فصلنامه مطالعات علوم اجتماعی
دوره ۷، شماره ۳، پائیز ۱۴۰۰
صفحات ۱۸۹-۱۷۷
Print ISSN: 2476-5074
www.uctjournals.com

بررسی جرم سرقت رایانه‌ای و تطبیق آن با سرقت سنتی در نظام حقوقی ایران

منیژه رنجبر
دانشجوی کارشناسی مهندسی کامپیوتر، دانشگاه پیام نور ساری، ساری، ایران

چکیده

یکی از کهن ترین و در عین حال پیشرفته ترین جرایم علیه اموال سرقت است؛که با ظهور رایانه و گسترش روز افزون آن در همه ی عرصه ها،از شکل ساده خود به صورت پیچیده و متنوع درآمده است.سارقان رایانه ای با نقض تدابیر امنیتی و ورود به رایانه دیگری میتوانند از راه روگرفت و برش به داده ها و اطلاعات اشخاص دست یابند. تبیین و تشریح ارکان تشکیل دهنده جرم سرقت رایانه ای و مقایسه با سرقت سنتی از جمله نحوه ربایش،لزوم یا عدم لزوم ارزش مالی داشتن داده ها،حرز محسوب شدن یا نشدن رایانه برای داده های موجود در آن و پرداختن به عنصر روانی و تحلیل و تشریح مجازات های اختصاص داده شده برای سرقت رایانه ای و و در نهایت وجوه اشتراک و افتراق جرم سرقت رایانه ای را با سایر عناوین مشابه از جمله اهدافی است که در این مقاله به آن می پردازیم.از آنجا که ماهیت تحقیق توصیفی-تحلیلی می باشد برای جمع آوری اطلاعات از روش کتابخانه ای و اسنادی استفاده شده است.بستر ارتکاب سرقت رایانه ای برخلاف سرقت سنتی که محیط فیزیکی است،فضای سایبر است.پس از بیان کلیات و مفاهیمی پیرامون سرقت رایانه ای وتبیین ارکان این جرم در کنار سرقت سنتی وتجزیه و تحلیل ضمانت اجراهای این جرم، نتایج بدست آمده عبارت است از اینکه سرقت رایانه ای جرمی کاملا مجزا از سرقت سنتی و سایر عناوین مشابه است.«داده ها» که موضوع این جرم هستند،ماهیتی کاملا جداگانه نسبت به «مال»،که موضوع سرقت سنتی است دارند؛و لازم نیست که دارای ارزش مالی باشند.وهمچنین از بین بردن تدابیر امنیتی و ورود به رایانه دیگری هتک حرز محسوب نمی شود.عنصر روانی نیز در این دو جرم یکی است کما اینکه در سرقت رایانه ای سوءنیت خاص یا قصد نتیجه برای تحقق جرم ضروری نیست. پس از بررسی واکنش های کیفری مقرر برای سرقت رایانه ای نتیجه ای که به دست می آید این است که اشخاص حقوقی نیز مورد مجازات قرار می گیرند.ودر نهایت فراوانی جرایم مشابهی که در رابطه با این نوع سرقت وجود دارد،نشان دهنده عدم کفایت ماده ۱۲ قانون جرایم رایانه ای برای پاسخگویی به این جرایم می باشد و توجه بیشتر قانونگذار را می طلبد.

واژه‌های کلیدی: سرقت رایانه‌ای، سرقت سنتی، جرم رایانه‌ای، فضای سایبر، نظام حقوقی.

۱- مقدمه

سرقت یا دزدی یکی از کهن ترین و گسترده ترین و در عین حال پیشرفته ترین جرایم بنیادی علیه حق مالکیت است که در تمام ادوار تاریخ ،به عنوان یک پدیده اجتماعی مجرمانه مورد تنفر و انزجار عمومی بوده و در قوانین و ادیان و اخلاق از آن به عنوان جرم و گناه و منکر یاد شده است. و همواره با عکس العمل شدید همراه بوده است سرقت نیز همچون جرایم دیگر، با پیشرفت جوامع بشری تحول یافته و از شکل ساده خود به صورت پیچیده و متنوع در آمده است. و سارقان برای ارتکاب این جرم از از اسباب و ابزار کاملتر و فنی تری استفاده نموده اند. پیداش رایانه و گسترش روز افزون آن در مراکز علمی ، اداری، تجاری، بانک ها و غیره صورت دیگری از این جرم را آورده است که علاوه بر تخصص و مهارت از ظرافت خاصی نیز برخوردار است (گلدوزیان، ۱۳۹۹).

یکی از سیاست های مهم قانونگذار در ایران، تصویب قانون جرایم رایانه ای و پیش بینی جرم سرقت رایانه ای در ماده ۱۲ آن می باشد، با این توضیح که « سرقت رایانه ای تنها در پیکره یک نشست در قانون جرایم رایانه ای جایگاه یافت و پس از آن در هیچ گامی، چشم ها را به سمت خود نکشاند و اندیشه ها را به سوی عنوانش نجنباند و بدین حال تصویب شد و هیچ صدایی برنخاست و نوشته ای پدید نیامد که این چه عنوان و ماده ای است؟ این از شگفتی‌های قانونگذاری در ایران است که مواد ۱۴ و ۱۵ که درباره محتویات مبتذل و مستهجن هستند، بی جهت بیشترین وقت و هزینه را در نشست ها از همان گام نخست می گیرند و در پایان نیز در جامعه به درستی نمود نمی یابند ولی ماده بسیار برجسته و با اهمیتی مانند ماده ۱۲ که درباره سرقت رایانه ای است در مدتی کوتاه پیش بینی می گردد و هیچ وقتی نمی یابد تا نقد شود یا از بودنش به نیکی یاد گردد.»" با بررسی و تحلیل ارکان جرم سرقت رایانه ای و مقایسه آن با سرقت سنتی به چند مسئله چالش بر انگیز دیگر پی می بریم: اول اینکه باید برای رفتار مجرمانه ربایش معنای عرفی آن را در نظر بگیریم تا بتوانیم آن را بر سرقت داده های رایانه ای در فضای سایبر بار کنیم. زیرا ربایش سایبری در قانون جرایم رایانه ای تنها به دو رفتار رو گرفت و برش در فضای سایبر اشاره دارد و نسبت به فضای بیرونی نگاهی ندارد. دومین چالش اینکه ارزش مال داشتن در سرقت سنتی مسئله ای است که بحث های فراوانی پیرامون آن شده است و عقیده عموم بر این است که موضوع سرقت سنتی باید دارای ارزش مالی باشد در همین راستا سرقت اشیایی مثل مشروبات الکلی و مواد مخدر سرقت محسوب نمی شود.ولی باید توجه داشت که علاوه بر اینکه قانون مدنی مال را تعریف نکرده است،سرقت محسوب نکردن این اعمال که عرفاً دارای ارزش مالی و قابل دادوستد هستند،باعث تجری مرتکبان آن می شود.ولی در سرقت رایانه ای در ماده ۱۲ به لزوم ارزش مالی داشتن داده (موضوع سرقت رایانه ای) اشاره نشده است و میتوان سرقت هر نوع داده‌ای را (با رعایت سایر شرایط) مشمول سرقت رایانه ای دانست.و سومین چالش در مورد سرقت رایانه ای این است که آیا تدابیر امنیتی لحاظ شده برای رایانه حرز داده ها و اطلاعات محسوب می شود؟و آیا میتوان ورود به رایانه و گذر از این تدابیر را هتک حرز فرض کرد و سارق را به سرقت مستوجب حد محکوم کرد؟که با توجه به استفتائات فقهی که از مراجع عظام در این رابطه وجود دارد و همچنین تفاوت این جرم با سرقت سنتی و همچنین حکومت قاعده «دراء» پاسخ به این سؤال منفی است. به عبارتی دیگر رایانه برای اطلاعات و داده ها حرز محسوب نمی شود. لذا در این تحقیق بر آنیم تا با بررسی و تبیین ارکان جرم سرقت رایانه ای و بررسی جایگاه آن در قانون جرایم رایانه ای، به تطبیق این جرم با سرقت سنتی بررسی چالش های آن به خصوص از لحاظ عنصر ربایش و لزوم ارزش مالی‌داشتن بپردازیم. و در نهایت این جرم را با سایر عناوین مشابه بسنجیم و پیشنهادات و راهکارهایی پیشگیری از آن را بیان کنیم.

۲- ادبیات تحقیق

۲-۱- سرقت رایانه‌ای

در قوانین و منابع موجود به صراحت تعریفی از سرقت رایانه ای نشده است،ولی با توجه به نظر متخصصان این رشته وبا توجه به قوانین ملی و بین المللی موجود و همچنین با توجه به تعریفی که از سرقت سنتی شد می توان گفت: سرقت رایانه ای عبارتست از ربایش داده ها و اطلاعات متعلق به دیگری ایا به عبارتی دیگر ارو گرفت و برش غیر مجاز داده های متعلق به

دیگری».به نظر می رسد محدوده چنین سرقتی از سرقت سنتی وسیع تر باشد،چرا که اطلاعات و داده هایی که جنبه مالی ندارند نیز در بر می گیرد مثل اینکه شخصی رمز عابر بانک یا اطلاعات سری رمز دار دیگری را از شبکه رایانه ای بدزدد. به نظر می رسد که چنین نظری درست نیست ، زیرا چیزی که اصالتا مالیت نداشته باشد داخل در مفهوم سرقت نیست عموم فقها نیز عقیده دارند که یکی از عناصر اصلی سرقت سال است و چیزی که مالیت نداشته باشد داخل در عنوان سرقت نیست.ولی با کمی تعمق در می یابیم که این نظر نمی تواند درست باشد، زیرا سبب می شود برخی موارد که مالی نیستند، ولی از جهات دیگر مهم تلقی می شوند، از محدوده قانون جزا خارج شوند. به عنوان مثال داده های مربوط به سلامتی و خصوصیات و راشی، که هر چند سالی نیستند و سوء استفاده و انتشار آنها فقط ممکن است بر خلاف تمایل شخص بوده و موجب سرافکندگی اجتماعی با عوارض اجتماعی دیگری برای او شود،یا داده های اعتقادی حزبی یا فردی که در رایانه یا ایمیل شخصی ذخیره شده است و یا داده های شخصی مربوط به محکومیت های کیفری که فرد با ورود به سیستم رایانه ای اداره تشخیص هویت، این اطلاعات را بر می دارد. چنین مواردی هر چند غیر مالی هستند ولی در جای خود و برای صاحبان آنها خیلی مهم و با اهمیت تلقی می شوند. البته دلیل دیگری که برای عدم لزوم مالیت داشتن داده های موضوع رایش در سرقت رایانه ای وجود دارد همان ماده ۱۲ قانون جرایم رایانه ای است که تعبیر اداده های متعلق به دیگری را به صورت مطلق به کار برده و آن را مقید به داده های مالی نکرده است. بنابر این شبهه ای وجود ندارد و واضح است که در سرقت رایانه ای،موضوع جرم هر داده ای می تواند باشد و مهم نیست که داده ها دارای ارزش مالی باشند یا نباشند.بلکه همین که داده ای متعلق به شخص دیگری باشد با جمع سایر شرایط رو گرفت با برش آنها سرقت رایانه ای محسوب می شود. البته در مباحث بعدی بیشتر به این موضوع می پردازیم. بنابراین در اینجا می توان گفت اولین وجه مشترک این سرقت باسرقت سنتی در تعریف،وجود عنصر ربودن و رایش در هر دو سرقت است که توصیف آن رو در مباحث آتی بیان میکنیم.دومین وجه مشترک این دو سرقت در تعریف،مخفیانه بودن آن است.(البته در لایحه قانون مجازات جدید این قید حذف شده است و سومین وجه مشترک در تعریف این دو سرقت، متعلق به دیگری بودن است. در اینجا به بیان همین مطالب بسنده میکنیم و تشریح و تحلیل بیشتر وجوه اشتراک و اختلاف بین این دو نوع سرقت را در فصول ومباحث آتی بیان می نمائیم (پاکزاد، ۱۳۹۸).

۲-۲- رکن قانونی جرم سرقت رایانه ای

همانطور که می دانیم پدیده های حقوقی، از جمله جرم، امری اعتباری هستند که بر مبنای قانون شکل می گیرند. در نظام حقوقی کشور ما، اعتبار قانونگذار، یعنی پیش بینی عنوان مجرمانه و مجازات آن، از ارکان ماهوی تشکیل دهنده جرم محسوب می شود و مانند ارکان مادی و معنوی برای تحقق جرم ضروری است.بنابراین لزوم رعایت اصل قانونی بودن جرایم و مجازاتها» و اتکای آن به قاعده ی عقلی قبح عقاب بلا بیان چنان بدیهی است که ما را از اقامه دلیل منع می کند. در مورد رکن قانونی جرم سرقت سنتی، قانونگذار ما در قانون مجازات اسلامی چندین ماده را برای حالات مختلف سرقت پیش بینی کرده است. که به شرح زیر است:

الف)مواد ۱۹۷ تا ۲۰۳ ذیل عنوان «حد سرقت»،در باب هشتم از کتاب دوم قانون مجازات اسلامی(۱۳۷۰)که در باب سرقت مستوجب حد می‌باشد.

حالات مختلف سرقت پیش بینی کرده است. که به شرح زیر است:

الف) مواد ۱۹۷ تا ۲۰۳ ذیل عنوان «حد سرقت ، در باب هشتم از کتاب دوم قانون مجازات اسلامی (۱۳۷۰) که در باب سرقت مستوجب حد می باشد.

ب) مواد ۶۵۱ تا ۶۶۷ در فصل بیست و یکم از کتاب پنجم قانون مجازات اسلامی (۱۳۷۵) که به ترتیب در باب «سرقت جمعی شبانه و مسلحانه توأم با آزار »، «سرقت مقرون به آزار»، «راهزنی»، «سرقت جمعی شبانه و مسلحانه)»، «شروع به سرقت مشدد»، «سرقت توأم با یکی از علل مشدده»، «کیف زنی و جیب بری »، «سرقت در شرایط بحرانی»، «سرقت وسایل و متعلقات تأسیسات عمومی»، «استفاده غیر مجاز از آب، برق، تلفن و گاز »، «سرقت تعزیری ساده)، «مداخله در اموال

مسروقه»، «مداخله در اشیاء توقیف شده »، «تهیه و یا ساخت هر نوع وسیله برای ارتکاب جرم»، «ربودنی که سرقت نیست»، «تکرار جرم سرقت»، «تکلیف به رد عین یا مثل یا قیمت مال مسروقه یا ربوده شده می باشد.

ج) ماده ۱۸۵ در باب هفتم از کتاب دوم قانون مجازات اسلامی (۱۳۷۰) که در باب «کیفیت محارب تلقی شدن سارق مسلح» می‌باشد.

د) مواد ۵۴۴ تا ۵۴۵ در فصل ششم از کتاب پنجم قانون مجازات اسلامی (۱۳۷۵) که به ترتیب در مورد «اهمال مستحفظ» منتهی به سرقت یا تخریب یا مدارک محفوظ در اماکن دولتی و سرقت یا تخریب یا معدوم نمودن اسناد و مدارک محفوظ در اماکن دولتی و یا در نزد مأمورین دولتی» می باشد (ابراهیم‌زاده، ۱۳۹۹).

ه) مواد ۶۸۳ و ۶۸۴ در فصل بیست و پنجم از کتاب پنجم قانون مجازات اسلامی (مصوب ۱۳۷۵) که این دو ماده نیز در باب «نهب و غارت و اتلاف اموال به نحو قهر و غلبه» و «چرانیدن و خراب کردن، خشکانیدن یا تضییع کردن باغ غیر از طریق سرقت آب و غیره می باشد. همانطور که ملاحظه می شود قانونگذار در مورد سرقت سنتی چندین ماده پیش بینی و برای حالات مختلف آن جرم انگاری نموده در حالی که تنها ماده قانونی که جرم سرقت رایانه ای را پیش بینی نموده و برای آن مجازات تعیین کرده است (موذن‌زادگان، ۱۳۹۵).

در مورد سرقت رایانه ای توجه بیشتر قانونگذار را می طلبد.در اینجا نکته ای که باید به آن اشاره کرد این است که مطابق ماده ۵۵ قانون جرایم رایانه ای:«شماره مواد (۱) تا (۵۴) این قانون به عنوان مواد (۷۲۹) تا (۷۸۲) قانون مجازات اسلامی (بخش تعزیرات یا عنوان فصل جرایم رایانه ای منظور و شماره ماده (۷۲۹) قانون مجازات اسلامی به شماره (۷۸۳) اصلاح گردد. بنابراین باید از ماده ۱۲ قانون جرایم رایانه ای به عنوان ماده ۷۴۰ قانون مجازات اسلامی یاد گردد. از آنجایی که قانونگذار در ماده ۷۲۷ قانون مجازات اسلامی موارد جرایم قابل گذشت را تعیین کرده،و مواد راجع به سرقت سنتی را در این ماده نیاورده،سرقت سنتی در بیشتر موارد از جمله جرایم غیر قابل گذشت می باشد ، تنها در مورد سرقت مستوجب حد است که قبل از شکایت مالباخته نزد قاضی جنبه حق الناسی و قابل گذشت دارد و بعد از شکایت نزد قاضی جنبه حق الهی و غیر قابل گذشت پیدا می کند.در مورد سرقت رایانه ای نیز با توجه به شباهتی که در این زمینه با سرقت سنتی دارد و همچنین با توجه به رابطه‌ای که این جرم با نظم عمومی دارد و از آنجایی که این جرم (ماده ۷۴۰ قانون مجازات اسلامی در شمار مواد ماده‌ی ۷۲۰ قانون مجازات نیامده است، این جرم نیز از جمله جرایم غیر قابل گذشت محسوب می شود (گلدوزیان، ۱۳۹۹).

۳-۲- اینترنت و فضای مجازی

همانطور که می دانیم اینترنت شبکه شبکه ها است. با توجه به محدودیت هایی که ایجاد یک شبکه در مقیاس گسترده به دنبال داشت،فناوری «ارتباط بین شبکه ای» پا به عرصه وجود گذاشت. دستاورد اصلی این فناوری امکان ایجاد ارتباط بین دو یا چند شبکه بود که در نهایت به تولد اینترنت به عنوان یک مجموعه ارتباط بین شبکه ای گسترده رده در تمام دنیا با یک زبان قراردادی مشترک منتهی گردید. پس اینترنت شامل تعداد زیادی کامپیوتر است که به وسیله مخابراتی و از طریق خطوط سیمی،ماهواره ای یا مایکروویو به هم متصل شده اند و با یک زبان یا قرارداد مشترک با هم ارتباط دارند».با افزودن یک جزء دیگر به تعریف بالا،تعریف کاملتر خواهد شد و آن «دروازه شبکه ای» است،که دستگاهی است که در محل اتصال بین دو شبکه واقع می شود و در ضمن برقراری امکان تبادل اطلاعات بین دو شبکه، اطلاعات را در قالب زبان قراردادی مشترک از پیش تعریف شده تنظیم می کند برای کلیه رایانه های آن دو شبکه قابل فهم شوند.بنابراین در تعریف اینترنت باید گفت،اینترنت «مجموعه جهانی شبکه ها و دروازه های شبکه ای است که با استفاده از یک زبان قراردادی مشترک با یکدیگر ارتباط برقرار می کنند. چنین شبکه عظیمی با این قابلیت های باورنکردنی توسط «آژانس پروژه های تحقیقاتی پیشرفته»وزارت دفاع آمریکا پایه گذاری شد.بر این مبنا که اولا تبادل اطلاعات بین مرکز تحقیقاتی و محققان این آژانس به سهولت و در کمال امنیت صورت پذیرد و ثانیا در صورت تهاجم نظامی به آمریکا با ایجاد مراکز اطلاعات نظامی در چند نقطه آن کشور و اتصال آنها از طریق یک شبکه رایانه ای،در صورت قطع ارتباط هر یک از مراکز موصوف،اطلاعات راهبری نظامی از سایر مراکز قابل دریافت

باشد ولذا شبکه ای به نام «آرپانت» در سال ۱۹۶۰ ایجاد شد و به تدریج با پیوستن شبکه های دیگر در سراسر دنیا به آن اینترنت شکل گرفت که مشخصه اصلی آن نسبت به سایر «ارتباطات بین شبکه ای»،استفاده از زبان قراردادی مشترک به نام «پروتکل کنترل انتقال یا پروتکل اینترنت» است که توسط وزارت دفاع آمریکا ارائه شده‌است (فضلی، ۱۳۹۸).

به هر تقدیر با حصول این امر و دسترسی به شبکه جهانی اینترنت و به تعبیر دیگر ایجاد و اتصال به شاهراههای الکترونیکی،بیش از پیش بر سرعت مبادله اطلاعات در زمینه های مختلف اقتصادی،سیاسی،اجتماعی و فرهنگی افزوده شده است و ساختار های جدید روابط متفاوتی را ایجاد کرده است که نیاز به نگاه جدید و اندیشه های نو حقوقی دارد.بنابراین ارتباط رایانه ای انقلابی در فرایند ارتباطات و به لحاظ آن در نظام حقوقی و اجتماعی و جهان صنعتی ایجاد کرده و خواهدکرد.

بر اثر پیشرفت و توسعه فناوری اطلاعات، امنیت ملی و اقتصادی کشور وابستگی روز افزونی به فناوری اطلاعات و زیر ساختهای اطلاعاتی پیدا می کند که هسته اصلی آن اینترنت است.این شبکه امروز شامل میلیونها رایانه است که از طریق آنها خدمات و فعالیت های سازنده و مخرب بسیاری صورت می پذیرد. آسیب هایی که از ناحیه این شبکه می تواند صورت گیرد از جمله عبارتند از :از کار افتادن زیر ساختهای اساسی، از کار افتادن خدمات اجتماعی بحران اقتصادی، تهاجم فرهنگی، تسهیل زمینه ظهور و توسعه انواع جرائم و غیره که می تواند از طرق مختلف همانند نفوذ ویروسها کرمها، اسبهای تراوا و هکرها هک کردن انجام شود (پاکزاد، ۱۳۹۸).

۴-۲- موارد تشدید و تخفیف مجازات سرقت رایانه ای

قانونگذار در فصل هشتم قانون جرایم رایانه ای بر اساس مواد ۲۶ و ۲۷ عوامل مشدده کیفر جرایم رایانه ای را پیش بینی نموده است. که مطابق آن می توان جرم سرقت رایانه ای را نیز تشدید کرد.

بر اساس ماده ۲۶ قانون مذکور در موارد زیر، حسب مورد مرتکب به بیش از دو سوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد.

الف) هر یک از کارمندان و کارکنان اداره ها سازمان ها یا شوراها و یا شهرداری ها و مؤسسه و شرکت های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه هایی که زیر نظر ولی فقیه اداره می شوند و دیوان محاسبات و مؤسسه هایی که با کمک مستمر دولت اداره می شوند و یا دارندگان پایه قضایی و به طور کلی اعضاء و کارکنان قوای سه گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیر رسمی به مناسب انجام وظیفه مرتکب جرایم رایانه ای شده‌باشند.

ب. متصدی یا متصرف قانونی شبکه های رایانه ای یا مخابراتی که به مناسب شغل خود مرتکب جرم رایانه‌ای شده‌باشد.

ج. دادها یا سامانه های رایانه ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه دهنده خدمات عمومی باشد.

د. جرم به صورت سازمان یافته ارتکاب یافته باشد.

ه. جرم در سطح گسترده ای ارتکاب یافته باشد (خرم‌آبادی، ۱۳۹۶).

این عوامل مشدد را به طور کلی می توان به چهار گروه تقسیم کرد. اولین عامل مدخل در این زمینه شخصیت حقوقی مرتکب جرم موضوع بند الف و ب ماده ۲۶ می باشد. به این معنا که چنانچه مثلا در مورد سرقت، سارقان از کارگزاران دولت و به طور کلی قوای سه گانه یا دستگاه‌ها و مؤسسات و شرکتهای وابسته به دولت یا آنهایی که به کمک مستمر دولت اداره می شوند و یا نهادهای انقلابی و بنیاد ها و مؤسسه هایی که زیر نظر ولی فقیه اداره می گردند و نیز مأموران به خدمت عمومی اعم از رسمی و غیر رسمی باشد و به مناسب انجام وظیفه مرتکب جرم مزبور شود، مجازات وی تشدید گردیده و به میزان بیش از دوسوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد. همچنین است در صورتی که سارق متصدی یا متصرف قانونی شبکه های رایانه ای یا مخابراتی باشد و به مناسب شغل خویش مرتکب این جرم گردیده باشد (میرمحمد صادقی، ۱۳۹۹).

سؤالی که ممکن است در اینجا پیش آید اینست که چنانچه نامبرده در حین انجام وظیفه «ولی نه به مناسب انجام وظیفه وشغل خویش مرتکب جرم رایانه ای مثلا احد از مستخدمین یک اداره یا آبدارچی آن با استفاده از لب تاب خود یا دیگری

مرتکب سرقت رایانه ای گردد. آیا در این قرض نیز مجازات وی تشدید می شود؟ در پاسخ اجمالا باید گفت تفسیر مضیق قوانین و تفسیر به نفع منهم چنین امری را اقتضا نمی کند.

اما دومین عامل مؤثر در تشدید کیفر را باید موضوع و وسیله جرم دانست. بدین توضیح که چنانچه داده ها یا سامانه های رایانه ای یا مخابراتی، قانونا متعلق به دولت یا نهاد ها و مراکز ارائه دهنده خدمات عمومی محسوب شود کیفر مرتکب به نحو مذکور تشدید می گردد (تحریری، ۱۳۹۳).

سومین عامل اثر گذار در شدت یافتن کیفر نفس چگونگی وقوع جرم می باشد، به این شرح که اگر جرم سرقت ارتکابی در سطح گسترده یا به صورت سازمان یافته واقع شود مجازات مرتکب به نحو مذبور تشدید می شود. عامل چهارم که می تواند در این رابطه نقش داشته باشد مسئله تکرار جرم است که در گفتار بعدی آن را بیان می نمائیم.

در مورد تخفیف مجازات در ماده ۲۲ قانون مجازات اسلامی آمده است: دادگاه می تواند در صورت احراز جهـات مخففه مجازات تعزیری و یا باز دارنده را تخفیف دهد و یا تبدیل به مجازات از نوع دیگری نماید که مناسبتر بـه حـال منهم باشد، جهات مخففه عبارتند از:

الف) گذشت شاکی یا مدعی خصوصی.

ب اظهارات یا راهنمایی های متهم که در شناختن شرکاء و معاونان جرم و یا کشف اشیایی که از جرم تحصیل شده است موثر باشد.

ج) اوضاع یا احوال خاصی که منهم تحت تأثیر آنها مرتکب جـرم شـده است. از قبیل: رفتار و گفتار تحریک آمیز مجنی علیه یا وجود انگیزه شرافتمندانه در ارتکاب جرم.

د) اعلام منهم قبل از تعقیب و یا اقرار او در مرحله تحقیق که مؤثر در زمینه کشف جرم باشد.

و)وضع خاص متهم و یا سابقه ی او.

ه) اقدام یا کوشش متهم به منظور تخفیف اثرات جرم و جبران زیان ناشی از آن.

در مورد امکان تخفیف مجازات در مورد سرقت رایانه ای باید گفت همانطور که قبلا نیز اشاره کردیم، قانونگذار در ماده ۵۵ قانون جرایم رایانه ای این جرم را جزء جرایم تعزیری آورده و شمار ماده را به ماده ی ۷۴۰ قانون مجازات اسلامی تغییر داده است.بنابراین از آنجایی که بر اساس ماده فوق قانونگذار می تواند در مورد جرایم تعزیری و بازدارنده تخفیف را اعمال کند،در مورد سرقت رایانه ای نیز با توجه با حالات مختلفی که در ماده آمده است،میتواند مجازات سارق رایانه ای را تخفیف دهد.البته در مورد سرقت سنتی تعزیری نیز چنین است. و می توان مجازات را تخفیف داده تنها قانونگذار در تبصره ماده ۶۶۶ قانون مجازات اسلامی تکرار جرم سرقت را عاملی دانسته است که دیگر نمی توان در مورد سارق جهات مخففه را اعمال کرد. این ماده مقرر می دارد: در تکرار جرم سرقت در صورتی که سارق سه فقره محکومیت قطعی به اتهام سرقت داشته باشد دادگاه نمی تواند از جهات مخففه استفاده نماید (فضلی، ۱۳۹۸).

۳- فرضیه‌های تحقیق

فرضیه شماره ۱: جرم سرقت رایانه‌ای، جرم جدیدی است و با سرقت سنتی مقرر در قوانین کیفری متفاوت است.

فرضیه شماره ۲: تفاوت و شباهت‌هایی بین جرم سرقت رایانه‌ای و سرقت سنتی و سایر عناوین مشابه وجود دارد.

۴- روش تحقیق

با توجه به ماهیت موضوع، نقطه تأکید این تحقیق مطالعاتی است که با استفاده از روش توصیفی به تشریح ابعاد مختلف جرم سرقت رایانه ای پرداخته است. تأکید بر فعالیت ها به ویژه قوانین و دستور العمل ها، برای جمع آوری اطلاعات مورد نیاز، استفاده از تحلیل محتوا را اجتناب ناپذیر ساخته است. استدلال های منطقی و عقلی از منابع به دست آمده با استفاده و تکیه بر اصول شناخته شده حقوقی مورد وفاق دکترین حقوقی و اصول کلی تبین شده در دانش اصول، در جهت حصول به نتیجه

مطلوب بر اساس روش تحلیل حقوقی، ضمن اینکه با بکارگیری سیستمها و سامانه های رایانه ای به عنوان مهمترین بستر ارتکابی جرایم رایانه ای و بررسی پرونده های کیفری موجود در این زمینه در صدد درک بهتر و تفسیر و تجزیه و تحلیل جرم سرقت رایانه ای بر آمده ایم .بنابراین در این تحقیق روش اسنادی و مقایسه ای (با ماهیتی توصیفی - تحلیلی) مورد استفاده قرار گرفته است. به دلیل اینکه برای گردآوری ادبیات موضوع از روش مطالعه کتاب خانه ای و استادی استفاده شده است، جامعه آماری وجود ندارد و با توجه به اینکه جامعه آماری وجود ندارد نمونه گیری صورت نمی گیرد.

۵- یافته‌های تحقیق

سرقت اسرار تجاری علاوه بر محیط فیزیکی که مشمول مقررات راجع به سرقت سنتی می شود، در فضای سایبر نیز امکان ارتکاب این جرم وجود دارد. از آنجایی که ابستر مبادلات الکترونیکی» تنها بخش کوچکی از فضای سایبر را تشکیل می دهد، این ماده با این اشکال اساسی مواجه است که بستر ارتکاب جرم را بسیار محدود ساخته است.

ایراد غیر قابل مسامحه دیگری که در اینجا وجود دارد و نشان دهنده ی عدم مطالعات کافی و دقیق در این زمینه است مربوط می شود به قربانی سرقت اسرار تجاری. در ماده ۶۴ قانون تجارت الکترونیکی، فقط اسرار تجاری بنگاهها و مؤسسات یعنی تنها اشخاص حقوقی مورد حمایت قانونگذار قرار گرفته اند، در حالی که این از بدیهیات است که نه حقیقی نیز نیازمند حمایت و پشتیبانی می باشند که فقط اسرار تجاری اشخاص حقوقی بلکه اسرار تجاری اشخاص البته به این نکته در تعریف سرقت اسرار تجاری اشاره نمودیم.

با توجه به همسانی عنوان سرقت رایانه ای و سرقت اسرار تجاری، ممکن است این چنین برداشت شود که این جرایم یکسانند و می توان هر دوی آنها را تحت عنوان سرقت رایانه ای بر طبق ماده ۱۲ قانون جرایم رایانه ای مجازات کرد، ولی پس از تحلیل ارکان جرم سرقت رایانه ای و مقایسه آن با جرم سرقت اسرار تجاری به این نتیجه می توان دست یافت که این جرایم کاملا از هم متمایزند. درست است که سرقت اطلاعات مالی و تجاری در فضای سایبر از طریق رو گرفت یا برش انجام می شود. ولی باید این نکته را نیز در نظر داشت که این تنها مربوط به بخشی از جرایم سرقت اطلاعات مالی و تجاری می شود که در فضای سایبر اتفاق می افتد و نیز انگیزه های مرتکبین این دو جرم با هم تفاوت دارد. در واقع سارق اطلاعات مالی و تجاری دارای انگیزه های مالی است ولی در مورد رو گرفت یا برش غیر مجاز تنها انگیزه های مالی وجود ندارد. همچنین رفتار سرقت رایانه ای فقط شامل رو گرفت یا برش غیر مجاز می باشد، در حالی که همانطور که می دانیم در مورد سرقت اطلاعات مالی و تجاری بخشی از رفتار ممکن است شامل این موارد بشود و قسمتی از جرم در محیط فیزیکی و فضای بیرونی اتفاق می افتد (رابینز، ۱۳۹۸).

سرقت اطلاعات مالی و تجاری به شیوه های گوناگونی ارتکاب می یابد که از جمله موارد رایج آن می توان به افشا و دسترسی به شماره حساب های مالی، مشخصات فردی مثل کد های امنیت اجتماعی و کدملی، دستیابی به رمز عبور و نام کاربری ایمیل اشخاص، دسترسی به کارتهای بدهی و کارت های دستگاههای خودپرداز و ... اشاره کرد. البته شیوه های تخصصی تری نیز برای ارتکاب سرقت اطلاعات مالی و تجاری وجود دارد که در اینجا به چند مورد آن به طور مختصر اشاره خواهیم کرد.

الف) صید اطلاعات

صید اطلاعات مالی از طریق ارسال یک ایمیل جعلی انجام می شود.که بر اساس آن وانمود می کند که یک بانک آنلاین یا مثلا یک پایگاه پرداخت وجه و یا انجام مزایده است. این ایمیل کاربر را به سوی یک پایگاه داده ای تقلبی هدایت می کند که ظاهر آن نشان می دهد که شخص به همان پایگاه داده ی قانونی موردنظر خود وصل شده است همچنین این پایگاه در ادامه ادعا می کند که کاربر باید اطلاعات شخصی خود را به روز کند. سپس این اطلاعات مسروقه در سایر اعمال متقلبانه مثل سرقت هویت و یا کلاهبرداری آنلاین به کار می رود. همچنین برخی از برنامه های «اسب تروا به منظور جاسوسی در مورد کاربران در حالیکه به شبکه متصل هستند، به کار می رود تا اطلاعات سری را برای انتقال به بیرون از پایگاه داده هدایت کند.

ب) تقلب در منشأ مراسلات الکترونیکی

تقلب در منشأ مراسلات الکترونیکی در لغت به معنای فریب دادن و تحمیق است. از لحاظ اصطلاحی تعاریف متعددی از آن شده است. در تعریف عام عبارتست از عملی که با استفاده از آن می توان طوری وانمود کرد که انتقالات از طریق یک کاربر غیر مجاز است و به عنوان مثال یک کاربر غیر مجاز برای دستیابی به یک کامپیوتر یا یک شبکه استفاده می‌کند (مکارم شیرازی، ۱۳۹۳).

ج) مهندسی اجتماعی

حملات مهندسی عبارتست از روند نفوذ به سیستم های رایانه ای از طریق کاربرد حیله های گوناگون در خصوص افراد جهت افشای کلمات عبور و اطلاعات مربوط به موار آسیب‌پذیر شبکه (فضلی، ۱۳۹۳).

پس از مروری بر مطالب پیش گفته متوجه جای خالی ماده ای در قانون جرایم رایانه ای که به جرم انگاری سرقت اطلاعات مالی و تجاری بپردازد احساس خواهد شد. و همچنین از آنجایی که ممکن است قسمتی از این جرم در فضای بیرونی رخ دهد، لازم است قانون گذار تدابیری را اتخاذ کند و قوانینی را وضع نماید تا به موجب آن سرقت اطلاعات مالی اشخاص در فضای غیر سایبر مثل موردی که شخصی برگه ی حاوی رمز عبور دستگاه خودپرداز بانکی دیگری را می رباید جرم انگاری شود زیرا از آنجا که می دانیم صرف ربودن این برگه مطابق با قوانین کیفری فعلی قابل تعقیب و مجازات نیست، هر چند با کمی تعمق می توان به اهمیت این عمل پی برد که چه بسا ممکن است ضرر و زیان های مالی غیر جبرانی برای قربانی به دنبال داشته باشد. همچنین لازم است اقداماتی انجام شود که امکان تحت تعقیب و پیگرد قرار گرفتن سارقان اطلاعات مالی و تجاری فراهم شود. البته این مشکل تمامی جرایم ارتکابی در فضای سایبر است که فراوانی رقم سیاه این جرم تأکیدی بر این گفته است.

بررسی جرم دسترسی غیر مجاز در ارتباط با سرقت رایانه ای

دسترسی غیر مجاز ۲ عبارت است از رخنه غیر قانونی به سامانه رایانه ای حفاظت شده. گاه گاه در زبان فنی هک یا رخنه گری گفته می شود؛ با این حال هک برابر با دسترسی غیر مجاز نیست و واژه ای نیست که تنها چهره سرزنش پذیر داشته باشد. هک به شیوه فنی رخنه به سامانه رایانه ای گفته می شود که به خودی خـود بـزه نیست و در میان رایانه دانان همچون یک هنر شناخته می شود. قانونگذاران نیز به این چهره فنی هک روی نموده و از این عنوان در قانون ها بهره نجسته اند، همچنانکه در ماده ۲ کنوانسیون بوداپست، از عنوان الدسترسی غیر قانونی بهره گرفته شده‌است. به هر حال اگر رخنه گری بدون اجازه و نسبت به سامانه دیگری که حفاظت شده است، انجام شود، دسترسی غیر مجاز خواهد بود (موذن‌زادگان، ۱۳۹۷).

نکته که درباره دسترسی گفتنی است این است که آیا با توجه به اینکه بیشتر بزه های رایانه ای از رهگذر دسترسی غیر مجاز انجام می یابند، می توان گفت که دسترسی مقدمه لازم دیگر بزه هاست. به عبارت دیگر اگر کسی به رایانه دیگری رخنه کرد و پس از آن داده اش را تخریب کرد یا داده های وی را از جایگاهش ربود و یا اینکه از رهگذر پخش ویروس به سامانه یک بانک وارد شد و با به دست آوردن شماره حساب ها، پولی را به حساب خود واریز نماید می توان گفت که دسترسی مقدمه لازم تخریب داده، سرقت رایانه ای و کلاهبرداری مرتبط با رایانه است؟ قانونگذار ایران درباره این قضیه که رفتار بزهکارانه ای مقدمه لازم جرم دیگری باشد، خاموش است و از این حیث نمی توان به راحتی از رهگذر مقدمه لازم، بتوان از کنار یک عنوان مجرمانه گذشت و آن را بزه ندانست. پیش از بررسی دسترسی غیر مجاز به عنوان مقدمه لازم جرایم رایانه ای، باید گفت که با توجه به مواد قانونی یا حقوق کیفری می توان گفت که در چهار حالت اگر رفتاری با رفتار دیگر همراه گردد که هر دو از دید قانون کیفری بزه باشند، امر تعدد جرم (معنوی و مادی) حاکم نخواهد بود و در هر حال بین آن دو رفتار تنها یک مورد بزه بوده و کیفر شدنی خواهد بود. این چهار حالت به طور ضمنی از بخش پایانی ماده ۴۷ قانون مجازات اسلامی بر می آید. بر پایه این بخش هرگاه مجموع جرائم ارتکابی در قانون عنوان جرم خاصی داشته باشد مرتکب به مجازات مقرر در قانون محکوم می گردد، به سخن دیگر مرتکب تنها به کیفری پیش بینی شده در ماده محکوم خواهد شد. با بررسی قانون ها، چهار حالت گفته

شده به شرح زیر است: حالت نخست هنگامی است که در رفتار مجرمانه به جهت یگانگی موضوع و شرایط همسان با هم انجام می شوند. مانند تهب و غارت و اتلاف موضوع ماده ۶۸۳ قانون مجازات اسلامی.

هرچند هم بتوان نهب و اتلاف را در یک معنا دانست ولی غارت به معنی ربایش آشکاره و پورش گونه است و از این رو در زیر سرقت جا می گیرد. در اینجا تخریب و سرقت با هم یک عنوان مجرمانه دانسته و اگر یکی از مرتکبین هـر دو رفتار را هم انجام داده باشد تنها به یک کیفر یعنی حبس از دو تا پنج سال محکوم خواهند شد. حالت دوم هنگامی است که جرمی خود به عنوان یکی از قسمت های رکن مادی بزه دیگر مطرح گردد. بر پایه ماده ۶۷۴ ، تلف کردن یکی از رفتارهایی است که خیانت در امانت آن رخ می دهد. حال اگر امین، به شیوه از میان بردن مال مورد امانت، به امانت گذار خیانت کند، تنها یک بژه انجام داده است و آن خیانت در امانت است هر چند بر پایه ماده ۶۷۷ تلف عمدی خود به تنهایی بژه به شمار می رود. دلیل اینکه اینجا تعدد معنوی بنیاد نمی گیرد، این است که رفتار موضوع ماده ۶۷۷ یعنی تلف یا از بین بردن، خود جزیی از رکن مادی خیانت در امانت شده و ویژگی سپردن شدن مال و امین بودن مرتکب سبب می گردد تا رفتار تلف کردن از عنوان بزهکارانه اتلاف عمدی به خیانت در امانت رخ نماید (جلالی فراهانی، ۱۳۹۴).

حالت سوم هنگامی است که جرمی توسط رفتار دیگری رخ دهد که این رفتار بر پایه قانون، عنوان مجرمانه دارد ولی به جهت واسطه بودن، جرم جداگانه ای به شمار نمی رود. برای نمونه طبق بند الف ماده یک قانون مجازات اخلالگران در نظام اقتصادی کشور، اخلال در نظام پولی یا ارزی کشور از طریق قاچاق عمده ارز یا ضرب سکه قلـب یـا جـعـل اسکناس یا وارد کردن یا توزیع نمودن عمده آنها اعم از داخلی و خارجی و امثال آن، جرم محسوب می گردد. در این بند و نیز بندهای دیگر این ماده، بزه اخلال در نظام اقتصادی از رهگذر رفتارهایی رخ می دهد که خود بزه اند. از این رو هر کس از طریق جعل اسکناس، اخلال در نظام اقتصادی پدید آورد، گویی دو بزه جعل اسکناس و اخلال در نظام اقتصادی را انجام داده است. با این حال در اینجا جعل اسکناس نمی تواند به جداگانه ای باشد، بلکه همچون واسط اخلال در نظام اقتصادی است. به سخن دیگر عنوان مجرمانه در اینجا اخلال از طریق جعل اسکناس است نه جعل اسکناس و اخلال در نظام اقتصادی و همین نشان می دهد که جعل اسکناس به عنوان یکی از پاره های رکن مادی اخلال در نظام اقتصادی مطرح می شود. هر چند این حالت همسـان بـا حـال دوم است ولی بایـد یـاد داشت در حالت دوم یک رفتار رخ می دهد و در حالت سوم دو رفتار، دو رفتار در حالت سوم یکی جعـل و دیگری اخـلال است. همچنین نباید پنداشت که در اینجا اخلال نتیجه است، بلکه مختل شدن نتیجه است و خود اخلال از باب متعـدی بوده و به معنای مختل کردن است (نوربهاء، ۱۳۹۷).

حالت چهارم هنگامی است که بزهی مقدمه لازم بزه دیگر باشد. این حالت را می توان به طور ضمنی از بخش پایانی ماده ۴۷ برداشت کرده با این حال بیشتر چهره نظری داشته که در رویه قضایی نیز گاه گاه به آن عمل شده است. از این رو باید آن را به طور در همان مورد خاص تفسیر کرد. ویژگی مقدمه لازم بودن در حالتی سبب می گردد تا رفتار مقدمه بزه نباشد که نوعی باشد نه موردی و پرونده ای. به سخن دیگر هرگاه و در هر جایی یک بزه توسط یک شخص ارتکاب یابد، مقدمه اش انجام بزه دیگر است. روشن است با نوعی دانستن مقدمه، موردهای آن بسیار اندک است؛ برای نمونه، بر پایه ماده ۴۹۸ «هر کس با هر مرامی، دسته، جمعیت یا شعبه جمعیتی بیش از دو نفر در داخل یا خارج از کشور تحت هر اسم با عنوانی تشکیل دهد یا اداره نماید که هدف آن برهم زدن امنیت کشور باشد و محارب شناخته نشود به حبس از دو تا ده سال محکوم می شود. در اینجا اگر کسی نمی تواند مرتکب بزه اداره کردن دسته یا جمعیتی را که بنیاد نگرفته، شود مگر اینکه در آغاز آن دسته یا جمعیت را تشکیل دهد. پس تشکیل دادن در اینجا مقدمه لازم اداره کردن است و اگر یک نفر هر دو رفتار را انجام دهد تنها یک بزه و آن هم اداره کردن را انجام داده است. با این حال نمی توان مقدمه لازم را به هر بزهی بار کرد، مانند حالتی که زندانی با ویران کردن دیوار زندان فرار کند، چون در اینجا ویران کردن تنها راه انجام بزه فرار نیست تا مقدمه لازم باشد. در اینجا ویران کردن یکی از مقدمه های فرار است نه مقدمه تنها و لازم. با سخن بالا روشن می گردد که آیا دسترسی غیر مجاز مقدمه لازم بزه های رایانه ای همچون اخلال در سامانه یا سرقت رایانه ای است یا خیر؟ دسترسی غیر مجاز مقدمه لازم برای بزههای رایانه ای نیست؛ چون دیگر بزه های رایانه ای بدون انجام دسترسی غیر مجاز نیز می توانند رخ دهند. مانند کسی که از رهگذر سامانه

خود، به کلاهبرداری رایانه ای می پردازد یا اینکه کسی از یک سیستمی که تدابیر حفاظتی ندارد، داده را ربوده یا تخریب کرده باشد. با این حال همچنانکه هتک حرمت منزل و سرقت از منزل دو بزه جداگانه اند، دسترسی غیر مجاز نیز اگر همراه با دیگر بزههای رایانه ای گردد، همچنان بزه جداگانه بوده و تعدد واقعی در اینجا حاکم خواهد بود. بدین حال، دسترسی غیر مجاز یک بزه رفتاری بوده و مطلق است و همین که دسترسی رخ دهد جدا از اینکه چه نشانه و نتیجه ای به بار آمده، بزه انجام شده است. بنابراین چنانچه در پرتو دسترسی، بزه های دیگری رخ دهد، مرتکب، چند بزه را انجام داده و نباید پنداشت که رفتارهای مجرمانه پسینی نتیجه دسترسی هستند.

۶- بحث و نتیجه‌گیری

جرایم رایانه ای امروزه درصد بالایی از جرایم را به خود اختصاص داده و هر روز شاهد عنوان و شکل جدیدی از این جرایم هستیم. قانونگذاران کشورهای مختلف با جرم انگاری این جرایم و با اندیشیدن تمهیداتی و همچنین پیروی از خط مشی های سازمانهای بین المللی مرتبط توانسته اند تا حد زیادی از وقوع آن پیشگیری کنند. کشور ما که یک کشور در حال توسعه است چند سالی است که با گسترش رایانه در بین مردم و با توجه به روند جهانی‌شدن و استفاده از فناوری های نوین ما نیاز به وجود قوانین نظم دهنده به محیط سایبر سال ها بود که احساس می شد. در نهایت پس از بررسی ها و تحقیقات لازم، قانون جرایم رایانه ای که مشتمل بر ۵۶ ماده و ۲۵ تبصره است در تاریخ ۲۰/۳/۱۳۸۸ به تایید شورای نگهبان رسید.

در این مقاله به بررسی جنبه های مختلف این جرم از جمله تعاریف و مفاهیم، جایگاه، ارکان تشکیل دهنده و ضمانت اجرا ها پرداخته شد و برای اینکه فهم و درک این جرم راحت تر گردد در کنار آن سرقت سنتی نیز مورد بحث و بررسی قرار گرفت .

نتایجی که از این مقاله بدست آمده است بدین شرح می باشد: پس از تحلیل ارکان تشکیل دهنده جرم سرقت رایانه ای در مقایسه با سرقت سنتی به وجود تفاوتها و شباهت هایی بین این دو جرم پی بردیم.از جمله اینکه رفتـار مجرمانه در هر دو جرم رباش است.البته رباش در سرقت رایانه ای تفاوتهایی با رباش در سرقت سنتی دارد. بدین ترتیب که رباش در سرقت رایانه ای بر اساس ماده ۱۲ قانون جرایم رایانه ای شامل گونه رفتار است: یکی « رو گرفت » و دومی برش» که در رو گرفت بر خلاف تمام حالات سرقت سنتی، عین داده ها همچنان در اختیار صاحب آن قرار دارد. موضوع جرم در سرقت سنتی مال است که بحث های فراوانی پیر و لزوم ارزش مالی داشتن موضوع جرم صورت گرفت و این مال تنوع زیادی دارد ولی موضوع جرم سرقت رایانه ای محدود به داده و اطلاعات است که بیان گردید داده ماهیتی جداگانه نسبت به مال دارد و لازم نیست که داده های موضوع سرقت رایانه ای دارای ارزش مالی باشند.زیرا اولا در ماده ۱۲ داده به صورت مطلق آمده و دوماً آنچه در رابطه با داده و اطلاعات حایز اهمیت است محتوای آنهاست. در سرقت رایانه ای عنصر غیر مجاز بودن لازم است که در واقع معادل همان عدم رضایت در سرقت سنتی است.

در مورد اینکه آیا رایانه می تواند حرز اطلاعات و داده ها باشد ؟نیز گفتیم که با توجه به حاصل کلام فتاوی فقهاء از یک طرف، و تفاوتهایی که بین سرقت رایانه ای و سنتی وجود دارد از طرف دیگر، رایانه حرز اطلاعات و داده ها محسوب نمی شود. یکی از تفاوت های مهم بین این دو جرمیستر ارتکاب جرم می باشد. که در سرقت رایانه ای بستر ارتکاب جرم فضای سایبر است که نوعی محیط مجازی است. در حالی که بستر ارتکاب جرم سرقت سنتی محیط بیرونی یا همان فضای فیزیکی است. مرتکبین این دو جرم هم تفاوت زیادی با هم ندارند. و هر چند هر کس می تواند مرتکب این دو جرم شود ولی از لحاظ ویژگی های شخصیتی و اخلاقی تفاوت هایی با هم دارند.

از لحاظ ویژگی های عمومی نیز بین این دو جرم شباهت هایی وجود دارد از جمله اینکه باید در هر دو جرم موضوع جرم به دیگری تعلق داشته باشد. و این تعلق به دیگری باید در لحظه ربودن نیز محقق باشد. همچنین باید رابطه علیت بین رفتار مجرمانه و نتیجه حاصله از جرم وجود داشته باشد. نتیجه ی جرم نیز در هر دو مورد سرقت، ربوده شده به محض ربودن است. در رکن روانی هر دو جرم وجود سؤنیت عام یا به عبارتی وجود قصد فعل مجرمانه ضروری است و نیز در هر دو جرم لازم است مرتکب آگاه به موضوع جرم باشد و علم به حکم نیاز نیست بجز در مورد سرقت مستوجب حد که در آن جهل به حرمت عمل

موجب می شود که مرتکب مسئولیت کیفری نداشته باشد. در مورد سؤنیت خاص نیز همانطور که بیان شد در سرقت سنتی وجود قصد خاص یا قصد نتیجه که همان «ربودن است، لازم می باشد ولی در سرقت رایانه ای صرف اینکه مرتکب ، قصد انجام فعل مجرمانه را به همراه علم به موضوع جرم
داشته باشد. کافی برای تحقق عنوان مجرمانه ی سرقت رایانه ای است.
و در نهایت اینکه با بررسی ضمانت اجراهای سرقت سنتی و رایانه ای این نتیجه بدست آمد که در خصوص سرقت سنتی تنوع در اعمال مجازات وجود دارد. در حالی که در سرقت رایانه ای تنها دو مورد مجازات برای دو قسمت سرقت رایانه ای پیش بینی شده است که نسبت به انواع سرقت های سنتی خفیف تر است. همچنین علاوه بر ضمانت اجرا های کیفری، ضمانت اجراهای تأمینی و جبرانی نیز لازم است که در مورد هر دو نوع سرقت به کار گرفته شود. و همچنین به این نتیجه رسیدیم که اشخاص حقوقی مانند اشخاص حقیقی می توانند مرتکب جرم شوند و باید آنها را دارای مسئولیت کیفری دانست هم در فضای بیرونی و هم در فضای سایبر. در واقع قانون جرایم رایانه ای اولین قانونی است که مسئولیت کیفری اشخاص حقوقی را به رسمیت شناخته است. و در آخر نیز به بیان راهکارهایی برای پیشگیری و مقابله با جرم سرقت رایانه ای پرداختیم که در دو شکل پیشگیری وضعی و پیشگیری اجتماعی بیان نمودیم.
نکته ای که در پایان باید خاطر نشان کرد این است که قانون فعلی ما در زمینه جرم سرقت رایانه ای هنوز با کاستیها و چالشهایی روبه رو است که توجه بیشتر قانونگذار را می طلبد.

۷- پیشنهاد ها

۱- یکی از مسائل و مشکلات مربوط به جرایم رایانه ای و از جمله سرقت رایانه ای این است که اکثر بزه‌دیدگان این جرایم از اعلام وقوع جرم به مراجع مربوطه خود داری می کنند. و ترجیح می دهند که به تعقیب موضوع مبادرت نکنند. برای رفع این مشکل می توان به اشخاصی که به عنوان بزه دیدگان بالقوه محسوب می شوند، آموزش داده شود. تا او لا قربانی این جرم واقع نشوند و ثانیا اگر قربانی یک جرم رایانه ای مثل سرقت شدند وقوع آن را به مراجع مربوطه گزارش دهند.

۲- کاربران رایانه ای باید مسئولیت حفظ نظم و امنیت اطلاعات شخصی خود را بر عهده بگیرند.هر فردی باید اطلاعات خود را به منظور جلوگیری از سرقت توسط سارقان، اداره کند. این پیشگیری می تواند از طریق تکه پاره کردن اسناد شخصی ،مرور مرتب کارت های اعتباری، گزارش کارت های مخصوص استفاده از دستگاههای خودپرداز بانک ها و محدود کردن استفاده از کد ملی و شماره شناسنامه و تاریخ تولد و سایر مدارک هویت شخصی، صورت بگیرد. برای مثال شخص بهتر است زمانی که می خواهد برای یکی از کارت های اعتباری اش رمز عبور تعین کند، از اطلاعات شخصی اش استفاده نکند. چرا که ممکن است تشخیص آن برای افراد به آسانی صورت گیرد.

۳- با توجه به اینکه درصد بالایی از مجرمین رایانه ای را کودکان تشکیل می دهند. لازم است تدابیری اتخاذ شود این افراد به عنوان مجرمین بالقوه در آینده مطرح نشوند. چه بسا همین کودکی که به قصد تفریح و سرگرمی مرتکب جرایم کوچک رایانه ای می شود، در بزرگسالی تبدیل به یک سارق حرفه ای شود. بنابر این باید آموزش های لازم به آنها و والدینشان داده شود.

۴- در زمینه های جدید حقوقی باید مطالعات تطبیقی و همکاری بین المللی بیش از گذشته گسترش یابد. به‌عنوان مثال جرایمی چون اسرقت هویت» و «سرقت اسرار و اطلاعات مالی و تجاری باید در قانون جرایم رایانه ای آورده شوند. از آنجا که در اثر این جرایم ضررها و خسارات غیر قابل جبرانی بر جامعه و البته قربانیان این جرایم وارد می شود، اکثر نظام های حقوقی اقدام به جرم انگاری این جرایم کرده‌اند.

۵- برای اولین بار مسئولیت اشخاص حقوقی در قانون جرایم رایانه ای به رسمیت شناخته شد. ولی بهتر است که در قسمت مربوط به کلیات قانون مجازات اسلامی نیز جایگاهی برای آن قائل شد. که البته در لایحه قانون مجازات اسلامی نیز پیش بینی شده است که امیدواریم که جایگاه خود را در این قانون حفظ کند.

منابع

۱. ابراهیم زاده پادشاه،حسن،حقوق مولفین بر نامه های رایانه ای،پایان نامه کارشناسی ارشد،دانشکده حقوق دانشگاه شهید بهشتی،۱۳۹۹.

۲. پاکزاد، بتول،جرایم رایانه ای، پایان نامه کارشناسی ارشد،دانشگاه شهید بهشتی تهران،۱۳۹۸.

۳. تحریری،فرزاد،دسترسی غیر مجاز به سیستم های رایا نه ای در حقوق ایران و اسناد بین المللی،پایان نامه کارشناسی ارشد حقوق جزا و جرم شناسی،دانشگاه مفید (ره)قم.۱۳۹۳.

۴. جلالی فراهانی، امیر حسین،مقاله پیشگیری وضعی از جرائم سایبر در پرتو موازین حقوق بشر،پاییز ۱۳۹۴.

۵. حقوق فن آوری اطلاعات و ارتباطات(مجموعه مقالات)معاونت حقوقی توسعه قضایی قوه قضائیه،گردآوری امیر حسین جلالی فراهانی،تهران، روزنامه رسمی جمهوری اسلامی ایران، ۱۳۹۸.

۶. خرم آبادی،عبد الصمد،تاریخچه وتعریف وطبقه بندی جرایم رایانه ای، مجموعه مقالات همایش بررسی ابعاد حقوقی فن آوری اطلاعات،۱۳۹۶.

۷. رابینز، استیفن. مبانی رفتار سازمانی. (۱۳۹۸). ترجمه امیدواران، کامیار و همکاران، چاپ سوم، انتشارات مهربان نشر، صفحه‌ی ۲۸۲.

۸. فضلی، مهدی،مسوولیت کیفری در فضای سایبر،معاونت حقوقی و توسعه قضایی قوه ی قضائیه مرکز مطالعات توسعه قضایی،تهران،خرسندی،۱۳۹۸.

۹. گلدوزیان،ایرج،حقوق جزای اختصاصی، انتشارات بخش فرهنگی دفتر مرکزی جهاد دانشگاهی، ۱۳۹۹.

۱۰. مکارم شیرازی، ناصر،تعزیر و گستره آن،گرد آوری ابوالقاسم علیان نژاد نشر مدرسه امام علی، ۱۳۹۳.

۱۱. موذن زادگان،حسنعلی،تقریرات آیین دادرسی کیفری، ۱۳۹۵.

۱۲. نور بها، رضا، زمینه حقوق جزای عمومی،تهران، نشر دادآفرین، ۱۳۹۷.

۱۳. میر محمد صادقی،حسین،جرائم علیه اموال و مالکیت،جلد یک،انتشارات امیر کبیر،۱۳۹۹