دوفصلنامه علمی
مطالعات فقه و حقوق رسانه
دانشکده رفاه

دوره ۱، شماره ۲
پاییز و زمستان ۱۳۹۸
صص: ۳۱-۴۹

جرایم سایبری علیه خانواده‌های ایرانی از منظر اجتماعی و فرهنگی

محبوبه موسیوند[۱]
فائزه ساکی[۲]

چکیده

پژوهش حاضر با هدف مطالعه و بررسی جرایم سایبری علیه خانواده‌های ایرانی از منظر اجتماعی و فرهنگی و با روش توصیفی ـ تحلیلی انجام شده است. در این پژوهش ضمن ارائه تاریخچه‌ای در خصوص جرایم سایبری، ویژگی‌ها و تفاوت‌های این دسته از جرایم نسبت به دیگر جرم‌ها، انواع آنها، آمارها و قوانین موجود در این زمینه، جرایم سایبری را که خانواده‌های ایرانی را تهدید می‌کند با رویکرد اجتماعی و فرهنگی بررسی نماییم و با پُرتکرارترین جرایمی که در این بستر صورت می‌گیرد آشنا شویم، مقوله بزه‌دیدگی و بزهکاری در فضای سایبر، زمینه‌های ارتکاب جرایم سایبری، گروه‌های هدف و آسیب‌پذیر از این جرایم را با رویکرد اجتماعی و فرهنگی بررسی نماییم که نتایج پژوهش حاکی از آن است که با توجه به گسترش فضای مجازی، کاهش سن حضور و استفاده از آن، ضریب نفوذ اینترنت، فضای مجازی و شبکه‌های اجتماعی در میان اقشار مختلف جامعه، امکانات و مزایای فراوان فضای مجازی و جذابیت‌های ظاهری و محتوایی آن، امروزه شاهد رشد روزافزون جرایم سایبری در کشور هستیم ازاین‌رو می‌توانیم جرایم سایبری را هم مانند سایر مسائل و چالش‌های اجتماعی و فرهنگی به‌مثابه تهدیدی علیه خانواده‌های ایرانی قلمداد کنیم که نیازمند پیشگیری، کنترل و مقابله از طریق روش‌ها و ابزارهای هدفمند و کاربردی می‌باشد.

واژه‌های کلیدی

جرایم سایبری، جرم، خانواده، فضای سایبر، فضای مجازی.

۱ـ استادیار گروه مطالعات علوم اجتماعی و توسعه، پژوهشکده زنان، دانشگاه الزهرا، تهران، ایران
m.moosivand@alzahra.ac.ir

۲ـ دانشجوی کارشناسی ارشد مطالعات زنان، دانشگاه الزهرا، تهران، ایران
sakifaezeh7@gmail.com

مقدمه

تمایل و گرایش روزافزون افراد جامعه به استفاده از فناوری‌های پیشرفته مانند اینترنت و رایانه، فضا و بستری مناسبی را جهت ظهور و بروز جرایم سایبری ایجاد کرده است و ازآنجایی‌که این جرایم و آسیب‌ها در فضای سایبر به وقوع می‌پیوندد و مانند دیگر جرایم، ماهیتی ملموس و عینی ندارد، نهادهای مربوطه به‌ویژه پلیس را هم برای کشف جرم با چالش‌هایی مواجه کرده‌اند *(رجبی تاج امیر، ۱۴۰۱، ص.۱۸)*. به‌بیان‌دیگر، جرایم سایبری دارای ویژگی‌های منحصربه‌فردی هستند که آنها را از جرایم سنتی متمایز می‌سازد، ویژگی‌هایی از قبیل سرعت، غیرملموس بودن، فراملی بودن، حجم جرایم و ... که اکثراً جنبه فنی ـ تخصصی دارند و اما مسئله حائز اهمیت این است که صرفاً این عوامل را نمی‌توان دلیل گسترش جرایم سایبری و ایجاد محدودیت در جهت پیشگیری و مقابله با آنها قلمداد کرد. به‌عبارت‌دیگر، عوامل دیگری همچون ابعاد فرهنگی ـ اجتماعی (مانند نوع بزهکاران، پایگاه اجتماعی ـ اقتصادی، عدم آشنایی کاربران با خطرات و آسیب‌های فضای مجازی) در درک این مسئله که باید برای مقابله، پیشگیری یا کنترل این جرایم از چه ابزارها و روش‌هایی باید استفاده کرد تأثیر قابل توجهی دارد *(جوان جعفری، ۱۳۸۹، ص.۱۸۱)*. به‌عبارت‌دیگر، بررسی جرایم سایبری و زمینه‌های گسترش آن علاوه‌بر عوامل فنی نیازمند این است که این مسئله از نظر فرهنگی، جامعه‌شناختی و روان‌شناختی هم مورد واکاوی قرار گیرد و بزهکار و بزه‌دیده به‌عنوان عضوی از اعضای خانواده که یا مرتکب جرم سایبری شده‌اند و یا قربانی آن شده‌اند بررسی شوند و دلایل، انگیزه‌ها و زمینه‌های ارتکاب جرم یا قربانی شدن مانند سن، جنسیت، تحصیلات، وضعیت اقتصادی، پایگاه اجتماعی، میزان سواد رسانه، آشنایی با تهدیدها و فرصت‌های فضای سایبر، میزان دانش حقوقی مرتبط با فضای مجازی و جرایم سایبری و ... مورد توجه قرار گیرد تا درنهایت بتوان متناسب با مقتضیات فرهنگی ـ اجتماعی جامعه برای مقابله و پیشگیری از جرایم سایبری تدبیری اندیشید.

در این پژوهش با روشی توصیفی ـ تحلیلی قصد داریم به این مسائل بپردازیم که جرایم سایبری چگونه جرایمی هستند؟ تاریخچه این جرایم به چه صورتی است؟ جرایم

سایبری چه انواعی دارند؟ ویژگی‌های جرایم سایبری و تفاوت آنها با جرایم سنتی چیست؟ جایگاه جرایم سایبری و رایانه‌ای در قوانین ایران چیست؟ آمارهای مربوط به جرایم سایبری در ایران (مانند این آمارها که: کدام‌یک از جرایم سایبری در ایران بیشتر رواج دارد و چه اقشاری از جامعه را بیشتر تحت تأثیر خود قرار می‌دهد؟ مجرمان سایبری بیشتر در چه رده سنی قرار دارند؟ پیامدهای حضور کودکان در فضای سایبر چیست؟ میزان کشف جرم، رسیدگی موفقیت‌آمیز نهادهای مربوطه و به‌طور خاص پلیس فتا به چه نحوی است؟) بیانگر چه موضوعی است و درنهایت این مسئله که جرایم سایبری چگونه به‌مثابه یک تهدید علیه خانواده‌های ایرانی قلمداد می‌شود؟ چه نوع جرایمی بیشتر خانواده‌ها را تهدید می‌کند؟ علل بزهکاری مجرمان و بزه‌دیدگی قربانیان به‌عنوان عضوی از اعضای خانواده چیست و مجرم یا قربانی شدن آنها چه پیامدهایی برای نهاد خانواده دارد و راهکارهای پیشگیری، کنترل و مقابله این جرایم چیست؟ پیامدهای حضور کودکان در فضای سایبر چیست؟ چه نوع جرایم سایبری و به چه علت زنان و دختران را تهدید می‌کند؟ در خصوص جرایم سایبری پژوهش‌های متعددی با رویکرد فنی مهندسی، حقوقی و جرم‌شناختی و ... انجام شده است که در ادامه به برخی از این پژوهش‌ها می‌پردازیم.

بر اساس پژوهش انجام‌شده توسط رجبی تاج‌امیر (۱۴۰۱)، تحت عنوان «ضرورت اتخاذ سیاست جنایی هماهنگ بین‌المللی پلیس در مقابله با جرایم سایبری» امروزه مقابله با جرایم سایبری یکی از مهم ترین چالش‌های پلیس قلمداد می‌شود و با توجه به گستردگی فضای مجازی، خسارات ناشی از آن، کثرت بزه دیدگان، فراملی بودن، پیچیدگی کشف جرم و تعقیب مجرم و بسیاری خصوصیات دیگر، مقابله با این جرایم تنها از طریق سیاست جنایی هماهنگ بین‌المللی پلیس محقق خواهد شد *(رجبی تاج‌امیر، ۱۴۰۱، ص.۲)*.

بر اساس پژوهش انجام شده توسط بروجردی علوی و ایلالی (۱۳۹۷)، تحت عنوان «پیامدهای زیست مجازی ایرانیان» که با روش کیفی و از طریق مصاحبه با ۲۵ نفر از خبرگان و کاربران فعال فضای مجازی انجام شده است، یافته‌ها حاکی از آن است که پیامدهای منفی حضور ایرانیان در فضای سایبر عبارت‌اند از: آسیب‌های اجتماعی،

اختلالات روانی، بی‌سازمانی اجتماعی، تحول در سبک زیستن، بروز چالش‌های فرهنگی، بحران هویت، ایجاد روزمرگی، شکاف بین‌نسلی و ایجاد جرایم سایبری *(بروجردی علوی و ایلالی، ۱۳۹۷، ص.۱۰٦)*.

بر اساس پژوهش انجام‌شده توسط علیوردی‌نیا و انواری (۱۳۹٤)، تحت عنوان «جرایم سایبری در ایران، مصادیق جرایم سایبری و راهکارهای مقابله با آن»، به‌منظور کاهش آسیب‌های ناشی از جرایم اینترنتی و سایبری می‌توان به ارتقاء سواد رسانه آحاد جامعه در استفاده از فضای مجازی و شناخت تهدیدها و فرصت‌های آن در پیشگیری و مقابله با جرایم سایبری اشاره نمود *(علیوردی نیا و انواری، ۱۳۹٤، ص.۱)*.

بر اساس پژوهش انجام‌شده توسط جوان جعفری (۱۳۸۹)، تحت عنوان «جرایم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای)»، فناوری اطلاعات و ارتباطات (به‌ویژه فضای سایبر) کلیه ابعاد زندگی بشر اعم از بعد اجتماعی، اقتصادی، سیاسی، فرهنگی، حقوقی، کیفری و ... را تحت تأثیر قرار داده است به‌طوری‌که تفاوت جرایم سایبری با جرایم سنتی سبب شده است که رویکرد کیفری معمول، اصول و مبانی متعارف آن پاسخگوی مقابله با این جرایم نباشد و درنتیجه تبیین یک رویکرد کیفری متمایز الزام‌آور تلقی شود (جوان جعفری، ۱۳۸۹، ص.۱٦۹)؛ که درنهایت می‌توان وجه تمایز پژوهش پیش‌رو را با سایر پژوهش‌های این حوزه در رویکرد اتخاذ شده به مسئله پژوهش قلمداد کرد.

۱. تاریخچه

در بخش تاریخچه قصد داریم به‌ترتیب به تعریف واژه فضای سایبر، جرایم سایبری و تاریخچه جرایم سایبری بپردازیم.

تعریف فضای سایبر: نویسنده داستان‌های تخیلی و علمی، ویلیام گیبسون، در سال ۱۹۸۱ واژه فضای سایبر را با هدف توصیف یک جهان نوین که مجازی بود، به‌کار برد *(کلاهی و مباشری، ۱۳۸٦، ص.۳۳)*.

تعریف جرایم سایبری: درخصوص جرایم سایبری تعاریف متعددی وجود دارد؛ برای‌مثال سازمان همکاری و توسعه اقتصادی اذعان می‌دارد که هر گونه عمل

غیرقانونی، غیرمجاز و غیراخلاقی نسبت به انتقال داده و پردازش خودکار، جرم سایبری تعریف می‌شود *(رجبی تاج امیر به نقل از زیبر، ۱۴۰۱، ص.۵)*، علاوه‌براین، کنوانسیون جرایم سایبری شورای اروپا، جرایم سایبری را به چهار گروه جرایم علیه تمامیت، محرمانگی و دسترسی‌پذیری سیستم‌ها و اطلاعات رایانه‌ای، جرایم مربوط به محتوا، جرایم مربوط به رایانه، جرایم مربوط به حق نشر و حقوق مربوطه تقسیم می‌کند *(رجبی تاج امیر، ۱۴۰۱، ص.۵-۶)*.

تاریخچه جرایم سایبری: نسل اول جرایم سایبری: از دهه ۶۰ میلادی تا اواخر دهه ۸۰، نسل اول جرایم سایبری پدیدار گشت که در این برهه زمانی، مجرمان از رایانه‌های کاربران به‌عنوان ابزاری جهت ارتکاب جرایم سنتی مانند سوءاستفاده و کلاهبرداری‌های مالی استفاده می‌کردند *(رجبی تاج امیر به نقل از جلالی فراهانی، ۱۴۰۱، ص.۵)*؛ نسل دوم جرایم سایبری: این دسته از جرایم از دهه ۸۰ میلادی آغاز و تا اواخر دهه ۹۰ ادامه پیدا کرد که در واقع به عنوان یک پل ارتباطی میان جرایم نوع اول و نوع سوم عمل می‌کرد *(رجبی تاج امیر به نقل از جلالی فراهانی، ۱۴۰۱، ص.۵)* و تمرکز اصلی آن بر نفوذ به داده‌ها و محتویات رایانه‌ها بود *(رجبی تاج امیر، ۱۴۰۱، ص.۵)*؛ نسل سوم جرایم سایبری: این نسل از جرایم سایبری در اواسط دهه ۹۰ میلادی شروع شد و تحت عنوان جرایم مجازی، جرایم محیط سایبری و جرایم سایبری شناخته می‌شود و ارتکاب جرم در آن بدون وجود اینترنت امکان‌پذیر نمی‌باشد *(رجبی تاج امیر به نقل از برایانت‌ها، ۱۴۰۱، ص.۵)*.

۲. انواع جرایم سایبری

انواع و مصادیق جرایم سایبری عبارت‌اند از: هرزه‌نگاری سایبری، فروش محصولات غیرقانونی، قماربازی برخط، جرایم مرتبط با مالکیت معنوی، جعل سند، افترا و نشر اکاذیب، نژادپرستی، جرایم علیه مذهب، سرقت اطلاعات، فیشینگ، سایبر تروریسم، هک کردن، دستکاری داده‌ها و ... *(علیوردی‌نیا و انواری، ۱۳۹۴، ص.۸-۱۱)* که کشورهای مختلف متناسب با مبانی فکری، فرهنگی، اخلاقی، دینی و ... خود اقدام به جرم‌انگاری در حوزه فضای سایبر می‌نمایند.

۳. ویژگی‌های جرایم سایبری

جرایم سایبری در مقایسه با جرایم سنتی از ویژگی‌های خاص و منحصربه‌فردی برخوردار هستند که عبارت‌اند از: ۱. سرعت: امکان انجام جرایم متعدد در سریع‌ترین زمان ممکن بدون حضور در محل ارتکاب جرم؛ ۲. ناشناختگی: ناشناخته بودن مجرمان به دلیل پیچیدگی و پُرهزینه بودن شناسایی مجرمان؛ ۳. حجم جرایم: امکان ارتکاب یک جرم و قربانی شدن هزاران نفر؛ ٤. ارزان بودن بزه: وسایل مورد نیاز برای ارتکاب جرم سایبری (اینترنت، رایانه و امثال آن) کم‌هزینه است، ازاین‌رو تعداد جرایم افزایش می‌یابد و به‌تبع آن، مقابله با آنها هم پیچیده‌تر می‌شود؛ ٥. عدم الزام مبنی بر حضور فیزیکی در صحنه جرم: در جرایم سنتی عمدتاً حضور فیزیکی مجرم در محل ارتکاب جرم و پنهان کردن آثار و ابزار جرم لازم است، اما جرایم سایبری این‌گونه نیست؛ ٦. فراملی بودن: جرایم سایبری در بستری خارج از مرزهای متعارف بین‌المللی اتفاق می‌افتد و مجرمان بدون اینکه نیازی به عبور کردن از مرزهای ملی و بین‌المللی داشته باشند، در هر نقطه‌ای از جهان که باشند می‌توانند اقدام به ارتکاب جرم نمایند که این مسئله ابزارها و روش‌های پیشگیری، کنترل، مقابله، نظارت، کشف جرم و شناسایی مجرم را پیچیده می‌کند؛ ۷. بالا بودن آمار سیاه: به‌دلیل پیچیده بودن کشف جرایم و مجرمان سایبری نسبت به جرایم سنتی و عدم تمایل سازمان‌ها و مؤسسات مربوطه در خصوص افشای این جرایم (به‌دلیل اینکه با انجام این کار فضای کسب خود را ناامن معرفی می‌کنند) شاهد آمار سیاه در این حوزه هستیم؛ ۸. خودکار بودن جرم: امکان هک و سرقت اطلاعات از طریق کلیک بر روی یک نشانی آلوده یا نصب یک برنامه کاربردی؛ ۹. درونی بودن جرم: در جرایم سنتی این امکان وجود دارد که جرایم از طریق افرادی که به موضوع جرم دسترسی دارند و مورد اعتماد سایرین هستند، رخ دهد، در جرایم سایبری هم مشاوران، شرکا، همکاران و ... عاملان اصلی بزه هستند و تمییز دادن آنها از افراد خارجی به سهولت امکان‌پذیر نیست؛ ۱۰. ضعف یا فقدان کنترل اجتماعی: غالباً منشأ قواعد جرایم سنتی، مبانی فرهنگی و اخلاقی جامعه است و ارتکاب این جرایم علاوه بر نقض قوانین کشورها، نوعی تعرض به هنجارها، ارزش‌ها و مبانی اخلاقی جامعه تلقی

می‌شود، افزون‌براین، این هنجارها دارای کارکرد خودکنترلی هستند و افراد از قضاوت مردم و ننگ حاصل از دستگیری نگران می‌شوند، اما جرایم سایبری وضعیت متفاوتی دارند زیرا برخی از رفتارها و اقدامات صورت‌گرفته در فضای مجازی هنوز جرم‌انگاری نشده‌اند و یا سابقه‌ای در جامعه ندارند، ازاین‌رو افکار و احساسات عمومی را برنمی‌انگیزند و درنتیجه فاقد کارکرد خودکنترلی هستند؛ ۱۱. غیرملموس بودن؛ ۱۲. بالابودن هزینه کشف، جرم، دستگیری، مجازات مجرم *(جوان جعفری، ۱۳۸۹، ص.۱۷۶-۱۸۳)*.

۴. جرایم سایبری و رایانه‌ای در قوانین

در این بخش از پژوهش به تعریف واژه جرم و عناوین و سرفصل‌های جرایم رایانه‌ای تعریف شده در قانون مجازات اسلامی ایران خواهیم پرداخت. بر اساس ماده ۲ قانون مجازات اسلامی مصوب سال ۱۳۹۲ «جرم عبارت است از هر رفتاری اعم از فعل یا ترک فعل که در قانون برای آن مجازات تعیین شده است» *(قانون مجازات اسلامی مصوب ۱۳۹۲)*. در قانون مجازات اسلامی مصوب سال ۱۳۹۲، بخشی از مجازات‌ها به مقوله جرایم رایانه‌ای اختصاص یافته است که بدین‌شرح می‌باشد: «فصل ۱: جرایم علیه محرمانگی داده‌ها و سیستم‌های رایانه‌ای و مخابراتی متشکل از دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای؛ فصل ۲: جرایم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی متشکل از جعل رایانه‌ای، تخریب و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی؛ فصل ۳: سرقت و کلاهبرداری مرتبط با رایانه؛ فصل ٤: جرایم علیه عفت و اخلاق عمومی؛ فصل ٥: هتک حیثیت و نشر اکاذیب؛ فصل ٦: مسئولیت کیفری اشخاص؛ فصل ۷: سایر جرایم؛ فصل ۸: تشدید مجازات‌ها» *(قانون مجازات اسلامی مصوب ۱۳۹۲)*؛ لازم به ذکر است که جرایم رایانه‌ای، سایبری و اینترنتی در سطح بین‌المللی هم جرم‌انگاری شده‌اند که در همین راستا می‌توان به طبقه‌بندی سازمان توسعه و همکاری اقتصادی، کمیته وزرای شورای اروپا و کنوانسیون جرایم سایبر اشاره کرد *(علیوردی‌نیا و انواری، ۱۳۹٤، ص.٦-۷)*.

۵. آمارهای مربوط به جرایم سایبری در ایران

با اهمیت و مسئله اجتماعی تلقی کردن مقوله‌ای تحت عنوان جرایم سایبری، اذعان به ارزش پژوهش و بررسی داشتن آن، اعتقاد به تأثیر آن بر خانواده نیازمند ارائه آمارهای رسمی از منابع معتبر می‌باشد به‌عبارت‌دیگر، اگر ما قائل بر تهدید شدن خانواده‌های ایرانی از جانب فضای سایبری باشیم، می‌بایست (فارغ از آمارهای سیاهی که می‌تواند در این‌باره وجود داشته باشد) آمارهای رسمی که افراد و منابع معتبر ارائه می‌کنند را ذکر نمائیم، زیرا عدم پرداختن به این مسئله می‌تواند این ذهنیت را در افراد به‌وجود آورد که جرایم سایبری، خانواده‌های ایرانی را تهدید نمی‌کند، این مسئله صرفاً یک تصور انتزاعی است، تحقیق و پژوهش در این زمینه از جایگاه خاصی برخوردار نیست و اساساً پرداختن به این پدیده موضوعیتی ندارد، به‌همین‌منظور در این پژوهش قصد داریم که به بخشی از آمارهایی که در این‌باره وجود دارد و نوعی همه‌جانبه‌نگری در آنها رعایت شده است بپردازیم، بدین‌صورت که در این پژوهش از آمارهای جدید و به‌روز مربوط به ۲-۱ سال اخیر که در مورد مباحثی همچون: بیشترین جرایم سایبری و اینترنتی در ایران؛ گروه‌های هدف مجرمان سایبری و اقشار آسیب‌پذیر در این حوزه؛ پیامدهای حضور کودکان در فضای سایبر؛ بیشترین فراوانی زمانی برای جرایم سایبری؛ پُرتکرارترین جرم سایبری در سال‌های اخیر؛ بازه سنی مجرمان سایبری؛ استان‌های دارای بیشترین و کمترین جرایم اینترنتی، میزان کشف جرم، رسیدگی و موفقیت نهادهای مربوطه و به‌طور خاص پلیس فتا می‌باشد، استفاده شده است.

بر اساس خبر منتشر شده در ۹ تیر ۱۴۰۰ در پایگاه اطلاع‌رسانی پلیس فتا تحت عنوان «افزایش ۱۷ درصدی کشف جرایم سایبری در خردادماه ۱۴۰۰؛ سرهنگ محمدعلی فرهودی رئیس پلیس فتا استان قزوین اذعان داشتند که: کلاهبرداری اینترنتی، هتک حیثیت، نشر اکاذیب و مزاحمت‌های اینترنتی به ترتیب بیشترین جرایم سایبری استان قزوین در خرداد ماه سال ۱۴۰۰ هستند».

بر اساس مصاحبه سرهنگ داوود معظمی گودرزی، رئیس پلیس فتای تهران بزرگ در تاریخ ۱۰ اسفند ۱۴۰۰ تحت عنوان «بیشترین جرایم سایبری در تهران چیست؟» با

خبرگزاری ایسنا: «مجرمان سایبری تلاش می‌کنند تا هربار و به بهانه‌های گوناگون از افراد جامعه کلاهبرداری کنند و طعمه‌های خود را از بین تمام اقشار و سنین مختلف انتخاب کنند، اما در بسیاری از پرونده‌ها مشخص شده است که کودکان و سالمندان یکی از گروه‌های هدف این مجرمان هستند و ازاین‌رو می‌توان گفت که کودکان و سالمندان دو قشر آسیب‌پذیر در مقابل مجرمان سایبری هستند؛ البته لازم به ذکر است که حدود ۹۰ درصد از پرونده‌ها و شکایات ثبت‌شده در پلیس فتا منجر به نتیجه شده و مورد رسیدگی قرار گرفته است».

بر اساس مصاحبه سرهنگ دوم علی محمد رجبی، رئیس مرکز تشخیص و پیشگیری از جرایم سایبری پلیس فتا در تاریخ ١٤ دی ١٤٠٠ تحت عنوان «زنگ خطر کاهش سن کودکان سایبری» با خبرگزاری ایرنا: با توجه به رشد و توسعه سریع فناوری شاهد بلوغ ذهنی کودکان در حوزه دیجیتال و فضای سایبر هستیم به‌گونه‌ای‌که کودکان به آسانی در فضای سایبر و شبکه‌های اجتماعی فعالیت می‌کنند و با مشکلات مختلفی مواجه می‌شوند که در صورت بی‌اطلاعی خانواده‌ها از این مسئله، شاهد بروز ناهنجاری‌های فراوان در کودکان خواهیم بود، علاوه‌براین، کودکان پیش از ورود به مدرسه با فضای سایبر آشنا می‌شوند و حتی بعد از ورود به مدرسه هم بیشترین زمانی که برخط هستند در منزل است ازاین‌رو خانواده‌ها نقش اساسی در تربیت و پرورش کودکان دارند».

بر اساس مصاحبه سردار وحید مجید رئیس پلیس فتا فرماندهی کل انتظامی در تاریخ ٢٤ آبان ١٤٠١ با خبرگزاری مهر: «٣٧ درصد از جرایم فضای سایبر مربوط به کلاهبرداری‌های اینترنتی است؛ بیشترین فعالیت کلاهبرداران اینترنتی مربوط به حوزه سایبر الکترونیک (مانند ارسال پیوندهای آلوده از طریق پیامک و پیام‌رسان‌ها) می‌شود؛ اغلب پیوندهای آلوده در روزهای پنجشنبه و جمعه برای افراد ارسال می‌شود و این دو روز بیشترین فراوانی زمانی برای جرایم سایبری را دارند؛ کلاهبرداری اینترنتی پُرتکرارترین جرم سایبری در سال ١٤٠١ بوده است؛ بیش از ٨٠ درصد مجرمان سایبری در بازه سنی بین ١٨ تا ٣٠ سال قرار دارند؛ سن مجرمان سایبری نسبت به دیگر مجرمان پایین‌تر است؛ البته در برخی از شاخه‌های کلاهبرداری و قمار سن

مجرمان بالاتر است اما درمجموع سن مجرمان سایبری نسبت به خودشان در سال‌های گذشته تغییری نداشته است».

بر اساس مصاحبه سردار وحید مجید رئیس پلیس فتا فرماندهی کل انتظامی در تاریخ ۱۸ اسفند ۱٤۰۰ تحت عنوان «استان‌های دارای بیشترین جرایم اینترنتی» با خبرگزاری ایسنا: «تهران بزرگ با ۱۱ درصد در رتبه نخست جرایم سایبری کشور قرار دارد و پس از آن خراسان رضوی با ۹ درصد، اصفهان با ۸ درصد، شیراز با ٦ درصد و خوزستان با ٤ درصد در رتبه‌های بعدی قرار دارند و کیش، سیستان و بلوچستان، خراسان شمالی، کهگیلویه و بویراحمد و لرستان دارای کمترین جرایم سایبری بوده‌اند».

بر اساس مصاحبه رئیس پلیس فتای فراجا در تاریخ ۲۰ آذر ۱٤۰۱ با خبرگزاری ایسنا: «کلاهبرداری اینترنتی، برداشت غیرمجاز اینترنتی، هتک حیثیت، نشر اکاذیب، دسترسی غیرمجاز به داده و مزاحمت اینترنتی بیشترین جرایم صورت گرفته در فضای سایبر بوده‌اند، اما به‌طور کلی کلاهبرداری‌های اینترنتی در صدر جرایم اینترنتی قرار دارند؛ لازم به ذکر است که قدرت کشف پلیس فتا در سال ۱٤۰۱ افزایش داشته است و ضریب کشف و به وقوع پلیس فتا در حدود ۹٤ درصد می‌باشد».

۶. جرایم سایبری علیه خانواده

در این بخش از پژوهش قصد داریم که با استناد به آمارهای ارائه شده که پیشتر ذکر شد جرایم سایبری و تأثیر آنها بر نهاد خانواده را از منظر اجتماعی و فرهنگی مورد واکاوی قرار دهیم، به‌بیان‌دیگر، در آمارهای ارائه شده جزئیاتی درخصوص بیشترین جرایم سایبری و اینترنتی در ایران (کلاهبرداری‌های اینترنتی، برداشت‌های غیرمجاز اینترنتی، هتک حیثیت، نشر اکاذیب، دسترسی غیرمجاز به اطلاعات و مزاحمت اینترنتی بیشترین جرایم انجام شده در فضای مجازی هستند)، گروه‌های هدف مجرمان سایبری و اقشار آسیب‌پذیر در این حوزه، پیامدهای حضور کودکان در فضای سایبر، بیشترین فراوانی زمانی برای جرایم سایبری، پُرتکرارترین جرم سایبری در سال‌های اخیر، بازه سنی مجرمان سایبری، استان‌های دارای بیشترین و کمترین جرایم اینترنتی، میزان کشف

جرم، رسیدگی و موفقیت نهادهای مربوطه و به‌طور خاص پلیس فتا مطرح شده است که فارغ از ویژگی‌های فنی که فضای مجازی برای ایجاد جرم بسترسازی می‌کند، شخص مجرم یا قربانی به عنوان فردی که بخشی از جامعه را تشکیل می‌دهد و عضو یک خانواده است، عملکرداش در مجرم شدن یا قربانی شدن، نوع جرمی که مرتکب شده‌اند، تکرار جرم یا بزه‌دیدگی، انگیزه‌های ارتکاب جرم و دلایل و قصور در بزه‌دیدگی، آثار و پیامدهای بزهکاری سایبری و بزه‌دیدگی سایبری برای خود و خانواده‌اش، ویژگی‌های زمینه‌ای یا جمعیت‌شناختی و ... از منظر فرهنگی و اجتماعی بسیار حائز اهمیت است، زیرا اگر ما قائل به اهمیت و ترویج دانش فضای مجازی و سواد رسانه باشیم می‌بایست بخشی از این اهداف (ارتقا سواد رسانه آحاد جامعه) را در بستر فرهنگی ـ اجتماعی جامعه تحقق بخشیم و با رویکردی جامعه‌شناختی، روان‌شناختی و فرهنگی این قضیه را بررسی نماییم و زیرساخت‌های گوناگون جامعه را در جهت پیشگیری و مقابله با این جرایم مستحکم کنیم تا از افزایش تعداد مجرمان و قربانیان سایبری بکاهیم. درهمین‌راستا چند نکته در آمارهای مطرح شده جالب توجه بوده است که عبارت‌اند از: کلاهبرداری‌های اینترنتی پُرتکرارترین جرم سایبری در ایران؛ بازه سنی ۸۰ درصد از مجرمان سایبری ۱۸ تا ۳۰ سال است؛ مزاحمت‌های اینترنتی جزء پُرتکرارترین جرایم سایبری در ایران؛ وجود نگرانی نهادهایی همچون مرکز تشخیص و پیشگیری از جرایم سایبری پلیس فتا درخصوص پیامدهای حضور کودکان در فضای سایبر، که در ادامه به این تحلیل این نکات از منظر جامعه‌شناختی و فرهنگی و ارتباط آن با نهاد خانواده خواهیم پرداخت.

الف) کلاهبرداری‌های اینترنتی پُرتکرارترین جرم سایبری و بازه سنی ۸۰ درصد از مجرمان سایبری ۱۸ تا ۳۰ سال می‌باشد: چنین به نظر می‌رسد که اگر بخواهیم ارتباط میان این دو گزاره را با نهاد خانواده مورد واکاوی قرار دهیم می‌توانیم چنین استنباط کنیم که اکثر مجرمان را جوانان ۱۸-۳۰ تشکیل می‌دهند، جوانانی که در جهان حقیقی تحت تعلیم و پرورش والدین، معلمان و اساتید خود در نهاد خانواده، مدرسه و دانشگاه و در جهان مجازی هم تحت تأثیر پدیده‌ای نوظهور تحت عنوان فضای سایبر بوده‌اند،

بستری که ماهیتی سیال، فرازمانی، فرامکانی دارد و سرشار از اطلاعات و دسترسی‌های گوناگون است که این موضوع جذابیت‌های ظاهری و محتوایی آن را چندین برابر می‌کند و افراد مختلف به‌ویژه جوانان را برای استفاده یا بهره‌برداری سوء از آن مانند کلاهبرداری اینترنتی ترغیب می‌کند و در مقابل هم عده‌ای را به دلیل اعتماد کاذبشان به این بستر قربانی می‌کند که این معضل می‌تواند یکی از دلایلی باشد که پژوهشگران حوزه فضای مجازی را بر آن داشته که پیوسته به تهدیدها و آسیب‌های فضای سایبر اذعان کنند، بر مقوله سواد رسانه تأکید ورزند و خطر بروز جرایم سایبری را گوشزد کنند. به‌نظر می‌رسد که فقدان سواد رسانه به قدری آسیب‌زا است که می‌تواند تا حد جرم سایبری پیشروی کند و یک جوان ۱۸–۳۰ ساله را که به‌مثابه عضوی از اعضای خانواده است به‌دلیل عدم آگاهی از قوانین فضای مجازی و گاهاً عدم نظارت اعتدال‌گونه والدین‌اش از حضور و چگونگی فعالیت او در فضای سایبر تبدیل به یک مجرم کند که درنهایت طبق قوانین با او برخورد شود و در آینده هم در جامعه به‌عنوان فردی که دارای سابقه کیفری است، شناخته شود و به‌تبع آن، از برخورداری از یک‌سری فرصت‌ها همچون اشتغال در برخی مشاغل محروم شود و آسیب‌هایی همچون حس سرخوردگی، ناامیدی و افسردگی در او ایجاد شود و در سوی‌دیگر هم، یک شخص را به‌دلیل فقدان سواد رسانه و فضای مجازی‌اش تبدیل به یک قربانی که اطلاعات و منابع مالی‌اش سرقت‌شده، تبدیل کند اما علاوه‌بر مسئله‌ای که تحت عنوان سواد رسانه و دانش فضای مجازی ذکر شد، پرسش‌های دیگری که غالباً جنبه اجتماعی و فرهنگی دارد، به‌وجود می‌آید از جمله اینکه: چرا افراد به‌ویژه جوانان ۱۸–۳۰ سال به جای استفاده مفید و سودمند از این بستر به جرایم سایبری روی می‌آورند؛ چه جرایمی را بیشتر مرتکب می‌شوند؛ دلیل گرایش‌شان به جرایم سایبری همچون کلاهبرداری اینترنتی چیست؛ آیا صرفاً با هدف تحریک حس کنجکاوی خود اقدام به جرایم سایبری می‌کنند؛ آیا تصور می‌کنند که جرم سایبری‌شان در عالم حقیقی بدون مجازات باقی می‌ماند؛ آیا وضعیت اقتصادی خود را در تضاد با الگوهایی که رسانه‌های جمعی و در رأس آنها فضای مجازی ارائه می‌کند، می‌بینند و تصور می‌کنند که هر آنچه که در این رسانه‌ها تبلیغ

می‌شود ماهیتی حقیقی دارد و برای اینکه به سرعت به موفقیت‌های مالی و اقتصادی دست یابند باید از هر اقدام و وسیله‌ای که سبب تسریع دستیابی به این هدف می‌شود استفاده کنند؛ آیا این مجرمان نسبت به قوانین مرتبط با جرایم سایبری و رایانه‌ای آگاهی نداشته‌اند؟ آیا این بزهکاران صرفاً یکبار اقدام به چنین اعمالی کرده‌اند و از آن پند گرفته‌اند یا اینکه جرایم خود را مکررا انجام داده‌اند و از آن پندی نگرفته‌اند؟ نوع و تعداد جرایم و تعداد قربانیان به چه صورتی بوده است؟ ویژگی‌های جمعیت‌شناختی مجرمان همچون جنسیت، سن، وضعیت اقتصادی، سطح تحصیلات و ... چه بوده است؟ آیا به‌صورت انفرادی اقدام به این جرم کرده‌اند یا اینکه به صورت سازمان‌یافته و گروهی اقدام به ارتکاب جرم کرده‌اند؟ آیا خانواده‌های این مجرمان از نحوه فعالیت آنها در فضای سایبر اطلاع داشته است؟ آثار و پیامدهای دستگیری این مجرمان برای خود و خانواده شان چه بوده است؟ آیا قربانیان جرایم سایبری به‌ویژه کلاهبرداری‌های اینترنتی نسبت به ارتقا دانش مجازی خود و عدم اعتماد کامل به فضای مجازی تلاش کرده‌اند؟ ویژگی‌های جمعیت‌شناختی بزه‌دیدگان همچون جنسیت، سن، وضعیت اقتصادی، سطح تحصیلات و ... چه بوده است؟ آیا این قربانیان به تمامی پیام‌ها، پیوندهای ارسالی، برنامه‌های پیشنهادی و ... اعتماد کرده‌اند؟ آیا بزه‌دیدگان نسبت به هشدارهایی که مکرراً توسط نهادهای مربوطه همچون پلیس فتا اطلاع‌رسانی می‌شود توجه لازم را داشته‌اند؟ آیا بزه‌دیدگان جرایم سایبری صرفاً یکبار قربانی این جرایم شده‌اند یا اینکه به صورت پیوسته مورد سوءاستفاده قرار گرفته‌اند؟ آیا بزه‌دیدگان دلایل قربانی شدن خود را بررسی کرده‌اند و برای تغییر عملکرد خود تلاشی انجام داده‌اند؟ بستر وقوع جرم تا چه اندازه برای انجام جرایم سایبری مهیا بوده است؟ آیا نهادها و متولیان حوزه سایبر اقدامات و فعالیت‌های لازم را جهت ایمن‌سازی این بستر و استفاده کاربران و مسدودسازی سوءاستفاده مجرمان انجام داده‌اند؟ و ... که این پرسش‌ها متناسب با عناصر تشکیل‌دهنده جرم (متشکل از بزهکار، بزه‌دیده، موضوع جرم، بستر وقوع جرم) مطرح شده است و پاسخگویی به آنها تا اندازه‌ای چالش‌برانگیز است، اما درمجموع به‌نظر می‌رسد که گروه‌های آسیب‌پذیر از جرایم اینترنتی و سایبری به‌ویژه

کلاهبرداری‌های اینترنتی که در صدر جرایم سایبری کشور قرار دارد عبارت‌اند از: افرادی با هر رده سنی و سطح تحصیلی که به‌سرعت به پیام‌ها، پیوندهای ناشناس و برنامه‌های پیشنهادی، اعتماد می‌کنند، سالمندانی که آشنایی کامل با این فناوری و نحوه استفاده از آن ندارند؛ کودکان و نوجوانانی که تصور می‌کنند فضای مجازی را به‌طور کامل می‌شناسند و تحت سوءاستفاده قرار نمی‌گیرند درحالی‌که اطلاعات کاربری خود را به سهولت در اختیار تارنماها یا افراد مختلف برای خرید اینترنتی و ... قرار می‌دهند؛ البته لازم به‌ذکر است صرفاً ۸۰ درصد از مجرمان در بازه سنی ۱۸-۳۰ سال هستند و پُرتکرار بودن جرم سایبری کلاهبرداری‌های اینترنتی بدان‌معنا نیست که تمامی مجرمان این بازه سنی صرفاً جرایم مالی سایبری انجام می‌دهند و مرتکب سایر جرایم اینترنتی نمی‌شوند و یا اینکه به‌صورت ترکیبی چند جرم را مرتکب نمی‌شوند بلکه به این معناست که با توجه به اینکه ۳۷ درصد از جرایم سایبری را کلاهبرداری‌های اینترنتی تشکیل می‌دهند و ۸۰ درصد از مجرمان در بازه سنی ۱۸-۳۰ سال قرار دارند، تقارن این دو مسئله با یکدیگر جالب توجه است و نیازمند بررسی عمیق می‌باشد.

ب) مزاحمت‌های اینترنتی: گونه‌ای دیگر از جرایم سایبری وجود دارند که بعد از کلاهبرداری‌های اینترنتی، برداشت‌های غیرمجاز، هتک حیثیت، نشر اکاذیب، دسترسی غیرمجاز به داده‌ها جزء پُرتکرارترین جرایم سایبری در ایران به‌شمار می‌رود و تحت عنوان مزاحمت‌های اینترنتی تعریف می‌شوند؛ چنین به‌نظر می‌رسد که درخصوص این جرایم می‌توان گفت که این سطح از جرایم سایبری زنان و دختران را بیش از سایرین تهدید می‌کند که درهمین‌راستا این پرسش‌ها مطرح می‌شود که: انگیزه و هدف بزهکاران از انجام چنین اعمال غیراخلاقی چیست؟ آیا بزهکاران نسبت به عواقب حقوقی فعالیت‌های خود اطلاع دارند؟ آیا بزه‌دیدگان مراقبت‌های لازم را درخصوص فعالیت‌های خود در فضای سایبر انجام داده‌اند؟ آیا بزه‌دیدگان به توصیه‌های نهادها و متولیان فضای مجازی توجه کرده‌اند؟ آیا بزه‌دیدگان هر نوع اطلاعات متنی، ویدئویی، صوتی و تصویری خصوصی خود را که بعداً زمینه سوءاستفاده دیگران را فراهم می‌کند، در تلفن همراه خود نگهداری کرده‌اند یا اینکه آنها را به فضای امنی که در دسترس سایرین نیست

منتقل کرده‌اند؟ آیا قربانیان اقدام به ارسال اسناد ویدئویی، متنی، صوتی و تصویری خصوصی خود برای افراد ناشناس کرده اند؛ آیا قربانیان به دلیل اعتماد نسبی خود به برخی افراد در فضای مجازی، اقدام به ارسال اطلاعات ویدئویی، متنی، صوتی و تصویری خصوصی خود برای آنها کرده‌اند؟ آیا بزه‌دیدگان اقدام به انتشار عمومی اسناد ویدئویی، متنی، صوتی و تصویری خصوصی خود در فضای مجازی کرده‌اند؛ بزه‌دیدگان چه نوع اطلاعاتی را در فضای سایبر به اشتراک می‌گذارند؟ آیا بزه‌دیدگان هر نوع اطلاعاتی را در اختیار دیگران قرار می‌دادند بی‌آنکه به عواقب احتمالی آن بیاندیشند؟ آیا بزه‌دیدگان پس از اطلاع از سوءاستفاده دیگران از اطلاعات خود این مسئله را به نهادهای مربوطه اطلاع دادند یا اینکه نسبت به این موضوع آگاهی نداشتند و مجدداً مورد سوءاستفاده بزهکاران قرار گرفتند؟ آیا نهادهای مربوطه وظایف خود را در جهت ایمن‌سازی فضای مجازی و مقابله با مجرمانی که مرتکب جرایم سایبری غیراخلاقی شده‌اند، انجام داده‌اند؟ و ... که این پرسش‌ها و پرسش‌های بی‌شمار دیگری درخصوص مسئله مزاحمت‌های اینترنتی وجود دارد که نیازمند بررسی و تحلیل عمیق می‌باشد.

ج) پیامدهای حضور کودکان در فضای سایبر: چنین به‌نظر می‌رسد که کودکان به‌عنوان عضوی از خانواده و جامعه، تحت تأثیر حساسیت‌های اجتماعی خاصی هستند بدین‌صورت که اگر اتفاق ناگواری در قالب یک جرم برای کودکان رخ دهد افکار و احساسات عمومی جریحه‌دار می‌شود و همگان خواستار مجازات مجرمان می‌شوند، اما در مورد جرایم سایبری که علیه کودکان خانواده‌های ایرانی رخ می‌دهد چندین نکته حائز اهمیت است و عبارت است از اینکه: آیا با توجه به آماری که پیشتر تحت عنوان «زنگ خطر کاهش سن کودکان سایبری» ذکر شد و حاکی از ورود کودکان به فضای سایبر پیش از ورود به مدرسه بود، این نگرانی دو چندان نمی‌شود که کاهش سن حضور در فضای مجازی و ورود کودکان به این بستر (درحالی‌که فاقد دانش، تجربه و به‌طور خاص سواد رسانه هستند) ممکن است که این کودکان را به مجرمان سایبری آینده تبدیل کند، کودکانی که طبق تصور ذهنی عامه مردم جایگاهشان در مقوله جرایم سایبری نقش قربانی بوده است و نه مجرم؛ آیا درخصوص ویژگی ضعف در کنترل اجتماعی یا فقدان

کنترل اجتماعی جرایم سایبری نسبت به جرایم سنتی که قبلاً در مورد آن صحبت شد، این ویژگی در مورد جرایم سایبری هم که علیه کودکان اتفاق می‌افتد صدق می‌کند یا اینکه به نحو دیگری عمل می‌کند؛ چه نوع جرایمی معمولاً علیه کودکان در فضای سایبر رخ می‌دهد و علت و روش‌های مقابله با آن چیست؟ آیا والدین پیش از آنکه این ابزارهای نوین را در اختیار فرزندانشان قرار دهند، از دانش رسانه و فضای مجازی مطلع بوده‌اند که آن را به فرزندان خود منتقل کنند؟ خانواده‌ها تا چه اندازه نسبت به ورود، نحوه فعالیت و محتواهای رصد شده توسط کودکانشان آگاه و دغدغه‌مند هستند؟ خانواده‌ها ابزارهای نوین همچون تلفن همراه و اینترنت را در چه سنی در اختیار کودکان قرار می‌دهند و آیا برای دسترسی به مضامین و محتواهای مختلف این ابزارها محدودیت منطقی، هوشمندانه و اعتدال گونه‌ای تعریف می‌کنند؟ آیا خانواده‌های نسبت به عواقب سوء حضور کودکانشان در فضای مجازی همچون بلوغ زودرس، قربانی جرایم سایبری شدن و ... آگاه هستند؟ آیا نهادهای مربوطه در جهت کنترل فضای مجازی و محدودیت دسترسی کودکان به بعضی بخش‌های فضای مجازی اقدامات کاربردی و هوشمندانه‌ای انجام داده‌اند؟ آیا وقایعی همچون کووید-۱۹ که دلیل ورود کودکان به فضای مجازی و یا افزایش استفاده آنها از فضای مجازی بوده است، از ابعاد گوناگون مورد بررسی قرار گرفته است؟ و تعداد بی‌شماری دیگر پرسش چالش‌برانگیز که نوع نگاه اجتماعی ـ فرهنگی ما را نسبت به جرایم سایبری را شکل می‌دهد؛ اما درمجموع می‌توان گفت که با توجه به اینکه کودکان تجربه، دانش و آگاهی گسترده‌ای در مورد مسائل مختلف به‌ویژه جرایم سایبری ندارند، می‌بایست خانواده‌ها ابتدا دانش مجازی و رسانه خود را ارتقا دهد و سپس با رعایت یک‌سری پیش‌فرض‌ها (مانند اینکه سن مناسب جهت در اختیار قرار دادن ابزارهای نوین (برای کودکان) چیست؟ چه نوع مضامین و برنامه‌هایی را کودکان می‌توانند مشاهده کنند که بر روی آنها اثر سوء نداشته باشد؟ و ...) اقدام به مدیریت هوشمندانه حضور کودکان در فضای مجازی و انتقال دانش مجازی به آنها نمایند.

نتایج

چنین به‌نظر می‌رسد که با توجه به افزایش ضریب نفوذ اینترنت و فضای مجازی، ارائه امکانات بی‌شمار، به‌روزرسانی خدمات مختلف مانند پیام‌رسان‌ها و ... امروزه حضور در فضای سایبر امری اجتناب‌ناپذیر و حتی در مواردی اجباری شده است و به آسانی نمی‌توان قدرت و امکانات بی‌حدوحصر آن را نادیده انگاشت، اما مسئله‌ای که دغدغه بسیاری از پژوهشگران حوزه سایبر است این موضوع می‌باشد که در فضای مجازی علاوه بر خدمت، تهدید هم ارائه می‌شود. به‌بیان‌دیگر فضای سایبر فارغ از مزایای قابل توجهی که دارد، آسیب‌ها و تهدیدهای متعددی را هم به جوامع بشری تحمیل می‌کند که جرایم سایبری یکی از آنها می‌باشد، اما برای اینکه یک جرم در فضای سایبر رخ دهد پیش‌فرض‌هایی لازم است مانند اینکه: بزه‌دیده تا چه اندازه از خود، اطلاعات، منابع مالی اش و ... در برابر مجرمان سایبری محافظت کند؟ چه عوامل و زمینه‌های فردی، اجتماعی، خانوادگی و اقتصادی‌ای سبب شود که یک فرد به مجرم سایبری تبدیل شود؟ جنسیت، تحصیلات، سن و ... بزه‌دیده چگونه باشد که او را برای قربانی شدن مستعد سازد؟ زمینه و بستر اینترنت و فضای مجازی تا چه اندازه ناامن باشد که مجرمان را برای ارتکاب جرم ترغیب کند؟ رسیدگی به وضعیت قربانیان، حمایت از آنها، کشف جرم و مجازات مجرم تا چه اندازه محوری تلقی شود که مجرم را از ارتکاب جرم بازدارد یا اینکه او را تشویق کند؟ و پرسش‌هایی دیگر از این قبیل که در وقوع یک جرم سایبری تأثیرگذار است، اما با توجه به نوع جرایمی که مجرمان سایبری انجام می‌دهند و آمار تأمل‌برانگیزی که در حوزه جرایم سایبری وجود دارد می‌توان چنین نتیجه گرفت که فقدان سواد رسانه در اقشار مختلف جامعه با هر رده سنی و تحصیلی احساس می‌شود؛ زیرا پُرتکرارترین جرم سایبری کلاهبرداری اینترنتی معرفی شده است و افراد جامعه به دلیل اینکه آگاهی کافی از پیشگیری یا مقابله با این جرایم نداشته‌اند به پیوندهای آلوده و ناشناس و ... اعتماد کرده‌اند و به آسانی قربانی جرایم سایبری شده‌اند؛ افزون‌براین زنان و دختران هم گاهاً قربانی یکی دیگر از جرایم پُرتکرار سایبری تحت عنوان مزاحمت‌های اینترنتی شده‌اند که درخصوص این دو جرم (کلاهبرداری اینترنتی و مزاحمت‌های

اینترنتی) توصیه می‌شود که افراد علاوه‌بر توجه به هشدارهای نهادهای مربوطه به‌ویژه پلیس فتا و ارتقا سواد رسانه خود، ترجیحاً از اصل خود مراقبتی استفاده نمایند و اطلاعات متنی، ویدئویی، تصویری و صوتی خود را به‌سهولت در فضای مجازی منتشر نکنند، اطلاعات و حساب‌های کاربری خود را در اختیار دیگران قرار ندهد، به پیوندها و برنامه‌های ناشناس اعتماد نکنند و به‌طور کلی به‌گونه‌ای در فضای مجازی رفتار کنند که امکان ارتکاب جرایم سایبری علیه آنها کاهش یابد، اما درخصوص کودکان و جرایم سایبری که علیه آنها اتفاق می‌افتد بدیهی است که والدین نقش اساسی دارند، بدین‌صورت که با ارائه تلفن همراه هوشمند، اینترنت و ... به کودکان در هر رده سنی و عدم نظارت اعتدال‌گونه و منطقی بر فعالیت‌ها و محتواهای رصد شده توسط آنها زمینه وقوع جرم سایبری علیه آنها را فراهم می‌کنند که توصیه می‌شود در عملکرد خود بازنگری نمایند تا کودکان قربانی جرایم سایبری یا مجرمان سایبری آینده نشوند. درخصوص مجرمان سایبری هم به‌نظر می‌رسد که از نظر فرهنگی و اجتماعی زمینه‌های ارتکاب آنها به این جرایم مورد بررسی قرار گرفته شود تا از ارتکاب مجدد جرم توسط آنها پیشگیری به عمل آید و نتیجه و برآیند این فعالیت‌ها (بدون افشای هویت مجرمان) در قالب فیلم، ویدئو و ... منتشر شود.

منابع

بروجردی علوی، مهدخت و ایلالی، سیدحسن(۱۳۹۷)، پیامدهای زیست مجازی ایرانیان، *فصلنامه مطالعات رسانه‌های نوین*، سال چهارم، شماره ۱۶، صص۷۵-۱۱۰.

پایگاه اطلاع‌رسانی پلیس فتا(۱۴۰۰)، *افزایش ۱۷درصدی کشف جرایم سایبری در خردادماه ۱۴۰۰*.بازیابی شده ۱۴۰۰/۴/۹ https://cyberpolice.ir/news//1400-155459

جوادی، محسن(۱۳۸۶)، *پژوهشنامه اخلاق و فناوری اطلاعات*. تهران: پژوهشگاه فرهنگ، هنر و ارتباطات وزارت فرهنگ و ارشاد اسلامی.

جوان جعفری، عبدالرضا(۱۳۸۹). جرایم سایبر و رویکرد افتراقی حقوق کیفری (با نگاهی به قانون مجازات اسلامی بخش جرایم رایانه‌ای)، *مجلهٔ دانش و توسعه (علمی -*

پژوهشی)، سال هفدهم، شماره ۳٤. صص۱٦۹-۱۹۳.
خبرگزاری جمهوری اسلامی ایران «ایرنا»(۱٤۰۰)، *زنگ خطر کاهش سن کودکان سایبری*. بازیابی شده در ۱٤۰۰/۱۰/۱٤ از https://www.irna.ir/news//84601825
خبرگزاری دانشجویان ایران «ایسنا»(۱٤۰۰)، *اعلام استان‌های دارای بیشترین جرایم اینترنتی*. بازیابی شده ۱٤۰۰/۱۲/۱۸ از https://www.isna.ir/news//1400121814381
خبرگزاری دانشجویان ایران «ایسنا»(۱٤۰۱)، *اعلام بیشترین جرایم سایبری در سال جاری*. بازیابی شده در ۹/۲۰/ ۱٤۰۱ از https://www.isna.ir/news//1401091912541
خبرگزاری دانشجویان ایران «ایسنا»(۱٤۰۰)، *بیشترین جرایم سایبری در تهران چیست؟*. بازیابی شده در ۱٤۰۰/۱۲/۱۰ از https://www.isna.ir/news/۱٤۰۰۱۲۱۰۰۷۷۹۳
خبرگزاری مهر(۱٤۰۱)، *۸۰ درصد مجرمان سایبری ۱۸ تا ۳۰ ساله‌اند*. بازیابی شده در ۱٤۰۱/۸/۲٤ از https://www.mehrnews.com/news/5623893/%DB%B8%DB%B0
رجبی تاج‌امیر، ابراهیم(۱٤۰۱)، ضرورت اتخاذ سیاست جنایی هماهنگ بین‌المللی پلیس در مقابله با جرایم سایبری، *تحقیقات حقوقی بین‌المللی*، دوره ۱۵، شماره ۵۵، صص۱-۲۳.
علیوردی‌نیا، اکبر، انواری، آمنه(۱۳۹٤)، جرایم سایبری در ایران، مصادیق جرایم سایبری و راهکارهای مقابله با آن، کنفرانس بین‌المللی علوم انسانی، روان‌شناسی و علوم اجتماعی، صص ۱-۱٦.
موسوی، سیدرضا و موسوی، سیداکبر(۱۳۹۵)، *قانون مجازات اسلامی مصوب ۱۳۹۲*، تهران: هزار رنگ.