فصلنامه حقوق مجلهٔ دانشکده حقوق و علوم سیاسی، سال ۳۷، شمارهٔ ۲، تابستان ۱۳۸٦ ، صفحات۱۱۲-۸۳

کلاهبرداری رایانه‌ای

از دیدگاه بین‌المللی و وضعیت ایران

عبدالصّمد خرّم آبادی*
دانشجوی دوره دکتری حقوق جزا وجرم شناسی
دانشکده حقوق و علوم سیاسی دانشگاه تهران

چکیده:

جرم کلاهبرداری رایانه‌ای یکی از مهمترین جرائم رایانه‌ای است. این جرم نیز مانند جرم کلاهبرداری کلاسیک ازجمله جرائم علیه اموال و مالکیت محسوب می‌شود. هر نوع کلاهبرداری ارتکاب یافته به وسیله رایانه، لزوما کلاهبرداری رایانه‌ای نامیده نمی شود، چرا که مجرمین از رایانه‌ها هم به عنوان وسیله ارتکاب کلاهبرداری کلاسیک و هم کلاهبرداری رایانه‌ای استفاده می‌کنند. کلاهبرداری رایانه‌ای و کلاهبرداری کلاسیک، از جهت فرآیند ارتکاب و عناصر تشکیل-دهنده با هم تفاوت دارند. این تفاوت باعث شده است که قوانین ومقررات مربوط به کلاهبرداری سنتی در مورد کلاهبرداری رایانه‌ای قابل اعمال نباشند. با توجه به بعد بین‌المللی جرائم رایانه‌ای برخی از سازمان‌های بین‌المللی منطقه‌ای و جهانی معیارهایی را برای تعریف جرم کلاهبرداری رایانه‌ای ارائه داده و از کشورهای عضو خواسته‌اند با رعایت آنها نسبت به جرم‌انگاری این جرم اقدام نمایند. در ایران کلاهبرداری رایانه‌ای 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 ٦٧ قانون تجارت الکترونیکی شده است . ماده ۸ پیشنویس قانون جرائم رایانه‌ای نیز از نظر فنی با اشکالاتی مواجه است. تهیه‌کنندگان این پیش‌نویس نیز نتوانسته‌اند کلاهبرداری رایانه‌ای را به درستی جرم انگاری نمایند. با توجه به جنبه بین‌المللی کلاهبرداری رایانه‌ای قانونگذار ایران باید در جرم انگاری این جرم از تجربیات دیگر کشورها وسازمان‌های بین‌المللی استفاده کند.

واژگان کلیدی:
کلاهبرداری رایانه‌ای - کلاهبرداری کلاسیک - داده‌های رایانه‌ای - اخلال در داده‌ها - اخلال در عملکرد سیستم رایانه‌ای - بستر مبادلات الکترونیکی - داده پیام - سوءاستفاده از برنامه‌ها و سیستم‌های رایانه‌ای - استفاده غیرمجاز از برنامه‌ها و سیستم‌های رایانه‌ای.

* فاکس : ۸۸۰۰۷۹۴۸
E mail: Infokhoram@yahoo.com

۱- مقدمه

کلاهبرداری رایانه‌ای یکی از جرائم ناشی از سوءاستفاده از فناوری اطلاعات است. فناوری اطلاعات پدیده منحصر به فرد عصر حاضر است که موجب پیشرفت و تغییر و تحول عظیم و عمیقی در تمام ابعاد و شئون زندگی انسان شده است. این پدیده با طرح مسائل جدید بسیاری از علوم را با چالش‌های جدی مواجه ساخته و آنها را تحت تاثیرقرار داده است. علم حقوق نیز به عنوان شاخه‌ای از علوم اجتماعی که تنظیم وتنسیق روابط انسانها را درچارچوب حیات جمعی برعهده دارد، عمیقا تحت تاثیر فناوری اطلاعات قرار گرفته است. در این راستا حقوق جزا بیشتر از سایر شاخه‌های حقوق تاثیر پذیرفته، چرا که این پدیده نه تنها امکان ارتکاب رفتارهای مجرمانه جدیدی را به وجود آورده که قبل از این به هیچ وجه امکان پذیر نبوده، بلکه با خلق دنیای جدیدی به نام فضای سایبر[1] ارتکاب بسیاری از رفتارهای مجرمانه مرسوم را تسهیل نموده است.کلاهبرداری رایانه‌ای از جمله جرائمی است که با پیدایش فناوری اطلاعات وارد عرصه حقوق جزای اختصاصی شده و اصول وقواعد حاکم برکلاهبرداری سنتنی را به چالش کشیده است. کلاهبرداری رایانه‌ای ازجهت اسمی ونتیجه حاصل از جرم با کلاهبرداری کلاسیک شباهت دارد، اما تفاوت آنها از جهت فرایند ارتکاب وعناصراختصاصی تشکیل دهنده جرم باعث شده است که کلاهبرداری رایانه‌ای به‌عنوان جرمی مستقل از کلاهبرداری کلاسیک مطرح شود. خاطرنشان می‌شود که هرگونه ارتکاب کلاهبرداری به‌وسیله رایانه کلاهبرداری رایانه‌ای محسوب نمی‌شود. رایانه از دوجهت در ارتکاب کلاهبرداری دخیل است :

۱- استفاده از رایانه برای ارتکاب کلاهبرداری کلاسیک، به این صورت که مرتکب از طریق رایانه، متوسل به وسایل متقلبانه گردیده و دیگری را فریب می‌دهد و مال او را می‌برد. در این صورت چون رایانه صرفا به عنوان وسیله ارتکاب جرم مورد استفاده

[1] -Cyber-space.

قرار می‌گیرد و نوع وسیله در تحقق کلاهبرداری کلاسیک موثر نیست، لذا عمل مرتکب با قوانین کیفری مربوط به کلاهبرداری کلاسیک قابل تعقیب و مجازات بوده وجرم ارتکاب‌یافته کلاهبرداری کلاسیک است که می‌توان آن را "کلاهبرداری کلاسیک رایانه-ای" نیز نامید.

۲- استفاده از رایانه برای ارتکاب کلاهبرداری رایانه‌ای ،به‌این صورت که مرتکب بدون فریب قربانی و یا نماینده وی از طریق مداخله ناروا در داده‌های رایانه‌ای یا عملکرد سیستم‌های رایانه‌ای مال او را می‌برد، یا از خدمات مالی متعلق به او بهره‌مند می‌شود. این نوع کلاهبرداری که عنصر مادی آن با کلاهبرداری کلاسیک متفاوت است و با قوانین کیفری مربوط به کلاهبرداری کلاسیک قابل تعقیب ومجازات نیست، کلاهبرداری رایانه‌ای نامیده شده است. در برخی از اسناد بین‌المللی این نوع کلاهبرداری ، کلاهبرداری مرتبط با رایانه نامیده شده است.[1]

نتایج پژوهش‌های انجام شده نشان می‌دهد که اولین کلاهبرداری‌های رایانه‌ای در دهه ۱۹۶۰ واقع شده‌اند (زیبر، ۱۳۷٦ الف، ص۱۰). این جرم از دهه ٦۰ تا امروز، اشکال متنوعی به خود گرفته است و نسل به نسل و گام به گام همپای ارتقاء وپیشرفت فناوری اطلاعات، متحول شده است. جرم کلاهبرداری رایانه‌ای از جمله اولین جرائم رایانه‌ای است که نظام‌های حقوقی کشورهای مختلف نسبت به آن عکس‌العمل قانونی نشان داده‌اند.در سیستم‌های قضایی بسیاری از کشورها مانند آلمان، بریتانیا، ایتالیا، اتریش، فنلاند، دانمارک، نروژ، سوئیس، سوئد، پرتغال، استرالیا و ژاپن، تعاریف قانونی کلاهبرداری کلاسیک محتاج این است که شخص(انسان زنده) فریب بخورد. بنابراین قوانین مربوط به کلاهبرداری کلاسیک در این کشورها شامل مواردی مانند سوءاستفاده ار صندوق‌های پرداخت و سایر صور کلاهبرداری رایانه‌ای که مرتکب صرفاً از طریق سوءاستفاده از رایانه و بدون فریب انسان مال دیگری را می‌برد، نمی‌شود. این

[1] - Computer- related fraud.

کشورها با اصلاح قوانین کیفری خود یا وضع قوانین جدید در مقابل کلاهبرداری رایانه‌ای عکس‌العمل نشان داده‌اند (زیبر، ۱۳۷٦ ب، ص ۱۸)

قوانین جدید کلاهبرداری رایانه‌ای در کشورهای مختلف جهان، شامل مصادیق متعددی از سوءاستفاده‌های مالی رایانه‌ای می‌شوند که با کلاهبرداری کلاسیک شباهت داشته اما با قوانین مربوط به کلاهبرداری کلاسیک قابل مجازات نیستند ، در ذیل به تعدادی از آنها اشاره می‌شود.

الف- سوءاستفاده های رایانه‌ای

در بین سوءاستفاده‌های رایانه‌ای، سوءاستفاده از صورت‌حساب‌های مربوط به دستمزدهای شرکت‌های صنعتی، به‌علاوه سوءاستفاده ازموجودی حساب‌ها و بیلان‌ها در بانک‌ها از طریق تأثیر برعملکرد سیستم‌های رایانه‌ای، عمده‌ترین جرائم هستند. در حال حاضر این نوع سوءاستفاده‌ها در بسیاری از کشورها به‌عنوان کلاهبرداری رایانه‌ای تحت تعقیب و مجازات قرار می‌گیرند، (دزیانی، ۱۳۷۸، ص۳٤). در ایران بعضی از اساتید حقوق این‌گونه اعمال را به سرقت نزدیک‌تر دانسته و گفته‌اند: «...اطلاق عنوان کلاهبرداری به برخی از انواع آنچه بعضاً "کلاهبرداری رایانه‌ای" نامیده شده از قبیل دستکاری شخص در برنامه رایانه‌ای و انتقال پول به حساب خودش از نظر قانون ما خالی از اشکال نمی‌باشد و این‌گونه اعمال شاید به سرقت نزدیکتر باشند تا کلاهبرداری، چرا که نوعی ربایش مال غیر محسوب می‌شود» (میر محمد صادقی، ۱۳۷۸، ص۷۵.) به نظر می رسد اگر دستکاری در برنامه رایانه‌ای منجر به برداشت پول از حساب شرکت‌های خصوصی شود و این کار توسط کارمندانی که حساب‌های شرکت را در اختیار دارند و اموال به آنها سپرده شده باشد، صورت گیرد، ، عمل مزبور مصداق خیانت در امانت است واگر شرکت‌ها دولتی باشند و برداشت پول توسط کارمندان بانک‌های دولتی و یا ادارات دولتی انجام گرفته باشد، مشروط براین که این اموال در اختیار کارمند مربوطه باشد و به نحوی به وی سپرده شده باشد، موضوع منطبق با جرم

اختلاس است. اما در مواردی که حساب‌ها و وجوه در اختیار کارمند نبوده و کارمند مبادرت به برداشت کرده باشد یا اینکه شخصی غیر کارمند مبادرت به برداشت وجوه از اشخاص حقیقی یا اشخاص حقوقی خصوصی یا عمومی کرده باشد، موضوع مشمول خیانت در امانت یا اختلاس یا سرقت نخواهد شد. مرتکبین این موارد تحت شرایطی براساس قسمت اخیر ماده ۲ قانون تشدید مجازات مرتکبین و ارتشاء و اختلاس وکلاهبرداری مصوب ۱۳٦۷ مجمع تشخیص مصلحت نظام، به عنوان"تحصیل مال یا وجه از طریق غیرقانونی" قابل مجازات هستند. البته با توجه به چالش‌ها و نواقص قانونی موجود و نظریات مختلفی که در این زمینه وجود دارد، لازم است که قانونگذار ما نیز مانند قانونگذاران سایر کشورهای جهان به طور شفاف در مقابل آنچه که کلاهبرداری رایانه‌ای نامیده شده است عکس‌العمل قانونی مناسب نشان دهد.

ب- سوءاستفاده از صندوق‌های پرداخت

یکی دیگر از مصادیق جرم کلاهبرداری رایانه‌ای در کشورهای مختلف دنیا، سوءاستفاده‌های متعدد از صندوق‌های پرداخت و ابزارهای پرداختی مشابه است. اگرچه بسیاری از این سوءاستفاده‌ها منجر به مبالغ کمی از خسارت و ضرر شده است، اما آمارها نشان می‌دهد که سوءاستفاده از کارت‌ها از نظر تعداد موارد نسبت به سوءاستفاده‌های کلاسیک خیلی بیشتر است. (زیبر ۱۳۷٦ ب، ص ۱۱۷)

امروزه اشکال سوءاستفاده از صندوق‌های پرداخت، از استفاده ساده از کارت‌های مسروقه و سوءاستفاده از کارت‌ها با کمک رایانه، به ساخت مستقل کپی کارت‌ها تغییر شکل داده است. جدا از کارتهای صندوق پرداخت دیگر کارتهای مغناطیسی مانند کارت‌های تلفن یا کارت‌های مربوط به شرط بندی اسب‌ها نیز مورد سوءاستفاده قرار گرفته‌اند. (همان).

ضرر و زیان کلی حاصل از کلاهبرداری‌های ناشی سوءاستفاده از کارت‌های اعتباری، از حجم وسیعی برخوردار است. در سال ۱۹۸۲ کلاهبرداری‌های ناشی از

سوءاستفاده از کارت‌های اعتباری در آمریکا یک میلیارد دلار خسارت به بار آورده است. درسال۱۹۸۵ خسارت ناشی از سوءاستفاده از کارت‌های اعتباری در انگلستان۵۰ میلیون پوند تخمین زده شده است. (میر محمد صادقی، ۱۳۷۸، ص ص ۳۷و۳۸)

با توجه به تعریفی که سازمان‌های بین‌المللی برای کلاهبرداری رایانه‌ای ارائه داده اند، مصادیق کلاهبرداری رایانه‌ای بسیار فراتر از موارد مذکوراست. در این نوشتار تعریف و عناصر اختصاصی تشکیل‌دهنده جرم کلاهبرداری رایانه‌ای از دیدگاه اسناد و توصیه‌نامه‌های بین‌المللی و مقررات جمهوری اسلامی ایران مورد بحث و بررسی قرار می‌گیرد.

۱-کلاهبرداری رایانه‌ای از دیدگاه اسناد وتوصیه‌نامه‌های بین‌المللی

الف- تعریف کلاهبرداری رایانه‌ای

شباهت کلاهبرداری رایانه‌ای از جهت نتیجه جرم به کلاهبرداری کلاسیک و تفاوت بین آنها از جهت فرایند ارتکاب، باعث شده است که تعریف کلاهبرداری رایانه‌ای از جهاتی مشابه و از جهات دیگر متفاوت با کلاهبرداری کلاسیک باشد. بعضی از سازمان‌های بین‌المللی به منظور آشنایی کشورهای عضو با جرائم رایانه‌ای و اتخاذ سیاست جنایی واحد در مبارزه با این جرائم برخی از مصادیق جرائم رایانه‌ای را تعریف کرده‌اند. کلاهبرداری رایانه‌ای از جمله جرائمی است که سازمان‌های بین‌المللی در جرم انگاری آن اتفاق‌نظر داشته و تعاریفی را برای آن ارائه داده‌اند.

سازمان همکاری اقتصادی و توسعه (OECD)[1] در گزارش سال ۱۹۸٦ خود تحت عنوان "جرائم مرتبط با رایانه، تحلیل سیاست‌های اقتصادی"، کلاهبرداری رایانه‌ای را به شرح زیر تعریف کرده است: کلاهبرداری رایانه‌ای عبارت است از: «وارد کردن، تغییر

[1]– Organisation for Economic cooperation and Development

دادن، پاک کردن یا متوقف کردن داده‌ها یا برنامه‌های رایانه‌ای که به‌طور ارادی و با قصد انتقال غیرقانونی وجوه یا هر چیز با ارزش دیگری صورت گرفته باشد.»

http://www.OECD.org/document/19/02340-2649--34255-1815059-1-1-1-)

(,00.htm

شورای اروپا[1] در توصیه‌نامه شماره R(۸۹)۹ مصوب ۱۹۸۹، کلاهبرداری رایانه‌ای را به شرح زیر تعریف کرده است: «هرگونه وارد کردن، تغییردادن، حذف کردن یا متوقف کردن داده‌ها یا برنامه‌های رایانه‌ای یا دیگر مداخلات در پردازش داده‌های رایانه‌ای که به قصد تحصیل امتیاز غیر قانونی برای خود یا شخص دیگر انجام شود و بر نتیجه پردازش اثر گذارد و به این طریق موجب ایجاد زیان اقتصادی یا تصرف مال دیگری شود.» کلاهبرداری رایانه‌ای نامیده می‌شود.

.(http://www.convention.coe.int/teraty/en/reports/html/185. htm)

سازمان همکاری و توسعه اقتصادی در ۲۱ دسامبر ۱۹۵۹ با امضای اعلامیه مشترکی که رؤسای دولتهای فرانسه، ایالات متحده امریکا، جمهوری فدرال آلمان و بریتانیا امضاء نمودند با هدف توسعه کشورهای توسعه نیافته و گسترش روابط بازرگانی بین‌المللی ایجاد شد. در حال حاضر این سازمان متشکل از مهمترین کشورهای دارای اقتصاد آزاد است. علاوه بر کشورهای اروپایی عضو ، کشورهای کانادا ، ژاپن ، استرالیا و زلاند نو ، دیگر اعضای این سازمان هستند.

۱- مسأله جرم رایانه‌ای درسال ۸۶- ۱۹۸۵ در برنامه کار کمیته اروپایی مشکلات ناشی از جرم (وابسته به شورای اروپا) قرار گرفت. این کمیته خود کمیته‌ای تخصصی به نام"کمیته منتخب کارشناسان جرم رایانه‌ای" را برای مطالعه این موضوع تشکیل داد. "کمیته منتخب کارشناسان جرم رایانه‌ای" کار خود را در سال ۱۹۸۵ میلادی آغاز کرد. مطالعات و تحقیقات انجام شده تاکنون منتهی به مصوبات مهم و قابل توجهی شده است توصیه‌نامه شماره ۹ (۸۹) R شورای اروپا از جمله این مصوبات است. این توصیه نامه در ۱۳ سپتامبر ۱۹۸۹ از سوی هیأت وزرای شورای اروپا پذیرفته شد و شامل رهنمودهایی برای قانونگذاران ملی در مورد جرم رایانه‌ای است. توصیه‌نامه مذکور حاوی ۵ فصل و ۳ ضمیمه می‌باشد. فصل اول این توصیه‌نامه در مورد ملاحظات کلی (از جمله مربوط به سیاست جنایی) است، در فصل دوم دو فهرست اجباری و اختیاری از جرائم رایانه‌ای، در فصل سوم مشکلات مربوط به آئین دادرسی، در فصل چهارم جنبه‌های بین‌المللی و در فصل پنجم آن دیگر جنبه‌های جرم رایانه‌ای ذکر شده است.

به موجب ماده ۸ کنوانسیون جرائم سایبر[۱]، کلاهبرداری رایانه‌ای عبارت است از:"هرگونه وارد کردن، تغییردادن، حذف یا متوقف کردن داده‌های رایانه‌ای یا اخلال در عملکرد یک سیستم رایانه‌ای که به صورت عمدی و بدون حق و به قصد تحصیل متقلبانه یا ناروا و بدون حق یک منفعت اقتصادی برای خود یا دیگری انجام گرفته و موجب وارد شدن ضرر مالی به دیگری[۲] شود."[۳].

(http://conventions.coe.int/treaty/en/treatys/html/185.htm)

آیا با توجه به معیارهایی که سازمان‌های بین‌المللی برای جرم انگاری کلاهبرداری رایانه‌ای ارائه داده‌اند، می‌توان قوانین مربوط به کلاهبرداری کلاسیک را در مورد آنچه که کلاهبرداری رایانه‌ای نامیده می‌شود، اعمال کرد؟ برای پاسخ به این سؤال اجزاء مادی تشکیل دهنده جرم کلاهبرداری کلاسیک را بر اساس ماده۱ قانون تشدید

۱- پیش‌نویس کنوانسیون جرائم سایبر توسط کمیته‌ای به نام" کمیته متخصصین جرائم سایبر" (PC-CY) تهیه شد. " کمیته متخصصین جرائم سایبر" در ٤ فوریه ۱۹۹۷ توسط کمیته وزرای شورای اروپا تشکیل گردید و کار خود را در آوریل ۱۹۹۷ شروع کرد. نسخه اولیه پیش‌نویس کنوانسیون مذکور در آوریل ۲۰۰۰ تهیه و منتشر گردید . نسخه نهایی پیش‌نویس و گزارش توجیهی آن در ژوئن ۲۰۰۱ تهیه وجهت تأیید تسلیم کمیته اروپایی مشکلات ناشی از جرم شد و پس از تأیید آن مرجع، جهت تصویب و امضاء به کمیته وزرای شورای اروپا تسلیم گردید و نهایتاً در ۲۳ سپتامبر ۲۰۰۱ در بوداپست به تصویب و امضای کشورهای عضو شورای اروپا و چهار کشور آمریکا، کانادا، آفریقای جنوبی و ژاپن رسید. این سند از آن به بعد مبنای روابط بین اعضای شورا و سایر کشورهای جهان، می‌باشد. این کنوانسیون دارای ٤ فصل است. فصل یکم آن راجع به تعریف واژه‌های تخصصی، فصل دوم در مورد حقوق جزای ماهوی(انواع جرائم رایانه‌ای) و حقوق جزای شکلی (آیین دادرسی کیفری)، فصل سوم در خصوص همکاری‌های بین‌المللی و فصل چهارم آن در مورد مقررات مربوط به امضاء ،لازم‌الاجرا شدن و الحاق به کنوانسیون است.

2 - Loss of property to another.

۳- ماده ۸ کنوانسیون جرائم سایبر(مصوب۲۳ اکتبر۲۰۰۱بوداپست)درخصوص جرم انگاری کلاهبرداری رایانه‌ای مقرر داشته است:«کشورهای عضو کنوانسیون جرائم سایبر باید اقدام به وضع قوانین و مقرراتی نمایند که ضرورتاً براساس حقوق داخلی خود هرگونه: الف- ورود، تغییر، حذف یا متوقف کردن داده‌های رایانه‌ای، ب- اخلال در عملکرد یک سیستم رایانه‌ای را که به صورت عمدی و بدون حق و به قصد تحصیل متقلبانه یا ناروا و بدون حق یک منفعت اقتصادی برای خود یا دیگری انجام گرفته و موجب وارد شدن ضرر مالی به دیگری شود، جرم-انگاری نماید.

مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری مورد بررسی قرار داده و با اجزاء مادی تشکیل دهنده جرم کلاهبرداری رایانه‌ای موضوع ماده ۸ کنوانسیون جرائم سایبر مقایسه می‌کنیم. ماده۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری، مقررداشته:

«هرکس از راه حیله و تقلب مردم را به وجود شرکت‌ها یا تجارتخانه‌ها یا کارخانه‌ها یا مؤسسات موهوم یا به داشتن اموال و اختیارات واهی فریب دهد، یا به امور غیرواقع امیدوار نماید یا از حوادث و پیش‌آمدهای غیرواقع بترساند و یا اسم یا عنوان مجعول اختیار کند و با یکی از وسایل مذکور یا وسایل تقلبی دیگر وجوه و یا اموال و یا اسناد یا حوالجات یا قبوض یا مفاصاحساب و امثال آنها را تحصیل کرده و از این راه مال دیگران را ببرد، علاوه بر رد مال به صاحبش به حبس از یک تا هفت سال و پرداخت جزای نقدی معادل مالی که اخذ کرده است، محکوم می‌شود.»

بر اساس ماده ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری، اجزاءمادی تشکیل دهنده جرم کلاهبرداری کلاسیک عبارتند از:۱- توسل به وسایل متقلبانه،۲- اغفال دیگری،۳- تحصیل سند یا وجه یا مال، ٤- بردن مال غیر.

بر اساس ماده ۸ کنوانسیون جرائم سایبر، اجزاء مادی تشکیل دهنده جرم کلاهبرداری رایانه‌ای عبارت اند از: ۱- مداخله بدون حق در داده‌ها یا سیستم‌های رایانه‌ای، ۲- وارد کردن ضرر به دیگری.

همانگونه که ملاحظه می‌شود، ماده یک قانون تشدید مجازات مرتکبین اختلاس و ارتشاء وکلاهبرداری، برخلاف ماده ۸ کنوانسیون جرائم سایبر، عنصر"اغفال" به معنی فریب خوردن قربانی جرم را برای تحقق کلاهبرداری کلاسیک لازم می‌داند. بنابراین یکی از تفاوت‌های اساسی بین کلاهبرداری رایانه ای وکلاهبرداری کلاسیک این است که تحقق کلاهبرداری کلاسیک مستلزم اغفال و فریب خوردن قربانی جرم است. در کلاهبرداری کلاسیک عنصر اغفال موجب می‌شود که قربانی جرم مال خود را دو دستی و حتی با التماس و اصرار زیاد تقدیم مرتکب کند. در حالی که کلاهبرداری رایانه‌ای

بدون فریب قربانی جرم و از طریق مداخله ناروا در داده‌های رایانه‌ای یا عملکرد سیستم رایانه‌ای محقق می‌شود و همین امر باعث شده است که قوانین مربوط به کلاهبرداری کلاسیک در مورد جرم کلاه‌برداری رایانه‌ای قابل اعمال نباشد.

ب- رکن مادی

با توجه به ماده ۸ کنوانسیون جرائم سایبر،: رکن مادی جرم کلاهبرداری رایانه‌ای از رفتار مرتکب، موضوع جرم، وسیله جرم، و نتیجه جرم تشکیل شده است.که به شرح زیر مورد بررسی قرار می‌گیرند:

رفتار مرتکب

کلاهبرداری رایانه‌ای جرمی است که با فعل مرتکب واقع می‌شود. ماده ۸ کنوانسیون جرائم سایبر، افعالی را که می‌توانند منجر به تحقق جرم کلاهبرداری رایانه‌ای شوند به دو دسته تقسیم نموده است که عبارتند از:

۱- هرگونه وارد کردن، تغییردادن، حذف، یا متوقف کردن بدون حق داده‌های رایانه‌ای که منجر به خسارت مالی به دیگری شود.

۲- هرگونه اخلال بدون حق در عملکرد سیستم رایانه‌ای که منجر به خسارت مالی دیگری شود.

اصطلاح "وارد کردن داده‌های رایانه‌ای"[1] هم شامل وارد کردن داده‌های غیرصحیح وهم شامل وارد کردن غیرمجاز داده‌های صحیح به یک سیستم رایانه‌ای می‌باشد (دزیانی، ۱۳۷٦،ص ۱۳۲). اصطلاح مذکور هم شامل وارد کردن داده‌ها از طریق صفحه کلید و سایر تجهیزات مربوط به واحد ورودی رایانه است که از نزدیک صورت می‌گیرد، و هم شامل ارسال داده از یک رایانه راه دور به رایانه دیگر متصل به شبکه است.

[1] - Input of computer data.

اصطلاح "تغییر داده‌های رایانه‌ای"[۱] به معنی تبدیل کردن داده‌ها است. "حذف داده‌های رایانه‌ای"[۲] برابر با تخریب یک شئ فیزیکی و محسوس می‌باشد. این عمل آنها را تخریب کرده و باعث می‌شود تا قابل تشخیص و فهم نباشند. "متوقف کردن داده-های رایانه‌ای"[۳] به معنای هر فعلی است که از فراهم بودن داده‌ها برای فردی که حق دسترسی به رایانه دارد جلوگیری می‌کند یا جریان دسترسی به اطلاعات را قطع می‌کند. Convention on cybercrime, 2001, P.87)

"اخلال در عملکرد سیستم رایانه‌ای"[٤] نیز یک عنوان کلی است که شامل اعمال و افعال زیادی می‌شود. گزارش توجیهی کنوانسیون جرائم سایبر (ش. ۸۷) در خصوص معنی اصطلاح اخلال در عملکرد سیستم رایانه‌ای اشعار داشته: «به منظور حصول اطمینان از اینکه کلاهبرداری شامل همهٔ انواع دستکاری‌های مربوطه می‌شود، عناصر تشکیل‌دهنده بند الف ماده ۸ کنوانسیون شامل وارد کردن، تغییر دادن، حذف کردن و متوقف کردن داده‌ها به وسیله عنوان کلی اخلال در عملکرد سیستم رایانه‌ای، موضوع بند ب ماده ۸ کنوانسیون، تکمیل شده است. عنوان کلی اخلال در عملکرد سیستم رایانه‌ای، شامل اعمالی نظیر انواع دستکاری سخت‌افزارها، جلوگیری از خروج داده‌ها به صورت پرینت (چاپ) و تأثیر گذاشتن بر ثبت و ذخیره یا جریان داده‌ها یا توانایی اجرای برنامه‌ها می‌باشند.» بنابراین فعل مرتکب در کلاهبرداری رایانه‌ای عبارت است از انواع دستکاری‌های متقلبانه رایانه‌ای که در بندهای الف و ب ماده ۸ کنوانسیون جرائم سایبر احصاء شده‌اند.

1- Alteration of computer data.

2- Deletion of computer data.

3- Suppression of computer data.

4 -Interference with the function of computer system.

موضوع جرم

موضوع جرم کلاهبرداری رایانه‌ای مانند جرم کلاهبرداری کلاسیک،"اموال متعلق به‌غیر" است. اما تفاوتی که اموال موضوع کلاهبرداری رایانه‌ای با اموال موضوع کلاهبرداری کلاسیک دارد این است که اموال موضوع کلاهبرداری رایانه‌ای در هنگام کلاهبرداری به طور مستقیم وابسته به داده ها و سیستم‌های رایانه‌ای هستند. به عبارت دیگر با مسامحه در تعبیر می‌توان گفت اموال موضوع کلاهبرداری رایانه‌ای باید بدون واسطه در اختیار یا تصرف[1] سیستم‌های رایانه‌ای باشند تا بتوانند موضوع جرم کلاهبرداری رایانه‌ای واقع شوند. در کلاهبرداری رایانه‌ای مرتکب با تأثیر بر پردازش داده‌ها و عملکرد سیستم رایانه‌ای به طور مستقیم اموال را از حسابی به حساب دیگر منتقل و یا از تصرف یک سیستم خارج و آن را تصاحب می‌کند. گزارش توجیهی کنوانسیون جرائم سایبر(ش ۸۸) در این خصوص اشعار داشته: «دستکاری‌های متقلبانه در صورتی جرم‌انگاری می‌شوند که به" طور مستقیم" منجر به وارد آمدن ضرر اقتصادی یا موجب از بین رفتن تصاحب مالکانه دیگری بر اموالش شوند.»

اگر مداخله در داده‌ها و سیستم رایانه‌ای به طور مستقیم موجب تصاحب یا انتقال اموال دیگری به مرتکب یا شخص دلخواه وی نشود و یک انسان، واسطه تصاحب ویا انتقال اموال قرار گیرد، کلاهبرداری رایانه‌ای تحقق نخواهد یافت در این صورت آنچه که تحقق یافته جعل رایانه‌ای است که منجر به کلاهبرداری کلاسیک می‌شود. به عنوان مثال در بعضی از بانک‌ها عملیات بانکی را به صورت ترکیبی از عملیات رایانه‌ای و دستی انجام می‌دهند، به نحوی که مشتری با واردکردن کارت بانکی رایانه‌ای خود به

[1] واژه‌های "اختیار" و "تصرف" معمولاً برای انسان به کار برده می شوند ولی همان‌گونه که گفته شد بسیاری از اموری که سابقا به وسیله انسان انجام می شد امروزه توسط رایانه‌ها و سایر دستگاه‌های خودکار انجام می شود. بنابراین یک دستگاه مخصوص فروش اجناس یا یک دستگاه خودپرداز بانک کالاها و وجوه را برای فروش یا پرداخت به مشتری در اختیار یا تصرف دارد. مشتری با انجام عملیاتی کالا و یا پول را از تصرف این ماشین‌ها خارج می کند.

یک دستگاه ورودی مخصوص، مبلغ مورد درخواست را در سیستم رایانه‌ای تایپ کرده و متصدی صندوق با مشاهده خروجی سیستم و شناسایی مشتری مبلغ مورد درخواست را به صورت دستی به وی پرداخت می‌کند. حال اگر مشتری بانک یا شخصی که کارت مشتری را پیدا کرده است، با کارت بانکی که در دست دارد و یا با دستکاری دستگاه یا وارد کردن داده‌های کذب وارد حساب شخص دیگری شود و مبلغی را از حساب وی کسر کند و از صندوق‌دار بخواهد که مبلغ مذکور را به وی پرداخت کند، صندوق‌دار هم که از اقدامات متقلبانه بی‌اطلاع است، با این تصور که آن شخص ذی‌حق است مبلغ مذکور را به وی پرداخت کند، اقدامات وی تحت عناوین جعل رایانه‌ای وهمچنین استفاده از سند مجعول (کلاهبردای کلاسیک) قابل مجازات است. در اینجا کلاهبرداری رایانه‌ای تحقق نیافته است. چرا که یک انسان (صندوق‌دار) بین مرتکب و رایانه قرار گرفته است. و آن انسان از طریق اقدامات متقلبانه رایانه ای اغفال شده است و مبلغ مورد درخواست را به مرتکب پرداخت کرده است. اما اگرشخصی به یکی از صندوق-های خودپرداز بانک مراجعه و با دستکاری در کارت بانکی و یا مداخله درسیستم صندوق، مبلغی را دریافت نماید، عمل وی مصداق کلاهبرداری رایانه‌ای است چرا که مال مورد کلاهبرداری به سیستم رایانه ای سپرده شده است ومرتکب با مداخله متقلبانه در داده یا سیستم مال را به‌طور مستقیم و بدون واسطه قرار گرفتن انسان دیگری تصاحب نموده است.

اموال موضوع کلاهبرداری رایانه ای ممکن است به صورت اموال ملموس ویا به صورت داده‌های رایانه‌ای (اموال غیرملموس) باشند. مثلاً زمانی که شخصی با ورود به سیستم رایانه‌ای یک بانک،وجوهی را که به صورت داده های رایانه ای درحساب بانکی شخص دیگری ذخیره شده است به حساب خود یا حساب شخصی دیگر واریز می‌کند، در این حالت داده‌های رایانه‌ای که نمادی از اموال هستند، به جای اموال جابجا و از حساب شخصی به حساب شخص دیگر منتقل شده‌اند. همچنین ممکن است اموال ملموس مانند پول نقد (اسکناس) یا کالا به صندوق‌های پرداخت بانک یا

دستگاه‌های رایانه‌ای مخصوص فروش سپرده شده باشد ومرتکب با دستکاری متقلبانه داده‌های رایانه‌ای ویا مداخله متقلبانه در عملکرد سیستم رایانه‌ای تعبیه شده در آن دستگاه‌ها ویا جعل کارت‌های مخصوص به طور مستقیم، پول یا کالاهای سپرده شده به دستگاه‌های مزبور را تحصیل و تصاحب کند.

گزارش توجیهی کنوانسیون جرائم سایبر(ش ۸۸) در خصوص انواع اموال موضوع جرم کلاهبرداری رایانه‌ای اشعار داشته است: «اصطلاح "از دست دادن اموال" مفهوم گسترده‌ای دارد.این اصطلاح شامل از دست دادن پول، اموال منقول وغیرمنقول دارای ارزش اقتصادی می باشد.»

وسیله ارتکاب جرم

کلاهبرداری رایانه‌ای جرمی است که به وسیله رایانه ارتکاب می‌یابد و بستر ارتکاب آن رایانه است. بنابراین وسیله جرم یعنی رایانه جزئی از اجزاء تشکیل‌دهنده عنصر مادی این جرم محسوب می شود.

نتیجه جرم

جرم کلاهبرداری رایانه‌ای همانند جرم کلاهبرداری کلاسیک از جمله جرائم مقید به نتیجه است. یکی از تفاوت‌های اساسی که موجب تشخیص این جرم از دیگر جرائم رایانه‌ای مانند اخلال در داده[1]، اخلال در سیستم[2] وجعل رایانه‌ای[3] می شود این است که نتیجه این جرم با جرائم مزبور فرق دارد.

نتیجه جرم کلاهبرداری رایانه‌ای ضرر و زیانی است که بدون حق از طریق خارج شدن مال از ید مالکانه مالک به صاحب مال وارد می‌شود. با مقایسه نتیجه جرم

1- Data interference.

2- System interference.

3- Computer forgery.

کلاهبرداری رایانه‌ای با سایر جرائمی که اعمال تشکیل‌دهنده آنها با این جرم تقریباً مشترک است، تفاوت بین آنها به آسانی مشخص می شود. نتیجه جرم اخلال در داده، صرف تخریب ویا آسیب وارد شدن به داده‌های رایانه‌ای است. نتیجه جرم اخلال درسیستم، ایجاد وقفه واختلال جدی در کارکرد سیستم رایانه‌ای است. نتیجه جرم جعل رایانه‌ای، ایجاد یک سند الکترونیکی غیرصحیح است. اما نتیجه جرم کلاهبرداری رایانه‌ای ضرر وزیان مالی بالفعل حاصل از هرگونه دستکاری متقلبانه در داده‌ها یا سیستم رایانه‌ای است که بدون حق به صاحب مال وارد می‌شود. یکی از تفاوت‌های کلاهبرداری رایانه‌ای موضوع کنوانسیون جرائم سایبر، با کلاهبرداری کلاسیک در حقوق ایران، این است که در حقوق ایران مرتکب باید به مال دیگری دست یابد و از این طریق به دیگری ضرروارد آورد تاجرم کلاهبرداری تحقق یابد، اما در کلاهبرداری رایانه‌ای موضوع کنوانسیون جرائم سایبر اگر مرتکب قصد کسب منفعت مالی داشته باشد و موجب ضرر صاحب مال شود حتی اگر مالی به دست نیاورده باشد جرم کلاهبرداری رایانه ای تحقق خواهد یافت.

گزارش توجیهی کنوانسیون جرائم سایبر (ش ۸۸) در خصوص نتیجه جرم کلاهبرداری رایانه‌ای اشعار داشته است: «دستکاری‌های متقلبانه در صورتی جرم انگاری می‌شوند که به‌طور مستقیم منجر به وارد آمدن ضرر اقتصادی و یا موجب از بین رفتن تصاحب مالکانه دیگری بر اموالش شوند و مرتکب با هدف کسب سود اقتصادی غیرقانونی برای خود یا شخص دیگر عمل کرده باشد و اصطلاح "از دست دادن اموال"، مفهوم گسترده‌ای دارد. این اصطلاح شامل از دست دادن پول، اموال منقول وغیرمنقول دارای ارزش اقتصادی می باشد.»

اصطلاح" بدون حق" در ماده ۸ کنوانسیون جرائم سایبر، دو بار به کار رفته است.یک بار درمورد اقداماتی که رفتار مجرمانه جرم کلاهبرداری را تشکیل می‌دهند و یک بار در مورد نتیجه جرم کلاهبرداری. گزارش توجیهی کنوانسیون جرائم سایبر در این خصوص اشعار داشته: «اعمال مربوط به این جرم باید" بدون حق" ارتکاب یافته

باشد و منافع اقتصادی نیز باید" بدون حق" تحصیل شده باشد تا جرم کلاهبرداری تحقق یابد.»

ج-رکن معنوی

اجزاء تشکیل‌دهنده رکن معنوی کلاهبرداری رایانه‌ای عبارت اند از: علم مرتکب، سوءنیت عام وسوءنیت خاص.

علم مرتکب

به موجب ماده ۸ کنوانسیون جرائم سایبر یکی از شرایط کلاهبرداری رایانه‌ای این است که رفتارهای مجرمانه که جزئی از عنصر مادی این جرم را تشکیل می‌دهند باید بدون حق باشند، همچنین ضرر و زیان اقتصادی که مجرم در اثر اقدامات مزبور به صاحب مال وارد می‌کند، باید بدون حق باشند تا جرم کلاهبرداری تحقق پیدا کند، بنابراین علم مرتکب به بدون حق بودن اعمال و بدون حق بودن نتیجه این اعمال، شرط تحقق کلاهبرداری رایانه‌ای بوده وجزئی از اجزاء رکن معنوی آن را تشکیل می دهد. چنانچه مرتکب اشتباهاً فکر کند که حق انجام اعمال و دستیابی به نتیجه را دارد هر چند که عمداً مرتکب اعمال مذکور شود، جرم محقق نخواهد شد. منظور از اشتباه جهل به موضوع است نه جهل به قانون، چرا که جهل به قانون رافع مسئولیت کیفری نیست.

سوءنیت عام

بنا بر صراحت ماده ۸ کنوانسیون جرائم سایبر، کلاهبرداری رایانه‌ای جرمی عمدی است. بنابراین تحقق آن نیاز به سوءنیت عام مرتکب دارد. سوءنیت عام مرتکب عبارت است از خواستن ارتکاب یکی از اعمال مندرج در بندهای (الف) یا (ب) ماده ۸

کنوانسیون که منجر به کلاهبرداری می‌شوند. اگر مرتکب در اثر بی‌احتیاطی یا غفلت یکی از اعمال مذکور را انجام داده باشد، حتی اگر منجر به نتیجه مجرمانه هم بشود، جرم کلاهبرداری رایانه‌ای تحقق نخواهد یافت.

سوءنیت خاص

جرم کلاهبرداری رایانه‌ای یک جرم مقید به نتیجه است. شرط تحقق کلاهبرداری رایانه‌ای این است که مرتکب علاوه بر خواستن عملی که منجر به کلاهبرداری رایانه‌ای می‌شود نتیجه جرم (ضرر صاحب مال) را نیز بخواهد. اگر مرتکب بدون اینکه قصد نتیجه را داشته باشد، اعمال مذکور در ماده ۸ را انجام داده باشد، عمل او کلاهبرداری رایانه‌ای محسوب نمی‌شود. علاوه بر آن باید اعمال مذکور در ماده ۸ کنوانسیون را با قصد متقلبانه یا ناروای تحصیل منفعت اقتصادی برای خود یا دیگری انجام داده باشد. بنابراین سوءنیت خاص در جرم کلاهبرداری رایانه‌ای دارای دو جزء است ۱- خواستن ضرر صاحب مال، ۲- قصد متقلبانه یا ناروای تحصیل سود برای خود. اگر قسمت دوم یعنی قصد متقلبانه تحصیل سود برای خود نباشد، ممکن است این جرم با جرم اخلال در داده‌ها و اخلال در سیستم تداخل پیدا کند.

گزارش توجیهی کنوانسیون جرائم سایبر (ش ۹۰)،درخصوص عنصرمعنوی جرم کلاهبرداری رایانه‌ای اشعار داشته: «جرم کلاهبرداری رایانه‌ای باید به صورت عمدی ارتکاب یافته باشد. عنصر قصد عام در این جرم به عمل دستکاری یا مداخله در سیستم رایانه‌ای که موجب از دست دادن اموال دیگری می‌شود برمی‌گردد. این جرم همچنین نیاز به یک قصد خاص متقلبانه یا ناروای دیگری برای به دست آوردن یک سود اقتصادی یا منفعت دیگری دارد. پس به عنوان مثال اقدامات تجاری با توجه به رقابت بازار که ممکن است برای شخصی ضرر اقتصادی وبرای دیگری سود داشته باشد چون با قصد متقلبانه یا ناروا صورت نمی‌گیرد، مشمول کلاهبرداری رایانه‌ای نمی‌شود.....»

۳- کلاهبرداری رایانه‌ای در قانون تجارت الکترونیکی ایران

در ایران تنها قانونی که در خصوص کلاهبرداری رایانه‌ای وجود دارد، قانون تجارت الکترونیکی مصوب ۱۰/۱۷/ ۱۳۸۲ است. قانون تجارت الکترونیکی شامل هشت عنوان مجرمانه است که کلاهبرداری رایانه‌ای در بستر تجارت الکترونیکی، یکی از این جرائم می‌باشد. باتوجه به توضیحاتی که در مورد رکن مادی و معنوی جرم کلاهبرداری رایانه‌ای از دیدگاه کنوانسیون جرائم سایبر داده شد، در این قسمت از بحث، ارکان تشکیل‌دهنده جرم کلاهبرداری کامپیوتریِ موضوع قانون تجارت الکترونیکی، به طور تطبیقی مورد بررسی قرار می گیرد.

الف- رکن قانونی

قانونگذار ایران با علم به اینکه کلاهبرداری رایانه‌ای با ماده ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری قابل مجازات نیست، در هنگام وضع قانون تجارت الکترونیکی ، کلاهبرداری رایانه‌ای در بستر مبادلات الکترونیکی را جرم انگاری کرده است. ماده ٦۷ قانون تجارت الکترونیکی در مورد جرم کلاهبرداری رایانه‌ای مقرر داشته : «هر کس در بستر مبادلات الکترونیکی با سوءاستفاده و یا استفاده غیرمجاز از (داده پیام)ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف (داده پیام)، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند 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.

تبصره: مجازات شروع به این جرم نیز جرم محسوب و مجازات آن حداقل مجازات مقرر در این ماده می‌باشد.»

ب- رکن مادی

رفتار مرتکب

جرم کلاهبرداری موضوع ماده ٦٧ قانون تجارت الکترونیکی ازجمله جرایمی است که تحقق آن نیاز به فعل مثبت مرتکب جرم دارد. این جرم از جمله جرایم مرکب است که از چهار جزء زیر تشکیل شده است

۱. انجام اعمالی مانند سوءاستفاده و یا استفاده غیرمجاز از (داده پیام)ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر واردکردن، محو کردن، متوقف کردن (داده‌پیام) و مداخله در عملکرد برنامه یا سیستم رایانه‌ای،

۲. فریب دیگری یا گمراهی سیستم‌های پردازش خودکار و نظایر آن،

۳. تحصیل وجوه، اموال یا امتیازات،برای خود یا دیگری،

٤. بردن مال دیگری.

فقدان هر یک از اجزاء فوق، عدم تحقق جرم کلاهبرداری موضوع ماده ٦٧ قانون تجارت الکترونیکی را به دنبال دارد.

اصطلاحات "سوءاستفاده" و "استفاده غیرمجاز" در این قانون تعریف نشده‌اند و معلوم نیست که چرا به‌رغم شباهت این دو اصطلاح، قانون‌گذار از هر دو استفاده کرده است. واژه‌های "داده پیام" و "سیستم رایانه‌ای" و "وسایل ارتباط از راه دور" به موجب ماده ۲ قانون تجارت الکترونیکی تعریف شده‌اند. بند (الف) ماده مذکور در مورد تعریف داده پیام مقرر داشته: «داده پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری، یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.» بند (و) ماده مذکور نیز در خصوص تعریف سیستم رایانه‌ای مقرر داشته: «سیستم رایانه‌ای هر نوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت‌افزاری، نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار (داده پیام) عمل می‌کند.» به موجب بند (ف) ماده مذکور «وسایل

ارتباط از راه دور عبارت از هر نوع وسیله‌ای است که بدون حضور فیزیکی هم‌زمان تأمین‌کننده و مصرف‌کننده جهت فروش کالا و خدمات استفاده می‌شود.»

تعاریفی که ماده ۲ قانون تجارت الکترونیکی از «داده پیام» و «سیستم رایانه‌ای» به عمل آورد، تعریف مجهول به مجهول است چه اینکه در تعاریف مزبور اصطلاحاتی مانند «وسایل الکترونیکی»، «وسایل نوری»، «فناوری‌های جدید اطلاعات»، «پردازش»، «سخت‌افزار»، «نرم‌افزار» وجود دارد که خود نیاز به تعریف دارند. به علاوه اصطلاح «برنامه رایانه‌ای» که در متن ماده ٦٧ قانون مذکور به کار رفته نیاز به تعریف دارد.

یکی ازضعف‌های بزرگ این قانون این است که اصطلاحات فنی و تخصصی را که دارای بار حقوقی هستند تعریف نکرده است. این امر هم موجب اجمال و ابهام و عدم شفافیت قانون مزبور گردیده و هم امکان تفسیرموسع را برای مجریان قانون فراهم کرده است. به هر حال رویه قضایی ودکترین باید با ارائه تعریف دقیق هر یک از اصطلاحات فوق، مانع از تفسیر موسع قانون مذکور شوند. در این راستا با توجه به جنبه بین‌المللی و فرامرزی جرائم فناوری اطلاعات و مخصوصاً جرائم مربوط به تجارت الکترونیکی، نباید از تعاریفی که اسناد بین‌المللی درمورد اصطلاحات مذکور ارائه داده‌اند غافل شد. ماده ۳ قانون تجارت الکترونیکی درمورد نحوه تفسیر مواد و اصطلاحات این قانون مقرر داشته است: «در تفسیر این قانون همیشه باید بر خصوصیت بین‌المللی، ضرورت توسعه، هماهنگی بین کشورها در کاربرد آن و رعایت لزوم حسن‌نیت توجه کرد.» البته خود قانونگذار در هنگام بیان تعریف اصطلاحات این قانون رعایت این مهم را نکرده است. به‌عنوان مثال تعریفی که برای داده پیام ارائه کرده است با تعاریفی که سازمان‌های بین‌المللی برای این اصطلاح ارائه داده‌اند بسیار متفاوت است.

علاوه برسوءاستفاده و یا استفاده غیرمجاز از (داده پیام)ها، برنامه‌ها و سیستم‌های رایانه‌ای که به آنها اشاره شد، افعالی نظیر ورود، محو و توقف داده پیام‌ها و مداخله در عملکرد برنامه‌ها و سیستم‌های رایانه‌ای و غیره نیز ازجمله افعالی هستند که تحت

شرایطی می‌توانند در بستر مبادلات الکترونیکی منجر به جرم کلاهبرداری رایانه‌ای موضوع ماده ٦٧ قانون تجارت الکترونیکی شوند.

کلاهبرداری موضوع ماده ٦٧ قانون تجارت الکترونیکی ایران شباهت‌هایی با کلاهبرداری موضوع ماده ۸ کنوانسیون جرائم سایبر دارد، اما از جهات مختلف نیز با معیارهایی که‌کنوانسیون جرائم سایبر برای تعریف کلاهبرداری رایانه‌ای تعیین کرده است تفاوت دارد. برخی از تفاوت‌های آنها به شرح زیر است.

اولاً به موجب ماده ۸ کنوانسیون جرائم سایبر، رفتارهای مجرمانه‌ای که می‌توانند منجر به کلاهبرداری رایانه‌ای شوند حصری هستند، این اعمال عبارتند از: ورود، تغییر، حذف یا متوقف کردن داده‌های رایانه‌ای یا اخلال در عملکرد یک سیستم رایانه‌ای. اما به موجب ماده٦٧ قانون تجارت الکترونیکی رفتارهای مجرمانه‌ای که می‌توانند منجر به کلاهبرداری رایانه‌ای شوند تمثیلی بوده و عبارت اند از سوءاستفاده و یا استفاده غیرمجاز از داده پیام‌ها، برنامه‌ها و سیستم‌های رایانه‌ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف داده پیام، مداخله در عملکرد برنامه یا سیستم رایانه‌ای و غیره.

ثانیا اعمالی که به عنوان رفتار مجرمانه جرم کلاهبرداری رایانه‌ای در ماده ٦٧ قانون تجارت الکترونیکی از آنها نام برده شده است، در صورتی منجر به کلاهبرداری می‌شوند که یا موجب فریب دیگران یا سبب گمراهی سیستم‌های پردازش خودکار و نظایر آن شود. بنابراین فریب دیگران و یا گمراهی سیستم‌های پردازش خودکار، جزء رفتار مجرمانه در جرم کلاهبرداری رایانه‌ای موضوع ماده ٦٧ قانون تجارت الکترونیکی است. در صورتی که عنصر فریب و یا گمراه کردن سیستم جزء عناصر جرم کلاهبرداری رایانه‌ای موضوع ماده ۸ کنوانسیون جرایم سایبر نیست. علت گرایش کشورهای مختلف به جرم‌انگاری کلاهبرداری رایانه‌ای محض این است که این جرم بدون نیاز به فریب یک انسان تحقق می‌یابد. در نتیجه عنصر مادی آن با عنصر مادی کلاهبرداری رایانه‌ای کلاسیک متفاوت بوده و با قوانین کلاسیک قابل مجازات نیست.

لذا قانونگذاران ناچار شده‌اند قوانین جدیدی برای تعقیب و مجازات کلاهبرداری رایانه‌ای محض وضع کنند. سیاق عبارات ماده ٦۷ قانون تجارت الکترونیکی بیانگر این است که قانونگذار ایران از واقعیت مزبور مطلع بوده است، چه اینکه برای جرم کلاهبرداری رایانه‌ای گمراهی سیستم‌های پردازش خودکار و نظایر آن را جایگزین عنصر "فریب" انسان کرده است. ظاهراً قانونگذار ایران معتقد است و بر این عقیده نیز اصرار دارد که عنصر فریب حتی در کلاهبرداری رایانه‌ای محض لازم است. با این تفاوت که در کلاهبرداری رایانه‌ای محض به جای انسان، سیستم پردازش داده فریب می‌خورد. به نظر می‌رسد که دیدگاه قانونگذار دارای ایرادات و اشکالات اساسی است. زیرا به کار بردن واژه" گمراهی" برای یک موجود بی‌جان از نظر ادبی صحیح نیست، به علاوه سیستم پردازش از نظر علمی به هیچ‌وجه گمراه نمی‌شود. آنچه که یک سیستم ارائه می‌دهد پاسخ به اطلاعاتی است که وارد آن می‌شود. اگر اطلاعات درست به سیستم داده شود پاسخ درست ارائه خواهد داد. اگر با حیله و تقلب اطلاعات غلط وارد سیستم شود، نباید انتظار داشت که سیستم این اطلاعات غلط را نادیده گرفته و پاسخ درستی که مغایر با این اطلاعات است ارائه دهد. اگر شخص با وارد کردن یا حذف یا متوقف کردن داده‌های رایانه‌ای یا مداخله در عملکرد سیستم یا برنامه رایانه‌ای کاری کند که سیستم پردازش به طور خودکار پاسخ محاسبات را غلط ارائه دهد، در اینجا نیز سیستم گمراه نشده است بلکه در لحظه محاسبه اختلال در سیستم یا اختلال در داده‌ها رخ داده است و نام آن را نمی‌توان گمراهی سیستم گذاشت. در حال حاضر ماده ٦۷ قانون تجارت الکترونیکی هم شامل کلاهبرداری کلاسیک و هم شامل کلاهبرداری رایانه‌ای می‌شود. با وجودی که کلاهبرداری کلاسیک ارتکاب یافته به وسیله رایانه با ماده ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری قابل تعقیب و مجازات است، مشخص نیست که چرا قانونگذار در ماده ٦۷ قانون تجارت الکترونیکی متعرض کلاهبرداری کلاسیک رایانه‌ای نیز شده است.

نتیجه اینکه قانونگذار در ماده ٦٧ قانون تجارت الکترونیکی نه تنها نتوانسته است کلاهبرداری رایانه‌ای محض را به درستی جرم‌انگاری کند بلکه موجب شده است که در حال حاضر دو نوع مجازات برای کلاهبرداری کلاسیک رایانه‌ای وجود داشته باشد.۱- مجازات موضوع ماده ٦٧ قانون تجارت الکترونیکی برای کلاهبرداری کلاسیک رایانه‌ای ارتکاب یافته در بستر مبادلات الکترونیکی، ۲- مجازات موضوع ماده ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری، برای کلاهبرداری‌های کلاسیک رایانه‌ای ارتکاب یافته در سایر بسترها.

ثالثاً تفاوت دیگر جرم کلاهبرداری رایانه‌ای موضوع ماده ٦٧ قانون تجارت الکترونیکی با کلاهبرداری موضوع ماده ۸ کنوانسیون جرائم سایبر از این جهت است که تحقق جرم کلاهبرداری موضوع ماده ۸ کنوانسیون جرائم سایبر مستلزم تحصیل وجوه، اموال یا امتیازات مالی نیست. اگر مرتکب اقداماتی مانند ورود، محو، تغییر و توقف بدون حق داده‌های رایانه‌ای یا اخلال بدون حق در عملکرد سیستم رایانه‌ای را به قصد تحصیل بدون حق و متقلبانهٔ یک منفعت اقتصادی برای خود یا دیگری انجام داده باشد و موجب از دست رفتن اموال دیگری شود، ولو اینکه مرتکب منفعت مالی برای خود و یا دیگری تحصیل نکرده باشد، جرم کلاهبرداری تحقق می‌یابد. اما به موجب ماده ٦٧ قانون تجارت الکترونیکی مرتکب باید از طریق اقداماتی مانند وارد کردن، محوکردن، تغییردادن و متوقف کردن بدون حق داده‌های رایانه‌ای یا اخلال بدون حق در عملکرد سیستم رایانه‌ای وجوه، اموال یا امتیازات مالی برای خود یا دیگران تحصیل کند و از این طریق مال دیگری را ببرد تا جرم کلاهبرداری رایانه‌ای تحقق پیدا کند.

موضوع جرم

موضوع کلاهبرداری رایانه‌ای مانند کلاهبرداری کلاسیک "اموال متعلق به شخص دیگر" است. با این تفاوت که اموال موضوع کلاهبرداری رایانه‌ای برخلاف اموال

موضوع کلاهبرداری کلاسیک، ارتباط ناگسستنی با داده‌های رایانه‌ای دارند. قبلاً توضیحات لازم در این خصوص داده شد.

وسیله جرم

کلاهبرداری رایانه‌ای جرمی است که به وسیله رایانه ارتکاب می‌یابد و بستر ارتکاب آن رایانه است. بنابر این وسیله جرم یعنی رایانه جزء اجزاءتشکیل دهنده عنصر مادی این جرم محسوب می شود.

نتیجه جرم

نتیجه جرم کلاهبرداری موضوع ماده ٦٧ قانون مجازات الکترونیکی عیناً مانند نتیجه جرم در کلاهبرداری کلاسیک است و آن عبارت است از بردن مال دیگری است.در اینجا اشاره به این نکته را لازم می‌دانم که باید بین دو مقوله تحصیل وجوه یا اموال و مال دیگری را بردن قائل به تفکیک شد چراکه تحصیل وجوه یا اموال جزء افعال مجرمانه تشکیل دهنده جرم کلاهبرداری است. اما مال دیگری را بردن یعنی به دیگری ضرر وارد کردن جزء نتیجه جرم کلاهبرداری است. اگر کسی از راه وارد کردن، محوکردن، تغییردادن و متوقف کردن بدون حق داده‌های رایانه‌ای اموالی تحصیل کند که مربوط به خودش باشد، در این صورت به‌رغم تحصیل مال، کلاهبردار محسوب نمی‌شود چرا که به موجب ماده ٦٧ قانون تجارت الکترونیکی بردن مال دیگری لازمه تحقق کلاهبرداری است و در این فرض مرتکب مال دیگری را نبرده است بلکه مال خود را برده است.

مجازات جرم

به موجب ماده ٦٧ قانون تجارت الکترونیکی مجازات جرم کلاهبرداری رایانه‌ای، حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال مأخوذه است. با توجه به

اینکه مجازات مقرر در ماده ٦٧ قانون تجارت الکترونیکی هم مربوط به کلاهبرداری رایانه‌ای وهم کلاهبرداری کلاسیک ارتکاب یافته از طریق رایانه است و در عین حال کلاهبرداری کلاسیک ارتکاب یافته از طریق رایانه با ماده ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری نیز قابل مجازات است؛ بنا براین در حال حاضر دو نوع مجازات برای کلاهبرداری کلاسیک ارتکاب یافته از طریق رایانه وجود دارد. با این توضیح که اگر کسی در بستر مبادلات الکترونیکی با سوءاستفاده از سیستم‌ها یا داده‌های رایانه‌ای، دیگری را بفریبد و مال او را ببرد، به موجب ماده ٦٧ قانون تجارت الکترونیکی مستوجب یک تا سه سال حبس است. لیکن اگر با سوءاستفاده از سیستم‌ها یا داده‌های رایانه‌ای در سایر بسترها دیگری را بفریبد و مال او را ببرد، به موجب ماده ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری مستوجب یک تا هفت سال حبس است. مشخص نیست که چرا قانونگذار ایران برای کلاهبرداری رایانه‌ای در بستر تجارت الکترونیکی مجازات کمتری از کلاهبرداری موضوع ماده۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری تعیین کرده است. این در حالی است که در کشورهای دیگر برای نوع رایانه‌ای جرائم، مجازات بیشتری از نوع کلاسیک آن تعیین کرده‌اند و دلیل آن این است که ارتکاب جرائم رایانه‌ای هزینه کمتر و خسارت بیشتری به دنبال دارد.

ج-رکن معنوی جرم

عنصر معنوی جرم کلاهبرداری رایانه‌ای موضوع ماده ٦٧ قانون تجارت الکترونیکی، تقریباً مانند عنصر معنوی جرم کلاهبرداری موضوع ماده یک قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری است. بنابراین عنصر معنوی این جرم از سه جزء علم مرتکب، سوءنیت عام و سوءنیت خاص تشکیل شده است. مرتکب باید علم

به متقلبانه بودن اعمالی که منجر به کلاهبرداری رایانه‌ای می‌شود، داشته باشد. همچنین عمداً اعمالی را که منجر به کلاهبرداری رایانه‌ای می‌شوند انجام دهد، چه اینکه اصل بر عمدی بودن جرائم است مگر اینکه قانونگذار بر غیرعمدی بودن جرمی تصریح کرده باشد. سوءنیت عام مرتکب جرم کلاهبرداری رایانه‌ای موضوع ماده ٦٧ قانون تجارت الکترونیکی عبارت است از اینکه مرتکب انجام اعمال مذکور در ماده ٦٧ را اراده کرده و خواسته باشد. سوءنیت خاص در جرم کلاهبرداری رایانه‌ای موضوع ماده ٦٧ قانون تجارت الکترونیکی، قصد نتیجه جرم و به عبارت دیگر قصد بردن مال دیگری است. انگیزه تاثیری در تحقق این جرم ندارد و مرتکب باید اعمال مذکور در ماده ٦٧ قانون تجارت الکترونیکی را به قصد بردن مال غیر انجام داده باشد تا کلاهبرداری محقق شود.

۴- کلاهبرداری رایانه‌ای در پیش‌نویس قانون جرایم رایانه‌ای[۱]

ماده ۸ پیش نویس قانون جرایم رایانه‌ای در مورد کلاهبرداری مقرر داشته است: «هر کس از سیستم‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن تغییر، محو، ایجاد، توقف داده‌ها، یا اخلال در عملکرد سیستم سوءاستفاده نماید و از این طریق وجه یا مال یا خدمات مالی و یا امتیازات مالی برای خود یا دیگری تحصیل کند کلاهبردار محسوب و به مجازات مقرر برای کلاهبرداری محکوم خواهد شد.

ماده ۸ پیش‌نویس قانون جرائم رایانه‌ای دارای اشکالات زیر است:

۱ـ منوط و مقید کردن کلاهبرداری رایانه‌ای به احراز "سوءاستفاده از سیستم‌های رایانه‌ای یا مخابراتی" صحیح به نظر نمی‌رسد. چه اینکه معنی اصطلاح سوءاستفاده از سیستم‌های رایانه‌ای و مخابراتی روشن و مشخص نمی‌باشد. هیچ‌یک از اسناد بین‌المللی مربوط به جرائم رایانه‌ای نیز احراز سوءاستفاده از سیستم‌های رایانه‌ای را شرط تحقق کلاهبرداری رایانه‌ای ندانسته‌اند. در ماده ۸ کنوانسیون جرائم سایبر به جای اصطلاح "سوءاستفاده از سیستم‌های رایانه‌ای" اصطلاح " [استفاده] بدون حق"

۱- مرکز مطالعات راهبردی توسعه قضایی قوه قضاییه در اواخر سال ۱۳۸۱ اقدام به تشکیل کمیته مبارزه با جرایم رایانه‌ای جهت تهیه لایحه قانونی جرایم رایانه ای نمود. کمیته مزبور پیش نویس قانون جرایم رایانه‌ای و گزارش توجیهی آن را در خرداد سال ۱۳۸۳ تهیه کرده است. پیش نویس قانون جرایم رایانه‌ای در خرداد سال۱۳۸۳ در یک همایش تخصصی تحت عنوان "همایش بررسی ابعاد حقوقی فناوری اطلاعات"، مورد بحث و بررسی قرار گرفت و از طریق رسانه‌های عمومی از حقوقدانان سراسر کشور خواسته شد تا پیشنهادات و انتقادات خود را در خصوص این پیش‌نویس ارائه دهند. پس از وصول پیشنهادات و انتقادات کمیته مبارزه با جرایم رایانه‌ای با ایجاد تغییراتی در متن اصلاح شده، پیش‌نویس لایحه جرایم رایانه‌ای را در مهرماه۱۳۸۳ به ریاست قوه قضاییه تقدیم نمود. ریاست قوه قضاییه دستور بررسی مجدد آن را در یک کمیسیون تخصصی که با حضور ریاست قوه قضاییه و تعدادی از قضات عالی رتبه و برخی از اعضای کمیته مبارزه با جرایم رایانه‌ای تشکیل می‌شد، صادر کرد. کمیسیون مزبور با تشکیل جلسات متعدد و با اعمال تغییراتی در پیش‌نویس مزبور آن را اصلاح کرد. متن نهایی پیش‌نویس توسط ریاست قوه قضاییه در اواخر فروردین ماه ۱۳۸٤ به هیات دولت تسلیم شد. هیات دولت لایحه مذکور را در اواخر بهار ۱۳۸٤به مجلس شورای اسلامی تقدیم نموده است. متن نهایی پیش نویس قانون جرایم رایانه‌ای در چهار بخش تنظیم و تدوین شده و دارای ۳۹ ماده است.

به‌کار رفته است با توجه به جنبه فراملی جرائم رایانه‌ای بهتر است به منظور هماهنگی با سایر کشورهای دنیا برای تبیین کلاهبرداری رایانه‌ای از ادبیاتی استفاده شود که در اسناد بین‌المللی مربوط به کلاهبرداری رایانه‌ای مورد استفاده قرار گرفته است.

۲ـ یکی از ارکان اصلی واساسی جرم کلاهبرداری بردن مال متعلق به غیر است در پیش‌نویس ماده ۸ قانون جرایم رایانه‌ای اشاره‌ای به بردن مال غیر و یا وارد آمدن ضرر به غیر نشده است. در این ماده صرف تحصیل وجه یا مال یا منفعت یا خدمات و یا امتیازات مالی برای خود یا دیگری به عنوان نتیجه جرم کلاهبرداری محسوب شده است. در نتیجه به موجب ماده مذکور اگر کسی از طریق سوء استفاده از رایانه وجه یا مالی را به دست آورد که متعلق به خود او بوده است، عمل او جرم محسوب می شود در حالیکه چنین عملی نباید کلاهبرداری تلقی شود. بنابراین برای رفع این نقص باید عبارت «مال متعلق به غیر» به متن ماده مذکور اضافه شود.

نتیجه گیری وپیشنهادات

۱–کلاهبرداری رایانه‌ای جرمی است که به وسیله رایانه ارتکاب می‌یابد. اما هر نوع کلاهبرداری که به وسیله رایانه ارتکاب یابد کلاهبرداری رایانه‌ای نامیده نمی‌شود؛ چرا که کلاهبرداری کلاسیک هم به وسیله رایانه قابل ارتکاب است.

۲– یکی از تفاوت‌های اساسی بین کلاهبرداری کلاسیک و کلاهبرداری رایانه‌ای این است که عنصر اغفال به معنای فریب قربانی جرم یکی از اجزای تشکیل‌دهنده عنصر مادی جرم کلاهبرداری کلاسیک است. اما کلاهبرداری رایانه‌ای بدون اغفال قربانی جرم تحقق می‌یابد. این تفاوت اساسی باعث شده است که مقررات مربوط به کلاهبرداری کلاسیک در مورد کلاهبرداری رایانه‌ای قابل اعمال نبوده و این جرم نیاز به قانون خاص داشته باشد.

۳– ماده ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری، تحصیل مال غیر توسط مرتکب را شرط تحقق کلاهبرداری دانسته است؛ اما کنوانسیون جرائم

سایبر چنین شرطی را برای تحقق کلاهبرداری رایانه‌ای لازم نمی‌داند. براساس ماده‌ی ۸ کنوانسیون جرائم سایبر، اگر مرتکب به قصد کسب منفعت مالی برای خود یا دیگری یکی از اعمال مندرج در آن ماده را انجام داده و موجب ضرر صاحب مال شود؛ هرچند که مالی کسب نکرده باشد؛ عمل وی کلاهبرداری رایانه‌ای است. این تفاوت ناشی از اختلاف دیدگاه قانونگذار ایران و دیدگاه تنظیم‌کنندگان کنوانسیون جرائم سایبر در مورد عناصر تشکیل‌دهنده جرم کلاهبرداری است و هیچ ارتباطی به تفاوت جرم کلاهبرداری کلاسیک و کلاهبرداری رایانه‌ای ندارد. بنابراین لازم نیست که قانونگذار ما در این خصوص از کنوانسیون جرائم سایبر تبعیت نماید.

٤-با توجه به اینکه کلاهبرداری کلاسیک ارتکاب یافته به وسیله رایانه (کلاهبرداری کلاسیک رایانه‌ای) با مادهٔ ۱ قانون تشدید مجازات مرتکبین اختلاس و ارتشاء و کلاهبرداری قابل تعقیب و مجازات است؛ پیشنهاد می‌شود به منظور اجتناب از تورم کیفری ماده ٦٧ قانون تجارت الکترونیکی به نحوی توسط قانونگذار اصلاح شود که فقط کلاهبرداری رایانه‌ای را در بستر تجارت الکترونیکی در برگیرد و در عین حال چون گمراهی سیستم‌های پردازش خودکار، جزء عناصر تشکیل دهنده‌ی کلاهبرداری رایانه‌ای نیست، ماده‌ی مذکور از این جهت نبز نیاز به اصلاح دارد. در ضمن دلیلی برای کاهش مجازات کلاهبرداری در بستر تجارت الکترونیکی نسبت به کلاهبرداری‌های ارتکاب یافته در سایر بسترها وجود ندارد. بنابر این یا باید مجازات ماده ۱ قانون تشدید مجازات مرتکبین اختلاس ارتشاء و کلاهبرداری کاهش داده شود و یا اینکه مجازات کلاهبرداری موضوع ماده‌ی ٦٧ قانون تجارت الکترونیکی را با آن هماهنگ نمود.

۵- ماده ۸ پیش‌نویس قانون جرائم رایانه‌ای نیز دارای اشکالات فنی است. چنانچه اشکالات آن به نحوی که در این مقاله اشاره شده برطرف شود و به تصویب قانونگذار برسد؛ این ماده قانونی برای تمام کلاهبرداری‌های رایانه‌ای ارتکاب یافته در همه بسترها

قابل اعمال است. در این صورت قانونگذار می‌تواند برای اجتناب از تورم کیفری، ماده ٦٧ قانون تجارت الکترونیکی را صراحتا ملغی نماید.

منابع و مآخذ:

الف- فارسی:

۱. دزیانی، محمد حسن، (۱۳۷۸) جزوه گزارش توجیهی جرایم رایانه‌ای، مقررات لازم درحقوق جزای ماهوی، دبیرخانه شورای عالی انفورماتیک،

۲. دزیانی، محمد حسن،(۱۳۷٦) جرم رایانه‌ای، گزارش دستاوردهای شورای اروپا در ارتباط با توصیه‌نامه ۹ R(۸۹)، (ترجمه) ، جزوه جرائم رایانه ای، جلد اول ، دبیر خانه شورای عالی انفورماتیک،

۳. زبیر، اولریش، (۱۳۷٦) الف " پیدایش بین المللی حقوق کیفری اطلاعات " ترجمه محمد حسن دزیانی، جزوه جرائم کامپیوتری، جلد سوم، شورای عالی انفورماتیک.

٤. زیبر الریش، کاسپرسن ریک، واندربرژه گی ، (۱۳۷٦)" ب اشتورمان کیس، جنبه‌های قضایی امنیت و جرم کامپیوتری"، ترجمه محمد حسن دزیانی، جزوه جرائم کامپیوتری، جلد دوم، دبیرخانه شورای عالی انفورماتیک،

۵. میر محمد صادقی،(۱۳۷۸) دکتر حسین، جرائم علیه اموال و مالکیت، نشر میزان، تهران، چاپ ششم،

ب- انگلیسی:

1. Computer –related crime: Analysis of Legal policy, OECD, paris, 1986: http://www.OECD.org/document/19/02340-2649--34255-1815059-1-1-1-,00.ht

2. Convention on cybercrime, Budapest, 23 XI.2001, http://conventions.coe.int/treaty/en/treatys/html/185.htm

3. Convention on Cybercrime, Explanatory Report (adopted on 8 November 2001) , http: www//cm.coe.int/ta/rec/1989/89r 9.htm

4. Recommendation (89) 9 on computer related crime and final report of the European committee on crime problems, Strasbourg, 1990, Concil of Europe, http://convention.coe.int/teraty/en/reports/html/185. htm

کسی که مایل است خیر دیگران را تأمین کند خیر خودش را هم تأمین کرده است.

(کنفوسیوس)