Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 2, Issue 3, 2022

Banking Crimes in Cyberspace in Iranian Law and International Documents

Fatemeh Al-Sadat Ghoreishi Mohammadi[1]

1-Member of the Faculty, Department of Law, Payame Noor University, Tehran, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: ***45-55***

Corresponding Author's Info
ORCID: *0009-0009-0162-2825*
TELL: *+989133233813*
Email: *fateme.ghoreishi@pnu.ac.ir*

Article history:
Received: *19 Jul 2022*
Revised: *16 Agu 2022*
Accepted: *02 Sep 2022*
Published online: *23 Sep 2022*

Keywords:
Banking Crimes, Cyberspace, International Documents.

ABSTRACT

Along with the growing use of electronic tools in banking and payment services, computer crimes related to these tools have also increased. Banking crimes in the cyberspace are important issues that affect the economic security of citizens and the trust and credibility of the banking system. Examining the approach of international documents to this category of crimes is also important because the aforementioned crimes are often transnational. The present article is descriptive and analytical and has been investigated using the library method. The findings indicate that in jurisprudence, although crimes such as phishing have not been discussed, but by resorting to the rules governing traditional crimes, it is possible to deal with banking crimes in cyberspace. In Iran's criminal law, there are no special laws in the field of banking crimes, and mainly, the computer crimes law governs electronic banking crimes. The United Nations, Interpol, and the Council of Europe are among the international organizations that, according to their goals and activities, have taken actions in the field of dealing with computer crimes. In the meantime, the adoption of the Convention on Computer Crimes is a turning point in the field of international coordinated actions.

How to Cite This Article: Ghoreishi Mohammadi, F (2022). " Banking Crimes in Cyberspace in Iranian Law and International Documents" . *Journal of Comparative Criminal Jurisprudence*, 2(3): 45-55.

فصلنامه فقه جزای تطبیقی
www.jccj.ir
انجمن علمی فقه جزای تطبیقی ایران
فصلنامه فقه جزای تطبیقی

دوره دوم، شماره سوم، پاییز ۱۴۰۱

جرایم بانکی در فضای مجازی در حقوق ایران و اسناد بین‌المللی

فاطمه السادات قریشی محمدی *[۱]

۱. عضو هیأت علمی، گروه حقوق، دانشگاه پیام نور، تهران، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۴۵-۵۵

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۹-۰۰۰۹-۰۱۶۲-۲۸۲۵

تلفن: ۹۸۹۱۳۳۲۳۳۸۱۳+

ایمیل: fateme.ghoreishi@pnu.ac.ir

سابقه مقاله:

تاریخ دریافت: ۱۴۰۱/۰۴/۲۸

تاریخ ویرایش: ۱۴۰۱/۰۵/۲۵

تاریخ پذیرش: ۱۴۰۱/۰۶/۱۱

تاریخ انتشار: ۱۴۰۱/۰۷/۰۱

واژگان کلیدی:

جرایم بانکی، فضای مجازی، اسناد بین‌المللی.

چکیده

همزمان با رشد روزافزون بهره‌گیری از ابزارهای الکترونیکی در خدمات بانکی و پرداخت، جرایم رایانه‌ای مرتبط با این ابزارها نیز افزایش یافته است. جرایم بانکی در فضای مجازی از مسائل مهم و تأثیرگذار بر امنیت اقتصادی شهروندان و اعتماد و اعتبار نظام بانکی است که تبیین رویکرد حقوقی نسبت به آن ضروری است. بررسی رویکرد اسناد بین‌المللی به این دسته از جرایم نیز از این جهت اهمیت دارد که جرایم مذکور در بسیاری مواقع فراملی است. مقاله حاضر توصیفی تحلیلی بوده و با استفاده از روش کتابخانه‌ای به بررسی موضوع مورد اشاره پرداخته شده است. یافته‌ها بر این امر دلالت دارد که در فقه هرچند جرایمی چون فیشینگ محل بحث و نظر نبوده اما با توسل به قواعد حاکم بر جرایم سنتی، امکان رسیدگی به جرایم بانکی در فضای مجازی وجود دارد. در حقوق کیفری ایران، قوانین ویژه‌ای در زمینه جرایم بانکی تدوین نشده و عمدتاً قانون جرایم رایانه‌ای بر جرایم بانکداری الکترونیک حاکم است. سازمان ملل متحد، اینترپل و شورای اروپا از جمله سازمان‌های بین‌المللی هستند که با توجه به اهداف و فعالیت‌های خود، در زمینه مقابله با جرایم رایانه‌ای اقداماتی را انجام داده‌اند. در این میان تصویب کنوانسیون جرایم رایانه‌ای نقطه عطفی در حوزه اقدامات هماهنگ بین‌المللی است.

مقدمه

امروزه رایانه و سایر دستگاه‌های الکترونیکی در تمام جوانب زندگی مدرن نفوذ کرده‌اند و این وسیله سودمند که تا پیش‌ازاین به‌صورت ابزاری در جهت کمک به اجرای قانون مورداستفاده قرار می‌گرفت به وسیله‌ای در دست مجرمان برای ارتکاب جرم تبدیل شده است (تراب‌زاده، ۱۳۸۸: ۱-۲). میل و اشتیاق به استفاده از رایانه و اینترنت و بهره‌مندی از مزایای آن، یک تمایل جهانی است که با سرعت قابل‌توجهی هم درحال افزایش می‌باشد. اگرچه زمینه مشارکت جوامع را در فرآیند اقتصاد، داده‌پردازی فراهم می‌سازد، بااین‌وجود، شرایط و بستر مساعدی نیز برای ظهور پدیده‌های نوین بزهکاری به وجود آورده است که جرایم ارتکابی در فضای مجازی یکی از این پدیده‌های نوین به‌شمار می‌رود (خدا قلی، ۱۳۸۳: ۱۸). 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 (شیرزاده،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 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. البته باید توجه داشت که پیشرفت‌های نوین بانکی نیز مانند سایر حوزه‌های سایبری 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 قابل‌پیگیری و مساوات هستند و نیازی به تصویب قوانین جدید ندارند و گروه دوم شامل جرایمی هستند که قبل از تولد و رشد بانکداری نوین به‌هیچ‌وجه امکان ارتکاب آن وجود نداشته است. به‌علاوه عواقب و پیامدهای فناوری مجرمانه می‌تواند خیلی بیشتر ازگذشته و غیرقابل‌تصور باشد. چراکه مصونیت‌های جغرافیایی یا مرزهای ملی، آنرا محدود می‌کند که موجب سوءاستفاده گسترده مجرمین به‌ویژه گروه‌های جنایتکار سازمان‌یافته، از سیستم‌های الکترونیکی بانک‌ها گردیده است.

درخصوص جرایم بانکی یا جرایم رایانه‌ای، پژوهش‌های متعددی انجام‌شده است: مصطفی السان در مقاله‌ای به بررسی ابعاد حقوقی بانکداری اینترنتی پرداخته است (السان، ۱۳۸۴). مهران مولوی و سایرین نیز در مقاله‌ای، نقش فناوری اطلاعات در جرایم اینترنتی شبکه بانکی را مورد بررسی قرار داده‌اند (مولوی و دیگران، ۱۳۹۵). همچنین علیرضا تلخابی علیشاه در مقاله‌ای، امنیت مجازی خدمات بانکی اینترنتی و تأثیر آن برجذب مشتریان بانک تجارت را بررسی کرده است (تلخابی علیشاه، ۱۳۹۵). در مقاله حاضر اما به بررسی این سؤال پرداخته‌شده است که جرایم بانکی در فضای مجازی چگونه قابل‌بررسی است؟ ابتدا به جرایم بانکی در فضای مجازی با نگاهی به حقوق ایران و رویکرد اسناد بین‌المللی پرداخته‌شده و بحث شده است.

۱- جرایم بانکی در فضای مجازی

در فضای مجازی امکان جرایم بانکی متعددی وجود دارد. در این قسمت تلاش شده مهم‌ترین جرایم بانکی و رویکرد حقوق ایران نسبت به این جرایم بررسی شود.

۱-۱- سرقت و تقلب در کارت اعتباری الکترونیکی

با جایگزین شدن کارت اعتباری به‌جای اسکناس در طی زمان، بزهکاری مالی در این حوزه نیز به‌تناسب همین انتقال جابه‌جاشده است. بنابراین، تقلب در کارت عادی 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 درکارت‌های اعتباری، در مقایسه با دیگر جرایم پولی، به دلیل نو بودن روش‌های الکترونیکی پرداخت دشوارتر است. حال‌آن‌که در عمل خلاف این موضوع اثبات‌شده است (Scarpitti,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؟ پرسش دوم آن است که آیا جعل وجه الکترونیکی 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 می‌ماند. چنین قاعده‌ای درباره پول اجرا نمی‌شود. اگر شخص مقداری پول یابد و با آن کالایی بخرد، ثمن در مالکیت بایع وارد می‌شود، حتی اگر سارق بر آنید مشروع نداشته باشد (زیبر،۱۳۸۳: ۴۱). به‌موجب قانون بروات انگلیس مصوب ۱۸۸۲، **«کسی که با حسن نیت اوراق بهادار را به دست می‌آورد، صرف‌نظر 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 به‌قدری شیوع یابد که جایگزین پول شود و مالک اولیه ازلحاظ ثبت، نام مالک برای آن متصور نباشد، می‌توان اعتقاد داشت که واجد وصف انتقال بوده و لذا قاعده فوق در مورد آن مجری خواهد بود.

۱-۲- جعل پول الکترونیکی

باوجود، دستگاه‌های نوین امکان‌کشف جعل در پول الکترونیکی نسبت به پول کاغذی بسیار آسان‌تر است. این فرض تقویت‌شده است که ازلحاظ ایمنی این نوع از وسایل اعتباری در رتبه برتری قرار دارند. به‌منظور اجتناب از جعل، اسم رمزی که در پول‌الکترونیکی به‌کار می‌رود باید به‌گونه‌ای باشد که قابلیت افشا شدن نداشته باشد. برای تحقق این موضوع از توانمندی مهندسانی بهره‌گیری می‌شود که با فنون جعل و راه‌های مقابله با آن آشنایی دارند. یا وجود این، هیچ‌گاه نمی‌توان مدعی شد که جعل پول الکترونیکی قابل‌تصور نیست. درعین‌حال این ادعا مطرح‌شده 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: ۶۹). به‌هرروی، 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 ازلحاظ سقوط تعهد یا بدهکار کردن طرف مقابل، فاقد هرگونه اثر حقوقی است. به لحاظ نظری، مسؤولیت بر کسی تحمیل می‌شود که درفرض پرداخت‌های متعدد به‌موجب پول جعلی واحد، زنجیره تأدیه از او آغازشده است. باوجوداین، ازآن‌رو که گاه یافتن مسؤول اصلی دشوار است، به لحاظ 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).

این حالت نیز قابل‌تصور است که‌کشف جعلی بودن پول الکترونیکی به‌هنگام در جریان بودن آن، ممکن نباشد، اما آنگاه که برای تبدیل آن به ارز واقعی مراجعه می‌شود، این موضوع کشف شود، بدین طریق که به‌طور مثال معلوم شود دو یا چند پول‌الکترونیکی با شماره سریال واحد موجود است. در چنین مواردی، ، خسارت بر کسی تحمیل می‌شود که به‌منظور دریافت ارزش واقعی پول الکترونیکی اقدام کرده

است. این نکته بدیهی است که حق مراجعه افراد مذکور به مسؤول واقعی با رعایت قواعد عام حقوق مسؤولیت مدنی هیچ‌گاه منتفی نیست.

برخی کشورها مقررات آزاد و منعطفی برای نقل‌وانتقال سرمایه و معاملات ارزی دارند. به‌طور مثال، بحرین، هنگ هنگ، پاناما و سنگاپور از این جمله‌اند. برخی کشورهای دیگر به‌منظور حمایت از پول رایج داخلی محدودیت‌های مبادلاتی را حفظ کرده‌اند (Simmons,2002: 323-326). چنین محدودیت‌هایی علاوه براین‌که بر پرداخت‌های مربوط به انتقال سرمایه اعمال می‌شود، بلکه در مورد تمامی معاملات ارزی مجری خواهد بود. بیشتر کشورها مقررات و تشریفات مربوط به معاملات ارزی خود را حفظ کرده‌اند. بااین‌همه، ماده ۸ (بخش ۲ الف) توافق‌نامه بین‌المللی اعتبار پولی،[1] دولت‌های عضو را از تحمیل محدودیت‌هایی درزمینه پرداخت و انتقالات مربوط به معاملات ارزی پیش از تصویب توافقنامه مذکور منع می‌کند. این مقررات از سوی‌کشورهایی وضع‌شده است که پول رایج داخلی آن‌ها در معاملات و پرداخت‌های بین‌المللی کاربرد دارد. ایران ازجمله کشورهایی است که به‌رغم عضویت در توافق‌نامه، مفاد ماده مذکور را نپذیرفته است (Hans,2001: 318).

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 قابل‌پردازش 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 گرفته‌شده 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 سامانه‌های‌الکترونیکی، به‌طورقطع، 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.

چنان‌چه در ماده ۷ و ۸ قانون جرایم رایانه‌ای موردتوجه قرارگرفته، جعل رایانه‌ای ممکن است باهدف 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 داده‌ها یا ایجاد اخلال در عملکرد سامانه باشد. درحقوق 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. درحقوق ایران، هرگاه تغییر داده‌ها یا وارد ساختن متقلبانه داده، موجب اخلال یاتخریب 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. دراین حالت، قواعد مربوط به تعدد معنوی اجرا می‌شود کیفر جرمی اعمال می‌شود که مجازات آن شدیدتر است.

۱-۳- فیشنگ

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 یک‌لحظه بی‌احتیاطی می‌کند، پهن‌می‌نماید. حربه معمول در رمزگیری آن است‌که شخص رمزگیر،[2] یک‌نامه الکترونیکی

[2] -Phisher

که به نظر می‌رسد از مؤسسه مالی‌مشتری (بزه‌دیده) یا تارنمای تجارت‌الکترونیکی وی ارسال‌شده، برای قربانی می‌فرستد. برای جلب‌توجه مشتری و ایجاد اعتماد در او، علامت تجاری و سایر مشخصات ظاهری شرکت اصلی در متن نامه گنجانیده شده و حتی به مشتری هشدارهای‌لازم درجهت رعایت نکات ایمنی داده می‌شود. به‌طور معمول، در نامه الکترونیکی به‌گیرنده گفته می‌شود که باید اطلاعات حساب وی، درجهت پیشگیری ازکلاهبرداری یا به دلیل نقض فنی که پیش‌آمده، 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 شودکه اطلاعات را مؤسسه مالی وی ارسال کرده است. درحالی‌که پایگاه (تارنمای) مذکور هم ساختگی است (Lcncy,2005: 259). 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.

سرقت هویت[1] و کلاهبرداری در هویت،[2] عناوین دیگری است که برای توصیف دستیابی متقلبانه به اطلاعات شخصی افراد از قبیل شماره‌حساب 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. به همین 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 ازآن جهت که طراحان عملیات مجرمانه رمزگیری، اطلاعات شخصی مشتریان متعددی را از مؤسسه واحد به دست آورده و اقدام به سوءاستفاده می‌نمایند. رمزگیری، درصورتی‌که تنها باهدف 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 متوقف کردن 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 ازکلاهبرداری رایانه‌ای، باوجود ماده یک «قانون تشدید مرتکبین ارتشاء اختلاس و کلاهبرداری» که جرم کلاهبرداری را به‌طور دقیق تعریف می‌کند، مایه انتقاد است. به نظر 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 به نظر می‌آید که تلاش قانون جرایم رایانه‌ای برای جرم انگاری تمامی تخلفاتی که در فضای مجازی ارتکاب می‌یابد، باعث دو اشکال عمده شده است: اول، دور شدن از تعریف منطقی بسیاری از جرایم که در قانون مجازات اسلامی تعریف‌شده‌اند. 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.

[1] -Identity Theft
[2] -Identity Fraud

ماده ۶۷ قانون تجارت الکترونیک، تعریف دقیق‌تری از کلاهبرداری رایانه‌ای ارائه می‌دهد. معلوم نیست که باوجوداین ماده، چرا قانون جرایم رایانه‌ای، ماده ۱ را با ایرادات اساسی، به جرم‌کلاهبرداری مرتبط با رایانه اختصاص داده است. در هرحال، به نظر می‌رسد که کلاهبرداری باعناوین مجرمانه‌ای 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 قرار دادن رمز عبور، کد دستیابی یا داده‌های رایانه‌ای یا هر نوع اطلاعات مشابه به‌طور غیرمجاز به‌نحوی‌که به‌وسیله سیستم رایانه‌ای یا مخابراتی یا داده‌های مربوط قابل‌دست‌یابی باشد»** را جرم اعلام کرده بود. بند (ب) ماده ۲۵ قانون جرایم رایانه‌ای با کوتاه کردن عبارت فوق، قید «بدون رضایت» (دارنده) را علاوه بر غیرمجاز به متن پیشین افزوده است.

کنوانسیون اروپایی جرم مجازی، نوعی جرم مرتبط باکلاهبرداری را تعریف کرده که در آن از مفهوم «فریب» عدول شده است. طبق ماده ۸ این کنوانسیون: **«هریک از دولت‌ها موظف‌اند قانونی را وضع کرده و موازینی 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 مخفی کردن داده رایانه‌ای. ب- هر نوع مداخله در عملکرد یک سامانه رایانه‌ای با هر قصد متقلبانه یا فریب‌آمیز برای به دست آوردن 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 بر همان اساس قابل مجازات خواهد بود.

یکی از مواردی که جرم سرقت یا کلاهبرداری می‌تواند در مورد آن مطرح شود، کارت‌های بانکی است. تجار و کسبه، به دلایل مختل اطلاعات مربوط به کارت‌های پرداخت مشتریان را در اختیاردارند، یا حداقل می‌توانند به هنگام استفاده از کارت نسبت به آن‌ها اطلاع پیدا کنند. این اطلاعات، به بهانه استفاده در مراجعه‌های بعدی، شرکت در قرعه‌کشی یا اطمینان فروشنده نسبت به تعلق کارت به خود مشتری، دریافت می‌شوند.

دارنده کارت هم می‌تواند از این وسیله در تجارت‌الکترونیکی سوءاستفاده 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 سوءاستفاده شده است.

۲- رویکرد اسناد و سازمان‌های بین‌المللی

به‌منظور مقابله با جرایم رایانه‌ای و رفع چالش‌های موجود در این حوزه، برخی کنوانسیون‌های بین‌المللی به تصویب رسیده‌اند که کنوانسیون ۲۰۰۱ بوداپست با عنوان «کنوانسیون جرایم رایانه‌ای» یکی از آن‌ها است. پیش‌نویس کنوانسیون جرایم سایبری توسط کمیته‌ای به نام«کمیته متخصصین جرایم سایبر (PC-CY) تهیه شد. کمیته متخصصین جرایم سایبر در ۴ فوریه ۱۹۹۷ توسط کمیته وزرای شورای اروپا تشکیل گردید و کار خود را در آوریل ۱۹۹۷ شروع کرد و نسخه اولیه پیش‌نویس‌کنوانسیون مذکور در آوریل ۲۰۰۰ تهیه و منتشر گردید. نسخه نهایی پیش‌نویس و گزارش توجیهی آن در ژوئن ۲۰۰۱ تهیه و جهت تأیید تسلیم کمیته اروپایی مشکلات ناشی از جرم شد و پس از تأیید آن جهت تصویب و امضاء به کمیته وزرای شورای اروپا تقدیم 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 گردید.

این کنوانسیون دارای ۴ فصل است که فصل اول آن راجع به تعریف واژه‌های تخصصی و فصل دوم آن در مورد حقوق کیفری ماهوی (انواع جرایم رایانه‌ای و حقوق کیفری شکلی آیین دادرسی کیفری) می‌باشد. در فصل سوم به همکاری‌های بین‌المللی اشاره دارد و فصل چهارم آن اختصاص به مقررات مربوط به امضاء، لازم الاجراء شدن و الحاق به کنوانسیون است (خرم‌آبادی، ۱۳۸۶: ۴). در مقدمه این کنوانسیون چنین آمده است: **«دولت‌های امضاء کننده این کنوانسیون باهدف دستیابی به اتحاد فراگیر میان اعضاء و با اعتقاد به‌ضرورت اتخاذ سیاست‌های جنایی عمومی در حمایت جامعه در برابر جرایم سایبری، به تصویب قوانین مناسب و گسترش همکاری‌های بین‌المللی اقدام کرده و با آگاهی از تحولات شگرفی که در اثر همگرایی و تداوم روند جهانی‌شدن شبکه‌های رایانه‌ای و داده‌های الکترونیکی به‌منظور ارتکاب جرایم و بااحساس نیاز به همکاری بین دولت‌ها و بخش‌های خصوصی درزمینه مبارزه با جرایم سایبری و حمایت از منافع مشروع در توسعه فن‌آوری اطلاعات در راستای تصویب قوانین یکپارچه و یکسان در این زمینه گام برمی‌دارند».** دبیرخانه شورای‌عالی انفورماتیک، راهنمای سازمان ملل برای پیشگیری از جرایم مرتبط با رایانه این‌کنوانسیون پیشنهاد می‌کند که دولت‌های طرف قرارداد به انحای گوناگون در موارد لازم بالأخص در مسائل مربوط به ارائه دلایل جرم و اعلام دقیق محل وقوع آن، به یکدیگر یاری رسانند. در این‌کنوانسیون هماهنگ‌سازی بین حقوق‌کیفری داخلی و مقررات یکپارچه بین‌المللی در خصوص عناصر تشکیل‌دهنده جرایم سایبری به چشم می‌خورد (رضوی،۱۳۸۶: ۸).

اهداف کنوانسیون بوداپست شامل موارد ذیل می‌شود که عبارت‌اند از: الف) هماهنگی ارکان تشکیل‌دهنده جرم در حقوق جزای ماهوی داخلی کشورها و مسائل مربوطه در بخش جرایم فضای سایبر. ب) فراهم آوردن اختیارات لازم آیین دادرسی‌کیفری داخلی برای پی‌جویی و تعقیب جرایمی که با استفاده از سیستم‌های رایانه‌ای انجام می‌شود یا مدرک مرتبط با جرم به شکل الکترونیکی است. ج) تدوین سیستم سریع و مؤثر همکاری بین‌المللی (خرم‌آبادی،۱۳۸۶: ۴). ازاین‌رو متن کنوانسیون نیز به چهارفصل تقسیم می‌شود: ۱. استفاده از اصطلاحات. ۲. اقدامات داخلی کشورهای عضو. ۳. قوانین ماهوی و قانون آیین دادرسی ۴. فصل پایانی (باقری اصل،۱۳۸۴: ۷).

مسأله جرم رایانه‌ای در سال‌های ۱۹۸۵–۸۶ 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. این کمیته کار خود را در سال ۱۹۸۵ میلادی آغاز کرد. مطالعات و تحقیقات انجام‌شده تاکنون منتهی به مصوبه‌های مهم و قابل‌توجهی شده است. توصیه‌نامه‌های شماره ۹ (۸۹) R و شماره ۱۳ (۹۵) ازجمله این مصوبات است که به ترتیب در ۱۳ سپتامبر ۱۹۸۹ و ۱۱ سپتامبر ۱۹۹۵ از سوی کمیته وزیران شورای اروپا پذیرفته شد و شامل رهنمودهایی برای قانونگذاران ملی در مورد جرایم رایانه‌ای و آیین دادرسی مرتبط با فن‌آوری اطلاعات است.

سازمان ملل متحد یکی از اولین سازمان‌های بین‌المللی است که به اهمیت جرایم الکترونیکی اشاره‌کرده است. مجمع عمومی سازمان ملل در دسامبر ۲۰۰۰ و ژانویه ۲۰۰۲ قطعنامه‌های ۵۵/۶۳ و ۵۶/۱۲۱ را در مورد مبارزه با سوءاستفاده تبهکاران از فن‌آوری‌های ارتباطی به تصویب رسانده است. قطعنامه ۵۵/۶۳ بیان می‌دارد که کشورها برای از بین بردن پناهگاه امن برای کسانی که مرتکب جرایم الکترونیکی می‌شوند باید قوانین ویژه‌ای تدوین نمایند. در این قطعنامه هم‌چنین عنوان‌شده که دولت‌ها باید جهت جلوگیری از سوءاستفاده تبهکاران از فن‌آوری اطلاعات اقدامات لازم را

انجام دهند. پیشنهاد قطعنامه ۵۵/۶۳، آموزش قوانین اجرایی در مورد جرایم الکترونیکی است (سادوسکای و همکاران، ۱۳۸۴: ۲۷۴). کما این‌که بیانیه یازدهمین کنگره پیشگیری از جرایم و عدالت کیفری سازمان ملل متحد به سال ۲۰۰۵ هم به جرایم رایانه‌ای اختصاص‌یافته است (جاوید نیا، ۱۳۸۷: ۲۵).

این سازمان هم‌چنین باانتشار نشریات و متون مختلف، جهت پیشگیری از جرایم سایبری و مبارزه با آن، اقدامات شایان توجهی را انجام داده که ازجمله می‌توان به نشریه سیاست جنایی سازمان ملل درزمینه جرایم سایبری اشاره کرد. هرچند مطالب مندرج در این نشریه جنبه الزام‌آور به خود نمی‌گیرد، بااین‌وجود در راستای اتخاذ سیاست‌های لازم برای زدودن این پدیده نوین بزهکاری، ایده‌های جدیدی به کشورها داده و مساعدت‌های شایسته‌ای به آن‌ها کرده است.

سازمان‌های منطقه‌ای نیز در راستای نیل به هدف مبارزه با جرایم سایبری از هیچ تلاشی در این زمینه دریغ نمی‌ورزند. شورای اروپا نقش فعالی را ایفاء نموده است و در متنی که این شورا تهیه نموده لیستی از چالش‌های موجود در حوزه جرایم سایبری و واکنش‌های نوین مطرح‌شده به‌منظور رفع این چالش‌ها به چشم می‌خورد. در متن یادشده، در کنار ارائه پیشنهادهای ماهوی، درخصوص مسائل شکلی ازجمله آیین رسیدگی به جرایم سایبری نیز راه‌حل‌هایی ارائه گردیده است (رضوی، ۱۳۸۶: ۹-۱۰). پلیس بین‌الملل نیز سال‌های متمادی است که فعالیت خود را در مبارزه با جرایم سایبری آغاز کرده است. این سازمان با بهره‌گیری از متخصصان و کارشناسان کشورهای عضو چند گروه کاری را در این زمینه تشکیل داده و روسای واحدهای مبارزه با جرایم‌سایبری کشورهای باتجربه عضو سازمان را گرد هم آورده است (رضوی،۱۳۸۶: ۱۲). در اینترپل دوره‌های خاصی برای آموزش پلیس کشورهای عضو از سال ۱۹۸۳ برگزار می‌شود. هر دو سال اینترپل اقدام به برپایی کنفرانس بین‌المللی درزمینه جرایم اینترنتی به‌منظور مبادله اطلاعات و توانایی‌ها درزمینه تحقیقات در قضایای اینترنتی می‌نماید (تقی زاده انصاری،۱۳۸۸: ۱۶۰-۱۶۲).

نتیجه‌گیری

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. تقلب در کارت اعتباری و وجه الکترونیکی، جعل پول‌الکترونیکی، رمزگیری، سرقت هویت، کلاهبرداری از مهم‌ترین جرایم بانکداری الکترونیکی است. بستر انجام بزه‌رایانه‌ای، فضای سایبر است. ماهیت و ویژگی‌های خاص جرایم در محیط سایبر، مراجع قضایی و انتظامی را با چالش‌های جدیدی مواجه کرده است. یکی از این چالش‌ها، داشتن جنبه بین‌المللی است. ابعاد جرایم ارتکابی در فضای مجازی، نه‌تنها حاکمیت سرزمینی یک دولت را تحت‌تأثیر قرار می‌دهد، بلکه تمامی دولت‌های جهان را در برمی‌گیرد. جعل پول الکترونیکی، سرقت و تقلب در کارت اعتباری الکترونیکی، فیشنگ و پولشویی الکترونیکی از جمله جرایم بانکی است در حقوق ایران و اسناد بین‌المللی تلاش‌های در جرم‌انگاری و مقابله با این جراین صورت گرفته است. در فقه نیز با اینکه به دلیل نوظهور بودن این جرایم نمی‌توان به شواهد مستقیمی دست یافت اما بر اساس قواعد سنتی جرم‌انگاری قابل تبیین هستند. نکته مهم این است که ماهیت جرایم سایبری این‌گونه است که هیچ حدومرز سرزمینی مشخصی را نمی‌شناسد. ابعاد یادشده موجب طرح مباحثی چون صلاحیت تعدد و تعارض قوانین کیفری و قابلیت ارتکاب جرایم مذکور علیه قربانیان بی‌شمار می‌شود. چالش دیگر، مشکل تعریف واحد از جرایم سایبری است. ازآنجاکه این جرایم در اشکال مختلفی ارتکاب می‌یابند، سخن گفتن درخصوص تعریف واحد، شرایط و ارکان این جرایم، قدری مشکل به نظر می‌رسد. جرایم رایانه‌ای به عنوان یکی از مدرن‌ترین جنایات سازمان یافته فراملی است

که در عصر حاضر امنیت جامعه بین‌المللی را به شدت تهدید می‌نماید. وانگهی، هر چند اتخاذ تدابیر داخلی از سوی کشورها برای مقابله با جرایم رایانه‌ای اهمیتی حیاتی داشته و لازم می‌باشد لیکن کافی به نظر نمی‌رسد. از این رو برای مبارزه با این چالش تکنولوژی، هماهنگی و همکاری بین‌المللی به عنوان مکمل اقدامات درون مرزی دولت‌ها ضروری خواهد بود.

ملاحظات اخلاقی: ملاحضات اخلاقی در این پژوهش انجام شده است.

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

سهم نویسندگان: نگارش تمام مقاله بر عهده نویسنده بوده است.

تشکر و قدردانی: از همه کسانی که در نگارش این مقاله همکاری نموده‌اند، نهایت قدردانی و امتنان را دارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین مالی انجام گرفته است.

منابع و مآخذ

الف. منابع فارسی

– السان، مصطفی (۱۳۸۴). «ابعاد حقوقی بانکداری اینترنتی». *مجله پژوهش‌های حقوقی*،۴ (۷): ۱۸۵–۲۰۸

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

– باقری اصل، رضا (۱۳۸۴). «ناظر علمی کنوانسیون جرایم سایبر و گزارش توجیهی آن گروه ارتباطات و فن‌آوری‌های نوین». تهران: گروه کارشناسان، کمیسیون حقوقی و قضایی مجلس.

– تراب زاده، حسین (۱۳۸۸). «بررسی صحنه‌های جرم الکترونیکی». *مجله کارآگاه*، ۲(۶): ۱–۲.

– تقی زاده انصاری، مصطفی (۱۳۸۸). *سازمان جهانی پلیس جنایی اینترپل*. چاپ اول، تهران: انتشارات جنگل.

– تلخابی علیشاه، علیرضا؛ حسینی‌دانا، حمیدرضا و شعبانی صابر، داود (۱۳۹۵). «مدیریت امنیت مجازی خدمات بانکی اینترنتی و تأثیر آن برجذب مشتریان بانک تجارت». *مجله مطالعات رسانه‌ای*، ۳۴–۳۵: ۳۹–۴۸.

– جاوید نیا، جواد (۱۳۸۷). *جرایم تجارت الکترونیکی جرایم رایانه‌ای در بستر تجارت الکترونیکی*. چاپ اول، تهران: انتشارات خرسندی.

– خدا قلی، زهرا (۱۳۸۳). *جرایم کامپیوتری*. چاپ اول تهران: نشر آریان.

– خرم‌آبادی، عبدالصمد (۱۳۸۶). «کلاهبرداری رایانه‌ای از دیدگاه بین‌المللی و وضعیت ایران». *فصل‌نامه حقوق مجله دانشکده حقوق و علوم سیاسی*، ۳۷(۲): ۴–۲۳.

– رضوی، محمد (۱۳۸۶). «جرایم سایبری و نقش پلیس در پیشگیری از این جرایم و کشف آن‌ها». *فصل‌نامه دانش انتظامی*،۹(۱): ۸–۱۲.

– زیبر، ارلیش (۱۳۸۳). *جرایم رایانه‌ای*. چاپ اول، تهران: نشر گنج دانش.

– سادوسکای، جورج و همکاران (۱۳۸۴). *راهنمای فن‌آوری اطلاعات*. چاپ اول، تهران: نشر شورای عالی اطلاع‌رسانی دبیرخانه،

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

– صادقی نشاط، امیر (۱۳۸۶). «حقوق تجارت الکترونیک». *مجله کانون سردفتران و دفتر یاران*، ۷۵: ۶۳–۷۶.

– مولوی، مهران؛ سلطانی، لقمان و زیرک طلاتپه، بهنام (۱۳۹۵). «نقش فناوری اطلاعات در جرایم اینترنتی شبکه بانکی». *مجله مطالعات علوم کاربردی در مهندسی*،۲(۱): ۱– ۵.

ب. منابع انگلیسی

- Frank, R (2001). *Encyclopedia of Criminology and Deviant Behavior*. Vol.II, Brunnner-Routledge /Taylor and Francis Publishers.

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

- Lcncy, J (2005). *"Identity Theft in cyberspace: Crime control Methods and and Their Effectiveness in combating Phishing Attacks". Berkeley Technology Law Journal*, 259.

- Simmons, B, (2002). "Money and the Law: Why empty with the Public International Law of Money?". *Yale Journal of International Law*, 323-326.

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