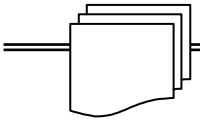
کلاه‌برداری رایانه‌ای در تجارت الکترونیکی

علی‌مراد حیدری*



چکیده: کلاه‌برداری رایانه‌ای، یکی از جرایم بستر مبادلات الکترونیکی، موضوع ماده‌ی ۶۷ قانون تجارت الکترونیکی ایران است.

رفتار مجرمانه‌ی این جرم از دو جزء "سوء استفاده یا استفاده‌ی غیرمجاز از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور" و "فریب اشخاص یا گمراه کردن سیستم‌های پردازش خودکار" تشکیل شده است. مصادیق سوء استفاده یا استفاده‌ی غیرقانونی در قالب انجام افعالی نظیر ورود، محو، توقف داده‌پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای دیده می‌شود.

بردن وجه، مال یا امتیاز مالی، نتیجه‌ی این جرم و محل وقوع این جرم، بستر مبادلات الکترونیکی است؛ یعنی بستری که در آن هرگونه روابط مالی الکترونیکی صورت می‌پذیرد است اعم از هرگونه فناوری جدید اطلاعات و ارتباطات همچون اینترنت، مخابرات، ماهواره و به‌طور کلی فضای سایبر.

رکن معنوی این جرم شامل عمد و اراده در انجام رفتار مادی،"استفاده‌ی غیرقانونی" (ورود، محو، توقف داده‌پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای) و قصد تحصیل وجه، مال یا امتیاز مالی برای خود مرتکب یا شخص مورد نظر اوست. مجازات کلاه‌برداری رایانه‌ای یک تا سه سال حبس و نیز پرداخت جزای نقدی معادل مال برده است که در مقایسه با مجازات کلاه‌برداری سنتی (یک تا هفت سال حبس و جزای نقدی معادل مال گرفته شده) دلایل متعددی تشدید مجازات کلاه‌برداری رایانه‌ای را نسبت به سنتی توجیه می‌کند!

واژگان کلیدی: کلاه‌برداری رایانه‌ای، کلاه‌برداری مرتبط با رایانه، بستر مبادلات الکترونیکی، تجارت الکترونیکی، جرم رایانه‌ای.

*. استادیار دانشگاه حضرت معصومه علیهاالسلام E mail: Heydarilaw@gmail.com

مقدمه:

تجارت الکترونیکی[1] روش نوین داد و ستد با استفاده از امکانات الکترونیکی و شبکه‌ی جهانی اینترنت است که تمام مراحل یک چرخه‌ی تجاری مانند تبلیغات، سفارش خرید، انعقاد قرارداد، تکمیل صورت حساب‌ها، پشتیبانی و خدمات پس از فروش به مشتریان را در بر می‌گیرد. در واقع، عناصر خاص دنیای سایبر یعنی سهولت، سرعت و همه جایی بودن آن، زمینه‌ی رشد و همه‌گیری این شیوه‌ی معاملاتی را فراهم آورده است و بیشتر شرکت‌های بزرگ تولیدی و خدماتی فعالیت گسترده‌ای را برای استفاده از این روش و حتی جایگزین کردن آن به جای روش تجارت سنتی آغاز کرده‌اند و بسیاری از دولت‌ها نیز در حال فراهم کردن بسترهای فنی، حقوقی و آموزشی گسترش این شیوه‌ی تجاری هستند و هر روز شاهد گسترش معاملات الکترونیکی و تنوع ابزارهای آسان‌کننده‌ی آن هستیم؛ به گونه‌ای که به جرأت، می‌توان تجارت الکترونیکی را تجارت هزاره‌ی سوم نامید. مرکز الکترونیکی بریتانیا[2] تجارت الکترونیکی را "هر نوع تجارت یا معامله‌ی اداری یا تبادل اطلاعاتی که با استفاده از هرگونه اطلاعات و فناوری ارتباطات به اجرا در می‌آید" تعریف کرده که تجارت تاجر با تاجر، تاجر با مشتری، دولت با مردم و نیز مبادله از طریق ابزارهایی همچون اینترنت، اینترانت، پست الکترونیکی و تبادل اطلاعات الکترونیکی را در بر می‌گیرد. (لارنس: ۱۳۸۳، ص۲۱۱) در واقع تجارت الکترونیکی یا کسب و کار الکترونیکی، انجام هرگونه امور تجاری و بازرگانی به صورت برخط[3] و از طریق شبکه‌ی جهانی اینترنت است که این امور می‌تواند شامل خرید و فروش عمده یا خرده کالای فیزیکی و غیرفیزیکی (نظیر اتومبیل یا نرم افزارهای کامپیوتری) ارائه خدمات

1 . Electronic Commerce.
2 . United Kingdom Electronic Center.
3 . On Line.

مختلف به مشتریان (نظیر مشاوره‌های پزشکی یا حقوقی) و دیگر موارد تجاری (همچون تبادل کالا با کالا و راه اندازی مناقصه‌ها و مزایده‌ها) باشد.(کورپر: ۱۳۸۰، ص۱۱) در این شیوه از تجارت، اینترنت نقش محوری دارد و رابطه‌ی بین دسترسی همگان به اینترنت و افزایش حجم تجارت الکترونیکی به گونه‌ای است که می‌توان آن را تجارت اینترنتی[1] نامید. تجارت الکترونیکی می‌تواند مزایای مختلفی مانند راحتی، قدرت انتخاب بیشتر، اطلاعات بیشتر درباره‌ی محصول و بهای کمتر را در اختیار مصرف‌کنندگان قرار دهد. همچنین با افزایش دسترسی به مجموعه کالاها و خدماتی که معمولا تنها در نواحی شهری موجود است، می‌تواند مزایای مهمی برای ساکنان روستاها و نواحی دوردست و مناطق مختلف داشته باشد.(Smith, 2000,p2)

از دید محققان، تجارت الکترونیکی سه بخش دارد: محصول، فرآیند و بازیگران تجارت؛ که ماهیت این سه بخش بر روی یک طیف از کاملا فیزیکی تا کاملا دیجیتالی قرار دارد. چنانچه ماهیت این سه بخش کاملا فیزیکی باشد، تجارت سنتی؛ اگر کاملا دیجیتالی باشد، تجارت الکترونیکی و اگر ماهیت این سه بخش حالت بینابین داشته باشد، تجارت نیمه الکترونیکی[2] نامیده می‌شود. (turban,2002, p33) بر اساس آمارهای کنفرانس سازمان ملل برای تجارت و توسعه (آنکتاد)[3] مجموع تجارت الکترونیک در سال ۲۰۰۶ ، ۸/۱۰۴ تریلیون دلار است که در این میان آمریکای شمالی ۳/۵، اروپای غربی ۱/۶،آسیا و اقیانوسیه ۱/۵، آمریکای لاتین ۰/۸۱۸ و سایر نقاط جهان ۰/۶۸۶ تریلیون دلار آن را به خود اختصاص داده اند. براساس آمارهای آنکتاد فروش آنلاین شرکت ها در

1 . Internet Commerce.

2 .Partial Electronic Commerce.

۳ . کنفرانس سازمان ملل برای تجارت و توسعه، یکی از ارکان مجمع عمومی سازمان ملل است که به موجب قطعنامه شماره (۱۹) ۱۹۹۵ مورخ ۱۹٦٤ مجمع عمومی برای تسریع رشد اقتصادی کشورها تشکیل شده است.

کشورهای در حال توسعه از کل تجارت آنها تا ۴۰ درصد، خرید آنلاین شرکت ها تا ۳۷ درصد و توزیع شرکت ها تا ۹ درصد است. براساس آمارها میزان تجارت الکترونیک ایران تا پایان سال ۸۴ حدود ۴۰ میلیارد ریال، تا پایان سال ۸۵ حدود ۱۰۰میلیارد ریال و تا پایان سال ۸۶ حدود یک هزار میلیارد ریال بوده است(www.sarmayeh.net/ShowNews.php)

هر چند حجم تجارت الکترونیکی در ایران چندان چشمگیر نبوده و حتی طبق ادعای برخی در میان شصت کشور، در رتبه‌ی ۵۸ از نظر تجارت الکترونیکی قرار گرفته است (نوری: ۱۳۸۴، ص۱۱۱)، لکن با اقدامات مختلفی که در سال‌های اخیر، چه در زمینه افزایش دسترسی کاربران به اینترنت و فراهم آوردن زیرساخت‌های فنی و تکنولوژی و چه در زمینه وضع قوانین و مقررات آسان‌کننده‌ی تجارت الکترونیکی صورت گرفته، حجم تجارت الکترونیکی در ایران به شدت در حال افزایش است و در حال حاضر تعداد بسیار زیادی از فروشگاه‌های اینترنتی وجود دارند که فروش کالا و خدمات دهی آنها به صورت برخط است. بنابراین، تجارت الکترونیکی چه از نظر بهره‌مندان از این روش و چه از نظر تنوع فعالیت‌ها در حال گسترش بوده است و در حالی که مبادلات الکترونیکی تا چندی قبل به تعداد معینی از شرکت‌ها محدود می‌شد، امروزه در حال ورود به عصر جدیدی است که در آن تعداد زیادی از اشخاص گمنام مصرف‌کننده، در شبکه حضور دارند.

افزون بر آن, محتوای این نوع مبادلات از محدوده‌ی مبادله‌ی داده‌های مربوط به سفارش دادن یا قبول سفارش، فراتر رفته و فعالیت‌های عمومی تجاری از قبیل تبلیغات, آگهی, مذاکرات, قراردادها و تسویه حساب‌ها را نیز در برگرفته است.

در کنار زیرساخت‌های فنی و بسترهای تکنولوژیکی و نیز افزایش آموزش معامله‌ی الکترونیکی، گسترش این نوع از تجارت و استقبال عمومی از آن در گرو اطمینان و اعتماد عمومی به این روش نوپیدای

معاملاتی است که بخشی از این اعتمادسازی از راه حمایت کیفری از تجارت الکترونیکی به‌ویژه حمایت از حقوق مصرف کننده و سازماندهی به تبلیغات اینترنتی، حمایت از داده پیام‌های شخصی، حمایت از حقوق مؤلف، حمایت از اسرار و علائم تجاری در بستر مبادلات الکترونیکی ایجاد می‌شود که قانون تجارت الکترونیکی، مصوب سال ۱۳۸۱ به آن توجه کرده است. چون هدف این نوشته بررسی عنوان مجرمانه‌ی "کلاه برداری رایانه ای" در بستر مبادلات الکترونیکی به عنوان بخشی از طرح کلی "جرایم تجارت الکترونیکی" است و نه بررسی حقوقی تجارت الکترونیک، بنابراین، مباحث مطرح شده بر این عنوان مجرمانه متمرکز شده و به شیوه‌ی رایج، نوشته‌های حقوق جزایی، بررسی جرم "کلاه‌برداری رایانه‌ای" در قالب ارکان سه گانه صورت می‌گیرد.

اما پیش از بررسی رکن قانونی جرم کلاه برداری رایانه ای، بیان این مطلب ضروری است که از حیث فقهی، در بین جرایم علیه اموال و مالکیت آن چه اصالت دارد، جرم سرقت است و فقهاء سایر اعمال منتهی به بردن اموال غیر- از جمله احتیال یعنی تحصیل مال با توسل به وسایل متقلبانه و فریب- را بصورت استطرادی و در حاشیه بحث از سرقت یا راهزنی و به عنوان مواردی که حد قطع در آن اجراء نمی شود مطرح کرده اند. از جمله محقق حلی در خاتمه بحث محاربه کتاب ارزشمند شرایع الاسلام، آورده است:" لا یقطع المستلب[1] و لا المختلس[2] و لا المحتال[3] علی الاموال بالتزویر و الرسائل الکاذبه بل یستعاد منه المال و یعزر و کذا

۱. مطابق آن چه شهید ثانی گفته، مختلس کسی است که مالی را به صورت مخفیانه از غیر حرز بر می دارد.

۲. مستلب نیز کسی است که بدون اسلحه کشیدن مالی را بصورت آشکار می گیرد و فرار می کند.(العاملی،۱۴۲۷ق، ج۴، ص۳۷۱)

۳. محتال کسی است که با استفاده از "حیله" و فریب مال را از متصرف می گیرد. در کتاب مبانی تکملهٔ المنهاج آمده است: وأما المستلب الذی یأخذ المال جهراً أو المختلس الذی یأخذ المال خفیةً و مع الاغفال و المحتال الذی یأخذ االمال بالتزویر والرسائل الکاذبهٔ فلیس علیهم حدّ و أنّما یعزّرون(خویی، ۱۴۲۲ ق، ج۱، ص۴۱۴)

المنبج[1] و من سقی غیره مرقدا"[2] یعنی بر مستلب، مختلس و محتال که با فریب و استفاده از نامه های دروغین اموالی را می برد حد قطع ید جاری نمی شود بلکه مال از این اشخاص پس گرفته شده و تعزیر می شوند. به همین صورت بر کسی که به دیگری بنگ خورانده یا کسی که به دیگری داروی خواب آوری داده و مال آنها را برده است، حد قطع جاری نمی شود.

با وجود این، در مورد محتال، روایت صحیحی از حلبی وجود دارد که از امام صادق(ع) سؤال کرده که: شخصی نزد دیگری آمده و گفته که فلانی مرا نزد تو فرستاده که فلان اموال را به من بدهی تا برایش ببرم و صاحب اموال نیز وی را تصدیق کرده و آن اموال را به وی داده است. پس از مدتی صاحب اموال، آن شخصی که گیرنده مال خود را پیک او معرفی کرده بود را دیده و به او می گوید که پیک تو نزد من آمد و من فلان مال را دادم برایت بیاورد، آیا نزد تو آورد؟ آن شخص با تعجب می گوید که من وی را نزد تو نفرستاده ام و کسی هم چیزی برای من نیاورده است! ... امام صادق(ع) در پاسخ به سؤال از حکم چنین عملی می فرمایند: "إن وجد علیه بینه إنه لم یرسله قطع یده"(عاملی، ۱۳۶۷، ج۱۸، ص۵۰۴) یعنی اگر دلیلی بر علیه گیرنده مال اقامه شود که آن شخص مورد ادعا گیرنده مال را نفرستاده، دست گیرنده مال قطع می شود.

روایت مذکور مورد عمل فقهاء قرار نگرفته و هر چند بعضی هم چون شیخ طوسی روایت را بر این مطلب حمل کرده اند که قطع، بخاطر افساد است و نه بخاطر سرقت(طوسی، ۱۳۹۰ق، ج۴، ص۲۴۳) و بعضی نظیر محقق اردبیلی، قطع ید در این روایت را از باب این که قطع هم یکی از انواع تعزیر است، کیفر تعزیری دانسته‌اند و نه حد محتال(اردبیلی،

۱. مطابق آن چه محقق اردبیلی گفته، منبِّج کسی است که بنگ به دیگری می خوراند تا او از حالت هوشیاری خارج شده و سپس مال او را می برد.

۲. ساقی مُرقِد نیز کسی است که داروی خواب آوری به دیگری می خوراند و سپس مال او را می برد.(اردبیلی، ۱۴۲۱ق، ج۱۳، ص۲۹۱)

۱۴۲۱ق، ج۱۳، ص۲۹۱)، لکن مشهور فقهاء، آن را قضیهٔ فی واقعه"[1] یعنی یک قضیه شخصی که در یک مورد خاص وارد شده تلقی کـرده انـد و در مواردی از این قبیل که شخصی با حیلـه و فریـب و نیرنـگ و گـول زدن صاحب مال، آن را از چنگ وی در می آورد، صـرفا حکـم بـه تعزیـر وی داده‌اند.

جواز تعزیر کسی که بدین صورت کلاه سر دیگران مـی گـذارد (کـلاه بردار!)، از این جهت است که این عمل مصـداق بـارزی از قاعـده فقهـی "أکل مال به باطل" است که در آیات ۱۸۸ سـوره بقـره و ۲۹ نسـاء مـورد نهی قرار گرفته است. در آیه ۲۹ سوره نساء آمده که: "ای اهل ایمان! مـال یکدیگر را به ناحق نخورید، مگر آن کـه تجـارتی از روی رضـا و رغبـت کرده و سودی ببرید."[2] نهی مذکور در آیه دارای دو اثر وضعی و تکلیفـی است. اثر وضعی آن در قالب فساد و بطلان چنـین معـاملاتی تجلـی پیـدا کرده که در نتیجه، چنین عملی، سبب مملک به شمار نیامده و گیرنده مال باید آن را به مالک واقعی آن مسترد نماید. اما اثـر تکلیفـی ایـن نهـی، در قالب حرمت چنین عملی نمایان می شود و در نتیجـه، ایـن عمـل حـرام، مشمول قاعده کلی "التعزیر لکل عمل محرم" است که طبق نظـر مشـهور فقهای امامیه[3] ـ و بلکه نظر مشهور فقهای اهل سنت[4] ـ، حـاکم مـی توانـد

۱. " **والاولی حمله علی قضیة فی واقعه اقتضت المصلحة فیها ذلک**" (نجفی، ۱۳۷٤، ج ٤۱، ص۵۹۸)

۲. **(یا أیها الذین آمنوا لا تأکلوا أموالکم بینکم بالباطل إلا أن تکون تجارة عن تراض منکم)**

۳. "**من فعل محرما أو ترک واجبا إلهیا عالما عامدا عزره الحاکم حسب ما یراه من المصلحة، علی المشـهور شهرة عظیمة، بل بلا خلاف فی الجملـة**"(خـویی، ۱۴۲۲ ق، ج۱، ص۴۰۷) البتـه معـدودی از فقهـا اعمـال تعزیر را منوط به کبیره بودن گناه کرده اند کما این که صاحب جواهر می فرماید: "**لا خلاف و لا إشـکال نصا و فتوی فی أن کل من فعل محرمـا أو تـرک واجبـا و کـان مـن الکبـائر فللإمـام تعزیـره بمـا لا یبلـغ الحد**"(نجفی، ۱۳۷۴، ج ۴۱، ص۴۴۸) و بعضی فقها نیز اعمال تعزیر را مشروط به عدم ترک بـا وعـظ و توبیخ و تهدید دانسته اند: "**ثم وجوب التعزیر فی کل محرم من فعل أو ترک إن لم ینته بالنهی و التـوبیخ و نحوهما فهو ظاهر، لوجوب إنکار المنکر. و أما إن انتهی بما دون الضرب فـلا دلیـل علیـه إلا فـی مواضـع مخصوصة ورد النص فیها بالتأدیب أو التعزیر**" (اصـفهانی،۱۴۱۶ه.ق.، ج۱۰، ص۵۴۳) لکـن نظـر مشـهور فقها، امکان تعزیر مرتکب معصیت بطور مطلق است.

۴. **مِن المتّفَق علیهِ أنّ التعزیرَ یکونُ فی کلّ معصیه** (عوده، ۱٤۰۵ه.ق.، ج۱، ص۱۲۸)

مرتکب عمل حرام را مطابق آنچه مصلحت می بیند تعزیر نماید. از سوی دیگر برابر اصل ۱۶۷ قانون اساسی و نیز ماده ۲۱۴ قانون ایین دادرسی کیفری ۱۳۷۸ و قوانین دیگر، در صورتی که در مورد خاصی عملی شرعا حرام بوده لکن قانون موضوعه در خصوص آن عمل وجود نداشته باشد، قاضی باید با مراجعه به منابع معتبر فقهی و فتاوای مشهور حکم قضیه را صادر نماید و نمی تواند به بهانه سکوت قانون از رسیدگی و صدور حکم امتناع نماید. با توجه به این موضوع، بدیهی است قوه مقننه به عنوان بازوی تقنینی حاکم اسلامی می تواند اعمال حرام شرعی را در قانون موضوعه جرم انگاری نموده و برای آن تعیین کیفر نماید که احتیال و تحصیل مال با توسل به حیله و فریب صرف نظر از نوع وسیله و نحوه تحقق فریب، یکی از مصادیق بارز این بحث به شمار می آید.

هم چنین از حیث فقهی، تشهیر محتال(یعنی مشهور کردن و شناساندن مجرم به مردم) نیز امکان دارد. فقهایی نظیر شیخ مفید(عکبری بغدادی،۱۴۱۳ق، ص۸۰۵)، شیخ طوسی(طوسی، ۱۴۰۰ق، ج۳، ص۳۳۵)، ابن ادریس(حلی،۱۴۱۱ق، ج۳، ص۵۱۲)، ابن حمزه(طوسی، ۱۴۰۸ق، ص ۴۳۳)، علامه حلی(حلی، ۱۴۲۲ق، ج۵، ص۳۸۴) و بسیاری دیگر از فقهاء از "شهر المحتال" یعنی شناسایی محتال به مردم سخن گفته اند. از جمله شیخ الطائفه (شیخ طوسی)، تشهیر عقوبت محتال را موجب بازدارندگی عمومی دانسته است: "و ینبغی للسلطان أن یشهره بالعقوبة لکی یرتدع غیره عن فعل مثله فی مستقبل الاوقات"(طوسی، ۱۴۰۰ق، ج۳، ص۳۳۵) یعنی شایسته است حاکم، مجازات محتال را آشکارا اجراء کند تا دیگران در آینده از انجام چنین اعمالی پرهیز نمایند.

استفاده از تشهیر اعم از این که در قالب تشهیر عقوبت یعنی اجرای علنی مجازات باشد یا تشهیر به عنوان کیفری مستقل، در جرایمی نظیر کلاه برداری مفید و مؤثر خواهد بود، بویژه در مواردی که مرتکبین این جرایم با استفاده از موقعیت اجتماعی، جایگاه شغلی، قدرت و نفوذ اداری خود و اطرافیانش و نیز با استفاده از قدرت تفکر و برنامه ریزی قادرند

مدت ها چهـره واقعـی خـود را مخفـی نگـاه داشـته و بـا حفـظ شـأن و شخصیت اجتماعی خود به بلعیدن اموال مردم بپردازند. افزون بـر ایـن در جرایم مالی رایانه ای و بویژه در جرایم تجارت الکترونیکی از جمله کـلاه برداری در بستر معاملات اینترنتی، که تبهکاران با سوء استفاده از دانـش و مهارت کار با رایانه و اینترنت و ورود به فضای مجازی که ناشناخته ماندن ویژگی بارز این فضا است اقدام به تحصیل اموال نامشـروع و بـردن مـال دیگران می نمایند، تشهیر ـ بویژه تشهیر رسانه ای که هم سنخ و مناسب با فضای مورد بحث است ـ ، اقدامی موثر در پیشگیری از این گونـه جـرایم خواهد بود چرا که در مورد این گروه از مجرمین، آن مجازاتی که بـیش از بقیه کیفرها تهدیدکننده و بازدارنده است، شناخته شدن هویت واقعی آنان برای جامعه و مردم است.

مبحث اول: رکن قانونی

از حیث حقوق موضوعه، اولین متن قـانونی کـه در ایـران، بـه جـرایم رایانه‌ای توجه کرد، قانون مجازات جرایم نیروهای مسلح، مصـوب ۱۰/۹/ ۱۳۸۲ بود. در ماده‌ی ۱۳۱ این قانون آمده است: "هرگونه تغییر یـا حـذف اطلاعات، الحاق، تقدیم یا تأخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن که به طور غیرمجاز توسط نظامیان در سیستم رایانه و نرم افزارهای مربوط صورت گیرد و همچنین اقداماتی از قبیـل تسـلیم اطلاعـات طبقـه بنـدی شده‌ی رایانه‌ای به دشمن یا افرادی که صلاحیت دسترسی به آن اطلاعات را ندارند، افشاء غیرمجاز اطلاعات، سرقت اشـیاء دارای ارزش اطلاعـاتی مانند سی دی یا دیسکت‌های حاوی اطلاعات یا معدوم کردن آنها یا سوء استفاده های مالی که نظامیـان بـه وسـیله‌ی رایانـه مرتکـب شـوند، جـرم محسوب و حسب مورد مشمول مجازات‌های مندرج در مـواد مربـوط بـه این قانون می‌باشند." هر چند ماده‌ی ۳۱ انواع مصادیق جرایم رایانـه‌ای را از هم جدا نکرده، با این حال "تغییر یا حذف اطلاعات، الحاق، تقـدیم یـا

تاخیر تاریخ نسبت به تاریخ حقیقی و نظایر آن" به جعل رایانه‌ای و "سوء استفاده‌های مالی" به کلاه‌برداری رایانه‌ای اشاره دارد.

افزون بر این، قانون تجارت الکترونیکی، مصوب سال ۱۳۸۱ و قانون جرایم رایانه‌ای، مصوب سال ۱۳۸۸ نیز به‌طور مشخص درباره‌ی جرم کلاه برداری رایانه‌ای حکم داده که در ادامه به طور کامل بررسی خواهد شد.

با این توضیح، مبنای قانونی جرم کلاه‌برداری در بستر تجارت الکترونیک، ماده‌ی ۶۷ قانون تجارت الکترونیکی، مصوب ۱۳۸۱/۲/۲۹ مجلس شورای اسلامی است که ذیل عنوان کلاه برداری کامپیوتری آمده است: "هرکس در بستر مبادلات الکترونیکی، با سوء استفاده و یا استفاده‌ی غیر مجاز از «داده‌پیام»ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف «داده‌پیام»، مداخله درعملکرد 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 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."

متن قانونی دیگر مرتبط با این موضوع، ماده‌ی ۱۳ قانون جرایم رایانه‌ای، مصوب ۱۳۸۸/۳/۵ مجلس شورای اسلامی است که به موجب آن: "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 مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه بر رد مال به صاحب آن، به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هر دو مجازات محکوم خواهد شد."

درباره‌ی رابطه‌ی این دو ماده باید به این مطلب توجه داشت که هر

چنـد از حیـث زمـانی، قـانون جـرایم رایانـه‌ای پـس از قـانون تجـارت الکترونیکی تصویب شده است، لکن چون قانون جـرایم رایانـه‌ای از نظـر بستر انجام جرم، عام است و قـانون تجـارت الکترونیکـی از ایـن جهـت خاص است، بنابراین، حکم عام پسین، ناسخ خاص پیشین نخواهـد بـود؛ فلذا در صورتی که کلاه برداری و نیز جعـل رایانـه‌ای در بسـتر مبـادلات الکترونیکی صورت گیرد، در موارد تعارض بین دو قانون، قـانون تجـارت الکترونیکی درباره‌ی عمل انجام شده حکم خواهد کرد.

جهت مقایسه‌ی قوانین داخلی مربوط به کلاه‌برداری رایانه‌ای بـا اسـناد بین‌المللی ـ که به نوعی تعریف جرم کلاه‌برداری رایانه‌ای[1] هـم محسـوب می‌شود ـ اشاره به ماده‌ی ۸ کنوانسـیون جـرایم سـایبری شـورای اروپـا، مصوب ۲۳ نوامبر ۲۰۰۱ بوداپست، ضروری به نظر می‌رسد. در ایـن مـاده ذیل عنوان "کلاه‌برداری مرتبط با رایانه" آمده است: "هر یک از اعضا باید به گونه‌ای قوانین و مقررات وضع کنـد کـه در صـورت لـزوم بـر اسـاس حقوق داخلی خود، هرگونه اقدامات عمدی و غیرحق را که به قصد فریب یا دیگر مقاصد ناروا و در جهت جلب منفعت اقتصـادی غیـر حـق بـرای خود یا دیگری صورت می‌پذیرد، جـرم‌انگـاری نمایـد کـه ایـن اقـدامات غیرحق هرگونه وارد کردن، تغییـر، حـذف یـا قطـع داده‌هـای رایانـه‌ای و هرگونه ایجاد اختلال در عملکرد یک سیستم رایانه‌ای را در برمی‌گیرد."

هم چنین در توصـیه نامـه‌ی شـماره‌ی ۹ (۸۹) R سـال ۱۹۸۹کمیتـه‌ی وزرای شورای اروپا فهرسـتی اجبـاری و فهرسـتی اختیـاری بـرای جـرم انگاری جرایم رایانـه‌ای بـه نماینـدگان کشـورها داده اسـت کـه دو جـرم کلاه‌برداری رایانه‌ای و جعل رایانه‌ای به عنوان نخستین مصـادیق فهرسـت حداقل (اجباری) ذکر شده است. در این فهرست، در تعریف کلاه‌بـرداری

۱. بعضی محققان، اصطلاح کلاه برداری اطلاعاتی (احتیال المعلوماتی – Informatics Fraud) را بـه جای کلاه برداری رایانه‌ای به کار بـرده و آن را "هرگونـه رفتـار متقلبانـه مـرتبط بـا عملیـات پـردازش الکترونیکی و به قصد تحصیل نفع یا امتیاز مالی" دانسـته انـد.(صـالح: ۲۰۰۰ م، ص۷) در حـالی کـه از جهت دامنه موضوع، نوع رفتار و قصد مجرمانه تطابق کامل بین دو اصطلاح وجود ندارد.

رایانه‌ای آمده است:" کلاه‌برداری رایانه‌ای عبارت است از وارد کردن، تغییر، محو، یا متوقف ساختن داده‌ها یا برنامه‌های رایانه‌ای یا دیگر گونه‌های ایجاد اختلال در جریان پردازش داده‌ها که در نتیجه‌ی آن، ضرر اقتصادی به اموال یا لطمه به حقوق مالکانه دیگری وارد شود، به قصد کسب منفعت اقتصادی غیرقانونی برای خود یا دیگری."

مبحث دوم: رکن مادی

اجزای رکن مادی کلاه برداری رایانه‌ای به شرح زیر بررسی می‌شود:

مرتکب جرم: قانون‌گذار تجارت الکترونیکی در ماده‌ی ۶۷ درباره‌ی مرتکب جرم به "هرکس" اشاره کرده که از نظر عرف حقوقی در شخص حقیقی ظهور دارد و هرچند برابر ماده‌ی ۵ تصویب نامه‌ی تاریخ ۱۳۸۴/۴/۵ هیأت وزیران درباره‌ی برنامه‌ی جامع توسعه‌ی تجارت الکترونیکی، "وزارت دادگستری مکلف است با همکاری قوه‌ی قضائیه، بانک مرکزی و وزارت بازرگانی نسبت به تدوین حقوق جزای ماهوی، شامل به رسمیت شناختن مسئولیت کیفری اشخاص حقوقی در محیط تجارت الکترونیکی و... تا پایان اسفندماه ۱۳۸۵ اقدام کند"، و حتی "تدوین قانون مسئولیت کیفری برای اشخاص حقیقی ـ حقوقی تا پایان شهریور ۱۳۸۵ "[1] در بند سوم ماده‌ی ۲ تصویب نامه مذکور جزء وظایف وزارت دادگستری دانسته شده، لیکن این توصیه‌ها هنوز در قلمرو تجارت الکترونیکی کاربردی نشده و برداشت‌های حقوقی منحصر به متن ماده‌ی ۶۷ قانون تجارت الکترونیکی است و همان‌گونه که گفته شد، مجرم از نظر این ماده، فقط اشخاص حقیقی است.

با وجود این، در قلمرو قانون جرایم رایانه‌ای، اشخاص حقوقی نیز دارای مسئولیت کیفری شناخته شده اند. برابر ماده‌ی ۱۹ این قانون، در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای

۱. روزنامه‌ی رسمی، شماره‌ی ۱۷۶۲۰– ۱۳۸٤/٦/۲.

منافع آن صورت گیرد، شخص حقوقی مسؤولیت کیفری خواهد داشت: " الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود. ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد. ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود. د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد."

نوع واکنش‌های قابل اعمال علیه اشخاص حقوقی نیز در ماده‌ی ۲۰ این قانون این‌گونه بیان شده: "اشخاص حقوقی موضوع ماده‌ی فوق، با توجه به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد: الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم، شخص حقوقی منحل خواهد شد."

به نظر نگارنده، با توجه به عام بودن قانون جرایم رایانه‌ای که وقوع جرم در بستر مبادلات الکترونیکی را هم در بر می‌گیرد، از یک سوی و نیز عدم تعارض بین قانون جرایم رایانه‌ای و قانون تجارت الکترونکی درباره‌ی مسئولیت کیفری اشخاص حقوقی ـ به سبب ذکر نشدن مسئولیت این اشخاص در این قانون ـ از سوی دیگر، در صورت ارتکاب کلاه برداری رایانه‌ای در بستر تجارت الکترونیکی توسط اشخاص حقوقی، می‌توان با استناد به قانون جرایم رایانه‌ای، این اشخاص را از لحاظ کیفری، مسئول شناخته و مجازات‌های بیان شده در این قانون را درباره‌ی آنان به کار برد.

موضوع جرم: قانون‌گذار در ماده‌ی ۶۷ ق.ت.ا. چهار مورد "داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور" را موضوع این جرم دانسته که سوء استفاده یا استفاده‌ی غیرمجاز از آن، رفتار مورد نظر مقنن را تشکیل می‌دهد.

داده پیام: این اصطلاح در قانون تعریف شده و برابر بند (الف) ماده‌ی ۲ قانون تجارت الکترونیکی، «داده‌پیام"[1]، هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسائل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات تولید،ارسال، دریافت، ذخیره یا پردازش می‌شود." این تعریف برگرفته از بند (ب) ماده‌ی ۲ کنوانسیون جرایم سایبری است که مطابق آن، "منظور از «داده رایانه‌ای» هرگونه نمایش حقایق، اطلاعات یا مفاهیم به شکلی مناسب است که برای پردازش در یک سیستم رایانه‌ای، که شامل برنامه‌ای مناسب است و باعث می‌شود که این سیستم عملکرد خود را به مرحله‌ی اجرا گذارد، مورد استفاده قرار می‌گیرد."

سیستم رایانه‌ای: این اصطلاح نیز در قانون تعریف شده و برابر بند (و) ماده‌ی ۲ قانون تجارت الکترونیکی، سیستم رایانه‌ای[2] "هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری ـ نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار «داده‌پیام» عمل می‌کند" این تعریف نیز برگرفته از بند (الف) ماده‌ی ۲ کنوانسیون جرایم سایبری است که به موجب آن، "منظور از «سیستم رایانه‌ای» هرگونه ابزار یا مجموعه‌ای از ابزارهای مرتبط و متصل به هم است که مطابق با یک برنامه، پردازش خودکار داده‌ها را انجام می‌دهد."

وسایل ارتباط از راه دور: این اصطلاح هم در قانون تعریف شده و برابر بند (ف) ماده‌ی ۲ قانون تجارت الکترونیکی، وسایل ارتباط از راه دور[3] عبارت از هر نوع وسیله‌ای است که بدون حضور فیزیکی هم‌زمان

1 . Data Message.
2 . Computer System..
3 . Means Of Distance Communication.

تأمین کننده و مصرف کننده جهت فروش کالا و خدمات استفاده می‌شود.

رفتار مادی: با نگاهی به ماده‌ی ٦٧ ق.ت.ا. که در ابتدای مقاله بیان شد، رفتار مادی این جرم از دو جزء "سوء استفاده یا استفاده‌ی غیرمجاز از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور" و "فریب اشخاص یا گمراه کردن سیستم‌های پردازش خودکار" برای رسیدن به نتیجه‌ی مورد نظر تشکیل شده است.

الف) سوء استفاده یا استفاده‌ی غیرمجاز از داده‌پیام، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور:

دو اصطلاح سوء استفاده و استفاده‌ی غیرمجاز از نظر مفهوم بسیار نزدیک به هم و ماهیتی یکسان دارند، به گونه‌ای که استفاده‌ی غیر مجاز، خود نوعی سوء استفاده است و از این رو برخی این دو واژه را به یک معنا دانسته و علت ذکر این دو واژه در متن قانون را ناشی از جرح و تعدیل بدون دقت قانونی در متون پیشنهادی دانسته اند (جاویدنیا: ۱۳۸۷، ص۲۲۸) و برخی دیگر نیز اصطلاح "استفاده‌ی بدون حق" را به جای دو اصطلاح مورد بحث پیشنهاد کرده‌اند (خرم آبادی: ۱۳۸۴، ص۲۲۶) با وجود این، می‌توان فرض کرد که فرد اجازه‌ی دسترسی و حتی استفاده از داده پیام‌ها، برنامه‌ها و سیستم رایانه‌ای را دارد لکن با سوء استفاده از اعتماد اجازه دهنده و با نقض عنصر امانت داری، از این موضوع سوء استفاده کرده و از این راه را به دست می‌آورد.

به هر حال، استفاده‌ی غیرقانونی از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور به صورت‌های مختلفی صورت می‌پذیرد و قانون‌گذار خود در ماده‌ی ۶۷ راه‌ها و مصادیق استفاده‌ی غیرقانونی را بیان کرده است، به گونه‌ای که عبارت "و ارتکاب افعالی نظیر ورود، محو، توقف داده‌پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره" بیان شده در این ماده، در واقع، تبیین و تفسیر "استفاده‌ی غیرقانونی" است و مصادیق این کار را بینان کرده است:

وارد کردن داده‌پیام: داده‌پیام وارد شده ممکن است راست باشد یا دروغ و ممکن است به داده‌پیام‌های موجود اضافه شود یا اینکه خود یک داده‌پیام جدید و کامل را سازد. کلاه‌برداری از راه وارد کردن[1]، مثل افزودن نام و مشخصات و داده‌پیام‌های تأکید کننده‌ی شرایط استحقاق متقاضی به قسمت تسهیلات بانک برای دریافت وام قرض الحسنه و یا افزودن نام یک کارگر یا کارمند واهی به لیست پرداخت حقوق شرکت یا اداره با شماره حساب خود متصدی سیستم برای دریافت مبلغ حقوق. این قانون (ورود داده‌های غیر صحیح و ورود غیرمجاز داده‌های صحیح) نه تنها سوء استفاده از چک‌های مسروقه و کارت‌های اعتباری در یک بانک اتوماتیک را شامل می‌شود، بلکه سوء استفاده از کارت شخصی و تجاوز از حدود اعتباری را نیز در بر می‌گیرد. (دزیانی: ۱۳۸۱، ص۷۵) در پژوهشی که دیوید کارتر، استاد دانشگاه میشیگان انجام داده، شایع‌ترین جرمی که در سال‌های اخیر در فضای سایبر گزارش شده، کلاه برداری با استفاده از کارت اعتباری[2] بود. سیستم‌کارتِ پرداختِ الکترونیکی، با عملیات انتقال الکترونیکی از حساب کارت مشتری بانکِ صادرکننده‌ی کارت به حساب بانکی فروشنده صورت می‌گیرد و بانکی آن را انجام می‌دهد که حساب فروشنده در آن قرار دارد و شبکه‌ی باز، پرداخت الکترونیکی گروه‌های بین‌المللی (مانند گروه ویزا کارت و گروه ماسترکارت) صورت می‌گیرد. کارت پرداخت الکترونیکی این حق را به مشتری می‌دهد که از راه شبکه‌ی اینترنت و اعلان کتبی یا تلفنی و با کم‌کردن قیمت از حساب کارت پرداخت الکترونیکی مخصوص به او به کالاها و خدماتی دست یابد و این کار، سفارش‌ای میلی تلفنی[3] نامیده می‌شود. برای اجرای این عملیات، کافی است مشتری به پایگاه الکترونیکی فروشنده در شبکه اطلاعاتی وارد شود و کالایی که قصد خرید آن را دارد انتخاب کند و عملیات خرید و فروش پس از پرکردن نمونه‌ی الکترونیکی ـ که بر صفحه‌ی رایانه ظاهر

1. Enter.
2. Credit Card Fraud
3. Mail Phone order

می‌شود ـ با اطلاعات‌کارت اعتباری مخصوص مشتری و آدرس او صورت می‌گیرد. پس از آن، فروشگاه قیمت کالا را از کارت پرداخت الکترونیکی کم می‌کند و آن را به آدرس مشتری ارسال می‌دارد. (شوابکه: ۲۰۰۹، ص۱۹۳) در واقع، انقلاب دیجیتال به دزدان اطلاعاتی، امکان جعل شماره‌ی کارت‌های اعتباری را به کمک برنامه‌هایی داده است که شماره کارت‌های بانک معینی را با افزودن عدد خاص بانکِ صادر کننده‌ی کارت به رایانه، جعل کند. افزودن بر آن به این کار امکان دریافت این شماره‌ها از راه شبکه‌های بازِ اینترنت و به‌کارگیری آن به شیوه‌ای غیرقانونی در عملیات خرید از شبکه را ایجاد می‌کند، به گونه‌ای که قیمت‌کالا از مشتریان قانونی این کارت‌ها کم می‌شود.(صغیر: ۱۹۹۹، ص۳۷) همچنین کلاه‌برداری کارت‌های اعتباری به این علت وسوسه انگیز است که هکرها در زمان کوتاهی تنها با یک تلفن، رایانه و مودم و وصل شدن به شبکه بدون نیاز به مهارت خاصی از کارت‌های اعتباری سوء استفاده می‌کنند.(باستانی: ۱۳۸۶، ص۶۹)

به سبب رواج و اهمیت کلاه‌برداری از راه کارت‌های اعتباری، توضیح بیشتر در این باره مفید خواهد بود. به طور کلی کلاه‌برداری با این روش یا زمانی است که صاحب قانون کارت آن را به کار می‌گیرد یا دیگری از آن استفاده می‌کند چون حالت دوم (استفاده دیگری از اطلاعات کارت) بیشتر در قالب سرقت اطلاعات و جعل صورت می‌پذیرد، در این نوشته تنها حالت استفاده‌ی صاحب قانونی کارت از اطلاعات کارت اعتباری در دو فرض سوء استفاده از اطلاعات کارت در زمان مدت اعتبار آن و یا به کارگیری اطلاعات کارت اعتباری پس از پایان مدت اعتبار یا بی‌اعتبار شدن آن (لغو اعتبار)، به شرح زیر بررسی می‌شود:

حالت اول: سوء استفاده از اطلاعات کارت اعتباری در زمان اعتبار آن:

سوء استفاده‌ی صاحب کارت از اطلاعات کارت پرداخت الکترونیکی

در شبکه‌ی اینترنت و از راه پرداخت قیمت کالا و خدماتی که در شبکه اینترنت تبلیغ می‌شود و با پرکردن فرم خرید الکترونیکی صورت می‌گیرد، با صاحب حساب می‌داند حساب بانکی او برای آنکه این مبالغ، کافی نیست. یا اینکه شخص به نقل و انتقال الکترونیکی از حساب بانکی دیگری بپردازد در حالی‌که از حساب بانکی خود در بانک صادر کننده‌ی کارت تجاوز کرده است. رویکرد قانون فرانسه در چگونگی جرم انگاری این فعل، متغیر و در نوسان است؛ برخی قوانین، این کار را سرقت دانسته‌اند در حالی‌که برخی قوانین دیگر این فعل را از نوع راه‌های متقلبانه بر می‌شمرند که نوعی کلاه برداری است.

دادگاه استیناف انگرز در حکمی که در این باره صادر کرده، بر خلاف تمام این قوانین، حکم کرده و می‌گوید: تصرف صاحب کارت در مبالغی بیش از حساب بانکی وی با قرار دادن کارت در یکی از دستگاه‌های توزیع خودکار، هیچ گونه جرم کیفری ایجاد نمی‌کند و دادگاه تجدید نظر فرانسه نیز این حکم را در سال ۱۹۸۲ تأیید کرد و در توضیح حکم خود آورده است: "با توجه به اینکه دادگاه استیناف، برای حکم به برائت متهم اثبات کرده است که برای آنکه متهم بتواند برداشت غیر قانونی داشته باشد ـ مطابق با قواعد فنی استفاده از دستگاه ـ از کارت به عنوان صاحب آن استفاده کرده و دادگاه استیناف با توجه به این امر، حکم خود را توجیه کرده است، در حقیقت وقایع نسبت داده شده به متهم، با بی‌توجهی به تعهدات قرارداد بیان شده و در ذیل هیچ قانون کیفری در نمی‌آید. (شوابکه: ۲۰۰۹، ص۱۹۵)

موضع حقوق‌دانان در باره‌ی انطباق این وضعیت، مختلف است، لکن بیشتر حقوق‌دانان با استناد به این مطلب که بانک دستگاه را برنامه ریزی است و اوست که به مشتری اجازه‌ی برداشتن و یا برنداشتن می‌دهد، با تقلب دانستن فعل صاحب‌کارت که از حساب بانکی خود تجاوز کرده، مخالفند. به اعتقاد ایشان، هنگامی که دستگاه اجازه‌ی پرداخت و تحویل پول را بدهد پس راه‌های متقلبانه برای وادار کردن دستگاه به پرداخت پول

فراهم نمی‌شود و چه بسا مشتری از راه‌های همیشگی برای استفاده از کارت بانکی پیروی کرده و از راه‌های متقلبانه برای قانع ساختن دستگاه به وجود اعتماد نادرست، استفاده نکرده است. این گروه همچنین گذاشتن تام وصف سرقت بر این کار را نیز انکار می‌کنند، زیرا سخت است که بگوئیم، صاحب کارت مبالغی را که از راه کارت خود و بدون رضایت بانک به دست آورده، دزدیده است. این سخن با برنامه‌ی الکترونیکی این دستگاه‌ها سازگار نیست، زیرا این برنامه به هر درخواست مطابق با سیستم از پیش تعیین شده‌ی بانک پاسخ می‌دهد. پس تحویل پول با رضایت بانک بوده و برخلاف آن نیست و تحویل مقدار بیشتر پول به سبب اشتباه صورت گرفته است و بانک حق دارد از مشتری بخواهد تا آنچه را بیش از حساب بانکی خود برداشته، باز پس دهد. همان‌گونه که این حقوق‌دانان دادن عنوان خیانت در امانت را بر این فعل نیز انکار می‌کنند، زیرا هر چند کارت به با توجه به عقد، ملک مقام صادر کننده‌ی آن است و او می‌تواند اعتبار کارت را از بین می‌رود و هر زمان بخواهد آن را باز پس گیرد ـ و در این حالت، مشتری می‌باید کارت را به بانک پس دهد و الا جرم خیانت در امانت مرتکب می‌شود ـ اما جز زمانی‌که تصرف و تسلط صاحب کارت بر مبالغ، در نتیجه‌ی استفاده از کارت در زمان اعتبار آن، صورت گیرد؛ اگرچه مخالفت با شروط عقد، به تعهدات قرارداد آسیب می‌رساند. (سامی الشوا: ۱۹۹۸، ص ۱۰۸)

حالت دوم: سوء استفاده از اطلاعات کارت اعتباری پس از پایان مدت اعتبار آن یا بی‌اعتبار شدن آن در زمان تعهد و التزام:

فرض اول: استفاده‌ی غیر قانونی از کارت اعتبار:

بعضی از بانک‌های صادرکننده‌ی کارت، کارت را در زمان مدت اعتبارش برای کیفر سوء استفاده‌ی مشتری از کارت، بی‌اعتبار می‌کنند. هنگامی که بانک کارت را بی‌اعتبارکرد و به مشتری در این باره اخطار داده شد، باید وی کارت را به بانک صادرکننده بازگرداند. اما گاه مشتری از

بازگرداندن کارت به بانک صادرکننده‌ی آن سرباز می‌زند و همچنان از اطلاعات آن استفاده می‌کند. این امر منجر به الزام بانک به تعهد و التزام این مبالغ برای فروشنده می‌شود. در بسیاری از موارد فروشنده از لغو اعتبار کارت آگاه نیست لذا شایسته است بانک لیستی از کارت‌های بی‌اعتبار را در اختیار فروشگاه‌ها قرار دهد. در این فرض، درباره‌ی وصف مجرمانه‌ی فعل به کارگیری اطلاعات‌کارت بی‌اعتبار با آگاهی صاحب‌کارت به این امر در تعهد و التزام سؤال مطرح می‌شود. در تحلیل حقوقی برای پاسخ به این سؤال میان دو حالت فرق می‌گذاریم:

صورت اول: خودداری صاحب کارت از بازگرداندن کارت، پس از خواستن بانک: چون ارتباط میان مشتری و بانک صادرکننده‌ی کارت اعتباری، ارتباطی قراردادی است و کارت اعتباری به موجب این ارتباط، ملک صادر کننده‌ی آن (بانک) باقی می‌ماند و این حق، حق استفاده‌ی مشتری از کارت را به هنگام خواستن، بانک به او واگذار می‌کند و این امر مبتنی بر عقد "عاریه‌ی استعمال" ـ یکی از عقود امانی[1] ـ است، استفاده‌ی مشتری از کارت اعتباری، پس از اینکه بی‌اعتبار شدن کارت به او اعلام شد و خودداری او از بازگرداندن کارت، فعل "تصاحب" شکل می‌گیرد که به سبب آن جرم خیانت در امانت[2] پیش می‌آید و برای وقوع تصاحب کافی است که صاحب کارت، بودن کارت در دست خود را انکار کند و استفاده‌ی از کارت با وجود خواستن بانک، شرط فعل نیست.

صورت دوم: استفاده‌ی صاحب کارت لغو اعتبار شده برای انجام تعهد در قبال فروشنده:

---

۱. بدین معنا که بانک عین کارت رابه مشتری قرض داده که از آن رایگان استفاده کند و مشتری بر عین کارت ملکیتی ندارد. برابر ماده‌ی ۶۵۳ قانون مدنی"عاریه عقدی است که به موجب آن احد طرفین به طرف دیگر اجازه می دهد که از عین مال او مجاناً منتفع شود."

۲. برابر ماده‌ی ۶۷۴ قانون مجازات اسلامی: "هرگاه اموال منقول یا غیر منقول یا نوشته‌هایی از قبیل سفته وچک و قبض و نظایر آن به عنوان اجاره یا امانت یا رهن یا برای وکالت یا هر کار با اجرت یا بی اجرت به کسی داده شده و بنا براین بوده است که اشیاء مذکور مسترد شود یا به مصرف معینی برسد و شخصی که آن اشیاء نزد او بوده آنها را به ضرر مالکین یا متصرفین آنها استعمال یا تصاحب یا تلف یا مفقود نماید، به حبس از شش ماه تا سه سال محکوم خواهد شد."

استفاده‌ی صاحب کارت پرداخت الکترونیکی بی‌اعتبار شده برای انجام تعهد در برابر فروشندگان از طریق خرید الکترونیکی، کلاهبرداری است. زیرا پرکردن این اطلاعات در برگه‌ی الکترونیکی خرید، به هدف اقناع دیگری به وجود اطمینان غیرواقعی صورت می‌گیرد و صرف گفتن یک دروغ نیست، خصوصا باید توجه داشت که لغو اعتبار کارت، از ارزش آن به عنوان وسیله‌ی اعتباری نیز می‌کاهد. افزون بر این، عنصر"تحویل" نیز در تحویل اجناس خریداری شده از فروشنده به صاحب قانونی کارت یا قبول فروشنده به استفاده از خدمات او دیده می‌شود. با وجود این، برخی اعتقاد دارند که استفاده‌ی صاحب قانونی از کارت بی‌اعتبار در برداشت پول‌ها و انجام نقل و انتقال الکترونیکی اوراق بهادار جرمی را شکل نمی‌دهد، زیرا فرض بر این است که دستگاه‌های برداشت الکترونیکی که به طور مستقیم با حساب‌های مشتریان در بانک، ارتباط دارند، اجرای هر تحویل یا تسلیم پول را که صاحب کارت آن را می‌خواهد، اگر بیش از حساب بانکی او باشد، رد می‌مایند و نمی‌پذیرند. (صغیر: ۱۹۹۹، ص۸۲)

فرض دوم: استفاده از کارت‌هایی که اعتبار آن به پایان رسیده:

کارت اعتباری برای مدتی معین و تا تاریخ مشخصی به مشتری تحویل داده می‌شود و هنگامی که تاریخ اعتبار آن به پایان رسید، مشتری باید آن را به بانک صادر کننده‌ی آن بازگرداند. اما گاه مشتری از بازگرداندن کارت به بانک صادر کننده‌ی آن سرباز می‌زند و همچنان از آن استفاده می‌کند و این‌جاست که درباره‌ی انطباق قانونی این فعل سؤال مطرح می‌شود. بعضی از حقوق‌دانان اعتقاد دارند که صاحب قانونی کارت، اگر برای فروشنده به وسیله‌ی کارت پرداختی که اعتبار آن به پایان رسیده، تعهد و التزامی ایجاد کند، جرم تقلب را مرتکب نشده است. زیرا دروغ صادر شده از صاحب کارت به میزان اعتبار کارت تعلق می‌گیرد نه بر اقناع فرد دیگری به وجود اطمینانی غیر واقعی. و فروشنده‌ای که طرف تعهدات قرارداد است می‌تواند به آسانی و با آگاه شدن از تاریخ اعتبارکارت که به صورت آشکار و روشن بر روی کارت نوشته شده است از میزان اعتبار کارت

باخبر شود. بنابراین مسئولیت در این جا بر عهده فروشنده است و او باید به تنهایی ضرر را تحمل کند، زیرا تعهد و التزام را در هنگام به کارگیری اطلاعات کارت بدون اعتبار پذیرفته است و به یکی از تعهدات قرارداد خود مانند جستجو از تاریخ اعتبار کارت آسیب وارد کرده است.(صغیر: ۱۹۹۹، ص۸۵)

از نظر نگارنده، این دیدگاه پذیرفته نبوده و تفاوتی بین این فرض و حالتی که بانک اعتبار کارت را لغو کرده و صاحب کارت دوباره از آن استفاده می‌کند، وجود ندارد، زیرا در این مورد نیز درج تاریخ انقضاء بر روی کارت بیان‌گر آن است که نوعی توافق ضمنی بین بانک و مشتری بر بازگرداندن کارت غیرمعتبر برای تعویض یا تمدید آن وجود دارد و استفاده‌ی صاحب کارت از آن، پس از انقضاء این مدت، به کار بردن وسیله تقلبی و فریفتن دیگران با امیدوارکردن به امور غیر واقعی است.

محو کردن داده‌پیام: محو به معنای حذف[1] و از بین بردن اطلاعات و داده‌ها است. مثل اینکه کارمندی با حذف سابقه‌ی دریافت حقوق خود از سیستم حسابداری شرکت، دوباره از شرکت حقوق بگیرد. (قوه قضائیه: ۱۳۸۳، ص۵۰)

متوقف کردن داده‌پیام: کلاه برداری از راه متوقف کردن داده پیام غالباً در مراحل انجام یک فرایند مبادله و انتقال داده پیام صورت می‌گیرد، مانند آنکه که در یک معامله‌ی تجاری پس از انجام مراحلی، نظیر بررسی حساب خریدار مبنی بر داشتن موجودی کافی، دستور کسر از حساب خریدار و واریز به حساب فروشنده صادر شود و معامله تمام شده فرض و کالا تسلیم خریدار شود اما خریدار با یک سری اقدامات که از قبل انجام داده، به طور کلی مانع از ارسال داده‌ی حاوی دستور پرداخت به بانک شود. (جاویدنیا: ۱۳۸۷، ص۲۳۳) امروزه کلاه برداری از راه وارد کردن، تغییر، محو و موقوف سازی در خروجی سیستم کامپیوتری (ماشین‌های تحویل‌دار خودکار بانک‌ها) معمولی‌ترین شیوه‌ی کلاه برداری

1. Delete

رایانه‌ای است. یکی دیگـر از روش‌هـای سـنتی و متـداول، روش "اسـب تراوا" است که در آن دستورالعمل‌های کامپیوتری به صـورت مخفیانـه در برنامه‌های کامپیوتری قرار داده می‌شود تا بدین ترتیب عملیات غیرمجاز و خلاف را هم زمان با عملیات معمول و مجاز برنامه اجرا کنند. ایـن روش قابلیت این را دارد که هیچ گونه اثـری در حـین اجـرا از خـود بـه جـای نگذارد. (باستانی:۱۳۸۳،ص ۵۱)

یک نمونه‌ی عملی جالب در این باره در اواسط دهه‌ی ۱۹۷۰ در آلمـان غربی رخ داد که شامل اخفای مبادلات هنگفت ارزهای خارجی در بانـک هرشتات بود. تمامی امور حسابداری بانـک هرشـتات در مـورد مبـادلات ارزهای خارجی و وجه به وسیله‌ی صفحه کلید یک کامپیوتر کوچک ثبت شده و متعاقباً به کامپیوتر مرکز منتقل می‌شد. کارمندان بانک با فشـار دادن کلید توقف روی صفحه کلید یک رایانه‌ی کوچک موفق شدند تعـدادی از مبادلات هنگفت ارزهای خارجی را مخفـی نگـاه دارنـد بـه صـورتی کـه داده‌های مربوط به مبادلات مذکور به رایانه‌ی مرکزی بانک منتقل نمی‌شد. بدین ترتیب کارمندان می‌توانستند تاییدیه‌ی کاملی از رایانـه‌ی کوچـک در باره این مبادلات بر طرف قرارداد (پیمان کار) بگیرند بدون اینکه هیچ‌گونه سابقه‌ی محاسباتی در این باره در رایانه‌ی مرکزی بانـک ثبـت شـود. ایـن عمل امکان مخفی ساختن ضررها و حفـظ وجهـه‌ی کلـی بانـک را بـرای معادلات آینده فراهم می‌کرد. به علاوه کارمندان می‌توانستند ادعا کنند کـه ضررها در اثر فعالیت تجاری بانک به وجود آمده و در معادلات خصوصی که به حساب خود انجام می‌دادند موفق شوند.(زیبر: ۱۳۸۳، ص۲۸)

مداخله در عملکرد برنامه یا سیستم رایانه‌ای: مداخله در عملکرد برنامه یا رایانه به معنای ایجاد اختلال[1] در جریان پردازش داده‌ها است. توقـف در خروجی سیستم کامپیوتری ماشین‌های خودپرداز به ویـژه عـابر بانـک‌هـا ساده‌ترین و معمولی‌ترین شیوه‌ی کلاه برداری کـامپیوتری اسـت. یکـی از

1. Interference.

این روش ها، روش پروگا[1] است و مکانیزم آن دریافت و کم کـردن چنـد سانتیم (واحد پول) از سپرده‌های متناوب مشتریان است. بـه عنـوان مثـال، یکی از کارکنان شرکت بیمه برنامه‌ای کامپیوتری را برای کـم کـردن کسـر خاصی از سانتیم در هر عملیات شرکت و فرستادن آن به حسـاب مخفـی خود به کار گرفته است.(شوابکه: ۲۰۰۹، ص۱۷۹) هم چنین گفتـه شـده، شناخته شده‌تـرین دسـت کـاری پـردازش تقلـب "سـالامی"[2] (سوسـیس ایتالیایی) است که در آن یک برنامه مبالغ کوچکی را از حساب ها در حین پردازش گروهی با کسر خرده گرد کرده و وجوه به دست آمده را در یـک حساب مخفی متعلق به متقلب قرار می‌دهد.(وایلدینگ: ۱۳۷۹، ص۲۹)

با توجه به عبارت "وارد کردن، تغییر، حذف یا قطع داده‌های رایانـه‌ای و هـرگونـه ایجـاد اخـتلال در عملکـرد یـک سیسـتم رایانـه‌ای" کـه در کنوانسیون جرایم سایبری بیان شده و نیز با توجه به عبارت "وارد کـردن، تغییر، محو، یا متوقف ساختن داده‌ها یا برنامه‌های رایانه‌ای یا دیگر اقسـام ایجاد اختلال در جریان پردازش داده‌ها" که در فهرسـت حـداقل شـورای اروپا آمده، به نظر می‌رسـد کـه عنـوان "اخـتلال در عملکـرد رایانـه" یـا "اخلال در جریان پردازش داده‌هـا" از عنـاوین چهارگانـه‌ی وارد کـردن، محو، تغییر و متوقف کردن عام‌تر اسـت کـه قـانون‌گـذاز قـانون تجـارت الکترونیک آن را قسیم عناوین بیان شده قرار داده است. به ایـن نکتـه نیـز باید توجه کرد که در قانون تجارت الکترونیکی بر خلاف متن کنوانسـیون جرایم سایبری و فهرست حداقل شورای اروپـا، عنـوان "تغییـر داده‌پیـام" نیامده است که البته با توجه به عبارت "ارتکاب افعـالی نظیـر" در مـاده‌ی ۶۷ که به رفتارهای مذکور جنبه تمثیلی بخشیده شاید بتوان ایـن نقـص را توجیه کرد.

در این باره یکی از جلوه‌های کلاهبرداری که در سال‌های اخیر شهرت زیادی یافته است، پدیده‌ای است که "سرقت هویت" نامیده مـی‌شـود. در

1. Perru que.
2. Salami.

این گونه سرقت، هویت یک شخص با روش‌های مخفیانه ربوده می‌شود؛ به این صورت که ایمیلی (رایانه‌ای) برای اشخاص فرستاده می‌شود و فرستنده در آن ادعا می‌کند از پرسنل نهادهای مالی مربوط به شخص است و از او می‌خواهد که جزئیات حسابش را دوباره در وب سایت مشابهی ثبت کنند. یا اینکه ایمیل مذکور ویروسی دارد که به طور مخفیانه مشخصات اعتباری اشخاص را ضبط و افشاء می‌کند. و هدف آن، به دست آوردن جزئیات اطلاعات شخص برای قادر ساختن اجرای عملیات کلاه برداری است؛ خواه با استفاده از امتیازات موجود شخص یا ایجاد امتیازات جدیدی با استفاده از هویت وی. بنابراین، سرقت هویت، شکلی از رفتار مقدماتی برای کلاه برداری است.(Walden, 2007, p 557)

همچنین یکی دیگر از شیوه‌های جدید و خطرناک کلاه برداری در خرید و فروش آنلاین، کلاه برداری به روش فیشینگ[1] است. فیشینگ یا صیادی، نوعی کلاه برداری از راه کارت اعتباری است که طی آن یک ایمیل جعلی آلوده به ویروس، جاسوس افزار یا بدافزار به کاربران ارسال می‌شود تا نفوذگران با استفاده از آن بتوانند اطلاعات کارت اعتباری کاربران را سرقت کنند. طبق گزارش ۲۹ اوت ۲۰۱۰ مر کز کلاه برداری بر خط شرکت امنیتی RSA[2] که در حوزه‌ی امنیت اینترنت فعالیت می‌کند، حملات فیشینگ اکنون به ۷۰۰۰ حمله در ماه رسیده است. بنا بر این گزارش، نرم افزارهای فیشینگ خیلی راحت به صورت آنلاین خرید و فروش می‌شود و حتی به در منزل کاربران نیز فرستاده می‌شود و اکنون فیشرها حتی می‌تواند برندهای معروفی همچون اپل و ایکس باکس مایکروسافت یا سونی را نیز هدف قرار دهند.

هم چنین تکنیک «کپی‌سازی سایت‌های معتبر» هم جای خاصی در لیست اقدامات فیشرها دارد. در این روش، نفوذگران با استفاده از کیت‌های فیشینگ به تقلید طراحی وب سایت‌های معتبر و قانونی پرداخته

1. Fishing.
2. RSA Online Fraud Resource Center.

و حتی جزئیات طراحی و لوگو را هم از قلم نمیاندازند. بدین ترتیب سایتی جعلی و مشابه سایت اصلی طراحی و به کاربران ارائه می‌شود. سپس هکرها یک پایگاه داده‌ی ایمیل[1] را که معمولا در اینترنت به آسانی به دست می‌آید، خریداری کرده و آن را در وب سایت جعلی درج می‌کنند. در نهایت سایتی سر از اینترنت در می‌آورد که در ظاهر به یک سایت معتبر شباهت دارد و در آن، کاربران به خرید آنلاین با استفاده از کارت اعتباری تشویق می‌شوند.[2]

ب) فریب اشخاص یا گمراه کردن سیستم‌های پردازش خودکار:

مطابق آنچه در ماده‌ی ۶۷ قانون تجارت بیان شده، فریب اشخاص یا گمراه کردن سیستم‌های پردازش خودکار شرط دیگر تحقق کلاه‌برداری رایانه‌ای دانسته شده است. درباره‌ی امکان فریب کامپیوتر، قوانین کشورهای مختلف رویکردهای متفاوتی دارند:

رویکرد اول: به موجب بعضی از قوانین، برای اینکه جرم تقلب و کلاهبرداری صورت پذیرد لازم است فریب خورده، شخصی حقیقی (انسان) باشد. بنابراین، فریب کامپیوتر به عنوان یک دستگاه، متصور نیست و در نتیجه، مواد قانونی سنتی جرم کلاه برداری درباره‌ی فریب کامپیوتری و سیستم اطلاعاتی آن کاربردی ندارد. بر اساس این رویکرد، هرکس وسایلی متقلبانه را در مقابله با سیستم‌های پردازش اطلاعات با هدف به دست آوردن سودی مادی یا دست‌یابی به خدمتی، به کار گیرد، به عنوان جرم کلاه‌برداری، به مفهوم سنتی آن، تحت پیگرد قرار نمی‌گیرد، زیرا در عملیات فریب، فرض بر این است که قربانی توان اندیشه درباره‌ی امور مغایر با حقیقت یا نادرست را که بر او عرضه می‌شود، از دست بدهد و این امر به اشتباه وی و در پی آن، تصرف در مال وی بینجامد. پس سیستم پردازش اطلاعات ـ هوش مصنوعی ـ نیاز به خصوصیت اندیشه و تفکر

1. e-mail database.
2. RSA Online Fraud Resource Center. http://www.rsa.com.

دارد در حالی‌که سیستم، فرمان هایی را که از پیش دریافت داشته است، اجرا می‌کند یا شیوه‌ی پردازش آن دستورها را دریافت می‌کند. (شوابکه: ۲۰۰۹، ص ۱۸۶)

رویکرد دوم: به موجب بعضی از قوانین دیگر، اجرای قوانین خاص جرم کلاه برداری سنتی درباره‌ی کلاه برداری اطلاعاتی نیز امکان دارد. قوانین کشورهای انگلوساکسون از این دسته است.

قضات انگلیسی، آقای Thomson V.R (متهم) را به جرم کلاه برداری در پرونده‌ای به نام Thomson محکوم کردند. او برنامه نویس یکی از بانک‌های کویت بود و برنامه‌ای نوشت که به رایانه دستور می‌داد تعدادی از حساب‌های برخی مشتریان را که در رایانه حفظ شده بود و تا مدتی هیچ تراکنش مالی در آنها اجرا نشده بود به حساب‌های دیگری که پس از بازگشت به انگلستان در برخی بانک‌های این کشور باز کرده بود، انتقال دهد و انتقال این اموال را بر ترک خدمت خود در بانکی که انتقال اموال از آن صورت گرفته بود، وابسته کرده بود. هنگامی که این کار را انجام داد، پس از بازگشت به انگلستان، نامه‌ای به مدیر بانک نوشت و از او خواست تا دارایی حساب‌هایش را در کویت به انگلستان انتقال دهد. هنگامی که کار او آشکار شد، او به اتهام دست‌یابی به اموال از راه فریب محکوم شد. قانون‌گذار انگلستان مسئله‌ی فریب و تقلب کامپیوتر را، پس از تصویب قانون سوء استفاده از رایانه در سال ۱۹۹۰، جرم دانست و در تغییراتی که در سال ۲۰۰۶ در قانون کلاه برداری ایجاد شد، به این مطلب اشاره شد که در کلاه برداری به همراه فریب، این فریب می‌تواند درباره‌ی یک ماشین (مکانیسم) نیز همانند یک شخص صورت گیرد. (Walden, 2007, p 55[۶])

در کانادا پیاده سازی دو ماده‌ی ۳۸۷ و ۳۸۸ قانون کیفری درباره‌ی کلاه برداری اطلاعاتی آسان است. قضات کانادایی در پرونده‌ی Reginar marin Ressonrce Analystet Limited متهمان را به جرم شروع در کلاه برداری محکوم کردند، زیرا از شماره حساب شخص دیگری برای ورود به سیستم اطلاعاتی استفاده کردند. در استرالیا نیز درباره‌ی مفهوم کلاه برداری تفسیر

موسعی ارائه شده است که در آن از قانون انگلستان الهام گرفته شده است. (شوابکه: ۲۰۰۹، ص۱۸۷)

درباره‌ی تحلیل حقوقی این مطلب، باید دانست که به کارگیری عنصر اغفال و فریب، شرط ضروری تحقق کلاه‌برداری سنتی است و در صورت نبود این جزء، بردن مال دیگری، عنوانی غیر از کلاه برداری خواهد داشت. از این روی، گفته شده که اغفال و فریب درباره‌ی شخص حقیقی تصورپذیر است و درباره‌ی دستگاه، فریب دادن و فریب خوردن معنایی ندارد[1] و اصولاً به سبب ممکن نبودن اغفال و فریب مال باخته است که نمی‌توان به عنصر قانونی کلاه‌برداری سنتی استناد کرد و بدین جهت، کلاه‌برداری رایانه‌ای از کلاه‌برداری سنتی جدا دانسته شده است. (جاویدنیا: ۱۳۸۷، ص۲۳۷) این مطلب بدین معنا است که به طور کلی صرف استفاده از رایانه، ماهیت جرم را از جرم رایانه‌ای سنتی به جرم رایانه‌ای محض تغییر نمی دهد. به عنوان نمونه، اگر کسی با قصد کشتن بیمار معینی، با ورود به سیستم رایانه‌ای بیمارستان و تغییر علائم و نسخه‌ی بیمار، سبب کشته شدن او شود وی جرم قتل عمد را مرتکب شده است و تفاوتی با قتل عمدی از راه ریختن سم داخل غذای «مجنی علیه» ندارد و با قوانین سنتی می‌توان قاتل را مجازات کرد. در این موضوع نیز در صورتی که شخصی با استفاده از رایانه و مثلاً با تبلیغات گمراه کننده از راه شبکه‌ی اینترنت اشخاصی را فریب داده و مال آنها را به دست آورد، این عمل از نظر ماهیت تفاوتی با کلاه‌برداری سنتی ندارد و نیازی به وضع قوانین جداگانه برای کلاه‌برداری رایانه‌ای نیست. به بیان دیگر، ما دوگونه جرم رایانه‌ای داریم: جرم رایانه‌ای سنتی که رایانه فقط وسیله‌ی انجام جرم است و جرم رایانه‌ای محض که رایانه موضوع جرم است و

۱. در همین باره بعضی از صاحب نظران معتقدند، چون در کلاه برداری، اغفال و فریب بزه دیده شرط است و اغفال و فریب هم تنها علیه انسان تصورپذیر است و ماشین را نمی توان فریب داد، فلذا دادن عنوان کلاه برداری به آنچه که کلاه برداری های رایانه‌ای نامیده شده، مانند دست کاری شخص در برنامه‌ی رایانه و انتقال پول به حساب خود، از نظر قانون ما بی‌اشکال نیست(حسین میرمحمدصادقی،۱۳۸۸،ص۷۷)

جرم در خارج از محیط رایانه ناممکن است و انجام آن قبل از پیدایش رایانه و اجزای فناوری اطلاعات امکان پذیر نبست؛ مانند دسترسی غیرمجاز و تنها نوع دومی که بیان شد به وضع قوانین جدید و مجزا نیاز دارد.

با وجود این و با اینکه نه در کنوانسیون جرایم سایبری، نه در فهرست حداقل شورای اروپا، نه در قوانین کشورهای دیگر و نه حتی در متن قانون جرایم رایانه‌ای عنصر "فریب" شرط کلاه‌برداری رایانه‌ای دانسته نشده است، لکن به نظر می‌رسد قانون‌گذار قانون تجارت الکترونیکی بنا داشته هرگونه استفاده از رایانه، چه به عنوان وسیله‌ی انجام جرم که با آن شخصی حقیقی را فریب داده، اغفال کنند و چه به عنوان موضوع جرم که با دستکاری خود سیستم و داده‌ها و برنامه‌ها منافع غیرقانونی به دست آید، درباره‌ی هر دو با عنوان کلاه برداری رایانه‌ای حکم دهد. به بیان دیگر، قانون‌گذار کلاه برداری رایانه‌ای سنتی و کلاه برداری رایانه‌ای محض را موضوع حکم واحدی قرار داده است.

از سوی دیگر، درباره‌ی گمراه‌کردن سیستم‌های پردازش خودکار گفته شده که این شرط، شرط محالی است، چون اصولاً درباره‌ی مورد سیستم پردازش خودکار، گمراهی معنا ندارد. (خرم آبادی: ۱۳۸۴، ص۲۲۸) زیرا وظیفه‌ی آن پردازش اطلاعات ورودی بر اساس قواعد منطقی یا برنامه‌ی از پیش تعیین شده و نمایش نتیجه‌ی این پردازش است. به عنوان نمونه، اگر ۲+۲ به رایانه داده شود، طبق برنامه‌ی داده شده به رایانه، به صورت خودکار عدد ۴ دیده می‌شود. حال اگر کاربر به اشتباه ۲+۲۰ را به رایانه بدهد، و سیستم عدد ۲۲ را نشان دهد، سیستم، گمراه نشده بلکه کاملا درست جواب داده ولی اطلاعات وارد شده غلط بوده است! لکن در این باره نیز باید توجه داشت، همان‌گونه که دیگران نیز اشاره کرده‌اند (بای و پورقهرمانی: ۱۳۸۸، ص۳۲۷) منظور از گمراهی سیستم این نیست که دستگاه یا رایانه فریب بخورد، بلکه منظور این است که فرد با انجام رفتارهای مذکور در ماده سبب شود که دستگاه یا رایانه از مسیر اصلی

خود (برنامه‌ای که داده شده تا رایانه بر اساس آن مسیر و هدف، عمل کند) منحرف شود و در این صورت گفته می‌شود که وی سیستم را گمراه کرده است. در حقوق فرانسه برخی اعتقاد دارند که به وسیله‌ی تقلب در سیستم رایانه‌ای و فریب آن برای دست‌یابی به اموال، وصف راه‌های متقلبانه محقق می‌شود و در پی آن، جرم کلاه‌برداری رخ می‌دهد. و بر این سخن، چنین استناد کرده‌اند که وارد ساختن وسایل تقلب یا فریب سیستم‌های اطلاعاتی جزو راه‌های متقلبانه است و تصور فریب رایانه بر این اساس ممکن است که در پشت این ابزار، انسانی قرار دارد که این ابزار را برنامه‌ریزی کرده است. (سامی الشوا: ۱۹۹۸، ص۷۳)

نتیجه حاصله: برابر ماده‌ی ۶۷ ق.ت.ا. در صورتی که رفتار مادی بیان شه در این ماده موجب شود که فرد از این راه برای خود یا دیگری وجوه، اموال یا امتیازات مالی به دست آورد و اموال دیگران را ببرد، مجرم محسوب می‌شود. بنابراین "بردن وجه، مال یا امتیاز مالی" نتیجه‌ی این جرم است. این در حالی است که در ماده‌ی ۱۳ قانون جرایم رایانه‌ای به دست آوردن "منفعت" یا "خدمات" نیز محقق کننده‌ی کلاه برداری رایانه‌ای دانسته شده است و این امر بیان‌گر جامعیت قانون جرایم رایانه‌ای نسبت به قانون تجارت الکترونیکی است.

به دست آوردن وجه یا مال یا امتیاز مالی ممکن است برای خود فرد باشد یا برای شخص مورد نظر وی، مثل ورود به سیستم یک بانک و انتقال مبلغی پول به حساب همسر یا یکی از بستگان خود. بنابراین اگر کسی با ورود به سیستم بانک، حساب‌ها را به هم ریخته و جابه‌جا کند و این فرایند، موجب تضرر کردن بعضی از حساب داران و بهره‌مند شدن بعضی حسابداران ناشناس دیگر شود، عمل این فرد با جرم موضوع ماده‌ی ۶۷ قانون تجارت الکترونیکی مطابقت ندارد.

از جنبه‌ی نظری، درباره‌ی تحقق کلاه برداری رایانه‌ای از این نظر، تردید شده است و به عقیده‌ی مخالفان جرم کلاه‌برداری رایانه‌ای، چون در کلاه‌برداری، به دست آوردن و انتقال مادی مال لازم است و در

کلاه‌برداری رایانه‌ای به سبب طبیعت غیرمادی موضوع جرم، یعنی داده پیام‌ها یا برنامه‌های رایانه‌ای، به دست آوردن و انتقال مادی مال امکان پذیر نیست فلذا کلاه‌برداری محقق نمی‌شود. (زراعت: ۱۳۸۵،ج۲، ص۱۶۳) رویه‌ی قضایی نیز تا قبل از تصویب قانون جرایم رایانه‌ای به کار بردن لفظ "مال" را اطلاعات رایانه‌ای که نمود فیزیکی ندارند، نمی‌دانست. (معاونت آموزش قوه‌ی قضائیه: ۱۳۸۷، ص۱۰۶۳)

این تردید به سبب ماهیت غیرمادی اطلاعات موجود در رایانه است. با وجود این، در حال حاضر در بسیاری از کشورها با توسعه در مفهوم مال[1] آن را شامل هر چیزی دانسته‌اند که ارزش دانسته و قابل تقویم به پول است و در این تعریف، اموال معنوی(غیرمادی) و داده‌ها و برنامه‌های رایانه‌ای هم در مفهوم مال داخل بوده و قوانین این کشورها ـ به ویژه کشورهای انگلو ساکسون، مانند ایالات متحده، انگلستان، کانادا، استرالیا و... هرگونه به کارگیری غیرمجاز رایانه برای تدلیس یا تسلط بر اموال دیگران مجازات در نظر گرفته‌اند. (سامی الشوا: ۱۹۹۳م، ص۱۲۸) در کشور ما نیز تصویب قوانینی همچون قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای به مباحث نظری در این باره پایان داده و امروزه از نظر قانونی درباره‌ی مال بودن داده‌ها و اطلاعات غیرمادی موجود در رایانه تردیدی نیست.

مطلب دیگری که باید درباره‌ی تحقق نتیجه در کلاه‌برداری رایانه‌ای بررسی شود، شروع به جرم است. برابر تبصره‌ی ماده‌ی ۶۷ ق.ت.ا.: "شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر در این ماده می‌باشد." از آن جا که این جرم مقید به نتیجه‌ی "بردن وجه، مال یا امتیاز مالی" است، مادام که نتیجه‌ی مورد نظر محقق نشود، جرم صورت نگرفته و در صورتی که رفتار مادی ورود، محو، توقف داده‌پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای انجام شده باشد، شروع به جرم محقق شده است.

1. Property.

نکته‌ی جالب توجه اینکه اگر شروع به جرم کـلاه‌بـرداری رایانـه‌ای در قالب ورود، محو، توقف و تغییر داده‌ها باشد، چون این رفتارها رفتار مادی جرم جعل، موضوع ماده‌ی ۶۸ قانون تجارت الکترونیکی نیز هسـت، فلـذا جرم جعل محقق می‌شود و شروع به جرم کلاه‌برداری، منتفی خواهد بـود و حتی اگر بر خلاف استنباط رایج حقوقی در این گونه موارد، بـه اجـرای قواعد تعدد اعتباری قائل باشیم، بـاز هـم چـون مجـازات جـرم جعـل در ماده‌ی ۶۸ یک تا سه سال حبس در نظر گرفته شده، که در رویه‌ی جـاری دادگستری غالباً حداقل، یعنی یک سال حبس، داده مـی‌شـود[1] و مجـازات پنجاه میلیون ریال جزای نقدی هـم بـدون حـداقل ذکـر شـده و حـداقل مجازات کلاه‌برداری هم یک سال حبس است، فلذا رجوع به قواعد تعـدد معنوی هم مشکلی را حل نمی‌کند. بنابراین، به نظر می‌رسد قانون‌گـذار در تبصره‌ی ماده ۶۷ ق.ت.ا. یا دست کم درباره‌ی بخشی از آن کـه بـه ورود، محو و توقف داده پیام اشاره دارد ـ دچار لغو شده است. و شـاید از ایـن رو است که در قانون جرایم رایانه‌ای برای شـروع بـه جـرم کـلاه‌بـرداری رایانه‌ای مجازاتی تعیین نشده است.

محل وقوع جرم: در بحث از رکن مادی جرم کـلاه بـرداری رایانـه‌ای، موضوع قانون تجارت الکترونیکی، محل وقوع جرم نیز موضوعیت داشـته و وقوع این رفتارها در بستر تجارت الکترونیکی شرط است.

منظور از بستر مبادلات الکترونیکی، بستری اسـت کـه در آن تعـاملات مالی الکترونیکی صورت می‌پذیرد که هرگونه فنآوری جدیـد اطلاعـات و ارتباطات همچون اینترنت، مخابرات، ماهواره و به طور کلی فضای سـایبر را در بر می‌گیرد. (وزارت بازرگانی، ۱۳۷۸، ص۴۳)

---

۱. اصولاً تعیین حداقل مجازات جرم تام برای شروع به آن جرم، روش درستی نیست، چـرا کـه نتیجـه‌ی آن، تعیین مجازات برابر برای جرم تام و شروع به جرم در بسیاری از موارد خواهد بود و تعیـین حـداقل مجازات مباشر برای معاون این گونه توجیه پذیر است که قاضی بـا توجـه بـه نقـش مباشـر و معـاون و مقایسه مجازات آن دو، مجازات مباشر را حداقل تعیین شده قـرار نخواهـد داد، در حـالی کـه دربـاره‌ی شروع به جرم، دو متهم وجود ندارد که قاضی بـرای شـروع کننـده حـداقل و بـرای مرتکـب جـرم تـام مجازات بیشتر را تعیین کند.

مبحث سوم: رکن معنوی

جرم کلاه‌برداری رایانه‌ای جرمی عمدی است. و اجزای رکن معنوی این جرم شامل سوء نیت عام (عمد و اراده) در انجام رفتار مادی "استفاده‌ی غیرقانونی" (ورود، محو، توقف داده‌پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای) و امثال آن است. تصریح ماده‌ی ۶۷ ق.ت.ا. به عبارات "سوء استفاده‌ی یا استفاده غیرمجاز از داده‌پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور" و "فریب اشخاص یا گمراه کردن سیستم‌های پردازش خودکار" بیان‌گر لزوم عمد و اراده‌ی فرد در انجام اعمال مذکور است.

بنابراین تحقق کلاه‌برداری رایانه‌ای همانند بسیاری از جرایم رایانه‌ای دیگر[1]، به سبب بی احتیاطی یا بی مبالاتی یا رعایت نکردن نظامات دولتی تصورپذیر نخواهد بود.

افزون بر این، در کلاه‌برداری رایانه‌ای سوء نیت خاص نیز ضرورت دارد که همانا قصد تحقق نتیجه، یعنی به دست آوردن، مال یا امتیاز مالی برای خود فرد یا شخص مورد نظر اوست. تبیین عنصر معنوی جرم کلاه‌برداری در این نمونه به خوبی آشکار است که به موجب آن، شخصی در نقطه‌ای نامعلوم با وارد شدن به شبکه‌ی بین‌المللی اینترنت و معرفی خود به عنوان تاجر و صاحب یک شرکت معتبر در یک سایت تجاری و ارائه‌ی (CA)[2] و

---

۱. با وجود این، در موارد استثنایی ممکن است بعضی از جرایم رایانه‌ای به صورت غیرعمد و به سبب بی احتیاطی و بی مبالاتی هم محقق به عنوان نمونه، برابر ماده‌ی ۲۳ قانون جرایم رایانه‌ای:" ارائه‌دهندگان خدمات میزبانی موظفند به محض دریافت دستور کارگروه (کمیته) تعیین مصادیق مذکور در ماده‌ی فوق یا مقام قضائی رسیدگی‌کننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه‌های رایانه‌ای خود، از ادامه‌ی دسترسی به آن ممانعت به عمل آورند. چنانچه عمداً از اجرای دستور کارگروه (کمیته) یا مقام قضائی خودداری کنند، منحل خواهند شد. در غیر این صورت، چنانچه در اثر بی احتیاطی و بی‌مبالاتی زمینه‌ی دسترسی به محتوای مجرمانه‌ی مزبور را فراهم کنند، در مرتبه‌ی نخست به جزای نقدی از بیست میلیون (۲۰،۰۰۰،۰۰۰) ریال تا یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال و در مرتبه دوم به یکصد میلیون (۱۰۰،۰۰۰،۰۰۰) ریال تا یک میلیارد (۱،۰۰۰،۰۰۰،۰۰۰) ریال و در مرتبه‌ی سوم به یک تا سه سال تعطیلی موقت محکوم خواهندشد."

۲. CA در تجارت الکترونیک، نهادی است مشابه اداره‌ی ثبت اسناد. این نهاد عهده دار ثبت داده‌های تجاری و تجار است تا بدین ترتیب تاجر، مجوز ورود به عرصه‌ی تبادلات الکترونیک را به دست آورد.

(PKI)[1] کـاملا دروغ و غیـر واقعـی مـی‌گویـد کـه کـالایی را بـا قیمـت معـین، نـوع و تعـداد مشـخص در اختیـار دارد کـه مـی‌توانـد در اختیـار مشـتریان قـرار دهـد. از طرفـی، خریـدارانی کـه در فضـای شـبکه‌هـا مشـغول تجـارت الکترونیکـی و خریـد و فـروش هسـتند، پـس از دریافت پیام، با برقراری ارتبـاط شـبکه‌ای (کـه غالبـا بـه صـورت پسـت الکترونیـک یـا ارسـال درخواسـت از راه شـبکه اسـت)، قبـول (خریـد) خود را اعـلام و مقـداری از کـالای مـورد نظـر را درخواسـت مـی‌کننـد. شخص فروشـنده پـس از جلـب اعتمـاد طـرف مقابـل (بـا دادن کـدهای CA و PKI) شـماره حسـاب یـا شـماره کـارت اعتبـاری خـود را بـرای دریافت وجه اعلام می‌کنـد. خریـدار نیـز پـس از پرداخـت وجـه (غالبـا به صـورت پرداخـت‌هـای الکترونیکـی) منتظـر دریافـت کـالا اسـت، در صورتی که شخص فروشـنده قـبلا بـا عملیـات متقلبانـه و نفـوذ توانسـته بـود کـدهای CA و PKI غیـر واقعـی را در اختیـار خـود گیـرد و بـدین گونه مبلغـی را بـه طـور غیرمجـاز بـه دسـت آورد. در ایـن مثـال، سـوء نیت عـام مجـرم در قالـب علـم بـه غیـر واقعـی بـودن کـدهای خـود و داشـتن عمـد در دریافـت پـول از خریـدار و سـوء نیـت خـاص وی در قصد خاص به دست آوردن پول از بزه دیده آشکار شده است.

مجازات کلاه‌برداری رایانه‌ای:

برابر مـاده‌ی ۶۷ قـانون تجـارت الکترونیکـی، مجـازات کـلاه‌بـرداری رایانه‌ای یک تا سه سال حبس و نیز پرداخـت جـزای نقـدی معـادل مـال گرفته شده است.[2] از سوی دیگر، مجازات کلاه‌بـرداری مـرتبط بـا رایانـه،

۱. PKI در تجارت الکترونیک به معنای زیرساخت کلید عمومی است. اسـاس تجـارت الکترونیـک و از محورهای عمده و مهم آن داشتن PKI برای تجار است. (باستانی: ۱۳۸٦، ص۹۳)

۲. رد مال تحصیل شده از جانب بزه کار به بزه دیده که در قالب عین، مثل یا قیمت آن محقق مـی شـود را نمی توان مجازات به حساب آورد بلکه نوعی مسئولیت مدنی است که طبق قواعد کلی باب ضـمان و هم چنین مواد کلی مثل ماده ۹ قانون مجازات اسلامی حکم به آن داده می شود. به موجـب ایـن مـاده:" مجرم باید مالی را که در اثر ارتکاب جرم تحصیل کرده است اگر موجود باشد عینا" واگر موجود نباشـد ، مثل یا قیمت آن را به صاحبش رد کند واز عهده خسارات وارده نیز برآید."

موضوع ماده‌ی ۱۳ قانون جرایم رایانه‌ای، حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون تا صد میلیون ریال یا هر دو مجازات خواهد بود.

با مقایسه‌ی بین مجازات کلاه‌برداری سنتی با کلاه‌برداری رایانه‌ای، موضوع قانون تجارت الکترونیکی، در می‌یابیم که مجازات کلاه برداری سنتی (یک تا هفت سال حبس و جزای نقدی معادل مال گرفته شده) شدیدتر از کلاه‌برداری رایانه‌ای در بستر تجارت الکترونیک است و این در حالی است که به سبب آسانی و هزینه‌ی کمتر انجام جرم برای مجرم، این کار ضررهای بیشتری برای بزه دیده به دنبال دارد؛ ضمن این که به جهت ناشناس ماندن بزه دیده، هزینه و وقت و تخصص بیشتری برای کشف جرم و تعقیب مجرمان به کار می‌رود. بنابراین چنین رویکردی از سوی مقنن توجیه‌پذیر نیست. با وجود این، نگارنده درباره‌ی علت تعیین مجازات کمتر برای کلاه‌برداری رایانه‌ای نسبت به کلاه‌برداری سنتی، این گفته را قبول ندارد که قانون‌گذار در سیاست کیفری خود، یا به جنبه‌ی ارعابی کیفرهای شدید اعتماد و اعتقاد نداشته است و یا به ملاحظات بین‌المللی و استرداد مجرمان کلاه‌برداری رایانه‌ای توجه شده است. (گلدوزیان: ۱۳۸۵، ص۳۵۷) بلکه چنین رویکردی را بیشتر نتیجه‌ی تعدد مراجع قانون‌گذار و دقت نکردن در روش‌های قانون نویسی می‌داند، امری که در مقایسه با دو جرم مشابه، یعنی کلاه‌برداری رایانه‌ای، موضوع ماده‌ی ۶۷ قانون تجارت الکترونیکی و کلاه‌برداری مرتبط با رایانه، موضوع ماده‌ی ۱۳ قانون جرایم رایانه‌ای، به خوبی دیده می‌شود.

نتیجه:

حمایت‌های حقوقی و به ویژه حمایت کیفری از تجارت الکترونیکی در کنار فراهم ساختن بسترهای فنی و امکانات ارتباطاتی و تکنولوژیکی، از مهم‌ترین ابزارهای گسترش و توسعه‌ی این شیوه از تجارت آسان، سریع و کم هزینه است. حمایت کیفری، به ویژه سبب جلب اعتماد

مشتریان و خریداران اینترنتی شده و جرأت انجام خرید برخط را در افراد به وجود می‌آورد. اعتمادسازی از راه حمایت کیفری از تجارت الکترونیکی در قالب حمایت از حقوق مصرف کننده و سازمان‌دهی تبلیغات اینترنتی، حمایت از داده‌پیام‌های شخصی، حمایت از حقوق مؤلف و حمایت از اسرار و علائم تجاری در بستر مبادلات الکترونیکی، اموری است که قانون تجارت الکترونیکی، مصوب سال ۱۳۸۱، به آن توجه کرده است.

حمایت از افراد در مقابل سوء استفاده کنندگان از بستر تجارت الکترونیک، از جمله در قالب جرم انگاری کلاه‌برداری رایانه‌ای دیده می‌شود که اجزاء و عناصر آن در متن مقاله بررسی شد. نکته‌ای که نگارنده بر آن تأکید دارد، این است که به نظر می‌رسد توسعه‌ی تجارت الکترونیک بر سه محور زیرساخت‌های فنی و ارتباطی، تدوین مقررات حقوقی و نیز آموزش تجارت الکترونیکی استوار است. از نظر محور دوم، یعنی تدوین چارچوب‌های حقوقی و به ویژه حمایت‌های کیفری اعتمادساز، از نظر نگارنده ـ با وجود نواقص و اشکالات موجود در قانون تجارت الکترونیکی که در همین نوشته هم به بعضی از آنها اشاره شد ـ مشکل چندانی وجود ندارد.

از دو محور دیگر، یعنی زیرساخت‌های فنی و ارتباطی و آموزش تجارت الکترونیکی، محور نخست، در کشور ما به سرعت در حال آماده شدن است و تهیه‌ی زیرساخت‌های فنی رشد خوبی داشته است. اما آنچه به کندی در حال انجام است و متأسفانه کمتر نیز بدان توجه شده و دغدغه‌ها نسبت به آن ضعیف‌تر است، بحث آموزش تجارت الکترونیکی است که افراد را قادر می‌سازد به بازار تجارت الکترونیکی وارد شده و با آگاهی از ضوابط و مقررات، حقوق و نیز تکالیف خود، چه به عنوان فروشنده و چه به عنوان خریدار، با اطمینان به معامله پرداخته، از مزایای تجارت الکترونیکی بهره‌مند شوند. امری که توجه به آن، امیدها را درباره‌ی توسعه‌ی تجارت الکترونیکی در کشور افزایش می‌دهد.

منابع:

۱. اردبیلی، المولی أحمد (المقدس الاردبیلی) ، مجمع الفایدة و البرهان، قم، مؤسسة النشر الإسلامی، الطبعة الثالثه، ۱۴۲۱ ق.

۲. اصفهانی، فاضل هندی، محمد بن حسن، کشف اللثام و الإبهام عن قواعد الأحکام، جلد۱۰، دفتر انتشارات اسلامی وابسته به جامعه مدرسین حوزه علمیه، قم، چاپ اول، ۱۴۱۶ ه ق.

۳. باستانی، برومند، جرایم کامپیوتری و اینترنتی؛ جلوه‌ای نوین از بزهکاری، تهران، بهنامی، چاپ دوم، ۱۳۸۶

۴. بای، حسینعلی و پورقهرمانی، بابک، بررسی فقهی حقوقی جرایم رایانه‌ای، قم، پژوهشگاه علوم و فرهنگ اسلامی، چاپ اول، ۱۳۸۸.

۵. پنلوپ، لارنس، کاربرد اینترنت در حقوق، ترجمه: سید قاسم زمانی و مهناز بهراملو، تهران، نشر میزان، چاپ اول، ۱۳۸۳.

۶. جاویدنیا، جواد، جرایم تجارت الکترونیکی، تهران، خرسندی، چاپ اول،۱۳۸۷.

۷. حلی، حسن بن یوسف بن المطهر الاسدی (علامه حلی)، تحریر الاحکام الشرعیه علی مذهب الامامیه، ج ۵، قم ، مؤسسة الامام الصادق ، الطبعة الاولی، ۱۴۲۲ ق.

۸. الحلی، محمد بن منصور بن أحمد بن إدریس، السرایر الحاوی لتحریر الفتاوی، ج۳ ، قم ، مؤسسة النشر الإسلامی، الطبعة الثانیه، ۱۴۱۱ق

۹. خرم آبادی، عبدالصمد، تاریخچه، تعریف و طبقه‌بندی جرم‌های رایانه‌ای، مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، قوه‌ی قضائیه، معاونت حقوقی و توسعه‌ی قضایی، سلسبیل، ۱۳۸۴.

۱۰. خویی، سید ابو القاسم موسوی، مبانی تکملة المنهاج، جلد۱، مؤسسة إحیاء آثار الإمام الخوئی، قم، چاپ اول، ۱۴۲۲ ه ق

۱۱. دزیانی، محمدحسن، جرایم کامپیوتری از حیث حقوق جزای اختصاصی، خبرنامه‌ی انفورماتیکف، شماره‌ی ۶۴، ۱۳۸۱.
۱۲. زراعت، عباس، حقوق جزای اختصاصی تطبیقی ـ ۲، جرایم علیه اموال و مالکیت، تهران، ققنوس، ۱۳۸۵.
۱۳. زیبر، اولریش، جرایم رایانه‌ای، ترجمه: محمدعلی نوری و دیگران، تهران، گنج دانش، چاپ اول، ۱۳۸۳.
۱۴. صغیر، جمیل، الحمایة الجنائیة و المدنیه لبطاقات الائتمان الممغنطه (دراسة تطبیقیه فی القضاء الفرنسی والمصری)، الطبعة الاولی، دارالنهضة العربیه، القاهره، ۱۹۹۹.
۱۵. طوسی، أبو جعفر محمد بن الحسن (شیخ طوسی)، النهایه فی مجرد الفقه و الفتاوی، بیروت، دار الکتب العربی، الطبعة الثانیه، ۱۴۰۰ ق.
۱۶. طوسی، محمدبن علی بن حمزه، المعروف بابن الحمزه، الفضیله إلی نیل الوسیله، قم، مکتبة آیةا...المرعشی النجفی، الطبعة الاولی، ۱۴۰۸
۱۷. طوسی، أبی جعفر محمد بن الحسن (شیخ طوسی)، الاستبصار فیما اختلف من الاخبار، ج۴، طهران، دارالکتب الاسلامیه، الطبعة الثالثه، ۱۳۹۰ق.
۱۸. عاملی، زین الدین بن علی الجبعی (الشهیدالثانی)، الروضةالبهیه فی شرح اللمعة الدمشقیة، ج۴، قم، مجمع الفکر الاسلامی، الطبعةالثانیه، ۱۴۲۷ق.
۱۹. عکبری البغدادی، محمدبن محمدبن النعمان، المعروف بالشیخ المفید، المقنعه، قم، کنگره جهانی هزاره شیخ مفید، چاپ اول،۱۴۱۳ ق .
۲۰. عوده، عبدالقادر، التشریع الجنائی الاسلامی، ج۱، بیروت، دار إحیاء التراث العربی، الطبعه الرابعه، ۱۴۰۵ق.
۲۱. قوه‌ی قضائیه، مرکز مطالعات راهبردی و توسعه‌ی قضایی و شورای عالی توسعه‌ی قضایی، کمیته‌ی مبارزه با جرایم رایانه‌ای، لایحه‌ی قانون مجازات جرایم رایانه‌ای (متن و گزارش توجیهی)، فروردین ۱۳۸۳.
۲۲. کورپر، استفانو و دیگران، تجارت الکترونیکی، ترجمه: خسرو مهدی پور عظیمی، تهران، موسسه‌ی فرهنگی و هنری دیباگران، چاپ اول، ۱۳۸۰.

۲۳. گلدوزیان، ایرج، حقوق جزای اختصاصی، تهران، انتشارات دانشگاه تهران، چاپ دوازدهم، ۱۳۸۵.
۲۴. محمد امین الشوابکه، جرائم الحاسوب و الإنترنت، عمان، دارالثقافه، الطبعة الاولی/ الاصدارالثالث، ۲۰۰۹.
۲۵. محمد سامی الشوا، الغش المعلوماتی کظاهرة إجرامیة مستحدثه، مقاله‌ی ارائه شده در همایش جرایم رایانه‌ای و سایر جرایم قلمرو فناوری اطلاعات، برگزار شده در تاریخ ۲۵ تا ۲۸ اکتوبر ۱۹۹۳.
۲۶. میرمحمدصادقی، حسین، جرایم علیه اموال و مالکیت، تهران، میزان، چاپ بیست و چهارم، پاییز ۱۳۸۸.
۲۷. نائل عبدالرحمن صالح، واقع جرائم الحاسوب فی التشریع الجزائی الاردنی، بحث ارائه شده در همایش حقوق، رایانه و اینترنت، برگزار شده در دانشکده‌ی حقوق دانشگاه امارات متحده‌ی عربی در سال ۲۰۰۰.
۲۸. نجفی، الشیخ محمدحسن، جواهرالکلام فی شرح شرایع الإسلام، ج ۴۱، تهران، دارالکتب الإسلامیه، الطبعةالرابعه، ۱۳۷۴ ش.
۲۹. نوری، اصول حقوقی تجارت الکترونیک با تأکید بر قانون تجارت الکترونیک ایران، مجله‌ی حوزه و دانشگاه، سال یازدهم، شماره‌ی ۴۴، پاییز ۱۳۸۴.
۳۰. وایلدینگ، ادوارد، جرایم رایانه‌ای، ترجمه: محمد هادی و دیگران، تهران، معاونت آموزش ناجا، ۱۳۷۹.
۳۱. وزارت بازرگانی، کمیته‌ی ادیفاکت، پیش‌نویس متن پیشنهادی قانون تجارت الکترونیکی، پاییز ۱۳۷۸.
32. http://www.rsa.com
33. sarmayeh.net/ShowNews.php
34. Smith ،Margaret, CONSUMERPROTECTIONAND, ELECTRONIC COMMERCE, Law and Government Division, 2000
35. Turban,Efraim.King,David.Lee,Jae.Warkentin,Merrill.Chung ،Michael, (2002), Electronic Commerce,Prentic Hall.
36. Walden, IanComputerCrimeAndInformationMisuse, ComputerLaw, Oxford University Press, Six Edition, Edited By: Chris Reed and John Angel,2007