است. در یک نظرسنجی آمریکایی در سال ۲۰۰۶، فقط دو کودک ۱۰ تا ۱۷ ساله از ۱۵۰۰ کودک، با این نوع محتوا برخورد داشتند که مشخص شد یکی از آنها، از طریق یک لینک گمراه‌کننده بوده است.

۲-۱-۱- محتویات نامناسب سن

محتوایی مانند نفرت، خشونت و یا پورنوگرافی بزرگسالان، گرچه عموماً غیرقانونی نیست، ولی ممکن است به کودکان و رشد آنها آسیب برساند. کودکان به طور تصادفی می توانند با چنین محتوایی برخورد کنند و یا این محتوا توسط همسالان به آنها ارجاع داده شود و یا عمداً به دنبال آن محتوا باشند. آنها همچنین می‌توانند مشغول رسانه-های تعاملی مانند بازی های ویدیویی آنلاین شوند که خشونت واقع گرایانه ای دارند. چنین محتوایی ممکن است به صورت تجاری ارائه شود و اغلب به صورت آزادانه در دسترس باشد و یا می‌تواند توسط کاربران اینترنت ایجاد شود. مطالب اینترنت در دسترس عموم مردم، اغلب به وضعیت خاص مخاطبان کودک، حساس نیستند. در حقیقت، محتویاتی که برای افراد زیر سن قانونی مضر است، گاهی کودکان را هدف قرار می‌دهد؛ به عنوان مثال، از طریق نام دامنه گمراه کننده. صفحات وب که از نفرت و

دشمنی حمایت می‌کنند نیز، حاوی بخش‌هایی برای کودکان، همراه با بازی ها و اطلاعات غلطی برای آنان می‌باشند.

۳-۱-۱- آگاهی و مشاوره زیان آور

مشاوره های زیان آور، منجر به خودکشی، مصرف مواد مخدر یا الکل، و یا ایجاد اختلالات خوردن (مثلا بی اشتهایی) خواهند شد. همانطور که هر شخصی می‌تواند چنین محتوایی را در وب قرار دهد، کنترل آن نیز بسیار دشوار است. هرچند اطلاعات در مورد این موضوعات می تواند مفید باشد، لیکن تمایز میان توصیه های زیان آور و مفید، گاهی دشوار است.

اطلاعات بسیار محدودی در مورد خطرات مربوط به مشاوره های آنلاین زیان آور مانند خودکشی یا مواد مخدر موجود است. برخی تحقیقات نشان می‌دهد که در این حیطه، زنان، بیشتر در معرض خطر بی اشتهایی و آسیب به خود (خودآزاری) هستند.

۲-۱- ریسک‌های تماس

خطرات تماس هنگامی رخ می‌دهد که کودکان به صورت آنلاین در ارتباط باشند؛ مثلا شرکت در یک چت آنلاین.

توجه به این ریسک‌ها بیشتر پیرامون این است که آیا:

۱-تعامل، به قصد آسیب رساندن به کودک است (به عنوان مثال cybergrooming)؛

۲-کودکان، در معرض تعاملات آنلاین نفرت زا هستند؛

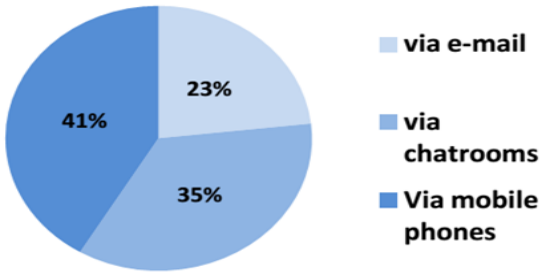
۳-کودک، به واسطه رفتار طرف مقابل، به خود آسیب برساند (به دلیل اشتراک فایل‌های غیرقانونی).

در ادامه مصادیقی از ریسک‌های تماس ذکر می‌شوند:

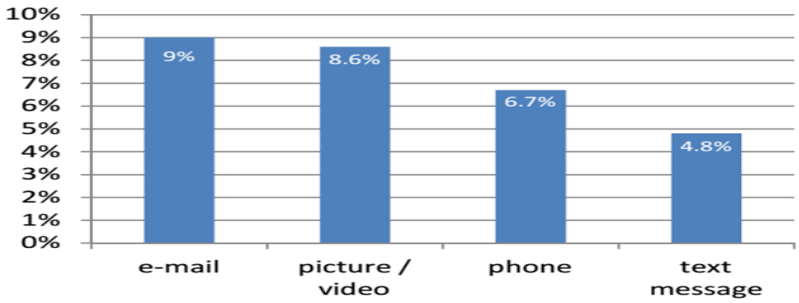
Online harassment: آزار و اذیت آنلاین، مسلماً شایعترین ریسک تماس است که کودکان با آن مواجه می شوند و محدوده هایی از: ارعاب، خجالت و حقارت، تا تهدیدات شدید از طریق وسایل الکترونیکی را در بر می گیرد. این کار می تواند به

شکل گردن‌کلفتی و قلدری سایبری، به اوج خود برسد که به موجب آن، افراد یا گروه‌ها با استفاده از فناوری اطلاعات و ارتباطات، به طور عمدی و مکرر به دیگران آسیب می-رسانند. اگرچه قربانیان آنها اغلب افراد کم سن و سال هستند، موارد آزار و اذیت کودکان بزرگسال نیز وجود دارند. استراتژی‌هایی شامل تهدیدهای مکرر از طریق ایمیل، پیام های متنی یا چت، انتشار در وب و یا گردش تصویرهای شرم آور، اغلب ناشی از نا آشنایی نسبی با رسانه های آنلاین می باشد، گر چه بیشتر قربانیان، هویت فرد آزاردهنده را می‌شناسند.

Flaming، نوعی از قلدری اینترنتی است که در آن، کودکان، یک مشاجره غیرمعمول شدید و تهاجمی را از طریق ایمیل یا پیام فوری دارند. در چنین تعاملاتی، قربانیان عموماً کودکان هستند. همانطور که شکل ۱-۶ و ۲-۶ نشان می دهد، تلفن همراه و ایمیل ها، مرکز اصلی این نوع آزار و اذیت می‌باشند.



شکل ۱-۶(میانگین قلدری سایبری دانش آموزان دبیرستانی در کانادا ۲۰۰۹)



شکل ۲-۶ (میانگین قلدری سایبری در سوئد بر روی دانش آموزان ۱۲ تا ۱۵ سال ۲۰۰۸)

توجه: نمودار فوق، میانگین دانش‌آموزان ۱۲ تا ۱۵ ساله در سوئد را که از طریق ایمیل، تصویر / ویدئو، تلفن و پیام متنی، مورد آزار و اذیت قرار گرفته اند، نشان می-دهد.

Cyberstalking ، نوع آزار و اذیت آنلاین است که در آن، تماس های یک فرد، به شکل تعقیب افراطی آنلاین، شامل تماس های مکرر و تهدیدات مخرب است؛ که ممکن است اطلاعات شخصی قربانی را به منظور ایجاد اضطراب روانی و جسمی، به خطر بیاندازد. آزار و اذیت اینترنتی و سایبری، رو به رشد و باعث نگرانی است و کودکان بزرگتر، بیشتر در معرض خطر قرار دارند. این آزار، با دسترسی به اینترنت و در دسترس بودن تلفن های همراه در میان جوانان، همبستگی و ارتباط دارد.

Illegal interactions؛ تعاملات غیرقانونی می توانند افراد زیر سن قانونی یا والدین را، در معرض خطر مجازات و جریمه کیفری یا مدنی قرار دهند. به عنوان مثال، دزدی آنلاین یا به اشتراک‌گذاری مطالب دارای حق تکثیر، در بعضی حوزه های قضایی مانند فرانسه، منجر به طی مراحل قانونی یا خطر تعلیق دسترسی به اینترنت در خانه شده است. شرط بندی (قمار) توسط کودکان زیر سن قانونی در اکثر کشورها غیر قانونی می‌باشد. درصورتی که کودکان، به یک کارت اعتباری یا سایر روش‌های پرداخت مانند تلفن همراه دسترسی داشته باشند در این صورت احتمال شرط‌بندی توسط آنان زیاد خواهد بود و این حالت یک تهدید مالی برای والدین به حساب می‌آید. اشتراک-گذاری فایلهای غیرقانونی، اغلب در مورد نوجوانان مطرح می‌شود.

۲- ریسک های مربوط به مشتری

در این زمینه، کودکان به عنوان مصرف‌کننده اینترنت، در موارد ذیل مورد هدف قرار می‌گیرند:

- پیام های بازاریابی آنلاینی دریافت کنند که برای کودکان، نامناسب است (به عنوان مثال: محصولات محدود به سن، مانند الکل)؛

- در معرض پیام های تجاری باشند که به راحتی شناخته نمی شوند (مثلا تعیین سطح محصولات) یا مواردی که فقط برای بزرگسالان در نظر گرفته شده است (به عنوان مثال خدمات دوستیابی)؛

- از ساده لوحی و بی تجربگی آنها سوء استفاده شود که احتمالا یک خطر اقتصادی (به عنوان مثال کلاهبرداری آنلاین) را ایجاد می کند.

۳- ریسک های حریم خصوصی و امنیت اطلاعات

خطرات حفظ حریم خصوصی و امنیت اطلاعات، برای همه کاربران به خصوص کودکان وجود دارد. کودکان، گروه آسیب پذیری از کاربران آنلاین هستند، زیرا اغلب آگاهی و ظرفیت پیش‌بینی عواقب احتمالی (مثلا افشای اطلاعات شخصی آنلاین در اینترنت) را ندارند و این در حالی است که سازوکارهای حفاظتی موجود ممکن است برای حفاظت حریم خصوصی و امنیت موثر، ناکافی باشد.

۱-۳- حریم خصوصی اطلاعات کودکان

کودکان، خطر حریم خصوصی اطلاعات را هنگامی متحمل می شوند که اطلاعات شخصی آنها از طریق اینترنت، به صورت خودکار جمع آوری می شود. به عنوان مثال، می‌توان به کوکی ها اشاره نمود که افراد بر اساس درخواست یک ارائه‌دهنده سرویس اطلاعاتی (به عنوان مثال هنگام ثبت نام یا خدمات) یا به طور داوطلبانه، اطلاعات شخصی خود را در فرم های آنلاین، پر می کنند.

۲-۳- خطرات مرتبط با امنیت اطلاعات

امنیت اطلاعات، به طور کلی، چالشی برای کاربران اینترنت است. با اینحال کودکان به طور خاص در معرض خطرات امنیت اطلاعات ناشی از کد مخرب مثلا بدافزار و جاسوس‌افزارها هستند. آنها از خطرات آگاهی ندارند و از خدمات با ریسک بالاتر، شامل نرم‌افزارهای مخرب استفاده می‌کنند. به عنوان مثال، جرایم آنلاین مانند آلوده‌کردن کامپیوتر خانواده که والدین از آن برای بانکداری آنلاین استفاده می‌کنند در کمین کودکان قرار دارد. جاسوس‌افزار تجاری، در وب‌سایت‌های کودکان قرار داده می‌شود و

در دستگاه کاربر ذخیره می‌شود تا رفتار آنلاین او را نظارت کند. این اطلاعات امکان دارد برای اهداف دیگر به عنوان مثال بازاریابی آنلاین استفاده شود. این موضوع در دپارتمان حفظ حریم خصوصی اطلاعات کودکان (برای کودکان، مدارس و خانواده‌ها، وزارت فرهنگ، رسانه و ورزش) مورد بررسی قرارگرفته است.

۴- تحمیل هزینه بیش از حد

استفاده بیش از حد از اینترنت یا خدمات تلفن همراه توسط افراد زیر سن قانونی میتواند هزینه های بالایی را برای والدین ایجاد نماید. به عنوان مثال، کودکان می‌توانند مشترک خدمات آنلاین مبتنی بر هزینه شوند یا در شرط بندی آنلاین، پول هزینه نمایند. همچنین، برخی از بازیهای محبوب آنلاین، نیاز به اشتراک دارند و بازیکنان می‌بایست هزینه هایی را برای خرید کالاهای مجازی یا کاراکترهای مجازی پیشرفته، صرف کنند.

۵- معاملات جعلی

هنگامی که کودکان وارد قرارداد فروش از راه دور می شوند، امکان تحقق معاملات جعلی فراهم می شود؛ اما در این معاملات، پول پرداخت می شود. مانند: دانلود آهنگ-های زنگ برای تلفن همراه؛ در این شرایط، کودکان ممکن است متوجه نشوند که هزینه های اضافی را پرداخت می‌کنند و یا حتی مشترک سرویسی هستند که هزینه-های آن، به طور منظم با کارت‌های پیش‌پرداخت، پرداخت می گردد.

به هر تقدیر باید پذیرفت که خطرات اقتصادی ناشی از بی‌تجربگی کودکان باعث می‌شود که آنها هدف مناسبی برای تقلب و کلاهبرداری آنلاین باشند. البته جوانانی که هنوز حساب بانکی یا کارت اعتباری ندارند، کمتر آسیب مالی متحمل می شوند اما با این حال، ممکن است قربانی سرقت هویت شوند و بهره برداری از اطلاعات شخصی آنها ممکن است منجر به سوابق اعتباری غلط گردد.

نتیجه‌گیری

فضای مجازی نباید تبدیل به سرزمینی بی‌قانون در بستر این جهان پهناور گردد. مستفاد از صلاحیت جهانی -یکی از مبانی قانونگذاری در فضای سایبر- باید توجه داشت نسبت به برخی اقدامات در مناطقی که مورد ادعای صلاحیت هیچ دولتی نیست، آن مناطق، به پناهگاه امن متخلفین و بزهکاران مبدل نشود و تدوین قانون با نگاه صلاحیت جهانی پرهیز از شکل‌گیری منطقه امن برای بزهکاران در مناطق بی‌طرف دولتها صورت پذیرد. بر این مبنا در کنوانسیون بوداپست، جایگاه صلاحیت جهانی در فضای سایبر، تأیید می شود.

امروزه با پیشرفت تکنولوژی و گسترش اینترنت و تشکیل و توسعه شبکه‌های مجازی با وساطت کامپیوترهای شخصی، گوشی‌های هوشمند، تبلت ها و غیره، اهمیت امنیت برای فعالیت در این فضاها، مخصوصاً برای کودکان و نوجوانان بیش از پیش احساس می شود. با پیشرفت فناوری اطلاعات و ارتباطات از یک سو و تنوع جرایم رایانه‌ای و کثرت بزه دیدگان بالقوه در ایران، ایجاد قوانین جدید مرتبط و به روز در این زمینه، ضرورت دارد تا بتواند پیامدهای منفی ناشی از فناوری اطلاعات را کنترل کرده و یا تقلیل دهد. تصویب قانون جرایم رایانه ای در ایران، گام مثبتی در جهت مقابله با مجرمان همگام با کمک به توسعه فناوری اطلاعات بود. نباید فراموش کنیم که اکنون با قوانینی در رابطه با جرایم رایانه ای روبه رو هستیم که تمامی کاربران رایانه و اینترنت کشور را در بر گرفته و تکلیف‌هایی را بر عهده ما گذارده است. از آنجایی که جرایم رایانه ای هر روز بیشتر شده و با شیوه های متفاوتی رخ می دهند، باید ابتدا به فکر پایه‌گذاری روش‌های پیشگیرانه بود. با تصویب قوانین بازدارنده می توان از رخداد این جرایم جلوگیری کرد و از آنجا که دولت الکترونیک در دستور کار قرار گرفته است، باید قوانین لازم را برای کاهش هر چه بیشتر این دسته مشکلات و وقوع جرم های رایانه ای، تصویب نمود تا بتوان در بخش های گوناگون همچون تجارت الکترونیک هم گام های خوبی برداشت.

همچنین باید از اجرای کامل و صحیح این قوانین، اطمینان حاصل کرد. بدون شک، انجام کارهای مطالعاتی و تحقیقاتی در زمینه موضوعات مهم، حساس و مبتلابه جامعه برای رصد نیازهای تقنینی و همچنین ضعف‌ها و قوت‌ها در اجرای قوانین مربوطه، یکی از ضروریات حوزه های دانشگاهی و پژوهشی است.

با مطالعه ی قانون جرایم رایانه ای، متوجه می شویم تنها دو شکل از انواع ضمانت اجرا یا همان مجازات وجود دارد: جریمه نقدی و زندان. گمان می رود تصویب قوانین سخت، اعمال دقیق و بدون رعایت مصالح شخصی توأم با تنوع و تناسب در ضمانت اجراهای به کار گرفته شده، شرایط مناسب تری را برای رشد و توسعه فناوری اطلاعات و ارتباطات همگام با صیانت از افراد جامعه به ویژه طیف کودکان و نوجوانان، فراهم آورد. دولت باید آسیب های بخش جرایم رایانه ای و اینترنتی را در کشور کاهش داده و با آموزش جوانان در خصوص چگونگی استفاده از اینترنت و توضیح اخلاق مجازی که اشاره به یک سری از رفتارهای سالم و مسئولانه در جامعه افراد حاضر در اینترنت دارد، نقش هدایت محور و پیشگیرانه خود را ایفا نماید.

در رابطه با یافته‌های این تحقیق، راهکارهایی به شرح ذیل قابل ارائه است:

۱- با توجه به این که جرایم رایانه ای از جمله جرایم فراملی محسوب می‌شود و یک سند خاص بین‌المللی الزام‌آور در این زمینه برای کشورها وجود ندارد، لذا در راستای همکاری و حمایت بیشتر از بزه دیدگان جرایم سایبری مبتنی بر سیاست حمایت از بزه دیدگان، مقررات ویژه ای توسط قوه مقننه تصویب گردد.

۲-در حقوق داخلی چون مقررات کیفری جامع و مؤثری در حمایت از بزه دیدگان کودک و نوجوان در فضای سایبر در قالب قانون جرایم رایانه ای و آیین دادرسی جرایم رایانه‌ای کشورمان پیش بینی نشده است و مقررات عام آیین دادرسی کیفری نیز به خوبی تأمین‌کننده حمایت لازم از این بزه دیدگان خاص نمی‌باشد، لازم است تا نسبت به توسعه قوانین فعلی در راستای حمایت از بزه دیدگان جرایم سایبری، اقدام گردد.

۳-معاونت پیشگیری از جرم قوه قضاییه در جهت ارتقاء سطح آموزش کودکان با همکاری صدا وسیما، ایجاد قرارگاه تولید انیمیشن مطابق با تجربه خوب کاراکترهای

آموزش راهنمایی ورانندگی ناجا، را در دستور کار قرار دهد و اقدام به آموزش بصری به سرمایه‌های اصلی کشور یعنی کودکان، از طریق فضای مجازی یا تلویزیون با هدف پیشگیری از ارتکاب جرایم در فضای مجازی، نماید.

۴-مراکز داده‌ای در کشور با محوریت موارد آسیب های فضای مجازی نسبت به کودکان و نوجوانان تشکیل شود تا پژوهشگران با سهولت تحقیقات پژوهشی خود را انجام داده و آسیب شناسی هدفمند و دقیقتری برای تبیین اولویت‌های برنامه‌ریزی و اقدامات عملی در خصوص حمایت از کودکان، به عمل آورند.

References

1. Shirzad K. Computer Crimes from the Perspective of Iranian Criminal Law and International Law. Tehran: Behine Publications; 2009. p.4.

2. Analysis of various types of cyber crimes, by Hassoun Y. No. 26, October and November 2010.

3. Farahani Jalali A H. An Introduction to the Criminal Procedure Code of Cybercrime. Tehran: Khorsandi Publications; 1998. p.1.

4. Hosseini B. Cybercrime against Children and its Criminological Fields. First Edition.Tehran: Afraz Publications; 2004.

5. Nemati Z. Pornography with a look at the law on how to punish persons who engage in illegal activities in audio-visual matters. Master's Thesis. Tehran: University of Tehran - Faculty of Law and Political Science; 2010.

6. Rezaie M, Babazadeh Moghadam H. Principles of Law and Regulation for the Internet with Emphasis on UNESCO and Council of Europe Resolutions. Quarterly Journal of Public Law Research 2014; 15(4): 43-82.

7. Ghannad F, Akbari M. Securityism of Criminal Policy. Criminal Law Research 2017; 5(18): 39-67.

8. Norris G, Lincoln R, Wilson P. Contemporary comment: An examination of Australian internet hate sites. Bond University. 2005.

9. Zamani G, Bahramlo M. [Translation of Human rights and the Internet]. Hick S, Halpin E, Hoskins E.(editors). Tehran: Khorsandi Publications; 2006.

10. Rezaee A. Electronic Commercial Law. Tehran: Mizan Legal Foundation; 2009.

11. Hasan Baigi E. law and Security in Cyberspace. Cultural Institution of International Studies and Researches. Abrar Moaser; 2005.

12. Kamal A. The Law of Cyber-Space, An Invitation to the Table of Negotiations. Published by United Nations Institute for Training and Research; 2005.

13. Omidi M. Iran ICT Newes. 2010; Available at: https://www.ictna.ir/

14. Stuart BI. Beyond our control? Confronting the limits of our legal system in the age of cyberspace; 2001.

15. Vacca JR. Computer forensics: computer crime scene investigation. Hingham, MA: Charles River Media; 2005.

16. Kamal A. The Law of Cyber-Space, An Invitation to the Table of Negotiations. Published by United Nations Institute for Training and Research; 2005.

17. Brancik K. Insider computer fraud: an in-depth framework for detecting and defending against insider IT attacks. Auerbach Publication; 2008.

18. Williams M. Virtually criminal: Crime, deviance and regulation online. London: Routledge; 2006.

19. InfoTech. Computer Crime Prevention Law. Access on: How countries handle computer crime. Ethics and Law on the Electronic Frontier; 2010.

20. Walden I. Computer crimes and digital investigations. Oxford: Oxford University Press, Inc.; 2007.

21. Casey E. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press; 2011.

22. Carroll JM. Computer security. Butterworth-Heinemann; 2014.