فصلنامه بین المللی قانون یار
License Number: 78864 Article Cod: 2020S4D14SH19M ISSN-P: 2538-3701

سیاست تقنینی حقوق کیفری ایران با رویکرد تامین امنیت فضای مجازی مختص کودکان

(تاریخ دریافت ۱۳۹۹/۰۲/۱۵، تاریخ تصویب ۱۳۹۹/۰۵/۱۲)

سیدعباس خلیل پور چالکیاسری
دانشجوی دکترا حقوق جزاوجرم شناسی
مسئول دفترحمایت حقوقی وقضایی ایثارگران لنگرود
پژوهشگر برگزیده کشور و دارنده تندیس پژوهشگر برتر سال ۱۳۹۸ از موسسه قانون یار

چکیده

پیشرفت خیره کننده فناوری اطلاعات درسال های آغازین سده بیست ویکم دگرگونی های بیشماری را در زمینه های فناوری واطلاعات بوجود آورده ودروازه دیگری را به جهان نوین گشوده بطوریکه تمام فعالیت های اقتصادی اجتماعی سیاسی فرهنگی و علمی بشر را به طور بنیادین دستخوش تغییر وتحول قرار داده است. علم حقوق نیز به عنوان شاخه ای از علوم انسانی که تنظیم روابط انسان ها را در چارچوب حیات جمعی به عهده داشته واز آنجایی که دنیای مجازی ودسترسی آسان و ساده کودکان به اینترنت و وجود خطرات اجتناب ناپذیر در این پهنه گسترده پرسش هایی را در خصوص اقدامات حقوقی صورت داده که برای جلوگیری از ورود کودکان در دنیای مجازی و اقدامات قانونی لازم جهت حفاظت آن ها پدید آورده است. رویکرد کیفری متمایز در حقوق کیفری ماهوی جرایم رایانه ای می تواندبا پیشگیری آسیب ها نسبت به کودکان و نوجوانان رابه حداقل ممکن کاهش دهددر 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 نهایتا" 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 قرار بگیرند مطرح می شود.

واژگان کلیدی: فضای مجازی، کودکان، حقوق کیفری، سیاست تقنینی، حقوق کودک

مقدمه

توسعه پدیده جهانی فناوری اطلاعات و ارتباطات تحولی شگرف در ابعاد مختلف حیات اقتصادی اجتماعی فرهنگی امنیتی وسیاسی ایجاد نموده است. انقلاب الکترونیک تبدیل به مهم ترین پدیده تعیین کننده معاصر شده است. روزانه ده ها هزار رایانه ورود خود را به دنیای جدید اعلام می کنند. فناوری اطلاعات و ارتباطات نه تنها صنعت، اقتصاد، تجارت و دیگر عرصه ها را تحت تأثیر قرار داده است، بلکه حقوق هم از این تحولات بی بهره نبوده است. به فراخور این تغییرات بنیادین، طبعاً حقوقدانان نیز همانند متخصصین دیگر رشته ها 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 چالش هایی هم دارد کودکان و نوجوانان هنگامی که به جهان اینترنت، پا می گذارند به گشت وگذار در اینترنت می پردازند. مجموعه فیلم های درون اینترنت که دسترسی پیدا می کنند، به گپ سرا های اینترنتی که سر می زنند و پیوند های اجتماعی معقول و نامعقول برقرار می کنند، در معرض خطر عناصری از اجتماع قرار می گیرند که در جهان واقعی از آنان پرهیز می کنیم وبه دلیل وجود محرک های پر جاذبه و مسحور کننده در اینترنت، کودکان و نوجوانان به عنوان سریع ترین کاربران در حال رشد بیشتر در معرض آسیب جنبه های منفی آن قرار می گیرند. آن ها اغلب اوقات از طریق آی پاد، سایت های ویدیویی، سایت های شبکه های اجتماعی، اتاق های چت، سایت هایی با چند بازیکن در بازی های تعاملی و بعلاوه دوربین های وب کم و گوشی های هوشمند، عملا در دسترس رسانه ها هستند. کودکان با ورود به اینترنت با دنیای جدید مواجه می شوند که در آنجا می توانند هم مجهولات زیادی کشف کنند و هم مطالب زیادی یاد بگیرند. وجود اطلاعات متعدد در اینترنت مزایای پرشماری برای نوجوانان فراهم می کند، اما تهدیدات جدی را نیز با خود با ارمغان می آورد مانند: قرار گرفتن در معرض آزار و اذیت جنسی، دسترسی به مواد مضر و غیرقانونی مخدر، الکل، سیگار، قمار و بسیاری از مواد پرخطردیگر. به دلایل روشنی نمی توان از کودکان و نوجوانان خواست 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 زندگی شان در جهان پر از تباهی بزهکاران فضای اینترنت به شدت به خطر می افتد. فضای اینترنت فضای پر از چالش است به نظر پژوهشگر یکی از وجوه تمایز واکنش به جرایم رایانه ای، کیفیت تعریف جرایم، تعریف و توسعه مسئولیت کیفری و تعیین مجازات در قوانین کیفری ظاهر می شود، به گونه ای که قابلیت اجرایی، ارعابی و بازدارندگی بیشتری به واکنش های کیفری ببخشد.

بخش اول: بیان مساله واهمیت حق بر شادی کودکان

آسیب ها و خطرات بالقوه موجود برای کودکان در سراسر جهان را می توان در سه دسته کلی هدف گیری تجاری و تبلیغاتی، بهره برداری و استثمار جنسی کودکان و نقض حریم خصوصی آن ها تقسیم کرد. کودکان در اینترنت بخش قابل توجهی از اطلاعات شخصی خود را در محیط هایی چون اتاق های گفت و گو شبکه های اجتماعی، سایت های بازی آنلاین و مثل آن افشا می کنند که جمع آوری داده های غیرقانونی آن ها تهدیدی جدی برای حریم خصوصی آن ها به شمار می آید چرا که هرگز مشخص نیست که این اطلاعات بدست چه کسانی می افتد و چگونه مورد استفاده قرار می گیرند چنین وضعیتی می تواند کودکان را در معرض استفاده های تجاری از اطلاعات آن ها با هدف گیری تبلیغاتی قرار دهد. در دهه اخیر پدیده سوء استفاده جنسی و هرزه کاری کودکان که عمدتا از طریق فریب و جمع آوری اطلاعات کودک در فضای وب صورت می گیرد. نگرانی جدی در جامعه ایجاد کرده است حال باید دید که حقوق کیفری برای جلوگیری از طعمه قرار گرفتن کودکان چه راهکارهای را پیش بینی کرده است. لذا در این مقاله سعی می شود تا به بررسی حقوقی(از منظر حقوق کیفری و جزای اختصاصی) امنیت جزایی برای کودکان و سامانه های رایانه ای در نظام حقوقی ایران جهت مقابله و پیشگیری هرچه بهتر از این جرایم، بیان مسائل و مشکلات و نقاط قوت و ضعف قوانین مصوبه بجهت اهمیت حق بر شادی کودکان و ارائه پیشنهادات و راه حل هایی برای حل این مشکلات با هدف ارتقای سطح دانش و اطلاعات در مورد جرایم فضای مجازی برای کودکان و بهره گیری از نتایج مقاله توسط مراجع تقنینی آموزشی پژوهشی و

ارائه پیشنهادهای مناسب و کاربردی به مقامات تقنینی و قضایی برای پیش بینی مقررات مناسب یا اصلاح قوانین و پاسخ های مناسب به جرایم فضای مجازی وشناسایی تفاوت های جرایم رایانه ای باعناوین سنتی مشابه در سایر قوانین کیفری وجزاییپرداخته شود. و از آنجایکه آسیب هاوخطرات بالقوه موجودبرای کودکان درسراسرجهان هدف گیری تجاری وتبلیغاتی، بهره برداری واستثمار جنسی، کودکان ونقض حریم خصوصی آنها وهمچون پدیده سوء استفاده جنسی و هرزه کاری کودکان عمدتا از طریق فریب و جمع آوری اطلاعات کودک در فضای وب صورت گرفته که می تواند موجب آسیب های غیر قابل جبران بر کودکان شود فضای مجازی از طریق زمینه های فرهنگی اجتماعی، بازیهای رایانه ی و فضای سایبری می تواند بر هویت کودکان موثرمی باشد. از انجاییکه کمتر راجب به سیاست تقنینی رویکردکیفری ایران برای امنیت کودکان در فضای مجازی تحقیق شده ضرورت دارد به جهت اهمیت وضعیت کودکان در فضای مجازی مورد بررسی و تحقیق صورت بگیرد.

بخش دوم: فضای مجازی

فضای مجازی عبارت است از مجموعهٔ ارتباطات درونی انسان ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی. به تعبیر دیگر، فضای مجازی فضایی است که در آن فعالیت های 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

بند اول: مهم ترین ویژگی های فضای مجازی

۱ – هزینه پایین ورود

۲– گمنامی

۳ – نامتقارن بودن در آسیب پذیری

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 رسانه ای بود

۹ – سهولت تعامل و تبادل اطلاعات با دیگران

۱۰ – سرعت بالای تبادل اطلاعات و امکانات قابل توجه اینترنت برای افر اد جامعه

بخش سوم: تعریف و تاریخچه جرایم رایانه ای

تعیین دقیق اولین جرم رایانه ای در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست و بعد از این تاریخ بود که گروه های هکر جرم های دیگری را مرتکب شدند. بر اساس آمارهای موجود در سال ۱۳۸۴، ۵۳ مورد پرونده مربوط به جرم اینترنتی و رایانه ای در کشور تشکیل شد. از مهم ترین موارد جرایم رایانه ای در سال گذشته 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 موضوعات متفرقه بوده است. هرجرمی که قانون گذار به صراحت رایانه را به منزله موضوع یا یا وسیله جرم جزء رکن مادی آن اعلام کرده باشد، یا عملا رایانه به منزله موضوع یا وسیله ارتکاب یا وسیله ذخیره یا پردازش یا انتقال دلایل جرم در آن نقش داشته باشد.

بخش چهارم: ویژگی جرایم رایانه ای

۱. سرعت

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 بزه کاری یعنی بزه کار، 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 بدون وجود مانعی به نام مکان، جرایم متعددی را در سریع ترین زمان مرتکب شوند

۲. ناشناختگی

ناشناختگی از اصول حاکم بر جرایم مجازی است. از یک سو اصولاً شناسایی کاربران ماشین متصل به شبکه امری پیچیده و پرهزینه است. از سوی دیگر استفاده از شیوه های سرقت مشخصات دیگر ماشین ها، استتار آنلاین و سایر مخفی کاری های موجود، امر شناسایی مرتکبین را به صورت معمول سخت و بعضا غیر ممکن ساخته است. 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 توسط بزه کار سریعاً نابود می شوند و یا به صورت اتوماتیک از بین می روند.

۳. حجم و ارزان بودن جرایم

مقیاس بزه های ارتکابی در فضای سایبر بسیار وسیع است و به علت امکانات موجود و فقدان محدودیت ها، بزه کار از الگوی سریالی و شبکه ای استفاده می کند. 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. مهم ترین 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

۴. رویکرد ایران در قانونگذاری فضای سایبر

رویکرد ایران در حیطه مدیریت داخلی اینترنت، مبتنی بر قانونگذاری ملی است. پیرو ابلاغ (سیاست های کلی شبکه های اطلاع رسانه ای رایانه ای) از سوی مقام رهبری، شورای عالی انقلاب فرهنگی، (مقررات و ضوابط شبکه های اطلاع رسانی 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 شد. نخستین قانون جامع و متمرکز در ایران با رویکرد قوانین داخلی ایران بر روش قانونگذاری ملی تکیه داشته وقانون جرایم رایانه ای، مصوب ۱۳۸۸ و قوانین اصلاحی آن، مندرج در قانون آیین دادرسی کیفری ۱۳۹۲ تدوین شده است.

بخش پنجم: صلاحیت قانونگذاری در فضای سایبر در حقوق ایران

صلاحیت قانون گذاری 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، ازجمله 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 داده اند. 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 رایانه ای) قانون جرایم رایانه ای، معیار وقوع (سامانه های رایانه ای) در قلمرو ایران است. معیار صلاحیت سرزمینی در مواد ۶ و۷ 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 درماده ۷ قانون مجازات اسلامی ب طور موسع آمده است وتمامی جرایم ازجمله جرایم رایانه ای رادربرمیگیرد. 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 درفضای 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 بارگذاررا مجرم تلقی کرده است و لذا او مشمول صلاحیت قانونی ایران میشود. بااینحال، 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 سامانه ها 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 کرده است. لذا رویکرد ایران در صلاحیت قانونگذاری در فضای سایبر، دربردارنده طیف متنوعی از صلاحیت های قانونگذاری سرزمینی، شخصی، واقعی و جهانی است.

بخش ششم: دلایل ومخاطرات فضای مجازی برای کودکان وسیاست تقنینی کیفری

بند اول: ریسک های آنلاین برای کودکان

سه دسته گسترده از ریسک های آنلاین برای کودکان عبارتند از:

۱)ریسک های (خطرات) فناوری اینترنت یعنی زمانی که اینترنت، رسانه ای است که در آن کودکان برای نمایش محتوا یا مکان تعامل از آن استفاده می کنند.

۲) خطرات مربوط به مصرف کنندگان برای کودکان آنلاین یعنی کودک به عنوان یک مصرف کننده آنلاین، مورد هدف قرار می گیرد؛

۳) خطرات حریم خصوصی اطلاعات و خطرات امنیتی یعنی خطراتی که هر کاربر اینترنتی با آن مواجه است و در آن کودکان، یک گروه کاربری آسیب پذیر خاص را تشکیل می دهند.

بند دوم: ریسک های فناوری اینترنت

۱) ریسک های محتوا (کودک، در معرض نمایش محتوای دردسترس 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).

بند سوم: محتویات نامناسب سن

محتوایی مانند نفرت، خشونت و یا پورنوگرافی بزرگسالان، گرچه عموما 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 میشود و یا عمدا به دنبال آن محتوا هستند. آنها همچنین میتوانند مشغول رسانه های تعاملی مانند بازی های ویدیویی آنلاین شوند که خشونت واقع گرایانه ای دارند. چنین محتوایی می تواند به صورت تجاری ارائه شود و اغلب به صورت آزادانه در دسترس است و یا می تواند 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 می دهد به عنوان مثال، از طریق نام دامنه گمراه کننده. صفحات وب که از نفرت و دشمنی حمایت می کنند نیز، حاوی بخشهایی برای کودکان، همراه با بازی ها و اطلاعات غلطی برای آنها هستند.

بند چهارم: آگاهی و مشاوره زیان آور

مشاوره های زیان آور، منجر به خودکشی، مصرف مواد مخدر یا الکل، و یا اختلالات خوردن (مثلا بی اشتهایی) خواهند شد. همانطور که هر شخصی از جمله افراد زیر سن قانونی، می تواند 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، دشوار است. اطلاعات بسیار محدودی در مورد خطرات مربوط به مشاوره های آنلاین زیان آور مانند خودکشی یا مواد مخدر موجود است.

بند پنجم: بازاریابی آنلاین کودکان

آگهی های آنلاین برای محصولات محدود به سن افراد زیر سن قانونی، مانند الکل، سیگار و داروهای تجویزی، باعث افزایش نگرانی هایی می شود که برای شیوه زندگی خطرناک هستند و کودکان را با تامین کنندگان آنلاین، ارتباط میدهند. امکان خرید آنلاین این محصولات برای کودکان، لزوما به این معنی نیست که آنها این کار را انجام می دهند بازاریابی اینترنتی آنلاین که کودکان را هدف قرار میدهد در یک صفحه وب محبوب کودکان، نمایش داده میشود و این میتواند در زمانی که عدم تفکیک محتوا و تبلیغات وجود دارد، مشکل ساز باشد. برای افراد زیر سن قانونی به خصوص بچه های جوانتر، محتوای تجاری، کمتر از سایر محتواها، قابل تمایز است. تبلیغات بازی ها [2]، مثالی از تکنیک های بازاریابی بحث برانگیز است که تبلیغات را با بازی ها و ویدیوهای آنلاین، ترکیب می کند. به همین دلیل، برخی از وکلای مدافع، در مورد استفاده از تبلیغات و نام های تجاری الحاق شده در وب سایتها که کودکان را هدف قرار می دهد، شک و تحقیق می کنند. آنها همچنین این موضوع را مطرح کرده اند که کدام رده سنی کودکان، در معرض شیوه های بازاریابی آنلاین قرار دارند. بازاریابی تبلیغات حاوی محتوای نامناسب، می تواند در استفاده روزانه از اینترنت، به کودکان آسیب وارد کند (مانند: آگهی ها یا هرزنامه هایی حاوی تصاویر صریح جنسی). گسترش شرطبندی و دوست یابی می تواند باعث ایجاد اختلال در کودکان و نوجوانان شود و رفتارهای پرخطر را که ممکن است منجر به زیان مالی و یا درخواست جنسی شود.

بند ششم: هزینه بیش از حد

استفاده بیش ازحد ازاینترنت یاخدمات تلفن همراه توسط افراد زیرسن قانونی میتواندهزینه های بالایی را برای والدین ایجاد کند. به عنوان مثال، کودکان می توانند مشترک خدمات آنلاین مبتنی برهزینه شوند یا درشرط بندی آنلاین، پول هزینه کنند. برخی از بازیهای محبوب

آنلاین، نیاز به اشتراک دارند و بازیکنان می بایست هزینه هایی را برای خرید کالاهای مجازی یا کاراکترهای مجازی پیشرفته، صرف کنند.

بند هفتم: معاملات جعلی

هنگامی که کودکان وارد قرارداد فروش از راه دور می شوند، معاملات جعلی انجام می شود، اما در این معاملات، پول پرداخت می شود. مانند: دانلود آهنگ های زنگ برای تلفن همراه. 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 کارت های پیش پرداخت، پرداخت می شود. خطرات اقتصادی ناشی از بی تجربگی کودکان باعث میشود که آنها هدف مناسبی برای تقلب و کلاهبرداری آنلاین باشند. نوجوانانی که هنوز حساب بانکی یا کارت اعتباری ندارند، کمتر آسیب مالی متحمل می شوند با این حال، ممکن است قربانی سرقت هویت شوند و بهره برداری از اطلاعات شخصی آنها ممکن است منجر به سوابق اعتباری غلط شود.

بند هشتم: حریم خصوصی اطلاعات کودکان و خطرات امنیتی اطلاعات

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، کوکی ها که افراد بر اساس درخواست یک ارائه دهنده 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. 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 جاسوس افزارها هستند. آنها از خطرات آگاهی ندارند و از خدمات با ریسک بالاتر، شامل نرم افزارهای مخرب استفاده میکنند. به عنوان مثال، جرایم آنلاین مانند آلوده کردن کامپیوتر خانواده که والدین از آن برای بانکداری آنلاین استفاده می کنند در کمین کودکان قرار دارد. جاسوس افزار تجاری، در وب سایت های کودکان قرار داده میشود و در دستگاه کاربر ذخیره می شود تا

رفتار آنلاین او را نظارت کند. این اطلاعات ممکن است برای اهداف دیگر به عنوان مثال بازاریابی آنلاین استفاده شود. این موضوع در دپارتمان حفظ حریم خصوصی اطلاعات کودکان (برای کودکان، مدارس و خانواده ها، وزارت فرهنگ، رسانه و ورزش) مورد بررسی قرارگرفته است.

نتیجه گیری

از جمله دغدغه های همیشه بشر در زندگی امنیت بوده است. امروزه با پیشرفت تکنولوژی و گسترش اینترنت و شبکه های مجازی توسط کامپیوتر های شخصی، گوشی های هوشمند، تبلت ها و غیره، اهمیت امنیت برای فعالیت در این فضاها، مخصوصا برای کودکان و نوجوانان بیش از پیش احساس می شود. با پیشرفت فن آوری اطلاعات و ارتباطات از یک سو و تنوع جرایم رایانه ای و کثرت بزه دیدگان بالقوه در ایران ایجاد قوانین قضایی جدید مرتبط و به روز ضرورت داردتا بتواند پیامدهای منفی فناوری اطلاعات را پیشگیری کرده و یا کاهش دهد. تصویب قانون جرایم رایانه ای در ایران، گام مثبتی در جهت مقابله با مجرمان و کمک به توسعه ی 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 تکلیف هایی را بر عهده مان گذارده است. از آنجایی که جرایم رایانه ای هر روز بیشتر و با شیوه های متفاوتی رخ می دهند، باید ابتدا به فکر را ههای پیشگیری باشیم. با تصویب قوانین بازدارنده می توان از رخداد این جرایم جلوگیری کردواز آنجا که دولت الکترونیک در دستور کار قرار گرفته است، باید قوانین لازم را برای کاهش هرچه بیشتر این دسته مشکلات و جرم های رایانه ای، تصویب شود تا بتوانیم در بخش های گوناگون همچون، تجارت الکترونیک هم گام های خوبی برداشته شود. همچنین باید از اجرای کامل و صحیح این قوانین نیز اطمینان حاصل کرد. بدون شک، انجام کارهای مطالعاتی و تحقیقاتی در زمینه ی موضوعات مهم، حساس و مبتلا به جامعه یکی از ضروریات حوزه های دانشگاهی است. بنابراین پیشنهاد می شود تا بتوانیم با آگاهی از خطرهای بالقوه جرم های رایانه ای، راه پیشگیری و مقابله با آن ها را به دست

آوریم. با مطالعه ی قانون جرایم رایانه ای، متوجه می شویم تنها دو شکل از انواع ضمانت اجراها یا همان مجازات وجود دارد: جریمه ی نقدی و زندان گمان می رود تصویب قوانین سخت، اعمال دقیق و بدون رعایت مصالح شخصی قوانین و تنوع در ضمانت اجراهای به کار گرفته شده، شرایط مناسب تری را برای رشد و توسعه فناوری اطلاعات و ارتباطات فراهم آورد. دولت باید آسیب های بخش جرایم رایانانه ای و اینترنتی را در کشور کاهش داده و با آموزش جوانان در چگونگی استفاده از اینترنت و توضیح اخلاق مجازی که اشاره به یک سری از رفتارهای سالم و مسئولانه در جامعه افراد حاضر در اینترنت است، خطاهای کمتری را شاهد باشیم. با آموزش اخلاق مجازی به درک خطر رفتارهای مضر و غیرقانونی آنلاین و یادگیری این که چگونه از خودمان محافظت کنیم دست می یابیم.

راهکارها

۱- با توجه به این که جرایم رایانه ای از جمله جرایم فراملی محسوب می شود و یک سند خاص بین المللی الزام آور در این زمینه برای کشورها وجود ندارد لذا در راستای همکاری و حمایت بیشتر از بزه دیدگان جرایم سایبری مبتنی بر حمایت از بزه دیدگان توسط قوه مقننه تصویب گردد.

۲-در حقوق داخلی چون مقررات کیفری جامع و مؤثری در حمایت از بزه دیدگان اطفال ونوجوانان سایبری در قانون جرایم رایانه ای و آیین دادرسی جرایم رایانه ای کشورمان پیش بینی نشده است و مقررات عام آیین دادرسی کیفری نیز به خوبی تأمین کننده حمایت لازم از این بزه دیدگان خاص نمی باشد، لازم است تا نسبت به اصلاح قوانین فعلی در حمایت از بزه دیدگان جرایم سایبری تهیه و تدوین گردد.

منابع و مآخذ

۵. نیک‌سیرت هشجین، جابر. ۱۳۸۹. «تهدیدات علیه کودکان در فضای سایبر و رهنمودهای مقابله با آنها». ماهنامه وب. ۱۰ (۱۱۸). ۲۰ ـ ۲۵.

۶. حسنوی، رضاو فرسایی، داریوش (۱۳۷۹). فرهنگ تشریحی کامپیوتر ماکروسافت ۲۰۰۰، تهران: انتشارات دانشیار.

۷. صدری، سید محمدرضا و کروبی، محمد تقی (۱۳۸۴). ابعاد حقوقی محیط سایبر در پرتو توسعه ملی، تهران: نشر بقعه.

۸ شریفی هولاسو، اسماعیل (۱۳۸۷). جامعه شناسی، پایان نامهٔ کارشناسی ارشد، دانشگاه تربیت مدرس.

۹. ابراهیم پور کومله، سمیرا (۱۳۹۱). آسیب های نوپدید شبکه های اجتماعی مجازی در کمین خانوادهٔ ایرانی، نخستین کنگرهٔ فضای مجازی و آسیب های اجتماعی نوپدید.

۱۰. جلالی فراهانی، امیرحسین (۱۳۸۹). کنوانسیون جرایم سایبر وپروتکل الحاقی آن، چاپ اول.

۱۱. راجی، سیدم، (۱۳۸۵)نگاهی به قانون تجارت الکترونیک، نشریه حقوقی گواه، شماره ۶و ۷.

۱۲. رضا پرویزی، بررسی ابعاد حقوقی فناوری اطلاعات، مرکز مطالعات راهبردی و توسعه قضایی، خرداد ۸۳، ص ۲۳.

۱۳. کامران شیرزاد، جرایم رایانه ای از دیدگاه حقوق جزای ایران و حقوق بین الملل، ص ۴.

۱۴. خبرنامه انفورماتیک، ش ۵۳، دبیرخانه شورای عالی انفورماتیک، ص ۲۷ و ۲۸.

۱۵. واکاوی انواع جرایم سایبری، حصون، شماره ۲۶، مهر و آبان ۱۳۸۹.

۱۶. رسول افضلی، محمد باقر قالیباف و میثم احمدی فیروزجایی(۱۳۹۲)، " تبیین تحولات مفهوم مرز در فضای سیاسی مجازی"، پژوهش های جغرافیای انسانی، دوره۴۵، شماره۱، ص ۲۳۵.

۱۷. خسرو شاهی، قدرت اله و پور قهرمانی، بابک (۱۳۹۰) پیشگیری اجتماعی از وقوع جرائم کودکان در پروتکل الحاقی به کنوانسیون حقوق کودک(درباره خرید و فروش، روسپیگری و هرزه نگاری کودکان). فصلنامه علمی ترویجی مطالعات پیشگیری از جرم، سال ششم، شماره ۱۸.

۱۸. نعمتی، زهرا (۱۳۸۹) هرزه نگاری با نگاهی به قانون نحوه ی مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز می نمایند؛ دانشگاه تهران – دانشکده حقوق و علوم سیاسی پایان نامه کارشناسی ارشد.

۱۹. حدادزاده نیری، محمد رضا (۱۳۸۸) جرایم منافی عفت. مجله حقوقی دادگستری، سال ۷۳ شماره۶۷.

۲۰. م، رضای، ح، بابازاده مقدم (۱۳۹۳). "اصول تدوین قوانین و مقررات برای اینترنت با تأکید بر مصوبات یونسکو و شورای اروپا"، فصلنامه پژوهش حقوق عمومی، سال پانزدهم، شماره ۴.

۲۱. گ، افتخارجهرمی، ا، اسلامی (۱۳۹۳). "نحوه اعمال صلاحیت دادگا ها در رسیدگی به جرایم فضای مجازی"، مجله حقوقی دادگستری، سال ۷۸، شماره ۸۸.

۲۲. ز، فرهادی آلاشتی، ع، ر، جوان جعفری بجنوردی (۱۳۹۶). " نقض آزادی جریان اطلاعات در فرآیند پیشگیری موقعیت مدار از جرائم سایبری"، پژوهش حقوق کیفری، سال پنجم، شماره ۱۸، ص ۱۰۰-۶۹.