راهبردهای کیفری در بانکداری نوین؛ با تأکید بر امضای الکترونیکی

حسین میرمحمدصادقی*

افشین آذری‌متین**

چکیده

به کارگیری فناوری اطلاعات در بانک باعث پدیدآمدن خدمات نوینی شده است، این خدمات که با بهره‌گیری از تجهیزات کامپیوتری ارائه شده است، ارزش‌های جدیدی را خلق و ایجاد کرده است، این ارزش‌ها عموماً فنی و تخصصی است، نقض این ارزش‌ها که علیه داده‌ها و سامانه‌های بانکی است، در قوانین جرایم کامپیوتری و تجارت الکترونیک پیش‌بینی شده است، و چون برای بستر بانکداری نوین (الکترونیک و مجازی) جرم انگاری مستقلی صورت نگرفته است، لازم است اجزاء و تجهیزات فنی شبکه بانکداری نوین با مفاهیم قوانین جزایی حوزه کامپیوتر تطبیق داده شود. بدین ترتیب امکان شناسایی رفتارهای مادی نقض ارزش‌های فنی در بانکداری نوین فراهم خواهد شد. یکی از این ابزارها شیوه تصدیق هویت رایانه‌ای از نظر حقوقی امضای الکترونیکی است که بدنه اصلی جرایم حوزه بانکداری نوین را به خود اختصاص داده است، براین اساس، مقاله حاضر قصد دارد ابتداء کارکرد امضای الکترونیکی را در درگاه‌های بانکی مثل خودپرداز شناسایی نماید، سپس در پرتو شناسایی کارکرد امضای موصوف؛ راهبردهای افتراقی متمایزکننده حقوق کیفری ماهوی سایبری نسبت به جرایم بانکداری نوین قابل تشخیص خواهد بود، به علاوه، از این رهگذر خلأهای قانونی و رفتارهای خاص جرم انگاری شده در بانکداری نوین از سایر جرایم سایبری تفکیک خواهد شد، بدین ترتیب کیفرها نیز شناسایی شده و امکان ارائه پیشنهاداتی برای تعیین نظام کیفری حاکم بر جرایم علیه امضای الکترونیکی در بانکداری نوین فراهم خواهد شد، به نظر می‌رسد استفاده از رویکرد ارفاقی پیامدگرا نسبت به سایر نظام‌های تعیین مجازات از کارایی بیشتری برخوردار باشد.

واژگان کلیدی

راهبرد کیفری، امضای الکترونیکی، دسترسی غیرمجاز، گذرواژه، کارت بانکی، امضای دیجیتال

---

* استاد و مدیر گروه حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی

Email: drsadeghi128@yahoo.com

** دانشجوی دوره دکتری حقوق کیفری و جرم‌شناسی دانشگاه شهید بهشتی (نویسنده مسئول)

Email: azarimatin@gmail.com

تاریخ ارسال: ۹۵/۱۰/۲ تاریخ پذیرش: ۹۶/۲/۲۵

فصلنامه راهبرد / سال بیست‌وششم / شماره ۸۲ / بهار ۱۳۹۶ / صص ۷۸-۴۹

جستارگشایی

نظریه ابزارگرایی،[۱] حقوق کیفری را به عنوان یک تکنیک مؤثر توصیف کرده است،[۲] این بدین معنی است که «حقوق کیفری برای دستیابی به نتیجه یا هدف خاصی به وجود آمده و کاربردی ابزارگونه برای دولت دارد و قادر است برای پیش‌برد اهداف ممکن استفاده شود» (افراسیابی و مصطفی زاده، ۱۳۹۳: ۲۴). بر این اساس، «حقوق کیفری ابزاری برای برقراری نظم اقتصادی جامعه، حفظ حریم حیثیتی افراد، ایجاد نظم سیاسی و موارد مشابه در جامعه است» (حبیب زاده و عمرانی، ۱۳۹۲: ۵۰). بدین ترتیب، رویکرد ابزاری به حقوق کیفری، رابطه نزدیکی با مفهوم راهبرد یا استراتژی دارد. «راهبرد، اقدامات و برنامه‌هایی برای رسیدن به اهداف از پیش تعیین شده است و چگونگی دستیابی به اهداف را مشخص کرده و به اینکه اهداف چه چیز هستند و یا چه باید باشند یا چگونه باید تعیین شوند کاری ندارد» (احمدوند، ۱۳۸۶: ۶۳). بنابراین، «ابزارگرایی یا راهبردهای کیفری، همان حق بر امنیت عینی و ذهنی اشخاص (احساس امنیت آنان) به عنوان یکی از حقوق بنیادین مردم است» (نجفی ابرندآبادی، ۱۳۹۱: ۱۴). و به دولت اجازه می‌دهد به نام و برای تأمین امنیت اشخاص و اموال، به این جهت که به صورت جمعی در جامعه زندگی و کار می‌کنند، در برابر بزهکاران و ناقضان قانون از قوای قهرآمیز استفاده کنند، در این چارچوب نظام کیفری، به عنوان ابزارهای اصلی دولت برای تحقق بخشیدن به این امنیت تدارک و به مناسبت استفاده شده و دولت‌ها امنیت مالی-حیثیتی افراد را از طریق جرم انگاری نقض این ارزش‌ها تضمین خواهند کرد (رحمانیان و حبیب زاده، ۱۳۹۲: ۶۶).

تحولات صنعتی و اقتصادی در پرتو اختراعات، اکتشافات و فناوری‌های ارتباطات و اطلاعات، خود از یک سو ارزش‌های جدیدی را به ارمغان آورده است و از سوی دیگر، جرم‌انگاری نقض این ارزش‌ها را توسط قانونگذار ضروری نموده است و بالاخره وسایل، فرصت‌ها، موضوع‌ها و زمینه‌های نو را برای بزهکاران فراهم ساخته است. «با متنوع شدن جرایم، راهبردها و پاسخ‌های حقوق کیفری به عنوان یک راهبرد جدید برای تولید و تضمین امنیت اجتماعی و سیاسی افتراقی سازی، لایه‌بندی یا طبقه بندی گردیده، دارای هندسه چند ضلعی شد و به راهبرد عمومی سیاست جنایی در مفهوم مضیق اضافه شد، در این زمینه می‌توان به جرایم رایانه‌ای اشاره کرد، که جرم‌انگاری‌ها و کیفرگذاری‌ها در قانون کیفری ماهوی و شکلی خاص تعریف شده است» (نجفی ابرندآبادی، ۱۳۹۲: ۵۴)، با توجه به اینکه جرایم رایانه‌ای به جای محیط حقیقی در محیط سایبری رخ می‌دهد، قرار گرفتن در این فضا محدود به اینترنت و کامپیوتر نیست و ابزارهای مورد استفاده در بانکداری نوین[۳] مانند کارت‌های

بانکی، دستگاه‌های خودپرداز و... نیز یک فضای سایبر است، بنابراین راهبردهای کیفری حاکم بر نظام بانکداری نوین از قواعد ماهوی حقوق کیفری سایبری تبعیت می‌کند.

بانکداری نوین یا اصطلاحاً بانکداری سبز،[۴] به گونه‌ای طراحی گردیده که قلم و کاغذ حذف شده است و خدمات بانکی مثل دریافت و انتقال پول یا گرفتن صورتحساب، توسط تجهیزات الکترونیکی کار گذاشته شده در خارج از شعب بانک، مانند دستگاه‌های خودپرداز ارائه یا زمینه استفاده از خدمات بانکی در بستر مخابرات یا اینترنت، مانند همراه بانک فراهم شده است. یعنی در عمل تحویلدارانی که عامل انسانی احراز هویت و تطابق امضا هستند وجود ندارند. «امضای مورد استفاده در این نوع از بانکداری، امضای الکترونیکی نامیده شده و چون دسترسی به خدمات ماشینی را فراهم می‌کند و دارای کارکرد حفاظتی است» (احمدی و خندان سویری، ۱۳۹۴: ۱۶۳)، از حالت نوشتاری به داده الکترونیکی یا کارت و تراشه تغییر ماهیت داده و شرایط صدور و استفاده از آن اختصاصی شده است، این نوع از امضاء، به دلیل اینکه مفهوم ایجاب و قبول و ارکان و آثار مسئولیت قراردادی را دگرگون کرده، مورد توجه پژوهشگران حقوق خصوصی واقع شده است، اما در حوزه حقوق کیفری فقط در برخی پژوهشهایی که راجع به جرایم رایانه‌ای و تجارت الکترونیکی وجود دارد، به شرایط صدور و نحوه استفاده از آن اشاره شده است. به نظر می‌رسد، علتی که باعث شده، به ابعاد جزایی امضای الکترونیکی پرداخته نشود، این است که ارزش‌های مورد حمایت از امضای الکترونیکی که مبنای فنی و تخصصی دارد، جرم انگاری مستقیم و مستقلی نسبت به آن صورت نگرفته است.

در حالی که امضای الکترونیکی یک سامانه امنیتی در سیستم بانکی است که از حریم خصوصی و ارزش اقتصادی در بانکداری الکترونیک حمایت می‌کند. بنابراین، این مقاله قصد دارد براساس دو نوع امضای الکترونیکی ساده و مطمئن (دیجیتال) که در بانکدای الکترونیکی و مجازی استفاده می‌شود، راهبردهای حقوق کیفری ماهوی در بانکداری نوین را که نوعی سیاست جنایی افتراقی- افتراقی در مقابل جرایم سایبری است، نسبت به جرایم علیه امضای الکترونیکی در دو قانون جرایم رایانه‌ای و تجارت الکترونیک شناسایی و تحلیل نماید و از این طریق برای پرسش‌های زیر پاسخی بیابد:

۱. چه جرایمی علیه امضای الکترونیکی ساده و دیجیتال رخ می‌دهد، روش ارتکاب آنها چگونه بوده و نقض کدامیک از قوانین کیفری ماهوی است؟

۲. کدام‌یک از نظام‌های تعیین مجازات پیامدگرا یا غیرپیامدگرا برای هریک از جرایم مناسب است؟

ضرورت و اهمیت تحقیق از این جهت است که، از یک طرف امضای الکترونیکی در سیستم بانکی شناسایی شده و براساس رفتارهای فیزیکی که برای هریک از جرایم کامپیوتری در قانون مربوطه پیش‌بینی شده است، و نقض ارزش‌های حاکم بر بانکداری نوین است، روش ارتکاب انحصاری شناسایی خواهد شد و از طرف دیگر به دلیل اینکه نوع مجازات‌ها معین و موازی است به‌طوری که قاضی را مخیر نموده است، حکم به حبس یا جزای نقدی را انتخاب کند، ولی نظامی برای تعیین مجازات وجود نداشته و تشخیص نوع و میزان مجازات را برای مقامات قضایی دشوار کرده است، امکان بررسی نظام تعیین مجازات و ارائه الگوی پیشنهادی را فراهم خواهد کرد.

بدین ترتیب مقاله حاضر با مبنا قرار دادن سامانه‌های الکترونیکی خدمات دهنده به مردم در بانکداری نوین و از طریق مطالعات کتابخانه‌ای و میدانی در واحد انفورماتیک سیستم بانکی و به دو روش توصیفی و تحلیلی، ضمن بررسی ایرادات قانونی، در دو قسمت، جرایم ارتکابی علیه هردو نوع امضای الکترونیکی را در نظام بانکی شناسایی و روش‌های ارتکابی هرکدام را بررسی کرده و در انتها نیز راهبردهای کیفری مربوط به تعیین مجازات موجود را نقد و پیشنهادهایی ارائه خواهد شد.

۱. راهبردهای کیفری در جرایم ارتکابی علیه امضای الکترونیکی ساده

نوع امضایی که در نظام بانکداری الکترونیکی استفاده شده است در درگاه‌های اینترنتی یا همراه بانک، روش گذرواژه، عبارت عبور یا شماره شناسایی شخصی است و در درگاه‌هایی مثل خودپرداز[۵] یا پایانه‌های فروشگاهی[۶] گذرواژه، به همراه کارت الکترونیکی است. «این امضاء طبق ماده (۷) قانون تجارت الکترونیکی مصوب ۱۳۸۲ از جایگاه قانونی امضای دستی برخوردار است.امضایی که بدین ترتیب به مشتریان بانکی اختصاص یافته است، صرفاً در حوزه داخلی هر بانک دارای اعتبار بوده و طبق ماده (۶) قانون تجارت الکترونیکی به عنوان امضای الکترونیکی ساده[۷] یا غیرمطمئن شناخته شده است» (شمس، ۱۳۹۲: ۱۴۸/۳). پس، شماره عبارت عبور اگر از طریق صفحه کلید دستگاه ثبت شد، یا همراه با کارت باشد، علامت[۸] منضم شده به داده پیام[۹] است که هویت امضاءکننده را تأیید کرده و همان امضای الکترونیکی نامیده شده در بند (ی) ماده (۲) قانون تجارت الکترونیکی است.[۱۰] بنابراین، به دلیل اینکه در بانکداری الکترونیکی، سامانه‌های بانکی به شیوه نصب گذرواژه یا گذرواژه به همراه کارت بانکی دارای تدابیر امنیتی است، جرم اصلی که علیه امضای الکترونیکی ساده ارتکاب می‌یابد دسترسی غیرمجاز است.

این جرم بسته به نوع درگاه بانکی، همراه با سایر بزه‌های رایانه‌ای است که مجموعاً جرایم ارتکابی علیه امضای الکترونیکی ساده را تشکیل خواهد داد، از آنجایی که در ماده ۵۵ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ تصریح شده مواد این قانون به عنوان فصل الحاقی قانون مجازات اسلامی (بخش تعزیرات) به شمار خواهد آمد، ماده ۷۲۹ قانون تعزیرات به عنوان عنصر قانونی جرم دسترسی غیرمجاز است.(۱۱) رفتار مادی این جرم شکستن تدابیر امنیتی داده‌ها یا سامانه‌های بانکی است و بر اساس نوع درگاه بانکی شیوه نقض تدابیر حفاظتی متفاوت خواهد بود. به همین دلیل، نوع درگاه بانکی، مبنای تقسیم بندی جرایم ارتکابی علیه امضای الکترونیکی ساده قرار خواهد گرفت.

۱-۱. دسترسی غیرمجاز از طریق درگاه‌های غیرحضوری

اگر کانال‌های ارتباط بانکی، اینترنت، موبایل یا تلفن ثابت باشد، تدابیر حفاظتی از نوع رمز عبور یا گذرواژه است.(۱۲) خدمات بانکی ارائه شده، رایانه‌ای محض است. بنابراین، «نفوذ یا رخنه‌گری به درگاه‌های غیرحضوری بانک از طریق دانش فنی امکان‌پذیراست. شیوه فنی رخنه به سامانه‌های رایانه‌ای هک نامیده شده است» (داوری دولت‌آبادی، ۱۳۹۳: ۲۵). هک به معنای نفوذ به یک سیستم رایانه‌ای است و هکر که در فارسی به رخنه‌گر و نفوذگر ترجمه شده، کسی است که با داشتن دانش برنامه‌نویسی و نرم‌افزار می‌تواند به یک سیستم رایانه ای نفوذ کند.(۱۳) 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(۱۴) نرم‌افزارهای ویژه‌ای اشاره دارد که در پیکره ویروس یا کرم رایانه‌ای و... به منظور ارتکاب سایر جرایم رایانه‌ای به کار رفته است.(۱۵)

بنابراین، سایر نرم‌افزارهایی که به عنوان 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 جرم‌انگاری گردیده(۱۶) و مستلزم حصول نتیجه خاصی نیست. به همین دلیل در زمره جرایم مطلق است(۱۷) و با این فرض نرم‌افزار مخرب اگر به عنوان ابزاری برای دسترسی غیرمجاز از طریق گذرواژه استفاده شود، چنانچه همراه با ارتکاب سایر جرایم رایانه‌ای باشد، از موارد تعدد جرم است که در زیر به این جرایم اشاره خواهد شد.

بزه دسترسی غیرمجاز جامع جرایم سایبری است، چون دروازه ورود برای ارتکاب سایر جرایم سایبری است، به همین دلیل سیاست کیفری توان‌گیری[1] 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: ۵۰۱)، غالباً نیز این افراد بلافاصله پس از آزادی مرتکب جرم خواهند شد،(۱۸) 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[2] استفاده شود، به عنوان نمونه رایانه ضبط شده یا استفاده از رایانه‌هایی که به اینترنت متصل هستند ممنوع شود (Smith, 2004: 64) یا خدمات بانکداری نوین ارائه نشود،(۱۹) 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 غیراز صاحب حساب بانک عملی نباشد (قناد، ۱۳۸۸: ۲۳۱).

۱-۱-۱. تغییر گذرواژه

گذرواژه، داده است، مجوز دسترسی به حساب‌های 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 ۶۷۵ 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،(۲۰) امکان دسترسی غیرمجاز هم فراهم گردیده است.این بدین معنی است که موضوع جرم ممانعت از دسترسی خود داده یا سامانه نیست، بلکه دسترسی به خدمات بانکی موضوع جرم است.به غیراز انتشار نرم‌افزار مخرب، یکی دیگر از روش‌های تغییر گذرواژه، مهندسی اجتماعی مبتنی بر کامپیوتر است.(۲۱) در این روش، مهندسی اجتماعی[3] (عالی‌پور، ۱۳۹۰: ۲۷۳) با استفاده از کامپیوتر است. صفحات جعلی یا فیشینگ(۲۲) یا رمزگیری، از این جمله است، باعث خواهد شد کلمه عبور یا گذرواژه کاربر افشاء شده و پس از آن نفوذگر قادر است به عنوان کاربر مجاز و از طریق درگاه‌های بانکی به‌طور

1. Incapacitation
2. Forfeiture and Restriction of use order
3. Social Engineering

غیرمجاز اقدام به تغییر گذرواژه نماید. شیوه باز کردن کیف رمزدار هم از جمله روش‌های غیرفنی دسترسی غیرمجاز است. در این روش رخنه‌گر مثل کسی که رمز کیف خود را فراموش کرده است، با سعی و خطا قصد دارد به شماره رمز دسترسی پیدا کند. بدین ترتیب، پس از اینکه دسترسی غیرمجاز صورت گرفت، امکان تغییر گذرواژه از طریق درگاه‌های بانکی به عنوان کاربر مجاز فراهم خواهد شد.(۲۳)

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 امکان‌پذیر است. مانند کسی که از طریق حساب کاربری بانکی خود واز 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، این نظریه مبتنی بر انسان اقتصادی یا بزهکار عقلانی است و فرد با تکیه بر تحلیل هزینه-فایده گزینه مجرمانه را انتخاب می‌کند (نعیمی، ۱۳۹۴: ۲۰۵)، به دلیل اینکه از نظر حداقل و حداکثر مجازات حبس، جرم ممانعت از دسترسی در ردیف حداقل این ضمانت اجرا قرار گرفته و مشابه سرقت رایانه‌ای یا دسترسی غیرمجاز است، بنابراین برای تشخیص اینکه کدام‌یک از مجازات‌های حبس یا جزای نقدی مناسب‌تر است، بهترین روش استفاده از گونه ارعاب نهایی است[۴]، در این گونه به نرخ تکرار جرم توجه شده است، 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 (Bagaric , 2011: 143).

۱-۱-۲. 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[۵] از قبل تعریف شده 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 جنس داده(۲۴) است. بدون گذرواژه کردن سامانه در قالب یکی از رفتارهای ماده ۷۳۶ قانون مجازات اسلامی قرار خواهد گرفت.

4. Marginal Deterrence
5. Date Center

در عمل تخریب گذرواژه دسترسی غیرمجاز نیست. چون، گذرواژه کارکرد امنیتی[۲۵] داشته و مجوز دسترسی به حساب‌های بانکی اشخاص در محل سرویس‌دهنده‌های مرکزی بانک را داده و از سایر داده‌های مالی و غیرمالی[۲۶] که حین فعالیت بانکی در سرویس‌دهنده‌های مرکزی بانک ذخیره شده است، حفاظت و حمایت می‌کند. مختل یا غیرقابل پردازش کردن گذرواژه نیز امکان‌پذیر نیست، چون به هرحال، گذرواژه‌ای 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[۲۷]. بنابراین نوع رفتاری که نسبت به گذرواژه رخ خواهد داد، حذف یا پاک کردن[۶] است، چون با پاک شدن گذرواژه، سرویس‌دهنده‌های مرکزی بانک در عمل فاقد تدابیر حفاظتی شده و با این روش امکان دسترسی غیرمجاز فراهم خواهد شد. 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[۲۸].

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 به حساب بانکی توسط هرشخصی فراهم خواهد شد، از این لحاظ ضمانت اجرای پیش‌بینی شده از نظر تحلیل اقتصادی فعل‌محور[۷] بوده و زیان‌محور[۸] 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: ۱۴۷)، نوع ضمانت اجرا نیز ارعاب جزئی[۹] 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 (Mieth & LU, 2005:21)، در حقیقت در شرایط مساوی مثل حالت قبل که 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، فرهادی، آلاشتی و ساداتی، ۱۳۹۵: ۶۵).

6. Delete
7. Act- Based
8. Harm- Based
9. Partial Deterrence

۱-۱-۳. شنود گذرواژه

دستگاه کامپیوتر شخصی یا گوشی تلفن ثابت یا همراه، مبدأ ارائه خدمات غیرحضوری بانکداری الکترونیکی است، پیام‌های ارسالی مشتریان شبکه بانکی توسط این تجهیزات به سرویس‌دهنده‌های مرکزی هر بانک ارسال خواهد شد. اگر ارسال پیام در مبدأ، از طریق تلفن ثابت باشد، بستر انتقال پیام واسط‌های سیم‌دار شبکه مخابرات است و چنانچه از تلفن همراه استفاده شود، واسط‌های بی‌سیم یا همان امواج الکترومغناطیسی وظیفه انتقال پیام را بر عهده دارند و در مورد اینترنت از هردو نوع واسط استفاده شده است.

اولین پیامی که توسط کاربران بانکی از طریق واسط‌های انتقال داده ارسال می‌شود، شماره گذارواژه یا شماره رمز حساب است. پس از اینکه تطبیق صحت رمز توسط سرویس‌دهنده‌های مرکزی بانک انجام شد، مجوز دسترسی به حساب بانکی اعطا خواهد شد وچون، شماره رمز محرمانه بوده و حریم خصوصی اشخاص است، صرفاً سامانه‌های مرکزی هر بانکی که در سامانه‌های شتاب (شبکه تبادل اطلاعات بانکی) یا شاپرک (شبکه الکترونیکی پرداخت کارتی) عضویت داشته باشد، صلاحیت دریافت شماره رمز را دارد. «بدین ترتیب، تراکنش ارسال شماره گذرواژه، به عنوان محتوای در حال انتقال ارتباطات غیرعمومی[۲۹] به حساب خواهد آمد، اگر با هر ابراز یا وسیله‌ای، در طول مسیر انتقال، گذرواژه شنود گردد، جرم موضوع ماده ۷۳۰ قانون مجازات اسلامی محقق خواهد شد» (الهی‌منش و سدره‌نشین، ۱۳۹۱: ۲۴).

در نتیجه در مبدأ یا مقصد، جرم شنود امکان‌پذیر نیست، چون در مبدأ که امکان ذخیره گذرواژه نیست و گذرواژه‌ای که در مقصد، ذخیره شده است، در حال انتقال و آمد و شد نیست و به همین دلیل اطلاع از گذرواژه در مقصد، دسترسی غیرمجاز است و اگر از نرم‌افزار مخرب یا ویروس‌ها و کرم‌های رایانه‌ای رخنه‌گر در طول مسیر انتقال گذرواژه استفاده شده و بدین شکل از کاراکترهای گذرواژه به‌طور غیرمجاز اطلاع حاصل شود. نفوذگر خواهد توانست در مسیر انتقال پیام توسط کاربر مجاز انحراف ایجاد نموده و اقدام به ارسال پیام بجای صاحب حساب یا کاربر مجاز به سامانه‌های بانکی و دسترسی غیرمجاز نماید.بدین ترتیب سه جرم انتشار نرم‌افزار مخرب، شنود و دسترسی غیرمجاز پدید آمده است.[۳۰] از جمله روش‌های شنود از طریق انتشار نرم‌افزار رخنه‌گر فارمینگ است. در فارمینگ کاربر با بازکردن ایمیل، کلید خوان را روی سیستم خود نصب کرده است، کلید خوان برنامه نرم‌افزاری است، کلیدهای زده شده توسط کاربر را ثبت کرده و با این روش نفوذگر، نام کاربری و رمز عبور ثبت شده اطلاع حاصل خواهد کرد. در این روش، دسترسی غیرمجاز، جرم پسینی شنود است. چون، رخنه‌گر بعد از اطلاع از

گذرواژه، در عملیاتی مجزا از طریق سامانه بانک به عنوان کاربر مجاز وارد شده و مرتکب جرم دسترسی غیرمجاز خواهد شد.

با توجه به مهارت فنی بالایی که مرتکب جرم شنود غیرمجاز دارد، راهبرد کیفری استفاده از ضمانت اجراهای ترمیمی و کیفرهای جامعه‌مدار است، زیرا از یک‌سو از دانش و تخصص محکوم علیه در فعالیت‌های مولد و مثبت استفاده خواهد شد و از سوی دیگر نتیجه مورد نظر این رهیافت، عبارت از ترمیم رابطه میان بزهکاران، بزه‌دیدگان و اجتماع است (بروکس، ۱۳۹۵: ۱۱۴)، این اندیشه به اصلاح بزهکاران و در بستر جامعه علاوه بر شرمساری بازپذیرکننده‌ای که جان برایث ویت مطرح کرده است، توجه نموده است (فرایبرگ، ۱۳۹۱: ۱۸۰). به عنوان مثال در سال ۲۰۰۳، در دعوای ایالات متحده آمریکا علیه تولیدکننده ویروس ملیسا (دیوید اسمیت) استفاده از دانش و تخصص متهم، منجر به دستگیری جان دویت سازنده ویروس آناکورنیکووا و سیمون والور سازنده ویروس گووکار شد.[۳۱]

۱-۲. 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 بوده[۳۲] و درج رمز اول کارت به منزله تأکید تراکنش و قبول شرایط درخواست به‌عمل آمده است. بنابراین امضای الکترونیکی از طریق روش حضوری دو ماهیت دارد.ماهیت فیزیکی به عنوان جسم کارت و ماهیت مجازی، رمزی است که دارنده کارت از آن آگاه است. قراردادن 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،[۳۳] که به ترتیب مورد بررسی قرار خواهد گرفت (آلبنیز، ۱۳۹۳: ۱۶۶).

۱-۲-۱. 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[۱۰] 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[۳۴] است.

روش‌های غیرفنی دسترسی به گذرواژه به شیوه انواع مهندسی اجتماعی مبتنی بر انسان است، در این روش از بی‌احتیاطی یا اطمینان بیش از حد انسان‌ها برای جمع‌آوری اطلاعات

10. Electronic Emanation

حساس استفاده شده است. نصب و استتار دوربین کوچک بالای دستگاه خودپرداز یا ایستادن کنار کاربر به منظور دیدن و خواندن کلمه عبور، به‌دست 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 وارد کردن رمز، از جمله این روش‌ها است،[۳۵] همه موارد در قوانین موجود جرم‌انگاری نشده است.[۳۶] درصورتی که طبق نظریه کنترل اجتماعی نای تهدید به مجازات باعث هم‌نوایی فرد با جامعه خواهد شد (نجفی ابرندآبادی، ۱۳۸۴: ۹۱).

در مقابل، طبق بند (ب) ماده ۷۵۳ قانون مجازات اسلامی، فروش، انتشار یا در دسترس قراردادن گذرواژه، بدون رضایت صاحب آن جرم و نوعی معاونت برای ارتکاب جرم دسترسی غیرمجاز است[۳۷] (محمد نسل، ۱۳۹۲: ۱۸۴).

۱-۲-۲. جعل و استفاده از کارت[۳۸]

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[۳۹] 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، به عنوان نشانه استفاده شده، قابل سنجش نبوده و نمی‌توان اعمال مجاز ریاضی روی آنها انجام داد. این کارت از نوع کارت قابل پردازش است.[۴۰] موقعی که کارت در دستگاه قرار می‌گیرد، اطلاعات کارت برای سیستم‌های متمرکز بانک ارسال خواهد شد، اگر صحت داشته باشد، مشتری خواهد توانست به صورت لحظه‌ای یا برخط،[۱۱] از کارت استفاده کند.

بنابراین برای اینکه دسترسی غیرمجاز از طریق درگاه‌های حضوری امکان‌پذیر گردد، علاوه بر داشتن رمز عبور، مستلزم در اختیار داشتن فیزیک کارت هم است. به این منظور، بزهکار باید از کارت اصلی خود کاربر استفاده کند،[۴۱] یا علائم کارت را روی کارت خالی دیگری کپی کند.[۴۲] کپی کردن کارت با هیچ کدام 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 صادر شده دارای تدابیر حفاظتی نیست،[۴۳] درنتیجه ارتکاب این عمل سرقت رایانه‌ای است.

11. Online

روش معمول برای سرقت اطلاعات کارت بانکی، استفاده از دستگاه اسکیمر[۱۲] 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 اطلاعات امنیتی کارت خود خواهد شد، این روش جرم سرقت رایانه‌ای را در زمره جرایم نیرنگ‌آمیز و متقلبانه قرار داده است، بنابراین راهبرد کیفری برای سرقت رایانه‌ای در بانکداری نوین، اصلاح و بازپروری[۱۳] 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 امکان‌پذیر باشد، به عنوان نمونه یکی 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،[۱۴] سیستم‌های رایانه‌ای برملا شده و در سطح شبکه گسترش یابد، زندانی شدن بسیار ناگوار است، این تلخ‌ترین تجربه زندگی من بود».(۴۴)

نوع دوم کارت‌های بانکی، کارت هوشمند[۱۵] است. در این کارت به جای نوار مغناطیسی، ریزپردازنده تعبیه شده است و پول الکترونیکی که نوعی داده مالی است، مستقلاً داخل ریز پردازنده ذخیره شده است، به همین دلیل نام دیگر آن کیف پول الکترونیکی[۱۶] است. علی‌رغم اینکه تراشه‌ها در بیشتر مواقع ماهیت فیزیکی به شکل کارت ندارند ولی این 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، به صورت برون‌خط،[۱۷] با درگاه بانکی ارتباط برقرار خواهد کرد، اگر ریزپردازنده کارت، از معتبر بودن دسترسی به کارت مطمئن نشود به کارت‌خوان اجازه دسترسی برای برداشت یا انتقال وجه نخواهد داد. کارت‌های هوشمند از نظر فنی یک سیستم رایانه‌ای (سامانه) هستند.(۴۵) اگر، حافظه کارت دستکاری و تغییر یابد جرم جعل کارت تحقق یافته است،(۴۶) حتی اگر دستکاری توسط صاحب کارت باشد.(۴۷) 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.(۴۸) به

12. Skimmer
13. Rehabilitation
14. Bug
15. smart card
16. electronic purse
17. offline

همین ترتیب، اگر دارنده کارت مانع پردازش داده‌ها شود به‌طوری که به‌وسیله درگاه‌های بانکی بتواند مبلغ بدهی خود را تسویه نماید ولی از موجودی حافظه کارت کم نشود، چون از طریق دستکاری داده‌ها[۴۹] 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: ۱۸۰).

در جرایم ذکر شده فرقی ندارد، نسبت به کارت معتبر انجام شود یا کارتی که غیرفعال شده و شماره آن باطل شده است[۵۰]. به‌هرحال، برای بانک ضرر معنوی دارد[۵۱] و باعث خواهد شد به اعتبار و شهرت تجاری بانک لطمه وارد شده و مشتریانش را از دست بدهد.[۵۲] آخرین مرحله دسترسی غیرمجاز، استفاده از کارت جعلی است و اگر کارت بانکی توسط یک نفر جعل شود و به‌وسیله کارت جعلی بتواند در درگاه‌های حضوری عملیات بانکی انجام دهد، مشمول تعدد مادی خواهد شد.

راهبرد کیفری در جرایمی که به‌وسیله کارت هوشمند ارتکاب یابد، بیان‌گرایی یا تقبیح عمومی[۱۸] است. از نظر ایده بیان‌گرای، مجازات صرفاً چیزی نیست که بر مجرمان واقع می‌شود، بلکه 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 این رو، بیان‌گرایان به دنبال محکومیت رفتارها هستند، نه افرادی که آن رفتارها را مرتکب شده‌اند، یعنی مجازات، بیان‌گر تقبیح جرایم است، نه اشخاص (بروکس، ۱۳۹۵: ۱۶۷).

ارتباط بین نظریه پی‌آمدگرایی تقبیح عمومی با این جرایم، تصور مالکانه‌ای است که مردم از کارت هوشمند دارند، به نظر می‌رسد، چون مردم خود را مالک و دارنده کارت می‌شناسند، ادعا خواهند کرد سوءنیت مجرمانه نداشته یا ارتکاب عمل برای ارضای حس کنجکاوی یا خودنمایی در میان همسالان بوده و محق به دستکاری بوده‌اند، بدین ترتیب از مجرمانه و غیرقانونی بودن عمل خود آگاهی نداشته‌اند،[۵۳] در نتیجه پیشگیری از تکرار جرم درصورتی امکان‌پذیر است که انتشار گسترده و اطلاع رسانی عمومی در رابطه با احکام صادره در این پرونده‌ها فراهم شود، زیرا در چنین شرایطی افزایش شدت مجازات‌ها با هدف دستیابی به ارعاب نمی‌تواند کارکرد مؤثری داشته باشد.

18. Denunciation

۲. راهبردهای کیفری در جرایم ارتکابی علیه امضای الکترونیکی مطمئن (دیجیتال)

ماده ۱۰ قانون تجارت الکترونیکی، امضای دیجیتال را نسبت به امضاءکننده منحصربه‌فرد شناخته و مواد ۱۴ و ۱۵ همین قانون امضای دیجیتال را قابل استناد در مراجع قضایی دانسته است، به‌طوری‌که، ادعای انکار و تردید نسبت به آن را نپذیرفته است. امضای دیجیتال در بستر بانکداری مجازی[۵۴] از طریق سامانه نماد[۵۵] (نظام مدیریت امنیت داده‌ها) اعمال و از نظر ساختاری همان کارت، توکن یا دستگاه سخت‌افزار و رمزنگاری است که حاوی نرم‌افزاری از جنس داده الکترونیکی به نام گواهی الکترونیکی است.[۵۶] از لحاظ فنی، امضای الکترونیکی از طریق رمزنگاری نامتقارن و به‌وسیله کلیدهای خصوصی و عمومی مرتبط با گواهی الکترونیکی تولید می‌گردد (Stephen, 2007: 86). این زوج کلید در زیرساخت کلید عمومی کشور برای رمزنگاری پیام توسط فرستنده و رمزگشایی توسط گیرنده استفاده شده است.[۵۷] بدین ترتیب، به محض اینکه مشتری بانک، کد کاربری و گذرواژه اختصاص داده شده را در سامانه نماد وارد نماید، این ابزار- که همزمان به رایانه کاربر اتصال دارد ـ به‌طور خودکار هویت کاربر را تأیید کرده و داده‌پیام‌های ارسالی را رمزنگاری و برای مخاطب[۵۸] که همان بانک است ارسال خواهد کرد.

بنابراین، به دلیل اینکه در بانکداری مجازی، تأمین امنیت کاربران با شیوه رمزنگاری، به‌وسیله توکن یا کارت هوشمند دارای تدابیر تأمینی است[۵۹] و بانک مرکزی، برای ثبت نام، صدور، استفاده و نگهداری گواهی‌های الکترونیکی ضوابط خاصی پیش‌بینی کرده است.[۶۰] جرایم ارتکابی علیه امضای دیجیتال در دو قسمت بررسی خواهد شد: قسمت اول، شامل جرایم علیه دستگاه رمزنگاری تولید امضای دیجیتال و قسمت دوم، جرایم مراکز صدور و دفاتر ثبت نام امضای دیجیتال است.

۲-۱. جرایم علیه دستگاه رمزنگاری تولید امضای دیجیتال

دسترسی غیرمجاز به سامانه نماد دو شرط دارد. اول، دانستن گذرواژه ورود به سامانه و دوم، در اختیار داشتن توکن یا کارت هوشمند ایجاد امضای دیجیتال است.

نحوه تحصیل رمز عبور یا گذرواژه، همان مواردی است که در قسمت امضای الکترونیکی ساده گفته شد و در اکثر موارد جرم نیست. ولی وارد کردن غیرمجاز داده‌های رمز عبور به سامانه، جرم دسترسی غیرمجاز است. استفاده غیرمجاز از دستگاه رمزنگاری هم دو حالت دارد: حالت اول استفاده غیرمجاز از دستگاه رمزنگاری بدون رضایت صاحب آن است. مانند، مواردی که دستگاه سرقت یا مفقود شده است. اگر، نفوذگر بتواند تدابیر تأمینی که برای فعال‌سازی

دستگاه پیش‌بینی شده است را نقض کند و گذرواژه عددی یا بیومتریک را فعال نماید، جرم رخ داده شده، دسترسی غیرمجاز است و اگر فعال‌سازی دستگاه موکول به ثبت گذرواژه یا اثر انگشت نباشد، جرمی رخ نداده است. حالت دوم، کپی داده‌های موجود در دستگاه رمزنگاری و ذخیره کردن آن در دستگاه سخت‌افزاری دیگری است. چون داده‌های دستگاه یا کارت، با رمزنگاری دارای تدابیر تأمینی است. ابتدا باید تدابیر تأمینی داده‌ها نقض شود که دسترسی غیرمجاز است و سپس کپی شود.(۶۱)

همان‌طور که در قسمت جعل کارت توضیح داده شد، رفتارهای تغییر، وارد کردن و ایجاد داده‌ها که در بند (ب) ماده ۷۳۴ قانون مجازات اسلامی آمده است با کپی یا روگرفت از داده تطابق ندارد. ماده ۶۸ قانون تجارت الکترونیکی هم به‌موجب ماده ۷۸۳ قانون مجازات اسلامی نسخ شده است (مرکز پژوهش‌های مجلس، ۱۳۸۷: ۱۸-۱۷). زیرا، «رفتارهای ورود و تغییر، در ماده ۷۳۴ قانون مجازات اسلامی به عنوان جعل پیش‌بینی شده است و رفتارهای محو و توقف هم بر ضد تمامیت داده و سامانه‌اند و با جعل نزدیکی ندارند» (قناد، ۱۳۹۰: ۷۲).

از طرف دیگر، «مصادیقی که برای استفاده کاربردی سیستم‌های رمزنگاری تولید امضاء به‌طور خاص آورده شده است،(۶۲) در حالت اول، استفاده از کلید اختصاصی بدون مجوز صادرکننده، به عنوان دسترسی غیرمجاز است و سه حالت بعدی (تولید امضای فاقد سابقه ثبت از فهرست دفاتر اسناد الکترونیکی، عدم انطباق وسایل با نام دارنده در فهرست دفاتر اسناد الکترونیکی و اخذ گواهی مجعول)(۶۳) ایجاد داده و همان جعل است» (جاویدنیا، ۱۳۸۷: ۲۹۴). بر فرض هم که قائل به عدم نسخ باشیم، موضوع جرم، داده‌های مالی و اثباتی است که داده‌های گواهی امضا، مالی نیست. اگر کپی یا روگرفت را با رفتار تکثیر مترادف بگیریم که مشمول مواد ۶۲ و ۷۴ قانون تجارت الکترونیکی گردد، «گواهی الکترونیکی، باید به عنوان یکی از مالکیت‌های فکری شناخته شود که در بستر مبادلات الکترونیکی مورد حمایت قرار گرفته است.(۶۴) چنانچه، گواهی الکترونیکی با موارد مورد حمایت در ماده ۶۲، قانون تجارت الکترونیکی مطابقت داده شود از جنس پایگاه داده است، چون مجموعه‌ای از داده‌های ذخیره شده، یکپارچه و به هم مرتبط است که تحت مدیریت یک سیستم کنترل متمرکز قرار دارد و توسط یک یا چند کاربر به‌صورت اشتراکی از یک سیستم کاربردی مورد استفاده قرار می‌گیرد و چهار عنصر سخت‌افزار، نرم‌افزار، کاربر و داده در آن وجود دارد» (روحانی رانکوهی، ۱۳۹۲: ۱۴-۱۶).

در عمل هم «گواهی الکترونیکی یک داده کامپیوتری است که برای مرکز گواهی امضاء مبین تأیید یا رد هویت ادعا کننده است و بین ابعاد حقوقی بالقوه و بالفعل با اشخاص موجود

ارتباط برقرار کرده است. به همین دلیل، با تعریف نرم‌افزار که در ماده (۲) آیین نامه اجرایی قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای آمده است، تطابق ندارد و مشمول حمایت کیفری مندرج در ماده ۱۳ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹ نیست» (صالحی و غلامعلی پور، ۱۳۸۹: ۱۶۱).

از طرف دیگر، در اسنادی که بانک مرکزی منتشر کرده است، برای گواهی الکترونیکی حق مالکیت معنوی پیش‌بینی گردیده و این حق متعلق به مرکز صدور گواهی است،[۶۵] ولی نقض حقوق انحصاری آن جرم‌انگاری نشده است. همچنین، پایگاه داده، اختراع-طرح صنعتی و علامت تجاری هم نیست. به همین دلیل، ماده ۶۱ قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری به عنوان ضمانت اجرای کیفری نقض آن نیست. برای اینکه این خلأ قانونی رفع گردد، در حال حاضر بر اساس ماده ۶ برنامه جامع توسعه تجارت الکترونیکی مصوب ۱۳۸۴ هیأت وزیران که وزارت ارتباطات و فناوری اطلاعات را به تدوین قانون جامع حمایت از داده الزام نموده است، همچنین لایحه قانون حمایت از سازندگان پایگاه‌های داده که توسط شورای عالی انفورماتیک تهیه گردیده است، ماده ۲ این لایحه برنامه‌ها و نرم‌افزارهای رایانه‌ای که برای ساخت یا عملیات پایگاه داده مورد استفاده قرار می‌گیرد را مشمول حمایتهای این قانون نمی‌داند. ماده ۴۴ این لایحه، نشر، پخش و عرضه بدون اجازه حقوق انحصاری سازندگان پایگاه داده را مشمول مجازات حبس از ۳ تا ۶ ماه قرار داده است[۶۶].

در نتیجه، اگر کپی داده را با سایر جرایم رایانه‌ای تطابق دهیم، با جرم سرقت رایانه‌ای موضوع ماده ۷۴۱ قانون مجازات اسلامی همخوانی دارد، چون دستگاه رمزنگاری به‌طور قانونی محل جایگیری داده‌ها است و روگرفت از آن در فضای سایبر انجام شده است. البته، چون عملیات رمزنگاری در امضای دیجیتال ماهیت جداگانه از رمز دارد، اگر کسی قصد داشته باشد تا به محتوای کلید خصوصی دسترسی یافته و با کشف رمز اقدام به کپی داده‌ها و ساخت دستگاه رمزنگاری نماید، چون مستلزم دسترسی به داده‌های در حال انتقال به سامانه‌های رایانه‌ای است مرتکب جرم شنود غیرمجاز ماده ۷۳۰ قانون مجازات اسلامی گردیده است.

۲-۲. جرایم مراکز صدور و دفاتر ثبت نام امضای دیجیتال

مرکز گواهی بانک مرکزی، طبق تبصره ۲ ماده ۴ آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی، اجازه دارد تا به‌طور مستقل اقدام به صدور گواهی الکترونیکی نماید. صدور گواهی الکترونیکی در بستر بانکداری، نیازمند روش‌های عملیاتی، حقوقی و فنی خاص خود است. به همین دلیل، بانک مرکزی موظف است، ضوابط اختصاصی صدور گواهی الکترونیکی در نظام بانکی را تدوین کرده و برای اطلاع عموم، در تارگاه مرکز گواهی بانک مرکزی منتشر نماید،

چون بستر بانکداری مجازی به بانک خاصی اختصاص نداشته و کل شبکه بانکی را پوشش داده، بانک مرکزی باید امکان دسترسی به وضعیت گواهی‌ها، از جمله ابطال گواهی را به صورت الکترونیکی برای طرف‌های اعتمادکننده (پذیرنده) فراهم کند. این اطلاعات که در محلی به نام مخزن گواهی‌ها نگهداری می‌شود، عمومی است و متضمن حق و تکلیف برای مردم است و هر شخص ایرانی حق دسترسی به این اطلاعات را دارد. ممانعت از دسترسی به این اطلاعات توسط مؤسسات عمومی، طبق بند الف ماده ۲۲ قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷ جرم است و مرتکب محکوم به پرداخت جزای نقدی خواهد شد.

از طرف دیگر، دفاتر خدمات صدور گواهی الکترونیکی شعب بانک‌هایی هستند که از مراکز گواهی بانک مرکزی مجوز دارند و بر اساس تبصره ۲ ماده ۱۲ آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی، دفاتر پیشخوان خدمات مرکز گواهی نامیده شده‌اند. این دفاتر، پس از اینکه هویت اشخاص متقاضی را با ارائه اسناد و مدارک مثبته احراز می‌نمایند،[۶۷] توکن یا کارت فیزیکی که از طرف مرکز گواهی اختصاص داده شده است را به متقاضیان تحویل خواهند داد.

ماده ۵۸ قانون تجارت الکترونیکی، اشاره دارد که اگر دفاتر خدمات صدور گواهی الکترونیکی، اطلاعات صاحب گواهی را که حاوی ریشه‌های قومی، نژادی، عقیدتی، مذهبی، خصوصیات اخلاقی، وضعیت جسمی و روانی، جنسی اشخاص است را در بستر مبادلات الکترونیکی و بدون رضایت صاحب گواهی، ذخیره، پردازش و یا توزیع نمایند؛ در حالت عمدی مشمول مقررات کیفری ماده ۷۲ قانون تجارت الکترونیکی قرار گرفته و اگر غیرعمدی باشد ماده ۷۳ این قانون ضمانت اجرای آن است.[۶۸] بنابراین، اگر اطلاعات مزبور و سایر اطلاعات شخصی صاحبان امضا، مثل شماره ملی یا کدپستی، شغل، وضعیت مالی و... که نزد دفاتر دارند و یا داده‌های مربوط به امضا که در فرایند ایجاد امضای الکترونیکی مطمئن به کار رفته است تا از شبیه‌سازی گواهی‌ها جلوگیری شود،[۶۹] به‌طورکلی «کلیه اطلاعاتی که به صورت محلی در تجهیزات مرکز صدور گواهی و نه در مخزن ذخیره شده‌اند در غیر از بستر مبادلات الکترونیکی و غیر از موارد قانونی افشا گردد، به دلیل اینکه به مناسبت شغل و وظیفه تحصیل شده است مشمول ضمانت اجرای کیفری ماده ۶۸۴ قانون مجازات اسلامی (تعزیرات) خواهد شد»[۷۰] (قماشی، ۱۳۸۵: ۳).

راهبرد کیفری نسبت به جرایمی که علیه گردش آزاد اطلاعات و حریم خصوصی رخ می‌دهد به دلیل اینکه جنبه حقوق بشری دارند، سزادهی در مفهوم نوین است. از نگاه سزاگرایان سنتی کانون توجه منطق مجازات، تنها جرم ارتکابی است. بدین ترتیب، مجازاتِ برابر با جرم، پاسخ طبیعی در برابر ارتکاب رفتار خلاف اخلاق و عدالت است که نظم مختل

شده اجتماع را دوباره احیا کرده و تعادل را در جامعه برقرار خواهد ساخت (پرادل، ۱۳۷۳: ۱۹). اما در شکل نوین سزاگرایی، اندیشه برابری جرم و مجازات تبدیل به تناسب کیفر با جرم ارتکابی شده است (جوان جعفری و ساداتی، ۱۳۹۲: ۱۳۴). منظور از تناسب میان بزه و کیفر این است که مجازات و محرومیتی که برای بزهکار تعیین خواهد شد، متناسب با لطمه‌ای باشد که در نتیجه عمل بزهکارانه بر جامعه وارد شده است، این هزینه‌ها شامل هزینه‌های آتی و گذشته است (یزدیان جعفری، ۱۳۸۷: ۱۲۳). هزینه‌های گذشته همان هزینه‌هایی است که افراد و شرکت‌ها بابت تدابیر احتیاطی در قبال جرم صرف می‌کنند، به عبارت دیگر هزینه‌های مربوط به پیشگیری از جرم و خدمات بیمه‌ای است، هزینه‌های آتی همان هزینه‌های مربوط به واکنش جرم است، شامل هزینه‌های نظام عدالت کیفری (دادگاه-پلیس) است که برای واکنش به جرم صرف می‌شود و هزینه‌های ناشی از ارتکاب جرم که به بزه‌دیدگان تحمیل می‌شود، هزینه فرصت از دست رفته که مربوط به صرف وقت و پیگیری پرونده توسط بزه‌دیده از طریق مراجع قضایی است را هم شامل خواهد شد (بابایی و انصاری، ۱۳۹۱: ۸۴). با توجه به اینکه زیان حاصل از این جرایم مادی نبوده و معنوی است، در کنار ضمانت اجراهای انضباطی و اداری که برای کارکنان بانک‌ها در نظر گرفته خواهد شد، جبران زیان معنوی به طریقی که در تبصره (۱) ماده (۱۴) قانون آیین دادرسی کیفری مصوب ۱۳۹۲ پیش‌بینی شده است، یکی از الزامات رعایت تناسب خواهد بود.

فرجام

بانکداری سنتی جای خود را به بانکداری الکترونیکی داده است، ولی هنوز هم بسیاری از خدمات بانکی به صورت حضوری ارائه می‌شود و در ادامه تحولات، بانکداری الکترونیکی هم جای خود را به بانکداری مجازی خواهد داد. زیرساخت اساسی بانک‌های مجازی امضای دیجیتال است که باعث شده است مردم بتوانند از طریق اینترنت و بدون هیچ واسطه‌ای خدمات بانکی را به صورت کاملاً غیرحضوری دریافت نمایند. شرط استفاده از خدمات بانکداری مجازی، اخذ گواهی الکترونیکی یا امضای دیجیتال از دفاتر مربوطه است. از این رهگذر جرایم و نظام مجازات‌های مربوط به جرایم در بانکداری نوین که مرتبط با امضای الکترونیکی است، تحلیل و بررسی شد.

قانون جرایم رایانه‌ای عام است و کلیه بسترهای مبادلات الکترونیکی را در بر می‌گیرد. پس، از حوزه‌های مختلفی که به صورت الکترونیکی خدماتی مثل بورس، آموزش، انتخابات، بانکداری و... را ارائه می‌نمایند، حمایت کیفری به‌عمل نیامده است. به همین دلیل، برخی ابهامات و کاستی‌ها وجود دارد که در حوزه کیفری بانکداری الکترونیکی، به خصوص در رابطه با امضای

دیجیتال قابل تأمل است. مهم‌ترین ابهام، عدم تعریف «غیرمجاز» در بانکداری الکترونیکی و مجازی است و مشخص نشده اگر درگاه بانکی در بانک یا مؤسسه بدون مجوز از بانک مرکزی مستقر باشد و یا حساب بانکی وجود دارد که با اسناد جعلی افتتاح شده یا استفاده برای مقاصد پول‌شویی دارد، مشمول حمایت‌های کیفری قانون جرایم رایانه‌ای قرار خواهد گرفت یا خیر. در حالی که طبق تبصره ماده ۷ قانون صدور چک، چک‌های صادره ناشی از معاملات نامشروع و ربوی مورد حمایت کیفری نیست.

در مورد دسترسی غیرمجاز، به عنوان اصلی‌ترین جرمی که در قلمرو جرایم علیه امضای الکترونیکی وجود دارد، ابهاماتی وجود دارد. توضیح داده شد که اگر کسی از گذرواژه کارت یا حساب دیگری به طور غیرمجاز مطلع شود. شماره گذرواژه را به دستگاه خودپرداز یا درگاه‌های اینترنتی وارد کرده و موفق به انجام تراکنش شود، جرم دسترسی غیرمجاز تحقق یافته است، و تناقضی که وجود دارد، این است که چون گذرواژه از جنس داده است، وارد کردن غیرمجاز داده، جرم جعل رایانه‌ای است[۷۱] و هر دو جرم جعل و دسترسی غیرمجاز از طریق وارد کردن غیرمجاز داده انجام خواهد شد. یعنی دارای روش ارتکاب مشابهی هستند، که باعث اشتباه در تعیین عنوان مجرمانه خواهد شد.[۷۲] برای رفع ابهام، لازم است ابتدا مفهوم «داده» مشخص شود، چون وارد کردن داده، معادل الصاق کردن نوشته در جعل سنتی است و با تغییر داده تفاوتی ندارد، بدین ترتیب مرز بین جرم دسترسی غیرمجاز و جعل رایانه‌ای قابل تشخیص خواهد گردید.

در قانون جرایم رایانه‌ای مجازات جرم دسترسی غیرمجاز که دروازه سایر جرایم رایانه‌ای نظیر سرقت، کلاهبردای، تخریب، جعل و... است، با جرم سرقت رایانه‌ای و فروش گذرواژه یکی است،[۷۳] ولی مجازات آن از سایر جرایم رایانه‌ای مثل کلاهبرداری، جعل و تخریب بسیار کمتر است[۷۴] و از جرم دسترسی بدون مجوز به پهنای باند بین‌المللی (ماده ۷۲۵) هم به مراتب کمتر است. در این مدل کیفرگذاری، اصل تناسب جرم و مجازات رعایت نشده است. هر چند، محرومیت از خدمات بانکداری الکترونیکی برای تکرارکنندگان جرایم رایانه‌ای در ماده ۷۵۵ قانون مجازات اسلامی پیش‌بینی شده است و از مدل ریسک‌مدار کنترل جرم تبعیت کرده است، ولی چون مشروط به تکرار جرم شده، بازدارنده نیست، چنانچه از روش ماده ۷۲۸ قانون مجازات اسلامی استفاده و قطع موقت خدمات عمومی مثل محرومیت از خدمات بانکداری الکترونیکی به عنوان مجازات تکمیلی یا تبدیلی پیش‌بینی و مشروط به تکرار جرم نمی‌گردید. چون، مرتکبین جرایم بانکداری الکترونیکی دارای تخصص بوده و اهداف مالی دارند، از کارایی بیشتری برخوردار بود.

«گذرواژه یک جزء اطلاعاتی است» (هیئت مؤلفان و ویراستاران انتشارات مایکروسافت، ۱۳۷۹: ۱۶۷). سرقت آن به تنهایی جرم نیست، چون فقط عین مال قابل دزدیده شدن است (میرمحمد صادقی، ۱۳۹۲: ۲۰۹). و همان طوری‌که سرقت گذرواژه به عنوان یک داده جرم نیست،(۷۵) در رابطه با نحوه تحصیل، جمع‌آوری، نگهداری، پردازش و در دسترس قرار دادن داده‌ها قانون خاصی هم وجود ندارد، این در حالی است که در بسیاری از کشورها مثل انگلستان، آلمان و فرانسه داده‌های شخصی مورد حمایت کیفری قرار گرفته‌اند.(۷۶) در ایران، با توجه به الزام مندرج در بند ه ماده ۱۳۰ قانون برنامه چهارم توسعه ۱۳۸۳و ماده ۶ برنامه جامع توسعه تجارت الکترونیکی ۱۳۸۴ هیأت وزیران، تصویب قوانین حمایت از حریم خصوصی و حمایت از داده‌ها ضروری است تا از حق مالکیت معنوی یا سرقت داده‌ها حمایت کیفری به عمل آید.

کیفرهایی که برای جرایم ارتکابی علیه امضای الکترونیکی در بانکداری نوین پیش‌بینی شده است، جملگی در زمره جرایم درجه شش قرار گرفته است و دارای مجازات حبس یا جزای نقدی است، هر دو نوع مجازات رویکرد سزادهی داشته و به دلیل اینکه در بسیاری موارد خسارات غیرمادی است، تشخیص تناسب را نیز برای تعیین ضمانت اجرا دشوار کرده است، از یک طرف معیاری برای استفاده از نوع مجازات یا میزان آن ارائه نشده است و از طرف دیگر به دلیل اینکه در ماده ۲۳ قانون آیین دادرسی کیفری ۱۳۹۲، تشکیل پرونده شخصیت برای جرایم پایین‌تر از درجه (۴) الزامی نیست، به نظر می‌رسد بحث فردی کردن و بازپروری نیز مدنظر قانونگذار نبوده است، پیشنهاد می‌شود چون اکثر مجازات‌ها مشمول برنامه‌های عدالت ترمیمی قانون مجازات اسلامی قرار می‌گیرند، به دلیل اینکه در نهادهایی چون تخفیف، تعویق صدور حکم، تعلیق اجرای مجازات، نظام نیمه آزادی، آزادی مشروط و جایگزین‌های حبس، جبران خسارت و ضرر و زیان بزه‌دیده یکی از شروط اعمال آنها است، در غیر از مواردی که طبق ماده ۷۵۴ قانون مجازات اسلامی مجازات‌ها تشدید خواهد شد و اقدامات تروریستی شناخته نشود (ماده ۷۳۹ قانون مجازات اسلامی)، از این نوع رویکرد ارفاقی استفاده شود، به خصوص در مورد هکرها خدمات عمومی رایگان، به خصوص انجام خدمت به بزه‌دیدگان حقوقی مثل بانک‌های خصوصی و دولتی و بانک مرکزی در اولویت قرار دارد.

پی‌نوشت‌ها:

(۱) ابزارگرایی معادل (Instrumentalism) در انگلیسی و (ذرائیت) در زبان عربی است. ابزار، به معنی وسیله و سبب چیزی است، در فلسفه ابزارگرایی، فکر چیزی جز یک وسیله برای موفقیت در زندگی نیست. ابزارگرایی نظریه‌ای است که ایده‌ها را ابزار عمل و کارایی را سنجه حقیقت می‌داند (کاپلستون، ۱۳۸۲: ۴۳۵).

(۲) در مقابل غیرابزارگرایان، حقوق کیفری را به عنوان واکنشی ذاتاً مناسب به برخی رفتارهای غیرقانونی معین توصیف می‌کنند.

(۳) با پیشرفت فناوری در صنعت بانکداری، بانکداری مجازی و بانکداری مجازی هیبریدی (الکترونیکی) به وجود آمده است. در واقع بانکداری مجازی زیرمجموعه بانکداری الکترونیکی نمی‌باشد. بلکه آخرین سطح بانک در ارائه خدمات بانکداری الکترونیکی به نام بانکداری مجازی تعریف می‌شود، به مجموع دو نوع بانکداری الکترونیکی و مجازی بانکداری نوین نیز گفته می‌شود (مبینی دهکردی و رسولی نژاد، ۱۳۹۰: ۱۹۶).

(۴) هدف از استفاده از این واژه، منحصراً اشاره و ارجاع به خدمات و محصولات مالی سازگار با محیط زیست است.

(۵) دستگاه خودپرداز با (ATM= Automated teller Machin) با شناسایی مشتری از طریق کارت بانکی، به مشتریان بانکها، امکان دریافت وجه از حساب، انتقال پول به سایر حسابها، پرداخت قبوض، خرید شارژ و بررسی گردش حسابشان را بدون نیاز به تحویل دار بانک ممکن ساخته است.

(۶) پایانه فروش (Pos = point of sale) یا کارت‌خوان فروشگاهی دستگاهی است که با پذیرش کارت بانکی، می‌تواند امکانی را فراهم کند که وجه به‌صورت الکترونیکی از حساب دارنده کارت به حساب فروشنده منتقل شود و معمولاً در فروشگاه‌ها و مراکز تجاری کاربرد دارد.

(۷) از جمله امضاهای دیگری که با فناوری ساده تولید شده است، امضای دستی اسکن شده، امضا با قلم نوری و کلیک کردن بر روی گزینه تأیید است. امضاهایی با فناوری زیست سنجی یا بیومتریک نیز وجود دارد، مبنای تشخیص هویتی استفاده شده، بر اساس خصیصه‌های منحصر به فرد فیزیکی و رفتاری کاربر است مثل اثر انگشت، تصویر شبکیه چشم، شکل هندسی دست و انگشت یا شناسایی از طریق صدا.

(۸) بند الف ماده (۳۰) قانون ثبت اختراعات، طرح‌های صنعتی و علائم تجاری مصوب ۱۳۸۶، علامت را تعریف کرده است، بدین معنی، علامت هر نشان قابل رؤیتی است که بتواند کالاها یا خدمات اشخاص حقیقی را از هم متمایز سازد. این تعریف با این عبارت که امضای الکترونیکی را علامت می‌داند از جهاتی شباهت دارد، زیرا علامت را معرف شخص دانسته است.

(۹) معادل واژه داده پیام در سیستم بانکی تراکنش است. تراکنش، یک پیام الکترونیکی است که مشتری بانک از طریق یکی از درگاه‌ها نظیر خودپرداز یا پایانه فروش تقاضا کرده و می‌تواند برداشت یا انتقال وجه انجام دهد.

(۱۰) طبق ماده ۱۳۰۴ قانون مدنی، لازم نیست در اسناد کاغذی امضاء همراه با متن در یک برگه باشند، بلکه امضاء می‌تواند در برگ جداگانه درج شده باشد، بدین ترتیب امضای الکترونیکی که علامت منضم شده یا متصل شده به داده پیام تعریف شده است، دارای اعتبار است.

(۱۱) جرم دسترسی غیرمجاز، رکن قانونی دیگری نیز دارد که خاص است. ماده ۷۳۲ قانون تعزیرات به نقض تدابیرامنیتی سامانه‌های رایانه‌ای به قصد دسترسی به داده‌های سری اشاره دارد، هرچند مرتکب به داده‌های سری دسترسی نیابد.

(۱۲) این رمز، رمز دوم یا رمز اینترنتی است، می‌تواند ثابت یا متغیرباشد. در حالتی که رمز متغیراست، برای هر بار ورود از طرف بانک رمز جدید به تلفن همراه صاحب حساب پیامک می‌گردد، یا از طرف بانک، دستگاه رمز ساز به صاحب حساب تحویل خواهد شد تا پس از درج نام کاربری یک رمز جدید که دارای مدت زمان اعتباری مشخص است اختصاص یابد.

(۱۳) هکرها براساس انگیزه نفوذ به سیستم‌های کامپیوتری، به دو دسته کلاه سیاه و کلاه سفید تقسیم شده‌اند. هدف، هکرهای کلاه سفید ارتقای امنیت در سیستم است، با شناسایی حفره‌های امنیتی، به رفع نقاط ضعف

سیستم‌ها کمک می‌کنند. اما هکرهای کلاه سیاه یا کراکرها، هدفشان تهاجمی و انجام کارهای خرابکارانه و غیرقانونی است.

(۱۴) سایر رفتارهایی که در بند الف ماده ۷۳۵ قانون مجازات اسلامی پیش‌بینی شده است، جزو جرایم مستقیم علیه گذرواژه نیست، بنابراین دسترسی غیرمجاز به درگاه‌های بانکی به این روش حاصل نخواهد شد.

(۱۵) از لحاظ عملی این جرم با ماده ۶۶۴ قانون مجازات اسلامی قابل مقایسه است،این ماده ساخت کلید یا هر نوع وسیله‌ای برای ارتکاب جرم را جرم‌انگاری کرده است.

(۱۶) این جرم مانند جرایم مندرج در مواد ۷۱۲ (ولگردی)، ۷۲۳ (رانندگی بدون پروانه)، ۵۵۵ (غصب عناوین دولتی) از جمله جرایم مانع است.

(۱۷) سوء نیت خاص این جرم، احراز قصد انتشار بدافزار به منظور ارتکاب سایر جرایم رایانه‌ای است.

(۱۸) برای اطلاعات بیشتر مراجعه شود به:

For More Info. see http://www.usdoj.gov/Uso/cac/pr/cac70627.1.html

(۱۹) ماده ۷۵۵ قانون مجازات اسلامی عدم ارائه خدمات الکترونیکی عمومی را برای افرادی پیش‌بینی کرده است که سابقه دوبار بیشتر تکرار جرم داشته باشند.

(۲۰) با تغییر گذرواژه ممانعت از دسترسی حاصل خواهد شد، بنابراین جرم موضوع ماده ۷۳۸ قانون مجازات اسلامی در زمره جرایم مطلق است.

(۲۱) اعتماد طبیعی انسان اصلی‌ترین و ابتدایی‌ترین روش برای هر حمله مهندسی اجتماعی است و مهندسین اجتماعی به این حقیقت امید دارند که مردم نسبت به اطلاعات با ارزش خود بی‌اطلاع و نسبت به محافظت از آن بی‌مبالات هستند. مهندسی اجتماعی هنری است که فرد را متقاعد خواهد کرد اطلاعات محرمانه خود را آشکار سازد.

(۲۲) فیشینگ (phishing) کنایه از ماهی‌گیری و بر پایه‌ی بی‌احتیاطی و فریب افراد، برای دسترسی به رمزهای عبور شخصی آنان است. در این روش فیشر صفحه‌ای مشابه درگاه پرداخت آنلاین می‌سازد، کاربر که وارد سایت جعلی شد و اطلاعات خود را وارد کرد، اطلاعات وی از طریق سایت جعلی برای نفوذگر ارسال و به سرقت خواهد رفت. قانون جرایم رایانه‌ای طراحی صفحه جعلی را جرم ندانسته است.

(۲۳) در این شیوه هرچند تدابیر امنیتی حفاظت شده به روش فنی برداشته نشده است، بدلیل اینکه مبنای جرم انگاری دسترسی غیرمجاز، حمایت از محرمانگی داده یا سامانه است، به همین دلیل رخنه‌گری محسوب شده و جرم دسترسی غیرمجاز تحقق یافته است. در مقابل، چون ممانعت از دسترسی، جرم خاص فضای مجازی است و در بستر سایبری تحقق خواهد یافت. شرط تحقق آن رخ دادن در بستر شبکه بانکداری الکترونیکی است. بنابراین هرگونه اقدام فیزیکی، مثل از بین بردن پاکتی که گذرواژه روی آن نوشته شده یا قطع کردن برق سیستم کامپیوتری به قصد ممانعت کاربر از دسترسی به درگاه بانک،جرم موضوع ماده ۷۳۸ نخواهد بود.

(۲۴) دانشنامه آزاد ویکی پدیا داده را چنین تعریف کرده است: به اعداد، حروف و علائمی که جهت فهم و درک مشترک از انسان‌ها یا رایانه سرچشمه گرفته داده می‌گویند. داده‌ها معمولاً از سوی انسان‌ها بصورت حروف، اعداد، علائم ارائه و در رایانه به صورت نمادهایی که همان رمزهای صفر و یک قراردادی هستند نشان داده شده است.

(۲۵) چون نقش گذرواژه امنیتی است، پس نتیجه پردازش استفاده اشتباه و مکرر از آن در سامانه‌های بانکی باعث مسدود شدن حساب خواهد شد.

(۲۶) داده‌هایی مثل میزان موجودی یا گردش حساب یا اطلاعات شخصی صاحب حساب داده محتوایی است. داده محتوا در بند (ب) ماده (۱) لایحه جرایم رایانه‌ای این‌گونه تعریف شده است : «هر نمادی از موضوع‌ها، مفهوم‌ها یا دستورالعمل‌ها نظیر متن، صوت یا تصویر، چه به صورت در جریان یا ذخیره شده که به منظور برقراری ارتباطات میان سیستم‌های رایانه‌ای یا پردازش توسط شخص یا سیستم رایانه‌ای، به‌کار گرفته شده و به وسیله سیستم رایانه‌ای ایجاد شود». بنابراین تخریب داده به معنی ناخوانا کردن آن، نسبت به این نوع از داده‌ها مصداق دارد و نسبت به داده‌های امنیتی عملی نیست.

(۲۷) غیرقابل پردازش کردن داده‌ها امکان‌پذیر نیست، چون از کار انداختن یا سلب کارایی و کارکرد داده نسبت به سامانه ارزیابی خواهد شد والا هر داده‌ای هرچند دستکاری شده باشد باز هم قابل پردازش است. منتهی نتیجه پردازش داده دستکاری شده به نتیجه مورد نظر کاربر منتج نخواهد شد.

(۲۸) سایر داده‌های ذخیره شده مربوط به حساب اشخاص، مانند میزان موجودی یا گردش حساب که حاصل تراکنش است، طبق ماده ۶ قانون تجارت الکترونیکی به عنوان اسناد بانکی به حساب آمده و صاحب حساب حق تغییر آنها را ندارد. از طرف دیگر، چون جزو حریم خصوصی اشخاص است، به‌کارگیری آنها توسط بانک هم تابع اصول خاصی است.

(۲۹) ارسال امواج رادیویی و تلویزیونی عمومی است.

(۳۰) اگر گذرواژه در مسیر انتقال شنود شود. چون، گذرواژه مجوز دسترسی به سامانه‌های بانکی است، نفوذگر از همین بستر خواهد توانست استفاده کرده و اقدام به دسترسی غیرمجاز نماید. به همین دلیل برخی سامانه‌های بانکی، رمز یا کد عبور متنی را قبل از دسترسی کاربر پیش‌بینی نموده‌اند که یک تدبیر امنیتی ضد شنود است. بدین ترتیب چون صفحه مانیتور کاربر برای نفوذگر قابل رؤیت نیست، امکان دسترسی غیرمجاز هم وجود نخواهد داشت، هرچند نفوذگر به گذرواژه دسترسی یافته باشد.

(۳۱) برای اطلاعات بیشتر رجوع شود به:

Australian Fereral Police 1991- 2003. Annual Reports 1991-2003, At: http://www.usdoj.gov/eriminal /cyber crime/ comrade.htm

(۳۲) طبق ماده ۵ دستورالعمل رعایت مقررات مبارزه با پول‌شویی در حوزه نظام‌های پرداخت بانکداری الکترونیکی، تطبیق هویت ارباب رجوع با اقلام اطلاعاتی شناسایی مشتری در مراجعات غیرحضوری از طریق ابزارهای شناسایی است.

(۳۳) به همین دلیل اگر جسم کارت به هر شکلی جعل شود، رمز کارت یا ماهیت مجازی، دسترسی غیرمجاز به روش تماسی را دشوار خواهد کرد.

(۳۴) برای اینکه اطلاعات کاربر از طریق سیم‌های رابط درگاه‌های حضوری شنود نشود، به روکش ضدمغناطیسی مجهز شده است.

(۳۵) یکی دیگر از روش‌های تحصیل گذرواژه، قراردادن صفحه کلید بدلی، شبیه صفحه کلید اصلی روی دستگاه خودپرداز است، به گونه‌ای روی خودپرداز مستقر است که کاربر متوجه نخواهد شد یک صفحه کلید اضافی روی شماره‌های اصلی قرار گرفته است، با این روش کاراکترهای گذرواژه کپی خواهد شد.

(۳۶) نوع دیگری از مهندسی اجتماعی از طریق نفوذ کلامی یا رفتاری است. چون، تحصیل متقلبانه پول صورت گرفته، کلاهبرداری سنتی است.در این روش فرد مالباخته برای اینکه پولی به حسابش واریز شود، به سمت دستگاه خودپرداز هدایت شده، پس از قراردادن کارت و درج رمز عبور، با راهنمایی کلاهبردار از منوی

انگلیسی دستگاه استفاده و بدون اینکه متوجه نوع عملیات بانکی شود، اقدام به واریز وجه به حساب مورد نظر کلاهبردار خواهد کرد.

(۳۷) چندی پیش مدیر سابق یکی از شرکت‌های همکار بانک مرکزی به خارج از کشور گریخت و با ایجاد یک وبلاگ، اقدام به انتشار اطلاعات کارت‌های مشتریان برخی بانک‌ها و رمز عبور آنها کرد. به همین دلیل، بانک مرکزی در فروردین ماه ۱۳۹۱ با انتشار اطلاعیه‌ای از دارندگان کارت‌هایی که طی چند ماه گذشته رمز خود را تغییر نداده بودند، تقاضا کرد تا نسبت به تغییر رمز اقدام نمایند.

(۳۸) عنصر قانونی جعل کارت‌های بانکی بند (ب) ماده ۷۳۴ قانون مجازات اسلامی است.

(۳۹) کد اعتبارسنجی (CVV2) عددی است که طول آن بین سه تا چهار رقم است، در سامانه کارت بانک تعریف شده و پشت کارت درج شده است.

(۴۰) چون کارت‌های حافظه غیرقابل پردازش هستند در بانکداری الکترونیکی کاربردی ندارند.

(۴۱) یکی از روش‌های به‌دست آوردن کارت، ریختن چسب مایع در محل کارت دستگاه خودپرداز است، پس از اینکه صاحب کارت از دریافت آن ناامید شد، سارقین کارت را برداشته و استفاده غیرمجاز خواهند نمود. روش تعویض کارت با استفاده از ناآگاهی مشتریان است، کاربری که مهارت ندارد، برای استفاده از دستگاه خودپرداز از افراد در صف خودپرداز کمک خواهد گرفت و برخی از آنها اقدام به تعویض کارت کرده‌اند.

(۴۲) کپی کردن غیرقانونی علائم نوار مغناطیسی بانکی روی کارت دیگر، اسکیمینگ (skimming) است، اسکیمرها دستگاه‌های کوچکی هستند که در محل ورودی دستگاه خودپرداز بانک‌ها یا خودپردازهای تقلبی و حتی روی دستگاه کارت خوان فروشگاهی نصب شده‌اند. رئیس پلیس فتای تهران در مهر ماه سال جاری از سرقت نامرئی ۷۰۰ میلیون تومانی از ۴۱ نفر خبر داد، در این روش دستگاه کپی روی کارت‌خوان فروشگاهی نصب می‌شود، پس از اینکه رمز مشتریان به بهانه کوتاه بودن سیم دستگاه کارت خوان دریافت شد، دسترسی غیرمجاز و سرقت صورت گرفته است.

(۴۳) اگر ثابت شود ضرر و زیانی که به دارنده کارت وارد شده است، به دلیل عدم پیش‌بینی تدابیر امنیتی در کارت است، طبق ماده ۳۵ قانون پولی و بانکی کشور مصوب ۱۳۵۵، خسارات وارده باید توسط بانک جبران شود.

(۴۴) برای اطلاعات بیشتر رجوع کنید به: http://news.bbc.co.uk/2/hi/uk-news/wales/2678773.stm

(۴۵) طبق بند (و) از ماده (۲) قانون تجارت الکترونیکی، سیستم رایانه‌ای، هرنوع دستگاه یا مجموعه‌ای از دستگاه‌های متصل سخت افزاری-نرم‌افزاری است که از طریق اجرای برنامه‌های پردازش خودکار داده عمل خواهد کرد.

(۴۶) چون درگاه‌های بانکی به صورت هوشمند به آخرین موجودی حساب کارت دسترسی دارند. اگر، ارقام موجود در کارت تغییر یابد، از نظر فنی امکان دارد، بدلیل مغایرت موجودی کارت با سامانه، امکان عملیات بانکی وجود نداشته باشد.در این حالت، چون جرم جعل مطلق است، تحقق جرم موکول به حصول نتیجه نیست.

(۴۷) این عمل، قابل مقایسه است با رفتار ذینفع چکی که با دستکاری چک و افزایش مبلغ،اقدام به جعل کرده است.

(۴۸) استنادپذیری کارت از شرایط جعل کارت نیست ولی در جعل داده، استنادپذیری شرط است. دلیل تفاوت این است که، کارت‌های پرداخت الکترونیکی بانکی سند تجاری نیستند که قابل استناد باشند و فقط حامل داده بوده و ابزاری برای پرداخت در تجارت الکترونیکی هستند. در مقابل طبق مواد ۶ و۱۲ و ۱۳ قانون تجارت

الکترونیکی، داده پیام در حکم نوشته‌ای است که متناسب با روش ایمنی به‌کار گرفته شده، دارای ارزش اثباتی است.

(۴۹) در این روش محتوای داده‌ها چنان عوض خواهد شد که غیراز منظور نظر بانک است و در حقیقت محتوا به یک محتوای موثق غیرواقعی تبدیل شده است.

(۵۰) صاحب کارت حق دارد بدلیل سرقت یا مفقود شدن کارت تقاضای ابطال آن را بنماید.

(۵۱) دستکاری کارت ابطال شده نسبت به صاحب کارت، یک جرم محال است، چون امکان ضرر مادی برای صاحب کارت وجود ندارد.

(۵۲) طبق ماده ۵۸۸ قانون تجارت، بانک‌ها به عنوان اشخاص حقوقی، حق مطالبه خسارت معنوی پیش‌بینی شده در ماده یک قانون مسئولیت مدنی مصوب ۱۳۳۹ و ماده ۱۴ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ را دارند.

(۵۳) برای اطلاعات بیشتر رجوع کنید به:

-http://www.gurdian.co.uk/internetnews/story/0,1369,517864/00.html

-smith, R, Grabosky , P. , Urbas, G.(2004), cyber criminals on trial , Cambridge University press, P. 38-41

(۵۴) شورای پول و اعتبار در تاریخ ۱۳۹۰/۲/۲۷ آیین‌نامه تأسیس و فعالیت بانک‌های مجازی را تصویب نموده است. بانک مجازی بانکی استکه شعبه ندارد و دریافت سپرده، اعطای اعتبار، صدور حواله، ضمانت‌نامه و گشایش اعتبارات اسنادی را از طریق درگاه‌های الکترونیکی مثل اینترنت، خودپرداز، پایانه فروش، تلفن همراه و غیره انجام می‌دهد.

(۵۵) سامانه نماد که دارای یک زیرساخت یکپارچه است، توسط بانک مرکزی پیاده‌سازی شده است، این امکان را در اختیار مشتریان شبکه بانکی قرار داده تا صرف نظر از اینکه کدام بانک به آنها خدمات ارائه کرده، بتوانند با یک گواهی امضای دیجیتال از خدمات کلیه بانک‌ها استفاده نمایند.

(۵۶) بند (ج) ماده یک آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی، گواهی الکترونیکی را تعریف کرده است. داده الکترونیکی حاوی اطلاعاتی در مورد مرکز صادره گواهی، مالک گواهی، تاریخ صدور و انقضا، کلید عمومی مالک و یک شماره سریال است که توسط مرکز میانی تولید و به گونه‌ای طراحی شده است که هر شخص خواهد توانست به صحت ارتباط بین کلید عمومی و مالک آن اعتماد کند.

(۵۷) بندهای ج،ح وخ ماده یک آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی، از زوج کلید با عناوین داده‌های ایجاد و وارسی امضای الکترونیکی یاد کرده است.

(۵۸) طبق بند (ج) ماده (۲) قانون تجارت الکترونیکی، مخاطب شخصی است که اصل ساز قصد دارد وی داده پیام را دریافت کند.

(۵۹) با توجه به تعریفی که از امضای دیجیتال در ماده ۱۰ قانون تجارت الکترونیکی آمده است، ثبت نام کاربری و گذرواژه برای دسترسی به سامانه نماد یا ثبت اثر انگشت یا گذرواژه برای راه‌اندازی توکن از اجزای امضای دیجیتال نیست.

(۶۰) بر اساس تبصره و بند (ب) ماده ۹ قانون برنامه پنج ساله توسعه جمهوری اسلامی ایران مصوب ۱۳۸۹، بانک مرکزی جمهوری اسلامی ایران در اردیبهشت ماه ۱۳۹۲ اقدام به انتشار دو سند نموده است.خط مشی مرکز گواهی که نیازمندی‌های عملیاتی، حقوقی و فنی مرکز گواهی را تشریح کرده است و دستورالعمل اجرایی

مرکز گواهی که به تشریح دستورالعمل و روش‌های اجرایی برای صدور و نگهداری و استفاده از گواهی‌های صادره توسط مرکز گواهی بانک مرکزی پرداخته است.

(۶۱) در این حالت دو جرم دسترسی غیرمجاز رخ داده است، چون تدابیر تأمینی داده‌ها و دستگاه رمزساز نقض شده است.

(۶۲) مجازات جعل رایانه‌ای حبس یا جزای نقدی است، در مقابل مجازات جعل تجارت الکترونیکی حبس و جزای نقدی تعیین شده که در هر دو حالت کمتر از حبس و جزای نقدی جعل رایانه‌ای است. بنابراین، چون در یکی یک مجازات وجود دارد که شدیدتر است و در دیگری دو مجازات تعیین می‌شود که خفیف‌تر است، امکان تشخیص قانون منسوخ، بر اساس شدت مجازات را دشوار کرده است.

(۶۳) چنانچه، اقدامات مزبور بصورت عمدی توسط سردفتر اسناد رسمی ارتکاب یابد، منطبق با بندهای ثانیاً و ثالثاً ماده ۱۰۰ قانون ثبت است و سردفتر به مجازات جاعل اسناد رسمی محکوم خواهد شد. به‌علاوه، چون در این موارد گواهی، بدون رضایت شخص صادر شده یا مبتنی بر دروغ و اشتباه متقاضی است، طبق بندهای پ و ث ماده ۱۹ آیین‌نامه اجرایی ماده ۳۲ قانون تجارت الکترونیکی، گواهی صادره باطل خواهد شد.

(۶۴) برای کپی کردن گواهی الکترونیکی، ابتدا باید تمام فرایند تولید اثر که در حافظه دستگاه رمزنگاری ذخیره شده است، تجزیه و تفکیک شود و سپس از آن روگرفت تهیه شود، به این عمل اصطلاحاً مهندسی معکوس گفته شده است.

(۶۵) بند ۹-۵ سند سیاست‌های گواهی الکترونیکی زیرساخت کلید عمومی کشور مصوب ۹۱/۴/۲۷ شورای سیاست‌گذاری گواهی الکترونیکی کشور، حق مالکیت معنوی کلیه گواهی‌های صادره و زوج کلید متناظر با گواهی (کلید خصوصی) را متعلق به مراکز صدور گواهی و مالک گواهی می‌داند و در بند ۹-۲ سند سیاست‌های گواهی مرکز ریشه مصوب ۱۳۸۷/۷/۳ شورای سیاست‌گذاری گواهی الکترونیکی، آمده است که مراکز صدور گواهی باید این حقوق را در دستورالعمل‌های خود بگنجانند. بدین ترتیب، بانک مرکزی در بند ۹-۵ اسناد و خط مشی مرکز گواهی و دستورالعمل اجرایی مرکز گواهی این حق را پیش‌بینی کرده است.

(۶۶) بند ۶-۱-۳ دستورالعمل‌های اجرایی مرکز گواهی بانک مرکزی، استفاده از نام‌های تجاری ثبت شده برای متقاضیان گواهی را ممنوع نموده است، پیشنهاد می‌شود برای اینکه از ارتکاب جرایم علیه علائم تجاری پیشگیری شود، همان‌طور که امکان استعلام آنلاین بانک‌ها با اداره ثبت احوال برای احراز هویت مشتریان برقرار شده است، ارتباط بر خط بانک مرکزی با اداره ثبت علائم تجاری فراهم گردد، بدین ترتیب از استفاده علائم تجاری متعلق به دیگران خودداری خواهد شد.

(۶۷) تصدیق هویت در سیستم بانکی، براساس دستورالعمل‌های چگونگی شناسایی مشتریان مؤسسات اعتباری مصوب شورای پول و اعتبار ۱۳۸۹ انجام می‌شود. همچنین، شعب بانک‌هایی که به عنوان دفاتر پیشخوان خدمات گواهی الکترونیک بانکی نماد تعیین شده‌اند، از طریق سامانه نهاب (نظام هویت سنجی الکترونیک بانکی) که به عنوان پرتال نماد پیاده‌سازی شده است، اقدام به تخصیص شماره شناسایی منحصر به فرد به افراد، در شبکه بانکی خواهند نمود. این شماره شهاب (شناسه هویت الکترونیکی بانکی) است.

(۶۸) طبق آیین‌نامه مدت و طرز نگهداری اوراق بازرگانی، اسناد و دفاتر بانک‌ها مصوب ۱۳۹۳ شورای پول و اعتبار، نگهداری اسناد هویتی بانک‌ها تا مدت‌های پیش‌بینی شده الزامی است و قابل محو و یا تغییر نیست. بنابراین نقض مواردی که در ماده ۵۹ قانون تجارت الکترونیکی پیش‌بینی شده است، از جمله جرایم علیه امضای دیجیتال نیست.

(۶۹) افشای کلید خصوصی گواهی از موارد ابطال است.

(۷۰) بند (ب) ماده ۷۵۳ قانون مجازات اسلامی علاوه بر گذرواژه، فروش یا انتشار یا در دسترس قرار دادن هر داده‌ای که امکان دسترسی غیرمجاز را فراهم کند جرم شناخته است. بنابراین، اگر داده‌های کارت پرداخت بانکی یا گواهی امضای الکترونیکی که برای دسترسی غیرمجاز استفاده شده است توسط کارکنان شبکه بانکی، در اختیار دیگران قرار گیرد، مشمول مجازات مشدد مندرج در بند (ج) ماده ۷۵۴ قانون مجازات اسلامی خواهد شد.

(۷۱) وارد کردن غیرمجاز داده همان دستکاری داده است که به معنی حذف کردن، اضافه کردن، تغییر دادن یا مکرر کردن داده تعبیر شده است و بدین ترتیب اطلاعات ذخیره شده متعلق به دیگری مورد تغییر قرار گرفته و به عنوان داده اصلی قلمداد خواهد شد. این عمل با وارد کردن غیرمجاز گذرواژه که باعث نقض تدابیر امنیتی سامانه‌ها می‌شود متفاوت است، نتیجه این عمل بر علیه محرمانگی و دسترسی غیرمجاز است ولی اولی تغییرداده و بر علیه صحت و تمامیت است.

(۷۲) قوانین کیفری فرد را مجازات و حقوق و آزادی‌های فردی را محدود خواهد کرد، پس باید کیفی باشد. به این اصل، اصل کیفی بودن قوانین کیفری گفته شده، یکی از مصادیق آن صریح و منجر بودن قوانین کیفری و عدم وجود ابهام در آنها است. پس، ضروری است به دلیل اینکه عناوین دو جرم جعل و دسترسی غیرمجاز به اشتباه مورد استفاده قرار نگیرد، رفع ابهام شود.یکی دیگر از مصادیقی که اصل کیفی بودن قوانین کیفری دارد، درج آثاری است که قانون کیفری برای فرد به دنبال دارد. این اصل در ماده ۶۲ قانون تجارت الکترونیکی که مربوط به حمایت از مالکیت معنوی است رعایت نشده واز روش احاله کیفر استفاده شده است، یعنی جرم را تعریف کرده بدون آنکه عنوان خاصی برای آن قرار دهد ولی مجازات را به قانون دیگری احاله داده است، چون جرم و مجازات در یک ماده قانونی و در کنار هم نیست، باعث شده مخاطبان قانون درک درستی از نوع عمل و مجازاتی که دارد نداشته باشند.

(۷۳) اگر دسترسی غیرمجاز با سایر جرایم رایانه‌ای همراه باشد، از موارد تعدد واقعی جرایم است و بر اساس ماده ۱۳۴ قانون مجازات اسلامی مصوب ۱۳۹۲ تعیین کیفر خواهد شد.

(۷۴) در قانون جرایم کامپیوتری تفاوتی بین مجازات جعل کارت پرداخت بانکی با جعل تراشه (توکن) که حاوی امضای دیجیتال است، وجود ندارد. در صورتی که امضای دیجیتال اهمیت و کاربرد بیشتری دارد. به همین ترتیب، تفاوتی بین مجازات دسترسی غیرمجاز به درگاه‌های حضوری و غیرحضوری، داده و سامانه، داده اشخاص دولتی و خصوصی یا داده اشخاص حقیقی و حقوقی پیش‌بینی نشده است.

(۷۵) سرقت فیزیکی کارت اعتباری یا توکن گواهی امضای الکترونیکی جرم نگاری نشده است، چون در عرف رایج نیست، در ازای آن پول یا کالای با ارزش دیگری پرداخت شود، اگر کارت به همراه گذرواژه سرقت شود، دارای ارزش اقتصادی است چون در ازای استفاده از آن می‌توان کالا خرید یا پول برداشت کرد، ولی این عمل سرقت غیررایانه‌ای نیست و همان دسترسی غیرمجاز است. کارتهای اعتباری بی‌نام، مثل کارتهای هدیه چون دارای سیستم حفاظتی از نوع گذرواژه است. علیرغم اینکه کارکردی مثل چک‌های تضمین شده یا اسکناس دارند و در اختیار هرکسی که باشد مالک آن است، سرقت فیزیکی و استفاده غیرمجاز از این کارت‌ها هم به عنوان جرم دسترسی غیرمجاز است.

(۷۶) بند (د) ماده ۷۵۴ قانون مجازات اسلامی، ارتکاب جرایم رایانه‌ای نسبت به داده‌های دولتی را مشمول تشدید مجازات قرار داده است.

منابع فارسی

احمدی، سیدمحمود و مهدی خندان سویری (۱۳۹۴)، ***نظام‌های مدیریت پرداخت و بانکداری الکترونیک در ایران***، پژوهشکده پولی و بانکی بانک مرکزی.

احمدوند، علی‌محمد (۱۳۸۶)، «درباره راهبرد، مقدمه‌ای بر تدوین طرح راهبردی در ناجا»، ***مجله توسعه انسانی پلیس***، شماره ۱۰.

افراسیابی، محمد اسماعیل و فهیم مصطفی‌زاده (۱۳۹۳)، «بررسی رویکرد ابزارگرا به حقوق کیفری ایران در پرتو قانون اساسی»، ***فصلنامه دیدگاه‌های حقوقی***، شماره ۶۸.

الهی‌منش، محمدرضا و ابوالفضل صدره‌نشین (۱۳۹۱)، ***محشای قانون جرایم رایانه‌ای***، تهران: مجد.

آلبینز، جی اس (۱۳۹۳)، ***سرقت و کلاهبرداری مالکیت فکری***، ترجمه حمیدرضا دانش ناری و سیدامین روح‌الامینی.

انصاری، اسماعیل (۱۳۸۸)، «تحلیل اثباتی و هنجاری حقوق کیفری و مجازات‌های بهینه از دیدگاه مکتب تحلیل اقتصادی حقوق»، ***فصلنامه اطلاع‌رسانی حقوقی***، شماره ۱۹ و ۲۰.

بابایی، محمدعلی و اسماعیل انصاری (۱۳۹۱)، «تحلیل هزینه‌های جرم»، ***مجله نامه مفید***، شماره ۹۴.

بروکس، تام (۱۳۹۵)، ***مجازات***، ترجمه محمدعلی کاظم نظری، تهران: میزان.

پرادل، ژان (۱۳۷۳)، ***تاریخ اندیشه‌های کیفری***، ترجمه علی‌حسین نجفی ابرندآبادی، تهران: دانشگاه شهید بهشتی با همکاری مؤسسه نشر یلدا.

جاویدنیا، جواد (۱۳۸۷)، ***جرایم تجارت الکترونیکی***، تهران: خرسندی.

جوان‌جعفری، عبدالرضا و سیدمحمدجواد اسلامی (۱۳۹۰)، «از سزاگرایی کلاسیک تا سزاگرایی نوین»، ***آموزه‌های حقوق کیفری***، شماره ۲.

جوان جعفری، عبدالرضا، فرهادی آلاشتی و سیدمحمدجواد ساداتی (۱۳۹۵)، «بازدارندگی و سنجش آن در فلسفه کیفر»، ***پژوهشنامه حقوق کیفری***، شماره ۱۴.

حبیب‌زاده، محمدجعفرو سلمان عمرانی (۱۳۹۲)، «تحلیل ساختاری رابطه حقوق کیفری و دانش سیاسی»، ***فصلنامه مطالعات حقوقی دولت اسلامی***، سال دوم، شماره ۲.

داوری دولت آبادی، مجید (۱۳۹۳)، ***هکرهای قانونمند (CEH)***، تهران: آترا.

رحمانیان، حامد و محمدجعفر حبیب زاده (۱۳۹۲)، «ابزارگرایی کیفری : قلمرو، مفهوم، شاخص‌ها»، ***پژوهش حقوق کیفری***، شماره ۵.

روحانی رانکوهی، سیدمحمدتقی (۱۳۹۲)، ***مفاهیم بنیادی پایگاه داده‌ها***، چاپ ششم، تهران: جلوه.

شمس، عبدالله (۱۳۹۲)، ***آیین دادرسی مدنی***، جلد ۳، چاپ بیست وسوم، تهران: دراک.

صالحی، جواد و علی غلامعلی پور (۱۳۸۹)، «حمایت از کپی رایت در حقوق کیفری»، ***آموزه‌های حقوق کیفری***، شماره ۱۳.

عالی‌پور، حسن (۱۳۹۰)، ***حقوق کیفری فناوری اطلاعات***، تهران: خرسندی.

غلامی، حسین (۱۳۸۸)، «سیاست کیفری سلب توان بزهکاری»، ***مجله تحقیقات حقوقی***، شماره ۵۰.

فرایبرگ، آریه (۱۳۹۱)، «تعیین مجازات بزهکاران یقه سفید»، ترجمه اعظم مهدوی‌پور، ***فصلنامه مطالعات پیشگیری از جرم***، شماره ۲۵.

قماشی، سعید (۱۳۸۵)، «بررسی جرم افشای اسرار حرفه‌ای»، ***ماهنامه دادرسی***، شماره ۵۸.

قناد، فاطمه (۱۳۹۰)، «جعل در بستر فناوری‌های اطلاعات و ارتباطات»، ***آموزه‌های حقوق کیفری***، دوره جدید، شماره ۲.

قناد، فاطمه (۱۳۸۸)، «پیشگیری کیفری از جرایم ارتکابی در فضای مجازی»، ***مجموعه مقالات نخستین همایش ملی پیشگیری از جرم، پیشگیری از تکرار جرم و بزه‌دیدگی***، معاونت آموزش ناجا.

کاپلستون، فردریک (۱۳۸۲)، ***تاریخ فلسفه (از فیشته تا نیچه)***، مترجم: داریوش آشوری، جلد هفتم، تهران: علمی و فرهنگی و سروش.

کی‌نیا، محمد (۱۳۸۸)، ***امضای الکترونیک***، تهران: میزان.

محمد نسل، غلامرضا (۱۳۹۲)، ***جرایم رایانه‌ای در ایران***، تهران: میزان.

مبینی دهکردی، علی و احسان رسول‌نژاد (۱۳۹۰)، ***شکل‌دهی به فضای نوین بانکداری، رویکرد دانش‌بنیان***، تهران: نور علم.

گرایلی، محمدباقر (۱۳۸۹)، «بررسی جعل و تخریب و اخلال رایانه‌ای»، ***آموزه‌های حقوق کیفری***، شماره ۱۴.

مرکز پژوهش‌های مجلس (۱۳۸۷)، ***اظهارنظر کارشناسی درباره لایحه جرایم رایانه‌ای (گزارش ۱)***، دوره هشتم، سال اول، شماره مسلسل ۹۱۳۸.

میرمحمد صادقی، حسین (۱۳۹۲)، ***جرایم علیه اموال و مالکیت***، چاپ سی‌وپنجم، تهران: میزان.

نجفی ابرندآبادی، علی‌حسین (۱۳۹۱)، «درباره امنیت شناسی (از حق بر امنیت تا حق بر تأمین)» در دیباچه کتاب ***مدیریت انسان‌مدار ریسک جرم***، نوشته سودابه رضوانی، تهران: میزان.

نجفی ابرندآبادی، علی‌حسین (۱۳۹۲)، «درباره سیاست جنایی افتراقی»، دیباچه ویراست چهارم کتاب ***سیاست جنایی***، نوشته کریستین لازرژ، چاپ چهارم، تهران: میزان.

نجفی ابرندآبادی، علی‌حسین، ***تقریرات درس جامعه‌شناسی جنایی دوره کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه شهید بهشتی***، نیمسال دوم سال تحصیلی ۸۴- ۱۳۸۳، قابل دسترسی از www.Lawtest.ir

نعیمی، سیدمرتضی (۱۳۹۴)، «تحلیل اقتصادی رفتار بزهکار و تبیین بازدارندگی مجازات»، ***پژوهشنامه حقوق کیفری***، سال ششم، شماره ۲.

هیئت مؤلفان و ویراستاران انتشارات مایکروسافت (۱۳۷۹)، ***فرهنگ تشریحی اصطلاحات کامپیوتری مایکروسافت***، ترجمه فرهاد قلی‌زاده نوری، تهران: کانون نشر علوم.

یزدیان جعفری، جعفر (۱۳۸۷)، «تأملی بر نظام هزینه- فایده در حقوق کیفری»، ***مجله فقه و حقوق***، شماره ۱۹.

منابع لاتین

Manson, Stephen (2007), ***Electroinc Signatures in Law***, London: Tothel Publishing.

Smith, R. Grabosky, P. Urbas G. (2004), ***Cyber Criminal on Trial***, Cambridge University Press.

Bagarvic, M. (2001), ***Punishment and Sentencing: A Rational Approach***, Cavendish Publishing Limited.