چکیده

در دنیای امروز که از آن به عصر اطلاعات یاد می کنند با ظهور رایانه ها ، حیاتی نو در همه عرصه های زندگی بشری ایجاد شده است ، سرعت و سهولت در دسترسی به اطلاعات و مبادله و توزیع اطلاعات در دنیای فاقد مرز ، موجب پیشرفت های بسیاری گردیده است . رایانه مزایایی برای بشر امروز به ارمغان آورده است با این حال این نکته را باید پذیرفت که رایانه ها دارای جنبه منفی نیز می باشند و آن ؛ خلق یکسری اعمال مجرمانه است که تا قبل از آن امکان ارتکاب چنین جرایمی ناممکن بوده است. در این مقاله سعی شده حول دو محور بحث شود ، ابتدا فضای سایبر و خصوصیات جرایم رایانه ای که باعث شده جرایم رایانه ای دارای جایگاه خاصی در حقوق کیفری شوند مورد تحلیل قرار می گیرد و محور بعدی کلاهبرداری رایانه ای به همراه عناصر تشکیل دهنده آن و نکات مهم این جرم می باشد.

کلمات کلیدی: جرایم رایانه ای ، فضای مجازی ، کلاهبرداری رایانه ای .

جهان بدون مرز در فضای مجازی (سایبر[1])

تنوع یافتن شیوه های ارتباطی، به هم پیوستن همه رسانه ها در یک متن گسترده تر دیجیتالی ، باز شدن راه برای رسانه های چندگانه متعامل و امکان ناپذیری کنترل امواج ماهواره ها که مرزها را در می نوردد یا ارتباطات کامپیوتری از طریق خط تلفن ، تمامی جبهه های سنتی نظارت دفاعی را قلع و قمع ساخت. توسعه تکنولوژی مخابراتی و پیشرفت در صنعت کابل ابزارهایی فراهم آورد که قدرت مخابره بی سابقه ای را میسر ساخت.[2] به گونه ای که شاید بتوان گفت جهانی شدن در فضای مجازی بیشترین نمود را داشته است. حتی می توان ادعا کرد که این امکان ، بزهکاری را تسهیل نموده و زمینه را برای همکاری باندهای جنایی در سطح جهان ممکن ساخته است. بدین سان در این مبحث مطالب را در دو قسمت بررسی خواهیم کرد؛ در گفتار اول فضای سایبر را تشریح نموده و در گفتار دوم به اوضاع و احوال جنایی در فضای سایبر خواهیم پرداخت.

تعریف فضای مجازی (سایبر)

در عصر حاضر حوزه های مختلف علوم با تحولات و ابداعات بسیاری مواجه بوده است. بعضی ابداعات حوزه هایی را هدف قرار داده اند که موجب بروز تحولات بنیادین و اساسی در زندگی بشر شده اند. یکی از بدیهی ترین و در عین حال حیاتی ترین عناصری که می توان از آن به عنوان وجه مشترک تمامی حوزه ـ ها نام برد اطلاعات است و دانشمندان به دنبال ابداع ابزاری بودند که بتواند کارایی بهره برداری از اطلاعات را به حداکثر برساند. به این ترتیب دستگاهی به نام رایانه به جامعه بشری عرضه شد.[3] انتقال و انتشار اطلاعات علاوه بر شبکه های ماهواره ای رادیویی و تلویزیونی از طریق شبکه های رایانه ای بین المللی هم صورت می گیرد که شناخته شده ترین آنها شبکه جهانی اینترنت است. این شبکه جهانی با اتصال رایانه های مختلف سراسر دنیا ایجاد شده و امکان دسترسی به اطلاعات موجود در رایانه های میزبان را برای همگان فراهم آورده است. فضایی که این شبکه و سایر شبکه های بین المللی ایجاد می کنند ، فضای مجازی و غیر قابل لمس است که فضای سایبر نامیده می شود.[4]

سایبر واژه ای است بر گرفته از لغت «kybernetes» به معنای سکاندار یا راهنما و نخستین کسی که واژه فضای سایبر را به کار برد ، «ویلیام گیتسون» نویسنده داستان های علمی- تخیلی ، در کتاب نورومنسر (neuromancer) بود. این اصطلاح به هر اتاق و هر فضائی اطلاق می شود که بوسیله نرم افزار در رایانه ایجاد می گردد و تجربه حقیقت مجازی را تولید می کند. اتاق فرمان را در دنیای مجازی رایانه به دست می ـ گیرد و چگونگی حس کردن و فهمیدن شرکت کنندگان را تحت تاثیر قرار می دهد. به جرات می توان

---

[1] -cyber

۲- مانوئل کاستلز، عصر اطلاعات، قدرت و هویت، جلد دوم، ترجمه حسن چاوشیان، طرح نو، چاپ ششم، تهران، ۱۳۸۹، ص۳۰۸.

۳- امیر حسین جلالی فراهانی، در آمدی بر آیین دادرسی کیفری جرایم سایبری، انتشارات خرسندی، چاپ اول، تهران، ۱۳۸۹، ص۱۴.

۴- محمد رضا محمدی، مسئولیت مدنی در فضای سایبر، مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات در نکوداشت مرحوم محمد حسن دزیانی، گردآوری امیر حسین جلالی فراهانی، نشر روزنامه رسمی، چاپ اول، تهران، ۱۳۸۸، ص۱۹۵.

گفت بزرگترین فضای سایبر را که میلیونها کاربر را به یکدیگر متصل می کند ، فضای مجازی اینترنت ذکر کرد.

تعریف حقوقی جرایم سایبری بسیار گسترده و جامع است که خود مقاله‌ای تخصصی و جداگانه را می‌طلبد، لذا از آن می‌گذریم و به تقسیم بندی کلی این جرایم از نگاه هدف و موضوع آن‌ها می‌پردازیم ، در این تقسیم‌بندی ۴ گروه اصلی وجود دارد:

۱. **تجاوز سایبری** : عبور از مرزها و محدودیت‌ها و ورود به حریم مردم و وارد کردن آسیب‌های گوناگون به مایملک مردم. مانند: هک‌کردن ، وارد کردن ویروس به رایانه و یا شبکه‌ای از رایانه‌ها.

۲. **فریب و دزدی سایبری** : این اعمال عموماً در حوزه اقتصادی و نقض مالکیت معنوی افراد صورت می‌گیرد. مانند: تقلب‌های بانکی و سرقت اطلاعات کارت اعتباری افراد.

۳. **هرزه‌نگاری سایبری** : نقض اصول اخلاقی و فطری برای اشاعه بی‌حیایی در جامعه.

۴. **خشونت سایبری** : بروز آسیب‌های روانی و یا تحریک دیگران برای انجام خشونت‌های فیزیکی علیه دیگران که نتیجه نقض قوانین حقوقی حفاظت فردی است.[۵]

دو گروه اول ، جرایمی را شامل می‌شود که علیه انواع مالکیت‌هاست ، گروه سوم دربردارنده جرایم اخلاقی است و گروه چهارم جرایم علیه افراد را دربر می‌گیرد. البته گروه دیگری از جرایم وجود دارند که علیه دولت‌ها صورت می‌گیرند و چنین تعریف می‌شوند: "شکستن قوانینی که برای حفظ و تامین تمامیت کشور و زیرساخت‌های آن تصویب شده‌اند." مانند: تروریسم ، جاسوسی و افشای اسرار رسمی.

اما نکته‌ای که در تمامی تعاریف جرایم سایبری مغفول مانده ، این است که این جرایم تنها شامل رایانه‌ها نمی‌شوند؛ بلکه بعضی دستگاه‌های‌الکترونیکی همچون گوشی‌های هوشمند ، دستگاه‌های خودپرداز و کارت‌های اعتباری خود زمینه‌ساز وقوع جرایم سایبری مختلف می‌شوند ، که در این تعاریف گنجانده نشده‌اند.

تا دو دهه پیش فضایی به نام فضای سایبر یا فضای الکترونیکی چندان مطرح نبود ولی این فضا اکنون تقریباً کل جهان را در بر گرفته است. در فضای سایبر بسیاری از فعالیت های اجتماعی ، اقتصادی و فرهنگی انجام می شود. از اطلاع رسانی گرفته تا بازرگانی الکترونیک و خرید و فروش از طریق اینترنت و انجام کارهای بانکی و انتشار آثار علمی و هنری و بسیاری اقدامات دیگر. اینترنت بر خلاف سایر رسانه ها به لحاظ مجازی بودن خود دنیایی در کنار دنیای واقعی ایجاد کرده است بر خلاف محیط های فیزیکی که در دنیای واقعی با مرزها و دیوارها از هم جدا می شوند فاقد هر گونه حد و مرز تعیین کننده ای است.[۶] این امر در عمل خود

۵- صادق سلیمی، جنایات سازمان یافته فراملی، انتشارات تهران صدا، چاپ اول، تهران، ۱۳۸۹، ص۱۷.

۶- مهدی فضلی، مسئولیت کیفری در فضای سایبر، انتشارات خرسندی، چاپ اول، تهران، ۱۳۸۹، ص۶۴.

مشکلات بسیاری را موجب می گردد. علیرغم این که فناوری نوین امکانات بسیار زیادی را برای انسان فراهم کرده است زمینه بسیار خوبی را نیز برای ارتکاب جرم یا ایجاد خسارت به دیگران فراهم آورده است.

جرم رایانه ای , جرم سایبری و جرم نرم افزاری را باید یکسان بدانیم؟

ماهیت جرم رایانه‌ای همانند واقعیت آن جدال‌آمیز و بحث‌انگیز است و هر شخص یا نهاد ملی یا بین‌المللی، تعریف متفاوتی از آن ارائه داده‌اند و به لحاظ اینکه در این مختصر مجال طرح آنها نیست ، باید به همین میزان بسنده کرد که **جرم رایانه‌ای** جرمی است که یا اطلاعات و نرم افزارهای رایانه‌ای موضوع جرم واقع می‌شوند یا سیستم رایانه‌ای وسیله ارتکاب جرم قرار می‌گیرد. اما بحث مهمتر در ماهیت جرم رایانه‌ای که بر جرایم رایانه‌ای و از جمله کلاهبرداری نیز تأثیرگذار است ، **جرم اینترنتی** به جرم قابل ارتکاب در محیط اینترنت گفته می‌شود و اگر بین شبکه‌های اطلاع رسانی متصل به هم از حیث خاص و عام و محلی و ملی و بین‌المللی بودن قائل به تفکیک شویم ، باید گفت اینترنت در مفهوم واقعی خویش به معنای شبکه‌های رایانه‌ای مرتبط به هم است که در سطحی گسترده کاربران و مشترکین متعددی را به هم پیوند می‌دهد. اما اگر شبکه‌های رایانه‌ای مرتبط به هم در قالب یک ساختمان یا شرکت یا نهاد بوده و یا اینکه محلی باشند، حمل شبکه اینترنت بر آنها بلااشکال نیست ، چه اینترنت خصیصه جهانی داشته و محصول ارتباط رایانه‌های بی‌شماری است. از این حیث جرم اینترنتی حتی از جرم شبکه‌ای که ناظر به هر نوع شبکهٔ اطلاع رسانی می‌باشد ، محدودتر خواهد بود. جرم سایبری به جرم قابل ارتکاب در محیط مجازی اینترنت و مخابرات گفته می‌شود. جرم سایبری از جرم اینترنتی عام‌تر است و علاوه بر اینکه شامل جرایم مخابراتی می‌شود می‌تواند به جرایم علیه نرم‌افزارهای یک رایانه که به صورت مجازی در سیستم رایانه‌ای قرار دارد نیز تسری داده شود و به همین دلیل در مقررات کشورها و اسناد بین‌المللی به ویژه کنوانسیون جرایم قابل ارتکاب در محیط سایبر بوداپست مصوب سپتامبر ۲۰۰۱ از عنوان جرم سایبری استفاده شده است.[۷] جرم نرم‌افزاری نیز غیر از اینکه از حیث عنوان موضوعات محدودی را در بر می‌گیرد ، جرایم مرتبط با عملکرد رایانه را نیز در بر نمی گیرد. اما با چشم پوشی از اصطلاح جرم سایبری که هم در حقوق کشورمان شناخته شده نیست و هم محدودتر از جرم رایانه‌ای است ، اصطلاح جرم رایانه‌ای از جهات مختلف مناسب به نظر می‌رسد. توضیح اینکه جرم رایانه‌ای شامل کلیه جرایمی می‌شود که به نوعی در آنها رایانه ایفای نقش می‌کند و از آنجایی که قوام و دوام اینترنت و فضای سایبر به وجود رایانه است و سیستم‌های ارتباطی و مخابراتی نیز با رایانه فعالیت می‌کنند و شبکه‌های محلی و منطقه‌ای نیز از رایانه شکل گرفته‌اند و از طرف دیگر نرم‌افزارهای رایانه‌ای جزئی از رایانه تلقی می‌شوند ، جرم رایانه‌ای شامل همه این عناوین می‌شود.[۸] البته جرم رایانه‌ای از حیث دایره شمول عنان گسیخته بوده و مفهومی عام‌تر از میزانی که مد نظر ماست ، دارد. بنابراین جرم رایانه‌ای را باید منصرف به عملکرد رایانه ، نرم‌افزارهای رایانه‌ای و داده و سیستم رایانه‌ای کرد والا هیأت

۷- مرسده شریفی ، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۷۹.

۸- کامران شیرزاد ، جرایم رایانه ای از دیدگاه حقوق جزای ایران و بین الملل، نشر بهینه فراگیر، چاپ اول، تهران، ۱۳۸۸.

رایانه و لوازم سخت افزاری آن بدون توجه به عملکرد و قابلیت آنها مشمول مقـررات مباحـث سـنتی حقـوق کیفری خواهد بود.

فرصت های ارتکاب جرم در فضای سایبر

فضای سایبر دارای ویژگی هایی است که هر فرد به آسانی می تواند وارد این شـاهراه اطلاعـاتی شـود و هـر اطلاعاتی که خواست وارد نماید. از جمله این ویژگی ها جهان شمول بودن ، کنترل ناپذیر بودن و آزاد بودن این فضا است. در این گفتار فضای سایبر و هویت مجرمانه ، کنترل ناپذیری فضای سایبر و دسترسـی آسـان به بزه دیده در سه قسمت به عنوان مهم ترین عوامل موثر بر شرایط مجرمانه جدید بحث خواهد شد.

۱- فضای سایبر و هویت مجرمانه

فضای مجازی که منشا تحولات گوناگونی در زندگی بشر بوده، به همان اندازه کـه شـرایط زنـدگی را بهبـود بخشیده است ، زمینه مساعدی برای ارتکاب جرم نیز بوده است. قربانیان جرایم سـایبری در واقـع قربانیـان پیشرفت تکنولوژی هستند.

سرعت ارتباطات به بزهکاران اجازه داد که آسانتر دست به ارتکاب جرم بزنند. پیامد فنون و شیوه های جدید زندگی دامن زدن به اشکال نوین بزهکاری از جمله جرایم فضای مجازی بود. رسانه های گروهی هم به نشـر روش های معمول توسط بزهکاران کمک کردند. از این طریق پیروان و مقلدانی در زمینـه بزهکـاری بوجـود آوردند.[۹] ویژگی مهمی که باعث به فعل درآوری اندیشه مجرمانه توسط بزهکاران سایبری می شود ناشـناس بودن و گمنامی در این فضا است و لذا بسیاری از مجرمین فضای سایبر قابل شناسایی نیستند.

فضای سایبر یک فضای مخفی است. مردم در این محیط در پشـت رایانـه هـای خـود کـه هویـت آنهـا را از دیگران مخفی می دارد ، محیطی امن و مطمئن می یابند تا هر آنچه کـه مـی خواهنـد را بـه معـرض اجـرا گذارند. چرا که نگاه های شماتت بار پلیس و مردم بر آنها نظاره ندارد تا آنان را از ترس دسـتگیری یـا شـرم رسوایی از ارتکاب خواسته هایشان باز دارد.[۱۰] این فرصت مغتنم در کنار دیگر شرایط مهیا، حتی کسانی کـه متعهد به رعایت هنجارهای اجتماعی هستند را وسوسه می کند تا روحیات پلیدشان را بروز دهند.[۱۱]

لذا مجعول بودن هویت افراد و پوشیده بودن فضای سایبر به افراد این اجازه را می دهد که به شـکلی افسـار گسیخته و فارغ از کنترل های اجتماعی و اخلاقی میدانی برای تاخت و تاز و عقده گشایی آنچه بدان دسـت نیافته اند بیابند. نمونه این امر را می توان در مورد انتشار تصاویر مستهجن کودکان در فضای سایبر دید که در عین حالی که وسیله سودآوری برای ارائه کنندگان این تصاویر گشـته ، بـرای خواسـتاران ارضـای غرایـز

۹- ژرژ پیکا، جرم شناسی، ترجمه علی حسین نجفی ابرند آبادی، چاپ اول، نشر میزان، تهران، ۱۳۸۹، ص۵۸.

۱۰- مهدی فضلی، مسئولیت کیفری در فضای سایبر، ص۶۴.

۱۱- امیر حسین جلالی فراهانی، پیشین، ص۱۷.

جنسی نیز دنیایی آزاد فراهم آورده تا هر لحظه که خواستند بتوانند به راحتی وارد این دنیـای خیـال گونـه شوند و تمایلات غریزی خود را فرو بنشانند.[۱۲]

۲- کنترل ناپذیری فضای سایبر

انقلاب اطلاعات به پیدایش شاهراه های اطلاعات منجر شده است که در سراسر جهـان و از طریـق شـبکه ـ های به هم متصل رایانه ای عمل می کند. دگرگونی سریع ارزشها و ساختارهای جامعـه بـه کـاهش کنتـرل منجر شده و نتیجه تبعی آن ارتکاب جرایم جرایم رایانه ای است که از طریق رشد فضای به هم متصل سایبر از مرزهای ملی نیز خارج شده است.[۱۳] به رغم این که این شبکه به لحاظ فنی رشد داشـته ، از لحـاظ رشـد ساختارهای اخلاقی و کنترل کننده که هر محیط برای استقرار نظم به آنها نیازمند است بسیار عقـب مانـده است. این محیط پلیس ندارد و سازمانی بر آن نظارت نمی کند ، مردم اشخاص را در حین ارتکاب جرم نمی بینند و هر کس هر آنچه می خواهد انجام می دهد.[۱۴] ویژگی های مهم فضای سـایبر از جملـه عـدم تمـاس چهره به چهره و عدم وجود پلیس و نهادهای نظارتی ، باقی نماندن آثاری از ردپای مجرمین و آزدی بی حد و حصر در اینترنت شرایط مناسبی را برای مجرمان فراهم می سازد تا مرتکب جرم شوند. سـالانه میلیاردهـا دلار نرم افزار به صورت غیر قانونی کپی می شود و هر روز شاهد افزایش آمار خریـد و فـروش ابـزار جـرایم سایبر مانند کدهای مخرب ، حملات اینترنتی و حفره های امنیتی هستیم.[۱۵] دامنه ایـن جـرایم روز بـه روز گسترده تر و روش های ارتکاب آن پیچیده تر و متنوع تر می شود زیرا فضای سایبر یک محـیط آزاد اسـت که در آن وجدان جمعی و هنجارهای هدایتگر اجتماعی و نظارتی بی معناست. در واقـع ویژگـی غیـر قابـل ملموس بودن فضای سایبر امکان نظارت را بر این محیط بسیار دشوار کرده است.

۳- دسترسی آسان به بزه دیده

فضای سایبر شرایطی را به وجود آورده که بزهکاران با کمتـرین هزینـه و اضـطراب ، بیشـترین خسـارات و صدمات را به بار آورده و در عین حال ناشناخته باقی بمانند. عوامل فرهنگی ، مشکلات روحی و روانی نظیـر افسردگی ، عصبانیت ، حسادت ، انتقامجویی ، حس تنفر ، تفریح و سرگرمی ، خودکم‌بینی و حقارت ، حس رقابت و... از جمله عواملی هستند که بزهکاران را در این فضای گمنامی جسورتر می کند.

فقر فرهنگی و پایبندنبودن به ارزش های جامعه و باورهای دینی یکی از عوامل مهم ارتکاب این قبیل جرایم در فضای مجازی است. کمرنگ شدن آموزه‌های دینی و اخلاقی ، اهمیت قائل نشدن برای توصیه های دینی

۱۲- مهدی فضلی، تخریب و اختلال در داده ها و سیستم های رایانه ای، مجموعه مقالات اولین همایش حقوقی فناوری اطلاعات، مرکز مطالعات راهبردی و توسعه قضایی قوه قضاییه، تهران، ۱۳۸۷، ص۱۲۷.

۱۳- ناریش اس دالال، نیم نگاهی به ذهن هکرها، ترجمه احسان زرخ، مجموعه مقالات حقوق فناوری اطلاعات و ارتباطات در نکوداشت مرحوم محمد حسن دزیانی، روزنامه رسمی، چاپ اول، تهران، ۱۳۸۸، ص ۴۲۸.

۱۴- مهدی فضلی، تخریب و اختلال در داده ها و سیستم های رایانه ای، ص۶۹.

۱۵- سوسن باستانی، بررسی عوامل موثر در وقوع جرایم در فضای سایبر و راهکارهای پیشگیری از آن، شرکت ناجی نشر، چاپ اول، تهران، ۱۳۸۹، ص۱۳۸.

برای حفظ آبروی مومن، بی تفاوتی به سرنوشت انسان های دیگر و... به این گرایش مجازی دامن زده است. بیشترین توقع از جوامع اسلامی که سنگ بنای خود را بر ارزش های دینی نهاده اند ، ارتقای سطح باورهای دینی و اخلاقی خصوصاً در بین نوجوانان و جوانان و ترویج و نهادینه کردن اصول و مبانی دین درهمه لایه های زندگی به منظور واکسینه کردن افراد در برابر طوفان های جدید زندگی بشری است.

شاید اگر فرمایش امام صادق(ع) را در خود درونی کنیم که «هر که مطلبی را بازگو کند تا آبروی مؤمن را بریزد و خوارش سازد تا او را از چشم مردم بیندازد ، خداوند او را از ولایت و سرپرستی خویش درآورد و به ولایت شیطان واگذار کند». یا این نقل از رسول خدا(ص) که «هر کسی آبروی برادر مسلمان خود را حفظ کند ، بدون شک ، بهشت بر او واجب می شود». قبح ارتکاب فعل مجرمانه را برای ما آشکارترکند. این نوع خودکنترلی ، ضمانت قوی برای مصونیت شخصیت افراد در برابر آسیب است و قبل از هر ابزار دیگر ، جامعه را از گزند فضای مجازی دور می کند. دین و قانون در کشور ما قابلیت های زیادی را برای ناامن کردن فضای مجازی به عنوان پناهگاه مجرمان اینترنتی فراهم کرده است.

بنابراین ارتکاب جرم در فضای سایبر بسیار آسان است. بزهکار با داشتن یک رایانه که امکان اتصال به اینترنت را دارد ، در خانه خود امکان ارتکاب جرم علیه بزه دیده ای را دارد که هزاران و حتی میلیونها کیلومتر از او فاصله دارد. در فضای سایبر بر خلاف بر خلاف محیط واقعی هیچ مجاورت و تماس چهره به چهره ای بین بزهکار و بزه دیده صورت نمی گیرد و همین امر شناسایی بزهکار را بر بزه دیده غیر ممکن می سازد. به همین دلیل رقم سیاه بزهکاری در فضای سایبر بسیار بالاست.[۱۶]

۴-عدم وابستگی به محل ارتکاب جرم و فراملی بودن :

به دلیل فراملی بودن ماهیت جرایم کامپیوتری اینگونه جرایم را باید جرایم بدون مرز نامید. در این جرایم لازم نیست که مجرم در محل وقوع جرم حضور فیزیکی داشته باشد .مسافت ، زمان و مکان مانعی برای آن به حساب نمی آید.حضور فیزیکی شخص در محل وقوع حادثه معنایی ندارد.[۱۷]

با کمک کامپیوتر و از طریق اینترنت ، سرقت از یک بانک و یا دست یابی به اطلاعات محرمانه نظامی در ظرف چند ثانیه امری بعید و دور از دسترس نمی باشد.

۵-گستردگی حجم خسارات حاصله:

از آنجایی که محدودیت های دنیای مادی در مورد این جرایم وجود ندارد و داده هایی که ارزش اقتصادی فراوانی دارند در یک حجم نگهداری می شوند لذا میزان خسارت آنها نسبت به جرایم کلاسیک بسیار گسترده تر است.[۱۸]

۱۶- حسن پوربا فرانی، حقوق جزای بین الملل، نشر جنگل، چاپ دوم، تهران، ۱۳۸۸، ص۸۵.

۱۷- برومند باستانی، جرایم کامپیوتری و اینترنتی جلوه ای از بزهکاری ، مجله تحقیقات حقوقی، ۱۳۸۲،ص ۳۵.

برای دستبرد زدن الکترونیکی به یک بانک نه سلاح لازم است و نه یک گروه سازمان یافته ، بلکه یک نفر می تواند با نفوذ به سیستم یک بانک میلیاردها دلار پول الکترونیکی را به حساب خود یا دیگری منتقل کند.این عدم محدودیت مادی در کنار گسترش نقش رایانه به عنوان جز لاینفک فعالیت روزانه شرکتها و بنگاه های تجاری ، سبب می گردد که با وقوع برخی جرایم حتی شرکتهای بزرگ به ورطه نابودی و ورشکستگی سقوط کند. عواقب جرایم کامپیوتری علاوه بر خسارات اقتصادی سنگین می تواند تهدیدی برای امنیت باشد. وابستگی امور حساس کشورها در زمینه های پزشکی ،مخابراتی ،هواپیمایی ، امور امنیتی و نظامی و غیره به عملکرد کامپیوتر باعث می شود تا کوچکترین خللی و خدشه در کاربرد این سیستم ها عواقب وخیم و جبران ناپذیری را به دنبال داشته باشد.

۶- سهولت از بین بردن آثار وقوع و بالا بردن رقم سیاه:

تنها ردی که از مجرم رایانه ای به جای می ماند یک سری ردپای الکترونیکی است که به راحتی و بدون حضور در محل استقرار سیستم رایانه ای حامل این رد پا ، می توان آن را از بین برد. البته به معنای عدم امکان بازیابی این داده نیست ، اما کار گروه تحقیق بسیار مشکل می کند.[۱۹]

دلیل وجود رقم سیاه ، عدم آگاهی و شناخت کامل بزه دیدگان از این جرایم ، عدم تمایل بزه دیدگان برای اعلام وقوع جرم کامپیوتری پس از کشف می باشد. در بخش تجارت این عدم تمایل به دو امر مربوط می شود ، برخی از بزه دیدگان ممکن است به دلیل هراس از تبلیغات سوء رسوایی و از دست دادن حسن شهرت خود تمایلی به فاش ساختن اطلاعات نداشته باشند ، دیگر بزه دیدگان نیز از سلب اعتماد سرمایه گذران و یا عامه ی مردم و یا پیامدهای اقتصادی ناشی از آن واهمه دارند. لذا برای مبارزه و پیش گیری از جرایم رایانه ای اینترنتی همکاری بزه دیده بسیار مهم و حائز اهمیت است. عدم آگاهی و شناخت کامل بزه دیدگان از این جرایم ، ترس شرکتها از لطمه به وجهه و اعتبار شرکت ، عدم تخصص ضابطین قضایی در شیوه ی کشف و تعقیب این جرایم فقدان امکانات کافی در این خصوص و اثبات آنها و گنجانده نشدن جرایم رقم سیاه بسیار بالاست تا انجا که سازمان اطلاعات و امنیت امریکا این رقم را ۸۵ تا ۹۵ درصد اعلام کرده است.[۲۰]

۷- نحوه ی تعقیب و رسیدگی به جرایم کامپیوتری و اینترنتی:

همانگونه که می دانیم نوین بودن جرم اینترنتی و کامپیوتری و شیوه ی ارتکاب اینگونه جرایم نحوه رسیدگی و تعقیب را از جهت مسائل آئین دادرسی با چالش هایی روبرو کرده است به گونه ای که تدابیر

۱۸- جعفر کوشا، جرایم رایانه ای در بستر تجارت الکترونیکی، انتشارات خرسندی، چاپ سوم، تهران، ۱۳۸۶، ص۹۸.

۱۹- همان.

۲۰- محمد حسن دزیانی، مسوولیت کیفری برای انتقال داده ها در شبکه های کامپیوتری بین المللی و چالش های جدید اینترنت، مجله تحقیقات حقوقی، شماره ۸۰، زمستان ۱۳۸۰، ص۱۷.

کلاسیک حقوقی به هیچ عنوان پاسخگو نبوده و با مشکلات عدیده ای در این زمینه روبـرو مـی باشـد.[۲۱] در جرایم جدید کامپیوتری ، به خصوص جرایم مرتبط با اینترنت و کشف بسیار دشوار و غیر قابل دسترسی می باشد. در واقع جایگزین شدن موضوعات غیرملموس و مجـازی بـه عـوض ادلـه ی مثبـت ملمـوس و عینـی تکنولوژی اطلاعات ، مسائل حقوقی نوینی را مطرح ساخته و از خصوصیات بارز جرایم اینترنتی و کامپیوتری است.

جرم رایانه ای ، جرم شبکه ای ، جرم سایبری و جرم نرم افزاری را باید یکسان بدانیم؟

ماهیت جرم رایانه‌ای همانند واقعیت آن جدال‌آمیز و بحث‌انگیز است و هر شخص یا نهاد ملی یا بین‌المللـی، تعریف متفاوتی از آن ارائه داده‌اند و به لحاظ اینکه در این مختصر مجال طرح آنها نیست ، بایـد بـه همـین میزان بسنده کرد که جرم رایانه‌ای جرمی است که یا اطلاعات و نرم افزارهای رایانـه‌ای موضـوع جـرم واقـع می‌شوند یا سیستم رایانه‌ای وسیله ارتکاب جرم قرار می‌گیرد. ، جرم اینترنتی به جرم قابل ارتکاب در محیط اینترنت گفته می‌شود و اگر بین شبکه‌های اطلاع رسانی متصل به هم از حیث خاص و عام و محلی و ملی و بین‌المللی بودن قائل به تفکیک شویم ، باید گفت اینترنت در مفهوم واقعی خـویش بـه معنـای شـبکه‌هـای رایانه‌ای مرتبط به هم است که در سطحی گسترده کاربران و مشترکین متعددی را به هم پیوند می‌دهد. اما اگر شبکه‌های رایانه‌ای مرتبط به هم در قالب یک ساختمان یا شرکت یا نهاد بوده و یا اینکه محلـی باشـند، حمل شبکه اینترنت بر آنها بلااشکال نیست ، چه اینترنت خصیصه جهانی داشته و محصول ارتباط رایانه‌های بی‌شماری است. از این حیث جرم اینترنتی حتی از جرم شبکه‌ای که ناظر به هر نـوع شـبکهٔ اطـلاع رسـانی می‌باشد ، محدودتر خواهد بود. جرم سایبری به جرم قابل ارتکاب در محیط مجازی اینترنت و مخابرات گفته می‌شود. جرم سایبری از جرم اینترنتی عام‌تر است و علاوه بر اینکه شامل جرایم مخابراتی می‌شود می‌توانـد به جرایم علیه نرم‌افزارهای یک رایانه که به صورت مجازی در سیستم رایانه‌ای قرار دارد نیز تسری داده شود و به همین دلیل در مقررات کشورها و اسناد بین‌المللی به ویژه کنوانسیون جـرایم قابـل ارتکـاب در محـیط سایبر بوداپست مصوب سپتامبر ۲۰۰۱ از عنوان جرم سایبری استفاده شده است.[۲۲] جرم نرم افزاری نیز غیـر از اینکه از حیث عنوان موضوعات محدودی را در بر می‌گیرد ، جرایم مرتبط با عملکـرد رایانـه را نیـز در بـر نمی گیرد. اما با چشم پوشی از اصطلاح جرم سایبری که هم در حقوق کشورمان شناخته شده نیست و هـم محدودتر از جرم رایانه‌ای است ، اصطلاح جرم رایانه‌ای از جهات مختلف مناسب به نظـر مـی‌رسـد. توضـیح اینکه جرم رایانه‌ای شامل کلیه جرایمی می‌شود که به نوعی در آنها رایانه ایفای نقش می‌کند و از آنجایی که قوام و دوام اینترنت و فضای سایبر به وجود رایانه است و سیسـتم‌هـای ارتبـاطی و مخـابراتی نیـز بـا رایانـه فعالیت می‌کنند و شبکه‌های محلی و منطقه‌ای نیز از رایانه شکل گرفته‌انـد و از طـرف دیگـر نـرم‌افزارهـای رایانه‌ای جزئی از رایانه تلقی می‌شوند ، جرم رایانه‌ای شامل همه این عناوین می‌شود.[۲۳] البته جرم رایانه‌ای از

۲۱- برومند باستانی، جرایم کامپیوتری و اینترنتی جلوه ای از بزهکاری ،ص ۳۵.

۲۲- مرسده شریفی ، جرایم رایانه ای در حقوق جزای بین المللی، پایان نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران، ۱۳۷۹.

۲۳- کامران شیرزاد ، جرایم رایانه ای از دیدگاه حقوق جزای ایران و بین الملل، نشر بهینه فراگیر، چاپ اول، تهران، ۱۳۸۸.

حیث دایره شمول عنان گسیخته بوده و مفهومی عام‌تر از میزانی که مد نظـر ماسـت ، دارد. بنـابراین جـرم رایانه‌ای را باید منصرف به عملکرد رایانه ، نرم‌افزارهای رایانه‌ای و داده و سیسـتم رایانـه‌ای کـرد والا هیـأت رایانه و لوازم سخت‌افزاری آن بدون توجه به عملکرد و قابلیت آنها مشمول مقـررات مباحـث سـنتی حقـوق کیفری خواهد بود.

شناسایی کلاهبرداری رایانه‌ای

کلاهبرداری رایانه ای به عنوان یکی از مهمترین اشکال جرایم اقتصادی در فضای رایانه و اینترنت جایگـاهی ویژه در قانونگذاری کشورهای مختلف و مباحث حقوقدانان یافته است. این جایگاه برجسته عمدتاً تـابع سـه عامل کثرت ارتکاب ، سهولت ارتکاب و فاعل ارتکاب است. کثرت و تنـوع ارتکـاب کلاهبـرداری رایانـه‌ای در کشورهایی که رایانه و اینترنت در فعالیت‌های روزمره به طور کامل رسوخ یافته ، بسیار نگران کننـده اسـت. علاوه بر اینکه کلاهبرداری یک پدیده همیشه بارور است که هر روز به اقسام مختلف نمود می‌یابـد ، کثـرت وقوع آن نیز خیره کننده‌تر از سایر جرایم رایانه‌ای است؛ مثلاً در کشور آلمان طبق آمارهای جنـائی پلـیس ، تعداد گزارش‌های واصله در سال ۱۹۹۹ به پلیس در قبال وقوع جرایم کلاهبرداری رایانه‌ای ، تغییر داده‌هـا ، سابوتاژ رایانه‌ای و جاسوسی اطلاعات رایانه‌ای به ترتیـب ۴۴۷۴ ، ۳۰۲ و ۲۱۰ بـوده اسـت. در همـین سـال تعداد محکومیت‌های صادره در خصوص کلاهبرداری رایانه‌ای ۲۱۵۷ فقره بوده است و حال آنکه در قبال سه جرم تغییر داده‌ها ، سابوتاژ رایانه‌ای و جاسوسی اطلاعات تنها هشت حکم محکومیت از سوی محاکم آلمـان صادر شده است.[۲۴] سهولت ارتکاب کلاهبرداری رایانه‌ای نیز یکی دیگر از خصایص این جرم است کـه عمـدتاً تابع ارتباط بی قید و شرط کاربران اینترنتی با هم است. اگر در قبال جرایمی همانند نفوذ غیرمجاز یا شـنود می‌توان از تدابیری همچون نصب باروی(دیواره) آتشین یا سایر تدابیر حفاظتی استفاده کرد یا اینکـه انتشـار محتویات مستهجن را با توسل به پالایش مهار کرد اما مرتکـب کلاهبـرداری رایانـه ای از آنجـا کـه رایانـه و اینترنت و نرم افزارهای آن را هدف خود قرار نمی‌دهد و صرفاً از آنها به عنوان وسیله‌ای برای به دام انداختن کاربر استفاده می‌کند ، از تار و پود تدابیر امنیتی و حفاظتی رسته است و فقط این زیرکی و درایت کاربر یـا استفاده کننده از رایانه یا اینترنت خواهد بود که کلاهبردار را ناکام بگـذارد والا کلاهبـردار در هـر شـرایطی خواه قربانی در شبکه اینترنتی باشد یا بیرون از شبکه و خواه از طریق گپ اینترنتی و خواه از طریـق ارسـال رایانامه می‌تواند به مقاصد شوم خود برسد. فاعل ارتکاب کلاهبرداری رایانه‌ای مهمترین عامل برجستگی این جرم است.[۲۵] هر چند غالباً مجرمان رایانه ای از اسـتعداد نسـبتاً بـالایی برخـوردار هسـتند امـا کلاهبـرداران رایانه‌ای اشخاصی هستند که زیرکی فریب دادن دیگران را با دانش رایانه‌ای درآمیخته‌اند و بـدون تردیـد در زمره مجرمان یقه سفید قرار می‌گیرند که به میزان خطرناکی و استعداد جنائی بالا ، قدرت انطباق اجتماعی قابل توجهی دارند و به همین ترتیب علی‌رغم اینکه توجهات دیگـران را نسـبت بـه اعمـال غیرقـانونی خـود برنمی‌انگیزانند، به راحتی و به کرات رایانه و اینترنت را جولانگاه مانورهای متقلبانه خود می‌سـازند. نظـر بـه

۲۴- جواد جاوید نیا، نقد وبررسی جرم های مندرج در قانون تجارت الکترونیکی، مجله حقوقی دادگستری، شماره ۵۹، ۱۳۸۶، ص۱۸.

۲۵- شهرام شعیبی، مقایسه جرم کلاهبرداری سنتی ورایانه ای در حقوق ایران، ماهنامه شماره ۷۶، سال سیزدهم، مهروآبان۱۳۸۸، ص۳۵.

این ویژگی‌ها که کلاهبرداری رایانه‌ای به همراه دارد ، توجه خاصی از سوی حقوقدانان نسبت بـه ایـن جـرم معطوف شده است و برخی از آنها کلاهبرداری رایانه ای را که مصداق برجسته سوءاستفاده از رایانه اسـت در زمره شایع‌ترین جرایم اقتصادی رایانه‌ای قلمداد می‌کنند. با این وصف ، اهمیت شناسایی جـرم کلاهبـرداری رایانه‌ای پوشیده نمی‌ماند.

تعریف کلاهبرداری رایانه‌ای

مناسب‌ترین تعریف از هر جرمی تعریفی است که خود قانونگذار ارائه می‌دهد و بنابه‌اینکه قانونگذار همواره از اینکه نتواند تعریف جامع و مانعی از یک عمل مجرمانه ارائه دهد ، هراسان است؛ در غالب موارد بدون ارائه تعریف به ذکر اوصاف شرایط جرم اکتفا می‌کند و بنابراین جرایم عمدتاً از سوی حقوقدانان تعریف می‌شوند. کلاهبرداری عبارت است از بردن مال دیگری از طریق توسل توأم با سوءنیت به وسایل متقلبانه. تعریف کلاهبرداری رایانه‌ای نیز به لحاظ اینکه رایانه در تحقق آن عمدتاً وسیله ارتکاب است ، قاعدتاً باید مشابه همین تعریف باشد.

برخی از نویسندگان جرایم رایانه ای (کامپیوتری) را مترادف با جرم سایبر[۲۶]می دانند و آن دو را دارای دو معنی و مفهوم می دانند. در تعریف «مفیتی» ؛ جرم کامپیوتری صرفاً عبارت از جرایمی است که در فضای سایبر رخ می دهد از این نظر جرایمی مثل هرزه نگاری ، افترا ، آزار و اذیت و سوء استفاده از پست الکترونیکی و سایر جرایمی که در آنها کامپیوتر به عنوان ابزار و وسیلهٔ ارتکاب جرم بکار گرفته می شود ، در زمرهٔ جرم کامپیوتری قرار نمی گیرد. در تعریف موسع از جرم کامپیوتری هر فعل و ترک فعلی که «در» یا «از طریق» یا «به کمک» رایانه و از طریق اتصال به اینترنت ، چه به طور مستقیم ، یا بطور غیرمستقیم رخ می دهد و توسط قانون ممنوع گردیده و برای آن مجازات در نظر گرفته شده است جرم کامپیوتری نامیده می شود. و بر این اساس جرایم کامپیوتری را می توان به سه دسته تقسیم نمود :

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

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

---

[۲۶]- جرم سایبر که معادل فارسی Cybercrime است به جرایم در فضای سایبر (مجازی) را گویند که زیر شاخه ای از حقوق سایبر هست که در ابعاد حقوقی، مدنی، عبادی و فنی را در بر می گیرد.

دستهٔ 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 ـ شود ، مانند «دسترسی غیر مجاز به سیستم های کامپیوتری».[۲۷]

اما با توجه به نکات زیر ضرورت ارائه تعریفی جداگانه از کلاهبرداری رایانه‌ای احساس می‌شود:

الف - فعل فیزیکی جرم کلاهبرداری توسل به وسایل متقلبانه و بردن مال دیگری است که البته نسبت به وسایل پرداخت مال مانند چک ، تحصیل آنها نیز به عنوان یکی از افعال فیزیکی مطرح می‌شود. به دلیل تعدد فعل فیزیکی در جرم کلاهبرداری است که از آن به جرم مرکب یاد می‌شود. اما کلاهبرداری رایانه‌ای سوءاستفاده مالی به وسیله رایانه است که از طریق افعال فیزیکی متعددی همچون وارد کردن، تغییر، محو و توقف داده‌های رایانه‌ای تحقق می‌یابد و در واقع فعل فیزیکی کلاهبرداری رایانه‌ای هر گونه سوءاستفاده مالی از طریق رایانه است هر چند در قالب افعال تمثیلی مذکور تحقق یابد و از این حیث یک جرم ساده تلقی می‌شود تا یک جرم مرکب.

ب - یکی از اجزای رکن مادی کلاهبرداری ، فریفته شدن قربانی است و لازمه فریفته شدن این است که قربانی جرم انسان باشد و عموماً برای مرتکب نیز شناخته شده باشد؛ هر چند ، در اکثر مواقع بین مرتکب و قربانی ارتباط عینی حاصل می‌شود اما در کلاهبرداری رایانه‌ای تحقق جزء فریب قربانی لازم نیست؛ چه علاوه بر اینکه در غالب موارد قربانی جرم برای کلاهبردار رایانه‌ای شناخته شده نیست ، ممکن است اقدامات خدعه‌آمیز مرتکب علیه سیستم رایانه‌ای باشد ، بدون اینکه در این میان انسانی فریفته گردد. پس به همین میزان که شخصی از طریق گمراه کردن رایانه و یا حتی بدون گمراه کردن آن و از طریق کسب برخی اطلاعات مالی از طریق رایانه مال یا مزایای مالی را تحصیل نماید ، کلاهبردار رایانه‌ای محسوب می‌شود.

ج - موضوع یا هدف جرم کلاهبرداری مال یا وسیله تحصیل مال است؛ لیکن در کلاهبرداری رایانه‌ای موضوع جرم فراتر می‌رود و علاوه بر مال شامل منافع مالی ، خدمات و امتیازات مالی نیز می‌شود؛ چون کلاهبرداری رایانه‌ای نوعی سوءاستفاده از رایانه و اینترنت است و از آنجایی که اکثر امکانات متضمن خدمات و مزایای مالی ، رایانه‌ای شده‌اند ، امکان سوءاستفاده از آنها زیاد است. جالب اینکه در قوانین برخی از کشورها کلاهبرداری از حد هر گونه سوءاستفاده مالی از طریق رایانه نیز فراتر رفته است؛ به عنوان مثال طبق بخش ۱۰۳۰ از ماده ۱۸ قانون جزای ایالات متحده امریکا مصوب ۱۹۸۳ و اصلاحی ۱۹۹۶، دسترسی بدون مجوز به اطلاعات طبقه‌بندی شده یا اطلاعات انرژی اتمی یا هر نوع اطلاعاتی که به کشور امریکا ضربه وارد نماید ، در زمره کلاهبرداری و فعالیت‌های مرتبط با آن به حساب آمده است.[۲۸]

۲۷- حسن بیگی ابراهیم، حقوق و امنیت در فضای سایبر، مؤسسهٔ فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر، چاپ اول، تهران، ۱۳۸۴، ص ۱۶۵.

۲۸- کامر داگلدس ای، ارتباط بین شبکه ای، ترجمه وحید فراهانی زاده، انتشارات جنگل،چاپ دوم، تهران، ۱۳۸۷، ص ۱ .

ارکان جرم کلاهبرداری رایانه‌ای:

تحصیل مال دیگری ممکن است با استفاده متقلبانه از رایانه انجام شود. در این صورت ارکان جرم مزبور با ارکان جرم کلاهبرداری به ویژه از نظر عنصر قانونی متفاوت است و به عنوان جرم خاص از کلاهبرداری موضوع ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء و اختلاس وکلاهبرداری مصوب ۱۳۶۷ مجمع تشخیص مصلحت نظام نیز متمایز می گردد.

الف-عنصر قانونی جرم:

ماده ۶۷ قانون تجارت الکترونیک

هرکس در بستر مبادلات الکترونیکی ، با سوء استفاده و یا استفاده غیر مجاز از « داده پیام ها» برنامه ها و سیستم های رایانه ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود ، محو ، توقف « داده پیام » ، مداخله در عملکرد برنامه یا سیستم رایانه ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه ، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مأخوذه محکوم می شود. در مورد عبارت سوءاستفاده نماید ، یعنی هرگونه اقدامات و دستیابی غیرمجاز را در واقع از مصادیق سوءاستفاده می توان ذکر کرد. مثلاً فرد با وارد کردن داده ها ، چه صحیح و چه کذب ، از امکانات فناوری استفاده می نماید و در نتیجه اموالی را برای خود یا دیگری کسب می کند ، یا اطلاعاتی را وارد می کند که وی در حسابش مقداری پول دارد و در نتیجه بانک برای وی مبلغی منظور کند .

تبصره – شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر در این ماده می باشد .

ماده ۱۳ قانون جرایم رایانه ای

این ماده مقرر داشته است : هرکس به طور غیرمجاز از سامانه های رایانه ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن ، تغییر ، محو ، ایجاد یا متوقف کردن داده ها یا مختل کردن سامانه ، 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 یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰.۰۰۰.۰۰۰) ریال تا یکصد میلیون (۱۰۰.۰۰۰.۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد. ماده ۱۳ به این شکل تنها اشخاص حقیقی است که میتوانند به این جرم ، محکوم شوند و اگر شخص حقوقی مرتکب آن شود مباحث مربوطه در ماده ۲۳ آمده است .

تغییر ، شامل تغییر غیرمجاز داده ها و اطلاعات است که بدین طریق مال ، وجه و خدمات مالی تحصیل می شود . از طریق محو نیز اطلاعات رایانه ای و مخابراتی حذف می شود و باز همان نتیجه مالی کسب می ـ شود و عبارت توقف یعنی ایجاد وقفه در فرایند تبادل داده ها و اطلاعات مثلاً دستور پرداختی که باید از

شعبه A به شعبه B برود ، کلاهبردار یک وقفه ایجاد می کند تا پرداخت از حساب وی صورت نگیرد و در نتیجه منافع مالی را کسب کند .[۲۹]

مداخله در عملکرد سیستم اختلال غیرقانونی در کارکرد سیستم است به هر شکلی اگر به تحصیل مال و منفعت بیانجامد کلاهبرداری است.عبارت و نظایر آن می رساند که این مصادیق حصری نیست و به هر شکلی که شخص از سیستم رایانه ای و مخابراتی که در ماده آمده است ، برخی معتقد بودند که به این سیستم ها ، سیستم ارتباطی هم اضافه شود ولیکن چون معنای سیستم ارتباطی گسترده و شاید دارای ابهام است ، ماده فقط سیستم رایانه ای و مخابراتی را مطرح کرده است . ایجاد وقفه در سیستم رایانه ممکن است موقت یادائمی باشد. مانند متوقف ساختن دستور پرداخت وجه به شخصی و طرف پرداخت قرار دادن خودبطور غیرمجاز.

منظور از سیستم رایانه ای ، وسیله یا مجموعه ای از وسایل وابزار مرتبط و به هم پیوسته است که مطابق با یک برنامه ای پردازش اطلاعات را انجام می دهد و منظور از سیستم مخابراتی ، سیستم و وسایل ارتباط از راه دور است به این ترتیب وقتی صحبت از سیستم رایانه ای یا مخابراتی می شود مصادیق مختلفی از کل وسایل مرتبط با رایانه و مخابرات را در برمی گیرد .

ب-عنصر مادی جرم

موضوع کلاهبرداری رایانه ای وجه یا مال یا منفعت یا خدمات یا امتیازات مالی است. کلاهبرداری رایانه ای به لحاظ موضوع از کلاهبرداری سنتی عام تر است و علاوه بر وجه و مال ، منفعت و خدمات و امتیازات مالی را نیز در بر می گیرد.

رایانه یا کامپیوتر وسیله ارتکاب جرم کلاهبرداری کامپیوتری است و ممکن است ارتکاب آن با رفتارهای مجرمانه دیگری مانند سرقت داده ها یا تغییر آنها و جعل و یا با نفوذ غیرمجاز همراه باشد که موضوع جرم کلاهبرداری کامپیوتری را تشکیل می دهد. بنابراین کامپیوتر گاهی خود ، موضوع ارتکاب جرم است مثل سرقت کامپیوتر و گاهی وسیله ارتکاب جرم کلاهبرداری کامپیوتری است؛ وقتی که استفاده متقلبانه از رایانه منتهی به تحصیل مال دیگری می شود.[۳۰]

کلاهبرداران ، معمولاً از هوش و استعدادهای زیادی برخوردارند و به ویژه در کلاهبرداری الکترونیکی از تخصّص و مهارت های فوق العاده هم استفاده می کنند. بدین ترتیب کشف جرایم آنان بسیار مشکل است. با توجه به قید واژه هرکس ، مرتکب این بزه همانند کلاهبرداری سنتی هر شخصی می تواند باشد.

۲۹- مجاب موسوی، بزهکاران یقه سفید، انتشارات مجد، چاپ سوم، تهران، ۱۳۸۶، ص۳۶.

۳۰- اولریش زیبر، جرایم رایانه‌ای، مترجمان: محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، نشر گنج دانش، چاپ اول، تهران، ۱۳۸۴، ص۶۳.

کلاهبرداری رایانه ای بزهی مرکب و دو رفتاری است. رفتار اول در آن که به طور تمثیلی در۱۳ قانون جرایم رایانه ای به آن اشاره شده است اعمالی چون وارد کردن ، تغییر، محو ، ایجاد یا متوقف کردن داده ها یا مختل کردن سامانه می باشند. این رفتارها باید به طور غیر مجاز صورت گیرند و اگر با اجازه انجام شوند ، کلاهبرداری رایانه ای رخ نداده ، هرچند که به تحصیل مال به طور غیر قانونی بینجامد.

رفتاردوم ، تحصیل اعم از دریافت واقعی یا مجازی یا منظور کردن اعتبار مالی برای خود می باشد. بستر انجام این بزه ، فضای سایبر است. بنابراین رفتارهای فیزیکی و تحصیل باید در فضای سایبر انجام گیرد. اگر فرد از رایانه و فضای سایبر تنها به عنوان وسیله ارتکاب جرم کلاهبرداری استفاده کند مثل این که از طریق تبلیغ ناروا در وبلاگ خود ، دیگری را فریفته و خود را دارنده مؤسسه اعزام دانشجو به خارج بشناساند و با دادن شماره حسابی ، کاربر یا کاربرانی را بفریبد تا پولی به حسابش بریزد یا در محیط بیرون پول یا مال را دریافت دارد ، کلاهبرداری سنتی انجام داده است نه رایانه ای.

ج-عنصر معنوی جرم

رکن روانی کلاهبرداری شامل عمد رفتاری یعنی عمد در رفتارهای رایانه ای تمثیلی و عمد در تحصیل مال یا منفعت و آگاهی مرتکب نسبت به تعلق مال یا منفعت یا خدمات مالی یا امتیازات مالی به دیگری است همچنین مرتکب باید بداند که انجام رفتارهای رایانه ای تمثیلی، بدون مجوز بوده است. رفتار مرتکب کلاهبرداری رایانه ای باید همراه با قصد فریب دیگری یا سبب اختلال و گمراهی سیستم های پردازش خودکار و نظایر آن شود.

(۱) عمد عام ، در سوءاستفاده و یا استفاده غیرمجاز از «داده پیام ها»، برنامه ها و سیستم های رایانه ای و وسایل ارتباط از راه دور است که با ارتکاب افعالی (نظیر ورود ، محو ، توقف «داده پیام» مداخله در عملکرد برنامه یا سیستم رایانه ای و غیره) دیگران را بفریبد و یا سبب گمراهی سیستم های پردازش خودکار و نظایر آن شود.

(۲)عمد خاص که تحصیل وجوه ، اموال یا امتیازات مالی و بردن اموال دیگران است .

بطوری که اگر مرتکب موفق به بردن اموال و وجوه دیگران نشود در مرحله شروع به جرم ومستوجب کیفر حداقل مجازات مقرر است.

در واقع ، عنصر مادی و معنوی جرایم عمدی ، مثل پشت و روی یک سکه است ، همیشه با هم ولی جدای از هم می باشند ، قصد متقلبانه از کیفیت عملیات قابل استنباط است.

نتیجه‌گیری:

جرایم رایانه ای یکی از پدیده های نوظهوری است که گرچه برخـی از جـرایم آن شـباهت هـایی بـا جـرایم سنتی دارد ، اما تفاوت هایی در روش و ماهیت و نوع جرم دارد که از لحاظ جـرم شناسـی و کیفرشناسـی و حقوق کیفری پژوهش های نوی را می طلبد.

جرایم رایانه ای به دلیل تأثیرات ناگواری که بر جامعه اطلاعاتی و کـاربران دارد ، برخـورد جـدی تـری را از سوی دولتمردان سیاسی و قضایی می طلبد. نظـارت و فیلتـر کـردن دقیـق تـر و جـدی تـری ، چـه بـرای جلوگیری از آسیب های امنیتی و چه آسیب های فرهنگی را می طلبد.

با توجه به پیشرفت تکنولوژی و اطلاعات ، بطور یقین افرادی سود جو و فرصت طلب نیز با فراگیـری دانـش درصدد سوء استفاده از تکنولوژی می‌باشند که این افراد سودجو ، امکانـاتی را کـه توسـعهٔ تکنولـوژی بـرای جامعه بشری به ارمغان می آورد دست خوش امیال و اغراض خـود سـاخته و باعـث ایجـاد مشـکلاتی بـرای استفاده کنندگان از تکنولوژی گردیده و باعث ایجاد شبهه و تردید برای اسـتفاده صـحیح از ایـن امکانـات و تکنولوژی شده‌اند تا جائیکه امروزه توجه دولتمردان ، حقوقدانان ، متخصصین در امر تکنولـوژی را بـه خـود معطوف کرده است. هرچه بیشتر تکنولوژی کامپیوتری توسعه یابد جرایم رایانه ای نیز توسـعه پیـدا خواهـد نمود ، ولی قوانینی که بتواند با این جرایم برخورد نماید پاسخگو نخواهد بود و دولتها می‌بایستی قوانین خود را متناسب با جرایم نمایند ، زیرا جرایم رایانه ای با جرایم غیر رایانه ای و کلاسیک اختلاف اساسی دارند.

اولاً: شیوهٔ ارتکاب آنها تقریباً آسان است.

ثانیاً: با منابعی اندک می‌توانند خسارات هنگفتی وارد نمایند.

ثالثاً: جرایم رایانه ای معمولاً در عرصه بین المللی بوده و معلوم نیسـت کـه کـدام حـوزهٔ قضـائی صـلاحیت رسیدگی به جرم را بر عهده دارد.

رابعاً: با توجه به بین المللی بودن جرایم رایانه ای ممکن است در بعضی از کشورها این موضوعات بـه عنـوان جرم تلقی نگردیده و یا حتی قانونی مبنی بر مجازات متخلفان وجود نداشـته باشـد و باعـث ایجـاد تعـارض گردد. لذا ضروریست که دولتها در مورد جرایم کامپیوتری قوانین کیفـری و نحـوهٔ مجـازات بـرای متخلفـان تصویب نموده تا شاید بتوانند مانع وقوع بزه رایانه ای شوند.

کلاهبرداری رایانه ای از جمله جرایمی است که با توجه به پیشرفت تکنولوژی پا به عرصه ظهور نهاده است ، جرایمی که با ویژگی های منحصر به فرد خویش قوانین سابق قدرت مقابله با آن را نداشته قانون ـ گذاران را مجبور به این کردند که قوانینی وضع کنند که جوابگوی این نیاز جامعه بشری باشد.

تدوین: عین اله مالامیری

صلوات بر محمد و آل محمد