

دو فصلنامه بین المللی تحقیقات حقوق قضایی

License Number: 86227 Article Number: Y4N3788 ISSN-P: 2717-1132

شناخت جرایم ارتكابی در فضای مجازی

علی صمدی اندزقی^۱

وکیل پایه یک دادگستری

دارنده تندیس پژوهشگر برتر از موسسه قانون یار سال های ۱۴۰۱ و ۱۴۰۲

سید محمد سجاسی

محقق و پژوهشگر

چکیده

هر روزه تعاملات به صورت گسترده در فضای مجازی بین افراد صورت می گیرد. گاه ممکن است این تعاملات منجر به تخلفاتی همچون کلاهبرداری، سرقت، انتشار محتوای مجرمانه و یا جعل مجازی شود. در این رابطه روند رو به رشد جرایم کامپیوتری موجب بروز چالش ها و تنش های گوناگونی در جوامع مدرن امروزی از جمله جوامع حقوقی گردیده است. جرایم از یک طرف می تواند شامل فعالیت های مجرمانه ای باشد که ماهیتی سنتی دارند مانند سرقت، کلاهبرداری، جعل و سوء استفاده مالی و یا اینکه ماهیتی کاملاً نوین و غیر قابل پیش بینی که توانسته است حقوق جزاء کلاسیک و آیین دادرسی را کاملاً به چالش انداخته و متحول نماید. همچنین باید توجه از آنجا که فضای سایبری و اینترنتی همواره رو به توسعه و گسترده بوده، روشهای ارتكاب جرم در این حوزه نیز افزایش داشته است همانطور که اشاره شد بسیاری از افراد به واسطه ارتكاب برخی افعال در فضای مجازی ندانسته مرتکب جرمی خاص و درخور مجازات می شوند. به همین دلیل و به جهت اهمیت موضوع در این مقاله سعی داریم به بررسی و تحلیل جرایم ارتكابی در فضای مجازی بپردازیم. روش تحقیق از نوع تحلیلی-توصیفی بوده و ابزار گردآوری داده ها فیش برداری است.

واژگان کلیدی: جرایم اینترنتی، جاسوسی اینترنتی، فضای سایبر، جرم کامپیوتری، هکر

^۱ نویسنده مسئول



بخش اول: بررسی و شناخت محیط سایبر

از لحاظ لغوی در فرهنگ های مختلف، سایبر Cyber A $\cong$ به معنای مجازی و غیر ملموس و مترادف لغت انگلیسی virtual می باشد. که با توجه به گستردگی مفهوم سایبر و اطلاق آن به تمام افعال و اقدامات واقع شده در محیط شبکه های بین المللی و بشمار بودن مصادیق سایبر به توصیه متخصصان و دانشمندان صاحب نام این رشته یافتن لغت معادل و یا ترجمه آن به زبان های دیگر، مجاز نمی باشد چراکه به عقیده این صاحب نظران با توجه به بسط مفهوم لغوی این واژه در سطح بین المللی، آن را تبدیل به یک لغت بین المللی نموده و ترجمه آن و یا یافتن معادلی برای آن ممکن است دایره شمول و مفهوم آن را محدود نماید.

اصطلاح سایبر را اولین بار ریاضیدانی به نام نوربرت وینر^۱ در سال ۱۹۵۰ بکار برد و مقصود وی از آن مطالعه ساز و کارهای ارتباطی، بازخورد و کنترل سیستم های زنده و ماشین ها بود. در این علم فرایندهای ارتباطی و کنترل سیستم های بیولوژیکی، مکانیکی و الکترونیکی و اصطلاحاتی، به ویژه مقایسه اینگونه فرایندها ما بین سیستم های زنده، و سیستم های مصنوعی صورت می پذیرد. اما واژه سایبر برای اولین بار توسط داستان نویسی به نام ویلیام گیbson^۲ در سال ۱۹۸۴ میلادی در یک داستان علمی - تخیلی و با عنوان فضای سایبر (cyber space) به کار گرفته شد.

(دفتر مطالعات و برنامه ریزی رسانه ها، ۱۳۸۸، ۷)

خلق اصطلاح سایبر که امروزه محور بسیاری از بحث هاست، در دهه ۹۰ خصوصاً از سال ۱۹۹۴ به بعد بود، البته قبلاً واژه سایبرنتیک مطرح بود اما فضای سایبر و به دنبال آن حقوق سایبر از این دهه شروع شد. مراد از سایبر در مباحث حقوقی مجموعه رایانه + مودم + مخابرات با ویژگی شبیه سازی و مجازی سازی است. (زندی، ۱۳۸۹، ۴۸)

برخی بیان داشته اند فضای سایبر شبکه ای از مجموعه لایتنهای از صفر و یک های دیجیتالی هستند که داده های الکترونیکی را تشکیل می دهند و آن داده ها نیز در قالب های مختلف مفاهیم را به شکل الکترونیکی منعکس می سازند و در واقع آنچه که از آن به عنوان فضای سایبر یاد می شود همین بستر است که داده های الکترونیکی در آن ذخیره و

^۱. Norbert wiener

^۲. William Gibson



به انحاء گوناگون پردازش و در نهایت به شیوه مورد نظر به شکل خروجی منعکس می شوند. (جلالی فراهانی، ۱۳۸۶، ۵۳)

باستانی (۱۳۸۳، ۵۶) فضای سایبر را اینگونه تشریح می کند :

A محیطی است مجازی و غیر ملموس موجود در فضای شبکه های بین المللی (این شبکه ها از طریق شاهراه های اطلاعاتی مانند اینترنت به هم وصل هستند) که در این محیط تمام اطلاعات راجع به روابط افراد، فرهنگ ها، ملت ها، کشورها و به طور کلی هر آنچه در کره خاکی به صورت فیزیکی و ملموس وجود دارد (به صورت نوشته، تصویر، اسناد) در یک فضای مجازی به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس استفاده کنندگان و کاربران می باشند و به طریق کامپیوتر، اجزاء آن و شبکه های بین المللی به هم مرتبط می باشند ≡

و در نهایت دکتر زندی (۱۳۸۹، ۵۴) می گوید :

A فضای سایبر، تمامیت الکترونیکی پدید آمده از طریق ارتباط جهانی مجموع وسایل ایجاد، ذخیره، پردازش و انتقال داده های الکترونیکی با ویژگی شبیه سازی و مجازی سازی است ≡

با توجه به توضیحات فوق و تعاریفی که از متخصصان بیان گردید می توان سایبر سپیس را چنین تعریف نمود :

A محیطی است مجازی و غیر ملموس موجود در فضای شبکه های بین المللی، که از تلفیق رایانه و مخابرات به وجود آمده است و محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه ای سریع و با ابزار خاص خود، در آن به وقوع می پیوندد ≡

بخش دوم : بررسی و شناخت جرایم رایانه ای^۱

تا کنون تعاریف گوناگونی از جرم رایانه ای از سوی سازمان ها، متخصصان و برخی قوانین ارائه شده که وجود تفاوت در آنها بیانگر ابهامات موجود در ماهیت و تعریف این تیپ از جرایم است. و قبل از هر چیز توجه به این نکته اهمیت دارد که تعبیر جرایم رایانه ای، با وجود پیدایش اصطلاحات جدید یاد شده در خصوص جرایم نوین مرتبط با فناوری اطلاعات، کماکان کلیت خود را حفظ کرده است و لذا مفهوم آن را در وسیع ترین شکل

^۱. Computer crimes



ممکن باید مدنظر داشت.

جرم کامپیوتری یا جرم در فضای مجازی دارای دو معنا و مفهوم است. در تعریف مضیق، جرم کامپیوتری صرفاً عبارت است از جرایمی است که در فضای سایبر رخ می دهد. از این نظر جرایمی مانند هرزه نگاری، افترا، آزار و اذیت و سوء استفاده از پست الکترونیک^۱ و سایر جرایمی که در آنها کامپیوتر به عنوان ابزار و وسیله ارتکاب جرم به کار گرفته می شود، در زمره جرم کامپیوتری قرار نمی گیرند. در تعریف موسع از جرم کامپیوتری هر فعل و ترک فعلی که در، یا از طریق یا به کمک یا از طریق اتصال به اینترنت، چه به طور مستقیم یا غیرمستقیم، رخ می دهد و توسط قانون ممنوع گردیده و برای آن مجازات در نظر گرفته شده است، جرم کامپیوتری نامیده می شود. (ضیایی پرور، ۱۳۸۳، ۷۲)

در تعریف دیگری جرم رایانه ای اینگونه بیان شده است: جرم به کلیه ی اعمال ضد اجتماعی و تنش هایی اطلاق می شود که به جامعه آسیب می رساند. در تعریفی دیگر جرم به فعل یا ترک فعلی گفته می شود که به خاطر اخلال در نظم عمومی جامعه از طرف قانونگذار منع شده و برای مرتکبین آن مجازات تعیین شده است. نیز براساس قانون مجازات اسلامی، A هر فعل یا ترک فعلی که در قانون برای آن مجازات تعیین شده باشد $\equiv$ جرم محسوب می شود. طیف گسترده افعال مجرمانه ای که ذیل مفهوم جرایم رایانه ای جا دارند و ماهیت متغیر آنها که ناشی از پیشرفت لحظه به لحظه ی فناوری اطلاعات و ارتباطات و شیوه های سوء استفاده از آن است، ارائه ی تعریف جامع و مانع و خالی از مناقشه را مشکل و چه بسا غیرممکن می سازد. تا آنجایی که در تعریف گسترده ای بیان می شود که هر فعل یا ترک فعلی که در یا A از طریق $\equiv$ یا A به کمک سیستم های رایانه ای $\equiv$ رخ می دهند جرم رایانه ای قلمداد می شود. (معاونت اجتماعی فرماندهی انتظامی، ۱۳۸۴، ۱۰۳) و بر این اساس جرایم کامپیوتری را می توان به سه دسته تقسیم نمود:

دسته اول: جرایمی هستند که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می شوند، مانند سرقت، تخریب و غیره.

دسته دوم: جرایمی هستند که در آنها کامپیوتر به عنوان ابزار وسیله توسط مجرم برای ارتکاب جرم به کار گرفته می شود.

^۱. E - mail



دسته سوم : جرایمی هستند که می توان آنها را جرایم کامپیوتری محض نامید. این نوع از جرایم کاملاً با جرایم کلاسیک تفاوت دارند و در دنیای مجازی به وقوع می پیوندند، اما آثار آنها در دنیای واقعی ظاهر می گردد، مانند دسترسی و شنود غیرمجاز در سیستم های کامپیوتری. (ضیایی پرور، ۱۳۸۳، ۷۲)

پیشرفت تکنولوژی و علم و دست یابی بشر به فناوری اطلاعات و استفاده از رایانه و پیدایش دنیای مجازی دارای پیامدهای مثبت و منفی فراوانی برای بشر بوده است. از جمله پیامدهای منفی آن، پیدایش جرایم رایانه ای بوده است. اما با توجه به مطالب مذکور در مورد جرایم رایانه ای، هر کشوری تعریفی خاص از این جرایم ذکر کرده است که برخی از این تعاریف عبارتند از :

• اتریش

پروفسور شیک یکی از حقوقدانان اتریشی در تعریف جرم رایانه ای بیان می دارد : جرم رایانه ای به هر عمل مجرمانه ای گفته می شود که در آن رایانه، وسیله یا هدف ارتکاب جرم باشد. (شیرزاد، ۱۳۸۸، ۳۵)

• ایالات متحده آمریکا

در ایالات متحده آمریکا تعریف وسیعی از جرم رایانه ای به عمل آمده مبنی بر آن که : هر اقدام غیرقانونی که با یک رایانه یا به کارگیری آن مرتبط باشد را جرم رایانه ای می گویند. یا هر اقدامی که به هر ترتیب با رایانه مرتبط بوده و موجب ایجاد خسارت به بزه دیده شود و مرتکب از این طریق منفعتی را تحصیل کند، جرم محسوب می شود. (عمیدی، ۱۳۸۷، ۲۰)

• کانادا

در کانادا نیز در تعریف جرایم رایانه ای این چنین بیان شده است : جرم رایانه ای شامل هر فعالیت مجرمانه ای است که در برگیرنده کپی، استفاده، جابجایی، مداخله، دسترسی یا سوء استفاده از سیستم های رایانه ای، عملکرد رایانه، داده ها یا برنامه های رایانه است. (شریفی، ۱۳۷۹، ۸۰)

• آلمان

پلیس جنایی فدرال آلمان در تعریفی از جرایم رایانه ای این چنین اعلام داشته است : جرم رایانه ای در برگیرنده همه اوضاع و احوال و کیفیاتی است که در آن شکل های پردازش الکترونیک داده ها، وسیله ارتکاب و یا هدف یک جرم قرار گرفته است و مبنایی برای نشان



دادن این ظن است که جرمی ارتکاب یافته است. (دزیانی، ۱۳۷۳، ۱۵۸)

• ایران

در حقوق ایران، نه در قانون تجارت الکترونیک و نه در قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۱۱/۱۱ هیچ تعریفی از این مفهوم ارائه نشده است. شاید دلیل آن اختلافات مبنایی است که میان حقوقدانان از تعریف جرایم رایانه‌ای وجود دارد. اما می‌توان به عنوان نمونه تعریف زیر را ارائه کرد : آن دسته از جرایمی که با سوء استفاده از یک سیستم رایانه‌ای بر خلاف قانون ارتکاب می‌یابد جرایم رایانه‌ای نام دارد. البته این دسته از جرایم را می‌توان شامل جرایم سنتی که به واسطه رایانه صورت می‌گیرد از قبیل کلاهبرداری و سرقت و نیز جرایم نوظهوری که با تولد رایانه پا به عرصه حیات گذاشته اند دانست، مانند جرایم علیه صحت و تمامیت داده‌ها. (طارمی، ۱۳۸۷، ۸۸) در واقع در حقوق ایران تعریف جرایم رایانه‌ای به سکوت واگذار شده و در بیشتر موارد تقریباً همان تعریف ارائه شده از طرف سازمان همکاری و توسعه اقتصادی را پذیرفته اند. (پاکزاد، ۱۳۸۰، ۳۸)

بخش سوم: طبقه بندی جرایم رایانه‌ای

در تقسیم بندی جرایم رایانه‌ای تاکنون چندین طبقه بندی و تقسیم بندی توسط محققان و متخصصان و حقوقدانان و علمای حقوق جزا مطرح گردیده است. از سوی دیگر، جرایم کامپیوتری و اینترنتی با توجه به خصیصه فراملی و فراسرزمینی بودنشان لازمه تعاون و همکاری بین المللی را ایجاد می‌کند و پدیده‌ای است که به دلیل شرایط خاص و ماهیت بین الملل بودن اینگونه جرایم، نوعی سیاست جنایی متحد الشکل را به دنبال می‌آورد. (حسینی خواه و رحمتی، ۱۳۸۹، ۶۰) در کشورهای پیشرفته قانونگذاران آنها با توجه به نیاز جامعه، انواع مختلفی از اعمال مجرمانه کامپیوتری را شناسایی و در قالب قوانین کیفری خود گنجانده اند که همزمان با این اقدامات پراکنده کشورها، مراجع بین المللی نیز فعالیت خود را در این زمینه آغاز و با دسته بندی جرایم شناخته شده، لیست هایی از اینگونه جرایم را به عنوان الگوی واحد و راهنما برای تدوین قوانین ملی کشورها ارائه نمودند.

بند اول : رایانه به عنوان منزله موضوع جرم

کامپیوتر نیز به عنوان پدیده‌ای که با سرعت فوق العاده زیاد و گنجایش بیش از حد جایگزین ذهن بشر شده، از تجاوزات و جرایم مستثنی نبوده است. کامپیوتر با تمام مزایایی که برای انسان دارد که از آن جمله می‌توان به سرعت، صحت، دقت، خستگی ناپذیری،



فراموش نکردن، نگهداری حجم عظیمی از اطلاعات اشاره کرد اما از گزند تجاوزات بشری به دور نبوده است و این همان جنبه منفی کامپیوتر یا نیمه تاریک آن است. امروزه شاهد تعداد زیادی جرایم هستیم که در زمینه کامپیوتر رخ می دهد حال چه به واسطه آن و چه علیه آن. (خداعلی، ۱۳۸۳، ۱۸) این جرایمی که کامپیوتر به منزله موضوع یا وسیله جرم است را به سه گروه زیر تقسیم نموده اند که عبارت است از :

۱. جرایمی که عامل آن خرابی در سیستم رایانه است

این فرض در مورد رایانه های محاسب است که به علل مختلف از جمله خرابی در بخش حافظه، ممکن است دچار اختلال شوند، به عنوان مثال شرکت های برق که صورت حساب های خود را به وسیله رایانه تهیه می کنند و توسط پست برای مشترکان ارسال می نمایند، بسیار دیده شده است که این رایانه ها در برآورد وجوه آب و برق و غیره دچار اشتباهاتی شده اند و باعث زیادی پرداخت بعضی از مشترکان یا پرداخت کم آنها می شود. جرایم ارتكابی توسط خود رایانه شاید امروزه به اندازه دیگر مسائل به چشم نخورد، ولی با پیشرفت سریع رایانه بعید به نظر نمی رسد، روزی فرا رسد که خود رایانه ها مباشرتاً مرتکب جرایمی شوند، به خصوص رایانه های نسل پنجم که قادر به تفکر هستند و گاهی طوری اعمال می کنند که از تفکر خودشان حاصل شده است.

(طاهری جیلی، ۱۳۷۲، ۱۲۳)

۲. جرایمی که به وسیله رایانه ارتکاب می یابند

هر جرمی که رایانه به منزله ابزار آن نقش داشته باشد یا دلایل و اطلاعات مربوط به آن در رایانه ذخیره یا پردازش یا منتقل شده باشد. (جاویدنیا، ۱۳۸۷، ۱۲۵)
این نوع جرایم به دو دسته تقسیم می شوند :

الف : خروج غیرمجاز اطلاعات و داده های رایانه ای

دریافت غیرمجاز اطلاعات از یک رایانه هنگامی، عنوان جرم به خود می گیرد که این اطلاعات سری باشند، به عنوان مثال : می توان به فعالیت چند جوان که چند سال پیش از مرکز اطلاعات نظامی فرانسه مقداری اسرار نظامی را به سرقت برده و به کشورهای بلوک شرق فروخته بودند اشاره کرد. (حسینی خواه و رحمتی، ۱۳۸۹، ۶۲)



ب: ورود اطلاعات غلط و داده های خلاف واقع به رایانه

از آنجا که مبنای کار رایانه اطلاعات و داده های اولیه است، پس می توانیم با دادن اطلاعات غلط و داده های خلاف واقع به رایانه عمل صحیحی را غلط و یا عمل غلطی را صحیح جلوه دهیم. این نمونه در دادگستری هایی که از رایانه برای بایگانی سوابق مجرمان استفاده می نمایند کاربرد بیشتری دارد. البته ممکن است اهداف دیگری نیز از دادن اطلاعات اشتباه به رایانه دنبال شود، مثل بی اعتبار کردن یک اداره، نتیجه دهی غلط رایانه ممکن است علل مختلفی داشته باشد از جمله:

- اشتباه در اطلاعات ورودی
- اشتباه در برنامه های کاربردی
- اشتباه عملیاتی از سوی متصدی رایانه
- اشتباه کشف نشده در نرم افزار سیستم
- اشتباه بر اثر خرابی نرم افزار که مسئول هر قسمت در صورت سوء نیت یا بی مبالاتی ممکن است مجرم شناخته شود. (پرهامی، ۱۳۷۲، ۱۸۰)

۳. جرایم علیه رایانه

چون اساس کار هر رایانه نرم افزارهایی است که در آن استفاده می شود، از این رو نرم افزارها دارای ارزش خاصی هستند و به همین علت همواره جرایم مربوط به نرم افزارها رو به افزایش است. اینگونه جرایم عبارتند از: سرقت نرم افزار، تخریب اطلاعات نرم افزار، تخریب نرم افزار، کپی برداری غیرقانونی از برنامه ها و تقلب در نرم افزارها. که این جرایم بر علیه سیستم رایانه ای صورت می گیرد. (حسینی خواه و رحمتی، ۱۳۸۹، ۶۲)

یکی از جرایم رایانه ای که خود به عنوان جرمی مستقل محسوب می شود، اما می تواند در بعضی از جرایم رایانه ای به عنوان جزئی از رکن مادی محسوب شود، شنود است. (حسن بیگی، ۱۳۸۴، ۲۵۳) جایگاه این بحث در تقسیم بندی های جزای اختصاصی، در مبحث جرایم علیه امنیت و آسایش عمومی قرار می گیرد و شامل موضوعاتی از قبیل دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه ای است.

عمل شنود تنها در خصوص امواج مطرح است این امواج ممکن است صوتی، الکترومغناطیسی و نوری باشند. صوت ایجاد شده هم ممکن است در اثر صحبت انسان، ضربات، کلیدهای دستگاه تایپ یا ضربات دستگاه تلگراف حاصل شود. البته امروزه با



تغییرات عمده در سامانه های مخابراتی، صرفاً صوت منتقل نمی شود؛ تصویر، عکس، اطلاعات نوشتاری و دیجیتالی از جمله مواردی هستند که انتقال و ارسال آنها به وسیله ابزارهای رایانه ای و یا مخابراتی انجام می شود. (ترکی، ۱۳۸۸، ۱۵) از آنجاکه بررسی و تحلیل در رابطه با جرم شنود غیرمجاز نیازمند نگارش یک پژوهش جداگانه است فلذا این موضوع درخور انجام پژوهشی جداگانه و مستقل است.

بخش چهارم: مصادیق نقض حریم خصوصی در فضای مجازی

نقض حریم خصوصی در فضای مجازی یکی از مهمترین مسائل روز جامعه ماست که از دو منظر قابل بررسی است یکی از جانب قربانیان نقض حریم خصوصی در فضای مجازی و دیگری از سوی ناقضین حریم خصوصی در فضای مجازی.

بزه دیدگان در فضای مجازی نقش مهمی را در بروز جرایم ناقض حریم خصوصی ایفا می کنند و در عین حال می توانند در اقدامات پیشگیرانه علیه جرایم سایبری یا همان (cyber prevention) نقش آفرین باشند. بسیاری از بزه دیدگان جرایم سایبری و کسانی که حریم خصوصی آنان در فضای مجازی نقض می گردد، استعدادی قابل توجه برای قربانی شدن^۱ بروز می دهند و به راحتی طعمه بزهکاران سایبری می شوند بعضی کلاهبرداری های اینترنتی ناشی از کسب اطلاعات به روش های بسیار ساده و سوء استفاده از عکس ها و اسرار شخصی نمونه هایی از این موضوع می باشد.

اشخاص بایستی نسبت به صیانت از حریم خصوصی خود همت نمایند، بسیاری اشخاص بدون رعایت مسائل امنیتی، خصوصی ترین اطلاعات خود را بر روی سیستم رایانه ای و یا حامل های داده نظیر فلش و کارت های حافظه و تلفن همراه و سی دی ذخیره می نمایند و به نوعی دست بزهکار سایبری را در تعرض به حریم خصوصی باز می گذارند و این چنین استعداد قربانی شدن در فضای مجازی را از خود نشان می دهند. جنبه دیگر موضوع همانطور که معروض گردید مربوط به ناقضان حریم خصوصی در فضای مجازی است. این بزهکاران زمانی که وارد فضای مجازی یا همان اینترنت می شوند در خیالی خام آن را ملک مطلق خود دانسته و اجازه هرگونه فعالیت و ورود به حریم خصوصی دیگران را به خود می دهند. (www.momtaznews.com)

^۱. immolate



در زیر به بعضی مصادیق نقض حریم خصوصی در فضای مجازی که در قانون جرایم رایانه ای جرم انگاری شده است می پردازیم :

- ۱- دسترسی غیرمجاز به داده های رایانه ای یا مخابراتی نظیر هک ایمیل یا اکانت اشخاص.
- ۲- شنود غیرمجاز محتوای در حال انتقال در سیستم های رایانه ای یا مخابراتی نظیر استفاده از نرم افزارهای شنود چت های اینترنتی.
- ۳- دسترسی غیرمجاز به داده های سری در حال انتقال در سیستم های رایانه ای یا مخابراتی یا حامل های داده یا تحصیل و شنود آن.
- ۴- در دسترس قرار دادن داده های سری در حال انتقال در سیستم های رایانه ای یا مخابراتی یا حامل های داده برای اشخاص فاقد صلاحیت.
- ۵- نقض تدابیر امنیتی سیستم های رایانه ای یا مخابراتی به قصد دسترسی به داده های سری در حال انتقال در سیستم های رایانه ای یا مخابراتی یا حامل های داده.
- ۶- حذف یا تخریب یا مختل یا غیرقابل پردازش نمودن داده های دیگری از سیستم های رایانه ای یا مخابراتی یا حامل های داده به طور غیرمجاز.
- ۷- از کار انداختن یا مختل نمودن سیستم های رایانه ای یا مخابراتی به طور غیرمجاز نظیر غیر فعال سازی دیتابیس تارنها و ممانعت از دسترسی اشخاص به پایگاه اینترنتی های شخصی.
- ۸- ممانعت از دسترسی اشخاص مجاز به داده های یا سیستم های رایانه ای یا مخابراتی به طور غیرمجاز.
- ۹- ربودن داده های متعلق به دیگری به طور غیرمجاز.
- ۱۰- هتک حیثیت از طریق انتشار یافتن صوت و فیلم تحریف شده دیگری به وسیله سیستم های رایانه ای یا مخابراتی.
- ۱۱- نشر اکاذیب از طریق سیستم های رایانه ای یا مخابراتی به قصد اضرار به غیر یا تشویش اذهان عمومی.
- ۱۲- فروش یا انتشار یا در دسترس قرار دادن گذرواژه یا هر داده ای که امکان دسترسی غیرمجاز به داده ها یا سیستم های رایانه ای یا مخابراتی متعلق به دیگری را فراهم کند.
- ۱۳- آموزش نحوه ارتکاب جرایم دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه ای و تخریب و اخلاف در داده ها یا سیستم های رایانه ای و مخابراتی.



ناقضین حریم خصوصی در فضای مجازی به دلایلی نظیر افسردگی، عصبانیت، حسادت، انتقام جوئی، حس تنفر، تفریح و سرگرمی، خود کم بینی و حقارت، حس رقابت و عدم توجه به اصول اخلاقی و ارزش های جامعه، خود را مجاز به ورود به حریم خصوصی قربانیان دانسته و خسارات جبران ناپذیری را به حیثیت و مال و حتی جان اشخاص وارد می سازند.

بخش پنجم: نگاهی به تهدیدات امنیت اطلاعات در فضای سایبر

فضای سایبر، علی رغم تمامی جنبه های مثبت دارای مجموعه ای گسترده از خطرات و تهدیدات امنیتی است که برخی از آنان بسیار جدی و مهم بوده و برخی دیگر از اهمیت کمتری برخوردار می باشند.

از نظر مفهومی میان ماهیت تهدیدات فضای سایبر و تهدیداتی که در دنیای واقعی وجود دارند هیچ تفاوتی نیست، بلکه تفاوت این دو مقوله برخاسته از خصوصیات فضای الکترونیکی و تهدیدات این حوزه است که باعث می شود بتوان از بروز آنها جلوگیری کرد و آنها را خنثی، یا شناسایی و رفع نمود. قطعاً تاکنون اخبار متعددی را در خصوص سرقت اطلاعات حساس نظیر شماره کارت اعتباری و یا شیوع یک ویروس کامپیوتری شنیده اید و شاید شما نیز از جمله قربانیان این نوع حملات بوده اید. آگاهی از تهدیدات موجود و عملیات لازم به منظور حفاظت در مقابل آنان، یکی از روش های مناسب دفاعی است. (امیریان، ۱۳۸۹، ۲۹۰)

بند اول : تهدید و ویروس های اینترنتی

ویروس برنامه ای است که به انتهای برنامه دیگر متصل می شود و یا وارد بدنه یک برنامه دیگر می گردد. وقتی آن برنامه به اجرا در می آید، ویروس نیز اجرا می شود و نسخه های خود را وارد فایل ها یا دیسک های دیگر می کند و بدین صورت خود را تکرار می نماید، و هنگامی که هر یک از فایل ها یا برنامه های آلوده اجرا می شوند این روند بار دیگر تکرار می گردد. ویروس ها از یک رایانه به رایانه دیگر منتقل می شود. اغلب ویروس ها خودشان را به فایل های اجرایی می چسبانند و برخی از آنها می توانند رکورد بوت اصلی، کدهای اجرایی خودکار و حتی در برخی موارد دیگر، فایل ها را هدف قرار دهند. برخی از ویروس ها برای از کار انداختن کامل رایانه طراحی شده اند، در حالی که برخی دیگر به حذف فایل های کاربر یا آسیب رساندن به آنها کفایت می کنند. در حالت کلی، هدف یک ویروس ویران کردن فایل و نفوذ به درون فایل ها و برنامه هاست.



بند دوم : تهدید کرم های اینترنتی

کرم برنامه ای است که از طریق شبکه کامپیوتری و به وسیله نفوذ در کامپیوترها به همان شیوه ای که هکر می تواند وارد آنها شود از یک کامپیوتر به کامپیوتر دیگر تکثیر شود. آنها بر خلاف ویروس ها هیچ کمکی از کاربران بی حواس نمی گیرند. آنها باید کامپیوتری را بیابند که بتوانند نفوذ کنند، حمله ای را انجام دهند و کپی خود را برای اجرا شدن به میزبان هدف انتقال دهند. در عمل، یک کرم به طور کامل گام هایی را که یک متجاوز به سوی کامپیوترها بر می دارد و از کامپیوتری به روی کامپیوتر بعدی می پرد به صورت خودکار انجام می دهد.

(ضیایی پرور، ۱۳۸۳، ۲۱۴)

بند سوم : تهدید اسب های تروآ

اسب های تروآ و اجزاء وابسته به آنها تهدیداتی هستند که اصالت اطلاعات ذخیره شده در سیستم یا داده های مبادله شده در شبکه ها را به خطر می اندازد. (جی. آیکو و همکاران، ۱۳۸۳، ۹۳) نام این نرم افزار از افسانه جنگ شهر تروآ در یونان برگرفته شده است. در آن افسانه، یونانی ها یک اسب چوبی بزرگ را از دروازه شهر به داخل می فرستند و هنگامی که اسب وارد شهر می شود تعداد زیادی سرباز یونانی از آن خارج می شوند و شهر را به تصرف خود در می آورند. از آن زمان به بعد " اسب تروآ " به معنای چیزی است که ظاهری عادی اما محتویاتی خطرناک دارد. در مفاهیم رایانه ای، اسب تروآ می تواند خرابی های زیادی به بار آورد و یا اعمالی غیر از آنچه که کاربر انتظار آن را دارد انجام دهد. این اصطلاح در سال های اخیر به برنامه های مخربی اطلاق می شود که معمولاً بدون اطلاع و اجازه کاربر وارد سیستم می شوند و به جمع آوری و ارسال اطلاعات می پردازند. (George Sadowsky، ۲۰۰۳، ۷۱)

این برنامه دو قسمت دارد ؛ که یه قسمت آن به کامپیوتر قربانی، و قسمت دیگر مدیریت سیستم است که در اختیار هکر می ماند. هکر قسمت سرور برنامه را به یک فایل (مثلاً عکس یا یک فایل جالب) متصل کرده و برای قربانی اتصال می نماید، کاربر بدون اطلاع از چنین فایلی عکس را باز و اسب تروآ به کامپیوتر منتقل می شود. با ورود این فایل به درون سیستم قربانی، هکر می تواند به وسیله سرور الحاق شده به آن کنترل کامپیوتر مذکور را توسط بخش مدیریت سرور در اختیار گرفته و اطلاعات مورد نیاز خود را دریافت نماید.



اطلاعاتی که توسط یک برنامه ترواً قادر به دریافت است می تواند از کلمه رمز برنامه های مختلف موجود در کامپیوتر قربانی باشد تا شماره رمز کارت اعتباری. (امیریان، ۱۳۸۹، ۲۹۳) نرم افزار های مخرب مذکور می توانند اطلاعاتی در مورد رایانه شما و فایل های موجود در آن بدست آورند و این اطلاعات را در اختیار نویسنده خود قرار دهند. این برنامه ها می توانند همه فایل های رایانه شما (حتی فایل های رمزگذاری شده) را بخوانند. اگر اطلاعات حساب بانکی یا کارت های اعتباری خود را در رایانه ذخیره می کنید ممکن است این داده ها مورد علاقه نفوذگران باشند. اگر از امضای خود در رایانه تصویری تهیه کرده باشید تا از آن در چاپ و یا ارسال نامه ها استفاده کنید، آن هم ممکن است بکار مهاجمان بیاید. جمع آوری این بسته های اطلاعاتی در کنار هم می تواند برای مهاجم این امکان را بوجود آورد که بتواند از هویت شما سوء استفاده کند. (George Sadowsky، ۲۰۰۳، ۷۳)

نتیجه گیری

در نتیجه گیری این مقاله باید گفت همانطور که می دانیم پیشرفت تکنولوژی کامپیوتری و اطلاعاتی به خصوص در زمینه تبادل اطلاعات در سطح بین المللی و بروز جرایم پیچیده تر و تخصصی تر مرتبط با این فناوری (جرایم سایبر)، مشکلات و معضلات بسیاری را برای کاربران کامپیوتر و اینترنت بوجود آورده است. مجرمان کامپیوتر بدون هراس از احتمال دستگیری یا تعقیب قانونی، در شبکه اینترنت به کمین نشسته اند و به عنوان تهدیدی جدی برای سلامت مالی شرکت های تجاری، مشتریان و کاربران شبکه و امنیت کشورها مطرح هستند. در جمع بندی کلی و پایانی پژوهش حاضر باید گفت جرایم سایبری می توانند شامل موارد زیر باشند:

۱. هکرینگ (Hacking): نفوذ به سیستم ها یا شبکه های کامپیوتری به صورت غیرقانونی با هدف دسترسی به اطلاعات حساس یا تخریب داده ها.
۲. بدافزار (Malware): استفاده از نرم افزارها یا برنامه های مخرب مانند ویروس ها، تروجان ها و ورم ها (worms) به منظور آسیب زدایی از سیستم ها یا دزدیدن اطلاعات که بخش زیادی از انواع جرایم سایبری در ایران را شامل می شوند.
۳. کلاهبرداری الکترونیکی (Phishing): تلاش برای به دست آوردن اطلاعات حساس از افراد به وسیله ایجاد سایت ها یا ایمیل های متقلب که به نظر می رسند معتبر هستند.



۴. سرقت هویت (Identity Theft): استفاده از اطلاعات شخصی دیگران به منظور سودجویی یا ارتکاب جرائم دیگر.
۵. حملات سایبری به زیرساخت‌های بحرانی: حملات به سیستم‌های اجتماعی، اقتصادی یا امنیتی یک کشور با هدف تخریب یا تخریب ساختارهای حیاتی.
۶. ترویج اطلاعات غیرقانونی (Cyber Espionage): جمع‌آوری اطلاعات حساس از سازمان‌ها یا دولت‌ها به صورت غیرقانونی.
۷. سوءاستفاده از رسانه‌های اجتماعی (Social Engineering): تلاش برای ترغیب افراد به انجام اقدامات خاص به وسیله فریب و مهندسی اجتماعی را شامل می‌شود.

همچنین باید توجه داشت انواع جرایم رایانه‌ای در ایران شامل موارد زیر می‌شوند:

- جعل رایانه‌ای
- جاسوسی رایانه‌ای و سرقت نرم افزار
- نشر اکاذیب و هتک حیثیت
- جرایم مرتبط با رایانه علیه حقوق شهروندان
- شنود غیرمجاز محتوای ارتباطات غیر عمومی
- انتشار، تولید و یا در دسترس قرار دادن گذرواژه یا داده‌هایی که دسترسی به آن‌ها غیرمجاز است
- سرقت خدمات
- مزاحمت اینترنتی
- توهین به مقدسات مذهبی در فضای مجازی
- انتشار محتویات مبتذل و مستهجن
- خراب‌کاری رایانه‌ای
- دسترسی یافتن غیر مجاز به دستگاه‌های پردازش داده
- ... و

بر اساس قانون ۲۵ جرایم رایانه‌ای اگر شخصی به برخی از انواع جرایم سایبری بالا اقدام کند، از ۹۱ روز تا یک سال به حبس محکوم شده و باید جریمه نقدی از ۵ تا ۲۰ میلیون ریال پرداخت کند. همچنین با نگاه به ماده ۲۹ قانون جرائم رایانه‌ای، رسیدگی به آن‌ها در



صلاحیت دادگاه محل وقوع جرم است ولی در صورتی که برای انواع جرائم سایبری که گزارش می‌شوند، محل دقیق وقوع جرم مشخص نشده باشد، تحقیقات اولیه باید در دادسرای محل گزارش جرم، صورت گیرد و پس از آن دادگاه مربوطه نتیجه و رای را اعلام و مجازات انواع جرایم رایانه ای را تعیین می‌کند.

همچنین لازم به ذکر است جرایم خرید اینترنتی متداول ترین راه برای دام افتادن قربانیان و ارتکاب جرم در فضای مجازی است. در این زمینه، مسائل متعددی وجود دارد که می‌توانند به عنوان جرایم مرتبط با خرید اینترنتی مطرح شوند. برخی از این جرایم عبارتند از:

۱. تقلب در خرید آنلاین (Online Fraud) این ممکن است شامل انواع تقلب‌های مرتبط با خرید آنلاین باشد که در آن افراد یا گروه‌ها سعی در فریب و گول زدن مشتریان دارند.

۲. سوءاستفاده از اطلاعات بانکی (Credit Card Fraud) حملاتی که هدف آن‌ها استفاده غیرمجاز از اطلاعات بانکی مشتریان به منظور خرید محصولات یا خدمات آنلاین است.

۳. تقلب در مزایده‌های آنلاین (Online Auction Fraud) فرآیندهای مزایده‌ای که به طور غیرمجاز تغییر می‌کنند یا اطلاعات نادرست در آن‌ها درج می‌شود.

۴. احتیال در خرید و فروش محصولات (Online Product Scams) شامل تقلب در فروش محصولات غیرموجود، ارائه کالاهای کیفیت پایین‌تر از توقعات، یا اطلاعات نادرست در مورد محصولات.

۵. سوءاستفاده از اطلاعات شخصی (Identity Theft) به دست آوردن اطلاعات شناسایی شخصی با هدف سوءاستفاده در فعالیتهای خرید آنلاین.

۶. جعل و سوءاستفاده از وبسایت‌های تقلبی (Fake Websites) ایجاد وبسایت‌های جعلی که به نظر می‌رسند معتبر و درخواست اطلاعات حساس از کاربران را دارند.

۷. فروش کالاهای تقلبی: خرید و فروش کالاهای جعلی یا تقلبی به مشتریان به عنوان محصولات اصلی.

۸. ترویج جعلی (Fake Advertising) استفاده از تبلیغات جعلی برای جلب مشتریان برای خرید محصولات یا خدمات غیرواقعی.



منابع و مآخذ

۱. آزادفلاح، راحله، جرایم کامپیوتری، پایان نامه کارشناسی ارشد، دانشگاه آزاد واحد تهران، واحد علوم تحقیقات، ۱۳۸۷.
۲. باستانی، برومند، جرایم کامپیوتری جلوه ای نوین از بزهکاری، تهران، انتشارات بهنامی، ۱۳۸۳، چاپ اول.
۳. بای، حسین علی و پورقهرمان، بابک، بررسی فقهی حقوقی جرایم رایانه ای، قم، پژوهشگاه علوم و فرهنگ اسلامی، پاییز ۸۸، چاپ اول.
۴. تاج زمان، دانش، مجرم کیست؟ انتشارات کیهان، تهران، ۱۳۶۸.
۵. جلالی فراهانی، امیرحسین، و باقری اصل، رضا، ۱۳۸۶، پیشگیری اجتماعی از جرائم و انحرافات سایبری، نشریه مرکز پژوهش های مجلس، شماره ۵۵.
۶. حاجی ده آبادی، محمدعلی، پیشگیری از جرم، در: دانشنامه امام علی (ع)، تهران، پژوهشگاه فرهنگ و اندیشه اسلامی، ۱۳۸۰.
۷. خسروشاهی، قدرت الله، پیشگیری از جرم در آموزه های قرآنی، بصیرت، ش ۳۰-۳۱، ص ۷۳-۵۵.
۸. دزیانی، محمدحسن، ۱۳۸۳، جرایم کامپیوتری، سازمان مدیریت و برنامه ریزی، دبیرخانه شورای عالی انفورماتیک کشور.
۹. رجبی پور، محمود، ۱۳۸۲، راهبرد پیشگیری اجتماعی از جرم، دانشگاه علوم انتظامی ناجا، سال پنجم، شماره ۳.
۱۰. رجبی پور، محمود، ۱۳۸۳، درآمدی بر پیشگیری مقتدرانه پلیس از جرم، دانشگاه علوم انتظامی ناجا، سال ششم، شماره ۲.
۱۱. سخاوت، جعفر، جامعه شناسی انحرافات اجتماعی، چاپ اول، تهران، انتشارات پیام نور، ۱۳۷۴.
۱۲. صفاری، علی، مبانی نظری پیشگیری از وقوع جرم، تحقیقات حقوقی، ش ۳۳-۳۴، زمستان ۱۳۸۰، ۲۶۷-۳۲۱.
۱۳. عنصری فرد، عباس، جریحه دار کردن عفت عمومی در حقوق ایران، تهران، انتشارات مجد، ۱۳۸۵.
۱۴. مجلسی، محمدباقر، بحارالانوار، بیروت، مؤسسه الوفا، ط: الثانیه، ۱۴۰۳ ه. ق.



۱۵. نجفی ابرندآبادی، علی حسین، ۱۳۸۰، تقریرات جرم شناسی، تنظیم محمد علی بابایی، دوره دکتراى دانشگاه تربیت مدرس.
۱۶. نوربهار، رضا، زمینه حقوق جزای عمومی، تهران، کانون نشر وکلای دادگستری، ۱۳۶۹.
۱۷. عالی پور، حسن، ۱۳۸۴، جرایم مرتبط با محتوای سیاه فناوری اطلاعات، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، نشر سلسبیل.