Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 3, Issue 5, 2024

Iran's Criminal Policy for Crimes against Electronic Banking with an Emphasis on Phishing

Somayeh Rahmani[*1]

1. PhD Student of Private Law, Central Tehran Branch, Tehran, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: 247-259

Corresponding Author's Info
ORCID: *0000-0003-1268-2822*
TELL: *+98127825993*
Email: *prsrahmanim@gmail.com*

Article history:
Received: *31 Aug 2023*
Revised: *22 Oct 2023*
Accepted: *26 Dec 2023*
Published online: *20 Feb 2024*

Keywords:
Banking, New Banking Services, Crimes Related to New Banking Services, Electronic Banking.

ABSTRACT

Electronic banking or online banking is a service provided by many banks and credit institutions and allows banking transactions to be conducted on the Internet using information and communication technology. The continuation of technological innovations and competition between existing banking organizations and new entrants has made a wider range of banking services and products available, but the rapid development of electronic banking capabilities, in addition to benefits, also brings risks. Modern banking goes hand in hand with new crimes and dealing with these crimes and criminal policy in dealing with these crimes is as necessary as the importance of banking. An important question that was raised and examined in this article is how to evaluate Iran's criminal approach to electronic banking crimes, especially phishing? The method of the present article is descriptive, analytical and library-based to investigate the mentioned question. The findings of the research indicate that in Iran's criminal law, there are no special laws in the field of banking crimes, and mainly, the law of computer crimes governs electronic banking crimes. In Iran's criminal law, the crime of phishing is punishable by imprisonment and a fine.

How to Cite This Article: Rahmani, S (2024). "Iran's Criminal Policy for Crimes against Electronic Banking with an Emphasis on Phishing". *Journal of Comparative Criminal Jurisprudence*, 3(5): 247-259.

فصلنامه فقه جزای تطبیقی
www.jccj.ir
دوره سوم، شماره پنجم، اسفند ۱۴۰۲

سیاست کیفری ایران در قبال جرایم علیه بانکداری الکترونیک با تأکید بر فیشینگ

سمیه رحمانی[*۱]
۱. دانشجوی دکتری حقوق خصوصی، واحد تهران مرکزی، تهران، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی
صفحات: ۲۴۷-۲۵۹

اطلاعات نویسنده مسؤول
کد ارکید: ۰۰۰۰-۰۰۰۳-۱۲۶۸-۲۸۲۲
تلفن: ۹۸۹۱۲۷۸۲۵۹۹۳+
ایمیل: prsrahmanim@gmail.com

سابقه مقاله:
تاریخ دریافت: ۱۴۰۲/۰۶/۰۹
تاریخ ویرایش: ۱۴۰۲/۰۷/۳۰
تاریخ پذیرش: ۱۴۰۲/۱۰/۰۶
تاریخ انتشار: ۱۴۰۲/۱۲/۰۱

واژگان کلیدی:
بانکداری، خدمات نوین بانکی، جرایم مرتبط با خدمات نوین بانکی، بانکداری الکترونیک.

چکیده

بانکداری الکترونیک یا بانکداری برخط، سرویسی است که توسط بسیاری از بانک‌ها و مؤسسات اعتباری ارائه می‌شود و اجازه می‌دهد تا تراکنش‌های بانکی بر بستر اینترنت و با استفاده از فناوری اطلاعات و ارتباطات رهبری و هدایت شوند. ادامه نوآوری‌های تکنولوژیکی و رقابتی بین سازمان‌های بانکی موجود و واردشوندگان جدید، باعث شده که طیف وسیع‌تری از خدمات و محصولات بانکی، قابل دسترس باشند، اما توسعه سریع قابلیت‌های بانکداری الکترونیک، علاوه‌بر منافع، خطرات و ریسک‌هایی را نیز با خود به‌همراه دارد. بانکداری نوین با جرایم نوینی همراست که پرداختن به این جرایم و سیاست کیفری در مقابله با این جرایم، به اندازه اهمیت بانکداری یک ضرورت است. سؤال مهمی که در این مقاله مطرح و بررسی شد، این است که رویکرد جنایی ایران به جرایم بانکداری الکترونیک به‌ویژه فیشینگ چگونه قابل ارزیابی است؟ روش مقاله حاضر توصیفی ـ تحلیلی و به‌صورت کتابخانه‌ای به بررسی سؤال مورد اشاره پرداخته شده است. یافته‌های تحقیق بر این امر دلالت دارد که در حقوق کیفری ایران، قوانین ویژه‌ای در زمینه جرایم بانکی تدوین نشده و عمدتاً قانون جرایم رایانه‌ای بر جرایم بانکداری الکترونیک حاکم است. برای جرم فیشینگ در حقوق کیفری ایران مجازات حبس و جزای نقدی تعیین شده است.

مقدمه

انقلاب فناوری اطلاعات به‌طور بنیادین جوامع را دستخوش تغییر و تحول نموده و اکنون به‌سختی می‌توان بخش‌هایی از جامعه را یافت که تحت تأثیر خود قرار نداده باشد. در دسترس‌بودن فناوری اطلاعات و جستجوی اطلاعات موجود در آن بدون توجه به فواصل جغرافیایی موجب رشد سرسام‌آور این اطلاعات و ارتقای سطح دانش بشری گردیده است، لذا این اطلاعات، باعث افزایش تغییرات اجتماعی و اقتصادی غیرقابل پیش‌بینی در زندگی بشری شده است. پیشرفت در فناوری اطلاع‌رسانی و ارتباطات شبکه‌های اطلاعاتی جهت افزایش سرعت و کیفیت در ارائه خدمات، بانکداری را نیز تحت تأثیر خود قرار داده است (شیرزاد، ۱۳۸۸: ۳۲). بانکداری الکترونیک می‌تواند کارایی و رقابت‌پذیری یک بانک را افزایش دهد، بنابراین مشتریان موجود و بالقوه می‌توانند از درجه تسهیلات بالاتری در تراکنش‌ها و معاملات، بهره‌مند شوند. زمانی که این تسهیلات ارائه‌شده توسط بانک، با خدمات جدید ترکیب می‌شوند، می‌توانند مشتریان نهایی بانک را فراتر از بازارهای سنتی، بسط و توسعه دهند، درنتیجه مؤسسات مالی در پذیرش قابلیت‌های بانکداری الکترونیک که شامل سیستم‌های بازاریابی پیچیده، امکان بانکداری از راه دور و برنامه‌های ارزش اندوخته می‌باشد، در حال تکاپو هستند. ایران با برخورداری از اقتصاد در حال توسعه، در چند دهه اخیر گام‌های اساسی در زمینه به‌کارگیری فناوری اطلاعات و ارتباطات در عرصه‌های مختلف کسب و کار، به‌ویژه بانکداری نوین برداشته است که از آن جمله می‌توان به راه‌اندازی دستگاه‌های خودپرداز، شبکه تبادل اطلاعات بین بانکی (شتاب) به خدمات اینترنتی بانک‌ها و ... اشاره نمود. باوجود این، بانکداری الکترونیکی در ایران نسبت به کشورهای پیشرفته و پیشرو در این زمینه‌ها فاصله بسیار زیادی دارد و برای رسیدن به آن نیازمند تلاش والای فعالان صفت بانکداری کشور است. با تأکید بر چشم‌انداز بیست‌ساله ایران و دستیابی به جایگاهی برتر در منطقه خاورمیانه و همچنین تأکید بر برنامه چهارم توسعه، بر اقتصادی متعامل با اقتصاد جهانی مبتنی‌بر فناوری اطلاعات چاره‌ای نخواهیم داشت که با بانکداری الکترونیکی توانمند و هوشمند پاسخگو، روبه‌رو شویم، البته باید توجه داشت که پیشرفت‌های نوین بانکی از برخی پیامدهای منفی نیز مبرا نبوده است و پیدایش انواع جرایم نوین در بهره‌برداری از فناوری اطلاعات، بخش جدیدی از آن به‌شمار می‌رود. جرایم خدمات نوین بانکی شامل دو گروه از جرایم می‌شود: گروه اول شامل جرایمی هستند که با مقررات مربوط به جرایم کلاسیک قابل پیگیری و مساوات هستند و نیازی به تصویب قوانین جدید ندارند؛ گروه دوم شامل جرایمی هستند که قبل از تولد و رشد بانکداری نوین به هیچ‌وجه امکان ارتکاب آن وجود نداشته است، به‌علاوه عواقب و پیامدهای فناوری محرمانه می‌تواند خیلی بیشتر از گذشته و غیرقابل تصور باشد، چراکه مصونیت‌های جغرافیایی یا مرزهای ملی، آن را محدود می‌کند که موجب سوءاستفاده گسترده، مجرمین به‌ویژه گروه‌های جنایتکار سازمان‌یافته، از سیستم‌های الکترونیکی بانک‌ها گردیده است. سؤال اصلی که در این خصوص مطرح است، این است که رویکرد جنایی ایران در قبال جرایم نوین بانکی و ازجمله فیشینگ چیست؟ فرضیه تحقیق نیز بدین‌شکل قابل طرح است که در حقوق کیفری ایران، جرایم خدمات نوین بانکی در قالب جرایم رایانه‌ای قابل تعقیب می‌باشد و نظام حقوقی ویژه‌ای در این خصوص وجود ندارد. به‌منظور بررسی سؤال و فرضیه مورد اشاره در ادامه جرایم بانکداری الکترونیکی بررسی می‌شود.

۱- تقلب در کارت اعتباری و وجه الکترونیکی

با جایگزین‌شدن کارت اعتباری به‌جای اسکناس در طی زمان، بزهکاری مالی در این حوزه نیز به تناسب همین انتقال جابه‌جا شده است. بنابراین تقلب در کارت‌های اعتباری با همان انگیزه و محرک‌هایی انجام می‌گیرد که در تقلب پولی یا جرایم مرتبط با چک مطرح است؛ فقط آنچه اتفاق افتاده، ایجاد این طرز تفکر در ذهن برخی از بزهکاران است که کشف و پیگرد جرایم مرتبط با تقلب در کارت‌های اعتباری، در مقایسه با دیگر جرایم پولی، به‌دلیل نوبودن روش‌های الکترونیکی پرداخت دشوارتر است، حال آنکه در عمل خلاف این موضوع اثبات شده است (Frank *et al*, 2001: 106-109).

البته وجه نقد الکترونیکی، ممکن است در معرض تقلب قرار بگیرد. نخستین پرسش آن است که چگونه ممکن است وجه الکترونیکی سرقت شود، آیا ممکن است گیرنده نسبت به آن محکوم شناخته شود؟ پرسش دوم آن است که آیا جعل وجه الکترونیکی ممکن است و چنانچه پاسخ مثبت باشد، خسارت برعهده چه کسی خواهد بود؟ اگر کالایی مانند خودرو سرقت شود، حتی اگر مورد معاملات متعدد قرار گیرد، اصولاً مالکیت مالک اصلی بر آن باقی می‌ماند. چنین قاعده‌ای درباره پول اجرا نمی‌شود. اگر شخص مقداری پول برباید و با آن کالایی بخرد، ثمن در مالکیت بایع وارد می‌شود، حتی اگر سارق بر آن ید مشروع نداشته باشد. به‌موجب قانون بروات انگلیس مصوب ۱۸۸۲، «**سندی قابل انتقال به‌حساب می‌آید و بر طبق همین قانون کسی که با حسن نیت اوراق بهادار را به‌دست می‌آورد، صرف نظر از منشأ مالکیت و این‌که از چه راهی آن را تحصیل می‌نماید، مالک شناخته می‌شود.**» اکنون پرسش آن است که آیا چنین قاعده‌ای را می‌توان درباره وجه الکترونیکی نیز اجرا کرد؟ در تطبیق با قانون ۱۸۸۲ باید اظهار داشت که روح قانون بیشتر اسناد مکتوب را دربر می‌گیرد، اما اگر استفاده از وجه الکترونیکی به قدری شیوع یابد که جایگزین پول شود و مالک اولیه از لحاظ ثبت، نام مالک برای آن متصور نباشد، می‌توان اعتقاد داشت که واجد وصف انتقال بوده، لذا قاعده فوق در مورد آن مجری خواهد بود (زیبر، ۱۳۸۳: ۴۱).

۲- جعل پول الکترونیکی

باوجود دستگاه‌های نوین، امکان کشف جعل در پول الکترونیکی نسبت به پول کاغذی بسیار آسان‌تر است. این فرض تقویت شده است که از لحاظ ایمنی این نوع از وسایل اعتباری در رتبه برتری قرار دارند. به‌منظور اجتناب از جعل، اسم رمزی که در پول الکترونیکی به‌کار می‌رود، باید به‌گونه‌ای باشد که قابلیت افشاشدن نداشته باشد. برای تحقق این موضوع از توانمندی مهندسانی بهره‌گیری می‌شود که با فنون جعل و راه‌های مقابله با آن آشنایی دارند. باوجود این، هیچ‌گاه نمی‌توان مدعی شد که جعل پول الکترونیکی قابل تصور نیست (Hans, 2001: 318).

در عین حال این ادعا مطرح شده که امکان جعل اسناد الکترونیکی ساده‌تر از اسناد کاغذی است، زیرا به‌طور مثال، صادرکننده می‌تواند سندی را پس از ارسال تغییر دهد و مدعی شود که تغییر از جانب او نبوده است (صادقی نشاط، ۱۳۸۶: ۷۵-۶۴). به هر روی، بحث اصالت قابلیت اعتماد یکی از بحث‌های بااهمیتی است که درباره اسناد الکترونیکی مطرح می‌شود.

در مقایسه با پول سنتی باید مدعی شد که پرداخت با پول الکترونیکی جعلی ایفای تعهد محسوب نمی‌شود و از لحاظ سقوط تعهد یا بدهکارکردن طرف مقابل، فاقد هرگونه اثر حقوقی است. به‌لحاظ نظری، مسؤولیت بر کسی تحمیل می‌شود که در فرض پرداخت‌های متعدد به‌موجب پول جعلی واحد، زنجیره تأدیه از او آغاز شده است. باوجود این، از آن رو که گاه یافتن مسؤول اصلی دشوار است، به‌لحاظ عملی و برای اجتناب از سردرگمی، خسارت بر کسی تحمیل می‌شود که به هنگام کشف جعل پول مذکور را در اختیار داشته است (Smith, 2002: 506).

وضعیت‌های مذکور و تحمیل مسؤولیت بر افرادی که در بیشتر موارد مسؤول واقعی جعل و تزویر در پول الکترونیکی به‌شمار نمی‌آیند، ممکن است مقبولیت پول الکترونیکی را در معرض خطر قرار دهد. به‌همین دلیل باید برای این موردها چاره‌ای اندیشیده شود و به‌طور مثال، مسؤولیت به بانک یا مؤسسه مالی تحمیل شده و از این راه، میان تمامی کاربران پول الکترونیکی توزیع شود (Simmons, 2000: 323-326).

ماده ۶ قانون جرایم رایانه‌ای، «تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا واردکردن متقلبانه داده به آن‌ها، تغییر داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سامانه‌های رایانه‌ای یا مخابراتی یا تراشه‌ها یا ایجاد یا واردکردن متقلبانه داده‌ها یا علائم به آن‌ها» را به‌عنوان جعل، قابل مجازات دانسته است. کیفر نسبتاً شدیدی هم برای این جرم در نظر گرفته شده که عبارت است از«حبس یک تا پنج سال یا جزای نقدی از بیست‌میلیون‌ریال تا یکصدمیلیون‌ریال یا هر دو.»

دسترسی غیرمجاز به سامانه‌های الکترونیکی، به‌طور قطع، محرمانگی اطلاعات موجود در آن‌ها را در معرض خطر قرار می‌دهد، اما خطر وقتی جدی‌تر می‌شود که شخص با دسترسی به سامانه، تمامیت و قابلت دسترسی اطلاعات را در سامانه دستخوش تغییر کرده یا داده‌های دلخواه خود را به آن‌ها بیافزاید. نتیجه تغییر غیرمجاز در داده‌ها می‌تواند ناهماهنگی در سامانه یا حتی خطر مرگ باشد، کما این‌که در یک پرونده پرستاری با تغییر داده مشخصات بیمار این خطر را ایجاد کرده بود.

در مورد سامانه مرتبط با تجارت الکترونیکی، ارزش مالی سامانه با اطلاعات و مدارکی که در آن قرار دارد و نه سخت افزارهای سامانه مشخص می‌گردد. تغییر در داده می‌تواند تعاملات تجاری را با اخلال جدی روبه‌رو سازد. در یک پرونده، شخصی با هک‌کردن یک سامانه مالی، داده‌هایی به آن وارد کرد که مانع از ذخیره داده‌های مالک سامانه می‌شد، هرچند در انگلیس، در این‌که جرم، تغییر غیرمجاز این موارد را دربر می‌گیرد یا خیر، اختلاف وجود دارد، اما اگر چنین موضوعی در ایران طرح شود، با استناد بند «ب» ماده ۶ قانون جرایم رایانه‌ای، جعل رایانه‌ای محسوب خواهد شد.

برای تحقق جرم جعل رایانه‌ای لازم نیست که مرتکب از این کار نفعی ببرد. همچنین ضرورتی ندارد که عامل بداند فعل او در تغییر داده‌ها یا واردکردن داده‌ها یا علائم به‌نحو غیرقانونی، کدام قسمت از سامانه را دستخوش تغییر ساخته یا در معرض خطر قرار می‌دهد. باید توجه داشت که این جرم می‌تواند علیه دارنده حقوق مالکیت فکری ادعا شده و به نتیجه هم برسد، چنانچه در یک پرونده (Rogert, 2005: 79)، پدیدآورنده نرم‌افزار، یکی بمب منطقی در آن طراحی کرده بود که در فرض بروز اختلاف در پرداخت، نرم‌افزار را از کار می‌انداخت.

چنانچه در ماده ۷ و ۸ قانون جرایم رایانه‌ای مورد توجه قرار گرفته، جعل رایانه‌ای ممکن است با هدف استفاده از داده‌ها یا کارت یا تراشه‌های مجعول برای اهداف دیگر باشد، کما این‌که حمله به یک سامانه و تحریف داده‌های آن، می‌تواند به‌منظور تخریب داده‌هایا ایجاد اخلال در عملکرد سامانه باشد. در حقوق انگلیس، به‌جای طرح دو جرم متفاوت، یعنی جعل رایانه‌ای و تخریب و اخلال در داده‌ها، جرم واحدی به نام «تغییر غیرمجاز» وجود دارد که تمامی این موارد را شامل می‌شود.

در حقوق ایران، هرگاه تغییر داده‌ها یا واردساختن متقلبانه داده، موجب اخلال یا تخریب در سامانه شود. جرم موضوع ماده ۶ قانون جرایم رایانه‌ای (جعل رایانه‌ای) و ماده ۸ همان قانون (تخریب و اخلال در داده‌ها) صدق خواهد کرد. در این حالت، قواعد مربوط به تعدد معنوی اجرا می‌شود کیفر جرمی اعمال می‌شود که مجازات آن شدیدتر است.

۳- سرقت هویت

استفاده از هویت دیگران در پرداخت‌های اینترنتی، یکی‌دیگر از جرایم بانکداری الکترونیک است که انجام می‌گیرد. در این جرم شخص، خود را به‌جای دیگری جلوه داده و تمام حقوق قانونی وی را دارا شده یا جرایمی را به نام او انجام می‌دهد. در برخی از کشورها، قوانین صریحی برای مقابله با سرقت هویت وجود دارد. برای مثال، در ایالات متحده آمریکا، قانون تشدید مجازات سرقت هویت، مجازات دو سال حبس به‌همراه کیفر هر جرمی که شخص مرتکب شود را برای سرقت هویت در نظر گرفته است. در این قانون، سرقت هویت به «دریافت، تصرف و یا استفاده عالمانه و بدون مجوز از هر وسیله شناسایی متعلق به دیگری» تعریف شده است. سرقت هویت اغلب برای ارتکاب جرایمی همچون کلاه‌برداری و تقلب انجام می‌گیرد و در هر حال به‌دلیل تعدد مادی ارکان ارتکاب این جرایم در مقایسه با سرقت هویت، مجازات دو جرم در مورد شخص اعمال می‌شود.

برای سرقت هویت در حقوق موضوعه ایران، نمی‌توان معادل خاصی یافت، حتی آن قسمت از قانون مجازات اسلامی که زیر عنوان «غصب عناوین و مشاغل» (مواد ۵۵۷-۵۵۵) آمده، «استفاده از نام، شماره شناسایی با عنوان شخص عادی یا با هدفی غیر از منظور شغلی و حرفه‌ای را شامل نمی‌شود.» مواد قانون جرایم رایانه‌ای نیز علی‌رغم تعریف موسع از جرایم رایانه‌ای، این مسأله را متذکر نشده‌اند، لذا ضرورت دارد تا ضمن مقررات خاص، جرم‌انگاری صحیحی نسبت به سرقت هویت و آثار مجرمانه آن به عمل آید، البته در ایران، بسیاری

از مصادیق سرقت هویت می‌تواند در قالب دسترسی غیرمجاز، جعل یا کلاه‌برداری رایانه‌ای مشمول قانون جرایم رایانه‌ای قرار گیرد.

مطابق ماده ۷۴۰ کتاب پنجم قانون مجازات اسلامی، **«هرکس به‌طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از شش‌میلیون (۶/۰۰۰/۰۰۰) ریال تا پنجاه‌میلیون (۵۰/۰۰۰/۰۰۰) ریال و در غیر این صورت به حبس از نودویک‌روز تا یک‌سال یا جزای نقدی از بیست‌میلیون (۲۰/۰۰۰/۰۰۰) ریال تا هشتادمیلیون (۸۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد»** (جزای نقدی مندرج در این ماده به‌موجب مصوبه مورخ ۱۳۹۹/۱۲/۲۵ هیأت وزیران تعدیل شد). همچنین مطابق ماده ۷۴۱ قانون مذکور، **«هرکس به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا متوقف‌کردن داده‌ها یا مختل‌کردن سامانه، وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، علاوه‌بر رد مال به صاحب آن به حبس از یک تا پنج‌سال یا جزای نقدی از پنجاه‌میلیون (۵۰/۰۰۰/۰۰۰) ریال تا دویست‌وپنجاه‌میلیون (۲۵۰/۰۰۰/۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد»** (جزای نقدی مندرج در این ماده به‌موجب مصوبه مورخ ۱۳۹۹/۱۲/۱۲ هیأت وزیران تعدیل شد).

در سال ۲۰۰۳، مرکز گزارش‌ها و تحلیل تراکنش‌های استرالیا، تخمین زده بود که کلاه‌برداری از طریق سرقت هویت، بیش از ۱/۱ میلیارد دلار آمریکا در استرالیا خسارت وارد کرده است. در ایالات متحده، تعداد سرقت و کلاه‌برداری مرتبط با هویت در کارت‌های پرداخت از ۵۶ میلیارد مورد در سال ۲۰۰۹ به ۳۷ میلیارد مورد در سال ۲۰۰۱ کاهش یافته است. همچنین تعداد بزه‌دیدگان در فاصله این دو سال ۲۶ درصد کاهش یافته و از ۱۱ میلیون نفر در سال ۲۰۰۹، به ۸/۱ میلیون نفر در سال ۲۰۰۱ رسیده است. رقم کلاه‌برداری شده از هر بزه‌دیده هم از میانگین ۴/۹۹۱ دلار برای هر نفر در سال ۲۰۰۹ به ۴/۶۰۷ دلار در سال ۲۰۱۰ کاهش یافته است (Javelin Strategy & Research, 2011: 45).

سرقت هویت می‌تواند نتیجه یافتن یک کارت شناسایی، ضبط اطلاعات مربوط به کارت‌های مغناطیسی به هنگام استفاده از آن‌ها در دستگاه‌های کارت‌خوان، هک‌کردن سامانه‌های رایانه‌ای و یا سرقت یا جعل مدرک شناسایی شخصی باشد. بدیهی است که بسیاری از اعمال، به‌عنوان مستقل قابل پیگیرد هستند.

وجود شماره‌های منحصربه‌فرد و اعتبار آن‌ها برای انجام اعمال و اقدامات خاص (برای مثال عملیات بانکی)، هرچند باعث کاهش تشریفات گردیده، اما احتمال سرقت هویت را افزایش داده است. سالانه، میلیون‌ها گذرنامه، گواهی‌نامه و کارت پرداخت با شماره‌های بی‌همتا صادر می‌شود و در اختیار شهروندان قرار می‌گیرد. در بسیاری از این موارد، بزهکار می‌تواند به سرقت هویت و استفاده از آن دست یابد. به‌عنوان مثال عینی، بزهکار می‌تواند با نصب دروبین بر روی صفحه کلید دستگاه خودپرداز، ابتدا شماره رمز کارت مشتری را به دست آورده و سپس با تعقیب کمتری و روبودن کارت وی، در حداقل زمان ممکن از آن برای برداشتن پول استفاده کند. به‌هرحال، راحتی ناشی از فناوری چنین اشکالاتی را هم در پی داشته است.

۴- کلاه‌برداری

رکن قانونی جرم کلاه‌برداری در حقوق جزای ایران، ماده ۱ قانون تشدید مجازات مرتکبین ارتشاء و اختلاس و کلاه‌برداری (قانون تشدید) است. این ماده، در عین جرم انگاری کلاه‌برداری، ارکان و شرایط تحقق این جرم را هم بیان می‌کند. ماده ۷ قانون تجارت الکترونیک در تعریف کلاه‌برداری رایانه‌ای از ماده ۱ قانون تشدید، اقتباس شده است.

ماده ۱۳ قانون جرایم رایانه‌ای در متنی که قابل انتقاد است، جرم کلاه‌برداری مرتبط با رایانه را به‌طور کلی توصیف می‌کند و ارکان ضروری این جرم را آن‌گونه که ماده قانون تشدید، ذکر کرده، بیان نمی‌کند. با این وضعیت، می‌توان دو نظریه متفاوت در تفسیر ماده ۱۳ قانون مذکور ارائه داد:

اول این‌که ماده ۱۳ را باید با در نظرگرفتن ماده ۱ قانون تشدید و ماده ۶۷ قانون تجارت الکترونیک معنا کرد. درحقیقت، مقنن با فرض این‌که مفهوم و ارکان کلاه‌برداری

در قوانین سابق مشخص شده، از تکرار مفاد موارد مذکور خودداری کرده است، به‌ویژه باید این نکته را در نظر گرفت که در روند مجموع‌سازی قوانین، قانون جرایم رایانه‌ای به موجب ماده ۵۵ آن، جزئی از قانون مجازات اسلامی محسوب می‌شود.

این طرز تلقی، به‌دلایل مختلف قابل دفاع نیست، ازجمله این‌که اولاً اگرچه قانون جرایم رایانه‌ای بخشی از قانون مجازات اسلامی محسوب می‌شود، اما قانون تشدید و قانون تجارت الکترونیک که به جرم کلاه‌برداری پرداخته‌اند، چنین وضعیتی ندارند. بنابراین منطقی‌ترین راهکار این بود که در قانون جرایم رایانه‌ای درخصوص مفهوم و ارکان کلاه‌برداری به دو قانون مذکور ارجاع داده می‌شد و یا این‌که مفاد مرتبط از این قوانین، در متن ماده ۱۳ قانون جرایم رایانه‌ای ذکر می‌گردید.

دوم این‌که عباراتی در ماده ۱۳ قانون مذکور به‌کار رفته که نشان می‌دهد مقنن درصدد ارائه مفهوم جدیدی از کلاه‌برداری بوده است. در قسمت اول این ماده مقرر شده که: «**هرکس به‌طور غیرمجاز با اعمالی همچون واردکردن، تغییر و ... (که جنبه حصری ندارند) از سامانه‌های رایانه‌ای یا مخابراتی، تحصیل مال یا هر نوع امتیاز مالی نماید، مجازات خواهد شد.**» در این ماده، مفهوم عامی از کلاه‌برداری ارائه‌شده که زمینه منطقی را برای طرح نظریه دوم فراهم می‌کند.

نظریه دوم در تفسیر ماده ۱۳ قانون جرایم رایانه‌ای آن است که این ماده، درصدد جرم‌انگاری هر نوع استفاده غیرمجاز از سامانه رایانه‌ای یا مخابراتی برای تحصیل مال یا هرگونه امتیاز مالی بوده است. ازاین‌رو مفهوم جدیدی از کلاه‌برداری ارائه شده که آن را به جرم «تقلب» در حقوق انگلیس نزدیک می‌کند و حتی از محدوده آن هم فراتر می‌برد. بخش ۱۵ قانون سرقت انگلیس (مصوب ۱۹۶۸) در تعریف جرم تقلب (با مسامحه و کلاه‌برداری) مقرر می‌دارد: «**۱- هر شخصی که با هر نوع فریبی، غیرصادقانه مالی را به‌دست آورد که متعلق به دیگری است و قصد محروم‌کردن دائمی مالک را از آن داشته باشد...؛ ۲- از نظر این بخش، «فریب» به‌معنای هر نوع فریبی (خواه عامدانه یا ناشی از بی‌توجهی) به‌وسیله گفتار یا کردار، در امور موضوعی یا حکمی... می‌شود.**»

در انگلیس، کمیسیون حقوقی، موضوع تقلب در فضای مجازی را مورد بررسی قرار داده و به این نتیجه رسیده است که جرم مذکور در بخش ۱۵ قانون ۱۹۶۸ کفایت نمی‌کند و باید جرم جدیدی تعریف شود. کنوانسیون اروپایی جرم مجازی، نوعی جرم مرتبط با کلاه‌برداری را تعریف کرده که در آن از مفهوم «فریب» عدول شده است. طبق ماده ۸ این کنوانسیون: «**هریک از دولت‌ها موظفند قانونی را وضع کرده و موزاینی را اتخاذ کنند که برای جرم‌انگاری عملی لازم است که با ارتکاب عامدانه و بدون مجوز، باعث خسارت به مال دیگری به‌وسیله این موارد، می‌شود: الف- هر نوع واردکردن، تغییر، حذف یا مخفی‌کردن داده رایانه‌ای؛ ب- هر نوع مداخله در عملکرد یک سامانه رایانه‌ای با هر قصد متقلبانه یا فریب‌آمیز برای به‌دست‌آوردن بدون مجوز هر نوع امتیاز اقتصادی برای خود یا دیگری.**» ذکر سرقت و کلاه‌برداری مرتبط با رایانه، زیر یک عنوان در فصل سوم از بخش یکم قانون جرایم رایانه‌ای نشان می‌دهد که هرجا دستیابی غیرقانونی به داده‌های متعلق به دیگری، در قالب کلاه‌برداری نگنجد، مشمول عنوان جرم سرقت (ربایش) بوده و در همان اساس قابل مجازات خواهد بود.

۵- تخریب و اخلال در داده‌ها یا سامانه‌های الکترونیکی

خرابکاری یا ایجاد اخلال در داده‌های رایانه‌ای یا سامانه‌های رایانه‌ای یا مخابراتی می‌تواند با اهداف متعددی صورت گیرد تا حدی که با تجارت الکترونیکی ارتباط این عمل اغلب با هدف فراهم‌کردن زمینه ارتکاب جرایم دیگر، ازقبیل دسترسی غیرمجاز به داده‌ها، جاسوسی اقتصادی، کلاه‌برداری، نقض حقوق مالکیت فکری و تعرض به علائم و اسرار تجاری انجام می‌گیرد.

مواد ۸ الی ۱۱ قانون جرایم رایانه‌ای به موضوع «تخریب و اخلال در داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی» اختصاص یافته است. از نظر این قانون، هر اقدامی که منتهی به تخریب یا اختلال در داده یا سامانه بوده یا باعث شود که افراد مجاز، امکان دسترسی به آن داده یا سامانه را نداشته

باشند، قابل مجازات است. مجازاتی که تعیین شده، به انتخاب دادرس می‌تواند حبس، جزای نقدی یا هر دو باشد.

هرگاه جرم اخلال یا تخریب داده، با هدف به‌خطرانداختن امنیت و آسایش عمومی ارتکاب یابد، به‌موجب ماده ۱۱ قانون جرایم رایانه‌ای، مجازات مرتکب، حبس از سه‌سال تا ده‌سال دانسته است. این وضعیت، قانون جاسوسی اقتصادی آمریکا را به یاد می‌آورد که در آن، دایره شمول جرایم علیه امنیت، از محدود مسائل اجتماعی و سیاسی فراتر رفته و اقدامات مجرمانه‌ای را که برعهده علیه اقتصاد ملی (در مفهوم کلان آن) صورت می‌گیرد، شامل شده است.

۶- افشای داده‌ها و تعرض به حریم خصوصی

در مورد مفهوم حریم خصوصی میان دانشمندان اختلاف نظر وجود دارد (انصاری، ۱۳۸۳: ۵۴-۱). در یک تعریف نسبتاً قابل قبول، حریم خصوصی را می‌توان به حق کنترل افراد نسبت به دسترسی دیگران به اطلاعات راجع به آن‌ها تعریف کرد. اطلاعات در این تعریف مفهوم عامی دارد و شامل هرگونه اطلاعات درخصوص ویژگی‌های شخصی، شخصیتی، جسمی، اقتصادی و ... می‌شود. وقتی که شخصی، بدون رضایت دیگری به اطلاعات وی در فضای مجازی دسترسی دارد، موضوع مهمی است که توجه دانشمندان مختلفی را به خود جلب کرده است (زرکلام، ۱۳۸۶: ۱۹۶-۱۷۳).

ظهور ابرتارنماهایی همچون فیس‌بوک، یوتیوب و اقبال میلیاردها نفر به آن‌ها، صیانت از حریم خصوصی را در دهکده جهانی اطلاعات در حد غیرممکن دشوار کرده است تا جایی که **اریک اشمیت**، مدیرعامل گوگل در کنفرانس تکنونومی ۲۰۱۰ اظهار داشت: **«مردم هنوز برای ورود به انقلابی که منتظر ماست، آماده نیستند و هنوز نگرانی‌های زیادی برای محافظت از حریم شخصی خود روی شبکه دارند. چیزی که امروزه دیگر حفظ آن غیرممکن است»** (Pushcharovsky, 2010: 228).

به‌نظر می‌رسد ادعای عدم امکان صیانت از داده‌های خصوصی در اینترنت، صرفاً برای رفع تکلیف از سازندگان و گردانندگان شبکه‌های ارتباطی ابزار می‌شود. باوجود این طرز تلقی که حفظ حریم خصوصی در فضای مجازی غیرممکن است، قانون جرایم رایانه‌ای در اقدامی که نشان می‌دهد، این قانون درصدد حمایت جدی از داده‌های شخصی می‌باشد؛ برای افشای داده‌های خصوصی در فضای مجازی، مجازات تعیین کرده است. به‌موجب ماده ۱۷ این قانون، **«هرکس به وسیله سیستم‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او منتشر کند یا در دسترس دیگران قرار دهد، به‌نحوی‌که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نودویک‌روز تا دوسال یا جزای نقدی از پنج تا چهل‌میلیون‌ریال یا هر دو مجازات محکوم خواهد شد.»**

افشای اطلاعات خصوصی ممکن است به‌دلیل نقص سهوی یا عمدی در طراحی مرورگرهایی باشد که برای شبکه جهانی (اینترنت) یا شبکه‌های خصوصی طراحی می‌شوند، کما این‌که شرکت موزیلا پذیرفته است که نسخه شماره ۵ و ۱۳ مرورگر این شرکت می‌تواند به‌دلیل اشکالی که در طراحی گزینه View آن وجود دارد، موجب افشای داده‌های حساس همچون اطلاعات بانکی و کارت‌های پرداخت شود.

گفته می‌شود اغلب مرورگرهای امروزی اطلاعاتی از کاربران خود را به سازندگان خود ارسال می‌کنند. فایرفاکس، اکسپلورر، کروم، سافاری و ...، از جمله مرورگرهای معروفی هستند که اطلاعاتی از حریم خصوصی کاربران خود را به دست سازندگان خود می‌رسانند. این اطلاعات در تبلیغات متناسب با ذائقه او استفاده شود. برنامه‌هایی هم برای خنثی‌کردن کارکرد جاسوسی مرورگرها ارائه و بازاریابی شده که ممکن است خود، ابزار جاسوسی باشند.

۷- فیشنگ (رمزگیری)

فیشنگ یا رمزگیری، کنایه از ماهی‌گیری است که در آن شکارچی قلاب یا تور خود را در محیط‌هایی که طعمه فراوانی برای صید وجود دارد یا در فضای مجازی، آنجا که استانداردهای ایمنی به‌درستی مراعات نشده یا مشتری برای یک لحظه بی‌احتیاطی می‌کند، پهن می‌نماید. حربه معمول در رمزگیری آن است که شخص رمزگیر، یک نامه الکترونیکی که به‌نظر می‌رسد از مؤسسه مالی مشتری (بزه‌دیده) یا تارنمای تجارت الکترونیکی وی ارسال شده، برای قربانی می‌فرستد. برای جلب توجه مشتری و ایجاد اعتماد در او،

علامت تجاری و سایر مشخصات ظاهری شرکت شرکت اصلی در متن نامه گنجانیده شده و حتی به مشتری هشدارهای لازم در جهت رعایت نکات ایمنی داده می‌شود. به‌طور معمول، در نامه الکترونیکی به گیرنده گفته می‌شود که باید اطلاعات حساب وی، درجهت پیشگیری از کلاه‌برداری یا به‌دلیل نقض فنی که پیش آمده یا سایر مسائل امنیتی به‌روز شود. بزهکار حتی یک رابط (لینک) به مشتری می‌دهد تا از آن طریق به پایگاه اصلی وصل شود و مطمئن شود که اطلاعات را مؤسسه مالی وی ارسال کرده است، درحالی‌که پایگاه (تارنمای) مذکور هم ساختگی است (Lcncy, 2005: 259-260). با مشاهده این ظواهر، مشتری حاضر می‌شود که اطلاعات شخصی خود را ارائه نموده و رمز عبور خویش را به‌روز کند، درنتیجه بزهکار به اطلاعات دقیق وی دست می‌یابد و از آن‌ها می‌تواند برای اقدامات مجرمانه بعدی (برداشت از حساب، انتقال وجه و ...) استفاده کند.

«یکی از روش‌های تقلب در پرداخت‌های الکترونیکی، فیشینگ، نسخه‌برداری یا دو نسخه‌نویسی‌کردن است. در این روش با ادعای قانونی‌بودن شرکت/ مؤسسه، از راه‌های گوناگون، ازجمله نامه الکترونیکی از افراد خواسته می‌شود که شماره کارت اعتباری و دیگر اطلاعات شخصی خود را ارائه کنند. باتوجه به جعلی‌بودن پایگاه‌های اینترنتی که از نظر ظاهری تقریباً هیچ تفاوتی با پایگاه واقعی ندارد، ممکن است مشتری دچار اشتباه شده و شناسه‌های درخواست را ارائه کنند. در این شیوه، ارتباط با پایگاه اینترنتی شرکت ادعایی نیز ممکن است با دریافت شماره و دیگر اطلاعات، این امکان برای متقابلاً فراهم می‌شود که به‌شماره حساب‌های بانکی افراد دسترسی یافته یا پیشینه الکترونیکی آنان را برای سرقت هویت به‌دست آورند» (Smedinghoff, 2005: 54).

برای پیشگیری از این دسته از جرایم، بانک‌ها می‌توانند به مشتریان خود یادآوری کنند که مؤسسه مالی آن‌ها هیچ‌گاه اطلاعات محرمانه را از طریق نامه الکترونیکی از آنان درخواست نخواهد کرد و آن‌ها باید چنین مطالباتی از سوی متقلبان را به بانک خود اطلاع دهند. برای جلوگیری از اختلاف میان طرفین (بانک و مشتری) و پیشگیری از جرایم، باید اقدامات زیر با دقت و تأمل درنظر گرفته شود:

– از اظهارات مشتری رونوشت کاغذی یا الکترونیکی تهیه شود تا درصورتی‌که شناسه کاربران و رمز عبور آنان ارائه شود، از ایجاد رمز عبورهای مشترک (برای دو یا چند فرد) خودداری شود.

– داده پیام‌های مربوط به مشتریان قابل بازیابی، بازبینی و بازرسی باشد و سیستم رایانه‌ای به‌گونه‌ای برنامه‌ریزی شود که تغییرات غیرسازمانی ـ خارج از روال بانکی ـ در آن آشکار شود.

– شناساندن پایگاه/ پایگاه‌های اینترنتی که ارتباط با بانک منحصراً از طریق آن‌ها امکان‌پذیر است و سفارش به مشتریان برای اجتناب از پاسخگویی به نامه‌های الکترونیکی یا دعوت‌نامه‌های مشکوک.

– بالابردن اطلاعات مشتریان از طریق ارائه اطلاعات فنی، قانونی و علمی لازم به آنان و یادآوری ضرورت گزارش‌دادن موارد مشکوک به پلیس، نیروهای امنیتی و سیستم بانکی.

– بررسی صورت حساب‌ها به‌وسیله مشتری به‌صورت محرمانه و ارائه‌نکردن رمزها و شماره‌های کلید به دیگر افراد.

– فراهم‌ساختن امکان تغییر رمز برای مشتریان از سوی بانک.

– تنظیم برنامه‌ای برای شناسایی و اعلام نامه‌های الکترونیک متقلبانه به مشتریان و اعلام احتیاط به آنان.

– ارتباط با پلیس اینترنتی و گزارش‌دادن موارد مشکوک به تقلب و کلاه‌برداری از سوی بانک و مشتری به آنان.

در موردهای که بزهکاری با سن کم با جسارت بسیار و توانایی فنی بالا، اقدام به فیشینگ یا جرایم مشابه می‌کند، اصولاً دستگیری او نیز چاره‌ساز نیست، چراکه به‌مثابه نوجوان‌بودن از مسؤولیت کیفری مبرا بوده و در عمل برای جبران خسارتی که در حجم وسیع وارد کرده است، وجهی در اختیار ندارد. بنابراین قانونگذاری باید ضمن درک صحیح این

واقعیت که بی‌اعتمادی مشتری را به روش‌های جایگزین ناامن نمی‌توان با شناسایی و کیفر بزهکاران منتفی ساخت، در پی ارائه و به‌روزرسانی استانداردهای ایمنی پرداخت‌های الکترونیکی باشد و در این‌باره سازمانی را که به ضوابط فنی و اصول حقوقی تسلط داشته باشد، مسؤول مدیریت، نظارت و پاسخگویی کند (Shitds, 2000: 14). ازآن‌رو که بحث‌های صرف علمی درباره ایمنی پرداخت‌های الکترونیکی از موضوع این مقاله خارج است از تفصیل بحث در این‌باره خودداری کرده و محققان را به منابع تخصصی مربوط که پاره‌ای از آن‌ها در زیرنویس ذکر شده است، ارجاع می‌دهیم (Arbaugh *et al*, 1997: 65-71).

سرقت هویت و کلاه‌برداری در هویت، عناوین دیگری است که برای توصیف دستیابی متقلبانه به اطلاعات شخصی افراد ازقبیل شماره حساب و شماره تأمین اجتماعی به‌کار می‌رود. اولین و غالب‌ترین خسارتی که به قربانیان رمزگیری وارد می‌شود، جنبه مالی دارد. درواقع فرایند رمزگیری برای بزهکاران، پیچیده بوده و مستلزم دانش فنی برای طراحی تارنمای مجازی و نام الکترونیکی تقلبی است. به‌همین دلیل، انگیزه مالی می‌تواند چنین عملیاتی را توجیه کند. برای شرکت‌ها و مؤسسات مالی، رمزگیری می‌تواند موجب بدنامی (بی‌اعتباری) و از دست‌دادن مشتری شود، به‌ویژه از آن جهت که طراحان عملیات مجرمانه رمزگیری، اطلاعات شخصی مشتریان متعددی را از مؤسسه واحد به‌دست آورده و اقدام به سوءاستفاده می‌نمایند. رمزگیری، درصورتی‌که تنها با هدف جرایم مالی انجام می‌گیرد، بزه خاص به‌شمار می‌آید که نمی‌توان معادل دقیقی برای آن در قوانین موضوعه کشورمان یافت. مجموعه عملیاتی که انجام می‌گیرد، درصورتی‌که منتهی به بردن مال شود، کلاه‌برداری یا در حکم آن محسوب می‌شود. همچنین عملیاتی که از طریق آن شخصی، به‌طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی یا ارتکاب اعمالی از قبیل واردکردن، تغییر، محو، ایجاد یا متوقف‌کردن داده‌ها یا مختل‌کردن سامانه وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، کلاه‌برداری است.

این طرز تلقی از کلاه‌برداری رایانه‌ای، باوجود ماده ۱ «قانون تشدید مرتکبین ارتشاء، اختلاس و کلاه‌برداری» که جرم کلاه‌برداری را به‌طور دقیق تعریف می‌کند، مایه انتقاد است. به‌نظر می‌رسد مقنن فرض را بر این گذاشته که دادرس یا عموم مردم، معنای کلاه‌برداری را می‌دانند و نیاز به ذکر «عملیات متقلبانه» به‌عنوان رکن اصلی کلاه‌برداری در ماده ۱۳ قانون جرایم رایانه‌ای وجود ندارد. چنین به‌نظر می‌آید که تلاش قانون جرایم رایانه‌ای برای جرم‌انگاری تمامی تخلفاتی که در فضای مجازی ارتکاب می‌یابد، باعث دو اشکال عمده شده است: اول، دورشدن از تعریف منطقی بسیاری از جرایم که در قانون مجازات اسلامی تعریف شده‌اند. برای این اشکال می‌توان ماده ۱۲ قانون جرایم رایانه‌ای را مثال زد که تعریف جدید از سرقت ارائه می‌دهد؛ دوم این‌که تعریف موسع از جرایم مختلف، باعث تداخل ارکان مادی و روانی بسیاری از آن‌ها می‌شود، درنتیجه فعل واحد ممکن است بدون هیچ منطقی، عناوین مجرمانه متعدد داشته باشد.

ماده ۶۷ قانون تجارت الکترونیک[1] تعریف دقیق‌تری از کلاه‌برداری رایانه‌ای ارائه می‌دهد. معلوم نیست که باوجود این ماده، چرا قانون جرایم رایانه‌ای، ماده ۱ را با ایرادات اساسی، به جرم کلاه‌برداری مرتبط با رایانه اختصاص داده است. در هر حال، به نظر می‌رسد که کلاه‌برداری با عناوین مجرمانه ای همچون سرقت، برای توصیف جرم رمزگیری کفایت می‌کند، چراکه عملیات رمزگیری مستلزم مقدماتی همچون ایجاد پایگاه اینترنتی موهوم یا استفاده از پایگاه موجود است که خود می‌تواند به‌عنوان مجرمانه مستقلی داشته باشد (السان، ۱۳۸۸: ۱۸۴). بند «ب» ماده ۱۲ قانون جرایم رایانه‌ای، «فروش انتشار و در دسترس قراردادن رمز عبور، کد دستیابی یا داده‌های رایانه‌ای یا هر نوع اطلاعات مشابه به‌طور غیرمجاز به‌نحوی‌که به‌وسیله سیستم رایانه‌ای یا

---

[1]- ماده ۶۷ ق.ت.ا: «**هرکس در بستر مبادلات الکترونیکی با 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 ... دیگران را بفریبد و یا سبب گمراهی سیستم‌های پردازش خود کار و نظایر آن شود و ازاین‌رو طریق برای خود یا دیگری وجوه، اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد، مجرم محسوب و علاوه‌بر رد مال به صاحبان اموال به حبس از یک تا سه‌سال و پرداخت جزای نقدی معادل مال مؤاخذه محکوم می‌شود.**»

مخابراتی یا داده‌های مربوط قابل دستیابی باشد» را جرم اعلام کرده بود. بند «ب» ماده ۲۵ قانون جرایم رایانه‌ای با کوتاه‌کردن عبارت فوق، قید «بدون رضایت» (دارنده) را علاوه بر غیرمجاز به متن پیشین افزوده است.

اما مقابله با رمزگیری جنبه پیشگیری نیز دارد. کار گروه آمریکایی مبارزه با رمزگیری، تخمین می‌زند که تنها در دو هفته از ماه دسامبر ۲۰۰۳، بیش از ۹۰ حمله رمزگیری با ارسال بیش از ۶۰ میلیون نامه الکترونیکی جعلی در اینترنت انجام گرفته و ۵ درصد از گیرندگان نامه‌ها، یعنی ۳ میلیون نفر در دام شکارچیان گرفتار شده‌اند. آمار دقیق زیان‌های وارده به صنعت و تجارت الکترونیکی، به‌دلیل منافع تجاری اینترنت و خودداری از ایجاد نسبت به ایمنی آن منتشر نشده است (Chesut, 2005: 13). برای پیشگیری از دچارشدن در دام رمزگیری، راهکارهای متعددی پیشنهاد شده است که اغلب جنبه پیشگیرانه دارد و به مهم‌ترین آن‌ها اشاره می‌شود:

– احتیاط شدید در مورد آن دسته از نامه‌های الکترونیکی که از اشخاص ناشناس دریافت می‌شود.

– در نظرگرفتن رمزهای عبور متفاوت برای حساب‌های بانکی متعدد، به‌نحوی‌که با فاش‌شدن یکی، حساب‌های دیگر در معرض خطر قرار نگیرد.

– از کلیک‌کردن بر روی لینک‌هایی که در نامه‌های الکترونیکی مشکوک داده می‌شود، باید خودداری کرد. به‌جای آن، کاربر (مشتری) می‌تواند لینک صحیحی که در اختیار دارد یا آن را از طریق موتورهای جستجو (گوگل، یاهو و ...) به‌دست می‌آورد، وارد کرده و درنتیجه مطمئن شود که وارد تارنمای جعلی نشده است.

– تماس تلفنی با مؤسسه مالی که حساب بانکی یا مالی نزد آن قرار دارد، چراکه بسیاری از مؤسسه‌های مالی، رمز عبور و سایر اطلاعات شخصی را از طریق نامه الکترونیکی (که می‌تواند غیرایمن باشد)، درخواست نمی‌کنند. همچنین در عرف بانکداری، به‌روزکردن اطلاعات شخصی، امری فوری محسوب نمی‌شود که برای انجام آن از نامه الکترونیکی استفاده شود.

– نباید به نامه‌های الکترونیکی که در آن‌ها اطلاعات مالی خواسته نمی‌شود، به دلایل فوق پاسخ داد.

– نرم‌افزار ضد ویروس را باید به‌طور مستمر به‌روز کرد تا ویروس‌هایی را که می‌توانند باعث انتقال اطلاعات از رایانه یا سامانه رایانه‌ای شوند، شناسایی کرده و درصورت امکان، نابود سازد.

– باید از آخرین مرورگرها و سیستم‌های عامل استفاده کرد، چراکه آن‌ها می‌توانند از برخی از حملات پیشگیری کنند.

– حساب‌های برخط را باید به‌طور منظم بازرسی کرد.

نتیجه‌گیری

برخی جرایم مربوط به پرداخت‌های الکترونیکی یا در فضای عادی و سنتی رخ نمی‌دهند یا انجام‌دادن آن‌ها در فضای مجازی ـ نسبت به جهان عادی ـ بیشتر و آثار مالی و اقتصادی خطرناک‌تر دارد. تقلب در کارت اعتباری و وجه الکترونیکی، جعل پول الکترونیکی، رمزگیری، سرقت هویت، کلاه‌برداری، تخریب و اخلال در داده‌ها یا سامانه‌های الکترونیکی و افشای داده‌ها و تعرض به حریم خصوصی از مهم‌ترین جرایم بانکداری الکترونیکی است. بستر انجام بزه رایانه‌ای، فضای سایبر است و این نکته را می‌توان از تعبیر «... داده‌ها یا علائم موجود در کارت‌های حافظه یا قابل پردازش در سیستم‌های رایانه‌ای یا مخابراتی یا تراشه‌ها» که در بند «ب» ماده ۷۳۴ قانون مجازات اسلامی، بند «ب» ماده ۶ قانون جرایم رایانه‌ای آمده است، برداشت کرد. بنابراین همه رفتارهای مد نظر در این ماده باید از رهگذر کنش‌های رایانه‌ای و در بستر رایانه و مخابرات انجام شود. پس اگر کسی داده رایانه‌ای را چاپ کند یا از روی صفحه نمایشگر رایانه عکس بگیرد و سپس بر روی کاغذ چاپ‌شده، دگرگونی پدید آورد، جعل رایانه‌ای نخواهد بود. ایجاد اختلال در کارکرد سیستم رایانه‌ای جرمی است که با ایجاد هرگونه اختلال در عملکرد سیستم محقق می‌شود و باید قید ورود ضرر را نیز مورد توجه قرار دارد. ایجاد اختلال در کارکرد سیستم رایانه‌ای باید به اندازه‌ای باشد که به‌لحاظ عرفی اختلال عمده انگاشته

شده و اغماض‌ناپذیر باشد. سیر تحول جوامع کنونی به‌شدت باوجود سیستم‌ها و داده‌های رایانه‌ای گره خورده است.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانت‌داری در استناد به متون و ارجاعات مقاله تماماً رعایت گردید.

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: نگارش تمام مقاله برعهده نویسنده بوده است.

تشکر و قدردانی: از تمام کسانی که بنده را در تهیه این مقاله یاری رسانده‌اند، سپاسگزارم.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی سامان یافته است.

منابع و مآخذ

الف. منابع فارسی

– السان، مصطفی (۱۳۸۸). *جنبه‌های حقوقی بانکداری اینترنتی*. چاپ اول، تهران: انتشارات پژوهشکده پولی و بانکی.

– انصاری، باقر (۱۳۸۳). «حریم خصوصی و حمایت از آن در حقوق اسلام، تطبیقی ایران». *نشریه دانشکده حقوق و علوم سیاسی (دانشگاه تهران)*، ۱۵(۶۶): ۱–۵۴.

– زرکلام، ستار (۱۳۸۶). «حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا)». *پژوهشنامه حقوق اسلامی*، ۸(۲۵): ۱۷۳–۱۹۶.

– زیبر، ارلیش (۱۳۸۳). *جرایم رایانه‌ای*. ترجمه محمدعلی نوری و همکاران، چاپ اول، تهران: انتشارات گنج دانش.

– شیرزاد، کامران (۱۳۸۸). *جرایم رایانه‌ای* .چاپ اول، تهران: نشر بهینه فراگیر.

– صادقی نشاط، امیر (۱۳۸۶). «حقوق تجارت الکترونیک». *مجله کانون سر دفتران و دفتر یاران*، ۲۳(۷۵): ۶۴–۷۵.

ب. منابع انگلیسی

- Chesut, R (2005). *The e- commerce safety Guide*. 1st ed., Bija: Publishers PayPal eBay.

- Frank, R.S & Carol Cagwin, L (2001). *Credit Card Frud In Ency clo pedia of Criminology and Deviant Behavior*. Edited by Cliftom D. Bryant , Vol 2, 1st ed., Bija: Taylor and Francis Publishers .

- Hans,V.H (2001). *The Law of International Trade*. 2nd ed, London: Publishers Sweet & Maxwell,.

- Javelin Strategy & Research (2011). *Identiy Fraud survey Report consumer version (prevention Detection-Resolution*. 1st ed., USA: University Publications California.

- Lcncy, J. L (2005). "Jennifer Identiy Theft in cyberpace Crime control Methods and and Their Effectiveness in combating Phishing Attacks". *Berkeley Technology Law Journal*, 5(20): 259-260.

- Rogert, J (2005). *The New Old Law of Electronic Money(Boston College Law School Faculty Papers*). 1st ed., Boston: University Publications Boston.

- Shitds, L.K (2000). "Logal Aspects of Electronic Contracts in the New Regime". *Available at: WWW. Ikshicids .ic.publications documents articles/pubo13.pdf*.

- Simmons, B. A (2000). "Moncy and the Law Why ompty with the Public International Law of Moncy ?". *Yale Journal of International Law*, 5(15): 323-326.

- Smedinghoff, T. J (2005). "The Legal Requitements for Creating Secure and Enforecable Electronic Transsction". *Journal of International Monctary Fund Current Developments in Monetary and Financial Law*,1(3): 54

- Smith, G (2002). *Internet Law and Regulation*. London: Publications Sweet & Maxwell.

- Arbaugh, W. A; Farber, D & Smith, J. M (1997). *A Secure and Reliable Bootstrap Architecture (In SP 97 Proceeding of the IEEE*

Symposium on Security and privacy). Bija: Anonymous Publications.'

- Pushcharovsky, Yu (2010). "Tectonic Structure and Geodynamics of the Divide between the Atlantic". *Journal of International Geotectonics*, 3(44): 228.