

## نگاهی حقوقی به پیدایش جرایم رایانه ای

امیرحسین صفدری<sup>۱</sup>، هانیه بابائی پور<sup>۲</sup>

<sup>۱</sup> دانش آموخته کارشناسی حقوق، دانشگاه شاندریز، مشهد (نویسنده مسئول)

<sup>۲</sup> دانش آموخته کارشناسی ارشد، فقه و مبانی حقوق اسلامی، دانشگاه آزاد، سبزوار

### چکیده

سایبر در لغت به معنی غیرواقعی و مجازی می باشد؛ و فعالیت های سایبری یا همان رایانه ای به زبان ساده یعنی: مجموعه ای از ارتباطات درونی انسان ها از طریق کامپیوتر و دستگاه های مخابراتی که بدون در نظر گرفتن جغرافیای فیزیکی آن انجام می شود. این روزها فعالیت های رایانه ای جزء اصلی و جدا نشدنی از زندگی افراد در جهان محسوب می شود، و بدیهی است که با پیشرفت روز افزون دانش فناوری اطلاعات و پا گذاشتن اینترنت به زندگی بشر از اینگونه فعالیت ها سوءاستفاده هایی هم بشود، که آسیب هایی را هم به دنبال داشته باشد. در جرایم سنتی و قدیمی جرم عموماً بر روی اشخاص، اموال، امنیت و... واقع می گردید، ولی در جرایم رایانه ای نوع آلت جرم به نوعی ماشین (کامپیوتر) تبدیل شده است. در ایران جرایم رایانه ای جرم انگاری شده است و قانونی تحت عنوان قانون جرایم رایانه ای در سال ۱۳۸۸ تصویب شده که امروزه نیاز به اصلاح آن شدیداً احساس می شود. بطور کلی جرایم سایبری را می توان به سه دسته تقسیم کرد، دسته اول: جرایمی است که رایانه و تجهیزات جانبی آن موضوع جرم واقع می شود مانند سرقت، تخریب و نظایر آن؛ دسته دوم: جرایمی است که در آن رایانه به عنوان ابزار و وسیله توسط مجرم برای ارتکاب به جرم از آن استفاده می شود؛ و دسته سوم: جرایمی است که می توان آن ها را جرایم محض رایانه ای نامید. در این مقاله علمی سعی شده است تا نگاهی هر چند مختصر به چگونگی پیدایش جرایم رایانه ای داشته باشیم و برخی از جرایم مهم در این حوزه را هم به شما معرفی کنیم تا نسبت به این جرایم آگاه شوید؛ روش تحقیق در این مقاله بر اساس تحقیقات کتابخانه ای و میدانی در جامعه می باشد.

**واژه های کلیدی:** جرایم رایانه ای، کامپیوتر، اینترنت، جامعه، حقوق

ژوبشگاه علوم انسانی و مطالعات فرهنگی  
پرتال جامع علوم انسانی

## ۱. مقدمه

فناوری اطلاعات و ارتباطات روز به روز در حال تکامل و پیشرفت است و تا لایه های پایین و جزئی جوامع بشری نفوذ پیدا کرده است. باید بگوییم که فضای مجازی زائیده فناوری اطلاعات و ارتباطات است، فضای که این روزها کاملاً انسان ها با آن انس گرفته اند و به آن علاقه مند شده اند؛ فضای مجازی که با دارا بودن قابلیت های منحصر به فردی چون دقت، سرعت، ذخیره سازی حجم بالای اطلاعات، خستگی ناپذیری، تبادل سریع اطلاعات، دسترسی آسان و محاسن بی شمار دیگر شده است تا ارتباطات نزدیک و نزدیکتر و به تبع آن، کارها سهل تر انجام بپذیرد. فضای مجازی با تمام قابلیت ها و پیچیدگی ها به شدت در مقابل این عوامل آسیب پذیر است؛ بر این اساس و با توجه به ویژگی های منحصر به فرد فضای مجازی، مجرمان و تبهکاران رغبت بیشتری در جهت استفاده از این فضا به ویژه از بستر شبکه های اجتماعی برای ارتکاب اعمال نابهنجار خود نشان میدهند که از این اعمال با عنوان "جرایم سایبری" یا همان (جرایم رایانه ای) یاد می شود. از سوی دیگر، جرم سایبری یا همان رایانه ای اغلب دارای بعد بین المللی است و ابعاد بین المللی این نوع جرایم موجب شده است تا افراد مختلف، از جمله: جرم شناسان، حقوقدانان، اساتید دانشگاه، پژوهشگران علم حقوق و پلیس به مطالعه و بررسی همه جانبه این پدیده ها روی آورند؛ به طوری که تدوین قوانین و اجرای مجازات با توجه به فراملی بودن ماهیت جرایم سایبری به مسئله ای پیچیده به ویژه در حقوق بین الملل تبدیل شده است؛ چرا که وقوع این نوع جرایم موجب تشدید خلأهای قانونی و قضایی حاکم در حقوق بین الملل همانند تشخیص صلاحیت دادگاه های کشورها نسبت به رسیدگی و نیز تعارض قوانین این کشورها در برخورد با جرایم سایبری شده است؛ بنابراین با توجه به خلأهای حقوقی و قضایی و حتی همکاری های انتظامی در سطح داخلی و بین المللی و به تبع آن سردرگمی و هزینه های کشف جرم نیز در مواجهه مقامات مسئول با این نوع جرایم بسیار مشهود می باشد. (صیح خیز، پورقهرمانی، صفاری ۱۳۹۹) رایانه خود بزرگ ترین فناوری عصر حاضر است و هم سایر فناوری های نوین یا به وسیله آن و یا بر بستر آن شکل می گیرند البته فناوری ها در کنار مزایای خود می توانند بسترساز سوءاستفاده هایی نیز باشند به خصوص اگر این فناوری رایانه باشد دامنه خطرهای آن هم افزایش می یابد. حقوق کیفری نوین، امروزه با جرایم و مجرمان رایانه ای طرف است که ماهیت و ویژگی این دسته از جرایم به نحوی اساسی با جرایم سنتی تفاوت دارد و امروزه، مجرمان رایانه ای در مکان هایی به غیر از نقاطی که آثار و نتایج اعمال آنها ظاهر می شود، قرار دارند. (جزایری، نعمت الهی، فارسانی؛ ۱۳۹۸) باتوجه به ویژگی اصلی جرایم سایبری یعنی امکان ارتکاب آن در فضای مجازی از هر نقطه مکانی و جنبه بین المللی آن، مقابله کارآمد با این جرایم نیازمند همکاری های کیفری بین المللی است. اگر چه فرامرزی بودن جرایم سایبری مانع بزرگی در تعقیب این جرایم است اما از آنجا که مجرمین سایبری همواره ردپایی از خود در محیط سایبری باقی می گذارند در موقعیت متزلزلی قرار دارند چرا که ادله جرایم آنان علی رغم فرامرزی بودن، از طریق همکاری بین المللی قابل دسترس هستند. حدود ۷۰ درصد همکاری های بین المللی در زمینه جرایم سایبری در چهارچوب معاهدات قضایی صورت میگیرد و به شدت نیاز است که این همکاری ها گسترده تر از قبل بشود. (نظامی نرج آبادی، ریسی؛ ۱۳۹۹)

## ۲- اصول و چارچوب نظری مقاله

## ۱-۲- پیشینه و تاریخچه جرائم رایانه ای

با پیدایش تکنولوژی کامپیوتری داده های عینی غیر ملموس دارای ارزش شده اند و اطلاعات موجود در رایانه نیز می تواند موضوع ارتکاب جرم قرار گیرد و به عبارتی دیگر در عین حال که رایانه دارای استفاده مثبت و فروانی است می تواند وسیله ای برای ارتکاب جرم توسط بزهکاران قرار گیرد. برای مثال ما شاهد تحقق این امر هستیم که به طور معمول نفوذکنندگان و هکرها، خود را جای کاربران معرفی می کنند و وارد سیستم می شوند و در مقابل حفاظت با اسم رمز وسیله ای برای حفاظت در برابر این دستیابی های غیر مجاز شناخته می شود. (دوکوهکی، ۱۳۹۶)

در هر حال برای بررسی تاریخچه جرائم رایانه ای از زمان پیدایش کامپیوتر تا اوایل هزاره سوم می توان به سه نسل اشاره کرد: **جرائم نسل اول:** اینگونه جرائم تا اواخر دهه ۸۰ مصداق دارد که بیشتر شامل سرقت و کپی برداری از برنامه ها و جرائم علیه حریم خصوصی در کامپیوتر بود که با گسترش تکنولوژی تبادل اطلاعات و ارتباطات بین المللی مورد بررسی قرار گرفت. **جرائم نسل دوم:** این جرایم بیشتر تحت عنوان جرائم علیه داده ها نمود پیدا کرده اند به طوری که این دهه تمامی جرائم علیه تکنولوژی اطلاعاتی، ارتباطاتی، کامپیوتری، ماهواره ای و شبکه های بین المللی تحت عنوان جرائم علیه داده ها اطلاق می شود. **جرائم نسل سوم:** تحقق جرائم سایبری یا رایانه ای محض بود. (باستانی، ۱۳۸۳)

از آنجایی که تعیین زمان اولین ارتکاب جرم کامپیوتری کار آسانی نیست و بطور دقیق هم نمی شود راجع به این مسله نظری داد ما به بیان چندین نظر که جز مهمترین نظر ها است در این موضوع می پردازیم؛ عده ای از محققان کامپیوتر را از زمان وجود چرتکه که ۳۵۰۰ سال قبل از میلاد در بعضی از کشورها بوده به نوعی بیان کرده اند. در سال ۱۸۰۱ با انگیزه مالی، «ژوزف ژاکارد» یکی از صاحبان کارخانه نساجی در فرانسه اولین کارت کامپیوتری را طراحی کرد، کارکنان ژاکارد با ترس و نگرانی از به مخاطره افتادن شغلی و زندگی خود درصدد برآمدند با اقدامات خرابکارانه مانع استفاده از این فناوری شوند و بدین ترتیب جرم رایانه ای مرتکب شدند. برخی از پژوهشگران هم قضیه «الدون رویس» آمریکایی در سال ۱۹۶۳ را اولین جرم رایانه ای می دانند؛ این شخص حسابدار یک شرکت آمریکایی بود و چون به زعم وی شرکت حقوق او را پایمال کرده بود با تهیه برنامه ای قسمتی از پول های شرکت را به خود اختصاص داد. (نامجویان، ۱۳۹۸) اما در خصوص تاریخ وقوع اولین جرم کامپیوتری در ایران نمی توانیم تاریخ وقوع آن را با سال ۱۳۴۱ که کامپیوتر وارد ایران شد همزمان بدانیم؛ زیرا در ابتدا استفاده از کامپیوتر بسیار محدود بوده است و در دهه ۵۰ و ۶۰ به تدریج تعداد کامپیوترها افزوده شده. (باستانی، ۱۳۸۳) اما به طور کلی تحقق اولین جرم رایانه ای در ایران را می توانیم تحت شرایطی درخردادماه ۱۳۷۸ بدانیم که در آن یک دانشجوی کامپیوتر و یه کارگر چاپخانه در کرمان چک های تضمینی را جعل می کردند. (نامجویان، ۱۳۹۸)

سرانجام کشور ایران هم نیز، همانند سایر کشورهای دنیا برای اتخاذ تدابیر امنیتی و مقابله با جرائم رایانه ای در کشور قانونی برای ارتکاب چنین جرائمی در حوزه کامپیوتر و فضای سایبری تدوین کرد که این قانون در سال ۱۳۸۸ به تصویب مجلس شورای اسلامی رسید. قانون جرایم رایانه ای در جلسه علنی روز سه شنبه مورخ ۱۳۸۸/۳/۵ توسط مجلس شورای اسلامی تصویب شد و در تاریخ ۱۳۸۸/۳/۲۰ به تایید شورای نگهبان رسید و در تاریخ ۱۳۸۸/۴/۳ جهت اجرا توسط رئیس جمهوری اسلامی ایران ابلاغ گردید. به طور کلی هم در قانون جرایم رایانه ای کشور ما که مصوب ۱۳۸۸ است عناوین مشخصی جرم انگاری شده است که شامل: ۱- جرائم علیه محرمانگی داده ها و سامانه های رایانه ای و مخابراتی که مربوط به دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه ای می شود. ۲- جرایم علیه صحت و تمامیت داده ها و سامانه های رایانه ای و مخابراتی که مربوط به جعل رایانه ای، تخریب و اخلال در سامانه های رایانه ای و مخابراتی می شود. ۳- سرقت و کلاهبرداری رایانه ای. ۴- جرائم علیه عفت و اخلاق عمومی در فضای رایانه ای. ۵- هتک حیثیت و نشر اکاذیب در فضای رایانه ای و... در قانون جرایم رایانه ای به آنها اشاره شده است که در حال حاضر این قانون نیازمند اصلاح می باشد.

## ۲-۲- تعریف جرایم رایانه ای (سایبری)

سایبر در لغت به معنی غیرواقعی و مجازی می باشد؛ و از نظر شکلی فضای سایبری پدیده ای است کل از جزء که میتواند ابعاد مختلفی را همانند اینترنت، مخابرات، رادیو، تلویزیون، موبایل و کلیه مواردی که از ویژگی های کلی یعنی شبکه، تهیه داده و انتقال داده برخوردار است را شامل گردد. در خصوص فضای سایبری و جرایم رایانه ای تعاریف زیادی مطرح شده است که برخی از این تعاریف شامل: ۱. (فضایی است در امتداد فضای فیزیکی که غیر قابل لمس بوده و توسط ابزار های رایانه ای و

الکترونیکی در جهت ارتباطات درونی انسان ها بر بستر تهیه، ساخت و انتقال داده های الکترونیکی ایجاد گردیده است). (حافظ نیا، ۱۳۹۱) ۲. ( هر عمل غیرقانونی، غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار یا انتقال داده ها) ( زیبر، ۱۳۹۰).  
 پروفیسور شیک حقوقدان برجسته اتریشی هم در تعریف جرم سایبری می گوید: ( جرایم رایانه ای عبارت است از هر گونه عمل مجرمانه ای که در آن رایانه، وسلیه یا هدف جرم باشد). ( شیرزاد، ۱۳۸۸). پس از این تعاریف بطور کلی و به زبان ساده به عنوان یک محقق و پژوهشگر علم حقوق پس از تحقیق و پژوهش در خصوص جرایم رایانه ای اگر بخواهم تعریف ساده ای از جرایم رایانه ای ارائه بدم باید بگویم که: جرایم سایبری یا همان جرایم رایانه ای جرایمی هستند که در فضای اینترنت و کامپیوتر با استفاده از ابزاری خاص انجام می شود که پیامدهای مختلفی به همراه دارد.

### ۳-۲- بررسی علل فرهنگی گرایش به جرائم رایانه ای

علل فرهنگی گرایش و تمایل افراد در جهان و ایران به جرائم اینترنتی می تواند زیر مجموعه وسیعی را به خود اختصاص دهد، اما آنچه را که بتوان به طور کلی از آن نام برد و در صدر این علل قرار بدهیم می توان به فقر فرهنگی در خصوص استفاده صحیح و سالم از فضای سایبری اشاره کرد. حال آن که از یک سو در محیطی که فقر فرهنگی حاکم است ابزار پرستی، ماده گرایی، روزمرگی، تکبر و طمع ورزی و سطحی نگری فکری در اجتماع آشکار است از سوی دیگر خود نگرش سطحی در جامعه باعث متأثر شدن از اندیشه های بی بنیان می شود که ممکن است این اندیشه ها در فضای مجازی مطرح شده و فرد را مغلوب خود سازد با این وجود از هم پاشیدگی هنجارها و عدم پایبندی به باورهای دینی خود از شاخص های دیگر فقر فرهنگی در جامعه ایران می باشد. بنابراین با وجود این علل، ارتکاب جرم در دنیای مجازی راحت تر و آسان تر شده و در برخی موارد بزهکاران با کمترین هزینه بیشترین خسارات و صدمات را به بار می آورند. به طور مثال ارتکاب جرائمی نظیر انتشار آثار مبتذل و مستهجن در فضای مجازی و یا تسهیل دسترسی افراد به محتوای مبتذل و مستهجن، توهین رایانه ای که همان توهین به افراد در فضای مجازی است نمونه ای از جرائم رایانه ای می باشد که به دلیل فقر فرهنگی در جامعه رخ میدهد. (دوکوهکی، ۱۳۹۶)

اگر چه فقر فرهنگی و مصادیق آن به عنوان یک علت کلی گرایش به جرائم اینترنتی مطرح می شود اما برای فهمیدن علل شخصی باید به بررسی انگیزه های افراد بپردازیم؛ که جدا از ضعف فرهنگی حاکم بر افراد جامعه و اجتماع، انگیزه های شخصی نیز در تحقق این جرائم نقش بسزایی دارد که شکل گیری این انگیزه ها خود برگرفته از همان سطحی نگری های فکری است. برای مثال در یکسری از جرائم رایانه ای انگیزه اصلی و شخصی فرد کسب منفعت مالی است ولی انگیزه هایی دیگری همچون: انتقام جویی، سرگرمی، خودنمایی، آزار و اذیت، آبروبری، اخاذی، سواستفاده های جنسی و... نیز در افراد دیده می شود.

بنابراین به طور کلی سه گروه از مجرمین در فضای سایبری را می توان اینگونه معرفی کرد: **گروه اول:** همان مزاحمان کامپیوتری هستند که با انگیزه دستیابی به سیستم های کامپیوتری و اطلاعات موجود در آن مرتکب جرم می شوند و اکثر آنها جوانانی هستند که برای تفریح و سرگرمی و ارضای حس برتری جویی خود دست به آن می زنند. **گروه دوم:** خلافکارهای حرفه ای هستند که با انگیزه کسب منفعت مالی و مادی معمولاً در مقوله جاسوسی، سرقت رایانه ای و کلاهبرداری های میلیونی در فضای سایبری فعالیت می کنند.

**گروه سوم:** سودجویانی هستند که تنها با انگیزه صدمه زدن و ایراد خسارت های مادی و غیرمادی به دیگران مرتکب جرم می شوند؛ این دسته بدون قصد منفعت و یا سرگرمی و تفریح مرتکب جرم می شوند این افراد معمولاً دارای اختلالات روحی و روانی بوده و یا با قصد انتقام جویی و لذت طلبی مرتکب جرم می شوند. (باستانی، ۱۳۸۳) برای مثال در جرایم مرتبط با محتوا در فضای مجازی که معمولاً حول محور امور مرتبط با جنسیت و هرزه نگاری می چرخد از جمله هرزه نگاری اطفال و بزرگسالان می باشد. (کاظمی سنجانی، ۱۳۹۶) بنابراین از یک سو شرایط حاکم بر جامعه از جمله وجود محیطی عاری از نظارت و کنترل و از سوی دیگر تضعیف باورهای دینی و اعتقادی و ارزش های فرهنگی و اجتماعی می تواند از عوامل مؤثر در

تحقق این دسته از جرائم اینترنتی باشد. بدون شک از بین بردن فقر فرهنگی که نقش بسزایی در شکل گیری انگیزه های اشخاص در ارتکاب به جرائم از جمله جرائم اینترنتی و سایبری دارد باید در اولویت فعالیت های فرهنگی اعضای جامعه و مسئولین جامعه قرار بگیرد.

#### ۴-۲- نگاهی به جرم هزینه نگاری یا پورنوگرافی در فضای مجازی

امروزه جرائم کامپیوتری و اینترنتی براساس ارزش ها و منافع نیز متنوع شده است؛ از جمله آن جرائم پورنوگرافی یا هزینه نگاری می باشد. این جرم یکی از مهمترین جرائم علیه اخلاق و عفت عمومی است. پورنوگرافی در مفهوم عامه به معنای مطالبی است که به قصد تحریک جنسی ارائه می شود و مصادیق آن می تواند در قالب نمایش، ارائه، تولید، تجارت و محتویات مستهجن و جنسی باشد. (قدسی. مجتهدسلیمانی، ۱۳۸۹). از آن جا که هر جرمی آسیب های اجتماعی و فردی را به همراه دارد این جرم نیز بر جامعه و خانواده ها آثار مخرب زیادی می گذارد. بزه دیدگان این نوع جرائم به طور معمول خانواده ها هستند که به دو بخش: ۱- کودکان و نوجوانان. ۲- بزرگسالان؛ تقسیم می شوند.

قابلیت دسترسی آسان و پایین بودن هزینه ارتکاب به این جرائم وقوع این دسته از جرائم را در جامعه تسهیل نموده است و این خود آثار مخربی بر جای می گذارد. یکی از آثار برجسته این دسته از جرائم رایانه ای بر خانواده ها متزلزل کردن روابط عاطفی و زناشویی بین زوجین جوان است؛ بر همین اساس بخشی از عوامل طلاق در کشورهایی که دچار فقر فرهنگی هستند از یک سو گسترش جرائم جنسی و منافی عفت است که گوشه ای از آن اعتیاد به فیلم ها و تصاویر مستهجن می باشد؛ و از سوی دیگر عده ای نیز برای کسب سودهای کثیف اقدام به تجارت جنسی می کنند. بنابراین باید گفت که با گسترش این دسته از جرائم و اعتیاد جنسی مجازی، زن و شوهرها از یکدیگر طلاق عاطفی میگیرند و همواره وقت خود را در فضای مجازی با افراد دیگر می گذرانند و این چنین بنیان خانواده ها متزلزل و سست می شود، و فرزندان در چنین خانواده هایی دچار انحرافات فرهنگی و اخلاقی شده و سلامت روح و روان آن ها به خطر می افتد. متأسفانه اعتیاد به دیدن فیلم های پورن باعث می شود که روابط جنسی سالم از بین برود و این عوامل به تدریج به نابودی خانواده ها و به تبع آن باعث نابودی جامعه سالم می شود. (رزمان، ۱۳۹۵) اما در کنار همه این مسائلی که بیان شد باید به این نکته مهم هم اشاره کنم که رایانه و اینترنت خود وسیله تعیین کننده و تاثیرگذار بر روی انحرافات اجتماعی نیستند، بلکه رایانه و اینترنت ابزاری است در دست انسان ها که تاثیرات این رسانه بر روی انحرافات اجتماعی مربوط به تغییراتی است که انسان ها خودشان بوسیله رایانه به جامعه عرضه می کنند. بنابراین باید بگویم که حفظ ارزش های اصلی یک جامعه اهمیت فراوانی دارد و نباید فراموش کرد که این رسانه می تواند با برنامه اصولی و کارشناسی شده از برخی از انحرافات اجتماعی بکاهد و جامعه ای ایده آل را برای مردم ترسیم کند.

#### ۵-۲- برخی از جرایم مهم و پر تکرار در فضای سایبر

بطور کلی در بین این همه جرمی که در فضای سایبری رخ می دهد چهار مورد از این جرایم در ایران امروزه پر تکرار و مهمتر نسبت به بقیه جرایم رایانه ای می باشد که این جرائم شامل:

۱. فیشینگ: جرمی که می توان رتبه نخست جرایم اینترنتی را به او اختصاص داد فیشینگ می باشد در جرم فیشینگ مجرمان به منظور فریب دادن کاربران اینترنتی و به دست آوردن اطلاعات محرمانه حسابشان اصولاً از طریق ایمیل های جعلی، پیامک های تبلیغاتی، سایت های خرید قلابی و... این کاربران را ترغیب می کنند تا اطلاعات شخصی حساب خود را در سایت های جعلی که توسط همین مجرمان طراحی شده است وارد کنند و از این طریق اطلاعات حساب افراد را به دست می آوردند و اقدام به کلاهبرداری های میلیونی می کنند، در این جرم مجرمان تلاش می کنند تا اطلاعاتی نظیر: رمز دوم کارت، شناسه کاربری، تاریخ انقضا کارت و... را بدست آورند. قانونگذار ما در خصوص مجازات افرادی که مرتکب جرم فیشینگ



می‌شوند به صراحت در ماده ۱۳ قانون جرائم رایانه‌ای می‌گوید: هرکس به طور غیرمجاز از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سیستم وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از ۱ تا ۵ سال یا جزای نقدی از بیست تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.

**۲. اسکیمر:** جرم اسکیمر را می‌توان تحت شرایطی یک نمونه از سرقت‌های اینترنتی نوظهور دانست، در جرم اسکیمر مجرم یک بخش جدیدی را به عابربانک یا دستگاه کارتخوان متصل می‌کند و از طریق این بخش متصل شده، این سودجویان اطلاعات کارت‌های بانکی مشتریان خود را کپی می‌کنند و بعد از آن با استفاده از کارت‌های عابربانک سفید این اطلاعات را رو آن کارت کپی کرده و حساب مشتریان خود را به این طریق خالی می‌کنند، به زبان ساده‌تر اسکیمینگ یعنی کپی غیرقانونی اطلاعات کارت بانکی شما بر روی یک کارت بانکی دیگر که از این طریق مجرم می‌تواند حساب بانکی شما را خالی کنند. قانونگذار ما در ماده ۱ قانون جرایم رایانه‌ای به صراحت بیان می‌کند: هرکس به طور غیرمجاز به داده‌ها یا سیستم‌های رایانه‌ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از ۹۱ روز تا ۱ سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد. قانونگذار ما در خصوص سرقت‌های اینترنتی هم به این سارقان حرفه‌ای مطابق با ماده ۱۲ قانون جرم رایانه‌ای می‌گوید: هرکس به طور غیرمجاز داده‌ای متعلق به دیگری را برآید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از یک تا بیست میلیون ریال و در غیر این صورت به حبس از ۹۱ روز تا ۱ سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.

**۳. شرط‌بندی‌های اینترنتی:** متأسفانه امروزه بحث شرط‌بندی‌های اینترنتی و یک شبه پولدار شدن در بستر فضای مجازی به شدت داغ شده و همین امر هم باعث شده جوانان زیادی وسوسه شوند و فریب این تبلیغات گسترده را بخورند و در آخر هم قربانی سایت‌های شرط‌بندی شوند. در خصوص شرط‌بندی‌های اینترنتی باید بگویم که مطابق با مواد ۷۰۵، ۷۰۶، ۷۰۷، ۷۰۸ قانون مجازات اسلامی بخش تعزیرات، در کشور ما هرگونه فعالیت اعم از شرکت، تبلیغ، طراحی، مدیریت، خرید و فروش سایت شرط‌بندی، نگهداری وسایل قمار و... چه در فضای حقیقی جامعه چه در فضای مجازی جرم می‌باشد و مجازات سنگینی هم دارد علاوه بر این مسائل از نظر فقهی هم قماربازی حرام می‌باشد. پس جوانان باید آگاه باشند و بدانند استفاده از سایت‌های شرط‌بندی تماماً ضرر و جرم می‌باشد و پشیمانی سودی ندارد.

**۴. دریافت جایزه:** یکی از قدیمی‌ترین جرایم اینترنتی و حقه‌های کلاهبرداران اینترنتی فریب افراد به بهانه برنده شدن آن‌ها در بانک یا قرعه‌کشی‌های مرکز خرید یا خریدهای اینترنتی و... می‌باشد، در این روش کلاهبرداران سایت‌های قرعه‌کشی جعلی درست کرده و با برنده اعلام کردن افراد اطلاعات حسابشان را بدست می‌آوردند و از این طریق حساب این افراد را خالی می‌کنند یا از آنها مبلغی پول دریافت می‌کنند تا جایزه آن‌ها را ارسال کنند که در مواجهه با این جور مسائل تحت هیچ شرایطی نباید به چنین افرادی اعتماد کرد. نکته مهمی که باید به آن دقت کنید این است که برای واریز هرگونه وجه به حساب شما اعم از جایزه، پاداش، برنده شدن در قرعه‌کشی‌ها و... هیچ نیازی به اعلام رمز دوم شما و یا اعلام تاریخ کارت بانکی شما نیست و در بعضی از موارد این سودجویان از شما می‌خواهند تا از کارت بانکی خود یک عکس برای آنها بفرستین تا پول را به حساب شما واریز کنند باید بدانید این کار باعث می‌شود شما قربانی کلاهبرداری یا سرقت اینترنتی شوید پس آگاه باشید و اطلاعات حساب‌های بانکی و اطلاعات کارت‌های عابربانک خود را در اختیار هیچ فردی قرار ندهید تا قربانی کلاهبرداری اینترنتی هم نشوید.

چند نکته مهم در خصوص پیشگیری از جرایم اینترنتی که شما را آگاه می کند که با رعایت این نکات از قربانی شدن در جرایم رایانه‌ای در امان میمانید: (۱) حتماً برای خریدهای اینترنتی از رمز یکبار مصرف (پویا) استفاده کنید و در بازه‌های زمانی کوتاه نسبت به تغییر رمز کارت بانکی خود اقدام کنید. (۲) مسدود کردن کارت‌های بانکی خود که امکان می‌دهد اطلاعاتشان فاش شده است. (۳) از سایت‌ها و اپلیکیشن‌های متفرقه که امنیت بالایی ندارند به هیچ عنوان استفاده نکنید. (۴) معتبرترین اپلیکیشن‌های موبایلی برای انجام پرداخت‌های اینترنتی اپلیکیشن‌هایی است که بانک صادرکننده کارت شما پیشنهاد می‌دهد و به نام بانک شما خدمات پرداخت آنلاین را انجام می‌دهد. (۵) سعی کنید از هر سایت یا پیج اینستاگرام یا گروه تلگرامی یا هر آگهی دیوار و... خرید اینترنتی انجام ندهید ابتدا از معتبر بودن آنها اطمینان حاصل کنید بعد خرید کنید. (۶) دقت کنید برای خرید اینترنتی اگر در هنگام ورود به سایتی ورود شما با اختلال مواجه شد یا احساس کردید روند خرید دچار ایراداتی است امکان دارد فیشینگ رخ داده باشد پس سریعاً رمز کارت بانکی خود را تغییر دهید و به پلیس فتا اطلاع دهید. (۷) وجود علامت قفل مانند کنار صفحات آدرس اینترنتی هم در تشخیص اعتبارات می‌تواند موثر باشد. (یادداشت علمی امیرحسین صفدری پژوهشگر علم حقوق در روزنامه اطلاعات)

۲

### ۳- نتیجه گیری

با رشد روزافزون فناوری اطلاعات و خدمات اینترنت، فعالیت‌های مجرمانه نیز در فضای مجازی افزایش شدیدی پیدا کرده است. جرایم رایانه‌ای یکی از پدیده‌های نوظهوری است که گرچه برخی از جرایم آن شباهت‌هایی با جرایم سنتی دارد، اما تفاوت‌هایی در روش و ماهیت و نوع جرم در آن وجود دارد. با توجه به این که فضای مجازی این روزها جز جدا ناپذیری از زندگی بشر شده است بطور یقین افرادی سودجو و فرصت طلب هم نیز با فراگیری دانش فضای سایبر در صدد سوء استفاده از تکنولوژی می‌باشند. که این افراد سودجو امکاناتی را که توسعه تکنولوژی برای جامعه بشری به ارمغان می‌آورد را دست خوش امیال و اغراض منفی خود قرار داده و باعث ایجاد مشکلات زیادی برای استفاده کنندگان از تکنولوژی می‌شوند و سبب ایجاد شبهه و تردید برای استفاده صحیح از این امکانات می‌شوند. متأسفانه باید بگوییم که کلاهبرداری‌های رایانه‌ای از جمله مهمترین جرایم در حوزه سایبر می‌باشد که در حال حاضر هم در کشور ما روز به روز در حال افزایش است؛ و با توجه به ویژگی اصلی جرایم سایبری یعنی ارتکاب آن در فضای مجازی از هر نقطه مکانی و جنبه بین‌المللی آن مقابله کارآمد با این جرایم نیازمند همکاری‌های بین‌المللی است. اگر چه که تحقیقات و پژوهش‌ها توسط محققان و پژوهشگران حوزه علم حقوق و جرایم سایبری در کشور ما تا به الان مفید بوده و باعث آگاهی مردم شده است اما هنوز هم نیاز است که کارهای پژوهشی و تحقیقاتی در زمینه‌های مختلف جرایم سایبری یا همان جرایم رایانه‌ای انجام شود تا اطلاعات مان در حوزه جرایم رایانه‌ای افزایش پیدا کند و راه حل‌هایی برای پیشگیری از جرایم رایانه‌ای پیدا کنیم. چند جرم دیگر هم از این جرایم مهم در حوزه فضای مجازی که این روزها به شدت دیده می‌شود شامل: نشر اکاذیب، توهین، تهدید افراد به افشای اسرار خصوصی آنها و... در این فضاها می‌باشد. باید بگوییم که چنانچه متأسفانه قربانی جرایم رایانه‌ای یا همان جرایم سایبری شدید پس از آگاهی سریعاً به مراجع قضایی و یا پلیس فتا تماس گرفته و یا مراجعه کرده و با اعلام وقوع جرم برای پیگیری و دستگیری این مجرمان اقدام کنید. شما برای ثبت شکایت خود در خصوص کلاهبرداری‌های اینترنتی باید به دادسرای جرائم رایانه‌ای مراجعه کنید، چرا که این دادسرا وظیفه رسیدگی به جرائمی که در بستر فضای مجازی و اینترنت رخ می‌دهد را بر عهده دارد؛ البته پیشنهاد می‌شود در مواجهه شدن با اینگونه از جرایم حتماً با یک حقوقدان و یا وکیل دادگستری مشورت کنید. به عنوان

یک محقق و پژوهشگر در حوزه علم حقوق پیشنهاد می‌کنم به مجلس شورای اسلامی که هر چه زودتر دست به اصلاح قانون جرایم رایانه ای سال ۱۳۸۸ بزند، و به کمک پژوهشگران و محققان حوزه جرایم سایبری، جامعه شناسی، جرم شناسی و... یک قانون علمی و جامع را به تصویب برساند تا خلاهای قانونی موجود در فضای سایبر پوشش داده شود چرا که این روزها شاهد ظهور جرایم و ترفندهای عجیبی در فضای سایبر هستیم که قانون جرایم رایانه ای مصوب ۱۳۸۸ هیچ اشاره ای به آنها نکرده است و این مسئله یک ضعف بزرگ در قانونگذاری برای کشور ما محسوب می‌شود. امیدوارم که این مقاله علمی برای جامعه بشری مفید باشد و باعث کاهش جرایم و آسیب‌ها در حوزه سایبر و رایانه شود.

#### ۴. قدردانی

با تشکر فراوان از زحمات دلسوزانه ی پدر و مادر عزیزمان که در تهیه این مقاله علمی پژوهشی ما را یاری کردند.

#### مراجع و منابع

۱. باستانی، برومند. جرائم کامپیوتری و اینترنتی جلوه ای نوین از بزهکاری. انتشارات بهنامی. تهران. چاپ اول، ۱۳۸۳.
۲. کاظمی سنجان، بیژن. جرائم کامپیوتری و سایبر. انتشارات قانون یار. تهران. چاپ اول، ۱۳۹۶.
۳. دوکوهکی، محمدرضا. بررسی جزائی جرائم رایانه ای و سایبری. انتشارات قانون یار. تهران. چاپ اول، ۱۳۹۶.
۴. نامجویان، محمدرضا. کجوتیان، مرجان. جرایم سایبری، انتشارات آلا قلم. تهران. چاپ اول، ۱۳۹۸.
۵. صبح خیز، رضا؛ پورقهرمانی، بابک؛ صفاری، علی؛ مقاله: الگوی راهبردی مقابله با جرایم سایبری در ایران، چاپ شده در فصلنامه مطالعات راهبردی ناجا، سال پنجم، شماره هجدهم، زمستان ۱۳۹۹.
۶. حافظ نیا، محمدرضا. جغرافیای سیاسی فضای مجازی، تهران، انتشارات سمت، ۱۳۹۱.
۷. جزایری، سیدعباس؛ نعمت‌اللهی، میثم؛ امیریان فارسانی، امین؛ مقاله: پیشگیری از جرایم سایبری و محدودیت‌های حاکم بر آن، چاپ شده در فصلنامه علمی- حقوقی قانون یار، دوره سوم، شماره ۱۲ زمستان ۱۳۹۸.
۸. صفدری، امیرحسین. یادداشت علمی؛ تحت عنوان: نگاه علم حقوق به جرایم سایبری. چاپ شده در روزنامه اطلاعات به شماره ۲۷۹۴۷ شنبه ۱۷ مهر ۱۴۰۰.
۹. زیبر، اولریش. جرایم رایانه ای، ترجمه: محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، تهران انتشارات گنج دانش، چاپ دوم، ۱۳۹۰.
۱۰. شیرزاد، کامران. جرایم رایانه ای از منظر حقوق جزای ایران و حقوق بین‌الملل، تهران، انتشارات شرکت نشر بهینه فراگیر، ۱۳۸۸.
۱۱. رزمن، علی. بررسی کیفری جرائم جنسی و منافی عفت با نگاهی بر فضای سایبر. قانون یار، تهران. چاپ اول، ۱۳۹۵.
۱۲. قدسی، زهرا. مجتهد سلیمانی، ابوالحسن. مقاله: جرائم رایانه ای علیه اخلاق و عفت در حریم خانواده. فصلنامه فقه و حقوق خانواده، ندای صادق. شماره ۵۳، پاییز و زمستان ۱۳۸۹.
۱۳. نظامی نرج آبادی، توقان؛ رئیسی، لیلا؛ مقاله: معاضدت قضایی متقابل در زمینه جرایم سایبری، چاپ شده در مجله پژوهش‌های حقوق جزا و جرم‌شناسی، شماره ۱۵، نیم سال اول ۱۳۹۹.
۱۴. قانون جرایم رایانه ای مصوب ۱۳۸۸.
۱۵. قانون مجازات اسلامی مصوب ۱۳۹۲.