فصـــــلنامه بیـــن المللـــــی قـــانـــون یـــار
License Number: 78864 Article Cod: 2020S4D15SH1M554 ISSN-P: 2538-3701

بررسی جزایی ابعاد و ارکان جرم کلاهبرداری رایانه ای

(تاریخ دریافت ۱۳۹۹/۰۳/۱۵، تاریخ تصویب ۱۳۹۹/۰۹/۱۲)

دکتر کیوان مرادی زاده

مقدمه

پیشرفت جوامع و به‌ویژه توسعهٔ فناوری‌ها و فضای مجازی سبب شکل‌گیری جرایمی شده‌است که درگذشتهٔ نه‌چندان دور به این شکل وجود نداشتند. جرایمی که با شکل و شیوه خاص ارتکاب خود و در عین حال در به‌دلیل تحققشان در ابعاد بسیار منتوع و گسترده؛ سبب شدند که کشورهای مختلف از جمله ایران، به تعریف و تبیین آن‌ها بپردازند و قوانین خاصی را نیز برای آنان ایجاد کنند. کلاهبرداری کامپیوتری یا رایانه‌ای (Cyber fraud) یکی از این جرایم است که در فضای مجازی ارتکاب می‌یابد. قانون‌گذار در سال ۱۳۸۸ قانونی را تحت عنوان قانون جرایم رایانه‌ای به تصویب مجلس رساند. در ماده ۱۳ این قانون کلاهبرداری رایانه‌ای تعریف شده‌است: «هرکس 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 مـال 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. قانون‌گذار در این ماده رفتارهایی که به‌وسیله آن‌ها جرم کلاهبرداری رایانه‌ای محقق می‌شود را مثال زده است. منظور از ورود، وارد کردن اطلاعات به رایانه برای پردازش است. برای مثال کسی که کارت عابر بانک دیگری را برداشته و با واردکردن رمز آن در دستگاه خودپرداز، حساب وی را خالی می‌کند؛ مرتکب جرم کلاهبرداری رایانه‌ای با وارد کردن داده

است. تغییر داده شامل انواع تغییرات جزیی و کلی در داده‌های افراد است. مثلا در داده‌های حساب بانکی خود تغییر ایجاد می‌کند و قسط پرداخت نشده را، پرداخت شده نمایش می‌دهد. در این مقاله قصد داریم به صورت عمقی و دقیق در ابتدا به شناسایی و ابعاد حقوقی جرم کلاهبرداری رایانه ای بپردازیم سپس ارکان تشکیل دهنده این جرم را مورد مداقه قرار دهیم.

واژگان کلیدی: کلاهبرداری رایانه ای، سرقت رایانه ای، هک کردن کامپیوتر، جرایم کامپیوتری، سایبر

مقدمه

ماهیت جرائم رایانه‌ای ناشی از توسعه روز افزون فناوری اطلاعات و ورود به عصر اطلاعات است که رایانه می تواند ابزار، هدف و موضوع ارتکاب جرم باشد، وغالبا به دودسته تفکیک می‌شوند دسته اول دارای عناوین و توصیف‌های جزایی کلاسیک هستند نظیر جعل رایانه‌ای،کلاهبرداری رایانه‌ای وجاسوسی رایانه‌ای که در این جرائم رایانه به عنوان ابزاری برای رفتار مجرمانه به کار می‌رود. دسته دوم جرایم رایانه‌ای جدیدند این جرائم ناشی از چگونگی به کارگیری فناوری اطلاعات هستند جرائمی نظیر دسترسی غیر مجاز، اختلال در داده ها وسیستم‌های رایانه‌ای هرزه نگاری این نوع جرائم جدید هستند . در هردو دسته موضوع جرم با فرض مال بودن و دارای ارزش بودن داده ها و اطلاعات: مال دیگران، امنیت، آسایش فردی، آسایش عمومی، اخلاق عمومی و حیثیت افراد است. عمومی‌ترین عنوان مجرمانه در حوزه فناوری اطلاعات هک است در حقیقت اولین اقدام برای شروع یک جرم رایانه‌ای یا بهتر بگوییم رفتار قابل سرزنش در فضای سایبر دسترسی غیر مجاز به داده ،رایانه ، شبکه به طور کلی هر سیستم رایانه‌ای است که مربوط به شخص دیگری باشد است این ورود غیر مجاز میتواند برای اطلاعات، داده‌ها، برنامه‌ها یا سیستم‌های رایانه‌ای غیر مجاز برای مرتکب: نشان دادن مهارت شخص، کسب مال مربوط به دیگری ، اختلال وخرابکاری ، جاسوسی و... باشد .این عمل فارغ از نیت مرتکب کاملاً یک رفتار قابل سرزنش وناپسند است . ونحوه ارتکاب این جرائم عبارت است از، ورود، تحصیل ، حذف، اختلال ، دستکاری و ... در. نبود قانون در عرصه سایبر همچون دیگر عرصه ها و مظاهر پیشرفت بشری به هرج و مرج می‌انجامد درست شبیه به آیین نامه رانندگی روز اولی که اتو مبیل ساخته شد کسی به مقررات آن توجه نمی‌کرد ولی امروزه کمتر کسی نافی لزوم مقررات رانندگی است اگر امروز مقررات رانندگی کان لم یکن تلقی شود چه روی می‌دهد. قوانین عرصه فناوری اطلاعات هم همین طور هستند اگر قانونی نباشد کدام آدم عاقلی می تواند خطر سرمایه گذاری در این عرصه را بپذیرد وکدام یک از شما در جایی سرمایه‌گذاری میکنید که پیوسته مورد تاخت و تاز ناقضین مال وحیثیت

افراد می‌شوند و هیچ قانونی برای جلوگیری و توبیخ آنها وجود ندارد. آیا شما ریسک رفتن به خیابان و رانندگی را می‌پذیرید؟. بر این اساس در لایحه ای که تحت عنوان جرائم رایانه‌ای توسط دولت تقدیم مجلس شد و اکثر عناوین مجرمانه هر دو دسته مذکور در لایحه جرم‌انگاری شده است البته غیر بخشی که در لایحه مربوط به جرم انگاری جرائم مذکور است بخش دیگری نیز که مشتمل بر آیین دادرسی ونحوه رسیدگی به جرائم رایانه‌ای ودیگر جرائمی که ناشی از توسعه کاربری فناوری اطلاعات است در این لایحه دیده شده است. لایحه پس از تصویب کلیات آن در مجلس شورای اسلامی در حال بررسی در شور دوم آن است که برای اصلاح برخی نقایص و اشکالات مرکز پژوهشهای مجلس گزارشی را تهیه نمود که این گزارش مورد توجه مجلس قرار گرفت و امیدواریم پس از رفع مشکلات این لایحه هرچه زودتر تصویب شده و و کشور ما نیز به جرگه کشور هایی بپیوندد که رفتار غیر مسئولانه افراد در محیط سایبر را مستوجب سرزنش دانسته است و پس از این ناظر فروش نرم افزار های هکری و آموزشهای هکری نباشیم زیرا تفاوتی بین مال ،اخلاق، حیثیت ، آبرو در محیط سنتی و سایبر وجود ندارد همانطور که آموزش دزدی ناپستد است آموزش هک هم عملی قابل سرزنش است. هم زمان با ورود انسان به هزاره دوم میلادی ، هم چنان شاهد جرم و جنایت های بی شماری هستیم اگر چه از نظر ماهوی دچار تغییر نگشته اما از نظر استفاده از ابزارها و وسایل گوناگون تغییرات شگرفی به خود دیده است. انسان امروزی هم چنان دزدی می کند ، آدم می‌کشد و به مال و حریم دیگران تجاوز می‌کند . در گذشته فرد با یک داس یک چوب و یا یک خنجر و کمی بعد با اسلحه ابزار تجاوز و دزدی و باج خواهی از اموال دیگران بود . اما امروزه با فشار دادن یک کلید و وارد کردن چند عدد می‌شود به حریم دیگران تجاوز و یا به مال او دست اندازی نمود .حوزه جرائم در زندگی امروز بشر آن قدر پیچیده شده که قانون گذاران مجبورند تحولات جرم را به صورت مداوم زیر نظر داشته باشند. به تدوین قوانین صحیح گام بردارند . اما همانطور که مشخص شد در زندگی اجتماعی امروز بشر تحولاتی صورت گرفته که به تاثیراز آن جرائم نیز اشکال متفاوتی گرفته است. جرائم اینترنتی مصداق بارز این تحولات در زندگی اجتماعی انسان ها می‌باشد. در مورد جرائم رایانه‌ای تعاریف

زیادی مطرح شده است.طبق تعریفی که سازمان ملل متحد از این نوع جرائم نموده جرم رایانه‌ای می تواند شامل فعالیت‌های مجرمانه‌ای باشد که ماهیتی سنتی دارند اما از طریق ابزار مدرنی مثل رایانه و اینترنت صورت می‌گیرد.از طرف دیگر متخصصان سازمان OECD تعریف متفاوتی از آنچه گفته شد ارائه داده اند آنها معتقدند سوء استفاده از رایانه ، هر نوع رفتار غیر قانونی ، غیر اخلاقی و غیر مجاز مربوط به پردازش خودکار و انتقال داده‌ها جرم اینترنتی محسوب می‌شود . از تعاریف ارائه شده می توان به این نتیجه رسید که حقیقتاً ماهیت جرم تفاوتی ندارد و این ابزار است که وقوع جرم در بستری جدید را فراهم می نماید . اما پیش از آنکه بخواهیم در مورد جرائم رایانه‌ای به بحث بپردازیم باید وارد حوزه جرائم سایبر شویم. جرائم در فضای سایبر یا فضای سایبری به واسطه تغییرات سریع فناوری اطلاعات در قلمرو سیستم‌های رایانه‌ای و مخابرات امکان وقوع می‌یابند در این گونه جرائم تاکید بر رایانه نیست بلکه رایانه وسیله ای است که ابزار وقوع جرم قرار می گیرد که به آن نسل سوم جرائم رایانه‌ای نیز می گویند.

بخش اول: بررسی ماهیتی ابعاد کیفری کلاهبرداری

با تصویب قانون تشدید مجازات مرتکبین ارتشاءاختلاس وکلاهبرداری مورخ ۱۳۶۴/۶/۲۸ توسط مجلس شورای اسلامی و طی کش و قوس های فراوان نهایتاً مورخ ۱۳۶۷/۹/۱۵ توسط مجمع تشخیص مصلحت نظام تایید شد و پس از این تاریخ لازم الاجرا شد. البته بگذریم از آنکه تایید و لازم الاجرا شدن این قانون از نظر قانون اساسی توسط مجمع خلاف است زیرا زمانی بوده است که اصلاً وجود حقوقی نداشته وحتی اصولاً بر فرض وجود این نهاد حقوقی حق قانون گذاری را ندارد . همچنین در قانون مجازات اسلامی در فصل یازدهم آن از عبارات ارتشاء و ربا و کلاهبرداری نام برده ولی عملاً در این فصل ماده ای در این زمینه وجود ندارد که می توان از اشکالات و نواقص قانون مجازات اسلامی بر شمرد. مطابق ماده (۱) قانون مجازات، مرتکبین ارتشاء و اختلاس و کلاهبرداری « هر کس از راه حیله و تقلب مردم را بوجود شرکت ها یا تجارتخانه ها یا کارخانه ها یا موسسات موهوم یا به داشتن اموال و

اختیارات واهی فریب دهد یا به امور غیر واقع امیدوار نماید یا از حوادث و پیش آمدهای غیر واقع بترساند یا اسم یا عنوان مجعول اختیار و به یکی از وسایل مذکور یا وسایل تقلبی دیگر وجوه یا اموال یا اسناد یا حوالجات یا قبوض یا مفاصا حساب و امثال آنها تحصیل کرده و از این راه مال دیگری را ببرد کلاهبردا محسوب و علاوه بر رد مال به صاحبش به حبس از یک تا هفت سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است محکوم می‌شود ...» از این ماده چنین بر می آید که برای تحقق جرم کلاهبرداری توسل به وسایل تقلبی و بردن مال غیر که همان نتیجه جرم است باید صورت گیرد. مطابق این ماده توسل به وسایل تقلبی باید موجب اغفال فرد شود و سپس مالی ربوده شود فی‌المثل ترک فعل نمی تواند توسل به وسایل متقلبانه باشد. اغفال و یا به تعبیر دیگر (فریب) برداشت نادرست و غلط از واقعیت را موجب می‌شود از شرایط اغفال این است که فرد مجنی علیه علم به تقلبی بودن وسیله متقلبانه نداشته باشد و هم چنین موضوع اغفال باید یک فرد یا افراد انسانی باشد تا غفلت صورت پذیرد مثلاً افرادی که محجور هستند اغفال در مورد آنها امکان ندارد زیرا این افراد فاقد بعضاً اراده و گاه تفکر لازم برای انجام امور هستند.

بخش دوم: بررسی و مداقه درکلاهبرداری رایانه‌ای

با ارائه مباحثی که در زمینه جرائم رایانه‌ای و کلاهبرداری شد مشخص شد ماهیتا :درپاسخ به این سوال یک چیز مسلم است که امروزه کلاهبرداری اینترنتی از کلاهبرداری های سنتی پیشی گرفته و چنان روز به روز بر پیچیدگی های این نوع جرائم افزوده می‌شود که به نظر می رسد حتی اگر چه قانون گذار در هر کشور و منطقه ای با توجه به تحولات لازمه دست به تدوین و تصویب جدید ترین قوانین بزند باز هم جوابگو نخواهد بود و قوانین در این زمینه ها جامعیت لازم و کافی را نخواهند داشت و همواره مجرمین راه کارها و راه حل های فرار از قوانین را سریع پیدا خواهند نمود. این جرم چندان تفاوتی با جرم سنتی کلاهبرداری ندارد و تنها وسایل و ابزار و تا حدی شیوه ی آن متفاوت‌تر شده است . اما آیا اینکه می توان با قوانین سنتی جوابگوی برخورد با مجرمانی که بصورت شبه و ناشناخته اقدام به کلاهبرداری می‌کنند

خواهیم برد یا نه؟ لذا با توجه به این مباحث آشکار خواهد بود که نه تنها قوانین سنتی ما در این زمینه کار آمدی لازم را نخواهند داشت بلکه قوانینی که طبق آخرین اراده قانون گذار به تصویب می رسد نیز شرایط لازم برای اجرا را نخواهد داشت . با گسترش روز افزون اطلاعات و فناوری داده‌های اطلاعاتی و خلاء قوانین موجود باعث می‌شود تا کلاهبرداران اینترنتی عرصه را برای خود باز تر ببینند و با سوء استفاده از این وضعیت بیشتر مرتکب کلاه برداری و جرم های اینترنتی شوند . اما اینکه آیا قوانین راجع به کلاهبرداری سنتی توان پوشش دادن کلاهبرداری اینترنتی را دارد یا خیر بحثی است که نیاز به ارائه دلایل موجه و لازم در این زمینه دارد با قیاس این دو می توان به این سوال جواب داد.

بند اول: تعریف اینترنت

اینترنت را مجموعه ای از شبکه ها گویند و از طریق آن شبکه‌ها ی مختلف رایانه‌ای توسط سخت افزار و نرم افزارهای مربوط و با قرار دادهای ارتباطی یکسان به یکدیگر متصل شده و با اختصاص آدرس‌های الکترونیکی خاص هر یک از آنها می توانند به صورت متن ، صدا ، تصویر و حتی فیلم تبادل اطلاعات کنند. بنابراین اینترنت موجب دسترسی آسان و سریع به حجم عظیمی از اطلاعات در کوتاه ترین زمان ممکن گردیده و هر روز در حال گسترش و توسعه می‌باشد بطوریکه امروز مانند اشعه ای نور خود را بر پنج قاره جهان افکنده و دنیای شگفت‌انگیزی را بوجود آورده که با ورود در آن می توان مطالب فراوانی در ماهیت شبکه ها و پایگاه آموخته و علاوه بر آن می توان به تمامی موضوعات موجود و قابل بررسی در جهان دست یافت. سال واقعی پیدایش اینترنت را سال ۱۹۸۳ می‌دانند چرا که در این سال تغییرات مهمی در کنترل شبکه ها صورت گرفت و بسیاری از شبکه ها از شبکه های اروپا و ژاپن ، توسط دروازه هایی به آرپانت وصل شدند . در سال ۱۹۹۰ آرپانت منحل شد و وظائف آن به ساختار گسترده تری بنام اینترنت محول شد و به دنبال آن ممنوعیت جابجایی پیام‌های تجاری نیز برداشته شد و با تبدیل سیستم عامل یونیکس دیگر برنامه ی کاربردی علمی به واسطه های تحت ویندوز استفاده از اینترنت برای عموم راحت شد و اینترنت کنونی بوجود آمد.

بند دوم: کلاهبرداری اینترنتی

حال با بیان تعاریف و مقدماتی دراین زمینه می توان به تعریف کلاهبرداری اینترنتی پرداخت.کلاهبرداری اینترنتی یکی از جرائم موسوم به « جرائم یقه سفیدها»است که با توسعه اینترنت و ارتباطات گسترش یافته است . در یک تعریف ساده از جرائم یقه سفیدها می‌توان گفت کسانی که به واسطه موقعیت اجتماعی ، اقتصادی و یا سیاسی خود به حقوق اعضاء جامعه تجاوز می‌کنند در شمار این جرائم قرار می‌گیرند . منظور از کلاهبرداری اینترنتی هرگونه کلاهبرداری است که بوسیله برنامه های کامپیوتری و رایانه‌ای یا ارتباطات شبکه اینترنتی صورت می‌گیرد مثلاً از طریق سایت ها (web پست الکترونیک (e-mail) یا اتاق های گفتگو(chat rooms) در واقع کلاهبردای اینترنتی به هر نوع طرح متقلبانه ای گفته می‌شود که یک یا چند بخش از اینترنت را به کار می‌گیرد و تا در خواست های متقلبانه ای را به منظور بردن اموال و احتمالاً انجام معاملات جعلی با قربانیان احتمالی مطرح سازد . بنابراین مشخص می‌شود که کلاهبرداری اینترنتی از زمانی رواج پیدا کرد که محیط مجازی مثل محیط اینترنت پا به عرصه وجود گذاشت و تقریباً حدود ده دهه است که از عمر این جرم می گذرد. اولین قانونی که در رابطه با جرائم اینترنتی به تصویب رسید در سال ۱۹۸۴ در کشور آمریکا بود که بعد ها در سال های ۱۹۹۴ و ۱۹۹۶ این قانون اصلاح گردید.ممکن است این سوال مطرح شود که آیا کلاهبرداری رایانه‌ای یا کامپیوتری با کلاهبرداری اینترنتی متفاوت است یا خیر ؟ در پاسخ به این سوال باید گفت که قبل از وجود اینترنت کامپیوتر وجود داشته و کامپیوتر مفهومی قدیمی تر دارد . کلاهبرداری رایانه‌ای یا کامپیوتری قبل از بوجود آمدن اینترنت وجود داشته ولی بعد از اینکه اینترنت‌بوجود آمدو محیط‌مجازی‌بوجود آمد کم کم اصطلاح کلاهبرداری کامپیوتری به کلاهبرداری اینترنتی تغییر نام پیدا بنحوی که بعضی معتقدند کلاهبرداری رایانه‌ای همان کلاهبرداری اینترنتی می‌باشد و این دو اصطلاح را به جای هم دیگر به کار می برند. اما بعضی دیگر معتقدند باید بین این دو اصطلاح تفاوت قائل شد و بطوریکه باید کلاهبرداری رایانه‌ای یا کامپیوتری را اعم از کلاهبرداری اینترنتی تلقی نماییم پس از این حیث کلاهبرداری رایانه‌ای مفهومی عام نسبت به کلاهبرداری اینترنتی دارد . ولی

به نظر می رسد قوانین مصـــوب در این زمینه نظریه اول را تایید می نماید.با بیان این مطالب می توان به این نتیجه رسید که باید میان کلاهبرداری سنتی و اینترنتی تفاوت قائل شد. بنابراین ماده ۱ قانون تشدید در هیچ شرایطی نمی تواند مستند قانونی ما قرار گیرد . از این رو با پذیرش این نظریه توسط قانون گذار ما در تاریخ ۱۳۸۲/۱۰/۱۷ قانون تجارت الکترونیک برای از بین بردن خلاء موجود در قوانین در این زمینه و تجارت الکترونیک به تصویب رسید . قانون تجارت الکترونیک مشتمل به ۸۲ ماده است که در ابواب و مباحثی و فصول مختلف به مباحثی در زمینه های کلیات و تعاریف و تفسیر قانون، اعتبار قرار داد های خصوصی ،پذیرش ارزش اثباتی امضاء الکترونیکی ،مبادله داده پیام ، حمایت انحصاری در بستر مبادلات الکترونیکی ، حمایت از داده پیام های شخصی، حفاظت از داده و پیام در بستر مبادلات الکترونیکی، حمایت از علائم تجاری جرائم و مجازات‌ها و کلاهبرداری کامپیوتری، جعل کامپیوتری نقص حقوق انحصاری در بستر مبادلات الکترونیک، جبران خسارت و دیگر مسائل متفرقه از جمله مهم ترین ابواب و مباحث و فصول این قانون می توان بر شمرد که به آن پرداخته است . در باب چهارم این قانون اولین مبحث قرار گرفته در این باب کلاهبرداری کامپیوتری است . که نشانگر میزان اهمیت و درجه آن در نظر قانون گذار است زیرا همانطور که مشخص شد بیشتر جرائمی که در حوزه جرائم رایانه‌ای اتفاق می افتد همین کلاهبرداری کامپیوتری است . ماده ۶۷ و هم چنین تبصره آن در قانون تجارت الکترونیک در باب چهارم از جرائم و مجازات ها و مبحث اول کلاهبرداری کامپیوتری تنها ماده در این زمینه است به‌عبارت دیگر تنها عنصر قانونی ما در این زمینه محسوب می‌شود . ماده ۶۷ قانون تجارت الکترونیک مقرر داشته است :هر کس در بستر مبادلات الکترونیکی ، با سوء استفاده و یا استفاده غیر مجاز از داده پیام ها ، برنامه ها و سیستم‌های رایانه‌ای و 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 سیستم‌های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه ، اموال یا امتیازات مالی تحصیل کند ، 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 می‌شود «هم چنین تبصره ی این ماده مقرر می‌دارد :شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر در این ماده می‌باشد . » با دقت در این ماده نیاز به توضیح برخی از این واژه ها خواهیم داشت در ابتدای قانون تجارت الکترونیک بعضی از این واژه ها در مواد مختلف بیان شده است. فی المثل ماده ۲ این قانون مقرر می‌دارد : الف – « داده پیام»(Data Mmessage)وهر نمادی از واقعه ، اطلاعات یا مفهوم است که با وسایل الکترونیکی ، نوری و یا فناوری‌های جدید اطلاعات تولید ، ارسال ، دریافت ، ذخیره ، یا پردازش می‌شود . در همان ماده در قسمت سیستم‌های رایانه‌ای(و)در تعریف« Computer System»می‌آورد. «هر نوع دستگاه یا مجموعه ای از دستگاههای متصل سخت افزاری نرم افزاری که از طریق اجرای برنامه های پردازش خودکار(داده پیام) عمل می‌کند» یا در قسمت (ف) همین ماده آورده است.

بخش سوم: مقایسه کلاهبرداری سنتی با کلاهبرداری رایانه‌ای

مقایسه کلاهبرداری سنتی با کلاهبرداری رایانه‌ای۱ قانون شدید مقایسه خواهیم کرد و به بیان تفاوت ها و شباهت آن خواهیم پرداخت . قانون گذار در صدر ماده ۶۷ قانون تجارت الکترونیک ابتدا به وجه تمایز و اینکه این جرم در کدام حیطه انجام می‌پذیرد پرداخته است . حیطه انجام جرم و موضوع انجام جرم بستر مبادلات الکترونیکی می‌داند در حالیکه در ماده ۱ ق . تشدید چنین چیزی نیست . دومین تفاوت این است که اعمالی که موجب می‌شود نهایتاً کسی را بفریبد و مالی را ببرد کاملاً متفاوت است با ماده ۱ق . تشدید . قانون گذار در ماده 67 قانون تجارت الکترونیک اشاره می‌کند 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. در حالیکه در ماده1 ق. تشدید آن چیزی که در نهایت موجب فریب و بردن مال دیگری می‌شود متفاوت از آنچه در ماده ۶۷ ق . ت. الکترونیک بیان شده است می‌باشد . آن چیزی که در ماده ۶۷ آمده و به نظر می رسد دید قانون گذار در خصوص ماهیت جرم کلاهبرداری تا قدری از گذشته متفاوت تر شده است این

است که در ماده ۱.ق. تشدید قانون گذار نتیجه جرم را صرفاً بردن مال غیر می‌دانست اما در ماده ۶۷ این وضع تا قدری با گذشته فرق دارد به این نحو که قانون گذار صرفاً نتیجه کلاهبرداری را بردن مال غیر نمی‌داند. بلکه اعمالی از قبیل تحصیل وجوه ، اموال ، یا امتیازات مالی را علاوه بر بردن مال دیگری از نتایج جرم کلاهبرداری تلقی کرده است .علاوه بر این نیز قانون‌گذار نه تنها تحصیل وجوه و اموال امتیازات مالی و بردن مال غیر را برای خود شخص مجرم ، جرم تلقی کرده بلکه حتی تحصیل و بردن اگر برای شخص غیر از خود شخص مجرم نیز باشد کلاهبرداری تلقی نموده است . البته مشخص ننموده که آیا شخص دیگر که در جرم دخالت دارد بنحوی شریک در جرم خواهد بود یا خیر؟ اگر بر فرض اینکه شریک در این جرم است آیا مجازات اصلی در خصوص وی قابل اعمال است یا خیر و دیگر آثار حقوقی که ممکن است در این زمینه بوجود آید ، متاسفانه تکلیفی مشخص ننموده است . از دیگر تفاوت‌هایی که می توان در بیان وجوه تمایز این دو ماده بر شمرده در میزان مجازات این دو جرم است . ماده ۱.ق تشدید مجازات فرد مجرم را علاوه بر رد اصل مال به صاحبش به حبس از یک تا ۷ سال و پرداخت جزای نقدی معادل مالـــی که اخذ کرده است می‌داند در حالیکه به ۶۷ بیان می‌دارد (علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال ماخوذه محکوم می‌شود) آنچه که مشخص است در میزان حداکثر مجازات جرم در دو ماده تفاوت دیده می‌شود . ماده ۱.ق تشدید حداکثر مجازات حبس را ۷ سال می‌داند در حالیکه ماده ۶۷ ق.ت الکترونیک حداکثر مجازات حبس را ۳ سال تعیین می‌کند و در خصوص دیگر مجازاتها کاملاً شبیه هستند یعنی هر دو ماده اتفاق نظر بر رد اصل مال به صاحبش و در حداقل مجازات حبس یک سال و در خصوص پرداخت جزای نقدی نیز معادل مال ماخوذه کاملاً با هم یکسان هستند. هر چند رد اصل مال به صاحبش چندان جنبه جزائی ندارد و اینکه بخواهیم آنرا در زمره مجازات بر شماریم کار غلطی است پس در بیان بهتر باید آنرا در زمره مسئولیت مدنی مجرم دانست اگر چه در مواد : ۱.ق .تشدید وم ۶۷ ق.ت .الکترونیک بین این دو تفاوتی قایل نشده است.

بخش چهارم: اولین جرایم اینترنتی در جهان و ایران

تاریخچه مشخصی از پیدایش جرم اینترنتی و کامپیوتری زمان وجود ندارد ولی به هرحال این دسته از جرائم را باید زائیده و نتیجه تکنولوژی ارتباطی و اطلاعاتی دانست. براساس مطالعات صورت گرفته منشاء پیدایش جرم کامپیوتری و اینترنتی به قضیه رویس برمی‌گردد؛ او که بعد از بی مهری مسئولان یک شرکت فروش عمده میوه و سبزی، به عنوان حسابدار آنها انتخاب می‌شود از طریق کامپیوتر اقدام به حسابرسی کرده و با تغییر قیمت ها و تنظیم درآمد جنس ، مبلغی از مرجع آن را کاهش و به جای خاص واریز می‌کند. رویس با ظرافت خاصی قیمت ها را تغییر می‌داد ، بعد از آن با نام ۱۷ شرکت محل و طرف قرارداد ، چک های جعلی صادر و از آن حساب برداشت می‌کرده به طوری که در کمتر از ۶ سال بیش از یک میلیون دلار بدست آورده است امابه علت نداشتن مکانیزم برای توقف این روند، رویس خودش را به محاکم قضایی معرفی می‌کند و به ۱۰ سال زندان محکوم می‌شود .بدین ترتیب زمینه پیدایش جرم رایانه‌ای شکل می‌گیرد و دادگاه را به تدوین قوانین مدون وا می‌دارد. براساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست. یک کارگر چاپخانه و یک دانشجوی کامپیوتر در کرمان اقدام به جعل چک های تضمینی مسافرتی کردند و چون تفاوت و تمایزی چندان بین جرم کامپیوتری و جرم اینترنتی وجود ندارد، عمل آن ها به عنوان جرم اینترنتی محسوب می‌شود. بعد از این بود که گروههای هکر موسوم به گروه مش قاسم و ..... جرم های دیگری را مرتکب می شدند، مواردی چون جعل اسکناس ، اسناد و بلیط های شرکت های اتوبوسرانی، جعل اسناد دولتی از قبیل گواهینامه ، کارت پایان خدمت ، مدرک تحصیلی و جعل چک های مسافرتی و عادی بخشی از این جرایم اینترنتی هستند. براساس آمارهای موجود در سال ۱۳۸۴ ، ۵۳ مورد پرونده مربوط به جرایم اینترنتی در کشور تشکیل شد که کشف جرائم آمار ۵۰ درصدی را نشان می‌دهد. از مهمترین موارد جرم اینترنتی و رایانه‌ای در سال گذشته ، ۳۲ مورد سوء استفاده از کارت‌های اعتباری ۱۱ مورد کلاهبرداری اینترنتی ، ۷ مورد ایجاد مزاحمت از طریق اینترنت ، ۳ مورد کپی رایت و ۲ مورد نشر اکاذیب از طریق اینترنت و ۵ مورد موضوعات متفرقه بوده است. باتوجه به آمارهای سال

۸۴ میزان کشفیات مربوط به کلاهبرداری ، جعل و سایر جرائم رایانه‌ای و اینترنتی ۱۱ درصد رشد را نشان می‌دهد. می توان گفت امسال هم جرایم رایانه‌ای و اینترنتی در کشورمان اتفاق افتاده که شاید یکی از مهمترین و خبرسازترین آنها ، توزیع سی دی مستهجن منسوب به یکی از بازیگران مشهور زن بود و از مصادیق بارز جرم رایانه‌ای است .

بخش پنجم: گسترهٔ جرائم کامپیوتری و اینترنت

در قرن حاضر با پیشرفت سریع تکنولوژی کامپیوتر و فناوری اطلاعات دامنه‌ی جرائم کامپیوتری و اینترنتی بُعد وسیعی از فعالیت‌های مجرمانه را، از یک سرقت جزیی یک کارت هوشمند اعتباری تا جاسوسی در سطح بین‌المللی در بر می‌گیرد. این نوع جرائم به تدریج از محدودهٔ یک سیستم داخلی یک سازمان دولتی در یک کشور به جرائم فراملی توسعه یافته است. کامپیوتر و سیستم‌های کامپیوتری گاهی ابزار جرم، گاه موضوع جرم، گاه هدف نهایی جرم و بعضاً بعنوان یک سمبل در ارتکاب جرم تلقی می‌گردد. برخی از اشکال جرائم کامپیوتری و اینترنتی تنها سبب بروز تغییراتی در اوصاف مجرمانه کلاسیک و برخی از عناصر متشکلهٔ جرم شده‌اند. و برخی دیگر بخصوص جرائم جدید به دلیل عدم انطباق با عناوین مجرمانهٔ جدیدی را می‌طلبد. جرائم کامپیوتری و اینترنتی براساس ارزش‌ها و منافع مورد حمله نیز متنوع‌اند. مثلاً جاسوسی کامپیوتری جزء جرایم علیه آسایش و امنیت عمومی، نفوذ و خدشه در سیستم‌های مالی جزء جرائم علیه اموال، تصاویر پورنوگرافی کودکان، جزء جرائم علیه تمامیت معنوی اشخاص(جرایم علیه محتوا) و ... می‌باشد. در سطح بین‌المللی تلاشهایی برای معرفی انواع جرایم کامپیوتری و اینترنتی و دسته‌بندی آنها صورت گرفته است. هدف اقدامات بین‌المللی حصول به یک اجماع جهانی در خصوص این جرایم است تا مقدمات تعاون بین‌الملل در زمینهٔ مبارزه و پیشگیری با این‌گونه جرایم به نحو مطلوب فراهم آید.این مهم با توجه به ظهور جرایم جدید و غیر قابل مقایسه به جرایم کلاسیک و حتی جرایم کامپیوتری ابتدایی، اهمیت ویژه‌ای دارد. کشورها نیز در برخورد با این پدیده و با توجه به

اشکالی که در هر یک از کشورهای جهان ظاهر شده است طبقه‌بندی‌هایی را از اینگونه جرایم ارائه داده‌اند که نهایتاً موجب تدوین قوانین بخصوص در این رابطه شده است.

بخش ششم: ارکان جرم کلاهبرداری کامپیوتری

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

بند اول: عنصر قانونی

شرط مقدم و لازم برای تحقق جرم در حکم کلاهبرداری کامپیوتری ماده ۶۷ قانون تجارت الکترونیکی مصوب ۱۷ دیماه ۱۳۸۲ مجلس شورای اسلامی است (روزنامه رسمی شماره ۱۷۱۶۷). قانون تجارت الکترونیکی، شامل مجموعه اصول و قواعدی است که برای مبادله آسان و ایمن اطلاعات در واسطهای الکترونیکی و با استفاده از سیستمهای ارتباطی جدید به کار می‌رود (ماده ۱قانون تجارت الکترونیکی). ماده ۶۷ قانون تجارت الکترونیکی می‌گوید: «هرکس در بستر مبادلات الکترونیکی، یا سوءاستفاده و یا استفاده غیرمجاز از «داده پیام»ها، برنامه‌ها و سیستمهای رایانه‌ای ووسایل 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 سیستمهای پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران رابربرد مجرم محسوب و علاوه بر، رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزاینقدی معادل مال مأخوذه محکوم می‌شود». شروع به جرم کلاهبرداری کامپیوتری نیز جرم تلقی و مستوجب کیفر است، زیرا تبصره ماده ۶۷قانون تجارات الکترونیکی می‌گوید: «شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر در این ماده میباشد». سوءاستفاده در

کلاهبرداری کامپیوتری عبارت است از: اقدامات و دستکاریهای غیرمجاز وغیرقانونی که شامل مصادیق زیر است:

الف) وارد کردن داده‌ها و اطلاعات اعم از صحیح و کذب = وقتی که وارد کردن داده‌ها واطلاعات منتهی به تحصیل مال یا وجه و امتیاز گردد جرم کلاهبرداری کامپیوتری محقق می‌شود. مانند وارد کردن اطلاعاتی به سیستم رایانه‌ای بانک یا یک مؤسسه مالی و واریز وجه مربوط به حساب خود یادیگری.

ب) تغییر غیرمجاز داده‌ها و اطلاعات رایانه‌ای = چنانچه جعل رایانه‌ای مصداق سوءاستفاده قرار گیرد و در نتیجه تغییر مزبور، مال، وجه امتیازات و خدمات مالی تحصیل گردد جرم محقق می‌شود. مانند تغییر عنوان شرکت یا مؤسسه مالی یا تجارتخانه یا بانک وقتی منتهی به این شود که مشتریان مؤسسات مزبور وجوه قابل پرداخت خود را به حساب شخص تغییر دهنده اطلاعات واریز نمایند.

ج) محو داده‌ها و اطلاعات رایانه‌ای و مخابراتی = شامل از بین بردن و حذف داده‌هاست. درصورتی که این محو در جهت تحصیل وجه یا امتیازات مالی باشد، میتواند از مصادیق کلاهبرداری کامپیوتری با سوءاستفاده از طریق محو داده‌ها و اطلاعات تلقی گردد.

د) توقف داده‌ها و اطلاعات رایانه‌ای = ایجاد وقفه در سیستم رایانه ممکن است موقت یا دائمی باشد. مانند متوقف ساختن دستور پرداخت وجه به شخصی و طرف پرداخت قرار دادن خود بطور غیرمجاز.

هـ) مداخله در کارکرد سیستم رایانه = ایجاد اختلال غیرقانونی و غیرمجاز در کارکرد سیستم کامپیوتری وقتی در جهت تحصیل مال یا وجه یا منفعت یا امتیاز یا خدمات مالی باشد، مرتکب برحسب توفیق یافتن در بردن مال یا امتیاز یا عدم موفقیت در تحصیل مال یا امتیاز، مرتکب کلاهبرداری کامپیوتری تام و یا شروع به کلاهبرداری تلقی می‌گردد.

بند دوم: عنصر مادی جرم کلاهبرداری کامپیوتری (یا رایانه‌ای)

رایانه یا کامپیوتر وسیله ارتکاب جرم کلاهبرداری کامپیوتری است و ممکن است ارتکاب آن بارفتارهای مجرمانه دیگری مانند سرقت داده‌ها یا تغییر آنها و جعل و یا با نفوذ غیرمجاز

همراه باشد که موضوع جرم کلاهبرداری کامپیوتری را تشکیل می‌دهد. 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 می‌شود. کلاهبرداران، معمولاً از هوش و استعدادهای زیادی برخوردارند و به ویژه در کلاهبرداری الکترونیکی از تخصّص و مهارت‌های فوقالعاده هم استفاده می‌کنند. بدین ترتیب کشف جرائم آنان بسیار مشکل است. عنصر مادی جرم کلاهبرداری کامپیوتری را که در واقع عملیات متقلبانه در جرم مزبور است،ضمن بیان تمایز و تفاوت جرم مزبور از کلاهبرداری عمومی به شرح زیر مورد توجه قرار می‌دهیم.

۱)تحصیل وجه یا مال از طریق دادن برنامه بدون مجوز و مخفیانه به کامپیوتر: در جرم کلاهبرداری کامپیوتری یا رایانه‌ای، مرتکب از طریق دادن بدون مجوز و مخفیانه برنامه‌ای به رایانه، موفق به تحصیل وجوه یا اموال، از بانک یا شرکت یا یک مؤسسه مالی می‌گردد. وجه تمایزکلاهبرداری کامپیوتری خاص با کلاهبرداری عمومی در این است که در کلاهبرداری رایانه‌ای قربانی جرم از نظر مرتکب ناشناخته است و لزوم فریب قربانی برای تسلیم مال به کلاهبردار منتفی است. درحالی که در کلاهبرداری عمومی، عملیات متقلبانه کلاهبردار، مقدم بر تحصیل مال و علت غائی تسلیم مال از طرف زیان‌دیده به کلاهبردار است.

۲)حصیل وجوه یا اموال از طریق تقلب در سیستم رایانه‌ای: کلاهبرداری کامپیوتری با عملیات متقلبانه در داده‌ها، اطلاعات و سیستمهای رایانه‌ای انجاممیپذیرد. مثلاً کلاهبردار، با برنامه‌نویسی خلاف واقع و نادرست یا تغییر داده‌ها در سیستم رایانه‌ای بانک یا تجارتخانه یا مؤسسات دیگر اقتصادی، مالی و تجارتی، مبادرت به تحصیل وجه یا مال می‌نماید.

بند سوم: عنصر معنوی جرم

رفتار مرتکب کلاهبرداری رایانه‌ای باید همراه با قصد فریب دیگری یا سبب اختلال و گمراهی سیستم‌های پردازش خودکار و نظایر آن شود.

(۱) عمد عام، در سوءاستفاده و یا استفاده غیرمجاز 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 بفریبد 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 مقرّر است. در واقع عنصر مادی و معنوی جرایم عمدی مثل پشت و روی سکه است همیشه با هم ولی جدای از هم می‌باشند، قصر متقلبانه از کیفیت عملیات قابل استنباط است.

بخش هفتم: شروع به کلاهبرداری رایانه‌ای

جرم کلاهبرداری یک جرم مقید است یعنی شرط وقوع آن نتیجه است. نتیجه جرم کلاهبرداری چه در ماده ۱.ق.ت و چه در ماده ۶۷ ق.ت. الکترونیک تحصیل و بردن مال غیر و وجوه و... بیان شده است . که البته نهایتاً به ضرر مجنی علیه منتهی می‌شود است یکی دیگر از وجوه تمایز کلاهبرداری عادی و کلاهبرداری کامپیوتری سمت مرتکب کلاهبردار است.

ماده ۱.ق . تشدید سمت مرتکب را بعنوان کیفیت مشدده جرم بیان کرده است . هر چند از نظر اصول کلی حقوق جزا نباید سمت مرتکب تاثیری در میزان مجازات داشته باشد . مثلاً بموجب قانون جزای عمومی (قانونی که قبل از انقلاب اسلامی اجرا می شد) سمت کلاهبردار در میزان تشدید مجازات تاثیری نداشت و زمانی موثر بود که از عنوان مربوطه سوء استفاده می شد در حالیکه بموجب ماده ۱.ق تشدید تفاوتی در این بین وجود ندارد و خواه فرد مرتکب جرم از این عنوان استفاده کند خواه نکند مجرم جرم کلاهبرداری محسوب و به جزای مشدد حبس ۲تا ده سال و انفصال ابد از خدمات دولتی و پرداخت جزای نقدی مالی که اخذ کرده است محکوم می‌شود . اما دید قانون گذار در این خصوص نیز در تصویب ق.ت . الکترونیک با گذشته متفاوت شده بنحوی که دیگر سمت یا عنوان فرد مرتکب در تشدید مجازات تاثیری ندارد و در نظر قانون گذار هر کسی که اعمال مجرمانه ماده ۶۷ را انجام دهد صرف نظر از

موقعیت ؛ عنوان و سمت وی به مجازات مقرر در این ماده محکوم خواهد شد.همانطور که پیش تر نیز بیان شد جرم کلاهبرداری یک جرم مقید است یعنی شرط وقوع آن نتیجه است.

نتیجه جرم کلاهبرداری چه در ماده ۱.ق.ت و چه در ماده ۶۷ ق.ت. الکترونیک تحصیل و بردن مال غیر و وجوه و... بیان شده است . که البته نهایتاً به ضرر مجنی علیه منتهی می‌شود.

تفاوت تحصیل با بردن مال: اما اینکه تفاوت تحصیل با بردن مال چیست ؟ سئوالی است که در پاسخ آن قانون گذار در ماده۶۷ به بیان آن پرداخته است . یعنی قانون گذار تحصیل را ویژه ی وجوه ، اموال یا امتیازات مالی دانسته در حالی که بردن را صرفاً ویژه‌ی مال می‌داند . بعبارت بهتر موضوع جرم مال و وجوه امتیازات مالی است که به تعبیر عام کلمه مال است.

اما مال چیست ؟ و به چه چیزی مال گفته می‌شود ؟ در کتاب ترمینولوژی حقوق تالیف دکتر محمد جعفر جعفری لنگرودی این چنین از مال تعریف شده » در اصل از فعل ماضی میل است بمعنی خواستن . در فارسی هم به مال خواسته می‌گویند . در اصطلاح چیزی است که ارزش اقتصادی داشته و قابل تقویم به پول باشد بنابراین حقوق مالی مانند حق تحجیر و حق شفعه و حق صاحب علامت تجاری هم مال محسوب است . در قانون مال تعریف نشده است .) و هم چنین در تعریف امتیاز این چنین بیان شده: « اختصاص شخص به داشتن حق یا حقوق معین مانند امتیاز استخراج نفت یا امتیاز کشیدن خط آهن و مانند اینها » با تعاریف مذکور مشخص می‌شود آن چیزی می تواند موضوع جرم کلاهبردای و بطور کل جرائم علیه اموال صورت گیرد که از نظر عقلایی و شرعی ارزش داشته و قابلیت تقویم داشته خواه از آن استفاده مادی شود خواه معنوی و از نظر شرعی باید قابل تملک باشد اگر چیزی قابل تملک نباشد منافع آن نیز قابل تملک نخواهد بود. بنابراین تحصیل وجوه و اموال و امتیازات مالی و بردن مال غیر زمانی مصداق پیدا می‌کند که بطور کلی دارای ارزش اقتصادی باشد پس حتی اگر فرد بواسطه اعمال متقلبانه فی‌المثل در فضای اینترنت فریب بخورد و ایمیل و رمز عبورآن را به کسی بدهد و فرضاً آن شخص بعداً رمز را تغییر دهد و ایمیل را به شخص پس ندهد مرتکب جرم کلاهبرداری اینترنتی نشده است زیرا فی الواقع از این طریق مالی را نبرده است و

همان طور که می‌دانیم ایمیل و پست الکترونیک علی الاصول بصورت رایگان قابل دسترسی است البته اگر از طریق بدست اوردن اطلاعات خاصی که ممکن است در ایمیل شخصی فرد فریب خورده باشد و از آن طریق مال یا امتیازات مالی را ببرد و یا تحصیل کند مجرم خواهد بود و ولی موضوع بحث ما فرضاً ایمیلی بود که هیچ اطلاعات مفیدی ندارد و حداقل برای ثبت نام آن وجهی پرداخت نشده باشد مسلم است در غیر این صورت شامل این بحث نخواهد بود . در ضمن اینکه دسترسی به اطلاعات شخصی و افشاء آن مطابق دیگر مواد قانونی ، قانون تجارت الکترونیک قابل پیگرد خواهد بود (هر چند عملاً این امکان وجود ندارد و تنها وسایل شناسایی مجرمین اینترنتی در اختیار نهادهای خاص دولتی قرار دارد.) اغفال(فریب یا سبب گمراهی)چیزی است که فرد مجنی علیه را به برداشت نادرست و اشتباه از واقعیت می‌کند و به تعبیر قانون گذار در ماده ۶۷ ق.ت.ا فریب یا سبب گمراهی را باعث می‌شود . پس برای تحقق عمل فریفتن شرایطی لازم است:مجنی علیه علم به تقلبی بودن وسیله متقلبانه نداشته باشد . موضوع اغفال باید یک فرد و یک اراده انسانی شد.بنابراین عملا کسی را می توان فریب داد یا اسباب گمراهی او را فراهم کرد که انسان بوده و دارای اراده و اختیار باشد . در حالیکه ماده ۶۷ چیزی غیر از این را عنوان می‌کند« هر کس ....ارتکاب افعالی نظیر ورود ، محو و مداخله در عملکرد و برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن شود.....» همانطور که دیدیم قانون گذار معتقد است نه تنها انسان نوعی را می توان اغفال کرد و مالی را برد بلکه می توان اسباب گمراهی سیستم‌های پردازش خودکار و دیگر سیستم‌های رایانه‌ای که احتمالاً منظور قانون گذار نظایر آن نیز همین بوده است (را فراهم نمود و احتمالاً مال یا وجوه و دیگرامتیازات مالی را برد . هر چند دیدگاه قانونگذار در این باره قابل انتقاد بنظر می رسد زیرا عقلاً و منطقاً قابل پذیرش نخواهد بود که انسان دستگاه را فریب دهد و نهایتاً مالی را ببرد ولی در توجیه آن می توان به این استدلال ضعیف که می‌گوید :(دستگاه مطابق اراده انسان ساخته شده و مطابق اراده انسانها فعالیت می‌کند و در این چارچوب است) شاید بتوان دیدگاه قانون گذار را توجیه نمود علاوه بر

اینکه باید پذیرفت که با توجه تازگی مسائل و عدم پیش بینی های لازم توسط قانون‌گذار در آن برحه‌ی زمانی نقص در قوانین آشکار باشد

بخش هشتم: کیفرهای جرم کلاهبرداری کامپیوتری

بند اول:کیفر کلاهبرداری تام

مجازات کلاهبرداری کامپیوتری،در اجرای ماده ۶۷ قانون تجارت الکترونیکی عبارت است از:حبس از یک سال تا سه سال و پرداخت جزای نقدی معادل مال ماخوذ،غلاوه بر رد مال به صاحب اموال. در حالی که کیفر کلاهبرداری عمومی،موضوع قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری ۱۳۶۷ یک سال تا ۷ سال حبس ویا۲ سال حبس می باشد. تعیین مجازات کم برای کلاهبرداری کامپیوتری می‌تواند ۲ حالت داشته باشد:یا قانونگذاری در سیاست کیفری خود به جنبه ارعابی کیفرهای شدید اعتماد و اعتقاد نداشته است و یا ملاحضات بین‌المللی و استرداد مجرمین کلاهبرداری کامپیوتری مورد توجه قرار گرفته است. ممکن است کلاهبرداری کامپیوتری همراه با جرائم دیگری مانند جعل یا استفاده از کارتهای مجعول باشد بدین ترتیب:

(الف)جعل کامپیوتری=چنانچه ایجاد یا محو یا تغییر داده ها و کلید علائم و کدهای قابل پردازش در سیستم رایه‌نه‌ای بدون تحصیل وجه،مال یا امتیاز باشد،جرم جعل کامپیوتری موضوع ماده ۶۸ قانون تجارت الکترونیک مطرح می گردد.ماده ۶۸ قانون مزبور می‌گوید:(هر کس در بستر مبادلات الکترونیکی،از طریق ورود تغییر،محو وتوفق(داده پیام)و مداخله در پردازش (دادخ پیام) و سیستم رایانه‌ای و یا استفاده از وسایل کاربردی سیستم رمزنگاری تولید امضاء مثل کلید اختصاصی،بدون مجوز امضاء کننده و یا تو.لید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی و یاعدم انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به جعل(داده پیام)دارای ارزش مالی و اثباتی نماید تا با ارائه آن به مراجع اداری،قضایی،مالی و غیره به عنوان(داده پیام)های معتبر استفاده نماید جاعل محسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون

ریال محکوم می‌شود) تبصره ماده ۶۸ قانون مزبور،مجازات شروع به جرم را حداقل مجازات مذکور در آن ماده می‌داند.

(ب)جعل،مقدمه کلاهبرداری کامپیوتری

از جمله،کارت‌های قابل پردازش ویا مورد استفاده در سیستم‌های رایانه‌ای که ممکن است جعل شوند؛کارتهای اعتباری،کارتهای بدهی و کارتهای مغناطیسی می‌باشد.جعل کارتهای مذبور،یک جرم مطلق است و قابل کیفر.ولی چنانچه جعل مذبور همراه با تحصیل وجوه یا اموال یا امتیازات مالی باشد،موضوع مشمول ماده ۶۷ قانون مزبور است.بنابراین جعل کارتهای قابل پردازش یا مورد استفاده در سیستم رایانه‌ای با مقررات موجود مقدمه جرم کلاهبرداری کامپیوتری تلقی می‌شود.کلاهبرداری از طریق کارتهای اعتباری معمولاً به این صورت است که کلاهبرداری بجای صاحب اصلی کارت اقدام به خرید اینترنتی می‌نماید. بدین ترتیب از یک سو،صاحب اصلی کارت اعتباری که کارت وی مورد سوء استفاده قرار می‌گیرد قربانی جرم است.از سوی دیگر،فروشنده کلا یا رائه کننده خدمات که بر اساس کارت اعتباری غیر مجاز توسط ارائه کننده متقلب،کالایی را برای فرد کلاهبرداری ارسال و یا خدماتی به وی ارائه کرده است نیز به عنوان قربانی مطرح می گردد.

(ج)تعدد مادی جرائم مختلف=با تصویب مقرارات جدید مربوط به (قانون مجازات جرایم رایانه‌ای)ممکن است،جعل و استفاده از جعل و کلاهبرداری کامپیوتری،جرائم مختلف تلقی شده وقاعده جمع مجازاتها برای کیفرهای مختلف مورد تصویب قرار گیرد.

بند دوم:مجازات کلاهبرداری اینترنتی

در مورد مجازات کلاهبرداری رایانه‌ای،تقریباً شبیه کلاهبرداری عادی،یک تا هفت سال و پرداخت جزای نقدی،معادل وجه یا مال یا قیمت منفعت یا خدمات و امتیازات مالی تحصیل شده است که این مجازات کلاهبرداری ساده در ماده یک قانون تشدید هم است. کلاهبرداری رایانه‌ای که از جمله جرایم کلاسیکی است که از ابتدا در جوامع بشری موجود بوده و مسئولان اداره جوامع هرگز نتواستند این جرایم را ریشه کن کنند. البته جالب این است که امروزه با

ظهور فناوری نوینی با نام کامپیوتر طریقه های ارتکاب این جرم متنوع‌تر به دام انداختن مجمان سخت‌تر شده است .در حقوق ایران کلاهبرداری رایانه‌ای برای اولین بار در لایحه مجازات جرایم رایانه‌ای جرم انگاری شده است.جوانب مختلف حقوقی این جرم در گفتگو با دکتر حسین میر محمد صادقی،حقوقدان برجسته کشورمان بررسی شده است. ماده ۱۳ مقرر داشته است:هرکس با انجام اعمالی نظیر واردکردن،تغیر،محو،ایجاد،توقف داده‌ها یا مداخله در عملکرد سیستم و نظایر آن از سیستم رایهنه‌ای یا مخابراتی سوء استفاده کند و از این طریق وجه یا مال یا منفعت یا خدمات مالی یا امتیازهای مالی برای خود یا دیگری تصاحب یا تحصیل کند در حکم کلاهبرداری محسوب و به حبس از یک تا هفت سال و پرداخت جزای نقدی معادل وجه یا مال یا قیمت منفعت یا خدمات مالی یا امتیازهای مالی که تحصیل کرده است محکوم می‌شود.اگر ما بخواهیم آنچه را که در این ماده مطرح شده ایت بحث کنیم و در وهله اول بر می‌خوریم به عبارت(هرکس)خوب ممکن است که به ذهن برسد که بهتر بوده قانونگذاری از واژه هر شخص استفاده می‌کرد تا اشخاص حقوقی را هم ذر بر بگیرد اما در اینجا واژه هر کس به کار رفته،چون ماده دیگری در این لایحه وجود دارد.در رابطه با وقتی که اشخاص حقوقی مرتکب این جرایم می شوند وبنابراین ماده ۱۳ به این شکل تنها شامل اشخاص حقیقی است که می توانید به این جرم،محکوم شوند و اگر شخص حقوقی مرتکب آن شود،مباحث مربوط در ماده ۳۳ است.در مورد عبارت(سوء استفاده نماید)یعنی هر گونه اقدامات و دستکاری غیر مجاز را در واقع از مصادیق سوء استفاده می‌توان ذکر کرد.مثلاً فرد با وارد کردن داده ها،چه صحیح و چه کذب،از امکانات فناوری استفاده می‌کند ودر نتیجه اموالی را برای خود یا دیگری کسب می‌کند.مثلاً اطلاعاتی را وارد می‌کند که وی در حسابش مقداری پول دارد و در نتیجه بانک برای وی مبلغی را منظور کند. اما(تغییر شامل تغیر غیر مجاز داده ها و اطلاعات است که بدین طریق مال،وجه وخدمات مالی تحصیل می‌شود.از طریق(محو نیز اطلاعات رایانه‌اثی و مجاراتی حذف می‌شود باز همان نتیجه مالی کسب می‌شود.از طریق(محو نیز اطلاعات رایانه‌ای و مخاراتی حذف می‌شود باز همان نتیجه مالی کسیب می‌شود وعبارت(توقف)یعنی ایجاد وقفه در فرآیند تبادل داده‌ها و اطلاعات،مثلاً

دستور پرداختی که باید از شعبه A به شعبه B برود،کلاهبردار یک وقفه ایجاد می‌کند تا پرداخت از حساب وی صورت نگیرد و در نتیجه منافی مالی را کسب کند. (مداخله در عملکرد سیستم)اختلاس غیر قانونی در کارکرد سیستم است به هر شکلی اگر به تحصیل مال ومنفعت بینجامد کلاهبرداری است.عبارت و نظایر آن می‌رساند که این مصادیق حصری نیست و به هر شکلی که شخص از سسیستم رایهنه‌ای و مخابراتی استفاده کرد و مالی را کسب کند،کلاهبرداری اتفلق می‌افتد.در مورد عبارت سیستم رایانه‌ای و مخابراتی که در ماده آمده است،برخی متقد بودند که به این سیستم‌ها،سیستم ارتباطی هم اضافه شود ولیکن چون معنای سیستم ارتباطی گسترده و شاید دارای ابهام است،ماده فقط سیستم رایانه‌ای و مخابراتی را مطرح کرده است.منظور از این سیستم رایانه‌ای،وسیله یا مجموعه‌ای از وسایل و ابزار مرتبط و هم پیوسته است که مطابق با یک برنامه‌ای پردازش اطلاعات را انجام می‌دهد و منظور از سیستم مخابراتی سیستم و وسایل ارتباط‌جمعی از راه دور است. به این ترتیب وقتی صحبت از سیستم رایانه‌ای یا مخابراتی می‌ود مصادیق مختلفی از کل وسایل مرتبط با رایانه و مخابرات را در می‌گیرد. در طرح عبارت " وجه یا مال یا منفعت یا خدمات مالی یا امتیازات مالی ... تحصیل کند " در این لایحه امتیازی مهم نسبت به کلاهبرداری عادی در قانون تشدید محسوب می‌شود. چون در قانون تشدید ماده یک می‌گوید: از این راه مال دیگری را ببرد و آنجا این انتقاد به مقنن وارد است که چرا بر خلاف برخی از کشورهای دیگر به منافع و خدمات مالی و امتیازات مالی اشاره نکرده است که کسی با حیله و تقلب موجب شود تا منفعت، خدمت یا امتیازات مالی غیر مجازی را کسب کند مثلاً این که پیرمردی حق بیمه عمر ر با وجود این که ۹۰ سال را در شناسنامه تبدیل به ۵۹ سال بکند تا با مبلغ بسیار کمتری بیمه شود. این مشکل و کمبود که در کلاهبرداری عادی وجود دارد خود به خود و البته خوشبختانه در مورد کلاهبرداری رایانه‌ای وجود ندارد بنابراین کسب هر گونه وجه، منفعت، خدمت و امتیاز مالی در حکم کلاهبرداری است. قطعاً این موارد جنبه مالی دارد و نه غیر از آن بنابرای اگر کسی به وسیله اعمال مذکور بتواند به مکان ممنوعی وارد شود مثلاً وارد دانشگاه شود قطعاً

کلاهبردار محسوب نمی‌شود پس باید آنچه تحصیل می‌شود صبغه مالی داشته باشد تا کلاهبرداری واقع گردد.

نتیجه گیری

با تعریفی که از جرم در حقوق جزا ارائه شد مشخص شد جرم به فعل یا ترک فعلی گفته می‌شود که قانون گذار برای آن مجازاتی در نظر گرفته است و برای آنکه جرم تلقی شود باید عنصر قانونی ، عنصر مادی و عنصر روانی یا معنوی جرم فراهم باشد. علی ایحال با تعریفی که از جرم رایانه‌ای داریم به آن دسته از اعمالی مجرمانه‌ای گفته می شد که ماهیتی سنتی دارند اما از طریق ابزار مدرنی مانند رایانه و اینترنت صورت می‌گیرد که با ارائه تقسیم بندی های جرائم رایانه‌ای به این مسئله پی بردیم که کلاهبرداری رایانه‌ای یا اینترنتی نیز جزءاین گونه جرائم قرار دارد . همانطور که قبلاً نیز گفته شد با توجه به این‌که در این زمینه با محدودیت قوانین و منابع لازم روبرو هستیم امید است قانون‌گذار فعلی ما با توجه به توسعه تکنولوژی که امروز دیگر مرزی را نمی‌شناسد و قوانین ملی دیگر نمی‌توانند کارایی لازم را از خود نشان دهند به تدوین و تصویب قوانین جامع که همگام با اصول بین‌المللی باشد بزند که خود این امر نیز مستلزم رعایت شرایط خاصی می‌باشد. تا از این طریق بتوان پیشگیری و مقابله مؤثر با جرائم رایانه‌ای پرداخت. این شرایط عبارتند از:

الف- دسترسی به فن‌آوریهای بازدارنده که این کار مستلزم محیط نظارتی متناسب است.

ب- آگاهی از خطرات بالقوه امنیتی و روش مقابله با آن‌ها.

ج- وجود موازینی برای قانون‌گذاری ماهوی و شکلی با ملاحظه فعایت‌های کیفری داخلی و بین‌المللی.

ه- همکاری مناسب میان تمام عوامل دخیل، شامل کاربران و مصرف‌کنندگان بخش صنعت، مراکز انتظامی و حفاظت اطلاعات. این کار برای پی‌جویی جرائم اینترنتی و حفظ امنیت عمومی ضروری است. بنابراین بخش‌های مختلف(کاربران و مصرف‌کنندگان و بخش صنعت و ...) باید در چارچوب وظایف و ضوابط مشخص عمل کند. دولت‌ها باید بدانند که

نیازهای مجریان قانون ممکن است موانعی در بخش صنعت و غیرو بوجود آورد لذا باید با اقدامات مناسب سعی در به حداقل رساندن این موانع کنند. در ضمن متن کامل تحقیق در این پایگاه اینترنتی موجود است.

منابع و مآخذ

قرآن کریم و بعد

الف) کتب فارسی

۱. امام خمینی، سید روح‌الله. (۱۴۲۱ق) تحریرالوسیله، تهران: مؤسسه تنظیم و نشر آثار امام‌خمینی، چاپ و نشر عروج، چاپ اول.

۲. بابازاده، قاسم. \"پیرامون کنوانسیون اروپائی جرائم کامپیوتری\" خبرنامه انفورماتیک ، شورای عالی انفورماتیک شماره ۸۱ فروردین ۸۱ ، ص ۳۸.

۳. باستانی، برومند، \"جرائم کامپیوتری و اینترنتی\"، چاپ بهنامی، سال ۱۳۸۳ ص ۲۷

۴. برومند باستانی«جرائم کامپیوتری و اینترنتی» انتشارات بهنامی، تهران،۱۳۸۳

۵. بهجت، محمدتقی. (۱۴۲۸ق) استفتائات، قم: دفتر معظم‌له، چاپ اول.

۶. جاویدنیا ، جواد جرایم تجارت الکترونیکی انتشارات خرسندی چاپ دوم ۱۳۸۸

۷. جعفری لنگرودی، محمد جعفر ، ترمینولوژی حقوق– انتشارات گنج دانش – ۱۳۸۳

۸ خداقلی – زهرا – جرایم کامپیوتری ، تهران – انتشارات آریان – چاپ اول ۱۳۸۳

۹. خداقلی –زهرا – جرایم کامپیوتری ، تهران – انتشارات آریان – چاپ اول ۱۳۸۳

۱۰. زراعت – عباس : شرح قانون مجازات اسلامی – نشر فیض ، چاپ دوم : بی تا – جلد دوم

۱۱. زندی، محمدرضا، تحقیقات مقدماتی در جرائم سایبری، تهران، انتشارات جنگل، ۱۳۸۹، چاپ اول،۵۰

۱۲. شیرزاد، کامران؛ جرایم رایانه-ای، تهران، نشر بهینه فراگیر، ۱۳۸۸، چاپ اول،۲۳

۱۳. صانعی ، پرویز ، حقوق جزای عمومی– جلد اول انتشارات گنج دانش – پاییز ۱۳۷۶

ب) کتب عربی

۱. فاضل لنکرانی، محمد. (۱۳۸۶) جامع‌المسائل (فارسی)، قم: انتشارات امیر قلم، چاپ یازدهم.

۲. فیومی، احمدبن‌محمد. (بی‌تا) مصباح‌المنیر. قم: منشورات دارالرضی، چاپ اوّل.

۳. گسن ، ریموند.(۱۳۷۰)جرم شناسی نظری، ترجمه مهدی کی نیا، انتشارات مجمع علمی و فرهنگی مجد.

۴. محبوبی، فرخ. (۱۳۸۱) دانش‌آموز نفوذگر، تهران: انتشارات ناقوس، چاپ اول.

۵. مرتضی زبیدی، محمدبن محمد. (۱۴۱۴ق) تاج‌العروس من جواهر القاموس، با تصحیح علی شیری، بیروت: دارالفکر للطباعة و النشر و التوزیع، چاپ اول.

۶. نجفی، محمدحسن. (بی‌تا) جواهرالکلام، تعلیق محمد قوچانی، بیروت: دار احیاء التراث العربی، چاپ هفتم.