مطالعات علوم سیاسی، حقوق و فقه

دوره ۹، شماره ۴، زمستان ۱۴۰۲

صفحات ۶۵۳-۶۳۲

Online ISSN: ٢٤٧٦-٤٤٦٩

Print ISSN: ٢٥٣٨-٢٠٣٩

www.irijournals.com

بزه کلاهبرداری رایانه ای با رویکرد مقارنه ای در حقوق ایران و انگلیس

شهرام روشندل

مدرس دانشگاه، پژوهشگر دکترای تخصصی حقوق جزا و جرم شناسی، عضو رسمی مرکز وکلا، کارشناسان و مشاوران خانواده قوه قضاییه

چکیده

پژوهش حاضر با هدف بررسی مطالعه تطبیقی جرائم کلاهبرداری رایانه ای در حقوق ایران و انگلیس اجرا شده است روش اجرای تحقیق توصیفی کتابخانه ای می باشد. در کلاهبرداری رایانه ای، رایانه صرفا وسیله ارتکاب جرم نیست، بلکه کلاهبرداری رایانه ای به این صورت است که مرتکب بدون فریب قربانی و از طرق مداخله در داده های رایانه ای یا عملکرد سیستم رایانه ای مال را می برد یا از خدمات دیگری بهره مند می شود؛ در واقع در این مورد، سیستم است که فریب می خورد یا سیستم به همراه یک انسان فریب می خورند در حالیکه در کلاهبرداری معمولی، لازم است. با توجه به بعد بین المللی جرائم رایانه ای خصوصا در کشور انگلیس و برخی از سازمان های بین المللی منطقه ای و جهانی معیارهایی را برای تعریف جرم کلاهبرداری رایانه ای ارائه داده و از کشورهای عضو خواسته اند با رعایت آنها نسبت به جرم انگاری این جرم اقدام نمایند. در ایران کلاهبرداری رایانه ای در بستر مبادلات الکترونیکی جرم انگاری شده، اما هنوز در سایر بسترها جرم انگاری نشده است. عدم توجه قانونگذار ایران به مسائل فنی مربوط به کلاهبرداری رایانه‌ای در بستر مبادلات الکترونیکی، باعث ایجاد اشکالاتی در ماده ۶۷ قانون تجارت الکترونیکی شده است. ماده ۸ پیشنویس قانون جرائم رایانه ای نیز از نظر فنی با اشکالاتی مواجه است. یافته های تحقیق حاکی از آن است که در مورد عنصر مادی جرم، موارد مرتبط با شخص مرتکب، غیرمجاز بودن عمل دسترسی، امکان ارتکاب این عمل از طریق فضای واقعی یا مجازی و مطلق بودن این جرم، در بین قوانین تیران و انگلیس اشتراک نظر وجود دارد و تنها تفاوت آن ها در حفاظت شده بودن داده یا سامانه از طریق تدابیر امنیتی است که این قید تنها در قانون ایران وجود دارد. در مورد عنصر معنوی جرم، در هر سه قانون سوءنیت عام باید احراز شود اما با توجه به مطلق بودن این جرم نیازی به سوءنیت خاص نیست. مجازات مرتکبان نیز با توجه به سیاست کیفری کشورهای مورد مطالعه کمابیش متفاوت تعیین شده است.

واژه‌های کلیدی: کلاهبرداری رایانه ای، بزه، فضای سایبری، حقوق ایران و انگلیس

مقدمه

کلاهبرداری رایانه ای یکی از مهم ترین جرایم رایانه ای است که مانند جرم کلاهبرداری کلاسیک از جرایم علیه اموال و مالکیت محسوب می شود. هر نوع کلاهبرداری ارتکاب یافته به وسیله رایانه، کلاهبرداری رایانه ای محسوب نمی شود و تفاوت هایی در ارکان این جرم مشاهده می شود. کلاهبرداری رایانه ای در قانون جرایم رایانه ای مورد جرم انگاری قرار گرفته است در حالیکه کلاهبرداری کلاسیک در قانون تشدید مجازات کلاهبرداران... مصوب ۱۳۶۷ مورد جرم انگاری قرار گرفته است. جرائم کامپیوتری از پیامدهای منفی عصر اطلاعات و کامپیوتر است، این جرائم اندکی پس از ورود کامپیوتر به زندگی انسان یعنی از دهه ۶۰ به بعد ظهور و بروز پیدا کردند. از مهمترین جرائم کامپیوتری که از آمار ارتکاب بالاتری نسبت به دیگر جرائم برخوردار است کلاهبرداری کامپیوتری است، (میرمحمدصادقی، ۱۳۹۱: ۵۴۹) ایران و ایالات متحده انگلیس از جمله کشورهایی هستند که به وضع قانون برای مقابله با این جرم پرداخته اند. در ایران ماده ۶۷ قانون تجارت الکترونیکی به جرم کلاهبرداری کامپیوتری اختصاص داده شده است در این ماده عنصر مادی این جرم سؤاستفاده و استفاده غیر مجاز از کامپیوتری می باشد و نتیجه آن تحصیل مال یا امتیاز مالی ذکر گردیده است. (زراعت، ۱۳۹۳: ۱۰۷) عنصر روانی این جرم در ایران علم و آگاهی مرتکب نسبت به عمل مجرمانه و نیز عمد و خواست وی در انجام عمل مجرمانه و نتیجه لازمه است. در حقوق جزای ایالات متحده انگلیس و در سطح فدرال ماده ۱۰۳۰ از مجموع قوانین ایالات متحده به انواع کلاهبرداری کامپیوتری اختصاص یافته است. عنصر مادی در اشکال گوناگون کلاهبرداری کامپیوتری در این ماده، غیر مجاز یا فراتر از جواز به کامپیوتر ذکر شده است در این کشور کلاهبرداری کامپیوتری باید منجر به نتایج مختلفی همچون تحصیل اطلاعات و یا ایراد خسارت گردد (درویش، ۱۳۹۴: ۶۹) و عنصر روانی انواع مختلف این جرم در انگلیس علم در ارتکاب جرم و نیز وجود اراده و خواست در انجام عمل مجرمانه و تحصیل نتایج مورد نظر است. مجازات جرم کلاهبرداری کامپیوتری در ایران حبس از یک تا سه سال و جزای نقدی معادل مال اخذ شده می باشد در حالی که در ایالات متحده انگلیس مجازات در نظر گرفته شده برای انواع کلاهبرداری کامپیوتری بسته به نوع کلاهبرداری حداکثر تا ۲۰ سال حبس یا جزای نقدی حداکثر تا ۳۵۰ هزار دلار تعیین شده است. (حبیب زاده، ۱۳۸۷: ۳۶۰)

در ایالات متحدهٔ انگلیس برای مقابله با تعرضات به این سه عامل مهم در عرصهٔ فناوری اطلاعات و تکنولوژی ارتباطات از سالها پیش اقدامات مهمی در تدوین قوانین و اعمال مجازات بر متجاوزان صورت گرفته است. البته به همین نسبت نیز اصلاحات مهمی هم در بخش ماهوی و هم در شیوهٔ اجرای آنها انجام شده است. تصویب اولین قانون در این زمینه به سال ۱۹۸۴ برمی‌گردد که کنگرهٔ انگلیس اقدام به تصویب قانونی آزمایشی جهت مقابله با جرایم ارتکابی در دنیای الکترونیک نمود. این قانون در سالهای ۱۹۹۴ و ۱۹۹۶ مورد بازنگری قرار گرفت و هم اکنون نیز قانون سال ۱۹۹۶ لازم الاجرا می‌باشد. این قانون در مادهٔ ۱۸ قانون ایالات متحده بخش ۱۰۳۰ آن گنجانیده شده است. (۱۰۳۰U.S.C.۱۸) لازم به ذکر است که کلیهٔ مفاد این بخش در راستای حمایت از تعرضات مربوط به این سه عامل مهم یعنی ۱) حفظ اطلاعات در برابر افشای غیرمجاز آنها (جعفری لنگرودی، ۱۳۸۷: ۲۱۳)

۲) حفظ صحت اطلاعات در برابر تغییر یا آسیب به آنها

۳) حفظ عملکرد مفید سیستم و در دسترس نگهداشتن اطلاعات، می‌باشد. اما همانطور که در تفاسیر قانونی مربوطه نیز مشخص شده قسمت a (۲) بیشترین وضوح را در حمایت از اولین عامل دارد و قسمت a (۵) نیز در مورد حمایت از عوامل دوم و سوم می‌باشد که در جای خود مورد بررسی قرار خواهد گرفت.

کلاهبرداری بردن مال غیر با توسل به وسایل متقلبانه است و به لحاظ تسلط بر مال غیر با سرقت و خیانت در امانت مشابه است، لیکن دارای خصوصیات ویژه ای است که آن را از جرائم مذکور جدا می کند. بررسی و تحلیل این موضوع در حقوق ایران و انگلیس دارای اهمیت فراوانی می باشد. از جمله به کار بردن وسیله متقلبانه، اغفال، مالباخته و تسلیم مال از طرف او به کلاهبردار ویژگی کلاهبرداری است که در سایر جرائم وجود ندارد. به لحاظ این که جرم مذکور از طریق مختلف واقع می شود، تحولات اجتماعی و در تغییر چهره های مختلف کلاهبرداری نقش مؤثر و مستقیم دارد. (پاد، ۱۳۹۲: ۶۴)

کلاهبرداری تنها جرمی است که رکن مادی آن واحد نیست یعنی رکن مادی این جرم مرکب از چند فعل است. آن چیزی که در خصوص جرم کلاهبرداری میان محاکم مطرح بود و موضوع اختلاف شد تعیین کیفر مجازات کلاهبرداری بوده بدین نحو که به موجب ماده ۱ قانون تشدید مصوب ۶۷ مجمع تشخیص مصلحت نظام : « هر کس مرتکب کلاهبرداری گردد از یک سال تا ۷ سال و جزای نقدی و رد مال محکوم می گردد و در تبصره ی ۱ ماده مرقوم ذکر شده است که با وجود جهات کیفیات تخفیف قضایی دادگاه می تواند مجازات حبس را تا ۱ سال یعنی حداقل مجازات مقرر در ماده ی ۱ تعیین نماید. تا این زمان آرای محاکم واحد بود واختلاف ایجاد نشده بود اختلاف زمانی ایجاد شد که قانون ماده ۱ سال ۷۰ به تصویب رسید که در ماده ی ۲۲ قانون مجازات اسلامی، قاضی می تواند با وجود کیفیات مخففه و شرایط آن مجازات را تخفیف یا تبدیل نماید. (آشوری، ۱۳۹۲) سوالاتی که در اینجا مطرح می شوند : جرایم کلاهبرداری رایانه ای در حقوق ایران و انگلیس تا چه اندازه باهم تفاوت دارند؟ آیا جرائمی که قانونگذار در حقوق ایران و انگلیس آنها را در حکم کلاهبرداری رایانه ای دانسته را کلاهبردار سایبری محسوب کرده است؟ آیا توصیف مجرمانه ی جرم کلاهبرداری و تعیین عنصر قانونی آن، تفاوت اساسی و مهمی را در دو نظام مختلف حقوقی ایران و انگلیس نشان می دهد؟ آیا فریب خوردن قربانی با این شرط که قربانی از متقلبانه بودن وسایل اطلاع نداشته باشد در حقوق ایران و انگلیس تفاوت دارد؟

۱-مفاهیم

۱-۱-تعریف مفهومی کلاهبرداری رایانه ای

در حقوق کیفری ایـران پیـش از تصویب قوانین مربوط به جرم‌انگاری رفتارهای قابل ارتکاب در محیطهای رایانه‌ای که وصف آن گذشت کلاهبرداری یک جرم شناخته شده در ماده یک قانون تشدید مـجازات مـرتکبین ارتشا ی، اختلاس و کلاهبرداری مصوب ۱۳۶۷ بود. در قـانون مـذکور از کلاهبرداری تعریفی ارائه نشده و تنها به ذکر مصادیقی از جرم اکتفا شده است که عبارتند از:

۱-مغرور کردن اشخاص به وجود شرکت، تجارت خانه، موسسات موهوم یا داشتن اخـتیارات مـوهوم.

۲-امیدوار کردن افراد به امـور غـیر واقع یا ترساندن از امور غیر واقع.

۳-اختیار کردن اسم، عنوان یا سمت مجعول. با این حال کلاهبرداری تعریف شده است به«بردن مال دیگری از طریق توسل توأم با سؤ نیت به وسایل یـا عـملیات متقلبانه» (میر محمد صادقی، ۱۳۸۵: ص ۵۱)

بنابراین از لحاظ رکن مادی با توجه به مصادیق مذکور که تمثیلی نیز می‌باشند کلاهبرداری تنها به صورت فعل مثبت مادی واقع می‌شود و این جرم با ترک فـعل مـحقق نمی‌شود. دیگر ایـنکه مرتکب باید با توسل به وسایل متقلبانه و اغفال بزه دیده موفق به بردن مال شود لذا کلاهبرداری از جـرایم مقید است که وقوع نتیجه در ارتکاب جرم شرط است. از لحاظ رکـن روانـی،

کلاهبرداری یـک جرم عمدی است که بایستی علاوه بر احراز سوء نیت عام یعنی علم به تعلق مال بـه غـیر و تقلبی بودن وسیله ارتکاب جرم، سوء نیت خاص یعنی قصد حصول نتیجه مجرمانه (بردن مـال غـیر)نیز احـراز گردد.

در مورد کلاهبرداری رایانه‌ای همانطور که قبلا متذکر شدیم با تصویب قانون تجارت الکترونیکی در ماده ۶۷، کـلاهبرداری رایانه‌ای در بستر مبادلات الکترونیکی جرم‌انگاری شد. همچنین در قانون جرایم رایانه‌ای ذیل فصل سـوم تحت عنوان سرقت و کـلاهبرداری مـرتبط با رایانه در ماده ۱۳ مقرر شده است: «هرکس به‌طور غیر مجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن دادها یا مختل کردن سامانه، وجه یا مال یا منفعت یـا خدمات یا امتیازات مالی برای خود یاد دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس ار یک تا پنج سال یا جزای نقدی از بیست میلیون (۲۰۰۰۰۰۰۰)ریال تا یکصد مـیلیون (۱۰۰۰۰۰۰۰۰) ریال یـا هر دو مجازات محکوم خوهد شد. » لازم به ذکر است با توجه به سکوت قانونگذار، در مقام جمع بین دو ماده مذکور می‌توان گفت هیچ یک نـاسخ دیـگری نـیست زیرا ماده ۶۷ مذکور خاص ارتکاب جرم در بستر مبادلات الکترونیکی است و از طریق مداخله در عملکرد برنامه یا سیستم رایانه‌ای با فریفتن دیگران یـا گـمراهی سـیستم‌های پردازش خودکار و نظایر آن محقق می‌شود و ماده ۱۳ قانون جرایم رایـانه‌ای عـام است که به‌طور مطلق هر نوع تحصیل مال یا منفعت و... را که به‌طور غیر مجاز از سامانه‌های رایانه‌ای یا مخابراتی و... صـورت گـرفته بـاشد را دربر می‌گیرد.

در نتیجه اگر عمل ارتکابی در بستر مبادلات الکترونیکی شرایط مـذکور در ماده ۶۷ را دارا باشد مشمول آن ماده، در غیر این صورت مشمول قواعد عام ماده ۱۳ قانون جرایم رایانه‌ای می‌باشد. بنابراین رکن قانونی جـرم کـلاهبرداری رایـانهٔا ماده ۶۷ قانون تجارت الکترونیکی و ماده ۱۳ قانون جرایم رایانه‌ای است که هـیچ یـک تعریفی از جرم کلاهبرداری رایانه‌ای ارائه نداده‌اند اما با توجه به فحوای مواد مذکور می‌توان این جرم را ایـن‌گونه تـعریف کـرد:«تحصیل خدمات و امتیازات مالی و یا بردن مال دیگری از طریق سوء استفاده یا اسـتفاده غـیر مـجاز از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور. » (تذهیبی، ۱۳۸۱: ۴۵)

مصادیق مورد اشاره در مواد مذکور از قبیل ورود، محو، توقف داده پیـام و مـداخله در عـملکرد برنامه یا سیستم رایانه‌ای تمثیلی است و گویای آن است که کلاهبرداری رایانه‌ای نیز با فـعل مـثبت واقع می‌شود و ترک فعل نمی‌تواند تشکیل دهنده رکن مادی جرم باشد. دیگر اینکه کـلاهبرداری رایـانه‌ای از لحـاظ مقید بودن به نتیجه و لزوم احراز سوء نیت خاص با نوع سنتی خود تفاوتی نـدارد بـا این حال موضوع کلاهبرداری رایانه‌ای«داده‌ها به عنوان نماینده اموال مادی»در سیستم‌های پردازش دادهـهاست، (نوربها، ۱۳۸۳:ص ۲۳)

تـفاوت اصـلی بین کلاهبرداری سنتی و کلاهبرداری رایانه‌ای در روش ارتکاب آنها خلاصه می‌شود. در نوع سنتی این جرم، مرتکب با تـوسل بـه وسایل تقلبی، مالباخته را اغفال می‌کند تا با رضایت (هرچند معیوب) مال خود را به او تسلیم کـند.

ازاین‌رو نـاآگاهی قـربانی از متقلبانه بودن، شرط تحقق جرم است (حبیب‌زاده، ۱۳۸۰: ص ۷۲)

لزوم فریب خوردن قربانی جرم کلاهبرداری نشان می‌دهد که ارتکاب ایـن جـرم تـنها علیه یک «انسان» قابل تصور است (میر محمد صادقی، ۱۳۸۵:ص ۷۶) و با فریب یک ماشین این جـرم مـحقق نمی‌شود. این در حالی است که با توجه به مفاد ماده ۶۷ قانون تجارت الکترونیکی امکان فریب ماشین‌ها و سـیستم‌های پردازش خـودکار و وقوع کلاهبرداری رایانه‌ای وجود دارد.

دیگر اینکه وجود رابطه مستقیم و قاطع بین تـوسل بـه وسایل متقلبانه با اغفال قربانی و بردن مـال او شـرط ضـروری تحقق جرم کلاهبرداری سنتی است (میر محمد صـادقی، ۱۳۹۱:ص ۶۴) بـا این حال مانورهای متقلبانه که در کلاهبرداری سنتی به

صورت انجام افعال، طرح اقوال و... بـه مـنظور بردن مال، غیر متجلی می‌گردد در کـلاهبرداری بـا استفاده از فـناوری‌های اطـلاعات و ارتباطات شکل سوء استفاده از انواع داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسـایل ارتـباط از راه دور را به خود می‌گیرد. (تقوی، ۱۳۸۲:ص ۱۳۴)

آنچه امروزه جرم رایانه‌ای، جرم اینترنتی، جرم سایبر یا حتی جرم علیه فناوری اطلاعات و ارتباطات نـام گـرفته است، در واقع همگام با رشد و تکامل عصر حاضر توسعه یافته و هر روز جلوه‌های نـوین و مـتنوع‌تری از آن مشاهده می‌شود. اما این اولین نکته‌ای که در درک مفهوم جـرائم رایـانه‌ای بـاید مدنظر داشت، این است که مفهوم رایانه فقط گـزینه‌هایی کـه ذهن ما به آنها معطوف می‌شود، مانند رایانه ی رومیزی یا قابل حمل را در برنمی‌گیرد، بلکه همان طـور که کـنوانسیون بین المللی جرائم سایبر (مصوب ۲۰۰۱)بـه ایـن موضوع صراحتا اشـاره کـرده، «سیستم رایـانه‌ای یک دستگاه یا مجموعه‌ای از دستگاه‌های مـتصل بـه هم یا مرتبط با هم است که به وسیله ی یک برنامه، داده‌های دیـجیتال را بـه طور خودکار پردازش می‌کند. » با اینکه بـحث راجع به این تعریف بـسیار اسـت و خود مجال دیگری می‌طلبد، اما قـدر مـتیقّن محرز است که حوزه ی تحت شمول سیستم رایانه‌ای بسیار گسترده‌تر از حوزه ی متصور ماست و همه دسـتگاه‌هایی کـه برنامه‌ای داشته باشند که داده‌هـای دیـجیتال را پردازش کـند، در برمی‌گیرد، مانند تلفن‌های هـمراه امـروزی، سیستم‌های پی‌جو، تلفن‌های ثابت حافظه‌دار و موارد دیـگر. هرچند ایـن واقعیت نیز انکار نمی‌شود که مثال کامل این تعریف همان رایانه‌های رومیزی یا قابل حمل است. (ساکی، ۱۳۸۶: ۹۸)

نکته ی دیـگری کـه باید به آن توجه داشت، مفهوم فضای تـبادل اطـلاعات است. با اینکه حـدود دو دهـه از بـه کارگیری این اصطلاح در حـوزه فناوری اطلاعات و ارتباطات نوین می‌گذرد، ولی همچنان میان صاحب‌نظران اختلاف نظرهای بنیادینی مشاهده می‌شود، به گونه‌ای که هنوز بـر سـر واقعی یا مجازی بودن آن هم اختلاف نـظر دارنـد. با ایـن حـال، تعریف سـاده و مورد قبولی که می‌توان از آن ارائه داد عبارت است از:«فضای واقعی و محسوس میان سیستم‌های رایانه‌ای که داده‌های دیجیتال در آن در جریان هستند.»

البته لازم بـه ذکـر اسـت تا اوایل دهه ی ۹۰ میلادی که سیستم‌های رایـانه‌ای ارتباط جـهانی بـا یـکدیگر نـیافتند و شـبکه‌های اطلاع‌رسانی رایانه‌ای به مفهوم امروزی خود به فعالیت نپرداختند، این فضا جایگاه واقعی خود را پیدا نکرد، و الاّ مفهوم آن حتی نسبت به یک سیستم رایانه‌ای مستقل نیز صدق می‌کند.

به نظر می‌رسد اگـر ما این مفهوم جامع را برای فضای تبادل اطلاعات بپذیریم، دیگر به کارگیری اصطلاحاتی نظیر جرم اینترنتی یا حتی جرم شبکه‌ای (که حوزه ی بسیار محدودی را در بر می‌گیرند) صحیح نخواهد بود. حتی اصطلاحی که امروزه تحت عنوان جـرم عـلیه فناوری اطلاعات و ارتباطات به کار می‌رود نیز صحیح نمی‌باشد. چرا که این حوزه حداقل تا به امروز در کشور ما علاوه بر فناوری دیجیتال، فناوری آنالوگ را هم در برمی‌گیرد که این امر بار مـفهوم فـضای تبادل اطلاعات را گسترده‌تر می‌کند و با اصول حقوقی در تعارض است. اما از آنجا که اصطلاح جرم سایبر هنوز در جامعه ی حقوقی و فنی، حتی در عرصه ی جهانی، جایگاه واقعی خود را نیافته است، ما از هـمان اصـطلاح جرم رایانه‌ای، اما در همان مفهوم مـوسع آنـ استفاده می‌کنیم. مؤید این کلام کنوانسیون بوداپست است که با اینکه عنوان جرائم سایبر دارد، اما جهت ملموس‌تر کردن مقررات خود سیستم رایانه‌ای را تعریف کرده و آن را مبنای عمل خـود قـرار داده است. بنابراین، ملاحظه می‌شود که ایـن دو عـنوان عملا با یکدیگر تفاوتی ندارند (ساکی، ۱۳۸۶: ۱۳۵).

با توجه به مطالب فوق، می‌توان در تعریف جرم سایبر یا رایانه‌ای گفت: «هرگونه فعل یا ترک فعلی که در فضای تبادل اطلاعات از طرف قانونگذار جرم قلمداد شود، جرم سایبر یا رایانه‌ای محسوب می‌شود»، حال چه نظیر آن در دنیای فیزیکی وجود داشته باشد، مثل جعل، کلاهبرداری، هزره‌نگاری یا پول‌شویی که در اینجا فضای تبادل اطلاعات این جرائم را تسهیل و تسریع می‌کند و به آنها جلوه‌ای نو می‌بخشد، چه اینکه یک«جرم صرف سایبر»۱ محسوب شود، مثل نشر ویروس یا، غیرمجاز که ارتکاب این اعمال فقط در فضای تبادل اطلاعات متصور است. البته باید اذعان داشت به لحاظ ادغام و درهم تنیدگی بیش از حد فعالیت‌های امروزی با فضای تبادل اطلاعات، به طور مشخص نمی‌توان جرائم را بر این مبنا تفکیک کرد.

وجود رایانه و اینترنت مسائل امنیتی خاص خود را نیز به دنبال داشته است که احتمال خطرهای امنیتی برای رایانه های مرتبط با شبکه های مانند اینترنت بیشتر است. گسترش جرائم ارتکابی با رایانه به اندازه¬ای - بوده که بیشتر کشورهای دنیا با اعمال قوانینی به مبارزه با این پدیده پرداخته و سعی در مهار آن دارند.

برای این پدیده نوظهور از اصطلاحاتی مانند جرائم اینترنتی، جرائم تکنولوژی و یا جرائم الکترونیکی استفاده می کنند و معمولاً این اصطلاحات به فعالیت های مجرمانه ای گفته می شود که یک کامپیوتر یا رایانه منبع، ابزار، هدف و یا محفل وقوع جرم باشد. جرائم رایانه ای امروز از گستردگی زیادی برخوردار است اما به طور خلاصه و براساس تقریبی دسته بندی دهمین کنگره سازمان ملل متحد در آوریل ۲۰۰۰در زمینه جرم و رفتار مجرمان در وین می توان آن را در چند دسته کلی بخش بندی کرد:

، غیر قانونی که عبارت از، به بخش یا کل یک سیستم کامپیوتری بدون داشتن حق و مجوز این کار است. جلوگیری غیر قانونی از، به داده هی شخصی با استفاده از ابزار تکنولوژیک و یا در داخل یک سیستم کامپیوتری مداخلات اطلاعاتی همچون آسیب رساندن، حذف، جایگزینی، تخریب ویا سرکوب و توقیف داده های کامپیوتری بدون مجوز مداخله در سیستم ها شامل انسداد و توقف جدی و بدون حق عملکرد سیستم های کامپیوتری با آسیب رساندن، حذف، جایگزینی، تخریب و یا توقیف داده های کامپیوتری، سوء استفاده از دستگاه ها، جعل هویت و کلاهبرداری الکترونیک. (ساکی، ۱۳۸۶: ۱۱۳) جرایم مجازی به جرایمی گفته می‌شود که در فضای مجازی رخ می‌دهند. فضای مجازی، مجموعه به هم پیوسته دنیای امروز از طریق رایانه و ارتباطات راه دور، بدون در نظر گرفتن مکان جغرافیایی است. در چنین فضایی، موضوعات مختلفی که ناشی از به کارگیری صحیح و مجاز دستاوردهای این فناوری می‌باشد، تا مسائل، مشکلات، اختلافات و دعاوی ناشی و مرتبط با آن و همچنین جرایم و تخلفات ناشی از استفاده غیر مجاز و اعمال مجرمانه نیز مطرح است که همان جرایم مجازی را تشکیل می‌دهند.

با رویکردی جامع می‌توان جرایم مجازی را شامل موارد زیر دانست:

۱.جرایم کلاسیک با توصیف مجازی، مانند کلاهبرداری مجازی و جعل مجازی؛

۲.جرایم علیه محتوا، مانند انواع پرنو گرافی و افترا؛

۳.جرایم صرف فناوری اطلاعات، مثل جرایم دستیابی؛

۴.جرایم مخابراتی، مانند شنود جرایم مربوط به تلفن‌های همراه سیستم‌های ماهواره‌ای؛

۵.جرایم با مبنای غیر جزایی، همچون: نقض کپی رایت، جرایم بانکداری الکترونیک و تجارت الکترونیک.

اما جرایم رایانه‌ای، بخشی از جرایم مجازی هستند که در آنها رایانه وسیله، هدف و یا واسطه ارتکاب جرم است و گاهی علیه اموال، گاهی علیه تمامیت معنوی اشخاص و بعضا علیه نرم‌افزار، داده و سخت‌افزار رایانه و گاهی نیز بر ضد آسایش و امنیت عمومی است. از این منظر، جرایم رایانه‌ای به سه گروه عمده تقسیم می‌شوند:

اوّل، جرایم اقتصادی مرتبط با رایانه، شامل: کلاهبرداری، جاسوسی، جعل، سرقت خدمات، دستیابی غیر مجاز و جرایم شغلی مرسوم از طریق داده‌پردازی.

دوم، جرایم علیه حقوق شخصی، شامل: افترا، توهین، افشای اسرار و نقض کپی‌رایت.

سوم، جرایم اجتماعی و ملّی، همچون: جرایم علیه امنیت ملی، کنترل جریان فرامرزی داده‌ها و تمامیت شبکه‌های ارتباطی داده‌ها.

قوانین و مقررات منسوخ و ساز و کار اجرایی ضعیف برای حفاظت اطلاعات تولیدی در شبکه‌ها و سیستم‌های اطلاعاتی، محیطی نامطلوب به وجود می‌آورد که می‌تواند برای تبادل اطلاعات دیجیتالی، مشکل آفرین باشد و راه رشد و گسترش آن را سد نماید.

وضع قوانین بسترساز در این مقوله، شامل سه حوزه اصلی حقوقی، فنی و مدیریتی می‌شود. در حوزه حقوق جزا، قوانین مربوط به جرم‌انگاری، دادرسی، صلاحیت، اعتبار ادله رایانه‌ای، و در قوانین حقوقی، قوانین مربوط به مالکیت فکری، تجارت الکترونیک، اصل و مصدق سند در محیط دیجیتال، به تدوین و تصویب نیاز دارند. (ولیدی، ۱۳۸۸).

همچنین در حوزه فنی، مقررات در قالب کد رفتاری و حرفه‌ای شامل شرح وظایف ISPها و دیگر ارائه کنندگان خدمات اینترنتی، مقررات امنیتی، استانداردها و مسئولیت‌های ناشی از حرفه‌های مرتبط، به تدوین و تصویب نیازمندند، که بعضا اقداماتی صورت گرفته یا در دست اقدام است. در حوزه حاکمیتی و مدیریتی نیز بحث کنترل جریان داده‌ها و قوانین مرتبط با آزادی جریان اطلاعات و حمایت از داده‌ها و امنیت آنها و قوانین در سطح بین‌المللی برای برخورد هماهنگ با جرایم مجازی، به وضع قوانین جدیدی نیازمند می‌باشند. (گلدوزیان ؛ ۱۳۹۱). در مورد جرائم کامپیوتری تعاریف مختلفی ارائه گردیده و اتفاق نظر در این تعاریف وجود ندارد. اولین گام در جهت تعریف جرائم کامپیوتری مربوط به سازمان همکاری و توسعه اقتصادی ((۱۲O.E.C.D) که در سال ۱۹۸۳ در پاریس، گروهی از متخصصین به دعوت این سازمان جمع شده بوده‌اند ارائه گردیده است که عبارت است از:سوء استفاده از کامپیوترها شامل هر رفتار غیر قانونی، غیر اخلاقی، یا غیر مجاز مربوط به پردازش خودکار و انتقال داده است در این تعریف گرچه به صراحت از جرائم کامپیوتری نام برده نشده است ولی منظور از سوء استفاده از کامپیوتر همان جرائم کامپیوتری می‌باشد. در تعریف دیگری آمده است: "هر عمل مثبت غیر قانونی که کامپیوتر در آن ابزار یا موضوع جرم باشد جرم کامپیوتری است گرچه تعریف فوق، تعریف بدی نمی‌باشد ولی کامل و جامع نیست زیرا در این تعریف فقط اشاره به عنصر مادی جرم نموده و ذکری از دیگر عناصر متشکلهٔ جرم و همچنین مصادیق جرائم کامپیوتری به میان نیامده است. پلیس جنائی فدرال آلمان نیز تعریفی از جرائم کامپیوتری ارائه داده که عبارتست از: جرم کامپیوتری در برگیرندهٔ همهٔ اوضاع و احوال و کیفیاتی است که در آن شکل های پردازش الکترونیک داده‌ها، وسیلهٔ ارتکاب و یا هدف یک جرم قرار گرفته است و مبنایی برای نشان دادن این ظن است که جرمی ارتکاب یافته است. همچنین بموجب نظر وزارت دادگستری آمریکا \"هرگونه عمل ناقص قانون کیفری که مستلزم آشنائی با دانش مربوط به تکنولوژی کامپیوتر جهت ارتکاب عمل، تعقیب و یا رسیدگی به آن باشد. (سلطانی، ۱۳۸۴: ۶۸)

۱-۲- ارکان بزه کلاهبرداری رایانه ای

کلاهبرداری رایانه‌ای در ماده ۷۴۱ قانون جرایم رایانه‌ای مورد جرم انگاری قرارگرفته است؛ یعنی ماده مذکور، عنصر قانونی بزه مرقوم است. در این ماده مجازات جرایم رایانه‌ای همچون جرم کلاهبرداری، هم حبس از یک تا پنج سال در نظر گرفته‌شده

است. همچنین به پرداخت جزای نقدی در حق دولت محکوم می‌شود. کلاهبرداری رایانه ای به عنوان یک جرم به نسبت نوظهور در قوانین کیفری ایران، به لحاظ ارکان مادی و معنوی با کلاهبرداری کلاسیک (موضوع ماده ۱ قانون تشدید مجازات مرتکبین ارتشا، اختلاس و کلاهبرداری) متمایز بوده و ویژگی های خاص خود را دارد. این نوع کلاهبرداری، که از رهگذر تقلب یا وارد کردن داده ها و یا اختلال در سامانه رایانه ای و مخابراتی واقع می شود، به لحاظ رکن مادی، در زمره جرایم مطلق بوده و به مجرد تحصیل وجه یا مال یا امتیاز یا خدمات مالی واقع می شود و ضرورتی به فریب بزه دیده، بردن مال، ورود ضرر یا انتقاع مرتکب نیست. وارد کردن داده ها در کلاهبرداری رایانه ای می تواند در قالب داده های صحیح یا داده های جعلی باشد. آنچه مهم است، غیر مجاز بودن رفتار مرتکب در وارد کردن داده است. تحصیل در این نوع کلاهبرداری، نتیجه محسوب نشده و بخشی از فرایند رکن مادی (آخرین فرایند) را تشکیل می دهد و از این رو، به لحاظ رکن معنوی، قصد نتیجه نیز شرط وقوع جرم نمی باشد. کلاهبرداری رایانه ای از حیث مرور زمان و انتشار حکم محکومیت، محدودیت های کلاهبرداری معمولی را نداشته و تابع مقررات عمومی است. چنانچه کلاهبرداری رایانه ای با سایر جرایم رایانه ای، مانند جعل، دسترسی غیر مجاز یا تخریب داده ها، تداخل نماید، تعدد منتفی بوده و فقط حکم به مجازات کلاهبرداری داده می شود.

۱-۳- تعریف فضای سایبر

واژه سایبر از لغت یونانی Kybernetes به معنی سکاندار یا راهنما مشتق شده است. نخستین بار این اصطلاح (سایبرنتیک) توسط ریاضیدانی به نام نوربرت وینر در کتابی با عنوان سایبرنتیک و کنترل در ارتباط بین حیوان و ماشین در سال ۱۹۴۸ بکار برده شده است. سایبرنتیک علم مطالعه و کنترل مکانیزم ها در سیستم‌های انسانی، ماشینی (و کامپیوتر ها) است. (باقرزاده، ۱۳۸۳: ۵۳)

سایبر پیشوندی است برای توصیف یک شخص، یک شی، یک ایده و یا یک فضا که مربوط به دنیای کامپیوتر و اطلاعات است. در طی توسعه اینترنت واژه های ترکیبی بسیاری از این کلمه سایبر بوجود آمده است که به تعدادی از آنها اشاره می کنیم:

فضای سایبر، حقوق سایبری شهروند سایبر، پول سایبر، فرهنگ سایبر، جرایم سایبری، راهنمایی فضای سایبر، تجارت سایبر، کانال سایبر و ....

واژه فضای سایبر نخستین بار ویلیام گیبسون نویسنده داستان علمی تخیلی در کتاب نورومنسر در سال ۱۹۸۴ به کار برده است. فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسانها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود.

یک سیستم آنلاین یا یک تلفن همراه یا یک دستگاه خودپرداز نمونه ای از فضای سایبر است که کاربران آن می‌توانند از طریق آن با یکدیگر ارتباط بر قرارکنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یاحرکات ماوس صورت می‌گیرد. این عدم جابجایی فیزیکی، محققان را واداشت که به مطالعه برخی شباهت‌های فضای سایبر با حالت های ناهشیاری، بخصوص حالت‌های ذهنی‌ای که در رویا ها ظاهر می‌شوند، بپردازند. (نوربها، ۱۳۸۹: ۳۲)

۱-۴-تعریف جرایم رایانه ای

مطابق ماده ۶۷ تحصیل وجه یا مال از طریق دادن برنامه بدون مجوز و مخفیانه به کامپیوتر، تحصیل وجوه یا اموال از طریق تقلب در سیستم رایانه ای از این نوع کلاهبرداری می باشد. 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 می‌نمایدپروفسور اولریش زیبر یکی از صاحب نظران معروف حقوق جزای رایانه معتقد است امروزه اجماع بین‌المللی براین است که جرم رایانه‌ای باید به طور کامل تعریف شود. با عنایت به شیوع کلاهبرداری رایانه ای و فراگیر شدن آن متاسفانه هنوز تعریف جامعی از کلاهبرداری رایانه ای که مورد پذیرش باشد ارائه نشده است. علت این امر دشواری ارائه تعریفی است که بتواند تمام اشکال جرم کلاهبرداری رایانه ای را شامل شود. در واقع می توان کلاهبرداری رایانه ای را بخشی از جرایم رایانه ای دانست. ماده ۶۷قانون تجارت الکترونیک، مقرر میدارد: هرکس در بستر مبادلات الکترونیکی، با سوء استفاده و یا استفاده غیر مجاز از) داده پیام (ها، بر نامه ها و سیستم ها ی 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 یا 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 ماخوذه محکوم می شود. 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 مجازات‌مقرر در این ماده می‌باشد». از حیث نقش رایانه در ارتکاب جرم، جرایم رایانه ای را می توان به سه دسته اصلی تقسیم نمود؛ (رهبر، ۱۳۸۷: ۶)

دسته اول: به جرایمی مربوط می شود که در آنها مورد جرم متعلقات رایانه و تجهیزات آن است. مانند سرقت، تخریب و غیره.

دسته دوم: جرایمی هستند که می توان انها را جرایم رایانه ای محض نامید که این نوع از جرایم رایانه ای کاملاً با جرایم کلاسیک تفاوت دارند و در دنیای مجازی این نوع از جرایم رایانه ای تحقق می یابد. منتها نتیجه آن در خارج پدیدار می شود. مانند، غیر مجاز به سیستم های کامپیوتری (جرایم رایانه ای خاص).

دسته سوم: به جرایم رایانه ای مربوط می شود که در آنها رایانه به عنوان ادوات ارتکاب جرم استفاده می شود مانند کلاهبرداری رایانه ای.

۱-۵-مرجع صالح

جرم کلاهبرداری با توجه به اینکه دارای ارکان مختلفی است، دادسرا و دادگاه صالح آن محلی است که جرم در آنجا کامل شده است و کلیه ارکان آن در آن محل تکمیل شده باشد. در رأی وحدت رویه شماره ۷۲۹ ـ ۱۳۹۱/۱۲/۱ هیأت عمومی دیوان عالی کشور آمده است: «نظر به اینکه در صلاحیت محلی، اصل صلاحیت دادگاه محل وقوع جرم است و این اصل در قانون جرایم رایانه‌ای نیز مستفاد از ماده ۲۹ مورد تأکید قانون‌گذار قرار گرفته، بنابراین در جرم کلاهبرداری مرتبط با رایانه هرگاه تمهید مقدمات و نتیجه حاصل از آن در حوزه‌های قضایی مختلف صورت گرفته باشد، دادگاهی که بانک افتتاح‌کننده حساب زیان‌دیده از بزه که پول به طور متقلبانه از آن برداشت شده در حوزه آن قرار دارد صالح به رسیدگی است. بنا به مراتب آرا شعب یازدهم و سی و دوم دیوان عالی کشور که براساس این نظر صادرشده به اکثریت آرا صحیح و قانونی تشخیص و تأیید می‌گردد. این رأی طبق ماده ۲۷۰ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری در موارد مشابه برای شعب دیوان عالی

کشور و دادگاه‌ها لازم‌الاتباع است.» لذا اگر به طور مثال در تهران، شخص الف مبادرت به سوء استفاده از برنامه های رایانه ای به قصد فریب دیگری نماید، در حالیکه مال از حساب فرد در اهواز برداشت شده باشد، دادسرا و دادگاه صالح، اهواز خواهد بود. (اسعدی، ۱۳۸۶: ۱۲۵)

۱-۶-عنصر تشکیل دهنده جرم کلاهبرداری

برای تشکیل جرم کلاهبرداری همچون بسیاری از جرایم دیگر به سه عنصر قانونی، مادی و معنوی نیاز است. عنصر قانونی جرم کلاهبردرای، ماده یک قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاهبرداری مصوب ۱۳۶۷/۹/۱۵ مجمع تشخیص مصلحت نظام به انضمام دو تبصره آن می باشد که در بخش های دیگر گزارش بیان خواهد شد. (شامبیاتی، ۱۳۹۴: ۹۸)

عنصر دوم جرم کلاهبرداری، عنصر مادی است که عبارتست از این که اولاً مرتکب به وسایل متقلبانه متوسل شود یا مانورهای متقلبانه از خود بروز دهد (مدارک و عناوییینی جعل کند، دفتر و شرکتی راه اندازی کند، مردم را به امور واهی امیدوار کند یا از امور واهی بترساند و استفاده از هر نوع وسیله ای که عرفاً وسیله متقلبانه محسوب می شود) دوم این که شخص مقابل (مالباخته) فریب بخورد و به او اعتماد کند. سوم این که کلاهبردار موفق شود مال دیگری را ببرد. مجموع این شرایط، عنصر مادی جرم کلاهرداری را تشکیل می دهد به نحوی که می توان گفت، هر یک از این سه رکن موجود نباشد عنصر مادی جرم کامل نبوده و جرم کلاهبرداری صورت نگرفته است. عنصر سوم مورد نیاز برای تشکیل جرم کلاهبرداری عنصر روانی است، از عنصر روانی، تحت عنوان "سوء نیت" نیز یاد می شود. برای این که فرد کلاهبردار محسوب شود، باید در ارتکاب اعمالی که عنصر دوم کلاهبرداری را تشکیل می دهد، سوء نیت داشته باشد. (شمس، ۱۳۹۱: ۱۲۴)

سوء نیت دو نوع است:

۱-سوء نیت عام ۲- سوء نیت خاص

سوء نیت عامل در جرم کلاهبرداری این است که مرتکب قصد ارتکاب اعمال مادی فیزیکی ذکر شده را داشته باشد، یعنی عمد در توسل به وسایل متقلبانه، سوء نیت خاص در جرم کلاهبرداری، یعنی این که مرتکب قصد بردن مال غیر را داشته باشد. اثبات وجود سوء نیت در مرتکب، بر عهده شاکی و دادستان می باشد و بنابر این در صورت عدم توانایی ایشان در اثبات سوء نیت مرتکب از اتهام کلاهبرداری تبرئه خواهد شد.

۱-۶-۱-عنصر قانونی کلاهبرداری رایانه ای

قانونگذار کشور ایران برای نخستین بار جرم کلاهبرداری رایانه ای را از طریق تصویب ماده ۶۷ قانون تجارت الکترونیک مصوب ۱۳۸۲ وارد قوانین جزایی ایران نمود. مطابق ماده ۶۷ قانون تجارت الکترونیک : «هر کس در بستر مبادلات الکترونیکی، با سوء استفاده و یا استفاده غیر مجاز از «داده پیام» 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 ردّ مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل

مال مأخوذه محکوم می شود.»تبصره ی ذیل ماده ۶۷ قانون فوق الاشاره نیز شروع به کلاهبرداری رایانه ای را صریحاً جرم محسوب و مجازات آن را یک سال حبس تعیین نمود.

قانونگذار مجدّداً در ماده ۱۳ قانون جرایم رایانه ای نسبت به جرم انگاری کلاهبرداری رایانه ای اقدام نموده است، بنابراین در حال حاضر عنصر قانونی جرم کلاهبرداری رایانه ای، ماده ۱۳ قانون جرایم رایانه ای می باشد. ماده ی ۱۳ قانون مذکور در تعریف جرم کلاهبرداری رایانه ای اشعار می دارد :

«هر کس به طور غیر مجاز 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 ردّ مال به صاحب آن به حبس از یک سال 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.»

۱-۶-۲-عنصر مادی جرم کلاهبرداری رایانه ای

در باب موضوع عنصر مادی کلاهبرداری رایانه ای موارد ذیل مورد عنایت می باشد:

۱- مرتکب جرم کلاهبرداری رایانه ای می تواند هر کس اعم از نظامی یا غیر نظامی و ایرانی یا خارجی باشد. همچنین وجود سمت یا موقعیت خاصی برای شخص مرتکب جرم کلاهبرداری رایانه ای شرط نشده است.

۲- در کلاهبرداری سنّتی، انجام مانور متقلبانه جهت وقوع عنوان مجرمانه ی کلاهبرداری لازم و ضروری است. در کلاهبرداری رایانه ای نیز عمل مادی مرتکب انجام اعمال متقلبانه بر روی سامانه های رایانه ای یا مخابراتی است. قانونگذار ایران از باب تمثیل شش مصداق از این اعمال متقلبانه را به صورت تمثیلی بیان نموده است یعنی این طرق حصری نبوده و طرق مشابه را نیز در بر خواهد گرفت.

طرق متقلبانه ی مذکور عبارتند از : ۱- وارد کردن داده ها (ورود غیر مجاز داده ها و یا وارد کردن داده های غیر مجاز)، ۲- تغییر داده های اصلی، ۳- محو داده ها، ۴- ایجاد داده ها، ۵- متوقف نمودن داده ها و نهایتاً ۶- مختل نمودن سامانه رایانه ای

۳- در کلاهبرداری سنّتی تأثیر مانور متقلبانه بر بزه دیده از طریق فریب، برای تحقق عنوان مجرمانه ی ضروری است چرا که لازمه اصلی کلاهبرداری، فریب خوردن شخص است. اعتقاد برخی از حقوقدانان این است که فریب مربوط به اشخاص حقیقی است و در باب سامانه های رایانه ای مصداق ندارد، در مقابل بسیاری از حقوقدانان اغفال سامانه هارا نیز ممکن می دانند و در این باب کلاهبرداری سنّتی را هم ردیف با کلاهبرداری رایانه ای می دانند. به نظر می رسد نظر دوم مورد قبول باشد و در واقع کلاهبردار با اغفال و فریب سامانه مال را از آن خود می نماید.

۴- عمل کلاهبردار می بایست به صورت غیر مجاز باشد. غیر مجاز بودن عمل مرتکب در کلاهبرداری رایانه ای همان متقلبانه بودن عمل او است.

۵- وارد نمودن داده ها از طریق ورود داده های غیر واقعی به درون سامانه صورت می گیرد. این عمل می تواند هم وسط افراد مجاز به ورود داده ها به سامانه صورت پذیرد هم توسط سایر افراد.

۶- ایجاد داده ها به وجود آوردن داده های جدیدی بر روی سامانه است به طوری که مرتکب جرم کلاهبرداری رایانه ای یا شخص دیگر را به طور غیر واقعی بستانکار یا دارای حقوق مالی جلوه دهد.

جرم کلاهبرداری رایانه ای جرم مقید به نتیجه است و قانونگذار حصول یکی از نتایج زیر را جهت تحقق جرم کلاهبرداری رایانه ای ضروری دانسته است:

۱- تحصیل وجه برای خود یا دیگری، ۲- تحصیل مال برای خود یا دیگری، ۳- تحصیل منفعت برای خود یا دیگری، ۴- تحصیل منفعت برای خود یا دیگری، ۵- تحصیل امتیازات مالی برای خود یا دیگری (گلدوزیان ؛ ۱۳۹۱)

۱-۶-۳-عنصر معنوی جرم کلاهبرداری رایانه ای

جرم کلاهبرداری رایانه ای از جرایم عمدی است و بنابر اصل عمدی بودن جرایم، وجود عمد در اقدامات متقلّبانه در شخص مرتکب جرم کلاهبرداری رایانه ای لازم است. وجود انگیزه خاصی در قوانین جزایی برای مرتکب جرم کلاهبرداری رایانه ای شرط نشده است و بنابراین مرتکب با هر انگیزه ای که مرتکب جرم کلاهبرداری رایانه ای شود تأثیری در عنوان مجرمانه نخواهد داشت. همچنین از آنجایی که جرم کلاهبرداری رایانه ای مقیّد به نتیجه است، بنابراین وجود سوء نیت خاص یعنی قصد تحصیل وجه، مال، منفعت، خدمات یا امتیاز مالی برای خود یا دیگری در شخص مرتکب جرم کلاهبرداری رایانه ای ضروری است. (سلطانی، ۱۳۸۴)

۱-۷-ضمانت اجرا و قابل گذشت بودن جرایم کلاهبرداری اینترنتی

جرم کلاهبرداری اینترنتی جرمی قابل گذشت است کلاهبرداری و کلیه جرایمی که در حکم کلاهبرداری هستند، بر اساس قانون کاهش مجازات حبس تعزیری مصوب سال ۱۳۹۹، در صورتی که موضوع آن ها کمتر از ۱۰۰.۰۰۰.۰۰۰ تومان باشد قابل گذشت محسوب می شوند. منظور از جرم قابل گذشت جرمی است که فرایند تعقیب، رسیدگی و صدور رای در آن ها منوط به درخواست شاکی است. بدون طرح شکایت شاکی در مراجع قضایی، امکان تعقیب و رسیدگی به این جرایم وجود ندارد و در صورت گذشت شاکی در فرایند دادرسی نیز رسیدگی قضایی به این جرایم متوقف می شود.کلاهبرداری از زمره جرایمی است که نوعی "اکل مال بباطل " محسوب می شود و با توجه به آیه " ولا تاکلو اموالکم بینکم بالباطل" با استفاده از عنوان کلی تعزیرات قابل مجازات است.

مطابق قوانین کیفری مجازات کلاهبرداری ساده با مشدد متفاوت است. کلاهبرداری مشدد کلاهبردرای است که در آن مرتکب مشمول یکی از سه حالت زیر باشد:

۱-کارمند دولت یا موسسات عمومی و شهرداری ها یا نهادهای انقلابی باشد

۲-مرتکب خود را به عنوان مامور دولت یا موسسات عمومی یا شهرداری، یا نهادهای انقلابی و شرکت های دولتی معرفی نماید

۳-مرتکب بای فریب مردم از تبلیغ عامه از طریق وسایل ارتباط جمعی از قبیل رادیو، تلویزیون، روزنامه، مجله یا نطق در مجامع و یا انتشار آگهی چاپی یا خطی استفاده کند.

به این کلاهبرداری ها کلاهبرداری مشدد اطلاق می شود و مجازات مرتکب آن علاوه بر رد مال به صاحب آن، دو تا ۱۰ سال حبس به علاوه جزای نقدی معادل مال مأخوذه است و نیز انفصال ابد از خدمات دولتی می باشد. (اردبیلی، ۱۳۹۴)

کلاهبرداری که شامل هیچ یک از انواع سه گانه فوق نباشد، کلاهبرداری ساده است و مرتکب آن به حبس از یک تا هفت سال به علاوه جزای نقدی معادل مال مأخوذه و رد مال محکوم می شود. مطابق تبصره یک این ماده در صورت وجود جهات و کیفیات مخففه دادگاه می تواند با اعمال ضوابط مربوط به تخفیف، مجازات مرتکب را فقط تا حد اقل مجازات مقرر در این ماده

(حبس) و انفصال ابد از خدمات دولتی تقلیل دهد ولی نمی تواند به تعلیق اجرای کیفر حکم دهد. همچنین تبصره دو این ماده مجازات جرم شروع به کلاهبرداری را بیان نموده است که عبارت است از: حد اقل مجازات مقرر در همان مورد و در صورتی که نفس عمل انجام شده نیز جرم باشد، شروع کننده به مجازات آن جرم نیز محکوم می گردد. اگر شروع کننده کارمند دولت و مرتبه کلی یا بالاتر یا همطراز آنها باشد از خدمات دولتی منفصل دائم می شود و در مراتب پایین تر به انفصال موقت از شش ماه تا سه سال محکوم خواهد شد. (آشوری، ۱۳۹۲: ۶۰)

۱-۸-تفاوت کلاهبرداری سنتی با جرم جرم کلاهبرداری اینترنتی

جرم کلاهبرداری اینترنتی با کلاهبرداری سنتی که در خارج از فضای مجازی و رایانه صورت می گیرد، تفاوت هایی دارد. در تعریف کلاهبرداری سنتی گفته می شود: کلاهبرداری یعنی انجام مانور متقلبانه برای فریب دادن دیگری و بردن مال او در نتیجه این فریب. در حالی که در جرم کلاهبرداری اینترنتی یا کلاهبرداری رایانه ای، اساسا عملکرد صاحب مال یعنی فریب خوردن یا نخوردن او موضوعیت ندارد و شخص کلاهبردار با استفاده از تغییرات فنی در داده یا سامانه، مال یا منفعت و امتیاز مالی شخص بزهدیده را به دست می آورد. بنابراین صرف اثبات تحصیل مال دیگری از طریق رایانه برای اثبات جرم کافی است و نیازی به اثبات وضعیت روانی بزهدیده یعنی فریب خوردن او وجود ندارد.

۱-۹-دلایل وقوع جرم کلاهبرداری

هر جرمی دارای ابعاد گوناگونی است، جرم پدیده تک بعدی نیست که بگوییم فقط فقر یا عامل دیگری موجب ارتکاب آن می شود. در به وجود آمدن این جرم پدیده های زیادی موثر هستند. (باهری، ۱۳۹۰) یکی از مواردی که با کلاهبرداری ارتباط مستقیم دارد بیکاری است، وقتی که مسئله تولیددر کشور دچار خدشه و کاهش شود طبیعتاً به خیل بیکاران افزوده می شود و ممکن است این افراد به دلیل اینکه از راه مشروع قادر به تامین نیازهای خود نیستند به کلاهبرداری دست بزنند. عنصر اصلی کلاهبرداری این است که از اعتماد مردم سوء استفاده شود، عموم کسانی که مورد کلاهبردرای واقع می شود در زندگی صادق و سالم زندگی کرده اند، البته این نکته را باید مد نظر داشت که طمع افرادی که مورد کلاهبرداری واقع می شوند نیز می تواند از دلایل دیگر وقوع جرم کلاهبرداری باشد. (پاد، ۱۳۹۲: ۵۴)

این افراد به دلیل طمع می خواهند بدون زحمت به ثروت برسند به همین دلیل بدون فکر خود را در دام کلاهبرداران قرار می دهند. از دیگر دلایل وقوع جرم کلاهبرداری می توان به سست شدن اعتقادات مردم اشاره کرد. عمده فرهنگ ما به اعتقادات مذهبی برمی گردد اکنون ترمیم اعتقادات مذهبی مهمترین عامل برای پیشگیری از وقوع جرم است. عامل دیگری که می تواند تاثیر زیادی در وقوع جرم کلاهبرداری در جامعه داشته باشد نداشتن برخورد قاطع با کلاهبرداران است. به این معنا که فرد پس از انجام دادن چند کار از راه های غیر قانونی و به عبارتی کلاهبرداری دستگیر شده و به زندان می افتد، ولی پس از آزادی هیچ پیگیری ای روی آن فرد ندارند و او بازهم می تواند دسته چک بگیرد و به فعالیت های اجتماعی و اقتصادی خود همانند افراد دیگر جامعه ادامه دهد و این خود باعث بروز مشکل است. (شمس، ۱۳۸۵)

۲-نظرات مختلف حقوقدانان در موضوع کلاهبرداری

دیدگاه اول؛ بر اساس این دیدگاه و نظریه طرفداران آن اساسا فرقی مابین کلاهبرداری و جرایم در حکم کلاهبرداری از حیث مجازات وجود ندارد لذا تمامی محدودیتها و مجازاتهایی را که قانونگذار برای کلاهبردار در نظر گرفته بر شخص در حکم کلاهبردار نیز بار می شود و دادگاه در مقام اعمال تخفیف حق ندارد از یک سال حبس مقرر در قانون تشدید مجازات مرتکبین ارتشا و اختلاس و کلاهبرداری پایین تر بیاید. (نظریه مشورتی شماره ۷/۷۲۴۸- ۷۳/۱۲/۱۰)

دیدگاه دوم؛ طرفداران این نظریه قائل به این هستند که قوانین جزایی باید به نفع متهم تفسیر شود؛ و چون در این زمینه ابهام وجود دارد و هرگاه در قوانین کیفری ما با ابهامی روبرو شویم باید آن را تفسیر کنیم و چون آخرین مرحله از مراحل تفسیر قوانین جزایی، تفسیر به نفع متهم است لذا باید نفع متهم را لحاظ کرده در جرایمی که در حکم کلاهبرداری بوده و شرایط اعمال تخفیف نیز مساعد می باشد از محدودیت موجود در تبصره ماده یک قانون تشدید چشم پوشی نمود. (پاد، ۱۳۹۲)

دیدگاه سوم؛ این دیدگاه را دکتر عباس زراعت در مقاله ای با عنوان گذشت در جرائم غیر قابل گذشت که در فصل نامه حقوق دانشگاه تهران به چاپ رسیده آورده است. بر اساس این دیدگاه بهتر است ما بین جرائمی که قانونگذار آنها را در حکم کلاهبرداری دانسته است مانند ماده یک قانون مجازات راجع به انتقال مال غیر که انتقال دهنده مال غیر را کلاهبردار محسوب کرده است و جرائمی که قانونگذار صرفا مجازات کلاهبرداری را در مورد آنها قابل اعمال می‌داند مانند ماده ۱۰۷ قانون ثبت اسناد و املاک، تفکیک قائل شد. بر اساس این دیدگاه در ارتباط با جرائم در حکم کلاهبرداری مانند انتقال مال غیر باید قائل بر ترتب همه احکام و آثار کلاهبرداری شد. لذا تخفیف به کمتر از حداقل قانونی امکان پذیر نیست اما در ارتباط با جرایمی که مرتکب فقط به مجازات کلاهبرداری محکوم می شود مانند ماده ۱۰۷ قانون ثبت اسناد و املاک، چون قانونگذار فقط از میان همه احکام کلاهبرداری، مجازات آن را در مورد این جرائم برقرار دانسته است و برقراری سایر احکام کلاهبرداری با تفسیر مضیق قانون به نفع متهم ناسازگار نیست لذا تخفیف مجازات تا کمتر از حداقل قانونی نیز امکان دارد. (گلدوزیان: ۱۳۹۱: ۷۱)

۳-گستره تاریخی قانون گذاری در مورد جرایم الکترونیک

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 روبیس برمی‌گردد که بعد از بی مهری مسئولان یک شرکت فروش عمده میوه و سبزی به عنوان حسابدار آنها انتخاب می شود از طریق کامپیوتر اقدام حسابرسی یا تغییر قیمت ها و تنظیم درآمدجنس، مرجعی از مرجع آنهاکاهش و به جای دیگری واریز می کند. رومیس با ظرافت خاصی قیمت ها را تغییر می داد. بعد از آن با نام ۱۷ شرکت محل و قراردادچک های جعلی صادر و ازآن حساب برداشت می کرد به طوری که در کمتر از ۶ 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 می کند و به ۱۰ سال زندان محکوم می شود. بدین ترتیب زمینه پیدایش جرم رایانه ای شکل می گیرد و دادگاه را به تدوین قوانین مدون وا می دارد. براساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ 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 گروهک-های هکر موسوم به گروه مش قاسم و.... جرم‌های دیگری مرتکب می‌شـدند، مواردی چون جعل اسکناس، اسناد و بلیط‌های شرکت‌های اتوبوس رانی، جعل اسناد دولتی از قبیل گواهینامه، کارت پایان خدمت، مدرک تحصیلی و.... مساله ای که نشان

دهنده گسترش روز افزون جرائم الکترونیکی در کشور است هر چند این جرائم سابقه ای طولانی در ایران و جهان دارند. تاریخچه¬ای دقیقی از پیدایش جرم الکترونیکی و کامپیوتری زمان وجود ندارد ولی هرحال این دسته از جرائم را باید زاییده و نتیجه تکنولوژی ارتباطی و اطلاعاتی دانست براساس مطالعات صورت گرفته منشا ی پیدایش جرم کامپیوتری و اینترنتی به قضیه رویس برمی گردد. او که بعد از بی مهری مسئولان یک شرکت فروش عمده میوه و سبزی به عنوان حسابدار آن ها انتخاب می شود از طریق کامپیوتر اقدام به حسابرسی کرده و با تغییر قیمت و تنظیم درآمد جنس، مبلغی از مرجع آن راکاهش و به جای خاص واریز می کند. (جزایری، ۱۳۸۸: ۱۳۲)

رویس با ظرافت خاصی قیمت ها را تغییر می داد بعد از آن با نام ۱۷ شرکت محل و طرف قرارداد چک های جعلی صادر وز آن حساب برداشت می کرد به طوریکه در کمتر از ۶ سال بیش از یک میلیون دلار بدست آورده است اما به علت نداشت مکانیزم برای توقف پیدایش جرم رایانهای شکل می گیرد و دادگاه به تدوین قوانین مدون وا می دارد. براساس اطلاعات موجود اولین جرم اینترنتی در ایران در تاریخ ۲۶ خرداد ۱۳۷۸ به وقوع پیوست یک کارگر چاپخانه و یک دانشجو کامپیوتر در در کرمان به جعل چک¬های تضمینی مسافرتی کردند و چون تفاوت و تمایز چندان بین جرم کامپیوتری و جرم اینترنتی وجود ندارد. عمل آنها به عنوان جرم اینترنتی محسوب می شود. بعد از این بود که گروهای هکر موسوم به گروه مش قاسم و... جرم های دیگری را مرتکب شدند.

چنانچه که شاید یکی از مهمترین و خبر ساز ترین پرونده ها توزیع سی دی های مستهجن به نمایش درآمده در سایت های مختلف از افراد مشهور از جمله بازیگران یا مردم عادی است. پیشرفت تکنولوژی و علم همواره با پیدایش چالش¬های جدید در زمینه ارتکاب جرم و اعمال مجرمانه هم همزمان بوده است که به طور خاص عصر کامپیوتر و اینترنت موج جدیدی از جرائم مرتبط را نیز به همراه داشته است. گسترش روز افزون اینترنت با سرعتی سرسام آور به رغم مزایای فراوان در عرصه¬های گوناگون سرگرمی، تجارت، ورزش، فرهنگ یا آموزش مشکلاتی را نیز به همراه داشته که به جرائم رایانه ای و اینترنتی معروف است. گسترش جرائم ارتکابی با رایانه ها به اندازه ای بوده که بیشتر کشورهای دنیا با اعمال قوانینینی به مبارزه با این پدیده پرداخت و سعی در مهار آن دارد.

یک کارشناس هندی در این زمینه می گوید:

امروزه دستاورد و احتمال موفقیت دزدان با استفاده از یک کامپیوتر بسیار بیشتر از یک اسلحه است. شاید تروریست¬های فردا نیز بتوانند با استفاده از یک صحفه کلید به جای یک بمب آسیب های بیشتری وارد آورند. برای این پدیده نوظهور از اصطلاحاتی مانند جرائم رایانه ای، جرائم اینترنتی، جرائم تکنولوژیک و یا جرائم الکترونیکی استفاده می کنند و معمولاً این اصطلاحات به فعالیت های مجرمانه ای گفته می شود که یک کامپیوتر یا رایانه، منبع، ابزار، هدف، و یا محل وقوع جرم باشد.

گسترش روز افزون اینترنت با سرعتی سرسام آور به رغم مزایای فراوان در عرصه های گوناگون سرگرمی، تجارت، ورزش، فرهنگ یا آموزش مشکلاتی را نیز به همراه داشته که به جرایم رایانه ای و اینترنتی معروف است. وجود رایانه و اینترنت مسائل امنیتی خاص خود را نیز به دنبال داشته است که احتمال خطرهای امنیتی برای رایانه های مرتبط شبکه هایی مانند اینترنت بیشتر است گسترش جرایم ارتکابی با رایانه به اندازه ای بوده که بیشتر کشورهای دنیا با اعمال قوانینی به مبارزه با این پدیده پرداخته و سعی در مهار آن داشته اند. (گلدوزیان؛ ۱۳۹۱)

۴-جرائم اینترنتی از نظر نوع اثرگذاری

جرائم اینترنتی از نظر نوع تاثیر به سه دسته کلی تقسیم می شوند:

۴-۱-جرائم بر ضد هنجارهای اجتماعی

ارزش های موجود در جامعه موجب ماندگاری و ثبات فرهنگی و اخلاقی آن جامعه می شود. به همین جهت هر جامعه ای در جلو گیری از محو یا کم رنگ شدن آن ها می کوشد. فرهنگ ایرانی اسلامی نیزدارای ارزش هایی است که باید به طرق مختلف ازجمله قراردادن ضمانت اجرا و برخورد با مهاجمان به ارزش ها در صیانت آن کوشید. علاوه بر ماده ۵۱۳ قانون مجازات اسلامی که قانونی عام و شامل برخی از جرائم اینترنتی نیز می شود. در قانون مطبوعات که طبق تبصره ۳ ماده ۱ شامل کلیه نشریات الکترونیکی ثبت شده بر اساس این قانو می شود. به جرم توهین به اسلام و مقدسات اشاره شده است. البته قانون مطبوعات را نمی توان شامل برخی مصادیقی دانست که خارج از این قانون هستند چرا که صحفات وب، داده ها و نشریات الکترونیکی ثبت نشده یا خارج از ایزان را شامل نمی شود. البته در ایران در برخی قوانین مصوب مثل لایحه حمایت از پدید آورندگان نرم افزار و قانون تجارت الکترونیک به برخی جرائم رایانه ای اشاره شده است. (شمس، ۱۳۸۵)

۴-۲-جرائم محتوا

از ارزشهای مترقی جوامع اسلامی حفظ عفت عمومی و اخلاق حسنه است. حفظ عفت عمومی، اقدامی پیشگیرانه از وقوع جرائم بسیاری است که ناشی از ایجاد هرج و مرج در رفتار افراد جامعه می شود. به عنوان نمونه یکی از عوامل وقوع جرم زنا، همجنس بازی، مساحقه و قوادی به هیجان در آوردن شهود مجرمان است که در اثر ترویج مطالب مستخجن افزایش خواهد یافت. از این رو قانون جرائم رایانه‌ای، فصل چهارم خود را به جرائم مرتبط با محتوا اختصاص داده است. به هرحال در تمام دنیا یک سری ارزش ها و آرمان هایی وجود دارد که نمی توان به حوزه آنها اهانت نمود و یا نشر برخی از مطالب ممنوع شمرده می شود. به عنوان مثال در اکثر کشورهای اروپایی پروژه‌های تبلیغاتی تروریسم و همچنین پرنوگرافی اطفال از طریق اینترنت در زمره جرائم اینترنتی شناخته می شوند. صرف نظر از اینکه تعریف ها از تروریسم چیست و چرا فقط مسایل مستهجن را در مورد کودکان ممنوع و پخش آن جرم می دانند این نکته قابل تامل است که برای مبارزه با جرائم اینترنتی خود هم قوانین بسیار محکم و سخت گیرانه تصویب می کنند که از جمله ی آن ها می توان به دستور العمل ۲۹ اکتبر سال ۲۰۰۴ اتحادیه اروپا اشاره کرد که براساس آن پلیس حق دارد در مواردی فوری و لازم به نظر می رسد بدون اینکه به فرد اطلاع دهد تمام اطلاعات متهم را اصطلاحاً پلمپ نماید و حتی وارد اطلاعات شخصی فرد شده و به تمام آن ها، پیدا کند و آن ها را برای ارایه به دادگاه جمع آوری نماید. (سلطانی، ۱۳۸۴: ۵۵)

۵-انواع جرائم الکترونیکی در حقوق انگلیس

۱. کلاهبرداری مرتبط با رایانه (به ویژه توسط کارکنان داخل سازمان)

۲. اعمال انتقامجویانه و کینه توزانه (توسط کارکنان سابق و ناراضی سازمان)

۳. جاسوسی های صنعتی و صنفی (افشا شدن اسرار صنعتی و صنفی)

۴. سوء استفاده های مالی حین نقل و انتقال اکترونیکی وجوه

۵. خطاهای رایانه ها و از بین رفتن برنامه ها و اطلاعات

کلاهبرداری رایانه ای در ایالات متحده انگلیس به حریم خصوصی اشخاص با یک نگاه کلی می توان خطرات حاصل از جرائم الکترونیکی را به دو دسته تقسیم بندی نمود:

دسته اول: شامل خطرات عمده نظیر کلاهبرداری، انتقام جویی و کینه توزی، جاسوسی صنعتی خطا و تجاوز به حریم خصوصی است.

دسته دوم شامل خطرات جزئی نظیر نفوذیها و ویروسیها می باشد. جهت کاهش جرائم الکترونیکی و جلو گیری یا بروز برخی وقایع ناگوار بهتر است.

۶-ادله الکترونیکی

هرگونه داده نرم افزار یا سخت افزار الکترونیکی که بتواند اطلاعات ارزشمندی در راستای اثبات ادعا، دفاع، کشف، جرم یا استدلال قضایی به دست دهد. دلیل الکترونیکی محسوب است. این اطلاعات که ممکن است در اسناد کاغذی موجود نباشد. می تواند نقش موثری در فرایند تعقیب کیفری یا دادرسی ایفا کند و با توجه به توسعه فناوری الکترونیک به ویژه فناوری اطلاعات و ارتباطات یکی از ابزارهای مهم فن حقوق محسوب خواهد بود.

اهمیت ادله الکترونیکی با توجه به گسترش استفاده از فناوری رایانه در زمینه مدیریت اطلاعات و افزا به رهگیری از سیستم رایانه‌ای ایجاد می‌شود که کشف آن و استناد بدان حائز اهمیت خاص است. در پرونده های مختلفی از دعاوی اخیر کشورهای توسعه یافته از جمله موارد آزار جنسی، نشر غیر مجاز، کلاهبرداری، اثبات ارتباط قربانی و متهم در موضوع قتل عمدی، اثبات سرقت اسرار تجاری و کاری و کشف دلیل و مدرک دال برسایر اعمال مجرمانه و غیره از ادله الکترونیکی بهره جسته‌اند. چه بسا اطلاعاتی که در ادله الکترونیکی یافت می‌شود اما در ادله دیگر آن را نمی‌توان یافت. چه بسا مطالب تایپ شده که چاپ از آن گرفته نشده‌است. چه بسا دلایل الکترونیکی مهمی که خوانده از وجود آن آگاهی نداشته یا نسبت به حذف یا ذخیره آن بیخبر مانده‌است. (روایی، میرزکی ۱۳۹۱ ص ۴۹)

طرح آیین‌دادرسی جرائم نیروهای مسلح و دادرسی الکترونیکی که با اصلاحاتی در جلسه مورخ هشتم مهرماه یکهزار و سیصد و نود و سه به تصویب کمیسیون قضائی و حقوقی مجلس شورای اسلامی بر اساس اصل هشتاد و پنجم (۸۵) قانون اساسی جمهوری اسلامی ایران رسیده و در جلسه مورخ ۳۰/۰۷/۱۳۹۳ شورای نگهبان مورد بحث و بررسی قرار گرفت و با توجه به اصلاحات به عمل آمده مغایر با موازین شرع و قانون اساسی شناخته نشده و به عنوان قانون به تصویب رسید و در تاریخ ۱۳۹۳/۰۸/۲۰ در روزنامه رسمی منتشر و از تاریخ ۱۳۹۴/۰۴/۰۱ لازم الاجرا می شود.

این قانون پس از کش و قوس های فراوان بالاخره به تصویب رسید تا راهی برای مقابله با جرائم اینترنتی و دادرسی الکترونیکی باز شود.

۶-۱-اسناد الکترونیکی در حقوق انگلیس

در حقوق ما سند (الف) نوشته های است که در مقام دعوی یا دفاع قابلاً استناد می شود. (ماده ۱۲۸۴ ق. م و ماده ۳۷۰ به بعد آیین دادرسی مدنی، (ب) مطلق دلیل است اعم از مکتوب یا ملفوظ و مرادف با مدرک است و در همین معنی عبارت «سند کپی» به کار رفته که تلویحاً از وجود سند غیر مکتوب حکایت دارد. (میرمحمدصادقی، شایگان، ۱۳۸۹ صص ۱۳۷-۱۶۲)

۶-۲-جرائم اینترنتی در حقوق انگلیس

از زمان ابداع اینترنت تا زمانی که استفاده از اینترنت شکل عمومی پیدا کرد، تصور از پیش تعیین شده‌ای درباره این امکان ارتباطاتی و اتفاقاتی که در آن می‌افتد وجود نداشته است. بسیاری از اتفاقات افتاده است و سپس کسانی به دنبال تبیین و در مواردی برخورد یا جلوگیری از آن برآمده‌اند. مطالب پیش رو به بررسی جرائم اینترنتی خواهد پرداخت و با مرور برتاریخچه اینترنت و وقوع این جرائم تلاش می کند تعریفی از آن ارائه کند، و مهمترین جرائم اینترنتی را معرفی کند.

اینترنت در سال ۱۹۶۴ توسط محققی به نام پائول باران در شرکت راند ابداع شد. وی به دنبال روشی برای مطمئن سازی ارتباط پنتاگون (وزارت دفاع، انگلیس) با اعضای ارتش در هنگام حمله واقعی اتمی بود و یک شبکه ارتباطات رایانه ای غیر متمرکز را پیشنهاد کرد که در آن رایانه مرکزی وجود نداشت.

در چنین شبکه ای که اینترنت شبکه آرپانتنام داشت حتی در صورت انهدام و خراب یک یا چند رایانه، همچنان امکان تبادل اطلاعات بین سایر رایانه های باقی مانده وجود خواهد داشت. در اوایل دهه ۷۰ میلادی محققان دریافتند که اینترنت علاوه بر روشی برای برقراری ارتباطات بین قسمت‌های مختلف ارتش، روش کم هزینه ای برای برقراری ارتباطات بین اشخاص و سازمان هاست (سلطانی، ۱۳۸۴).

۶-۳-جرائم رایانه ای در حقوق انگلیس

جرم رایانه‌ای در حقوق انگلیس بر دونوع است: در تعریف محدود (مضیق) جرمی که در فضای مجازی (سایبر) رخ دهد جرم رایانه‌ای است و بر اساس این دیدگاه اگر را یه ابزار و وسیله ارتکاب جرنم باشد آن جرم را نمی‌تواند زمره جرائم رایانه ای قلمداد کرد. در تعریف گسترده (موسع) هر فعل یا ترک فعلی که در یا «از طریق» یا «به کمک سیستم‌های رایانه‌ای» رخ می‌دهند جرم رایانه‌ای تلقی می‌شود. در کنفرانسیون بین‌المللی بوداپست (۲۰۰۱) چیزی تحت عنوان جرم رایانه‌ای مطرح نشده بلکه در فضای مجازی از نام برده شده که در فارسی به جرم مجازی تعبیر می‌شود. در اسناد و کنوانسیون بین‌المللی پیرامون جرائم رایانه‌ای رویکردی دوگانه وجود دارد به این معنا هم ارتکاب جرائم رایانه‌ای محض هک کردن و و هم ارتکاب برخی جرائم مانند جرائم سنتی با استفاده از سیستم‌های رایانه‌ای مانند نقض حقوق مالکیت معنوبی جرم انگاری تلقی شده‌است. (جعفری لنگرودی، ۱۳۸۷: ۳۲)

۶-۴-کلاهبرداری رایانه‌ای در حقوق انگلیس

از جمله جرائم اصلی سوء استفاده‌هایی کامپیوتری علیه اشخاص و یا دارایی افراد محسوب می‌گردد. دارایی عینی غیر مملوس در قالب داده‌های کامپیوتری مانند وجوه سپرده و پس انداز، تغییر و دستکاری کردن در ساعات کاری، متداولترین راه‌های کلاهبرداری کامپیوتری می باشد. در تجارت الکترونیک نقل و انتقال پول نقد و خرید و فروش کالاهای تجاری، به سرعت جای خود را به انتقال سپرده ها از طریق سیستمهای کامپیوتری داده است که نتیجتاً موجبات سوء استفاده کردن افراد سود جو و فرصت طلب را فراهم کرده است. کلاهبرداری کامپیوتری از طریق وارد کردن رمزها به خود پردازها و سو استفاده کردن از کارت های اعتباری دیگران ترین شیوه ارتکاب در کلاهبرداری کامپیوتری می‌باشد. (جعفری‌لنگرودی، ۱۳۸۷: ۷۱)

در ذیل به نمونه هایی از کلاهبرداریهای کامپیوتری اشاره می‌شود:

۱. سوء استفاده از شبکه تلفنی امروزه بعضی از افراد سود جو با استفاده از تکنیک‌های وارد خطوط تلفنی می‌شوند که آنها می-توانند مکالمات تلفنی خود را با هزینه‌های مشترکین دیگر انجام دهند. نوع دیگر سوء استفاده از شبکه تلفنی از طریق تجارت با شماره کارت‌های تلفن انجام می شود که از طریق کامپیوتر نفوذ یافتگی قرار می‌گیرد.

۲. سوء استفاده از صندوق‌های خود پرداز در گذشته، سوء استفاده از صندوق های خود پردازبا استفاده از کارت بانکهایی که به سرقت می‌رفت صورت می‌گرفت ولی امروزه با استفاده از سخت افزار و نرم افزار ویژه کامپیوتری، اطلاعات الکترونیکی غیر واقعی به صورت کد روی کارت بانک ثبت شده مورد استفاده قرار می‌گیرد.

۳. سوء استفاده از کارتهای اعتباری در حال حاضر، پیشتر معاملات از طریق اینترنت صورت می گیرد. مثلاً پرداخت قبوض برق، آب، تلفن و همچنین خرید کالا، شرکت در همایش‌های بین‌المللی و غیره معمولاً با استفاده از کردیت کارت (کارت اعتباری) استفاده می‌شود و معمولاً مشتری می‌بایست رمز کارت خود و دیگر جزئیات را قید نماید. بدین جهت بعضی افراد سود جو با فاش شدن رمز کارت اعتباری مشتریان سوء استفاده می‌نمایند.

۷-۴-جاسوسی کامپیوتری در انگلیس

جاسوسی کامپیوتری به عملی گفته می‌شود که شخصی یا گروهی برای دولت یک کشوری اطلاعات مخفیانه از دولت دیگر در ازای پول انجام می‌دهد به عنوان مثال می‌توان به موارد زیر اشاره نمود: در آلمان سازمان اطلاعاتی ک. گ. ب، روسیه به شخصی پول داده بود تا اطلاعات مخفیانه ارتش انگلیس را بدست آورد. یا در مواردی دیگر می‌توان گفت به قضیه لوس آلمان دانشمند هسته‌ای اشاره نمود که اطلاعات بسیار محرمانه هسته ای خود را در اختیار دولت چین قرارداده بود. ترور امروزه برخی اقدامات تروریستی با، به اطلاعات حفاظت شده صورت می پذیرد. (گلدوزیان، ۱۳۹۰: ۴۱)

نتیجه گیری

انتخاب عنوان «دسترسی غیرمجاز به سیستم های پردازش خودکار» برای این جرم در قانون جزای انگلیس و تقسیم دسترسی غیزمجاز رایانه ای به دسترسی ساده و دسترسی به قصد ارتکاب جرایم دیگر و تشدید مجازات برای مرتکبان شق اخیر در انگلستان از ابتکارات جالب قانونگذاران است که در کشور ما نیز قابل الگوگیری است.تبادل اطلاعات در فضای مجازی اینترنت و رایانه، بدون از آنجا که پیشگیری وضعی حتی در دنیای فیزیکی نیز ماهیتی فنی دارد، در حوزۀ جرائم سایبر به طور خاص مورد توجه قرار گرفته است. البته باید گفت این اقدام با محدودیتهای فراوانی مواجه است که می‌توان آن را از ابعاد مختلف بررسی کرد. اما به طور کلی، در عمل سه عامل مانع تحقق اهداف پیشگیری وضعی از این جرائم می‌شوند که عبارت‌اند از: ۱. مجرمان سایبر، طیف خاصی از اشخاص را تشکیل می‌دهند. گروهی از آنها که از لحاظ تخصص و مهارت در سطح بالایی قرار دارند، واقعاً خطرناک هستند و متأسفانه تدابیر پیشگیرانه در برابر آنها یارای مقاومت ندارد. بنابراین، تنها انتظاری که می‌توان داشت این است که تلاش شود از ارتکاب جرم افراد نیمه‌حرفه‌ای یا آماتور جلوگیری گردد یا زمینۀ بزه‌دیدگی افراد کاهش یابد. ۲. متأسفانه فضای سایبر با ویژگیهای منحصر به فرد خود، فی نفسه مانع تحقق اهداف پیشگیرانۀ وضعی است. در این فضا انواع ابزارهای ارتکاب جرائم سایبر در اختیار همگان قرار دارد و هرکس می‌تواند به فراخور تخصص و مهارت خود از آنها استفاده نماید. انتقال سریع و بسیار سادۀ اطلاعات و تجربیات حاصل از ارتکاب جرائم سایبر نیز می‌تواند مزید بر علت محسوب شود. ۳. از آنجا که این تدابیر صبغۀ فنی دارند، چندان قابل اتکا نیستند، زیرا چندی نمی‌گذرد که ضعفها و نحوۀ دور زدن آنها در فضای سایبر منتشر می‌شود؛ کما اینکه در کشورمان آنان که قصد خنثا کردن فیلترهای شبکه‌ای را دارند، در عمل با مشکلی مواجه

نیستند.علاوه بر این محدودیتها، موانع حقوق بشری بسیاری نیز سد راه تدابیر پیشگیرانهٔ وضعی قرار دارد. در این مقاله سعی شد موانع حقوق بشری بررسی شود و در این زمینه، سه اصل مهم آزادی بیان، جریان آزاد اطلاعات و حریم خصوصی انتخاب شد. در حال حاضر کمتر کشوری را می‌توان یافت که در قانون اساسی یا قوانین عادی خود به این اصول نپرداخته باشد. قانون اساسی کشور ما که به حق یکی از مترقی‌ترین قوانین اساسی دنیاست، به این اصول توجه ویژه‌ای داشته است. گرچه فضای سایبر ـ این پدیدهٔ شگفت‌انگیز قرن بیست و یکم ـ بسیاری از عرصه‌ها را با تحولات بنیادین مواجه کرده، سوء استفاده‌های فراوان از آن موجب پیش‌بینی تدابیر کیفری در این زمینه شده است. اما با توجه به مشکلات بسیاری که فراروی تدابیر کیفری وجود دارد، سیاست پیشگیری از وقوع این جرائم مناسب‌ترین تدبیر سیاست جنایی است. در این میان، پیشگیری وضعی یکی از اقدامات مهم محسوب می‌شود، اما با محدودیتهایی مواجه است که از جملهٔ آنها نقض موازین حقوق بشر است. ماهیت فضای سایبر به گونه‌ای است که تجلی هرچه بیشتر آزادی بیان و جریان آزاد اطلاعات را موجب شده و همچنین با امکاناتی که جهت برقراری انواع ارتباطات ایمن فراهم آورده، به نوعی در جهت حفظ حریم خصوصی افراد گام برداشته است. اما تدابیر پیشگیرانهٔ وضعی از جرائم سایبر، عمدتاً به گونه‌ای اجرا می‌شوند که این سه اصل حقوق بشری را نقض می‌کنند. این تحقیق درصدد است ضمن تبیین انواع تدابیر پیشگیری وضعی از جرائم سایبر، به تبیین چالشهای حاکم بر این تدابیر با موازین حقوق بشر بپردازد و اهمیت آن را برای جامعه بشری مشخ نماید.

با توجه به پیشرفت تکنولوژی و اطلاعات، بطور یقین افرادی سودجو و فرصت طلب نیز با فراگیری دانش در صدد سوء استفاده از تکنولوژی می‌باشد که این افراد سودجو، امکاناتی را که توسعهٔ تکنولوژی برای جامعه بشری به ارمغان می‌آورد دست خوش امیال و اغراض خود ساخته و باعث ایجاد مشکلاتی برای استفاده کنندگان از تکنولوژی گردیده و باعث ایجاد شبهه و تردید برای استفاده صحیح از این امکانات و تکنولوژی شده‌اند تا جائیکه امروزه توجه دولتمردان، حقوقدانان، متخصصین در امر تکنولوژی را به خود معطوف کرده است. هرچه بیشتر تکنولوژی کامپیوتری توسعه یابد جرائم کامپیوتری نیز توسعه پیدا خواهد نمود. ولی قوانینی که بتواند با این جرائم برخورد نماید پاسخگو نخوهد بود و دولتها می‌بایستی قوانین خود را متناسب با جرائم نمایند. زیرا جرائم کامپیوتری با جرائم غیر کامپیوتری و کلاسیک اختلاف اساسی دارند.

پیشنهادات کاربردی جرایم رایانه‌ای

با لحاظ قانونگذاریهای سابق و با التفات به خلوت افراد در محیط سایبر و تأمین محیط آزادیها حتی الامکان از جرم انگاری زاید اجتناب شود. با توجه به اینکه محیط مجازی رایانه و اینترنت دنیای جدیدی را پیش رو می نهد که ارتکاب جرایم در آن هم سریع صورت می گیرد و هم دارای جذبه است، حمایتهای بیشتری از افراد خاص و به ویژه اطفال و نوجوانان صورت بگیرد. ثالثاً علاوه بر مسؤولیت کیفری مرتکب جرم مرتبط با محتوا، مسؤولیت کیفری ارایه دهندگان خدمات اینترنتی و همچنین سایر اشخاص حقوقی پیش بینی گردد تا همگان برای سلامت و امنیت دنیای جدید سرباز شوند و در صورت تخلف بازخواست گردنددر برخی از کشورها، سوء استفاده ها مستلزم جرم انگاری و وضع قوانین کیفری جدیدی است. بعضی از تعاریف موسع بوده، شامل طیف گسترده ای از اعمال مجرمانه و سؤاستفاده های رایانه ای می شود و بعضی از تعاریف مضیق می باشد.

منابع و مآخذ

کتب

۱. اردبیلی، محمدعلی، (۱۳۹۴) حقوق جزای عمومی، جلد نخست، چاپ هشتم، تهران، نشر میزان.

۲. اسعدی، حسن (۱۳۸۶)، سازمان یافته ملی، تهران، نشر میزان.

۳. آشوری، محمد، (۱۳۹۲) بحثی پیرامون کلاهبرداری، مجله دانشکده حقوق و علوم سیاسی، شماره ۲۲/۱۳۵۴

۴. باقرزاده، احد، (۱۳۸۳) جرایم اقتصادی و پولشویی، چال اول، انتشارات مجد، تهران.

۵. باهری، دکتر محمد (۱۳۹۰)، نگرشی بر حقوق جزای عمومی، تهران: انتشارات مجد.

۶. پاد، ابراهیم، (۱۳۹۲)حقوق کیفری اختصاصی جلد دوم، چاپ اول، تهران، انتشارات رهام.

۷. پاد، ابراهیم، (۱۳۹۲)حقوق کیفری اختصاصی جلد دوم، چاپ اول، تهران، انتشارات رهام.

۸. تذهیبی، فریده (۱۳۸۱)، پول کثیف، ماهنامه بانک و اقتصاد، تهران، شماره ۲۴

۹. تقوی، مهدی، (۱۳۸۲) نهادهای پولی و مالی بین المللی، چاپ اول، پژوهشکده امور اقتصادی، تهران.

۱۰. جعفری‌لنگرودی، محمدجعفر (۱۳۸۷)، ترمینولوژی حقوق، تهران: گنج دانش.

۱۱. درویش، بهرام، (۱۳۹۴)حقوق جزای اختصاصی، جلد دوم (جرایم علیه اموال)، چاپ اول تهران، انتشارات نگاه بینه

۱۲. دیهیم، علیرضا، (۱۳۸۰) درآمدی بر حقوق کیفری بین المللی، چاپ اول، انتشارات وزارت امور خارجه، تهران.

۱۳. رهبر، فرهاد (۱۳۸۷)، پولشویی و روش‌های مقابله با آن، موسسه انتشارات و چاپ دانشگاه تهران.

۱۴. زراعت، عباس، (۱۳۹۳) حقوق جزای اختصاصی، جلد دوم (جرائم علیه اموال و مالکیت)، چاپ اول، تهران، انتشارات فکرسازان.

۱۵. ساکی، محمد رضا (۱۳۸۶)، آشنایی با جرم پولشویی، معاونت آموزش و تحقیقات قوه قضائیه، تهران، انتشارات جاودانه.

۱۶. سلطانی، محمد (۱۳۸۴)؛ادله الکترونیک (پایان نامه کارشناسی ارشد) دانشگاه تهران.

۱۷. شامبیاتی، هوشنگ، (۱۳۹۴) حقوق کیفری اختصاصی، جلد دوم، جرائم علیه اموال و مالکیت، چاپ هفتم، تهران، انتشارات ژوبین با همکاری انتشارات مجد.

۱۸. شمس، عبدالله، (۱۳۸۵)؛ ادله اثبات دعوا، انتشارات دراک، تهران، ، چاپ سوم

۱۹. گلدوزیان ؛ ایرج (۱۳۹۱)بایسته های جزای عمومی انتشارات میزان چاپ سوم

۲۰. میرمحمدصادقی، حسین (۱۳۹۱)، جرایم علیه اموال و مالکیت، تهران: نشر میزان.

۲۱. نوربها، رضا (۱۳۸۹)، زمینه حقوق جزای عمومی، تهران، انتشارات گنج دانش.

۲۲. ولیدی، محمدصالح (۱۳۸۸). بایسته‌های حقوق جزای عمومی، تهران، جنگل.

مقالات

۱. اسعدی، سیدحسن، نقش فزاینده پولشویی و مصادره اموال در قاچاق مواد مخدر، مجلس و پژوهش، شماره۳۷، سال دهم، بهار۱۳۸۶.

۲. امینی، محبوبه رهدارپور حامد، چنگایی فرشاد بازاندیشی درجرم کلاهبرداری به عنوان جرم مرکب پژوهشنامه حقوق کیفری، شماره ۵، بهار و تابستان ۱۳۹۱ ص ۲۱.

۳. پیشگیر، علی اصغر، بررسی پدیده پولشویی، فصلنامه بانک صادرات، سال ششم، شماره ۲۱، تابستان ۱۳۸۱.

۴. جزایری، مینا، جرم پولشویی به عنوان یک جرم مستقل، مجموعه سخنرانی ها و مقالات همایش بین المللی مبارزه با پولشویی، چاپ اول، نشر وفاق، تهران، ۱۳۸۸.

۵. حبیب زاده، محمدجعفر، مروری بر جرم کلاهبرداری در حقوق ایران، ماهنامه دادرسی، سال دوم، شماره هشتم، خرداد و تیرماه ۱۳۸۷

۶. دیوید هند مترجم: حمید پزشک فریب و ریاکاری با داده ها: کلاهبرداری در علوم مجله فرهنگ و اندیشه ریاضی، شماره ۴۱، پاییز ۱۳۸۷ ص ۱.

۷. رشیدی رامین کلاهبرداری بیمه ای : مفاهیم و چالش ها ماهنامه تازه های جهان بیمه، شماره ۱۱۶، دی و بهمن ۱۳۸۶ ص ۲۹.

۸. شایگان محمد رسول، ثابت سروستانی محمد امین راهکارهای مقابله با جرم کلاهبرداری رایانه ای در حقوق کیفری ایران فصلنامه کارآگاه، شماره ۹، زمستان ۱۳۸۸ صص ۳۲-۵۳.

۹. کاویانی مریم، وروایی اکبر بررسی تاثیر افزایش سالانه دیه بر نرخ وقوع جرایم کلاهبرداری و ارتشا فصلنامه پژوهش های اطلاعاتی و جنایی، شماره ۴۰، زمستان ۱۳۹۴ صص ۱۲۱-۱۴۲.

۱۰. میرمحمدصادقی حسین، شایگان محمدرسول بررسی تطبیقی کلاهبرداری سنتی و رایانه ای و مجازات های آن ها در نظام حقوقی ایران فصلنامه دیدگاه های حقوق قضایی، شماره ۵۲، پاییز و زمستان ۱۳۸۹ صص ۱۳۷-۱۶۲.

۱۱. روایی اکبر، میرزکی سید شمس الدین بررسی عوامل موثر بر کشف جرم کلاهبرداری رایانه ای فصلنامه پژوهش های اطلاعاتی و جنایی، شماره ۲۵، بهار ۱۳۹۱ ص ۴۹.