بررسی جرایم بانکداری الکترونیک با تاکید بر حقوق ایران

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، علاوه بر منافع، خطرات و ریسکهایی را نیز با خود به همراه 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.سوال مهمی که در این تحقیق بررسی شد این است که رویکرد جنایی ایران به جرایم بانکداری الکترونیک چگونه قابل ارزیابی است؟ یافته های تحقیق بر این امر دلالت دارد که در حقوق کیفری ایران، قوانین ویژه ای در زمینه جرایم بانکی تدوین نشده و عمدتا، قانون جرایم رایانه ای بر جرایم بانکداری الکترونیک حاکم است. در این تحقیق از روس تحلیلی توصیفی استفاده شده است.

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

۱- مقدمه

انقلاب فناوری اطلاعات بطور بنیادین جوامع را دستخوش تغییر و تحول نموده و اکنون به سختی می توان بخش هایی از جامعه را یافت که تحت تاثیر خود قرار نداده باشد. در دسترس بودن فناوری اطلاعات و جستجوی اطلاعات موجود در آن بدون توجه به فواصل جغرافیایی موجب رشد سرسام آور این اطلاعات و ارتقاء سطح دانش بشری گردیده است. لذا این اطلاعات، باعث افزایش تغییرات اجتماعی و اقتصادی غیر قابل پیش بینی در زندگی بشری شده است. پیشرفت در فناوری اطلاع رسانی و ارتباطات شبکه های اطلاعاتی جهت افزایش سرعت و کیفیت در ارائه خدمات، بانکداری را نیز تحت تأثیر خود قرار داده است[۱]. بانکداری الکترونیک میتواند کارایی و رقابت پذیری یک بانک را افزایش دهد، بنابراین مشتریان موجود و بالقوه میتوانند از درجه تسهیلات بالاتری در تراکنشها و معاملات، بهرهمند شوند. زمانیکه این تسهیلات ارائه

[۱] - شیرزاد، کامران، جرایم رایانه ای، تهران، نشر بهینه فراگیر،چاپ اول، ۱۳۸۸، ص ۳۲

شده توسط بانک، با خدمات جدید ترکیب می شوند، می توانند مشتریان نهایی بانک را فراتر از بازارهای سنتی، بسط و توسعه دهند. در نتیجه، مؤسسات مالی در پذیرش قابلیت‌های بانکداری الکترونیک که شامل سیستم های بازاریابی پیچیده، امکان بانکداری از راه دور و برنامه های ارزش اندوخته میباشد، در حال تکاپو هستند. ایران با برخورداری از اقتصاد در حال توسعه، در چند دهه اخیر گامهای اساسی در زمینه بکارگیری فناوری اطلاعات و ارتباطات در عرصه های مختلف کسب و کار ، بویژه بانکداری نوین برداشته است که از آن جمله می توان به راه اندازی دستگاههای خودپرداز، شبکه تبادل اطلاعات بین بانکی (شتاب) به خدمات اینترنتی یانکها و غیره اشاره نمود. با وجود این، بانکداری الکترونیکی در ایران نسبت به کشورهای پیشرفته و پیشرو در این زمینه ها فاصله بسیار زیادی دارد و برای رسیدن به آن نیازمند تلاش والای فعالان صفت بانکداری کشور است . با تاکید بر چشم انداز بیست ساله ایران و دستیابی به جایگاهی برتر در منطقه خاورمیانه و همچنین تاکید بر برنامه چهارم توسعه، براقتصادی متعامل با اقتصاد جهانی مبتنی بر فناوری اطلاعات چاره ای نخواهیم داشت که با بانکداری الکترونیکی توانمند و هوشمند پاسخگو، روربرو شویم.

البته باید توجه داشت که پیشرفت های نوین بانکی از برخی پیامدهای منفی نیز مبرا نبوده است و پیدایش انواع جرایم نوین در بهره برداری از فناوری اطلاعات، بخش جدیدی ازآن به شمار می رود. جرایم خدمات نوین بانکی شامل دو گروه از جرایم می شود؛ گروه اول شامل جرایمی هستند که با مقررات مربوط به جرایم کلاسیک قابل پیگیری و مساوات هستند و نیازی به تصویب قوانین جدید ندارند و گروه دوم شامل جرایمی هستند که قبل از تولد و رشد بانکداری نوین به هیچ وجه امکان ارتکاب آن وجود نداشته است. به علاوه عواقب و پیامدهای فناوری محرمانه می تواند خیلی بیشتر از گذشته و غیر قابل تصور باشد. چرا که مصونیت های جغرافیایی یا مرزهای ملی، آنرا محدود می کند که موجب سوء استفاده گسترده، مجرمین به ویژه گروههای جنایتکار سازمان یافته، از سیستم های الکترونیکی بانکها گردیده است. سوال اصلی که در این خصوص مطرح است این است که رویکرد جنایی ایران در قبال جرایم نوین بانکی چیست؟ فرضیه تحقیق نیز بدین شکل قابل طرح است که در حقوق کیفری ایران، جرایم خدمات نوبن بانکی در قالب جرایم رایانه ای قابل تعقیب می باشد و نظام حقوقی ویژه ای در این خصوص وجود ندارد. به منظور بررسی سوال و فرضیه مورد اشاره در ادامه جرایم بانکداری الکترونیکی بررسی می شود.

۲- تقلب در کارت اعتباری و وجه الکترونیکی

با جایگزین شدن کارت اعتباری به جای اسکناس در طی زمان، بزهکاری مالی در این حوزه نیز به تناسب همین انتقال جابه شده است. بنابراین ، تقلب در کارت عای اعتباری با همان انگیزه و محرک هایی انجام می گیرد 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 کارت های اعبتاری، در مقایسه بل دیگر جرایم پولی ، به دلیل نو بودن روش های الکترونیکی پرداخت دشوار تر است . حال آنکه در عمل خلاف این موضوع اثبات شده است[1].

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 الکترووینکی ممکن است و چنانچه پاسخ مثبت باشد، خسارت بر عهده چه کسی خواهد بود؟ اگر کالایی مانند خودرو سرقت شود، حتی اگر مورد معاملات متعدد قرار گیرد، اصولاً مالکیت مالک اصلی بر آن باقی می ماند. چنین قاعده ای درباره پول اجرا نمی شود. اگر شخص مقداری پول بربابد و با آن کالایی بخرد ، ثمن در مالکیت بایع وارد می شود، حتی اگر سارق بر آن ید مشروع نداشته باشد. به موجب قانون بروات انگلیس مصوب ۱۸۸۲، «سندی قابل انتقال به حساب می آید و بر طبق همین قانون کسی که با حسن نیت اوراق بهادار را به دست می آورد، صرف نظر از منشا مالکیت و اینکه از چه راهی آن را تحصیل می نماید، مالک شناخته می شود». اکنون پرسش آن است که آیا چنین قاعده ای را می توان درباره وجه الکترونیکی نیز اجرا کرد؟ در تطبیق با قانون ۱۸۸۲ باید اظهار داشت که روح قانون بیشتر اسناد مکتوب را در برمی گیرد، اما اگر استفاده از وجه الکترونیکی به قدری شیوع یابد که جایگزین

[1] - Frank, R .Scarpitti & Carol cagwin ,Lenhart,Credit Card Frud,In: Encyclopedia of Criminology and Deviant Behavior,Edited by Cliftom D. Bryant ,Vol.II, Brunnner-Routledge /Taylor and Francis Publishers ,2001.pp.106-109.at106

پول شود و مالک اولیه از لحاظ ثبت، نام مالک برای آن متصور نباشد، می توان اعتقاد داشت که واجد وصف انتقال بوده و لذا قاعده فوق در مورد آن مجری خواهد بود[۱].

۳-جعل پول الکترونیکی

با وجود، دستگاه های نوین امکان کشف جعل در پول الکترونیکی نسبت به پول کاغذی بسیار آسان تر است. این فرض تقویت شده است که از لحاظ ایمنی این نوع از وسایل اعتباری در رتبه برتری قرار دارند. به منظور اجتناب از جعل، اسم رمزی که در پول الکترونیکی به کار می رود باید به گونه ای باشد که قابلیت افشا شدن نداشته باشد. برای تحقق این موضوع از توانمندی مهندسانی بهره گیری می شود که با فنون جعل و راه های مقابله با آن آشنایی دارند. یا وجود این، هیچ گاه نمی توان مدعی شد که جعل پول الکترونیکی قابل تصور نیست.

در عین حال این ادعا مطرح شده که امکان جعل اسناد الکترونیکی ساده تر از اسناد کاغذی است؛ زیرا به طور مثال، صادر کننده می تواند سندی را پس از ارسال تغییر دهد و مدعی شود که تغییر از جانب او نبوده است.[۲] به هر روی، بحث اصالت قابلیت اعتماد[۳] یکی از بحث های با اهمیتی است که درباره اسناد الکترونیکی مطرح می شود.

در مقایسه باپول سنتی باید مدعی شد که پرداخت با پول الکترونیکی جعلی ایفای تعهد محسوب نمی شود و از لحاظ سقوط تعهد یا بدهکار کردن طرف مقابل، فاقد هر گونه اثر حقوقی است. به لحاظ نظری، مسئولیت برکسی تحمیل می شود که در فرض پرداخت های متعدد به موجب پول جعلی واحد، زنجیره تادیه از او آغاز شده است. با وجود این، از آن رو که گاه یافتن مسئول اصلی دشوار است، به لحاظ عملی و برای اجتناب از سردرگمی، خسارت بر کسی تحمیل می شود که به هنگام کشف جعل پول مذکور را در اختیار داشته است.[۴]

---

[۱] - زیبر، ارلیش، جرایم رایانه‌ای، ترجمه محمدعلی نوری و رضا نخجوانی و مصطفی بختیار وند و احمد رحیمی مقدم، تهران: نشرگنج دانش، چاپ نخست، ۱۳۸۳، ص ۴۱
۱- صادقی نشاط، امیر، حقوق تجارت الکترونیک، مجله کانون سر دفتران و دفتر یاران ،شماره ۷۵، آذر ۱۳۸۶، ص ۶۹.

2- ICA ,Authenticity of Electronic Records (ICA Study 13-1),Report prepared for UNESCO,by the International Council on Archives Committee on Archival Legal Matters,November ,November 2002 ,At www.ica.org/download .phpid=1624

3- Smith, Graham (Bitd & Bitd)and other Review by Eduatdo Uataran ,Internet Law and Regulation , Sweet & Maxwell,London 2002,p.506

این حالت نیز قابل تصور است که کشف جعلی بودن پول الکترونیکی به هنگام در جریان بودن آن، ممکن نباشد، اما آن گاه برای تبدیل آن به ارز واقعی مراجعه می شود، این موضوع کشف شود، بدین طریق که به طور مثال معلوم شود دو یا چند پول الکترونیکی با شماره سریال واحد موجود است. در چنین مواردی، به مثابه اصل، خسارت بر کسی تحمیل می شود که به منظور دریافت ارزش واقعی پول الکتروینکی اقدام کرده است. این نکته بدیهی است که حق مراجعه افراد مذکور به مسئول واقعی با رعایت قواعد عام حقوق مسئولیت مدنی هیچ گاه منتفی نیست.

حالت قابل تصور دیگر آن است که حتی به هنگام تبدیل به ارزش واقعی، به طور مثال پول کاغذی نیز، جعلی بودن پول الکترونیکی قابل تشخیص نباشد. افزون بر این ممکن است تشخیص اینکه کدامیک از دو پول الکترونیکی که شماره سریال واحد دارند جعلی است، دشوار یا ناممکن باشد و به همین دلیل بانک اجبار داشته باشد که هر یک از آنها را به ترتیب مراجعه تادیه کند. به نظر می رسد که در این باره، حقوق، قاعده ویژه ای ندارد و این ادعا که بانک باید پول نخستین را تبدیل کرده و پول دوم را از لحاظ زمان مراجعه جعلی محسوب کند به هیچ وجه منصفانه به نظر نمی رسد؛ زیرا هیچ دلیلی موجود نیست که ثابت کند پول نخستین قانونی و پول دوم جعلی است. وانگهی، چه بسا از لحاظ تاریخ صدور، پول دوم بر پولی که به لحاظ زمانی زودتر برای تبدیل به ارزش واقعی به بانک یا موسسه مالی ارائه شده است، مقدم باشد .

اگر نظام تبدیل به ارزش واقعی بانک، خواه به طور تصادفی یا به دلیل توافقنامه خاصی که با مشتریان دارد، اقدام به طی فرایند تبدیل به پول الکترونیکی جعلی کرده و سرانجام بانک ناچار از ایفا شود، درآن صورت پرسشی که می توان مطرح کرد آن است که زیان به چه کسی تحمیل می شود؟ به ظاهر در این باره، بانک، زیاندیده واقع می شود، اما بانک ها اغلب برای اخذ این مبالغ به صورت تخمینی از مشتریان خود در قالب کارمزد یا خدمات ویژه یا بهره، تدابیری اتخاذ می کنند.

وضعیت های مذکور و تحمیل مسئولیت بر افرادی که در بیشتر موارد مسئول واقعی جعل و تزویر در پول الکترونیکی به شمار نمی آیند، ممکن است مقبولیت پول الکترونیکی را در معرض خطر قرار دهد. به همین دلیل باید برای این موردها چاره ای اندیشیده شود و به طور مثال، مسئولیت به بانک یا موسسه مالی تحمیل شده و از این راه ، میان تمامی کاربران پول الکترونیکی توزیع شود.

برخی کشورها مقررات آزاد و منعطفی برای نقل و انتقال سرمایه و معاملات ارزی دارند. به طور مثال، بحرین، هنگ هنگ، پاناما و سنگاپور از این جمله اند. برخی کشورهای دیگر به منظور حمایت از پول رایج داخلی محدودیت های مبادلاتی را حفظ کرده اند.[۱] چنین محدودیت هایی علاوه بر اینکه بر پرداخت های مربوط به انتقال سرمایه اعمال می شود، بلکه در مورد تمامی معاملات ارزی مجری خواهد بود. بیشتر کشورها مقررات و تشریفات مربوط به معاملات ارزی خود را حفظ کرده اند. با این همه، ماده ۸ (بخش ۲ الف) توافقنامه بین المللی اعتبار پولی،[۲]دولت های عضو را از تحمیل محدودیت هایی در زمینه پرداخت و انتقالات مربوط به معاملات ارزی پیش از تصویب توافقنامه مذکور منع می کند. این مقررات از سوی کشورهایی وضع شده است که پول رایج داخلی آن ها در معاملات و پرداخت های بین المللی کاربرد دارد. ایران از جمله کشورهایی است که به رغم عضویت در توافقنامه، مفاد ماده مذکور را نپذیرفته است.[۳]

پرسشی که درباره پرداخت های الکترونیکی می توان مطرح کرد آن است که این شیوه های پرداخت تا چه حد موجب تحول در مقررات و محدویت های مربوط به انتقال ارز و اعتبار شده است؟ این پرسش بیشتر از این نگرانی ناشی می شود که ممکن است با پیشرفت روز افزون پرداخت های اینترنتی، نظریه از کنترل خارج شدن این پرداخت ها از دامنه اقتدار دولتها و شمول قوانین و مقررات مطرح باشد. به عبارتی، اگر به طور مثال پرداخت های اینترنتی کارتی با به کار گیری کارت های آمریکایی و بر مبنای دلار انجام گیرد و مصرف کننده برای تهیه کارت وادار به خرید کارت پرداخت از هر نقطه جهان ، مجبور به تادیه به دلار باشد، در آن صورت، به طور قطع مشکلات اقتصادی از بابت خروج بی رویه و حساب نشده ارز از کشور مطرح خواهد بود. اشکال مذکور تا حدود زیادی وارد است، زیرا به ویژه در کشورهایی که برای پرداخت های الکترونیکی نظام شخصی فراملی ندارند، تاجر، یا مصرف کننده ای که به خرید کالایا خدمات ویژه ای نیاز دارد، ممکن است وادار به خرید کارت پرداخت خارجی شود که دست کم، لازمه آن، تبدیل پول داخلی به پول همان کشور است.

انجام گرفتن چنین مبادله های پولی، خود ممکن است با مقررات ارزی منافات داشته و شخص، بدون اطلاع دولت خود بدان اقدام کرده باشد یا در فرض آگاه شدن دولت متبوع خود از داشتن آن کالا یا خدمات ممنوع شود. همان طور که بدیهی به نظر می رسد، این مشکل بیشتر به کشورهای جهان سوم ارتباط می

1- Simmons ,BA, "Moncy and the Law : Why ompty with the Public International Law of Moncy ?" Yale Journal of International Law ,2000.pp.323-326.
2-International Monetary Fund {IMf} July 22,1944: Entered force December 27,1945
3- Hans ,Van Houtte,The Law of International Trade,2nd ed, Sweet &Maxwell, London, 2001.p.318.

یابد، چرا که کشورهای پیشرفته، هر یک نظام، تشریفات و شیوه های متنوعی برای پرداخت های الکترونیکی در سطح بین المللی داشته و حتی ایده « بانکداری اینترنتی » را عملی ساخته اند. برطرف کردن مشکل نیز بیش از آنکه جنبه حقوقی داشته باشد، مستلزم گسترش فرایند پرداخت الکترونیکی است. به هر روی، نباید فراموش کرد که پرداخت های الکترونیکی هیچ گاه نافی یا محدود کننده مقررات آمره پولی، بانکی و ارزی نبوده است و اگر در این باره تقلب به مسامحه ای صورت گیرد، ناشی از محدودیت ها و ضعف نظام پرداخت کشورهایی ست که همسو باتحولات جهان پیشرفت نکرده است.

ماده ۶ قانون جرایم رایانه ای، تغییر یا ایجاد داده های قابل استناد یا ایجاد یا وارد کردن متقلبانه داده به آنها، تغییر داده ها یا علایم موجود در کارتهای حافظه یا قابل پردازش در سامانه های رایانه ای یا مخابراتی یا تراشه ها یا ایجاد یا وارد کردن متقلبانه داده ها یا علایم به آنها را به عنوان جعل، قابل مجازات دانسته است. کیفر نسبتا شدیدی هم برای این جرم در نظر گرفته شده که عبارت است از حبس یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال، یا هر دو.

دسترسی غیرمجاز به سامانه های الکترونیکی، به طور قطع، محرمانگی اطلاعات موجود در آنها را در معرض خطر قرار می دهد. اما خطر وقتی جدی تر می شود که شخص با دسترسی به سامانه، تمامیت و قابلت دسترسی اطلاعات را در سامانه دستخوش تغییر کرده یا داده های دلخواه خود را به آنها بیافزاید. نتیجه تغییر غیرمجاز در داده ها می تواند ناهماهنگی در سامانه یا حتی خطر مرگ باشد. کما اینکه در یک پرونده[1] 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 می گردد. تغییر در داده می تواند تعاملات تجاری را با اخلال جدی روبرو سازد. در یک پرونده[2] شخصی با هک کردن یک سامانه مالی، داده هایی به آن وارد کرد که مانع از ذخیره داده های مالک سامانه می شد. هر چند در انگلیس، در اینکه جرم، تغییر غیرمجاز این موارد را در بر می گیرد یا خیر، اختلاف وجود دارد؛ اما اگر چنین موضوعی در ایران طرح شود، با استناد بند(ب) ماده۶ قانون جرایم رایانه ای. جعل رایانه ای محسوب خواهد شد.

---

[1] –R.v.Rymer(1993), Times, 21December1993.

[2] - Zezev and Yarimaka v Governor of HM Prison Brixton and another, CACD , Cr App R 33. Coram: Lord Chief Justice Lord Woolf, Wright J Ratio: Wright J said: 'But if an individual,2002,P.33.

برای تحقق جرم جعل رایانه ای لازم نیست که مرتکب از این کار نفعی ببرد. همچنین، ضرورتی ندارد که عامل بداند فعل او در تغییر داده ها یا وارد کردن داده ها یا علایم به نحو غیرقانونی، کدام قسمت از سامانه را دستخوش تغییر ساخته یا در معرض خطر قرار می دهد. باید توجه داشت که این جرم می تواند علیه دارنده حقوق مالکیت فکری ادعا شده و به نتیجه هم برسد. چنانچه در یک پرونده[1]، پدید آورنده نرم افزار، یکی بمب منطقی[2] در آن طراحی کرده بود که در فرض بروز اختلاف در پرداخت، نرم افزار را از کار می انداخت.

متهم، ادعا می کرد که چون به موجب قرارداد، کلیه حقوق مالکیت فکری مربوط به نرم افزار را دارد، بنابراین حق هرگونه تغییری را در آن داشته است. با وجود این استدلال، دادگاه رای داد که وجود حق مالکیت فکری، اختیار ایجاد مانع در راه اجرای نرم افزار را به وجود نمی آورد؛ مگر اینکه در قرارداد طرفین شرط می شد که برای مثال، «در فرض عدم پرداخت قیمت، نرم افزار کار نخواهد کرد». دادگاه پدیدآورنده را مجرم شناخت و از جمله به این موضوع توجه کرد که نباید صرف تضمین پرداخت این حق را ایجاد کند که پدیدآورندگان نرم افزار بتوانند هر موقع که بخواهند آن را از کار انداخته و در نتیجه زیان مادی قابل توجهی به استفاده کننده وارد سازند.

چنانچه در ماده ۷ و۸ قانون جرایم رایانه ای مورد توجه قرار گرفته، جعل رایانه ای ممکن است با هدف استفاده از داده ها یا کارت یا تراشه های مجعول برای اهداف دیگر باشد. کما اینکه، حمله به یک سامانه و تحریف داده های آن، می تواند به منظور تخریب داده هایا ایجاد اخلال در عملکرد سامانه باشد. در حقوق انگلیس، به جای طرح دو جرم متفاوت، یعنی جعل رایانه ای و تخریب و اخلال در داده ها، جرم واحدی به نام «تغییر غیر مجاز»[3] وجود دارد که تمامی این موارد را شامل می شود.

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

---

[1] –Rogert, James S , "The New Old Law of Electronic Money",Boston College Law School Faculty Papers, 39 ,March 3 ,2005.P.79.

[2] - Logic bomb

[3] - Unauthorized Modification

۴- رمزگیری

رمزگیری یا فیشنگ،[1] کنایه از ماهیگیری[2] است که در آن شکارچی قلاب یا تور خود را در محیط هایی که طعمه فراوانی برای صید وجود دارد، یا در فضای مجازی، آنجا که استانداردهای ایمنی به درستی مراعات نشده یا مشتری برای یک لحظه بی احتیاطی می کند، پهن می نماید. حربه معمول در رمزگیری آن است که شخص رمزگیر،[3] یک نامه الکترونیکی که به نظر می رسد از موسسه مالی مشتری(بزه دیده) یا تارنمای تجارت الکترونیکی وی ارسال شده، برای قربانی می فرستد. 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 می شود. به طور معمول، در نامه الکترونیکی به گیرنده گفته می شود که باید اطلاعات حساب وی، در جهت پیشگیری از کلاهبرداری یا به دلیل نقض فنی که پیش آمده، یا سایر مسایل امنیتی به روز شود. بزهکار حتی یک رابط(لینک) به مشتری می دهد تا از آن طریق به پایگاه اصلی وصل شود و مطمئن شودکه اطلاعات را موسسه مالی وی ارسال کرده است. در حالی که پایگاه(تارنمای) مذکور هم ساختگی است.[4] با مشاهده این ظواهر، مشتری حاضر می شود که اطلاعات شخصی خود را ارایه نموده و رمز عبور خویش را به روز کند. در نتیجه، بزهکار به اطلاعات دقیق وی دست می یابد و از آنها می تواند برای اقدامات مجرمانه بعدی(برداشت از حساب، انتقال وجه، و...) استفاده کند.

یکی از روش های تقلب در پرداخت های الکترونیکی ، فیشینگ ،[5] نسخه برداری یا دو نسخه نویسی کردن است. در این روش با ادعای قانونی بودن شرکت/ موسسه، ار راه های گوناگون، از جمله نامه الکترونیکی از افراد خواسته می شود که شماره کارت اعتباری و دیگر اطلاعات شخصی خود را ارائه کنند. با توجه به جعلی بودن پایگاه های اینترنتی که از نظر ظاهری تقریباً هیچ تفاوتی یا پایگاه واقعی ندارد، ممکن است مشتری دچار اشتباه شده و شناسه های 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

---

1 - Phishing.
2 -Fishing
3 –Phisher
4 -Lcncy ,Jennifer, Lynch, Jennifer Identiy Theft in cyberpace: Crime control Methods and and Their Effectiveness in combating Phishing Attacks, Berkeley Technology Law Journal. Vol. 20, 2005, pp:259- 260.
۱- Phishing : شبیه سازی پایگاه اینترنتی موجود به منظور فریب کاربران به ارائه اطلاعات فردی یا مالی فاش کردن رمز عبور {منبع :فرهنگ لغت Babylon}

می شود که به شماره حساب های بانکی افراد دسترسی یافته یا پیشینه الکترونیکی آنان را برای سرقت هویت به دست آورند[۱].

در امریکا سازمان بازرسی فدرال[۲] برای شناساسی این دسته از تقلب ها «مرکز دادخواهی تقلب اینترنتی[۳]» را تاسیس کرده است تا از سرقت هویت، کارت اعتباری و تقلب در حساب ها جلوگیری کند. اقداماتی نیز با هماهنگی دیگر کشورها برای جلوگیری از این دسته از جرایم رایانه ای انجام گرفته است.[۴] می توان ادعاکرد که پیشگیری از جرایم اینترنتی مرتبط با بانکداری مستلزم همکاری، هماهنگی و تعامل میان کشورهاست و نمی توان بدون تدوین مقررات و دستور العلمل های متحد الشکل به نتایج پایداری دراین زمینه دست یافت. با توجه به گستره و شمول روابط مالی الکترونیکی که از حدود و مرزها فراتر میرود، کنترل جرایم مالی در فضای مجازی نیز فقط در صورتی امکان خواهد بود که زمینه مشارکت همه دولت ها و موسسه های بین المللی مرتبط فراهم شود.

برای پیشگیری از این دسته از جرایم، بانک ها می توانند به مشتریان خود یادآوری کنند که موسسه مالی آنها هیچ گاه اطلاعات محرمانه را از طریق نامه الکترونیکی از آنان درخواست نخواهد کرد و آن ها 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 تامل درنظر گرفته شود:

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

- داده پیام های مربوط به مشتریان قابل بازیابی، بازبینی و بازرسی باشد و سیستم رایانه ای به گونه ای برنامه ریزی شود که تغییرات غیر سازمانی– خارج از روال بانکی- در آن آشکار شود.

- شناساندن پایگاه/ پایگاه های اینترنتی که ارتباط با بانک منحصراً از طریق آن ها امکان پذیر است و سفارش به مشتریان برای اجتناب از پاسخگویی به نامه های الکترونیکی یا دعوت نامه های مشکوک.

---

[1] - Smedinghoff,T,J,"The Legal Requitements for Creating Secure and Enforecable Electronic Transsction ",International Monctary Fund: Current Developments in Monetary and Financial Law,Vol.3,April 2005,P.54

[3] - FBI { Federal Bureau of Investigation }
2-Mark T Gillet," Obrea Poindexter ; M Sean Ruff,Developments in Cyberbanking The Business Lawyer 2005;Feb 2005:60,2.p.1336

- بالا بردن اطلاعات مشتریان از طریق ارائه اطلاعات فنی، قانونی و علمی لازم به آنان و یادآوری ضرورت گزارش دادن موارد مشکوک به پلیس، نیروهای امنیتی و سیستم بانکی.

- بررسی صورت حساب ها به وسیله مشتری به صورت محرمانه و ارائه نکردن رمزها و شماره های کلید به دیگر افراد.

- فراهم ساختن امکان تغییر رمز برای مشتریان از سوی بانک.

- تنظیم برنامه ای برای شناسایی و اعلام نامه های الکترونیک متقلبانه به مشتریان و اعلام احتیاط به آنان.

- ارتباط با پلیس اینترنتی و گزارش دادن 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[۱] یا جرایم مشابه می کند، اصولاً دستگیری او نیز چاره ساز نیست؛ چرا که به مثابه نوجوان بودن از مسئولیت کیفر ی مبرا بوده و در عمل برای جبران خسارتی که در حجم وسیع وارد کرده است، وجهی دراختیار ندارد. بنابراین، قانونگذاری باید ضمن درک صحیح این واقعیت که بی اعتمادی مشتری را به روش های جایگزین ناامن نمی توان با شناسایی و کیفر بزهکاران منتفی ساخت، در پی ارائه و به روز رسانی استاندارد های ایمنی پرداخت های الکترونیکی باشد و در این باره سازمانی را که به ضوابط فنی و اصول حقوقی تسلط داشته باشد، مسئول مدیریت، نظارت و پاسخگویی کند[۲]. از آن رو که بحث های صرف علمی درباره ایمنی پرداخت های الکترونیکی از موضوع این مقاله خارج است از تفصیل بحث در این باره خودداری کرده و محققان را به منابع تخصصی مربوط که پاره ای از آن ها در زیر نویس ذکر شده است ارجاع می دهیم .[۳]

1-Markus J akson,"Moderling and Phishing Attacks,phishing Panel of Financial Cryptogaphy 2005 "; Tsow ,Alexx,Phishing with Consumer Electronics – Malicious Home Routers,School of Information ,Indiana University,At: www.13 s.de/-olmedilla /events/ MTW06 –papers/paper22.pdf.

2 - Shitds,L.K.(Solioitors) , "Logal Aspects of Electronic Contracts in the New Regime "2000, p. 14 .Available at: WWW. Ikshicids .ic.publications documents articles/pubo13.pdf.

2-W.A.Arbaugh;D.J.Farber , and Smith ,J.M, A secure and reliable bootstrap architecture, In SP 97 : Proceeding of the 1997 IEEE Symposium on Security and privacy ,pages 65-71, Washington ,DC,USA; Rachna Dhamija and J.D.Tyger The battle against phishing : Dynamic security skins ,In SOUPS 05 : Proceeding of the 2005 symposium on Usable privacy and Security ,pp.77-88,New Yourk ,NY ,USA,2005,ACM Press ,Javelin Strategy & Research.Identity theft survey report (consumer version),2006 Synovate .Federal trade commission identy

سرقت هویت[1] و کلاهبرداری در هویت،[2] عناوین دیگری است که برای توصیف دستیابی متقلبانه به اطلاعات شخصی افراد از قبیل شماره حساب و شماره تامین اجتماعی به کار می رود. اولین و غالب‌ترین خسارتی که به قربانیان رمزگیری وارد می شود، جنبه مالی دارد. در واقع، فرایند رمزگیری برای بزهکاران، پیچیده بوده و مستلزم دانش فنی برای طراحی تارنمای مجازی و نام الکترونیکی تقلبی است. به همین دلیل، انگیزه مالی می تواند چنین عملیاتی را توجیه کند. برای شرکتها و موسسات مالی، رمزگیری می تواند موجب بدنامی(بی اعتباری) و از دست دادن مشتری شود، به ویژه از آن جهت که طراحان عملیات مجرمانه رمزگیری، اطلاعات شخصی مشتریان متعددی را از موسسه واحد به دست آورده و اقدام به سوء استفاده می نمایند. رمزگیری، در صورتی که تنها با هدف جرایم مالی انجام می گیرد، بزه ی خاص به شمار می آید که نمی توان معادل دقیقی برای آن در قوانین موضوعه کشورمان یافت. مجموعه عملیاتی که انجام می گیرد، در صورتی که منتهی به بردن مال شود، کلاهبرداری یا در حکم آن محسوب می شود. همچنین، عملیاتی که از طریق آن شخصی، به طور غیرمجاز از سامانه های رایانه ای یا مخابراتی یا ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده ها یا مختل کردن سامانه وجه یا مال یا منفعت یا خدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند، کلاهبرداری است.

این طرز تلقی از کلاهبرداری رایانه ای، باوجود ماده یک «قانون تشدید مرتکبین ارتشاء اختلاس و کلاهبرداری» که جرم کلاهبرداری رابه طور دقیق تعریف می کند، مایه انتقاد است. به نظر می رسد، مقنن فرض را بر این گذاشته که دادرس یا عموم مردم، معنای کلاهبرداری را می دانند و نیاز به ذکر«عملیات متقلبانه» به عنوان رکن اصلی کلاهبرداری در ماده ۱۳ قانون جرایم رایانه ای، وجود ندارد. چنین به نظر می آید که تلاش قانون جرایم رایانه ای برای جرم انگاری تمامی تخلفاتی که در فضای مجازی ارتکاب می یابد، باعث دو اشکال عمده شده است: اول، دور شدن از تعریف منطقی بسیاری از جرایم که در قانون مجازات اسلامی تعریف شده اند. برای این اشکال می توان ماده ۱۲ قانون جرایم رایانه ای را مثال زد که تعریف جدید از سرقت ارایه می دهد. دوم اینکه، تعریف موسع از جرایم مختلف، باعث تداخل ارکان مادی و روانی

---

theft survey report ,2003:Ivan Remisk , " Secure online Card Activation Isnt ,Forrester ,April14,2005:Penny ,Gillespie and Michael Rasmussen ," Combating Fraud in Financial Services ," Forrester ,April 7,2004:ounce Labs ,Inc .Managing the Risk of Identity Theft:The Need for Software Security Assurance Topics White Paper;At www.ouncelabs .com /pdf/library /ID Theft .pdf.

[1] -Identiy Thft.

[2] -Identiy Fraud.

بسیاری از آن ها می شود. در نتیجه فعل واحد ممکن است بدون هیچ منطقی، عناوین مجرمانه متعدد داشته باشد.

ماده ۶۷ قانون تجارت الکترونیک،[۱] تعریف دقیق تری از کلاهبرداری رایانه ای ارایه می دهد. معلوم نیست که با وجود این ماده، چرا قانون جرایم رایانه ای، ماده ۱ را با ایرادات اساسی، به جرم کلاهبرداری مرتبط با رایانه اختصاص داده است. در هر حال، به نظر می رسد که کلاهبرداری با عناوین مجرمانه ای همچون سرقت، برای توصیف جرم رمزگیری کفایت می کند. چرا که عملیات رمزگیری مستلزم مقدماتی همچون ایجاد پایگاه اینترنتی موهوم یا استفاده از پایگاه موجود است که خود می تواند به عنوان مجرمانه مستقلی داشته باشد.[۲] بند(ب) ماده ۱۲ قانون جرایم رایانه ای، «فروش انتشار و در دسترس قراردادن رمز عبور، کد دستیابی یا داده های رایانه ای یا هر نوع اطلاعات مشابه به طور غیرمجاز به نحوی که به وسیله سیستم رایانه ای یا مخابراتی یا داده های مربوط قابل دستیابی باشد» را جرم اعلام کرده بود. بند(ب) ماده ۲۵ قانون جرایم رایانه ای با کوتاه کردن عبارت فوق، قید« بدون رضایت» (دارنده) را علاوه بر غیرمجاز به متن پیشین افزوده است.

اما مقابله با رمزگیری جنبه پیش گیری نیز دارد. کار گروه آمریکایی مبارزه با رمزگیری،[۳] تخمین می زند 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 نامه ها، یعنی ۳ میلیون نفر در دام شکارچیان گرفتار شده اند. آمار دقیق زیان‌های وارده به صنعت و تجارت الکترونیکی، به دلیل منافع تجاری اینترنت و خودداری از ایجاد نسبت به ایمنی آن منتشر نشده است.[۴] برای پیشگیری از دچار شدن در دام

---

[۱]- ماده ۶۷ ق.ت.ا: هر کس در بستر مبادلات الکترونیکی با سوء استفاده و یا استفاده غیر مجاز از اده پیام ها، برنامه ها و سیستم های رایانه ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف داده پیام، مداخله در عملکردبرنامه یا سیستم رایانه ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم های پردازش خود کار و نظایر آن شود و از این رو 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 سالو پرداخت جزای نقدی معادل مال مواخذه محکوم می شود».

[۲] - السان، مصطفی، جنبه های حقوقی بانکداری اینترنتی، چاپ اول، انتشارات پژوهشکده پولی و بانکی ، تهران،۱۳۸۸، ص۱۸۴.

[3] -U.S. Based Anti-Phishing Working Groub.

[4] –chesut, Robert, The e- commerce safety Guide, PayPal eBay 2005,p:13.

رمزگیری، راهکارهای متعددی پیشنهاد شده است که اغلب جنبه پیش گیرانه دارد و به مهمترین آنها اشاره می شود:[1]

- احتیاط شدید در مورد آن دسته از نامه های الکترونیکی که از اشخاص ناشناس دریافت می شود.

- در نظرگرفتن رمزهای عبور متفاوت برای حسابهای بانکی متعدد، به نحوی که با فاش شدن یکی، حسابهای دیگر در معرض خطر قرار نگیرد.

- از کلیک کردن بر روی لینک‌هایی که در نامه های الکترونیکی مشکوک داده می شود، باید خودداری کرد. به جای آن، کاربر(مشتری) می تواند لینک صحیحی که در اختیار دارد یا آن را از طریق موتورهای جستجو(گوگل، یاهو.....) به دست می آورد، وارد کرده و در نتیجه مطمئن شود که وارد تارنمای جعلی نشده است.

- تماس تلفنی با موسسه مالی که حساب بانکی یا مالی نزد آن قرار دارد. چرا که بسیاری از موسسه های مالی، رمز عبور و سایر اطلاعات شخصی را از طریق نامه الکترونیکی(که می تواند غیرایمن باشد)، درخواست نمی کنند. همچنین در عرف بانکداری، به روز کردن اطلاعات شخصی، امری فوری محسوب نمی شود که برای انجام آن از نامه الکترونیکی استفاده شود.

- نباید به نامه های الکترونیکی که در آن ها اطلاعات مالی خواسته نمی شود، به دلایل فوق پاسخ داد.

- نرم افزار ضد ویروس را باید به طور مستمر به روز کرد تا ویروس هایی را که می توانند باعث انتقال اطلاعات از رایانه یا سامانه رایانه ای شوند، شناسایی کرده و در صورت امکان، نابود سازد.

- باید از آخرین مرورگرها و سیستم های عامل استفاده کرد، چرا که آنها می توانند از برخی از حملات پیشگیری کنند.

- حساب های برخط را باید به طور منظم بازرسی کرد.

۵- سرقت هویت

[1] - Rosenberg,Arnold S, "Better than Cash ? Consumer Protection and the Global Debit Card Deluge ",Columbia Journal of Trananational Law 2004

استفاده از هویت دیگران در پرداختهای اینترنتی، یکی دیگر از جرایم بانکداری الکترونیک است که انجام می گیرد. در این جرم شخص، خود را به جای دیگری جلوه داده و تمام حقوق قانونی وی را دارا شده یا جرایمی را به نام او انجام می دهد. در برخی از کشورها، قوانین صریحی برای مقابله با سرقت هویت وجود دارد. برای مثال، در ایالات متحده آمریکا، قانون تشدید مجازات سرقت هویت،[1] مجازات دو سال حبس به همراه کیفر هرجرمی 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.[2] سرقت هویت اغلب برای ارتکاب جرایمی همچون کلاهبرداری و تقلب انجام می گیرد و در هر حال به دلیل تعدد مادی ارکان ارتکاب این جرایم در مقایسه با سرقت هویت، مجازات دو جرم در مورد شخص اعمال می شود.

برای سرقت هویت در حقوق موضوعه کشورمان، نمی توان 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 حرفه ای را شامل نمی شود. مواد قانون جرایم رایانه ای نیز علی رغم تعریف موسع از جرایم رایانه ای، این مساله را متذکر نشده اند و لذا ضرورت دارد تا ضمن مقررات خاص، جرم انگاری صحیحی نسبت به سرقت هویت و آثار مجرمانه آن به عمل آید. البته، در ایران، بسیاری از مصادیق سرقت هویت می تواند در قالب دسترسی غیرمجاز، جعل یا کلاهبرداری رایانه ای مشمول قانون جرایم رایانه ای قرار گیرد.

فناوری های جدید، سرقت هویت را آسان و سریع کرده است. بزهکار می تواند به راحتی از طریق چابگر رنگی، اسکنر، نرم افزارهای تغییر چهره و نرم افزارهای شبیه سازی کارت و مهر، خود را به جای دیگری جلوه داده و از حقوق و اختیارات وی بهره مند شود. بزهکار همچنین می تواند هویتی مجازی(که در عالم واقع وجود ندارد)، برای خود تعریف نموده و با این شیوه به ارتکاب جرم بپردازد.

در سال۲۰۰۳، مرکز گزارش ها و تحلیل تراکنش های استرالیا،[3] 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

1 -Identiy Thft Penalty Enhancement Act2004.
2 -18 U.S.C. 1028 A(a) (I).
3 -Australian Transaction Reports and Analysis Centre (AUSTRAC).

میلیارد مورد در سال ۲۰۰۱ کاهش یافته است. همچنین تعداد بزه دیدگان در فاصله این دو سال۲۶ درصد کاهش یافته و از ۱۱ میلیون نفر در سال۲۰۰۹ به ۸/۱ میلیون نفر در سال ۲۰۰۱ رسیده است. رقم کلاهبرداری شده از هر بزه دیده هم از میانگین ۴/۹۹۱ دلار برای هر نفر در سال ۲۰۰۹ به ۴/۶۰۷ دلار در سال ۲۰۱۰ کاهش یافته است.[1]

همانند رمزگیری، در مورد سرقت هویت هم بسیاری از شرکتها و موسسات، از پذیرش این موضوع که ناامنی در سامانه های رایانه ای و مخابراتی آنها باعث سرقت هویت می شود، طفره رفته و به دلایل اقتصادی، از افشای آمار مربوط به این جرایم خودداری می کنند.

سرقت هویت می تواند نتیجه یافتن یک کارت شناسایی، ضبط اطلاعات مربوط به کارت های مغناطیسی به هنگام استفاده از آنها در دستگاه های کارت خوان، هک کردن سامانه های رایانه ای و یا سرقت یا جعل مدرک شناسایی شخصی باشد. بدیهی است که بسیاری از اعمال، به عنوان مستقل قابل پیگیرد هستند.

وجود شماره های منحصر به فرد و اعتبار آن ها برای انجام اعمال و اقدامات خاص(برای مثال عملیات بانکی)، هرچند باعث کاهش تشریفات گردیده، اما احتمال سرقت هویت را افزایش داده است. سالانه، میلیون ها گذرنامه، گواهینامه و کارت پرداخت با شماره های بی همتا صادر می شود و در اختیار شهروندان قرار می گیرد. در بسیاری از این موارد، بزهکار می تواند به سرقت هویت و استفاده از آن دست یابد. به عنوان مثال عینی، بزهکار می تواند 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. به هر حال، راحتی ناشی از فناوری چنین اشکالاتی را هم در پی داشته است.

به عنوان مثال واقعی دیگر، مهمان پذیر یک هتل غذا خوری می تواند با نصب یک نرم افزار بر روی رایانه خود، کلیه اطلاعات شخصی و شناسه مربوطه به کارت پرداخت مشتریانی را که در آن مکان از کارت برای پرداخت استفاده می کنند، ذخیره نموده و بر فرض اینترنتی بودن حساب بانکی دارنده کارت، وجوهی از محل کارت به حسابی دیگر انتقال دهد. پیشگیری از بسیاری از این جرایم، بیش از اینکه راه حل، حقوقی داشته باشد، نیازمند طراحی و عملیاتی کردن نرم افزارهای دقیق رایانه ای، در راستای ارتقای

[1] -Javelin strategy & Research 2011 Identiy Fraud survey Report consumer version (prevention –Detection-Resolution, California, USA, February2011.

ایمنی فضای مجازی است. برای مثال، استفاده از شناسه های زیستی(از قبیل اثر انگشت، مردمک چشم و...) در کنار کارت شناسایی و شناسه های عددی می تواند در این راستا موثر باشد.

۶-کلاهبرداری

رکن قانونی جرم کلاهبرداری در حقوق جزای کشورمان، 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 می کند. ماده ۷ قانون تجارت الکترونیک در تعریف کلاهبرداری رایانه ای از ماده ۱ قانون تشدید، اقتباس شده است.

ماده ۱۳ قانون جرایم رایانه ای در متنی که قابل انتقاد است، جرم کلاهبرداری مرتبط با رایانه را به طور کلی توصیف می کند و ارکان ضروری این جرم را آن گونه که ماده قانون تشدید، ذکر کرده، بیان نمی کند. با این وضعیت، می توان دو نظریه متفاوت در تفسیر ماده ۱۳ قانون مذکور ارایه داد:

اول اینکه، ماده ۱۳ را باید با در نظر گرفتن ماده ۱ قانون تشدید و ماده ۶۷ قانون تجارت الکترونیک معنا کرد. در حقیقت، مقنن با فرض اینکه مفهوم و ارکان کلاهبرداری در قوانین سابق مشخص شده، از تکرار مفاد موارد مذکور خودداری کرده است. به ویژه باید این نکته را در نظر گرفت که در روند مجموع سازی قوانین، قانون جرایم رایانه ای به موجب ماده ۵۵آن، جزئی از قانون مجازات اسلامی محسوب می شود.

این طرز تلقی، به دلایل مختلف قابل دفاع نیست. از جمله اینکه، اولاً، اگر چه قانون جرایم رایانه ای بخشی از قانون مجازت اسلامی محسوب می شود، اما قانون تشدید و قانون تجارت الکترونیک که به جرم کلاهبرداری پرداخته اند، چنین وضعیتی ندارند. بنابراین، منطقی‌ترین راهکار این بود که در قانون جرایم رایانه ای در خصوص مفهوم و ارکان کلاهبرداری به دو قانون مذکور ارجاع داده می شد و یا اینکه مفاد مرتبط از این قوانین، در متن ماده ۱۳ قانون جرایم رایانه ای ذکر می‌گردید.

دوم اینکه، عباراتی در ماده ۱۳ قانون مذکور به کار رفته که نشان می دهد، مقنن درصدد ارایه مفهوم جدیدی از کلاهبرداری بوده است. در قسمت اول این ماده مقرر شده که هرکس«به طور غیرمجاز با اعمالی همچون وارد کردن، تغییر و..(که جنبه حصری ندارند) از سامانه های رایانه ای یا مخابراتی، تحصیل مال یا

هر نوع امتیاز مالی نماید، مجازات خواهد شد. در این ماده، مفهوم عامی از کلاهبرداری ارایه شده که زمینه منطقی را برای طرح نظریه دوم فراهم می کند.

نظریه دوم در تفسیر ماده ۱۳ قانون جرایم رایانه ای آن است که این ماده، درصدد جرم انگاری هر نوع استفاده غیرمجاز از سامانه رایانه ای یا مخابراتی برای تحصیل مال یا هر گونه امتیاز مالی بوده است. از این رو، مفهوم جدیدی از کلاهبرداری ارایه شده که آن را به جرم «تقلب»[1] در حقوق انگلیس نزدیک می کند و حتی از محدوده آن هم فراتر می برد. بخش۱۵ قانون سرقت انگلیس(مصوب۱۹۶۸)[2] درتعریف جرم تقلب(با مسامحه، کلاهبرداری) مقرر می دارد: «۱. هر شخصی که با هر نوع فریبی، غیر صادقانه مالی را به دست آورد که متعلق به دیگری است و قصد محروم کردن دایمی مالک را از آن داشته باشد،...۲. از نظر این بخش، «فریب»[3] به معنای هر نوع فریبی(خواه عامدانه یا ناشی از بی توجهی) به وسیله گفتار یا کردار، در امور موضوعی یا حکمی... می شود».

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 نمی کند و باید جرم جدیدی تعریف شود[4]. 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 جرم انگاری عملی لازم است که با ارتکاب عامدانه و بدون مجوز، باعث خسارت به مال دیگری به وسیله این موارد، می شود:الف- هر نوع وارد کردن، تغییر، حذف یا مخفی کردن داده رایانه ای.ب- هر نوع مداخله در عملکرد یک سامانه رایانه ای با هرقصد متقلبانه یا فریب آمیز برای به دست آوردن بدون مجوز هرنوع امتیاز اقتصادی برای خود یا دیگری».

ذکر سرقت و کلاهبرداری مرتبط با رایانه، زیر یک عنوان در فصل سوم از بخش یکم قانون جرایم رایانه ای نشان می دهد که هر جا دستیابی غیرقانونی به داده های متعلق به دیگری، در قالب کلاهبرداری نگنجد، مشمول عنوان جرم سرقت(ربایش) بوده و در همان اساس قابل مجازات خواهد بود.

---

1 -Fraud.
2 -Theft Act 1968.
3 –Decption.
4 - Law Commission Consultation Paper No155, Legislating the criminal cod Fraud and Deception, 1999, Paras, 8.36-8.58.

یکی از مواردی که جرم سرقت یا کلاهبرداری می تواند در مورد آن مطرح شود، کارتهای بانکی است. تجار و کسبه، به دلایل مختل اطلاعات مربوط به کارتهای پرداخت مشتریان را در اختیار دارند، یا حداقل می توانند به هنگام استفاده از کارت نسبت به آنها اطلاع پیدا کنند. این اطلاعات، به بهانه استفاده در مراجعه های بعدی، شرکت در قرعه کشی یا اطمینان فروشنده نسبت به تعلق کارت به خود مشتری، دریافت می شوند.

دارنده کارت هم می تواند از این وسیله در تجارت الکترونیکی سوء استفاده کند. برای مثال، پس از خرید الکترونیکی مدعی شود که کالای مورد معامله را دریافت نکرده است. همچنین دارنده کارت ممکن است پس از دریافت کالا، مدعی شود که از کارت وی سوء استفاده شده است.

یکی از بهترین راه ها برای پشیگیری از کلاهبرداری و سوء استفاده از اطلاعات در اینترنت، کاستن از تشریفات ابطال داده و اطلاعات سوخته است. برای مثال وقتی کارت پرداخت به همراه اطلاعات استفاده از آن فاش می شود، یا شناسه های شخصی(خصوصی) که می تواند در جرایم مالی به کار گرفته شود، گم شده یا به سرقت می رود، بانک ها و موسسات مالی باید برای شخص ذینفع این امکان را فراهم نمایند که در اولین فرصت و یا استفاده از سریع ترین ابزار ارتباطی، به تغییر شناسه ها یا بی اعتبار کردن ابزارهای پرداخت الکترونیکی اقدام نمایند. رمزگذاری اطلاعات، یکی دیگر از راههای پیشگیری از سرقت و سوء استفاده از اطلاعات می باشد. فناوری های متعدد برای رمز گذاری طراحی و ارایه شده است، از جمله استاندارد تراکنش الکترونیکی امن[1] که به طور مشترک به وسیله دو شرکت ویزا و مسترکارت در سال ۱۹۹۶ عملیاتی گردید. در این فناوری، از رمزگذاری کلید عمومی[2] قدرتمندی برای ایمنی و صحت داده های مربوط به تراکنش ها استفاده می شود. برای ارایه استاندارد هر چه بهتر، دو شرکت ویزا و مستر کارت، به طور مستقل از سال ۱۹۹۷ تا ۲۰۰۱ بر روی نسل جدیدی از ساز و کار تایید و تصدیق کار کردند. نتیجه امر ارایه پروتکل ایمنی سه بعدی[3] از سوی ویزا و استاندارد ایمنی دیگری[4] از سوی مستر کارت بود[5].

۷-تخریب و اخلال در داده ها یا سامانه های الکترونیکی

1 –secure Electronic Transaction(sET).
2 -Public Key cryprtography
3 -D secure Protocol.
4 -SPA UCAF.
5 - Brindle,Raymond Cox (Ed).In: Law of bank payments,Sweet & Maxwell, London 2004.P.56

خرابکاری یا ایجاد اخلال در داده های رایانه ای یا سامانه های رایانه ای یا مخابراتی می تواند با اهداف متعددی صورت گیرد تا حدی که با تجارت الکترونیکی ارتباط این عمل اغلب با هدف فراهم کردن زمینه ارتکاب جرایم دیگر، از قبیل دسترسی غیرمجاز به داده ها، جاسوسی اقتصادی، کلاهبرداری، نقض حقوق مالکیت فکری و تعرض به علایم و اسرار تجاری انجام می گیرد.

مواد ۸ الی ۱۱ قانون جرایم رایانه ای به موضوع «تخریب و اخلال در داده ها یا سامانه های رایانه ای 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 می تواند حبس، جزای نقدی یا هر دو باشد.

هرگاه جرم اخلال یا تخریب داده، با هدف به خطر انداختن امنیت و آسایش عمومی ارتکاب یابد، به موجب ماده ۱۱ قانون جرایم رایانه ای، مجازات مرتکب، حبس از سه سال تا ده سال دانسته است. این وضعیت، قانون جاسوسی اقتصادی[1] آمریکا را به یاد می آورد که در آن، دایره شمول جرایم علیه امنیت، از محدود مسایل اجتماعی و سیاسی فراتر رفته و اقدامات مجرمانه ای را که بر عهده علیه اقتصاد ملی(در مفهوم کلان آن) صورت می گیرد، شامل شده است.

۸- افشای داده ها و تعرض به حریم خصوصی

در مورد مفهوم حریم خصوصی میان دانشمندان اختلاف نظر وجود دارد.[2] در یک تعریف نسبتاً قابل قبول، حریم خصوصی را می توان 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 در خصوص ویژگیهای شخصی، شخصیتی، جسمی، اقتصادی و ... می شود. وقتیکه 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.[3]

---

[1] -Economic Espionage Act of 1996.

[2] - انصاری، باقر، حریم خصوصی و حمایت از آن در حقوق اسلام، تطبیقی ایران و فصلنامه حقوق دانشگاه تهران، شماره۶۶، زمستان۱۳۸۳.

[3] - زرکلام، ستار، حریم خصوصی ارتباطات اینترنتی(مطالعه در حقوق ایران و اتحادیه اروپا)، فصلنامه اندیشه صادق، شماره ۲۵، بهار و تابستان۱۳۸۶.

ظهور ابرتارنماهایی همچون فیس بوک و یوتیوب و اقبال میلیاردها نفر به آنها، صیانت از حریم خصوصی را در دهکده جهانی اطلاعات در حد غیر ممکن 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[۱]».

به نظرمی رسد، ادعای عدم امکان صیانت از داده های خصوصی در اینترنت، صرفاً برای رفع تکلیف از سازندگان و گردانندگان شبکه های ارتباطی ابزار می شود. با وجود این طرز تلقی که حفظ حریم خصوصی در فضای مجازی غیرممکن است، قانون جرایم رایانه ای در اقدامی که نشان می دهد، این قانون درصدد حمایت جدی از داده های شخصی می باشد؛ برای افشای داده های خصوصی در فضای مجازی، مجازات تعیین کرده است. به موجب ماده ۱۷ این قانون، «هر کس به وسیله سیستم های رایانه ای 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، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد».

افشای اطلاعات خصوصی، ممکن است به دلیل نقص سهوی یا عمدی در طراحی مرورگرهایی باشد که برای شبکه جهانی(اینترنت)یا شبکه های خصوصی طراحی می شوند کما اینکه شرکت موزیلا[۲] پذیرفته است که نسخه شماره ۵ و ۱۳ مرورگر این شرکت می تواند به دلیل اشکالی که در طراحی گزینه view آن وجود دارد، موجب افشای داده های حساس همچون اطلاعات بانکی و کارتهای پرداخت شود.

گفته می شود، اغلب مرورگرهای امروزی اطلاعاتی از کاربران خود را به سازندگان خود ارسال می کنند. فایرفاکس، اکسپلورر، کروم، سافاری و... از جمله مرورگرهای معروفی هستند که اطلاعاتی از حریم خصوصی کاربران خود را به دست سازندگان خود می رسانند. این اطلاعات در تبلیغات متناسب با ذائقه ی او استفاده شود. برنامه هایی هم برای خنثی کردن کارکرد جاسوسی مرورگرها ارایه و بازاریابی شده،[۳] که ممکن است خود، ابزار جاسوسی باشند.

---

[1] - Yu. M. Pushcharovsky, Tectonic structure and geodynamics of the divide between the Atlantic, Geotectonics, May 2010, Volume 44, Issue 3, pp 228

[2] - www.mozilla.org.

2-AntiBrowesersрy,,,Ad-Aware Internet Security.

۹- نتیجه گیری

. برخی جرایم مربوط به پرداخت های الکترونیکی یا در فضای عادی و سنتی رخ نمی دهند یا انجام دادن آنها در فضای مجازی- نسبت به جهان عادی- بیشتر و آثار مالی و اقتصادی خطرناک تر دارد. تقلب در کارت اعتباری و وجه الکترونیکی، جعل پول الکترونیکی، رمزگیری، سرقت هویت،کلاهبرداری، تخریب و اخلال در داده ها یا سامانه های الکترونیکی و افشای داده ها و تعرض به حریم خصوصی از مهمترین جرایم بانکداری الکترونیکی است. بستر انجام بزه رایانه ای، فضای سایبر است و این نکته را می توان از تعبیر «.....داده ها یا علایم موجود در کارت های حافظه یا قابل پردازش در سیستم های رایانه ای یا مخابراتی یا تراشه ها» که در بند ب ماده ۷۳۴ قانون مجازات اسلامی، بند ب ماده ۶ قانون جرایم رایانه ای آمده است برداشت کرد. بنابراین، همه رفتار های مد نظر در این ماده باید از رهگذر کنش های رایانه ای و در بستر رایانه و مخابرات انجام شود. پس اگر کسی داده رایانه ای را چاپ کند یا از روی صفحه نمایشگر رایانه عکس بگیرد و سپس بر روی کاغذ چاپ شده ، دگرگونی پدید آورد، جعل رایانه ای نخواهد بود». ایجاد اختلال در کارکرد سیستم رایانه ای جرمی است که با ایجاد هر گونه اختلال در عملکرد سیستم محقق می شود و باید قید ورود ضرر را نیز مورد توجه قرار دارد .ایجاد اختلال در کارکرد سیستم رایانه ای باید به اندازه ای باشد که به لحاظ عرفی اختلال عمده انگاشته شده و اغماض ناپذیر باشد. سیرتحول جوامع کنونی به شدت با وجود سیستم ها و داه های رایانه ای گره خورده است.

فهرست منابع:

الف- فارسی

۱. انصاری، باقر، حریم خصوصی و حمایت از آن در حقوق اسلام، تطبیقی ایران و فصلنامه حقوق دانشگاه تهران، شماره۶۶، زمستان۱۳۸۳.
۲. زرکلام، ستار، حریم خصوصی ارتباطات اینترنتی(مطالعه در حقوق ایران و اتحادیه اروپا)، فصلنامه اندیشه صادق، شماره ۲۵، بهار و تابستان۱۳۸۶.
۳. زیبر، ارلیش، جرایم رایانه‌ای، ترجمه محمدعلی نوری و رضا نخجوانی و مصطفی بختیار وند و احمد رحیمی مقدم، تهران: نشرگنج دانش، چاپ نخست، ۱۳۸۳.

۴. السان، مصطفی، جنبه های حقوقی بانکداری اینترنتی، چاپ اول، انتشارات پژوهشکده پولی و بانکی ، تهران،۱۳۸۸.
۵. شیرزاد، کامران، جرایم رایانه ای، تهران، نشر بهینه فراگیر،چاپ اول، ۱۳۸۸.
۶. صادقی نشاط، امیر، حقوق تجارت الکترونیک، مجله کانون سر دفتران و دفتر یاران ،شماره ۷۵، آذر ۱۳۸۶.

ب- لاتین

1. *Brindle,Raymond Cox (Ed).In: Law of bank payments,Sweet & Maxwell, London 2004.P.56*
2. *chesut, Robert, The e- commerce safety Guide, PayPal eBay 2005,p:13.*
3. *Economic Espionage Act of 1996.*
4. *Federal trade commission identy theft survey report ,2003.*
5. *Frank, R .Scarpitti & Carol cagwin ,Lenhart,Credit Card Frud,In: Ency clo pedia of Criminology and Deviant Behavior,Edited by Cliftom D. Bryant ,Vol.II, Brunnner-Routledge /Taylor and Francis Publishers ,2001.pp.106-109.at106*
6. *Hans ,Van Houtte,The Law of International Trade,2nd ed, Sweet &Maxwell, London, 2001.p.318.*
7. *ICA ,Authenticity of Electronic Records (ICA Study 13-1),Report prepared for UNESCO,by the International Council on Archives Committee on Archival Legal Matters,November ,November 2002 ,At www.ica.org/download .phpid=1624*
8. *International Monetary Fund {IMf} July 22,1944: Entered force December 27,1945.*
9. *Ivan Remisk , " Secure online Card Activation Isnt ,Forrester ,April14,2005.*
10. *Javelin Strategy & Research.Identity theft survey report (consumer version),2006 Synovate .*

11. *Javelin strategy & Research 2011 Identiy Fraud survey Report consumer version (prevention –Detection-Resolution, California, USA, February2011.*
12. *Law Commission Consultation Paper No155, Legislating the criminal cod Fraud and Deception, 1999, Paras, 8.36-8.58.*
13. *Lcncy ,Jennifer, Lynch, Jennifer Identiy Theft in cyberpace: Crime control Methods and and Their Effectiveness in combating Phishing Attacks, Berkeley Technology Law Journal. Vol. 20, 2005, pp:259- 260.*
14. *Mark T Gillet," Obrea Poindexter ; M Sean Ruff,Developments in Cyberbanking The Business Lawyer 2005;Feb 2005:60,2.p.1336*
15. *Markus J aksson,"Moderling and Phishing Attacks,phishing Panel of Financial Cryptogaphy 2005 "; Tsow ,Alexx,Phishing with Consumer Electronics – Malicious Home Routers,School of Information ,Indiana University,At: www.13 s.de/-olmedilla /events/ MTW06 – papers/paper22.pdf.*
16. *ounce Labs ,Inc .Managing the Risk of Identity Theft:The Need for Software Security Assurance Topics White Paper;At www.ouncelabs .com /pdf/library /ID Theft .pdf.*
17. *Penny ,Gillespie and Michael Rasmussen ," Combating Fraud in Financial Services ," Forrester ,April 7,2004.*
18. *R.v.Rymer(1993), Times, 21December1993.*
19. *Rogert, James S , "The New Old Law of Electronic Money",Boston College Law School Faculty Papers, 39 ,March 3 ,2005.P.79.*
20. *Rosenberg,Arnold S, "Better than Cash ? Consumer Protection and the Global Debit Card Deluge ",Columbia Journal of Trananational Law 2004*
21. *Shitds,L.K.(Solioitors) , "Logal Aspects of Electronic Contracts in the New Regime "2000, p. 14 .Available at: WWW. Ikshicids .ic.publications documents articles/pubo13.pdf.*
22. *Simmons ,BA, "Moncy and the Law : Why ompty with the Public International Law of Moncy ?" Yale Journal of International Law ,2000.pp.323-326.*
23. *Smedinghoff,T,J,"The Legal Requitements for Creating Secure and Enforecable Electronic Transsction ",International Monctary Fund:*

Current Developments in Monetary and Financial Law,Vol.3,April 2005,P.54

24. *Smith, Graham (Bitd & Bitd)and other Review by Eduatdo Uataran ,Internet Law and Regulation , Sweet & Maxwell,London 2002,p.506*
25. *W.A.Arbaugh;D.J.Farber , and Smith ,J.M, A secure and reliable bootstrap architecture, In SP 97 : Proceeding of the 1997 IEEE Symposium on Security and privacy ,pages 65-71.*
26. *Washington ,DC,USA; Rachna Dhamija and J.D.Tyger The battle against phishing : Dynamic security skins ,In SOUPS 05 : Proceeding of the 2005 symposium on Usable privacy and Security ,pp.77-88,New Yourk ,NY ,USA,2005,ACM Press .*
27. *www.mozilla.org.*
28. *Yu. M. Pushcharovsky, Tectonic structure and geodynamics of the divide between the Atlantic, Geotectonics, May 2010, Volume 44, Issue 3, pp 228*
29. *Zezev and Yarimaka v Governor of HM Prison Brixton and another, CACD , Cr App R 33. Coram: Lord Chief Justice Lord Woolf, Wright J Ratio: Wright J said: 'But if an individual,2002,P.33.*