Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

فصلنامه علمی فقه و حقوق نوین

Print ISSN: 2717- 1469
Online ISSN: 2717 - 1477

نمایه در SID، Noormags، ISC
Magiran، Ensani، GoogleScholar
www.jaml .ir
سال چهارم، شماره سیزدهم،
صفحات ۷۶-۵۳

تدابیر پیشگیری از جرایم درگاه‌های پرداخت اینترنتی

دکتر زینب نفر — دکتری فقه و مبانی حقوق اسلامی، دانشگاه تهران، تهران، ایران؛ استاد مدعو دانشگاه الزهرا ، ایران، تهران.

محمدحسین پاوند — کارشناسی ارشد حقوق جزا و جرم شناسی، دانشگاه آیت الله العظمی بروجردی(ره)، بروجرد، ایران

چکیده:

با گسترش جرایم مرتبط با درگاه‌های پرداخت اینترنتی، قوانین جزایی و تعیین مجازاتهای جرائم مالی پیشگیری از جرائم مرتبط با پرداخت‌های اینترنتی با چالش‌ها و آسیب‌های جدی مواجه شده که سبب نگرانی مردم گردیده است. از این رو هدف مقاله پیش‌رو با بهره‌گیری از روش توصیفی- تحلیلی واکاوی تدابیر و راهکارهای پیشگیری از آن است. اخلال در داده‌های درگاه‌های پرداخت‌های الکترونیکی، برداشت از حساب دیگران، جعل الکترونیکی ازجمله جرایم مرتبط با پرداخت‌های اینترنتی هستند. عوامل نرم‌افزاری، نبود آموزش کافی نحوه استفاده از دستگاه‌های پرداخت‌های و نبود نظارت کافی بر آن‌ها، دسترسی غیرمجاز علیه محرمانگی و سامانه‌های رایانه‌ای بانکی، مختل کردن کارکرد سیستم رایانه‌ای، مختل کردن سیستم‌های عملیاتی بانکی ازجمله عوامل وقوع جرایم مرتبط با پرداخت‌های اینترنتی است. تدابیر پیشگیری از جرایم مرتبط با پرداخت‌های اینترنتی دارای ویژگی‌های افتراقی تدابیر پیشگیری وضعی، تدابیر پیشگیرانه فنی جهت ایمنی سایت‌ها، تکلیف به عدم افشای اطلاعات و تدابیر پیشگیرانه اجتماعی به‌ویژه تدابیر پیشگیرانه محافظت مشتری از کدهای الکترونیکی، توجه مشتری به اعلامیه‌های صادره توسط موسسه مالی و اطلاع‌رسانی می‌باشند.

واژگان کلیدی: درگاه پرداخت، پرداخت اینترنتی، پیشگیری کیفری، کلاهبرداری اینترنتی

طبقه‌بندی JEL: فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

*مسئول مکاتبات: zznafar@gmail.com

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

۱- مقدمه

اگرچه دیر زمانی نیست که سیستم‌های رایانه‌ای و درگاه‌های اینترنتی در ایران جریان یافته است اما جرایم مرتبط با درگاه‌های اینترنتی و کارت‌های شتاب گسترش روزافزونی یافته و اگر برای این جرایم فاکتورهای پیشگیرانه در نظر گرفته نشود، به‌صورت معضل لاینحل درخواهد آمد. از الزامات پیشگیری جرایم درگاه‌های اینترنتی، شناخت روش‌های نفوذ، هک و سوءاستفاده‌های مالی در شبکه‌ی شتاب و اینترنت است. بر طبق آمار موجود۴۸.۵ درصد از جرائم برداشت از حساب بانکی است که بیشتر به دلیل عدم توجه مالکین در نگهداری رمزهایشان، سوءاستفاده اینترنتی از حساب‌هایشان یا نفوذ هکر به شبکه بانکی و برداشت پول بوده است. به‌طورکلی کلاهبرداری اینترنتی با استفاده از فیشینگ و فارمینگ سومین جرم سایبری در کشور تلقی می‌گردد. هویت جعلی نیز یکی از جدیدترین کلاهبرداری‌هایی است که در شبکه‌های اینترنتی صورت می‌گیرد. در حال حاضر رسیدگی به جرایم مرتبط با درگاه‌های اینترنتی در قالب قوانین کلاهبرداری و هم قانون جرایم رایانه‌ای ارزیابی می‌شود. یکی از موارد پیشگیری در جرایم درگاه‌های اینترنتی به‌روزآوری مداوم قوانین موجود مطابق با نوآوری مجرمان در انجام این‌گونه جرایم می‌باشد. از سویی دیگر لازم است سازوکارها و تدابیر پیشگیری (به‌عنوان ارکان مهم رسیدگی به جرایم درگاه‌های اینترنتی) گسترده‌تر و حرفه‌ای‌تر باشد. از سویی دیگر از سوی مردم تأکید می‌شود که با جرایم درگاه‌های اینترنتی مانند کلاهبرداری و اخاذی و غیره با قاطعیت برخورد شود و لازم است شدت عمل و اعمال مجازات نیز به همین ترتیب و جدیت صورت پذیرد. همچنین اطلاع‌رسانی و آگاهی‌بخشی به مردم در این مهم نقش به سزایی دارد. مراقبت از رمزهای اینترنتی، عدم ورود به سایت‌های ناشناس و عدم ارتباط با افراد ناآشنا در فضای مجازی، شناخت روش‌های گوناگون مجرمان در کلاهبرداری‌های اینترنتی استفاده از آنتی‌ویروس‌ها و حفاظت داده‌ها از این جمله می‌باشند. به‌طورکلی می‌توان وجوه پیشگیری از جرایم مرتبط با درگاه‌های اینترنتی را وضعیت حاکم بر قوانین ایران در نظر گرفت.

۱. مفهوم درگاه پرداخت‌های اینترنتی

پرداخت اینترنتی به پرداختن پول از طریق اینترنت، در قبال دریافت کالا یا خدمات اطلاق می‌شود به‌طوری‌که این پرداخت بدون نیاز به

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

حضور فیزیکی در بانک یا فروشگاه و از طریق اینترنت انجام شود. در واقع خریدار با استفاده از کارت‌بانکی خود می‌تواند از اینترنت خرید کند و پول آن را همان موقع پرداخت نماید.

تراکنش الکترونیکی وجه، به معنی هر نوع انتقال وجهی است که حداقل یکی از عملیات آن با استفاده از ابزارهای الکترونیکی انجام شده باشد؛ مثل پرداخت از طریق تلفن‌بانک، دستگاه خودپرداز و پایانه‌های الکترونیکی فروش. در این نوع تراکنش‌ها، طرفین رابطه، یعنی مشتری و بانک از قدرت یکسانی برخوردار نیستند و همواره این احتمال وجود دارد که بانک، شرایط ناعادلانه‌ای را به مصرف‌کننده‌ای که از خدمات او استفاده می‌کند، تحمیل نماید. از طرفی الکترونیکی بودن این نوع تراکنش‌ها، تهدیدات جدیدی برای مصرف‌کنندگان ایجاد کرده است که سابق بر این، در تراکنش‌های سنتی و مبتنی بر کاغذ، وجود نداشته است.(محمد نسل، ۱۳۹۲، ص۳٤)

اصطلاح پرداخت الکترونیکی وجوه از حیث فنی به استفاده از رایانه یا وسایل مخابراتی جهت ایجاد یا اجرایی نمودن فرآیند پرداخت تعریف می‌شود که در عمل، این مفهوم شامل استفاده از دستگاه‌های خودپرداز، سامانه‌ی نقطه‌ی فروش و نیز تراکنش‌های بر خط می‌باشد.(جعفرزاده، احمدی راد، ۱۳۹۱، ص۱۰۱) قانون انتقال الکترونیکی وجوه آمریکا مصوب ۱۹۷۸، انتقال وجه را بدین گونه تعریف می‌نماید:«انتقال وجوه به معنی مجموعه‌ای از تراکنش‌هایی است که با دستور پرداخت صادره توسط اصل ساز به‌منظور پرداخت وجه به ذینفع دستور، آغاز می‌شود. این اصطلاح شامل هرگونه دستور پرداخت صادره توسط بانک اصل ساز یا بانک واسط در اجرای دستور پرداخت اصل ساز می‌باشد. انتقال وجه با قبول دستور پرداخت اصل ساز توسط بانک ذینفع به سود ذینفع، کامل می‌گردد.» (Sienkiewicz,2002,p2)

اصطلاح انتقال الکترونیکی وجوه به معنی هرگونه انتقال وجهی جز تراکنش‌های انجام شده از طریق چک، حواله یا اسناد کاغذی مشابه است که از طریق پایانه‌ی الکترونیکی، وسایل تلفنی یا نوار رایانه‌ای و مغناطیسی به‌منظور ارائه سفارش، صدور دستور یا تجویز موسسه‌ی مالی به بده کار یا بستانکار نمودن حسابی اجرایی می‌شود. این اصطلاح بدون قید حصر شامل انتقالات نقطه‌ی فروش، تراکنش‌های دستگاه خودپرداز، واریز یا برداشت مستقیم و تراکنش‌های تلفنی می‌گردد.»

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

از دیدگاه نظری و بر اساس بند (a)(۱۰٤) مادهی ٤A قانون متحدالشکل تجاری، فرآیند انتقال وجوه {در بعد الکترونیکی و غیر الکترونیکی}، در واقع، یک سلسله دستورهای پرداخت است که با دستور اصل ساز[1] دایر بر پرداخت مبلغی معین به شخص ذینفع آغاز و با تأمین اعتبار بهحساب ذینفع توسط بانک کامل میشود. در این فرآیند، ارزش مالی از طریق بده کار یا بستانکار نمودن حساب اصل ساز به ذینفع منتقل میگردد. اغلب در فرآیند انتقال وجوه یک یا چند بانک واسط که دستور پرداخت را از بانک اصل ساز یا بانک دیگر دریافت میکنند، وجود دارد و بانک دریافتکنندهی دستور، متعاقباً آن را به بانک واسط یا بانک ذینفع، منعکس مینماید. در یک فرآیند سادهی انتقال وجه، اصل ساز به بانکش اعلام میکند که حسابش را بده کار و به بانک ذینفع منعکس کند که حساب ذینفع را بستانکار نماید. این درخواستها[2] بهعنوان دستور پرداخت تلقی میشود. چنان چه بانک اصل ساز درخواست مذکور را قبول کند، اصل ساز نسبت به بانکش متعهد پرداخت مبلغ مندرج در مفاد دستور خود میگردد. راهنمای حقوقی آنسیترال در خصوص انتقال الکترونیک وجوه، دستور انتقال وجه را چنین تعریف مینماید: «پیام یا بخشی از یک پیام که دستور یا جزئیات لازم برای انتقال وجه را دربر دارد. ضمناً دستور انتقال وجه میتواند شامل انتقال اعتبار یا انتقال بدهی باشد.»(جعفرزاده، احمدی راد، ۱۳۹۱، ص۱۰۲)

قانون نمونهی آنسیترال در خصوص انتقال اعتباری بینالمللی مصوب ۱۹۹۲، در بند b مادهی ۲ «دستور پرداخت» را چنین تعریف مینماید: «دستور بدون قید و شرط صادره توسط ارسال کننده به بانک دریافت کننده دایر بر ارائهی مبلغ مشخص یا قابلتعیینی به ذینفع، مشروط بر اینکه اولاً مقرر باشد تأمین وجه برای بانک دریافتکنندهی دستور، بر اساس بده کار نمودن حساب ارسال کننده یا دریافت مبلغ

[1] اصطلاح «اصل ساز»، ترجمه ی کلمه ی ((Originator میباشد که به تبعیت از قانون تجارت الکترونیکی مصوب ۱۷/۱۰/۸۲ ۱۳ انتخاب شده است. قانون یادشده در بند «ب» ماده ی ۲ در مقام تعریف اصطلاح مذکور مقرر می دارد: «منشا اصلی داده پیام است که داده پیام به وسیله ی او یا از طرف او تولید یا ارسال می شود؛ اما شامل شخصی که در خصوص داده پیام به عنوان واسطه عمل میکند نخواهد شد.»

[2] دقت در مفهوم درخواست نشان میدهد که به کارگیری اصطلاح «دستور پرداخت» که ترجمه لفظ به لفظ عبارت ((Payment order میباشد، در واقع خالی از مسامحه نیست.

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

از وی صورت گیرد و ثانیاً، مفاد دستور مقرر نکرده باشد که پرداخت بنا به درخواست ذینفع، تحقق یابد.»

در نظام حقوقی ایران، بند «ح» ماده‌ی ۱ آیین‌نامه‌ی بانکداری الکترونیکی ضمن به‌کارگیری عبارت انگلیسی «Electronic Fund Transfer» در عمل به تعریف اصطلاح پایانه‌ی فروش اقدام نموده است. به نظر می‌رسد استعمال عبارت انگلیسی مذکور، از باب مسامحه در بیان بوده، چرا که با دقت در تعریف ارائه شده، مشخص می‌گردد که تعریف مذکور در واقع تعریف اصطلاح پایانه‌ی فروش و ترجمه‌ی عبارت «Point of Sale» بوده که در واقع یکی از روش‌های انتقال الکترونیکی وجوه است.[3] نظر به موارد مذکور، تعریف صحیح برای دستور پرداخت در تحقیق حاضر عبارت است از :«دستور ارسالی به بانک دایر بر ایجاد اعتبار یا بدهی به میزان مبلغ مشخص یا قابل تعیین برای ذینفع به وصفی که دستور مذکور حاوی شرطی جز زمان پرداخت نباشد.»

(Fry, 2020, p1401) دستور مشتری به بانکش دایر بر انجام عملی اضافه بر پرداخت یا وصول وجه، دستور انتقال الکترونیکی وجه محسوب نمی‌شود.

به استناد بند (i)(a۱)(۱۰۳) ماده‌ی ٤ A قانون متحدالشکل تجاری، دستور پرداخت نباید حاوی هیچ‌گونه شرطی جز زمان پرداخت باشد. الزامی به این‌که پرداخت، عندالمطالبه باشد، وجود ندارد. مشتری بانک، آزاد است مقرر کند که پرداخت به ذینفع در تاریخ معین یا قبل از آن صورت گیرد. براساس بند ۳۰۱ ماده‌ی فوق، مشتری می‌تواند علاوه بر تاریخ پرداخت در مفاد دستورش، تاریخ اجرای دستور را نیز مشخص نماید. بر مبنای عنصر مذکور، مواردی که در متن دستور به بانک اعلام گردید؛ بانک زمانی نسبت به پرداخت اقدام نماید که ذینفع یا اشخاص دیگر، تعهد مفروض خود را ایفا نمایند یا بانک اسناد معینی را دریافت کند، به دلیل مشروط بودن، مصداق دستور پرداخت نمی‌باشد.

---

[3] در واقع پایانه های فروش، ماشین هایی هستند که مانند یک اسکنر اعتباری عمل می‌کند و معمولاً در فروشگاه های بزرگ، مراکز تجاری، هتل ها، فرودگاه ها و... مورد استفاده هستند و به کاربر اجازه می‌دهند پرداخت صورت‌حساب‌های خرید کالا و خدمات خود را از طریق کارت انجام دهد. در این روش پرداخت، پول بلافاصله‌ی و یا بافاصله زمانی نسبتاً کوتاهی از حساب بانکی کاربر به‌حساب فروشگاه یا مرکز تجاری منتقل می‌شود. (قناد، ۱۳۸۸، ص۲۵)

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

مخاطب دستور پرداخت، باید بانک باشد. بانک در حوزه‌ی انتقال الکترونیکی وجوه، در بند ۱۰۵(۲) ماده‌ی ٤ A مذکور به‌عنوان شخصی معرفی‌شده که در تجارت بانکداری به‌نوعی دخیل باشد؛ این مفهوم شامل بانک‌های ذخیره، انجمن‌های پس‌انداز و وام، اتحادیه‌ی اعتباری و شرکت‌های تراست می‌باشد. در خصوص تراکنش‌های مصرف‌کننده، قانون انتقال الکترونیکی وجوه از اصطلاح «موسسه‌ی مالی» به‌جای بانک استفاده نموده و در مقام بیان مصادیق آن در ماده‌ی ۱٦۹۳(a)(۸) به «بانک ایالتی و ملی، انجمن سپرده و وام ایالتی و فدرال، بانک سپرده‌ی متقابل، اتحادیه‌ی اعتباری ایالتی و فدرال، یا هر شخصی که مستقیم یا غیرمستقیم، حساب مصرف‌کننده‌ای را در اختیار دارد» اشاره کرده است. با توجه به این مراتب، دستور به شخص بدهکار دایر بر پرداخت مبلغ معینی به ثالث، شرط موردبحث را تأمین نمی‌کند. البته دستور پرداخت می‌تواند به‌صورت مستقیم یا غیرمستقیم به بانک منعکس گردد. (عباسی نژاد؛ مهرنوش، ۱۳۸۸، صص ۲۱٤-۲۲٦)

ضرورت ندارد که دستور پرداخت از طریق وسایل الکترونیکی، اصل سازی گردد. بر اساس بند ۱۰۳(a)(۱) ماده‌ی ٤A قانون منظور، دستور کتبی یا شفاهی به بانک دایر بر انتقال مبلغ معین، دستور پرداخت محسوب می‌گردد. اطلاق لفظ «دستور» مفید این معناست. در عمل، دستور پرداخت هر بانک به بانک بعدی در یک زنجیره به‌صورت الکترونیکی منعکس می‌گردد و اغلب، دستور پرداخت اصل ساز به بانکش نیز به‌صورت الکترونیکی منتقل می‌شود، لکن وسیله‌ی انتقال از حیث حقوقی مؤثر در مقام نیست. دستور پرداخت ممکن است با هر وسیله‌ای و حتی در برخی موارد از طریق وسایلی با سرعت کم مانند پست عادی انجام شود. (اکرمی، ۱۳۹۵، صص۲۱۹- ۲۳۰) براساس مطالب ارائه شده روشن می‌شود که تعاریف ارائه‌شده‌ی بین‌المللی در نظام حقوقی ایران نیز موردقبول است، چرا که از حیث ماهیت فنی، فرآیند مذکور در کشورهای مختلف، واجد تفاوت عمده‌ای نمی‌باشد.

۲. مبنای پیشگیری اجتماعی سرقت هویت برای ارتکاب کلاهبرداری در پرداخت اینترنتی

جعل هویت در بانکداری نوین، جنبهٔ فنی و تخصصی دارد و یکی از اشکال تقلب علیه

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

سیستم پردازش خودکار داده‌هاست. ابزار مورد استفاده نیرنگ و تزویر است. این روش رفتار شخص را در وضعیت عدم تعادل قرار داده که برخلاف عدالت است. وقتی از این حالت عدم تعادل مشخص سوءاستفاده شود، یعنی فریب مؤثر واقع شده و تحصیل مال صورت پذیرفته است. در این صورت بزهکار توانسته به یک هدف ضد ارزش که همان منافع اقتصادی نامشروع است دست یابد، ارزش نقض شده امنیت اقتصادی و موردحمایت حقوق جزاست. معیار جرم انگاری آن نیز جلوگیری از ضرر است. (شاکری، ۱۳۸۲، ص۱۱) به همین دلیل این جرم اقتصادی و مبتنی بر تزویر است. در مقابل، استفاده منصفانه و متعادل از زرنگی که مفهومی مقبول و خنثی است، جرم نیست، ولی نیرنگ به‌عنوان وسیله‌ای که باعث نقض یک ارزش موردحمایت حقوق جزا شده است، وسیلهٔ مجرمانه بوده و محکوم است. بدین سبب حقوق جزا به حقوق وسایل نیز تعبیر شده است. ماهیت کلاهبرداری با روش جعل هویت مبتنی بر دروغ است؛ چون اطلاعات شفاهی و غیرشفاهی غلط ارائه می‌شود تا دیگری فریب بخورد و اطلاعات امنیتی حساب یا کارت‌بانکی خود را افشا نماید. این اقدام نوعی خشونت انحرافی به‌حساب آمده (گسن، ۱۳۸۹، ص ۲۵) و دروغی فریبنده است که باعث خواهد شد کاربران بانکداری الکترونیک متوجه حملهٔ مزورانه و نیات واقعی طرف مقابل نشوند و چون به گفته‌های دروغ اعتماد کرده و در نتیجه دفاعی برای حفاظت از اطلاعات بانکی خود پیش‌بینی نکرده‌اند، به همین خاطر جزء دروغ‌های حمله و دفاع از نوع منفعت محور است. (زینالی، ۱۳۸۱، ص۱۰۳) در حقیقت دروغ‌گو در قالب یک فعالیت روان‌شناختی ارتباطی جلب اطمینان کرده و رفتار مخاطب را هدایت خواهد کرد. درحالی‌که اگر اطلاعات درست بود نتایج متفاوتی به دنبال داشت و مخاطب در مسیر موردنظر کلاهبردار که همان کسب منافع است، قرار نمی‌گرفت. بنابراین این نوع دروغ خودخواهانه است؛ چون برای کسب منافع صورت گرفته است. بر اساس روان‌شناسی اجتماعی نیز این دروغ‌گویان ماهرند و از قدرت کنترل کامل هیجانات و توان بالای کنترل رفتارهای کلامی و غیرکلامی برخوردارند. عمل دروغ‌گویی یک اقدام تعاملی و دوسویه است و برای رسیدن به هدف تحصیل مال همانند یک مجموعهٔ ساختاری از عناصر است. یکی از عناصر ساختاری، شرایط و اوضاع‌واحوال دروغ

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

است که در دو سطح ایجاد خواهد شد؛ سطح اول مربوط به‌جایی است که ایده توسل به‌دروغ شکل‌گرفته و به آن اوضاع‌واحوال ایجادکننده گفته‌اند. این شرایط به القای اندیشهٔ توسل به‌دروغ در وجدان فرد کمک خواهد کرد. (آذری متین، میرمحمد صادقی ۱۳۹۵، صص۳۵ – ٦٤) در رابطه با کلاهبرداری در بانکداری نوین، شرایط ایجادکننده توسعهٔ نوآوری‌های فنی مانند توسعهٔ پرداخت و دریافت پول با کارت بانکی است که موجب شکل‌گیری شرایط ایجادکننده دروغ گردیده و ارتکاب جرم کلاهبرداری را با نظریهٔ فرصت تبیین کرده است؛ زیرا در وضعیت کنونی، استفاده از فناوری‌های نوین اطلاعاتی با توسعه و رشد قابل توجه فرصت‌های کلاهبرداری قابل توجیه است؛ (بیات و دیگران، ۱۳۸۷، ص٤٨) اما باید خاطرنشان ساخت که اگر این اوضاع‌واحوال، اثر افزایشی بر برخی از اشکال دروغ داشته باشد، همه مرتکب آن نمی‌شوند. بی‌تردید شخصیت مرتکب در اینجا بی‌تأثیر نیست. در هر حالت، شرایط و اوضاع‌واحوال باید گذر از اندیشه به فعل را اجازه دهد. اینجاست که نوع دوم اوضاع‌واحوال یعنی شرایط محقق کننده ظاهر خواهد شد.(همان، ص ١٤٧)

۳. آسیب‌شناسی برنامه‌های مبتنی بر پیشگیری وضعی از جرایم مرتبط با پرداخت‌های اینترنتی

اقدامات مبتنی بر پیشگیری وضعی از جرایم مرتبط با پرداخت‌های اینترنتی شامل روش‌هایی مانند نظارت بر مراکز عرضه کنندهٔ اینترنت، فیلترینگ و غیره است. در ادامه، باید بیان کرد این نوع پیشگیری اساساً بزه دیده محور است. بنابراین، با پیشگیری اجتماعی که بزهکار را در کانون توجه خود قرار می‌دهد، متفاوت است، هرچند در اینجا مجرم به‌طور غیرمستقیم مطرح است. (نجفی ابرندآبادی، ۱۳۸۲، ص ۱۷۱) با اینکه عملی کردن این نوع پیشگیری درباره جرائم اینترنتی به‌ویژه جرایم مرتبط با پرداخت‌های اینترنتی بسیار مشکل است، باز هم جایگاه خاصی در سیاست جنایی کشورها برای مقابله با این جرم دارد و برخلاف کاستی‌های ذاتی این نوع پیشگیری، در بعضی موارد کارایی دارد. (صفاری، ۱۳۸۱، ص ۲۳۳-۱۹۳؛ نجفی ابرندآبادی، ۱۳۸۲، ص ۵۵۹) ازجمله مهم‌ترین انتقادهای وارده در این زمینه، به مصادیق موجود در محور اصلی افزایش زحمت ارتکاب جرم و افزایش خطرات ارتکاب جرم برمی‌گردد. علت این است که این دو محور عملاً تشکیل دهندهٔ

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

عمده‌ترین بخش مربوط به برنامه‌های مبتنی بر پیشگیری از جرایم مرتبط با پرداخت‌های اینترنتی در سیاست جنایی ایران هستند. با نگاهی به مصادیق، می‌توان سیاست جنایی ایران در این زمینه را به این شرح نقد کرد و ایراد گرفت که برای مثال، در بحث به‌کارگیری فیلترینگ و گذرواژه‌ها، مهم‌ترین نقد وارده این است که از طرفی، مسئولان سعی در اجرای فیلترینگ به‌طور تخصصی و کلی دارند، اما از طرف دیگر، آماده‌سازی زیرساخت‌های موجود برای این کار را کمتر موردتوجه قرار می‌دهند، به‌طوری‌که امروزه در جامعه شاهدیم بحث فیلترینگ به موضوعی سلیقه‌ای تبدیل‌شده است و آیین‌نامه یا دستورالعملی مشخص و مدون برای آن وجود ندارد و صرفاً بر اساس یک سری مسائل عمومی و سلیقه‌ای انجام می‌گیرد. موضوع مهم‌تر اینکه به دلیل موضوعات یادشده، متأسفانه به‌کارگیری برنامه‌های گذر از فیلتر در جامعه روبه افزایش است. (انصاری، ۱۳۹۵، صص ۱٤٥ – ١٦٤) البته موضوع به‌کارگیری این ابزارها نیز، از مهم‌ترین نقدهایی است که می‌توان بیان کرد. به این شرح که چرا با وجود صرف هزینه‌های هنگفت و صرف وقت فراوان برای فیلترینگ سایت‌های نامناسب، باید به راحتی برنامه‌های گذر از فیلتر قابل‌دسترسی و خرید باشد و عملاً همهٔ زحمات برای فیلترینگ زیر سؤال برود. (خلقی، ۱۳۸۸، ص۱۱۹) نقد دیگر نیز که می‌توان به برنامه‌های مبتنی بر پیشگیری وضعی در ایران وارد کرد، مربوط به بحث ناکافی بودن میزان آگاهی مردم و مدیران ارگان‌های مختلف هنگام مواجهه با جرایم مرتبط با پرداخت‌های اینترنتی است که این مسئله نیز طبیعتاً مربوط می‌شود به اینکه ارگان‌های مسئول به این مورد کمتر توجه کرده‌اند، به‌طوری که برای مثال، میزان آگاهی افراد از اینکه انواع مختلف جرایم مرتبط با پرداخت‌های اینترنتی چطور رخ می‌دهد و چه مواردی می‌تواند مشکوک باشد، پایین‌تر از حد معمول است، هرچند در سال‌های اخیر سعی شده است از طریق رسانه‌های جمعی و روزنامه و کتاب، سطح آگاهی مردم بالا برود، هنوز هم راه بسیار طولانی برای رسیدن به کمال مطلوب در این زمینه در پیش است.

پیشگیری در ارتکاب جرم مؤثر و سودمندتر از مبارزه و مجازات می‌باشد. در جرایم مرتبط با پرداخت‌های اینترنتی پیشگیری باید به‌عنوان هدف عمده هرگونه سیاستگذاری در این خصوص باشد. (گسن، ١٣٧٤، ص١٧٩)

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

پیشگیری از ارتکاب این‌گونه جرایم نوین به لحاظ تجاری اداری – اجتماعی امری مهم بوده و بستگی به کارایی و امنیت فناوری مدرن اطلاعات دارد. ضمن اینکه اجرای تدابیر امنیتی و پیشگیری از جرایم مرتبط با پرداخت‌های اینترنتی باید با توسعه فناوری اطلاعات همگام باشد.

۴. پیشگیری از دسترسی غیرمجاز از طریق درگاه‌های غیرحضوری

اگر کانال‌های ارتباط بانکی، اینترنت، موبایل یا تلفن ثابت باشد، تدابیر حفاظتی از نوع رمز عبور یا گذر واژه است. خدمات بانکی ارائه شده، رایانه‌ای محض است. بنابراین، «نفوذ یا رخنه گری به درگاه‌های غیرحضوری بانک از طریق دانش فنی امکان‌پذیر است. شیوه فنی رخنه به سامانه‌های رایانه‌ای هک نامیده شده است». (داوری دولت‌آبادی، ۱۳۹۳، ص ۲۵) هک به معنای نفوذ به یک سیستم رایانه‌ای است و هکر که در فارسی به رخنه گر و نفوذگر ترجمه شده، کسی است که با داشتن دانش برنامه‌نویسی و نرم‌افزار می‌تواند به یک سیستم رایانه‌ای نفوذ کند. شیوه‌های دسترسی هکرها بسیار گوناگون هستند و امکان دارد همراه با سایر بزه‌ها باشد.

انتشار نرم‌افزار مخرب یکی از عناوین قانونی روش نفوذگری به سامانه‌های بانکی است، بند الف ماده ۷۳۵ قانون مجازات اسلامی به انتشار نرم‌افزارهای ویژه‌ای اشاره دارد که در پیکره ویروس یا کرم رایانه‌ای و...به منظور ارتکاب سایر جرایم رایانه‌ای به کار رفته است. بنابراین، سایر نرم‌افزارهایی که به‌عنوان بدافزار شناخته شده وبرای ارتکاب بزه‌های رایانه‌ای کاربرد ندارند، مشمول حکم این قانون قرار نخواهد گرفت؛ مانند نرم‌افزارهایی که با ارسال بیش از اندازه اسپم یا پیام الکترونیکی باعث کم شدن پهنای باند اینترنت خواهد شد. چون رفتار انتشار نسبت به بد افزار برای نفوذ به سامانه‌های بانکی موضوع جرم است، به‌طور مستقل جرم انگاری گردیده و مستلزم حصول نتیجه خاصی نیست. به همین دلیل در زمره جرایم مطلق است و با این فرض نرم‌افزار مخرب اگر به‌عنوان ابزاری برای دسترسی غیرمجاز از طریق گذر واژه استفاده شود، چنانچه همراه با ارتکاب سایر جرایم رایانه‌ای باشد، از موارد تعدد جرم است. (نجفی ابرندآبادی، ۱۳۸٤، صص۲۲۹-۲۱۷) بزه دسترسی غیرمجاز جامع جرایم سایبری است، چون دروازه ورود برای ارتکاب سایر جرایم سایبری است، به همین دلیل سیاست کیفری

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

توان گیری نسبت به مرتکبین جرم دسترسی غیرمجاز ضروری است، زیرا زندانی کردن بزهکار او را ناتوان کرده و مانع فعالیت‌های مجرمانه او خواهد شد.(غلامی، ۱۳۸۸، ص ۵۰۱) غالباً نیز این افراد بلافاصله پس از آزادی مرتکب جرم خواهند شد، در نتیجه بازپروری آن‌ها در زندان تأثیری نداشته است، به همین دلیل پیشنهاد شده است، در رابطه با این افراد از قرارهای مصادره و تحدید کاربرد استفاده شود، به‌عنوان نمونه رایانه ضبط شده یا استفاده از رایانه‌هایی که به اینترنت متصل هستند ممنوع شود یا خدمات بانکداری نوین ارائه نشود، این راهبرد کیفری در صورتی مؤثر است که دولت امکان نظارت فراگیر نسبت به مراکز ارائه دهنده خدمات اینترنتی مثل کافی‌نت‌ها را داشته باشد تا امکان بهره‌برداری اینترنتی محکومین از این مراکز عمومی عملاً سلب شود و بانک‌ها نیز آن‌چنان سازوکارهای کنترلی داشته باشند که امکان استفاده از اینترنت بانک، به غیر از صاحب حساب بانک عملی نباشد.(قناد، ۱۳۸۸ ، ص ۲۳۱)

۴-۱. تغییر گذرواژه

گذرواژه، داده است، مجوز دسترسی به‌حساب‌های بانکی را صادر می‌کند، نوع دسترسی بانک‌ها به گذرواژه کاربران بانکی از نوع عملیاتی است، بنابراین، بانک‌ها مجازند با درخواست کاربران یا در مواردی که سایت بانک هک شده، اقدام به تغییر گذرواژه نمایند. از طرف دیگر مقامات قضایی یا ضابطان دادگستری نیز طبق ماده ٦٧٥ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ اجازه دارند تا از طریق تغییر گذرواژه اقدام به توقیف داده‌ها نمایند. بنابراین، اگر شخصی نرم‌افزار مخرب منتشر نموده و به‌طور غیرمجاز باعث تغییر گذرواژه نزد سرویس‌دهنده‌های مرکزی بانک شود، علاوه بر اینکه باعث ممانعت از دسترسی کاربر مجاز به خدمات بانکداری نوین شده است، امکان دسترسی غیرمجاز هم فراهم گردیده است. این بدین معنی است که موضوع جرم ممانعت از دسترسی خود داده یا سامانه نیست، لکه دسترسی به خدمات بانکی موضوع جرم است. به غیر از انتشار نرم‌افزار مخرب، یکی دیگر از روش‌های تغییر گذرواژه، مهندسی اجتماعی مبتنی بر کامپیوتر است. در این روش، مهندسی اجتماعی با استفاده از کامپیوتر است. (عالی‌پور، ۱۳۹۰، ص ۲۷۳) صفحات جعلی یا فیشینگ یا رمزگیری، از ین جمله است، باعث خواهد شد کلمه عبور یا گذرواژه کاربر افشاء

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

شده و پس‌ازآن نفوذگر قادر است به‌عنوان کاربر مجاز و از طریق درگاه‌های بانکی به‌طور غیرمجاز اقدام به تغییر گذرواژه نماید. شیوه باز کردن کیف رمزدار هم ازجمله روش‌های غیرفنی دسترسی غیرمجاز است. در ین روش رخنه گر مثل کسی که رمز کیف خود را فراموش کرده است، با سعی و خطا قصد دارد به شماره رمز دسترسی پیدا کند. بدین ترتیب، پس‌ازاینکه دسترسی غیرمجاز صورت گرفت، امکان تغییر گذرواژه از طریق درگاه‌های بانکی به‌عنوان کاربر مجاز فراهم خواهد شد. در تعیین مجازات جرم ممانعت از دسترسی، چنانچه همراه با دسترسی غیرمجاز باشد، تعدد واقعی حاکم خواهد بود، زیرا جرم ممانعت از دسترسی بدون انجام دسترسی غیرمجاز امکان پذیر است؛ مانند کسی که از طریق حساب کاربری بانکی خود و از طریق سرویس‌دهنده‌های مرکزی بانک اقدام به ارتکاب جرم ممانعت از دسترسی نماید. مناسب‌ترین راهبرد کیفری نسبت به این جرم، روش پیامدگرای ارعابی یا بازدارندگی است، ین نظریه مبتنی بر انسان اقتصادی یا بزهکار عقلانی است و فرد با تکیه بر تحلیل هزینه – فایده گزینه مجرمانه را انتخاب می‌کند (نعیمی، ۱۳۹٤، ص ۲۰۵) به دلیل اینکه از نظر حداقل و حداکثر مجازات حبس، جرم ممانعت از دسترسی در ردیف حداقل ین ضمانت اجرا قرار گرفته و مشابه سرقت رایانه‌ای یا دسترسی غیرمجاز است، بنابراین برای تشخیص اینکه کدام یک از مجازات‌های حبس یا جزای نقدی مناسب‌تر است، بهترین روش استفاده از گونه ارعاب نهایی است، در این‌گونه به نرخ تکرار جرم توجه شده است (میرمحمد صادقی ۱۳۹٦، صص٤۹–۷۸)، پس اگر نرخ تکرار جرم هرکدام از ضمانت اجراهای معین و موازی (حبس یا جزای نقدی) کمتر باشد از آن نوع ضمانت اجرا استفاده خواهد شد.

۴-۲. حذف گذرواژه

گذرواژه یا رمز عبوری که صاحب حساب استفاده خواهد کرد، باید با الگوریتم‌های کدنگاری که برای هر حساب بانکی به‌طور جداگانه در سرویس‌دهنده‌های مرکزی بانک‌ها از قبل تعریف‌شده است، تطابق داشته تا اجازه عملیات بانکی برای کاربر صادر شود. بنابراین اگر کسی قصد دسترسی غیرمجاز به سامانه‌های بانکی را داشته باشد، یکی از روش‌های فنی، استفاده از نرم‌افزار مخرب است تا سرویس‌دهنده‌های مرکزی بانک برای یک کاربر خاص بدون گذرواژه گردد. چون گذرواژه از

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

جنس داده است. بدون گذرواژه کردن سامانه در قالب یکی از رفتارهای ماده ۷۳۶ قانون مجازات اسلامی قرار خواهد گرفت. در عمل تخریب گذرواژه دسترسی غیرمجاز نیست. چون گذرواژه کارکرد امنیتی داشته و مجوز دسترسی به‌حساب‌های بانکی اشخاص در محل سرویس‌دهنده‌های مرکزی بانک را داده و از سایر داده‌های مالی و غیرمالی که حین فعالیت بانکی در سرویس‌دهنده‌های مرکزی بانک ذخیره شده است، حفاظت و حمایت می‌کند. مختل یا غیرقابل‌پردازش کردن گذرواژه نیز امکان پذیر نیست، چون به هرحال، گذرواژه ای که دستکاری شده است، غیرقابل پردازش نشده و قابل پردازش است، ولی نتیجه پردازش، کارایی و کارکرد صدور مجوز دسترسی به سامانه یا سرویس‌دهنده‌های مرکزی بانک را ندارد، بدین ترتیب امکان دسترسی غیرمجاز وجود ندارد. بنابراین نوع رفتاری که نسبت به گذرواژه رخ خواهد داد، حذف یا پاک کردن است، چون با پاک شدن گذرواژه، سرویس‌دهنده‌های مرکزی بانک در عمل فاقد تدابیر حفاظتی شده و با ین روش امکان دسترسی غیرمجاز فراهم خواهد شد. (الهی‌منش و صدره‌نشین، ۱۳۹۱، ص ۲٤) با وجود اینکه گذرواژه عینی نیست، ولی در عالم خارج متعلق به صاحب حساب است و چون امنیت کاربر را تأمین خواهد کرد، تخریب و حذف گذرواژه از طرف مالک (صاحب حساب) جرم نیست.(فرایبرگ، ۱۳۹۱، ص ۱۸۰) جرم تخریب گذرواژه برخلاف ممانعت از دسترسی برای صاحب حساب بانکی احتمال خسارت بیشتری دارد، زیرا با بدون گذرواژه شدن، تدابیر حفاظتی برداشته شده و امکان دسترسی به‌حساب بانکی توسط هرشخصی فراهم خواهد شد، از این لحاظ ضمانت اجرای پیش‌بینی شده از نظر تحلیل اقتصادی فعل محور بوده و زیان محور نیست، زیرا سازماندهی پاسخ کیفری به رفتار مجرمانه مبتنی بر زیان وارده نیست و ضمانت اجرا با توجه به نوع فعل انجام شده و بدون درنظر گرفتن نتایج زیان بار رفتار بزهکارانه (فعل مجرمانه) به بزهکار تحمیل خواهد شد. (انصاری، ۱۳۸۸، ص ۱٤۷) نوع ضمانت اجرا نیز ارعاب جزئی است، چون کیفر حبس پیش‌بینی شده از نظر حداقل و اکثر بالاترین میزان را در جرایم کامپیوتری دارد، بنابراین تهدید به ضمانت اجرا ارزش ارعابی داشته و فرد تصمیم به ارتکاب جرمی خواهد گرفت که ضمانت اجرای سبک‌تری دارد. در حقیقت در شرایط مساوی مثل حالت قبل که

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

نتیجه یکسانی برای بزهکار دارد، فرد ارتکاب جرم ممانعت از دسترسی را انتخاب خواهد کرد و در این حالت می‌توان گفت ارعاب جزئی مؤثر واقع شده است.(جوان جعفری و اسلامی، ۱۳۹۵، ص ٦٥)

۵. پیشگیری از دسترسی غیرمجاز از طریق درگاه‌های حضوری

در روش حضوری (تماسی)، قرار دادن کارت پرداخت بانکی در درگاه‌های حضوری مثل دستگاه خودپرداز یا پایانه فروش برای شناسایی دریافت کننده خدمات الکترونیکی بود و درج رمز اول کارت به منزله تأکید تراکنش و قبول شرایط درخواست به عمل آمده است. بنابراین امضای الکترونیکی از طریق روش حضوری دو ماهیت دارد. ماهیت فیزیکی به‌عنوان جسم کارت و ماهیت مجازی، رمزی است که دارنده کارت از آن آگاه است. قرار دادن کارت بانکی و درج گذرواژه یک تدبیر حفاظتی در درگاه‌های حضوری است و دسترسی غیرمجاز از طریق این درگاه‌ها دو شرط دارد، تحصیل غیرمجاز گذرواژه و دوم جعل و استفاده از کارت که به ترتیب موردبررسی قرار خواهد گرفت. (آلبینز، ۱۳۹۳، ص ١٦٦)

۵-۱. روش‌های تحصیل رمز کارت

روش فنی استراق سمع یا شنود غیرمجاز رمز کارت از طریق درگاه‌های حضوری، شیوه دریافت امواج است. دستگاه خودپرداز و پایانه فروش مثل هر رایانه‌ای امواج الکترومغناطیسی ساطع می‌کند که نشت الکترونیکی نامیده شده است، به محض فشرده شدن کلیدهای صفحه کلید، امواج از طریق سیم‌های حامل جریان الکترونیکی در محیط اطراف منتشر شده که به وسیله تجهیزات خاصی قابل شنود و آشکارسازی است. روش‌های غیرفنی دسترسی به گذرواژه به شیوه انواع مهندسی اجتماعی مبتنی بر انسان است، در ین روش از بی‌احتیاطی یا اطمینان بیش از حد انسان‌ها برای جمع‌آوری اطلاعات حساس استفاده شده است. نصب و استتار دوربین کوچک بالای دستگاه خودپرداز یا ایستادن کنار کاربر به منظور دیدن و خواندن کلمه عبور، به دست آوردن پاکتی که رمز اولیه کارت درون آن نوشته شده از طریق جست‌وجو در زباله‌های بانکی یا حتی اعلام رمز صاحبان کارت به متصدیان فروشگاه‌ها برای واردکردن رمز، از جمله این روش‌ها است، همه موارد در قوانین موجود جرم انگاری نشده است. در صورتی که طبق نظریه کنترل اجتماعی تهدید به

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

مجازات باعث هم‌نوایی فرد با جامعه خواهد شد.(نجفی ابرندآبادی، ۱۳۸٤، ص ۹۱) در مقابل، طبق بند (ب) ماده ۷۵۳ قانون مجازات اسلامی، فروش، انتشار یا در دسترس قرار دادن گذرواژه، بدون رضایت صاحب آن جرم و نوعی معاونت برای ارتکاب جرم دسترسی غیرمجاز است.(محمد نسل، ۱۳۹۲، ص ۱۸٤)

۵-۲. پیشگیری از جعل و استفاده از کارت

از نظر فناوری ساخت، کارت‌های بانکی دو نوع دارد و روش جعل هرکدام متفاوت است. در کارت‌های مغناطیسی اطلاعات مشتری شامل: شماره کارت، کد اعتبارسنجی و تاریخ انقضا در نوار مغناطیسی پشت کارت قرار گرفته است. این اطلاعات، علائمی منحصر به فرد از جنس داده است که برای درک و استفاده کاربر در درگاه‌های الکترونیکی، تبدیل به شماره و عدد شده است. چون به‌عنوان نشانه استفاده شده، قابل سنجش نبوده و نمی‌توان اعمال مجاز ریاضی روی آنها انجام داد. این کارت از نوع کارت قابل پردازش است موقعی که کارت در دستگاه قرار می‌گیرد، اطلاعات کارت برای سیستم‌های متمرکز بانک ارسال خواهد شد، اگر صحت داشته باشد، مشتری خواهد توانست به‌صورت لحظه‌ای یا برخط از کارت استفاده کند. بنابراین برای اینکه دسترسی غیرمجاز از طریق درگاه‌های حضوری امکان پذیر گردد، علاوه برداشتن رمز عبور، مستلزم در اختیار داشتن فیزیک کارت هم است. به این منظور، بزهکار باید از کارت اصلی خود کاربر استفاده کند، یا علائم کارت را روی کارت خالی دیگری کپی کند. کپی کردن کارت با هیچ‌کدام از رفتارهای مادی جعل کارت تطابق ندارد. چون، تغییر و واردکردن داده به معنی دگرگونی نسبت به داده‌های موجود است و ایجاد داده هم به معنای پدیدآوردن داده‌ای است که تاکنون وجود نداشته است. به علاوه، دسترسی غیرمجاز هم نیست چون کارت‌های مغناطیسی که توسط بانک‌ها صادرشده دارای تدابیر حفاظتی نیست، درنتیجه ارتکاب ین عمل سرقت رایانه‌ای است. (میرمحمد صادقی، آذری متین، ۱۳۹٦، صص٤۹-۷۸) روش معمول برای سرقت اطلاعات کارت بانکی، استفاده از دستگاه اسکیمر است، این وسیله روی کارت خوان‌های فروشگاهی و دستگاه‌های خودپرداز قابل نصب است، کاربر بانکداری نوین که از نصب این وسیله بی‌اطلاع است، عملاً مسبب افشاء

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

اطلاعات امنیتی کارت خود خواهد شد، این روش جرم سرقت رایانه‌ای را در زمره جرایم نیرنگ آمیز و متقلبانه قرار داده است، بنابراین راهبرد کیفری برای سرقت رایانه‌ای در بانکداری نوین، اصلاح و بازپروری است، زیرا شاخص‌های حالت خطرناک در بزهکاران این جرم در زمینه استعداد مجرمانه و سازگاری اجتماعی بالا بوده و شخص را نیازمند بازپروری قرار داده است. به نظر می‌رسد در رابطه با سارقین رایانه‌ای دسترسی به این هدف امکان پذیر باشد، به‌عنوان نمونه‌یکی از بزهکاران رایانه‌ای که پس از ۸ ماه از زندان آزاد شده بود، اظهار داشته است: «من از اشتباهاتم درس گرفتم، دیگر هیچ‌گاه ویروس تولید نخواهم کرد، هیچ‌گاه اجازه نخواهم داد که حفره‌های امنیتی سیستم‌های رایانه‌ای برملا شده و در سطح شبکه گسترش یابد، زند نی شدن بسیار ناگوار است، این تلخ‌ترین تجربه زندگی من بود.» نوع دوم کارت‌های بانکی، کارت هوشمنداست. در این کارت به جای نوار مغناطیسی، ریزپردازنده تعبیه شده است و پول الکترونیکی که نوعی داده مالی است، مستقلاً داخل ریزپردازنده ذخیره شده است، به همین دلیل نام دیگر آن کیف پول الکترونیکی است. علی‌رغم اینکه تراشه‌ها در بیشتر مواقع ماهیت فیزیکی به شکل کارت ندارند ولی ین کارت چون قابل پردازش بوده و حافظه دارد یک نوع تراشه است. در واقع، کارت هوشمند همانند یک کامپیوتر کوچک، بدون نیاز به اتصال به سرویس‌دهنده‌های مرکزی بانک، به‌صورت برون خط با درگاه بانکی ارتباط برقرار خواهد کرد، اگر ریزپردازنده کارت، از معتبر بودن دسترسی به کارت مطمئن نشود به کارت خوان اجازه دسترسی برای برداشت یا انتقال وجه نخواهد داد. کارت‌های هوشمند از نظر فنی یک سیستم رایانه‌ای (سامانه) هستند. اگر حافظه کارت دستکاری و تغییر یابد جرم جعل کارت تحقق یافته است، حتی اگر دستکاری توسط صاحب کارت باشد. چون به وجودآورنده داده‌های موجود در کارت بانک است و دارنده کارت صرفاً متصرف داده‌ها است. بنابراین، اگر صاحب کارت با دستکاری حافظه، مبلغ موجودی را افزایش دهد، چون برخلاف قرارداد با بانک رفتار کرده است، عملش غیرمجاز بوده و جعل است. به همین ترتیب، اگر دارنده کارت مانع پردازش داده‌ها شود به‌طوری که به وسیله درگاه‌های بانکی بتواند مبلغ بدهی خود را تسویه نماید ولی از موجودی حافظه کارت کم نشود، چون از طریق

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

دستکاری داده‌ها باعث از کار انداختن و سلب کارآیی و کارکرد ریزپردازنده کارت شده است، عمل وی جرم اخلال‌گری در سامانه‌های رایانه‌ای موضوع ماده ۷۳۷ قانون مجازات اسلامی است (گرایلی، ۱۳۸۹، ص ۱۸۰) در جرایم ذکر شده فرقی ندارد، نسبت به کارت معتبر انجام شود یا کارتی که غیرفعال شده و شماره آن باطل شده است. به هرحال، برای بانک ضرر معنوی دارد و باعث خواهد شد به اعتبار و شهرت تجاری بانک لطمه وارد شده و مشتریانش را از دست بدهد. آخرین مرحله دسترسی غیرمجاز، استفاده از کارت جعلی است و اگر کارت بانکی توسط یک نفر جعل شود و به وسیله کارت جعلی بتواند در درگاه‌های حضوری عملیات بانکی انجام دهد، مشمول تعدد مادی خواهد شد. راهبرد کیفری در جرایمی که به وسیله کارت هوشمند ارتکاب یابد، بیان گرایی یا تقبیح عمومی است. از نظر ایده بیان گرای، مجازات صرفاً چیزی نیست که بر مجرمان واقع می‌شود، لکه چیزی است که عموم به وسیله‌اش با آنها ارتباط برقرار می‌کنند، به عبارت بهتر، جرایم رفتارهایی هستند که عموم محکومشان می‌کند و بیان رسمی محکومیت آنها، مجازات است، از ین رو، به دنبال محکومیت رفتارها هستند، نه افرادی که آن رفتارها را مرتکب شده‌اند، یعنی مجازات، بیان‌گر تقبیح جرایم است، نه اشخاص.(بروکس، ۱۳۹۵، ص ۱۶۷)

۶. تدابیر پیشگیرانه فنی و امنیتی سایت‌ها

تدابیر فنی آن دسته از اقداماتی است که در قلمرو بانکداری الکترونیکی به منظور امنیت الکترونیکی بکار گرفته می‌شود. منظور از تدابیر امنیتی، تدابیر فنی و رایانه‌ای است و به شیوه‌های گوناگون مانند نصب دیوار آتش، نصب گذرواژه، رمزنگاری انجام می‌گیرد. روشن است که این شیوه‌ها تدابیر فیزیکی و انسانی را دربر نمی گیرد. تدابیر امنیتی را می توان از طریق مطلع ساختن بزهدیدگان بالقوه و درمعرض خطر، بواسطه پردازش داده‌ها و نیز ازطریق مشاوره امنیتی بکار گرفت. این امر را می‌توان ازطریق مشاوران امنیتی مستقل، تأییدکنندگان نرم افزاری و سخت‌افزاری، کمپانی‌های بیمه، دانشگاه‌ها، مؤسسات تحقیقاتی، سرویس‌های خبری و دیگر عوامل اجرایی دولتی به مرحله اجرا گذاشت. از آنجایی که تجهیزات الکترونیکی بانکداری نوین از سه

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

قسمت شامل نرم‌افزار، سخت‌افزار و داده‌ها تشکیل یافته، هر بخش به منظور امنیت آن دارای روش‌های خاص خود بوده لذا لازم است در برقراری این مهم اتخاذ روش فنی خاصی صورت پذیرد. هرچند اتخاذ تدابیر فنی ارتکاب جرایم مرتبط با پرداخت‌های اینترنتی را به‌طورکلی محو نمی‌کند ولی برخی از صاحبان سیستم‌ها از اتخاذ تدابیر فنی لازم خودداری می‌نمایند، این گروه برای خود دلایلی دارند مثلا تعیین بعضی از ابزارهای فنی سبب افزایش هزینه‌ها می‌شود. (شیرزاد، ۱۳۸۸، ص۱۰۸) با این حال، هدف اساسی در برقراری روش‌های فنی آن است که ارتکاب این جرایم به‌ویژه ارتکاب جرایم مهم و خطرناک به حداقل رسانیده شود.

در خصوص روش‌های فنی برخورد با جرایم نوین تدابیر زیر را می‌توان مورد لحاظ قرار داد.

الف- اشتراک تمامی بخش‌های صنعت و بانک‌ها در به‌کارگیری معیارهای ایمنی در هر سطح ملی و بین‌المللی با توجه به ماهیت بین‌المللی تکنولوژی اطلاعات و پردازش داده‌ها.

ب- به‌کارگیری تدابیر امنیتی اختیاری توسط کاربران.

ج- تحمیل تدابیر امنیتی اجباری در برخی بخش‌های خاص و حساس.

د- تشویق مدیران و رؤسای سازمان‌ها به اعمال تدابیر فنی لازم.(شریفی، ۱۳۷۹، ص۲۰۳)

امنیت فیزیکی، امنیت مخابرات الکترونیکی، امنیت سخت‌افزاری و نرم‌افزاری، امنیت عملیاتی از جمله مصادیق تدبیر فنی هستند.(شیرزاد ینگ آباد، ۱۳۸۲، ص۱۸۱) با توجه به این اوصاف نتیجه می‌گیریم ساده‌ترین ابزارها برای اتخاذ تدابیر غیرکیفری، تدابیر فیزیکی است. مثل جلوگیری از دستیابی غیرمجاز به سیستم‌ها و تجهیزات الکترونیکی بانک مانند حفاظت از محل استقرار تجهیزات الکترونیکی اصلی بانک (سرورها) جلوگیری از آثار وارده بر پایانه در اثر عوارض و پیامدهای الکترونیکی مثل آتش‌سوزی و جلوگیری از آثار وارده بر پایانه یا سرور بانک در اثر سوانح سخت‌افزاری و همچنین تدابیر نرم‌افزاری مشتمل بر کنترل در دستیابی غیرمجاز با نصب برنامه‌های حفاظتی بر روی سرورها و ایستگاه‌های کاری مرتبط با خدمات نوین بانک کنترل در مرحله ورودی و خروجی، رمزگذاری و غیره است. البته رمزگذاری با دادن یک رمز عبور به هر یک از

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

کاربران (مشتریان بانک) از روش‌های متداول می‌باشد که در هر سیستمی مورد استفاده قرار می‌گیرد. مهمترین وظیفه موسسات مالی در انتقال الکترونیکی وجوه، رعایت کلیه احتیاط‌ها و مراقبت‌های لازم در اجرای دستور پرداخت صادره توسط مشتری است. رعایت احتیاط و مراقبت از جانب موسسه مالی می‌تواند دارای دو جنبه باشد:

اول آنکه در انتقال الکترونیکی وجوه، موسسه مالی براساس روش‌های امنیتی مورد توافق با مشتری، دستور پرداخت صادره را شناسایی و تصدیق نموده و در صورت تأیید و تصدیق بر مبنای آن عمل می‌نماید. حال در صورتی که موسسه مالی دستور پرداخت صادره را تصدیق نماید به تبع آن حساب مشتری را بدهکار کند، اما مشتری ادعا کند که دستور پرداخت بدون مجوز صادر شده است، در گام اول بار اثبات این امر که موسسه مالی کلیه مراقبت‌ها و احتیاط‌های لازم را به عمل آورده و دستور پرداخت صادره براساس روش‌های امنیتی مورد توافق، دستور پرداختی معتبر بوده بر عهده موسسه مالی قرار خواهد گرفت. پس اگر دستور پرداخت صادره به هر دلیلی مبهم و یا متضمن هرگونه ایرادی باشد، موسسه مالی یا باید از اجزای دستور پرداخت خودداری کند و یا قبل از اجرا باید از مشتری بخواهد تا دستور پرداخت صادره را اصلاح و یا آن را تأیید نماید و اگر موسسه مالی بدین‌ترتیب عمل ننماید، احتیاط و مراقبت لازم را به عمل نیاورده است.(شیرزاد، ۱۳۸۸، ص۱۱۲)

دوم آنکه موسسه مالی به منظور رعایت احتیاط و مراقبت‌های لازم باید از سیستم‌های رمزنگاری مناسب و برنامه‌های نرم‌افزاری معقول و مناسب و ایمن به منظور حفاظت از وجوه متعلق به مشتری استفاده نماید. در صورت استفاده از سیستم‌های مناسب، احتمال صدور دستور پرداخت‌های بدون مجوز هم کاهش خواهد یافت. به‌طور قطع، روش امنیتی به کار گرفته شده باید با میزان وجوه موضوع انتقال، نوع و عملکرد مشتری که برای پرداخت‌های کلان و تجاری و یا پرداخت‌های خرد از بانکداری الکترونیکی استفاده می‌کند، متناسب باشد. در مواردی ممکن است موسسه مالی مرتکب تقصیر شود و یا حتی بدون آنکه تقصیر منتسب به موسسه مالی باشد، مسئولیت جبران خسارت ناشی از انتقال الکترونیکی غیر مجاز برعهده موسسه مالی قرار گیرد. احراز چنین امری از جمله امور حکمی است که در هر پرونده

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

متفاوت بوده و به نظر قاضی پرونده بستگی دارد و با توجه به مبانی و منابع مسئولیت مدنی در هر نظام حقوقی متفاوت خواهد بود. دستورالعمل مصوب ۲۰۰۷ اتحادیه اروپا، ارائه دهندگان خدمات پرداخت را ملزم دانسته است تا اطمینان حاصل نمایند که مشخصه‌های امنیتی ابزار پرداخت توسط هیچ شخصی به غیر از استفاده کننده از خدمات پرداخت که حق استفاده از ابزار پرداخت را دارد، قابل دسترسی نیست. به علاوه، آن دستورالعمل، ارائه دهندگان خدمات پرداخت را از ارسال ابزار پرداخت در صورتی که استفاده کننده از خدمات درخواست ننموده، منع کرده است.

نتیجه‌گیری

بانکداری نوین در قالب درگاه‌های اینترنتی شرایط ارتکاب گونه‌هایی از جرایم نوین و شیوه‌های ارتکابی غیرمرسوم در جرایم سنتی را به وجود آورده است. اخلال در داده‌های درگاه‌های پرداختهای الکترونیکی، برداشت از حساب دیگران، جعل الکترونیکی از جمله جرایم مرتبط با پرداخت‌های اینترنتی هستند و قابل ارتکاب در عصر بانکداری نوین هستند. عوامل نرم‌افزاری، نبود آموزش کافی نحوه استفاده از دستگاههای پرداخت‌های اینترنتی، نبود نظارت بر دستگاههای پرداخت‌های اینترنتی و دسترسی غیرمجاز علیه محرمانگی و سامانه‌های رایانه‌ای بانکی از جمله علل وقوع جرایم مرتبط با پرداخت‌های اینترنتی است. صرف‌نظر از ضعف قانونی ضعف ساختار اداری و مدیریتی یقیناً موجب بروز جرایم مرتبط با پرداخت‌های اینترنتی می‌گردد. عدم آموزش کاربران در عرصه بانکداری نوین عدم تمایل به استفاده از برخی از نرم‌افزارهای نوین بانکداری مزید بر علت است که شاهد بروز جرایم مرتبط با پرداخت‌های اینترنتی باشیم، چرا که به جرأت بیان می‌شود که اکثر نرم‌افزارهای بانکداری نوین تماماً قدیمی و به هیچ‌وجه قسمت عمده آن به‌روزرسانی نشده و قابلیت نفوذ را داراست.

قوانین کیفری و تعیین مجازاتهای جرائم مالی به پیشگیری از جرائم مرتبط با پرداختهای اینترنتی دارای چالشها و آسیب‌های جدی می‌باشند. توضیح اینکه سیاست مقنن ایرانی در قبال جرایم مرتبط با پرداخت‌های اینترنتی صرفاً واکنش کیفری است که در چند ماده و یک قانون خاص به نام جرایم رایانه‌ای خلاصه شده است و در واقع از دست‌آوردهای دیگر توسط سایر کشورها و سازمان‌های بین‌المللی بهره

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

زیادی نبرده است، چرا که رشد و توسعه‌یافتگی بانکداری نوین به همان‌قدر زندگی ما را راحت و سهل نموده است که فارغ از محدودیت زمان و مکان که می‌توانیم فعالیت مالی و اقتصادی خود را انجام دهیم، به همان میزان زندگی فردی و اجتماعی ما را در معرض خطر قرار می‌دهد. شاید باور چنین پدیده‌ای درزمان حیات بانکداری سنتی برای کارشناسان و حقوقدانان مشکل و قابل درک نبود. ولی اکنون با این حقیقت روبه‌رو هستیم که جرایمی تحت عنوان جرایم مرتبط با پرداخت‌های اینترنتی وجود دارد، ناگزیر از انجام واکنش‌های کیفری و غیرکیفری نوین در مقابل آن هستیم. هر قدر میزان شناخت ما نسبت جرایم مرتبط با پرداخت‌های اینترنتی بیشتر باشد، واکنش سیستم حقوقی ما در مقابل این نوع جرایم مناسب‌تر و بهتر خواهد بود. گرچه در کشور ایران نواقصی در مبحث قوانین و لوایح مربوط به جرایم مرتبط با پرداخت‌های اینترنتی بسیار وجود دارد که خود حاکی از شناخت نادرست از بانکداری نوین و موضوعات مرتبط با آنچه در زمینه پرداخت‌های اینترنتی و چه در زمینه جرایم مرتبط با آن است. تدابیر پیشگیری از جرایم مرتبط با پرداختهای اینترنتی دارای ویژگی‌های افتراقی تدابیر پیشگیری وضعی به‌ویژه حفاظت فیزیکی، تدابیر پیشگیرانه فنی جهت ایمنی سایت‌ها، تدابیر اداری و سازمانی، تکلیف به عدم افشای اطلاعات و کدگذاری یا رمزنگاری و تدابیر پیشگیرانه اجتماعی به‌ویژه تدابیر پیشگیرانه محافظت مشتری از کدهای الکترونیکی، توجه مشتری به اعلامیه‌های صادره توسط موسسه مالی و اطلاع‌رسانی می‌باشند.

در جهت پیشگیری غیرکیفری از بروز جرایم مرتبط با پرداخت‌های اینترنتی به‌عنوان جایگزین واکنش کیفری که می‌تواند به‌عنوان مکمل یا در کنار جرم‌انگاری جرایم مرتبط با پرداخت‌های اینترنتی در پیشگیری و مبارزه با این جرایم نوین نقش تعیین‌کننده‌ای داشته باشد، می‌تواند به موارد زیر در قالب واکنش‌های غیرکیفری اشاره نمود.

۱- ارتقای تدابیر امنیتی نرم‌افزاری پرداخت‌های اینترنتی و به‌روز بودن سیستم‌های امنیتی بانکداری نوین

۲- استانداردسازی شیوه‌های ارائه درگاه‌های پرداخت‌های اینترنتی از طریق مجزا و سیستم قابل‌قبول و پذیرفته دنیا

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

۳- تربیت و آموزش بازرسان در حوزه درگاه‌های پرداخت‌های اینترنتی

٤- تربیت و جذب کارشناسان انفورماتیکی ماهر و انجام آموزش‌های مستمر لازم و تخصصی حتی با بهره‌گیری از کارشناسان انفورماتیکی دیگر کشورها در حوزه درگاه‌های پرداخت‌های اینترنتی

۵- باید پلیس فتا و قضات مخصوص به‌صورت تخصصی آموزش ببینند. آموزش تخصصی پلیس فتا از بدو تحصیلات انتظامی باید شروع شود و به‌صورت تخصصی‌تر پلیس فتای مبارزه با جرایم پرداخت‌های اینترنتی وجود داشته باشد. مثلاً پلیس جعل الکترونیکی و به تبع آن قضات متخصص هم باید در هر شهر و استان وجود داشته باشد.

سپاسگزاری

از معاونت محترم پژوهشی به خاطر حمایت حمایت معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود.

از آقای دکتر عبدالله علیزاده به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.

از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.

نگارندگان بر خود لازم می‌دانند از آقای دکتر محمد رسول آهنگران به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

۷- منابع

- آذری متین افشین، میرمحمد صادقی حسین، رویکرد جرم شناختی به جعل هویت برای ارتکاب کلاهبرداری در بانکداری نوین، آموزه های حقوق کیفری، پاییز و زمستان ۱۳۹۵، شماره ۱۲، صص۳۵ -۶۴.
- آلبینز، جی اس، سرقت و کلاهبرداری مالکیت فکری، ترجمه حمیدرضا دانش ناری و سیدامین روح الامینی، ۱۳۹۳.
- الهی منش، محمدرضا و ابوالفضل صدره نشین، محشای قانون جرایم رایانه ای، تهران: مجد.
- اکرمی، سام، سعیده اکرمی، پیشگیری غیرکیفری در جرایم اینترنتی مطالعات علوم سیاسی، حقوق و فقه، زمستان ۱۳۹۵، شماره ۴، صص۲۱۹- ۲۳۰.
- انصاری، اسماعیل، «تحلیل اثباتی و هنجاری حقوق کیفری و مجازات های بهینه از دیدگاه مکتب تحلیل اقتصادی حقوق»، فصلنامه اطلاع رسانی حقوقی، شماره ۱۹ و ۲۰، ۱۳۸۸.
- انصاری، جلال؛ میلانی، علیرضا، نقد سیاست جنایی ایران در قبال کلاهبرداری اینترنتی، حقوق جزا و سیاست جنایی، بهار و تابستان ۱۳۹۵، شماره ۳، صص ۱۴۵ – ۱۶۴.
- بروکس، تام، مجازات، ترجمه محمدعلی کاظم نظری، تهران: میزان، ۱۳۹۵.
- بیات، بهرام، جعفر شرافتی پور، نرگس عبدی، پیشگیری از جرم با تکیه بر رویکرد اجتماع محور: (پیشگیری اجتماعی از جرم) تهران: نیروی انتظامی جمهوری اسلامی ایران، معاونت اجتماعی، اداره کل مطالعات اجتماعی، ۱۳۸۷.
- جوان جعفری، عبدالرضا و سیدمحمدجواد اسلامی، «از سزاگرایی کلاسیک تا سزاگرایی نوین»، آموزه های حقوق کیفری، شماره ۲، ۱۳۹۵.
- خلقی، مسلم، مبانی حقوقی پیشگیری از جرم، تهران: انتشارات نورالسجاد به سفارش ستاد مردمی پیشگیری و حفاظت اجتماعی دادگستری، ۱۳۸۸.
- داوری دولت آبادی، مجید، هکرهای قانونمند (CEH)، تهران: آترا، ۱۳۹۳.
- زینالی، حمزه، پیشگیری از بزهکاری و مدیریت آن در پرتو قوانین و مقررات جاری ایران، فصلنامه رفاه اجتماعی، سال دوم، شماره ششم، ۱۳۸۱.
- شاکری، ابوالحسن، قوه قضاییه و پیشگیری از وقوع جرم، مجموعه مقالات همایش علمی – کاربردی پیشگیری از وقوع جرم، تهران، ۱۳۸۲.
- شریفی، مرسده، جرایم رایانه‌ای در حقوق جزای بین‌الملل، پایان‌نامه کارشناسی ارشد دانشگاه آزاد، ۱۳۷۹.
- شیرزاد ینگ آباد، کامران، بررسی جرایم رایانه‌ای در قلمرو حقوق کیفری ایران و حقوق بین‌الملل، پایان‌نامه کارشناسی ارشد دانشگاه آزاد، ۱۳۸۲.
- شیرزاد، کامران، جرایم رایانه ای، تهران، نشر بهینه فراگیر، چاپ اول، ۱۳۸۸.
- صفاری، علی، انتقادات وارده به پیشگیری از جرم. مجلهٔ تحقیقات حقوقی، شماره های ۳۵ و ۳۶، ۱۳۸۱.
- فرایبرگ، آریه، «تعیین مجازات بزهکاران یقه سفید»، ترجمه اعظم مهدوی پور، فصلنامه مطالعات پیشگیری از جرم، شماره ۲۵، ۱۳۹۱.
- قناد، فاطمه، پیشگیری کیفری از جرایم ارتکابی در فضای مجازی، مجموعه مقالات نخستین همایش ملی پیشگیری از جرم، پیشگیری از تکرار جرم و بزه دیدگی، معاونت آموزش ناجا، ۱۳۸۸.
- عالی پور، حسن، حقوق کیفری فناوری اطلاعات، تهران: خرسندی، ۱۳۹۰.
- عباسی نژاد، حسین؛ مهرنوش، مینا، بانکداری الکترونیکی، تهران، سمت، چاپ دوم، ۱۳۸۸.
- غلامی، حسین، «سیاست کیفری سلب توان بزهکاری»، مجله تحقیقات حقوقی، شماره ۵۰، ۱۳۸۸.
- گرایلی، محمدباقر، «بررسی جعل و تخریب و اخلال رایانه ای»، آموزه های حقوق کیفری، شماره ۱۴، ۱۳۸۹.
- گسن، ریموند، جرم‌شناسی بزهکاری اقتصادی (نظریهٔ عمومی تزویر)، برگردان شهرام ابراهیمی، تهران، میزان، ۱۳۸۹.
- ----------، جرم شناسی نظری، ترجمه مهدی کی نیا، تهران، انتشارات مجد، ۱۳۷۴.
- محمد نسل، غلامرضا، جرایم رایانه ای در ایران، تهران: میزان، ۱۳۹۲.

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

- میرقاسم جعفرزاده، حمید احمدی راد، تحلیل ماهیت حقوقی انتقال الکترونیکی وجوه با روی کرد انتقال حق، تحقیقات حقوقی، تابستان ۱۳۹۱، ویژه نامه شماره ۹.
- میرمحمد صادقی حسین، آذری متین، افشین، راهبردهای کیفری در بانکداری نوین؛ با تاکید بر امضای الکترونیکی راهبرد، بهار ۱۳۹۶، شماره ۸۲، صص۴۹-۷۸.
- نجفی ابرندآبادی، علی حسین، تقریرات درس جامعه شناسی جنایی، دوره کارشناسی ارشد حقوق جزا و جرم شناسی دانشگاه شهید بهشتی، نیمسال دوم، ۱۳۸۴.
- ----------، تقریرات درس جرم شناسی. دورهٔ کارشناسی ارشد مجتمع آموزشی عالی قم، گردآورنده مهدی سیدزاده، ۱۳۸۲-۱۳۸۱.
- نعیمی، سیدمرتضی، «تحلیل اقتصادی رفتار بزهکار و تبیین بازدارندگی مجازات»، پژوهشنامه حقوق کیفری، سال ششم، شماره ۲، ۱۳۹۴.
- Sienkiewicz, Stanley J, «The Evolution of EFT Networks from ATM's to New on Line Debit Payment Product USA, Federal Reserve Bank of Philadelphia, April. ۲۰۰۲.
- Fry, P. B., Basic Concepts in: Article A ۴: Scope and Definitions, USA, The Business Lawyer, 2020.

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

Scientific Journal of Modern Jurisprudence and Law

Print ISSN: 2717- 1469
Online ISSN: 2717 - 1477

Profile in ISC,SID, Noormags, Magiran, Ensani, GoogleScholar
www.jaml .ir
forth Year, Issue 13
, Pages 53-76

Measures to prevent crimes of internet payment portals

Dr. Zainab Nafer — PhD in Jurisprudence and Fundamentals of Islamic Law, University of Tehran, Tehran, Iran; Visiting professor at Al-Zahra University, Tehran, Iran.

Mohammad Hossein Pound — Master of Criminal Law and Criminology, Grand Ayatollah University of Borujerdi (RA), Borujerd, Iran.

Abstract

With the spread of crimes related to online payment portals, criminal laws and the determination of punishments for financial crimes, the prevention of crimes related to online payments has faced serious challenges and harms, which has caused people to worry. Therefore, the aim of the upcoming article is to analyze the measures and solutions to prevent it by using the descriptive-analytical method. Disturbances in the data of electronic payment portals, withdrawals from other people's accounts, electronic forgery are among the crimes related to online payments. Software factors, lack of sufficient training on how to use payment devices and lack of sufficient monitoring of them, unauthorized access against confidentiality and bank computer systems, disrupting the functioning of the computer system, disrupting bank operational systems are among the factors of the occurrence of crimes related to Internet payments. Measures to prevent crimes related to internet payments have different characteristics, situational prevention measures, technical preventive measures for the security of websites, mandate not to disclose information and social preventive measures, especially preventive measures to protect the customer from electronic codes, customer attention to the announcements issued by the financial and information institution. Are.

Keywords: payment gateway, internet payment, criminal prevention, internet fraud.

JEL Classification: Jurisprudence - Law - Criminal and Criminology - International Law - Private Law

* Corresponding author**:***zznafar@gmail.com*