

ویژگی‌ها و بررسی جرایم کلاهبرداری رایانه‌ای در نظام حقوقی ایران

مسلم صفری

کارشناسی حقوق، دانشگاه پیام نور شوش

چکیده

کلاهبرداری رایانه‌ای یکی از جرایم مهم در سیستم حقوقی ایران و اکثر کشورهای جهان به شمار می‌آید و با توجه به تنوع و پیچیدگی‌های خاص این جرم تعقیب و دستگیری مجرمان مشکل‌تر از تعقیب و دستگیری سایر مجرمان می‌باشد، در بیشتر موارد قربانیان تمایل چندانی به افشای جرم ندارند. این جرایم قابل لمس نبوده اما می‌تواند خطرات بی‌شماری را به دنبال داشته باشد یکی از ویژگی‌های این جرایم فرامرزی بودن، سهولت ارتکاب جرم و ناشناختگی مجرمین می‌باشد و این جرایم روز به روز در حال افزایش می‌باشد. این جستار که با روش توصیفی-تحلیلی و بر مبنای مطالعات کتابخانه‌ای صورت گرفته است، بر آن است که ضمن تعاریف جرم، جرم کلاهبرداری، و کلاهبرداری رایانه‌ای و انواع آن اشاره کرده و در پایان به دیدگاه حقوقی و کیفری نسبت به کلاهبرداری رایانه‌ای در قانون کیفری ایران بپردازد. با توجه به اینکه مسأله کلاهبرداری رایانه‌ای یکی از مهمترین مسائل حقوقی و انسانی است، ضرورت انجام این پژوهش مهیا شد. نتیجه این جستار حاکی از آن است که «کلاهبردار رایانه‌ای» از قدیمی‌ترین اشکال جرایم رایانه‌ای با ابعاد مالی است.

واژه‌های کلیدی: جزاء، جرم‌شناسی، کلاهبرداری رایانه‌ای، نظام حقوقی ایران

مقدمه

امروزه می‌توان به وضوح نیاز به رایانه و ابزار مرتبط به آن را در زندگی روزمره مشاهده کرد. با به وجود آمدن رایانه، کارهای انسان متحول شد و سهولت و آسایش بیشتری نسبت به قبل در کارها به چشم می‌خورد، اما به همان اندازه نیز مشکلاتی به وجود آورد. از جمله مشکلات رایانه‌ای، وابستگی شدید و عدم تحرک افراد در انجام امور و بیماری‌های روحی و جسمی و در همین راستا، جرائم رایانه‌ای را نیز به وجود آمد. هنوز نیم قرن از اختراع اولین رایانه نمی‌گذرد، البته سرعت عمل آن از ابتدایی‌ترین ماشین حساب‌های دیجیتال امروزی نیز کمتر بود، اما به هر حال تحولی شگرف در دنیای علم و فناوری محسوب می‌شد و از همین رو رایانه‌ها در این مدت کم به خوبی توانستند جای خود را در تمامی شئون زندگی انسان باز کنند و به نوعی خود را در تمامی پیشرفت‌ها سهیم سازند.

کلاهبرداری یکی از عنوان‌های مجرمانه کنایه‌آمیز است که به ظاهر با در نظر گرفتن اصل قانونی بودن بزه‌ها و مجازات و اصل لزوم شفافیت قوانین کیفری این عنوان با اجزا و عناصر تشکیل‌دهنده آن همخوانی ندارد، چه برخلاف عناوین مجرمانه‌ای همچون قتل، سرقت، انتقال مال غیر یا خیانت در امانت که در معنای لغوی و اصطلاحی، عناصر تشکیل‌دهنده و مصادیقی را که در برمی‌گیرد عیان می‌سازد، کلاهبرداری رایانه‌ای صرفاً کلاهبرداری از طریق رایانه نیست تا به واسطه آن نقش رایانه در حد یک وسیله ارتکاب جرم معرفی گردد؛ بلکه کلاهبرداری رایانه‌ای جرمی است که رایانه در آن نقش اساسی ایفا می‌کند و عمدتاً برخی از اجزای تشکیل‌دهنده رکن مادی کلاهبرداری را تحت‌تأثیر قرار می‌دهد و به همین دلیل است که کلاهبرداری رایانه‌ای از کلاهبرداری عام یا سنتی متمایز می‌شود.

کلاهبرداری رایانه‌ای، کلاهبرداری اینترنتی یا کلاهبرداری آنلاین اصطلاحات رایجی است که به حکم قانون می‌تواند از جرائم در حکم کلاهبرداری تلقی شود. در واقع، ضرورت، اجتناب‌ناپذیر استفاده از کامپیوتر در امور و امکان سوءاستفاده از آنکه از موارد بحران مهم در عصر دیجیتال است، قانونگذار را به عکس‌العمل قانونی واداشت. عنصر مادی جرم کلاهبرداری مهمترین و پیچیده‌ترین رکن محسوب می‌شود که عبارت است از رفتار مرتکب که باید به شکل فعل مثبت باشد ترک فعل نمی‌تواند هیچ‌گاه عنصر مادی جرم کلاهبرداری را تشکیل دهد.

ارائه‌ی آمار دقیق از تعداد واقعی جرایم رایانه‌ای و ضرر مالی که مجرمین وارد می‌کنند به چند دلیل ممکن نیست؛ نخست آنکه بیشتر جرایم رایانه‌ای قابل شناسایی نیستند. دوم، تنها تعداد انگشت شماری از جرایم رایانه‌ای به مقامات بالاتر گزارش داده می‌شوند. حفاظت از فضای مجازی به دلیل پیچیدگی بالای این گونه جرایم بسیار دشوار است. این مجرمین ابزارهای زیادی در دسترس دارند؛ بیشتر جرایم از طریق استفاده از رایانامه‌های ناشناس، استفاده از ابزارهای رمزگذاری و دستیابی به سیستم‌های دسته‌سومی رخ می‌دهند که مأموران قانون را برای یافتن و تعقیب مجرم با دشواری مواجه می‌کند. عموم مردم از ضررهایی که مجرمین رایانه‌ی وارد کرده و در آینده نیز وارد می‌کنند، آگاهی کافی ندارند.^۱

روش تحقیق

پژوهش حاضر یک تحقیق از نوع توصیفی اسنادی است بر اساس روش تحقیق کتابخانه‌ای، برای جمع‌آوری اطلاعات بعد از ماخذشناسی و گردآوری منابع، از ابزارهای فیش و فرم‌های مربوط به نکته‌برداری استفاده خواهد شد. بدین صورت که بعد از ماخذیابی کتب، مجلات و سایت‌های اینترنتی، اسناد مربوط به موضوع، فهرست موقت از مطایب مورد نیاز را تهیه و سپس با آماده‌سازی فیش‌ها، مرحله فیش‌برداری شروع و مطالب با استفاده از تکنیک ماخذگذاری به روش علمی تنظیم خواهد شد.

انصاری، باقر، ۱۳۹۸، حقوق ارتباط جمعی، چاپ هفتم، تهران: انتشارات سمت، ص ۱۲۱!

مفهوم جرم

جرم و جرمیه، با فتح جیم گفته شده است که به معنای قطع کردن است، اصل جرم بریدن میوه از درخت است، و برای هر کسب و کار زشت و مکروه استفاده شده است، و به معنی وادار کردن به کارهای ناپسند اطلاق می‌شود.^۲

مطابق ماده ۲ قانون مجازات اسلامی مصوب: ۵ / ۸ / ۱۳۷۰ هر رفتاری اعم از فعل یا ترک فعل که در قانون برای آن مجازات تعیین شده است، جرم محسوب می‌شود. مقابله با جرم، به دلیل آثار مخرب آنها در روابط اجتماعی و زندگی آحاد مردم، به عنوان یکی از وظایف اساسی حکومت‌ها و دولت‌ها درآمده است.^۳

عده‌ای می‌گویند: جرم یک پدیده اجتماعی است: یعنی عوامل فرهنگی، اجتماعی و محیطی در بروز رفتار مجرمانه مؤثر است؛ بنابراین، باید در شناخت و تبیین جرم، از روش جامعه‌شناختی سود جست و از مشاهده وقایع، ملاحظات آماری، شرایط زندگی، رابطه بین جرم و سایر عوامل غفلت نکرد. این گروه، جرم را چنین تعریف کرده‌اند: جرم عبارت است از نقض نظام اجتماعی و رفتاری که با ضوابط فرهنگی و اجتماعی حاکم بر جامعه مغایرت دارد و احساسات عمومی را جریحه‌دار می‌سازد. جرم مخالفت با اوامر و نواهی کتاب و سنت یا ارتکاب عملی است که به تباهی فرد یا جامعه بیانجامد. هر جرم را کیفری است که شارع بدان تصریح کرده یا اختیار آن را به ولی سپرده است.^۴

عناصر تعریف قانونی جرم**الف: عنصر قانونی:**

مراد از قانونی بودن جرم آن است که مادامی که قانون‌گذار عمل یا ترک عملی را امر یا نهی نکرده باشد، جرم محسوب نمی‌شود و قابل مجازات نیست. مراد از عنصر قانونی جرم این است که جرم فقط به کاری گفته می‌شود که در قانون ذکر شده و برای آن کیفری تعیین شده باشد. مراد از قانون، مفهومی گسترده است که علاوه بر قانون به معنای اخص، شامل آیین نامه‌ها، معاهدات بین‌المللی تصویب شده و حتی رویه قضایی، عرف، منابع فقهی و فتاوی معتبر نیز می‌شود.

ب: عنصر مادی جرم:

عبارت است از ترک یا فعلی که به صورت عمل یا قول از مرتکب سر بزند و از نظر قانون ممنوع باشد. مانند ایراد ضرب و جرح به دیگری یا خودداری از پرداخت نفقه زوجه یا اهانت به دیگری. ضرورت وجود عنصر مادی جرم، بدین معنا نیست که همیشه برای تحقق جرم باید تمام اجزای عنصر مادی حاصل شده باشد، چون ممکن است مقدار عمل انجام شده، که به علت وجود موانع خارجی (و نه انصراف مجرم) به نتیجه مورد نظر منتهی نشده، خود عنوان مجرمانه داشته و مشمول کیفری خاص باشد. در این صورت، مجرم، به عنوان شروع کننده جرم، مجازات می‌شود.

ج: عنصر روانی:

اصفهان، راغب، ۱۳۷۳. المفردات فی الغریب القرآن، ص ۹۱.

صص ۱، شماره ۱، دوره جنایی، های سیاست و جزا حقوق اینترنتی، کلاهبرداری قبال در ایران جنایی سیاست نقد ۱۳۹۵. ع. میلانی، ج. انصاری، ایران ساوه، اسلامشهر و واحد اسلامی، آزاد ۱۶۴-۱۴۵. دانشگاه

عمومی، دوره دو جلدی، تهران: نشر میزان، ص ۱۲۶. جزای حقوق. اردبیلی، محمدعلی، ۳۷۷.

و این همان قصد مجرمانه و سوء نیت است. قصد مجرمانه عبارت است از تمایل به انجام عملی که قانون آن را نهی کرده است و برای تحقق عمل مجرمانه (جرم)، قصد و علم و اختیار به عنوان عنصر روانی، شرط اصلی است. مراد از عنصر روانی (اخلاقی) جرم آن است که مجرم باید اراده یا شعور نقض قانون و ارتکاب جرم را داشته باشد.

تعریف قانونی جرم در قانون مجازات

ماده ۲ قانون مجازات اسلامی بیان می‌کند که هر رفتاری اعم از فعل یا ترک فعلی که در قانون برای آن مجازات تعیین کرده باشد جرم محسوب می‌شود و لذا اقدامات تأمینی و تربیتی جرم را متذکر نشده است.

تعریف جرم کلاهبرداری

ماده (۱) «قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری» در حال حاضر عنصر قانونی جرم کلاهبرداری است و اشعار می‌دارد: «هر کس از راه حيله و تقلب مردم را به وجود شرکت‌ها یا تجارت‌خانه‌ها یا کارخانه‌ها یا مؤسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد یا به امور غیر واقع امیدوار نماید یا از حوادث و پیش آمدهای غیرواقع بترساند و یا اسم و یا عنوان مجهول اختیار کند و به یکی از وسایل مذکور و یا وسایل تقلبی دیگر، وجوه و یا اموال یا اسناد یا حوالجات یا قبوض یا مفاصا حساب و امثال آنها را تحصیل کرده و از این راه مال دیگری را ببرد کلاهبردار محسوب و علاوه بر رد اصل مال به صاحبش از یک تا ۷ سال و پرداخت جزای نقدی معاون مالی که اخذ کرده است محکوم می‌شود و ...»

بدین ترتیب می‌بینیم که قانون تعریفی را از جرم کلاهبرداری ارائه نکرده است و به ذکر برخی مصادیق آن اکتفا کرده است و ما هم تعریف یکی از حقوقدانان برتر را در این رابطه آورده ایم. به این شرح که: «کلاهبرداری عبارت است از بردن مال دیگری از طریق توسل توأم با سوء نیت به وسایل یا عملیات متقلبانه».^۵

عناصر متشکله جرم کلاهبرداری

هر جرم از سه عنصر قانونی، مادی، و روانی تشکیل می‌شود و برای محکوم شدن متهم به ارتکاب جرم باید کلیه اجزای این عناصر توسط مرجع تعقیب اثبات شود.

گفتار اول: عنصر قانونی

در این رابطه لازم به ذکر است که به نظر بعضی نگارندگان عنصر قانونی را نباید به عنوان یک عنصر مجزا مورد بررسی قرار داد و عنصر قانونی در واقع پرتوی از اصل قانونی بودن جرم و مجازات و زیربنای عناصر مادی و روانی است. یعنی بنا به تصریح قانون است که ما می‌توانیم رفتار یا حالت خاصی را به عنوان عنصر مادی یا روانی جرمی بشناسیم پس رابطه بین عنصر قانونی و دو عنصر مادی و روانی یک عنصر طولی است نه عرضی و بدین ترتیب بحث از عنصر قانونی به طور مجزای از عناصر مادی و روانی موضوعیت ندارد. در هر حال عنصر قانونی جرم عام کلاهبرداری ماده (۱) قانون تشدید است.

گفتار دوم: عنصر مادی

عنصر مادی متشکل از ۳ جزء است به این شرح: ۱- رفتار فیزیکی که بسته به نوع جرم، فعل (مثلاً سرقت) یا ترک فعل (مثلاً جرم عدم اعلام ارتشا) است. ۲- مجموعه شرایط و اوضاع و احوال که وجود یا عدم آنها از نظر قانون

۵ - میر محمد صادقی، حسین. ۱۳۸۵، جرایم علیه اموال و مالکیت ص ۵۱.

شرط تحقق جرم می باشد. ۳- نتیجه حاصله از رفتار متهم که باید رابطه علیت با جزء اول فوق الذکر داشته یعنی رفتار متهم باعث نتیجه مجرمانه شده باشد.

گفتار سوم: عنصر روانی

حقوق جزا تا پایان قرن دوازدهم به انسان تنها به عنوان یک ابزار در ایجاد صدمه می نگریست و در مجازات کردن او توجهی به سوء نیت و عنصر روانی اش نداشت. بنابراین همان طور که حکم به از بین بردن چیزهایی که موجب بروز صدمه شده بودند (مثلاً حیوانات و یا چاقو یا تبری که در جرم قتل مورد استفاده قرار گرفته بود) می دارد، انسان مجرم را نیز، بدون توجه به قصد و نیت وی و تنها به علت ایراد صدمه از سوی او به دیگری مجازات می کرد. از حدود اواخر قرن دوازدهم تغییر جهت مهمی روی داد. از این زمان انسان به عنوان یک «عامل اخلاقی» شناخته شد که تنها در صورتی قابل مجازات محسوب می گشت که ارتکاب جرم را برگزیده باشد.^۶

عنصر روانی کلاهبرداری از دو جزء سوء نیت عام و سوء نیت خاص تشکیل می شود، منظور از سوء نیت عام اداره خودآگاه فرد در ارتکاب عمل مجرمانه و در اینجا عبارت از قصد استفاده از وسیله متقلبانه (و عمد در فعل) است. به عبارت دیگر کلاهبردار باید با علم به نقلی بودن وسیله مورد استفاده خود در استفاده از آن عمد داشته باشد پس هرگاه کسی به اشتباه، ولی صادقانه، معتقد به غیر متقلبانه بودن وسایل مورد استفاده خود باشد مثلاً وقتی از مردم برای خانه سای پول می گیرد واقعاً قصد خانه سایی داشته و فکر کند که از عهده این کار برخواهد آمد و یا استفاده از وسایل متقلبانه در حالت ناهشیاری مثلاً در حالت مستی رکن سوء نیت عام متزلزل خواهد بود. جزء دوم عنصر روانی جرم کلاهبرداری «سوء نیت خاص» یعنی قصد بردن مال دیگری است. فرد مرتکب از توسل به وسایل متقلبانه می تواند در پی اهداف مختلفی باشد از قبیل جلب نظر دیگری برای ازدواج، انتقام جویی، کسب شهرت و اعتبار و بسیاری اهداف دیگر. حال از میان همه این اهداف، وجود و اثبات قصد خاص بردن مال دیگری برای تحقق جرم کلاهبرداری ضروری است. باید اضافه کنیم که منظور از قصد بردن مال دیگری قصد بردن مال خاص یا مقدار معینی مال یا مال شخص معینی نمی باشد، برای مثال اگر کسی به قصد بردن اتومبیل دیگری از وسایل متقلبانه استفاده کند، ولی صاحب اتومبیل، تحت تأثیر وسایل متقلبانه مذکور، دوچرخه خود را در اختیار وی بگذارد یا این که به قصد گرفتن صد هزار ریال از دیگری به وسایل متقلبانه متوسل شود، ولی دیگری صد میلیون ریال در اختیار او بگذارد، در محکوم کردن وی به ارتکاب جرم کلاهبرداری اشکالی وجود نخواهد داشت، همین طور قصد بردن مال قربانی خاص نیز موثر در مقام نمی باشد.

کلاهبرداری (جرایم) رایانه‌ای

در دنیای امروز که از آن به عصر اطلاعات یاد می کنند، شاهد آن هستیم که با پیشرفت جهانی رایانه های شخصی و تجاری، فعالیت انسان ها در تمامی زمینه ها از حالت سنتی و دستی خارج کرده است. 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. این پیشرفت ها در زمینه های مختلف علوم و فناوری، باعث بالا رفتن سطح زندگی و آسایش بشر شده است. هر چند رایانه مزایایی برای بشر امروز به ارمغان آورده است، اما باین حال این نکته را باید پذیرفت که

۶. د.ک، تحلیل مبانی حقوق جزا، ص ۱۸-۱۷ و ۷۳-۷۱.

رایانه‌ها دارای جنبه منفی نیز می‌باشند و آن؛ خلق یکسری اعمال مجرمانه است که تا قبل از آن امکان ارتکاب چنین جرائمی ناممکن بوده است.

طبق تعریف ارائه شده از سوی گروهی از کارشناسان که به دعوت سازمان همکاری و توسعه اقتصادی OECD در پاریس در سال 1890 گرد آمده بودند، جرم رایانه‌ای را به این صورت تعریف کرده‌اند «هر عمل غیر قانونی، غیراخلاقی یا غیرمجاز نسبت به پردازش خودکار و یا انتقال داده‌ها جرم رایانه‌ای است»^۷ پروفیسور زیبراولریش از محققین مطرح در عرصه جرایم رایانه‌ای این تعریف را از این حیث سودمند دانسته است که امکان استفاده از فرضیات مختل و همه مطالعات جرم‌شناسی، کیفری، اقتصادی پیشگیرانه یا حقوقی را فراهم کند.

از جمله جرائم جدید ارتکاب یافته در این حوزه، کلاهبرداری است. جرم کلاهبرداری به عنوان یکی از جرائم علیه اموال و از قدیمی‌ترین جرائم محسوب می‌گردد. جرمی با چنین قدمت و سابقه که به صورت تفصیلی در ماده ۷۱ «قانون تشدید مجازات مرتکبین اختلاس، ارتشاء و کلاهبرداری» به آن پرداخته شده است. اکنون در کنار تعریف کلاسیک خود، شق جدیدی را در فضای رایانه‌ای در خود پرورده است که از آن به «کلاهبرداری رایانه‌ای» تعبیر می‌شود. تجسم عموم از کلاهبرداری آن است که انسانی با چرب‌زبانی و حيله و فریب، اموال دیگری را از چنگ او درآورد، ولی در دنیای ماشینی امروز لازم نیست انسان‌ها برای بردن اموال یکدیگر به شیوه‌های سنتی متوسل شوند.

ارایه یک تعریف از جرم رایانه‌ای می‌تواند به جهات ذیل دارای اهمیت باشد:

الف) بدون تعریف جرم رایانه‌ای جمع‌آوری اطلاعات آماری معنادار که می‌تواند به منظور تجزیه و تحلیل ساختارها و الگوهای جرم استفاده شود غیرممکن خواهد بود.

ب) چنانچه تعریف واحد یا تعریفی که از لحاظ ماهوی دارای تفاوت اساسی نباشند از جرم رایانه‌ای نداشته باشیم کاربران فنآوری اطلاعات و مقامات مجری قانون (مقامات تعقیب و تحقیق و قضات دادگاه‌ها) در وضعیتی نامشخص و فضایی مبهم قرار گرفته و نمی‌توانند تکالیف و وظایف قانونی خود را به نحو مطلوب انجام دهند.

ج) ارایه یک تعریف معین از جرم رایانه‌ای و همچنین داده‌های آماری و اطلاعات صحیح مبتنی بر یک تعریف معین برای آموزش عمومی افراد جامعه به منظور مقابله با تهدیدها و جلوگیری از ارتکاب جرم از طریق توسعه راه‌های حفاظتی و بازدارنده ضروری است.

د) به لحاظ فراملی بودن جرایم رایانه‌ای تعریف معین از جرم رایانه‌ای می‌تواند در انجام معاضدت قضایی و همکاری‌های بین‌المللی برای مبارزه با جرم رایانه‌ای موثر می‌باشد.^۸

تجارت‌خانه‌های یا شرکت‌ها وجود به را مردم تقلب و حيله را از کس هر کلاهبرداری؛ و ارتشاء اختلاس، مرتکبین مجازات تشدید «قانون 1 ماده غیر واقع آمده‌های پیش و حوادث از یا نماید امیدوار واقع غیر امور به یا دهد فریب واهی و اختیارات اموال داشتن به یا موهوم موسسات یا ها کارخانه مفاصا یا یا قبوض حوالجات یا اسناد یا اموال یا و وجو دیگر تقلبی وسایل یا و مذکور وسایل از یکی به و کند اختیار مجعول عنوان یا و اسم یا و بترساند و سال 7 تا یک حبس از به صاحبش، به مال اصل رد بر علاو و محسوب کلاهبردار ببرد را دیگری مال را این از و کرد تحصیل آنها امثال و حساب شود می محکوم است کرد اخذ که مالی معادل نقدی جزای پرداخت

فناوری حقوقی‌های جنبه بررسی همایش‌های مقاله ای، مجموعه رایانه جرم‌های بندی طبقه تعریف تاریخچه، عبدالصمد، (۱۳۸۴). آبادی خرم سلسبیل، ص ۲۶. تهران: قضایی، چاپ اول، توسعه و حقوقی معاونت قضائیه قوه گردآورنده: اطلاعات

انواع جرایم رایانه‌ای

جرایم کامپیوتری یا رایانه‌ای قابل طبقه‌بندی در سه رتبه یا نسل می‌باشند:

۱- جرایم طبقه‌ی نخست

حدوداً از سال‌های ۱۹۶۰ به بعد با به خطر افتادن حقوق فردی در کشورهای پیشرفته آغاز گشت. کثرت پدیده سرقت برنامه‌ها، استفاده غیرمجاز سیستم‌های رایانه‌ای جرایم اقتصادی مرتبط با رایانه، جاسوسی رایانه‌ای، سابوتاژ رایانه‌ای، نفوذ در رایانه‌های دیگران، تحت عنوان جرایم رایانه‌ای متجلی گردید.

۲- جرایم طبقه‌ی ثانی (جرایم علیه اطلاعات و داده‌ها)

این نوع جرایم در واقع همزمان با توسعه و پیشرفت تکنولوژی اطلاعات در قلمرو زندگی و توسعه‌ی ارتباطات بین‌المللی در دهه ۹۰، رو به شکل‌گیری و فزونی پیدا نمود. در این بازه‌ی زمانی مذکور سرعت زیاد تکنولوژی و پیشرفت روز افزون آن به ویژه تکنولوژی تلفنی و مخابراتی، کامپیوتری و نیز شبکه جهانی اینترنت زمینه‌ساز اقدامات مجرمانه و خرابکارانه بر علیه خطوط ارتباطی و داده‌ها در خصوص فناوری گشت. و به صورتی که بیان شد کم‌کم نسل دوم جرایم رایانه‌ای به نام جرایم علیه داده‌ها که مرکب از تکنولوژی مخابراتی و تکنولوژی رایانه بود کم‌کم ظهور و گسترش یافت.

۳- جرایم دسته‌ی سه یا همان جرایم سایبر

زمانی که رایانه در آستانه هزاره سوم «محیط سایبر» را به جهانیان ارائه کرد، قدرت واقعی خود را به اجرا گذاشت، قدرت فضای مجازی به قدری بالاست که گزاف نیست اگر بگوییم هر آنچه را که انسان بتواند متصور گردد نمونه مجازی آن در این محیط بیاید قابل دسترسی و قابل ساختن است که در حوزه‌های مختلف در جهت مثبت و منفی قابل استفاده و کاربرد می‌باشد. امروزه این فضای مجازی توان انجام امور مجازی نظیر رانندگی مجازی، جراحی مجازی و خلبانی مجازی و... را برای کسب مهارت برای ایشان فراهم ساخته است. و این ابزار کارآمد که ساخته‌ی انسان است همانند هر ابزار دیگری اگر چه دارای آثار زیاد و منافع فراوان در جهت تسهیل و روانسازی و پیشرفت زندگی انسان می‌باشد، اما زمینه ساز ارتکاب جرایم مختلف برای مرتکبان جرایم سایبری گشته است. در این نوع جرایم بدون آنکه از مرتکب اثری به جای بماند یا حتی مرتکب در موقعیت خطرناک قرار بگیرد، جرم واقع می‌گردد و مرتکب نیز از پیامدهای جرم فرار می‌کند. این جرایم تحت عنوان «جرایم سایبر» یا (جرایم در محیط مجازی) شناخته شده‌اند.^۹

تاریخچه اولین مجرم رایانه‌ای در جهان و ایران

تاریخچه مشخصی از زمان پیدایش جرم الکترونیکی و کامپیوتری وجود ندارد، ولی به هر حال این دسته از جرایم را باید زائیده و نتیجه تکنولوژی ارتباطی و اطلاعاتی دانست. براساس مطالعات صورت گرفته منشأ پیدایش جرم کامپیوتری و اینترنتی به قضیه روییس برمی‌گردد که بعد از بی‌مهری مسئولان یک شرکت فروش عمده میوه و سبزی به عنوان حسابدار آنها انتخاب می‌شود از طریق کامپیوتر اقدام حسابرسی یا تغییر قیمت‌ها و تنظیم درآمدجنس، مرجعی از مرجع آنها کاهش و به جای دیگری

مالمیر، محمود، زرخ، احسان، ۱۳۸۹. پیشگیری از بزه‌دیدگی سایبری، تهران، فصلنامه علمی ترویجی، مطالعات پیشگیری از جرم، سال پنجم، شماره^۹

واریز می‌کند. رومیس با ظرافت خاصی قیمت‌ها را تغییر می‌داد. بعد از آن با نام 17 شرکت محل و قراردادچک های جعلی صادر و از آن حساب برداشت م کرد به طوری که در کمتر از 6 سال بیش از یک میلیون دلار بدست آورده است، اما به دلیل نداشتن مکانیزم برای توقف این روند رومیس خودش را به محاکم قضایی معرفی می‌کند و به 10 سال زندان محکوم می‌شود. بدین ترتیب زمینه پیدایش جرم رایانه ای شکل می‌گیرد و دادگاه را به تدوین قوانین مدون وا می‌دارد. براساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ 26 خرداد 1378 به وقوع پیوست. این جرم توسط یک کارگر چاپخانه و یک دانشجوی کامپیوتر صورت گرفت که در کرمان اقدام به جعل چکهای تضمینی، مسافرتی کردند. بعد از این بود که گروهک‌های هکر موسوم به گروه مش قاسم و جرم‌های دیگری مرتکب می‌شدند، مواردی چون جعل اسکناس، اسناد و بلیط‌های شرکت‌های اتوبوس‌رانی، جعل اسناد دولتی از قبیل گواهینامه، کارت پایان خدمت، مدرک تحصیلی و... گسترش روز افزون اینترنت با سرعتی سرسام‌آور به رغم مزایای فراوان در عرصه‌های گوناگون سرگرمی، تجارت، ورزش، فرهنگ یا آموزش مشکلاتی را نیز به همراه داشته که به جرایم رایانه‌ای و اینترنتی معروف است. وجود رایانه و اینترنت مسائل امنیتی خاص خود را نیز به دنبال داشته است که احتمال خطرهای امنیتی برای رایانه‌های مرتبط شبکه‌هایی مانند اینترنت بیشتر است گسترش جرایم ارتكابی با رایانه به اندازه‌ای بوده که بیشتر کشورهای دنیا با اعمال قوانینی به مبارزه با این پدیده پرداخته و سعی در مهار آن داشته‌اند.^{۱۰}

ویژگی‌های جرایم رایانه‌ای

۱- فراملی بودن جرایم رایانه‌ای

جرم رایانه‌ای به دلیل ماهیتش اختصاص به محیط فیزیکی محدود نیست و می‌تواند به آسانی در سطح دنیا ارتکاب یابد. چون جامعه نو به شدت به اطلاعات وابسته است جرایم کامپیوتری به راحتی در مقیاسی بین‌المللی به وقوع می‌پیوندد و مسافت، زمان و مکان مانعی برای آن به حساب نمی‌آید. در این جرایم لازم نیست مجرم در محل وقوع جرم حضور فیزیکی داشته باشد، یک فرد می‌تواند از عراق به رایانه‌های وزارت دفاع آمریکا نفوذ کند و اطلاعات را در رایانه‌های دبی ذخیره کند؛ سپس آنها را به روس‌ها بفروشد. یا مثلاً برای سرقت از یک بانک مدت مشخصی لازم است که سارق با حضور در محل دست به چنین عملی بزند ولی ارتکاب جرم رایانه‌ای در مدتی کوتاه و بدون حضور در محل امکان‌پذیر است. به عنوان مثال در سال 1980 چهار جوان در مدرسه دالتون آمریکا از طریق یک سیستم کامپیوتری با شبکه اطلاعات و ارتباطات کامپیوتری کانادا ارتباط پیدا کرده و اطلاعاتی به دست آوردند.

شبکه جهانی اینترنت به مفهوم واقعی یک دهکده جهانی است که مرزهای ملی در آن معنا و مفهوم خود را از دست داده است. طبیعی است مجرمان ترجیح می‌دهند به لحاظ مصون ماندن از واکنش سریع دستگاه قضایی و انتظامی کشوری که نتیجه جرم در آن آشکار می‌شود از کشور دیگری اقدام به اعمال مجرمانه بنمایند و چنانچه مالی از این اقدامات حاصل شود در کشور سومی به عنوان جایگاه امن ذخیره گردد؛ بنابراین در عمل و در غالب موارد جرایم رایانه‌ای و تجارت الکترونیکی یک جرم حداقل دو کشور را درگیر خود می‌نماید. به نحوی که شاید بر خلاف جرایم سنتی که غالباً محدود ملی داشتند بتوان اصل را بر فراملی بودن جرایم رایانه‌ای نهاد. در حال حاضر تمام حوزه‌های اقتصادی از جمله بانکداری و هواپیمایی بین‌المللی به شدت و حتی به طور انحصاری به شبکه‌های مخابراتی بین‌المللی وابسته‌اند.

انصاری، باقر، ۱۳۹۸، حقوق ارتباط جمعی، چاپ هفتم، تهران: انتشارات سمت، ص ۹۸.

۲- تنوع مرتکبان

در برخی جرایم ارتکاب جرم مستلزم آشنایی با تکنیک یا تکنولوژی خاصی است. در جرایم رایانه‌ای کامپیوتر هدف یا وسیله و واسطه ارتکاب جرم است؛ بنابراین مجرم تا حدی از تخصص را داراست. بسته به نوع جرم کامپیوتری گاه آشنایی کلی با این تکنولوژی کافی و گاه نیاز به تخصص در سطح بالاست. سطح مهارت معمول در مجرمان کامپیوتری محور برخی از مباحث را تشکیل می‌دهد. برخی عقیده دارند سطح مهارت شاخصی برای مجرمان کامپیوتری به شمار نمی‌آید حال آنکه بعضی دیگر بر این باورند مجرمان بالقوه کامپیوتری افرادی باهوش باذوق و شوق و دارای انگیزه اند که آماده رویارویی با چالش‌های تکنولوژی هستند، یعنی همان خصایصی که در کارمندان بخش داده پردازی بسیار مورد پسند است.

تاریخ نشان داده است که طیف گسترده‌ای از افراد مرتکب جرایم کامپیوتری شده‌اند: دانشجویان، آماتورها، تروریست‌ها و اعضای گروه‌های جرایم سازمان یافته. سن مجرمان بین ده تا شصت سال است و دامنه مهارت آنها از سطح تازه‌کار تا حرفه‌ای را می‌پوشاند. بنابراین مجرمان کامپیوتری غالباً افرادی معمولی هستند و نه ابر تبه کارانی با توانای‌ها و استعداد‌های بی‌همتا. هر فردی با هر سنی و با داشتن مهارتی نه چندان زیاد و با انگیزه چالش‌های فنی امکان کسب منابع، اشتهار یا انتقام یا اشاعه باورهای عقیدتی یک مجرم رایانه‌ای بالقوه محسوب می‌شود.

۳- سهولت از بین بردن آثار وقوع جرم و مشکلات تعقیب و آیین دادرسی جرایم رایانه‌ای

نویسندگان جرایم رایانه‌ای و شیوه ارتکاب این گونه جرایم، نحوه رسیدگی و تعقیب را از جهت مسایل آیین دادرسی با چالش‌هایی رو به رو کرده است. مشکلات اولیه در تحقیقات مقدماتی بروز می‌کند چون عنصر مادی جرم کامپیوتری از طریق وارد کردن، محو، تغییر و... داده‌ها، اطلاعات، برنامه‌ها و سیستم کامپیوتری، مخابراتی و... تحقق می‌یابد. مقامات تعقیب و تحقیق دارای اختیاراتی هستند که در قوانین دادرسی کیفری بدان اشاره شده و به هنگام بازجویی، بازرسی، معاینه محل، توقیف اشیای مربوطه و... بر چگونگی کار آنها حکم فرماست. اما در جرایم رایانه‌ای با محیط‌های دیجیتالی سرو کار داریم و به تبع خصایص این محیط‌ها بر قواعد مرسوم اثر می‌گذارد.

حقوق جزا یک سره بر حمایت یا بحث از اشیاء و موضوعات و اهداف مادی، ملموس و فیزیکی پرداخته و از اشیاء، موضوعات و اهداف غیرمادی، غیر ملموس و غیر فیزیکی غافل مانده است. از این رو قواعد دادرسی برای همان اهداف یاد شده تبیین شده اند.^{۱۱}

دشواری‌ترین بخش از مشکلات ناظر به ادله اثبات دعواست. ادله اثبات به تبع جرم مطرح می‌شود از این رو تعریف دلیل کامپیوتری، نوع دلیل، منابع آن، شیوه تحصیل آن، قابلیت قبول، نحوه ارایه و چگونگی صدور حکم بر مبنای آن در محیط‌های دیجیتالی همه از موارد متنازع فیه است که تا حد زیادی قوانین مرسوم در مورد آنها ساکت است.^{۱۲}

تنها ردی که از مجرم رایانه‌ای برجای می‌ماند یک سری رد پاهای الکترونیکی است که به راحتی و بدون حضور در محل استقرار سیستم رایانه‌ای حامل این رد پاها می‌توان آنها را از بین برد. البته این به معنای عدم امکان بازبایی این داده‌ها نیست، اما کار گروه تحقیق را بسیار مشکل می‌کند. در اثر عواملی همچون عدم آگاهی و شناخت کامل بزه‌دیدگان از این جرایم، ترس

سال کشور) انفورماتیک عالی شورای دبیرخانه نشریه (انفورماتیک تخصصی خبرنگار سایبری، کامپیوتری جرایم شروع محمدحسن ۱۳۸۳. دزیانی^{۱۱}
 ۹۳، شماره نوزدهم
 همان منبع، ص ۴۱.

شرکت‌ها از لطمه به وجهه و اعتبار شرکت و از دست دادن اعتماد سرمایه‌گذاران، عدم تخصص ضلبطان قضایی در شیوه کشف و تعقیب این جرایم و فقدان امکانت کافی در این خصوص مشکلات فنی خاص در کشف و اثبات آنها و گنجانده نشدن عنوان جرایم رایانه‌ای در آمار رسمی به طور مجزا، رقم سیاه جرایم رایانه‌ای بسیار بالاست. تا آنجا که سازمان اطلاعات امنیت آمریکا این رقم را 85 تا 98 درصد اعلام نموده است.^{۱۳}

۴- سرعت بالای ارتکاب و قابلیت تکرار فراوان

جرایم رایانه‌ای غالباً بسیار سریع به وقوع می‌پیوندند و از شروع جرم تا اجرای آن فاصله‌ای وجود ندارد. گاهی فاصله تنها به اندازه فشردن یک کلید است مرتکب می‌تواند با استفاده از خصوصیات پیش گفته برای یک بار برنامه‌ای را روی رایانه هدف نصب نماید که مثلاً به طور مکرر مبالغ ناچیزی از حساب یک فرد یا شرکت برای او واریز شود و این امر تا بی‌نهایت تکرار شود این بدان علت است که عمل فیزیکی که مجرم انجام می‌دهد یک بار انجام می‌شود، اما رایانه به طور خودکار آن را تکرار می‌کند.^{۱۴}

۵- حجم صدمات و خسارات

در جرایم کلاسیک گاه مجرم برای حصول موفقیت در ارتکاب جرم باید مسیری دشوار و گاه تا حدی دشوار را طی کند تا در نهایت بتواند مالی را دریافت کند یا خسارتی به دیگری وارد آورد. حجم این مال بدست آمده یا خسارت وارده از یک حدی فراتر نمی‌رود، اما در جرم کامپیوتری به دلیل سهولت ارتکاب و حجم زیاد موضوعات، سرعت عملکرد کامپیوتر، عدم نیاز به تخصص یا تخصص بالا، عدم نیاز حضور فیزیکی مرتکب در محل و ... همگی موجب گردیده تا حجم صدمات و خسارات وارده افزون گشته و گاه به چندین هزار برابر جرایم معمولی برسد. وسعت خسارات وارده ناشی از یک نفوذ غیر قانونی یا گسترش ویروس در اینترنت می‌تواند در کسر ثانیه صدها هزار استفاده کننده در سراسر جهان را متحمل خسارت کند. عواقب جرایم کامپیوتری علاوه بر خسارات اقتصادی سنگین می‌تواند تهدیدی جدی برای امنیت بشر باشد. وابستگی امور حساس کشورها در زمینه‌های پزشکی، مخابراتی، هواپیمایی، امور امنیتی و نظامی و... به عملکرد کامپیوترها باعث می‌شود تا کوچکترین اختلال و خدشه در کار این سیستم‌ها عواقب وخیم و جبران ناپذیری را به دنبال داشته باشد.^{۱۵}

بررسی جرایم کلاهبرداری رایانه‌ای در نظام حقوقی ایران

قانون تجارت الکترونیکی در تاریخ ۱۳۸۲/۱۰/۱۷ تصویب گردید این قانون شامل هشت عنوان مجرمانه است که کلاهبرداری رایانه‌ای در بستر تجارت الکترونیکی، یکی از عناوین آن می‌باشد. ماده 67 قانون مزبور به کلاهبرداری رایانه‌ای اختصاص دارد، لذا جهت روشن نمودن موضوع ارکان تشکیل دهنده جرم کلاهبرداری رایانه‌ای موضوع ماده ۶۷ قانون الکترونیکی مورد بررسی قرار می‌گیرد.

۱- از حیث عنصر قانونی

تهران: انتشارات بهنامی، ص ۲۶. بزهکاری، چاپ اول، از نوین ای جلوه اینترنتی و کامپیوتری جرایم برومند. ۱۳۸۲. باستانی^{۱۳}!

همان منبع، ص ۴۶!

همان منبع، ص ۴۷!

عنصر قانونی لازم‌الاجرا در قوانین ایران ماده 67 ق.ت.ا، است که در تاریخ 1382/10/24 به تأیید شورای نگهبان رسیده است و ماده 13 قانون جرائم رایانه‌ای که 1388/3/5 به تصویب رسیده است. ماده 67 قانون تجارت الکترونیکی: «هرکس در بستر مبادلات الکترونیکی با سوءاستفاده و یا استفاده رایانه‌ای وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف(داده پیام)، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سامانه‌های پردازش خودکار و نظایر آنها شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند وام وال دیگران را ببرد، مجرم محسوب و به مجازات محکوم می‌شود.

تبصره: مجازات شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر ماده می‌باشد. ماده 13 قانون جرائم رایانه‌ای: «هر کس به طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند... به مجازات محکوم خواهد شد.»

۲- از حیث عنصر مادی

۲-۱- رفتار مرتکب

از سیاق الفاظ به کار رفته در قانون مثل «محو»، «مختل کردن سامانه» و ... برمی‌آید که تحقق جرم فوق همانند کلاهبرداری سنتی فقط با فعل مثبت متصور است. همچنین در ماده یک قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری ذکر «توسل به وسایل تقلبی دیگر» که در ادامه قانون‌گذار به نحو تمثیل به ذکر مصادیقی از امور متقلبانه می‌پردازد، همگی دال بر فعل مثبت است. این رفتار مرتکب از سه جزء زیر است و بنابراین، جرم مرتکب به حساب می‌آید:

۱- سوءاستفاده یا استفاده غیرمجاز از «داده پیام»ها، برنامه‌ها و سامانه‌های رایانه‌ای و استفاده از محو، تغییر و غیره.

۲- فریب خوردن دیگران یا گمراه شدن سامانه‌های پردازش خودکار و مانند آن

۳- تحصیل وجوه، اموال یا امتیازهای مالی و بردن اموال دیگران از طریق اعمال یاد شده برای خود یا دیگران.

۲-۱-۱- سوءاستفاده یا استفاده غیرمجاز

واژه‌های «سوءاستفاده» یا «استفاده غیرمجاز» یک معنا دارند و ذکر هر دو واژه را می‌توان ناشی از عدم دقت لازم در تنظیم متن قانون دانست.

- (۱) «محو داده پیام» به معنای از بین بردن چنین داده‌ای است که به نظر می‌رسد از فهرست حداقل شورای اروپا گرفته شده است. برای مثال، اگر کارمندی با حذف سابقه دریافت حقوق خود از سیستم حسابداری شرکت، معادل حقوق خود را دوباره دریافت کند و با این عمل منفعت مالی برای مرتکب به دست آید، مرتکب محو داده پیام شده است.
- (۲) «توقف داده پیام» به معنای مصدري «متوقف کردن» داده پیام است که از تعریف فهرست حداقل شورای اروپا گرفته شده است. متوقف کردن می‌تواند موقتی یا دائمی باشد.

سال ۱۹۸۵-۱۹۸۶ توسط در جرائم کامپیوتری موافقتنامه تصویب نمود اشار زیر اقدامات به می‌توان کامپیوتری جرائم زمینه در المللی بین عرصه دُر و تدوین برای اروپا شورای تخصصی ۱۹۸۹ کمیته سال در شد. برداشته کامپیوتری جرائم با مرتبط قوانین تدوین برای زیادی گام های اروپا شورای المللی بین انجمن که همایشی در. گرفت قرار نیز شورا تصویب که مورد نمود پیشنهادهایی کامپیوتری جرائم به مربوط جنائی سیاست نمودن یکنواخت مبادرت اروپا، شورای میلادی 2001 سال در نهایتاً. نمود تدوین مستقل کامپیوتری جرائم عنوان به را مسائل از یکسری سال ۱۹۹۴ داشت در جزا حقوق می باشد گفتار هشت و چهل و چهار فصل شامل موافقتنامه این که نمود کامپیوتری جرائم موافقتنامه وضع به

۳) «متوقف کردن داده پیام» به این طریق می‌تواند واقع شود که طی یک معامله تجاری، پس از انجام مرحله‌هایی همچون بررسی حساب خریدار مبنی برداشتن موجودی کافی، دستور کسر از حساب خریدار واریز به حساب فروشنده صادر شده و معامله تمام شده فرض شود و کالا تسلیم خریدار گردد، اما خریدار با سلسله اقدام‌هایی که از قبل انجام داده، به طور کلی مانع فرستادن داده حاوی دستور پرداخت به بانک شده باشد. یا اینکه به طور موقت جلوی داده مربوط را سد کرده تا فوراً با مراجعه به یک دستگاه خودپرداز یا مراجعه به بانک از رهگذر امکانات بانکداری اینترنتی، وجوه مزبور را قبل از وصول دستور پرداخت به بانک به حساب دیگری منتقل کند. این فعل‌های یاد شده تمثیلی هستند. «مداخله در عملکرد برنامه یا سیستم رایانه‌ای» این عبارت در تعریف توصیه‌نامه شورای اروپا از کلاهبرداری رایانه‌ای آمده است. در قانون جرائم رایانه‌ای از «مختل کردن» استفاده شده است.

۲-۱-۲- فریب افراد و گمراهی دستگاه‌ها

فریب خوردن از جمله مؤلفه‌های لازم برای تحقق این جرم دانسته شده است. اما آوردن این جزء در رکن مادی جرم کلاهبرداری رایانه‌ای از نوآوری‌های قانون‌گذار ایرانی است و در هیچ‌یک از اسناد بین‌المللی این مؤلفه در تعریف کلاهبرداری رایانه‌ای نیامده است. زیرا فلسفه پیش‌بینی عنوان مجرمانه «کلاهبرداری رایانه‌ای» بر وجود مؤلفه «فریب» در کلاهبرداری سنتی و عدم آن در این عنوان جدید مبتنی است. در واقع، قانون‌گذار ایرانی با ذکر این عبارت «کلاهبرداری رایانه‌ای سنتی» را که به معنای فریفتن مالباخته از رهگذر امکانات جدید رایانه‌ای مانند صفحه‌های وب یا پست الکترونیکی است. در این ماده جرم انگاری کرده و آن را از شمول ماده 1 ق.ت.م خارج کرده است. در حقیقت، ماده 67 ق.ت.ا.^۷ از جهت اختصاص به «بستر مبادلات الکترونیکی» خاص مؤخر است که عام مقدم را، تخصیص می‌زند.

در نتیجه، اگر شخصی در بستر مبادلات الکترونیکی با پخش تبلیغات موهوم با استفاده از شبکه اینترنت مرتکب کلاهبرداری رایانه‌ای سنتی شود، مشمول این ماده است؛ بنابراین، مجازات وی کمتر از فردی است که خارج از این بستر عین همین اقدام را انجام دهد یا اینکه تبلیغات موهوم را به صورت دستی بین افراد پخش کند که این امر خلاف اصول قانون‌گذاری منصفانه است. گمراه کردن به معنای «او را سرگردان کردن»، «او را فریب دادن» هیچ‌یک از این مفاهیم در مورد رایانه قابل تحقق نیست. با این وصف، اگر کسی مرتکب اعمال مندرج در صدر ماده 67 شود و از آن رهگذر اموالی هم تحصیل کند، ولی موجب فریب دیگران نشده باشد، عمل وی مشمول این ماده نخواهد شد زیرا گمراه کردن سیستم رایانه‌ای قابل تحقق نیست در نتیجه اصولاً «کلاهبرداری رایانه‌ای محض» در این ماده جرم انگاری نشده است.

وسایل و رایانه‌ای سیستم‌های و از «داده پیام» برنامه‌ها مجاز غیر استفاد یا و استفاد سوء با الکترونیکی، مبادلات بستر در کس ماده ۶۷: «هلا سبب یا و بفریبید را دیگران غیر و رایانه‌ای سیستم یا برنامه عملکرد در مداخله ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف داده پیام دیگران را اموال و کند تحصیل مالی امتیازات یا اموال، وجوه دیگری یا خود برای طریق این از و شود آن نظایر و خودکار پردازش سیستم‌های گمراهی می‌شود محکوم مأخوذ مال معادل نقدی جزای پرداخت و سال سه تا یک از حبس به اموال صاحبان به مال رد بر علاو و محسوب مجرم ببرد می‌باشد ماد این در مقرر مجازات حداقل آن مجازات و محسوب جرم نیز جرم این به شروع: تبصره

۳-۱-۲- تحصیل وجوه، اموال و...

این جزء یکی از موارد زیر را دربر می گیرد:

1- تحصیل مال متعلق به دیگران برای خود یا دیگری.

2- تحصیل وجوه برای خود یا دیگری.

3- تحصیل امتیازهای مالی برای خود یا دیگری.

صرف تحصیل وجه یا امتیاز مالی (مانند وام) برای تحقق جرم کفایت می کند و گرفتن مبلغ وام برای تحقق جرم ضرورت ندارد. این تحصیل باید برای خود مرتکب یا دیگری باشد. از نظر حقوق دانان چنین برداشت می شود که منظور از «دیگری» «فرد مورد نظر مرتکب» است. البته ضرورتی ندارد که آن «دیگری» از قصد مرتکب آگاهی داشته باشد.

۳- از حیث عنصر معنوی

قانون گذار در ماده ۶۷ قانون تجارت الکترونیک اشاره می کند هر کس با سوء استفاده یا استفاده غیر مجاز (عنصر معنوی یا روانی جرم) از راه دور ارتکاب افعالی نظیر ورود، محو، توقف داده پیام مداخله در عملکرد برنامه یا سیستم (عنصر مادی جرم) بشود. رفتار مرتکب کلاهبرداری رایانه‌ای باید همراه با قصد فریب دیگری یا سبب اختلال و گمراهی سیستم های پردازش خودکار و نظایر آن شود.

۱- عمد عام، در سوء استفاده و یا استفاده غیر مجاز از «داده پیام» ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور است که با ارتکاب افعالی (نظیر ورود، محو، توقف «داده پیام» مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره) دیگران را بفریبید و یا سبب گمراهی سیستم‌های 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 و مستوجب کیفر حداقل مجازات مقرر است. در واقع، عنصر مادی و معنوی جرائم عمدی مثل پشت و روی یک سکه است، همیشه با هم ولی جدای از هم می‌باشند، قصد متقلبانه از کیفیت عملیات قابل استنباط است.

مجازات جرم کلاهبرداری رایانه‌ای

مجازات اصلی این جرم عبارت است از «حبس از یک تا پنج سال و جزای نقدی معادل مال گرفته شده» در خصوص جزای نقدی مقرر در ماده، این ابهام وجود دارد که اگر فرد امتیازی مالی به دست آورده باشد، آیا به جزای نقدی محکوم خواهد شد یا خیر؟ به نظر می‌رسد که با توجه به اصل تفسیر محدود قوانین کیفری و تفسیر به نفع متهم پاسخ سؤال فوق منفی خواهد بود.

در مورد مجازات شروع به کلاهبرداری نیز روشن نیست که حداقل کدام مجازات مقرر در ماده مورد نظر است و انگهی، در شروع به کلاهبرداری مالی به دست نیامده است که حکم به جزای نقدی داده شود. در نتیجه به نظر می‌رسد که برای شروع به این جرم باید مجازات حبس را ملاک قرارداد. مجازات در قانون جرائم رایانه‌ای: مرتکب علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد.^{۱۸}

۱۸، ۵۹، شماره دادگستری، حقوقی مجله الکترونیک، تجارت قانون در مندرج های جرم و بررسی نقد جواد، ۱۳۸۶، نیا، جاویدا

نتیجه‌گیری

جرایم رایانه‌ای جرایمی سازمان یافته‌اند که از طریق اشخاص حرفه‌ای و با سواد انجام می‌شوند و همیشه قوانین رایانه‌ای امروزه برای مجازات مجرمین کافی، اما کامل نمی‌باشد چون هر روز جرایم جدیدی به وجود می‌آید که برای مجازات آنها نیاز به قوانین جدید داریم.

همانگونه که جرایم اینترنتی همیشه در حال روز شدن هستند بایستی تلاش کرد تا بتوان با نو شدن جرایم هر ساله قوانینی را که در زمینه جرایم جدید قابل اعمال باشد ارائه کرد چون رایانه و اینترنت همیشه شکل‌های مختلفی به خود می‌گیرند برای پیشگیری از این جرایم باید همه دستگاه‌ها تلاش کنند و مردم نیز توصیه‌های مسئولین را در این مورد جدی بگیرند و در هنگام استفاده از اینترنت و رایانه مورد استفاده قرار دهند تا مورد سوء استفاده دیگران قرار نگیرند. همچنین اگر دیدند سایت یا وبلاگی برخلاف قوانین تعیین شده در حال ارائه مطلب باشد موضوع را سریعاً به دادستانی اطلاع تا نسبت به اعمال فیلتر در مورد آن سایت اقدام شود قضات نیز می‌بایست به شدت با کسانی که اقدام به جرایم رایانه‌ای می‌کنند برخورد نمایند چون این جرایم هم سبب بردن مال و هم سبب بردن آبروی اشخاص می‌گردد.

برخورد قضات نیز در پیشگیری از وقوع جرم اهمیت دارد بایستی سعی شود در زمینه جرایم رایانه‌ای مجازات‌ها بازدارندگی بیشتری داشته باشد تا هم سبب ارباب مردم و هم سبب عبرت گرفت مجرمین شود تا دیگر اقدام به چنین جرایمی ننمایند.

منابع و مأخذ

۱. اصفهانی، راغب. (۱۳۷۳). *المفردات فی الغریب القرآن*، تهران: انتشارات مصطفوی.
۲. انصاری، باقر. (۱۳۹۸). *حقوق ارتباط جمعی*، چاپ هفتم، تهران: انتشارات سمت.
۳. اردبیلی، محمدعلی. (۱۳۷۷). *حقوق جزای عمومی*، دوره دو جلدی، تهران: نشر میزان.
۴. انصاری، ج.، میلانی، ع. (۱۳۹۵). *نقد سیاست جنایی ایران در قبال کلاهبرداری اینترنتی*، حقوق جزا و سیاست‌های جنایی، دوره 1، شماره ۱، صص ۱۶۴-۱۴۵. دانشگاه آزاد اسلامی، واحد اسلام شهر و ساوه، ایران.
۵. باستانی، برومند. (۱۳۸۳). *جرایم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری*، چاپ اول، تهران: انتشارات بهنامی.
۶. خرم‌آبادی عبدالصمد. (۱۳۸۴). *تاریخچه، تعریف طبقه‌بندی جرم‌های رایانه‌ای*، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات گردآورنده: قوه قضائیه معاونت حقوقی و توسعه قضایی، چاپ اول، تهران: سلسبیل.
۷. جاوید نیا، جواد. (۱۳۸۶). *نقد و بررسی جرم‌های مندرج در قانون تجارت الکترونیکی*، مجله حقوقی دادگستری، شماره ۵۹.
۸. دزیانی محمدحسن. (۱۳۸۳). *شروع جرایم کامپیوتری سایبری*، خبرنامه تخصصی انفورماتیک نشریه دبیرخانه شورای عالی انفورماتیک کشور) سال نوزدهم شماره ۹۳،
۹. میر محمدصادقی، حسین. (۱۳۸۵). *جرایم علیه اموال و مالکیت*، تهران: نشر میران.
۱۰. مالمیر، محمود، زرخ، احسان. (۱۳۸۹). *پیشگیری از بزه‌دیدگی سایبری*، تهران، فصلنامه علمی ترویجی، مطالعات پیشگیری از جرم، سال پنجم، شماره ۱۷، صص ۳۲

Characteristics and examination of computer fraud crimes in Iran's legal system

Muslim Safari

Abstract

Computer fraud is one of the most important crimes in the legal system of Iran and most countries of the world, and due to the diversity and complexities of this crime, the pursuit and arrest of criminals is more difficult than the pursuit and arrest of other criminals. In most cases, the victims do not have much desire to disclose the crime. These crimes cannot be touched, but they can lead to countless dangers. One of the characteristics of these crimes is that they are cross-border, the ease of committing crimes, and the unknown nature of the criminals, and these crimes are increasing day by day. This research, which was done with descriptive-analytical method and based on library studies, aims to point out the definitions of crime, fraud crime, and computer fraud and its types, and at the end, it points to the legal and criminal point of view of computer fraud. in the criminal law of Iran. Considering that the issue of computer fraud is one of the most important legal and humanitarian issues, the necessity of conducting this research was provided. The result of this research indicates that "computer fraud" is one of the oldest forms of computer crimes with financial dimensions.

Keywords: punishment, criminology, computer fraud, legal system of Iran
