فصلنامه یافته های نوین درعلوم انسانی، علوم اجتماعی و روانشناسی شماره ۱- دوره ۱- صفحات ۳۶-۴۹
Journal of new findings in Social Sciences, Educational Sciences and Psychology

مسئولیت مدنی بانک ها در قبال خسارات ناشی از عدم اجرای بخشنامه های بانک مرکزی در باب کلاهبرداری رایانه ای

سعید بیگدلی
فارغ التحصیل مقطع کارشناسی ارشد رشته حقوق خصوصی دانشگاه علوم قضایی و خدمات اداری

چکیده

همواره در جریان فعالیت بانکداری مجازی امکان ورود خسارت به مشتریان به انحا مختلف مطرح است که یکی از آنها کلاهبرداری رایانه ای است .بانک مرکزی جهت پیشگیری ازاین امر بانک ها را مکلف به بستر سازی برای اجرای سیاست های بانکداری از جمله اجرای رمز پویا نموده است لکن بانک ها به جهت جذب مشتریان وسهولت در کار آنان با توسل به هر طریق ممکن سعی در عدم اجرای آن سیاست ها و پابرجایی اقداماتی همچون رمز ایستا درفعالیت های بانکی دارند.حال مسئله این است که اگر خسارتی در اثرعدم اجرای این موارد به مشتریان وارد شود چه کسی مسئول است؟ که به طور کلی ، باتوجه به نظریات حقوقی و فقهی و مواد قانونی موجود درنظام حقوقی ایران به نظر می رسد که بتوان نظریه مسئولیت مطلق بدین معنا که اگر به مشتری خساراتی در این راستا وارد شود بانک مسئول است؛ مگر آنکه خود مشتری سبب و زمینه ورود این خسارات را فراهم نماید.اثبات حاکمیت نظریه مسئولیت مطلق بانک ها واستناد به آن ، قطعا بسیاری از مشکلات فعلی در روابط بانک ها و مشتریان را کاهش خواهد داد.

واژگان کلیدی: مسئولیت مدنی، بانک ،خسارت ، بخشنامه های بانک مرکزی، کلاهبرداری رایانه ای

امروزه باتوجه به گسترش فضای مجازی همه فعالیت های بشر بخصوص فعالیت های اقتصادی دراین فضا قرار گرفته است و بیشتر مردم این فضا را برای فعالیت های اقتصادی خود برگزیده اند.یکی از اقسام فعالیت های اقتصادی مجازی ،بانکداری مجازی است .بانک ها برای انطباق خود با این پیشرفت ها بانکداری درفضای سایبر را ایجاد ودراختیار عموم قرار داده اند ؛ لکن این فضا ازامنیت صد درصدی برخوردار نبوده وممکن است بستر ارتکاب جرایمی گردد ؛که یکی از مهم ترین این جرایم ،کلاهبرداری های رایانه ای هستند که دراین فضا صورت می گیرند؛که بانک ها حسب مسئولیت ذاتی خود مکلف به حفظ وحراست از منابع مشتریان هستند می بایست امنیت لازم برای بانکداری مجازی را تامین نمایند وازطرفی هم بخشنامه های صادره ازسوی بانک مرکزی ، همچون بخشنامه ای درخصوص الزام بانک ها به استفاده از رمز پویا نیز براین مهم تاکید کرده است.حال این پرسش مطرح می شود که اگر بنا به دلایلی از جمله عدم رعایت بخشنامه فوق الذکر که منجر به کلاهبرداری های رایانه ای شود این منابع آسیب ببیند چه شخصی وتا چه میزان وبنا به چه علتی مسئول است؟ وچه نظریه ای دراین خصوص پذیرفته شده است؟امروزه جبران ضرر وزیان وارده به افراد قواعد ومبانی متعددی دارد که می بایست درباب مسئولیت مدنی پاسخ مقتضی را جست وجو نمود؛که دراین باب نظریاتی ازجمله نظریه تقصیر،خطر،مسئولیت محض ومسئولیت مطلق درحقوق وقواعد غرور واقدام درفقه مطرح شده است.

دراین پژوهش درصددآنیم تا ابتدا به تعریف اصطلاحات مرتبط پرداخته ،سپس به کلاهبرداری رایانه ای وامنیت بانکداری اشاره نموده وسپس به قوانین وبخشنامه ها دراین خصوص اشاره نموده ودرادامه مبانی ونظریات مسئولیت مدنی ونظرات وقواعد فقهی دراین خصوص را ذکر نموده ودرپایان نیز نتیجه گیری بحث را بیان نماییم.

درزمینه سابقه پژوهشی در موضوع معنونه مسئولیت مدنی بانک ها درقبال خسارات ناشی از عدم اجرای بخشنامه های بانک مرکزی تاکنون این موضوع به صورت دقیق مورد تبیین قرار نگرفته است؛لکن ، درموضوعات مشابه این موضوع مقالاتی چند توسط دکتر محقق داماد، خرم آبادی ، عبدالهی، قنبری، ملکوتی ومیرشکاری نگارش گردیده که دراین پژوهش حسب مورد اشاره خواهد شد.

تعاریف واصطلاحات

با توجه به اینکه درتمامی پژوهش ها یافتن درک صحیحی از موضوع، مستلزم ارائه تعاریفی چند ازموضوعات کلیدی آن می باشد؛دراین فصل برآنیم تا بطور مختصر تعاریفی از اصطلاحات بنیادین پژوهش ارائه نماییم:

- **مسئولیت:** در لغت "مسئولیت، مصدر جعلی از مسئول، ضمانت، ضمان، تعهد و مواخذه است.(دهخدا-۱۳۷۷) آنچه که انسان از وظایف و اعمال و افعال عهده دار و مسئول آن باشد". و در اصطلاح حقوقی مسئولیت" تعهد قانونی (قهری یا اختیاری) شخص درمقابل دیگری است خواه مالی باشد یا غیر مالی .که تقسیم بندی های گوناگونی ازمسئولیت در علم حقوق ارائه گردیده است که آنچه که دراین پژوهش مورد توجه است مسئولیت مدنی است.

- **مسئولیت مدنی:** دارای دو معنا عام وخاص می باشد .معنای عام آن که مترادف ضمان قهری می باشد که عبارتست ازتکالیفی که درنتیجه امر مشروع یا نامشروعی،بدون اینکه قرارداد صحیحی در میان باشد،پدید می آیدیا به عبارت دیگر الزام به پرداخت مالی یا انجام امری است،بدون اینکه الزام مزبور ناشی ازتراضی طرفین وقرارداد باشد. (صفایی،۱۳۹۶) ولی مسئولیت مدنی به معنای خاص عبارتست از تکلیف شخص به جبران زیانی که براثر عمل نامشروع(بجز غصب) به دیگری وارد شده است. (صفایی ،۱۳۹۶)که این مسئولیت مدنی به معنای خاص یا ناشی ازنقض قرارداد است یا ناشی از جرم یاشبه جرم .که مسئولیت قراردادی الزام به جبران خسارت ناسی از عدم اجرای تعهدات قرار دادی است ولی مسئولیت مدنی غیر قرار دادی الزام به جبران ضرر ناشی ازعمل زیان آور نامشروعی است که خارج ازقرارداد روی داده که ناشی از جرم(عمل نامشروع زیان آور عمدی اعم ازاینکه جرم کیفری باشد یا نه)وشبه جرم(عمل نامشروع زیان آور،غیرعمدی وناشی از بی احتیاطی وبی مبالاتی) است .(صفایی،۱۳۹۶)
- **بانک:** بانک نوعی مؤسسه مالی است که دارای مجوز به عنوان دریافت کننده سپرده‌هاست. دو نوع بانک وجود دارد: بانکهای تجاری و بانکهای سرمایه گذاری .در بیشتر کشورها، بانکها به‌وسیله دولت یا بانک مرکزی قانون گذاری می‌شوند.
- **بانکداری وفعالیت های بانکی:** مدیریت تجهیز و تخصیص منابع در بازار پول را بانکداری می‌گویند. مجموعه‌ای از فعالیت‌ها در عملیات بانکی، شامل سیاستگذاری و برنامه‌ریزی و سازماندهی و اجرا، نظام بانکداری نام دارد.فعالیت های بانکی نیز فعالیت هایی هستند که بانک ها در زمینه های اقتصادی وخدمت رسانی به مشتریان وجذب سرمایه انجام می دهند که این فعالیت ها ممکن است مستلزم حضور مشتری باشد یا بصورت غیر حضوری ومجازی این فعالیت ها انجام وخدمت رسانی صورت گیرد.

- **بانکداری مجازی:** بانکها برای اینکه بتوانند در بازار مالی از مزیت رقابتی بهره مند شوند و این مزیت را حفظ کنند، باید همواره بتوانند خود را با شرایط جدید سازگار کنند و فن آوری های جدید را بپذیرند. بانک مجازی بانکی مانند سایر بانک ها است، با این مزیت که قادر است خدمات خود به مشتریانش را به جای شعبه های فیزیکی در فضای مجازی (مانند اینترنت) ارائه کند. در یک بانک مجازی مشتریان و کاربران یکی شده و از طریق اینترنت از خدمات بانکی استفاده می کنند.نقطه اشتراک این بانکها با بانکهای سنتی حداقل در شروع کار شخصیت حقوقی مستقل، اساسنامه، هیأت مدیره و سرمایه و نقطه افتراق، دارایی های فیزیکی شناخته می شود.

بانک مجازی یک بانک رایانه ای است که قادر به انجام اکثر امور بانکی است که بانک های عادی انجام می دهند. با این تفاوت که نیازی به مراجعه به شعبه نخواهد بود و افراد از هر رایانه خانگی می توانند امور بانکی،تجارت و بازرگانی مورد نظر خود را به انجام برسانند. به عبارت دیگر در بانکداری مجازی، تمام مراحل، از واریز پول برای سپرده گذاری، تا دریافت و انتقال وجه، و مبادله اسناد بین بانکی با تمام کشورهای جهان و .... از طریق رایانه انجام می شود. همچنین اجرای قوانین ضدپولشویی و امنیت بالا و شفافیت مبادلات با راه اندازی این بانک ها میسر خواهد شد.بانک های مجازی نسل نوینی از بانکها بوده که با استفاده از آخرین دستاوردهای فن آوری اطلاعات و ارتباطات و بی نیاز از شعبه فیزیکی، خدمات و محصولات متنوع بانکی را به

عموم عرضه می نمایند. دسترسی ۲۴ ساعته (درهرزمان و هرمکان)، سهولت دسترسی، سرعت و امنیت از جمله مزیت های این قبیل بانکها است که آینده صنعت بانکداری را دگرگون خواهد ساخت.بانکهای مجازی درآینده نه چندان دور نقش بانک های فعلی را خواهند داشت؛ با این تفاوت که با تشکیل این بانک، به جای اینکه مشتری به صورت مستقیم به بانک مراجعه کند؛ به راحتی می تواند از طریق رایانه شخصی، امور بانکی خود را انجام دهد.بانک های مجازی بانک هایی دانش محور می باشند و با توجه به این که چابکی ، خلاقیت و ارائه خدمات در همه وقت و همه جا از ویژگی های بانک های مجازی به شمار می رود.

طرح موضوع

در این قسمت به بیان مسئله و طرح کلی موضوع اشاره نموده و سپس در مقام ارائه راه حل برخواهیم آمد.

کلاهبرداری رایانه ای

پیشرفت جوامع و به ویژه توسعه فناوری‌ها و فضای مجازی، سبب شکل‌گیری جرایمی شده که درگذشته نه چندان دور به این شکل وجود نداشتند؛ جرایمی که با شکل و شیوه خاص ارتکاب خود و در عین حال به دلیل تحققشان در ابعاد بسیار متنوع و گسترده، سبب شدند، کشورهای مختلف از جمله ایران، به تعریف و تبیین آن‌ها بپردازند و قوانین خاصی را نیز برای آنان ایجاد کنند .کلاهبرداری کامپیوتری یا رایانه‌ای (Cyber fraud) یکی از این جرایم است که در فضای مجازی ارتکاب می‌یابد. همان طور که از اسم کلاهبرداری رایانه‌ای پیداست، این جرم در محدوده‌ای خاص قابل ارتکاب است و آن هم در فضای مجازی و بین داده‌های رایانه‌ای و سامانه‌های کامپیوتری است. از همین نکته یکی از تفاوت‌های مهم این جرم با کلاهبرداری معمول و سنتی مشخص می‌شود. در کلاهبرداری سنتی باید جرم در دنیای واقعی رخ دهد و بزه‌دیده جرم فریب بخورد و مالش را در اختیار کلاهبردار قرار دهد اما در کلاهبرداری رایانه‌ای، کلاهبردار از طریق فضای مجازی و با تغییر دادن داده‌ها و اطلاعات فرد، حتی بدون آگاهی بزه‌دیده، اموال وی را تصاحب می‌کند، کلاهبرداری رایانه ای یکی از جرائم ناشی از سوء استفاده از فناوری اطلاعات است.فناوری اطلاعات پدیده منحصر به فرد عصر حاضر است که موجب پیشرفت و تغییر و تحول عظیم و عمیقی در تمام ابعاد و شئون زندگی انسان شده است.این پدیده با طرح مسائل جدید بسیاری از علوم را با چالش های جدی مواجه ساخته و آنها را تحت تاثیر قرار داده است. علم حقوق نیز با عنوان شاخه از علوم اجتماعی که تنظیم و تنسیق روابط انسان ها را در چارچوب حیات جمعی برعهده دارد،عمیقا تحت تاثیر فناوری اطلاعات قرار گرفته است. در این راستا این فضا امکان ارتکاب رفتار های مجرمانه جدیدی را به وجود آورده که قبل از این به هیچ وجه امکان پذیر نبوده است.کلاهبرداری رایانه ای از جمله جرائمی است که با پیدایش فناوری اطلاعات وارد عرصه حقوق شده است. (خرم آبادی ، ۱۳۸۶)

بنا به اعلام مراجع رسمی ذی صلاح براساس آمار در ده ماه اخیر جرایمی که بستر آن ها فضای مجازی است و جرایم رایانه ای محسوب می شوند،۱۴۰درصد افزایش داشته است و کلاهبرداری های رایانه ای با ۳۰۰ درصد رشد بیشترین جرم رایانه ای را در کشور رقم می زند.

کلاهبرداری رایانه ای جرمی است مستقل از کلاهبرداری کلاسیک که استفاده از رایانه و فضای مجازی محور اصلی این جرم است چرا که مرتکب از طریق رایانه متوسل به وسایل متقلبانه گردیده و دیگری را فریب می دهد و مال او را می برد و یا ممکن است که مرتکب بدون فریب قربانی و یا نماینده وی(که منظور در این پژوهش به طور خاص بانک مد نظر است) از طریق مداخله ناروا در داده های رایانه ای یا عملکرد سیستم های رایانه ای مال او را ببرد،یا از خدمات مالی متعلق به او بهره مند شود. جرم کلاهبرداری رایانه از جمله اولین جرایم رایانه ای است که نظام های حقوقی کشور های مختلف نسبت به آن عکس العمل نشان داده اند. در بین سوء استفاده های رایانه ای سوء استفاده از موجودی حساب ها و بیلان ها در بانک ها از طریق تاثیر بر عملکرد سیستم های رایانه ای عمده ترین جرایم هستند.در این میان ضرر و زیان ناشی از سوء استفاده از کارت های مغناطیسی و اعتباری از حجم وسیعی برخوردار است. (خرم آبادی ،۱۳۸۶)

در ایران برخی از اساتید بیان نموده اند که :«...اطلاق عنوان کلاهبرداری به برخی از انواع آنچه بعضا کلاهبرداری رایانه ای نامیده شده از قبیل دستکاری شخص در برنامه رایانه ای و انتقال پول از حساب خودش از نظر قانون ما خالی از اشکال نمی باشد واینگونه اعمال شاید به سرقت نزدیکتر باشد تا کلاهبرداری،چرا که نوعی ربایش مال غیر محسوب می شود.»(میر محمد صادقی ، ۱۳۹۵) لکن در ایران مطابق قوانین موجود اینگونه مواردکلاهبرداری رایانه ای محسوب شده است ؛ بدین شرح که مطابق ماده ۶۷ قانون تجارت الکترونیک مصوب ۱۳۸۲ مقرر شده است که :«هرکس در بستر مبادلات الکترونیکی با سوء استفاده و یا استفاده غیرمجاز از داده پیام ها،برنامه ها و سیستمهای رایانه ای و وسایل ارتباط از راه دور و ارتکاب افعالی نظیر ورود، محو، توقف، مداخله در عملکرد برنامه یا سیستم رایانه ای و غیره دیگران را بفریبد و یا سبب گمراهی سیستم های پردازش خودکار و نظایر آن شود و از این طریق برای خود یا دیگری وجوه،اموال یا امتیازات مالی تحصیل کند و اموال دیگران را ببرد مجرم محسوب و علاوه بر رد مال به صاحبان اموال به حبس از یک تا سه سال و پرداخت جزای نقدی معادل مال ماخوذه محکوم می شود.» و نیز وفق ماده ۱۳قانون جرایم رایانه ای مصوب ۱۳۸۸تصریح شده است که:«هر کس به طور غیرمجاز از سامانه های رایانه ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن،تغییر،محو،ایجاد یا متوقف کردن دادهها یا مختل کردن سامانه،وجه یا مال یا منفعت یاخدمات یا امتیازات مالی برای خود یا دیگری تحصیل کند،علاوه بر رد مال به صاحب آن،به حبس از یک تا پنج سال یا جزای نقدی از بیست میلیون ریال تا یکصد میلیون ریال یا هردو محکوم خواهد شد.»ولی با وجود جرم انگاری قانونگذار با توجه به گسترش روز افزون و جهانی شدن،اینترنت و تجارت های الکترونیکی اینگونه بزهکاری ها رو به افزایش است که نیازمند امنیت بانکداری الکترونیک است.که برای دستیابی به این مهم باید در حوزه های مدیریت امنیت کشور، مراکز تولیدی و سازمانهای مصرف کننده و بانک ها به عنوان ارتباط دهندگان مراکز مختلف ارتباط منطقی را به طور هماهنگ حفظ نموده و با آموزش و فرهنگ سازی در مورد امنیت و تلاش جهت بالابردن انگیزه استفاده از بانکداری و خدمات الکترونیکی شاهد پیشرفت اقتصادی کشور باشیم .شبکه ارتباط اینترنتی ناامن است و تبادل اطلاعات از طریق اینترنت بدون در نظر گرفتن موارد ایمنی خطرناک است و افراد غیرمجاز ممکن است به اطلاعات حساس در حین انتقال و یا بر روی سرویس دهنده های اینترنتی دسترسی پیدا کرده، آنها را تغییر و یا حذف کنند. از آنجاییکه، بانکداری الکترونیکی در بستر شبکه

و اینترنت انجام می شود لذا باید مکانیسمی جهت ضمانت انجام هر تراکنش بانکی که در آن داده های حساس مالی نیز رد و بدل می شود وجود داشته باشد.

امنیت بانکداری

اینترنت به عنوان یک شبکه عمومی، با مباحث جدیدی پیرامون محرمانگی و امنیت اطلاعات مواجه است. از این رو، بانکداری اینترنتی و آنلاین می‌تواند مخاطره‌های فراوانی برای موسسات و بنگاه‌های اقتصادی به همراه داشته باشد و این مخاطره‌ها با گزینش و انتخاب یک برنامه جامع مدیریت ریسک، قابل کنترل و مدیریت خواهد بود .

در حال حاضر حجم وسیعی از اطلاعات مالی، اعتباری و شخصی بر روی شبکه های مبتنی بر اینترنت در سرتاسر جهان ذخیره شده و می شود. از سوی دیگر از آنجایی که مسیر گردش اطلاعات و منابع روی شبکه بسیارند، لذا مشخص نمیباشد که اطلاعات مذکور کجا می روند و چه اشخاصی از آنها بهره برداری مینمایند. بدین ترتیب، حفظ امنیت اطلاعات از مباحث مهم تجارت و بانکداری الکترونیک به شمار می آید. هرچند امنیت مطلق وجود ندارد اما لااقل برای برخورداری از یک وضعیت غیرشکننده میباید هزینه هایی را صرف نمود.از جمله زیرساخت های مورد نیاز پیشبرد بانکداری الکترونیکی و روشهای نوین بانکداری به موارد ذیل می توان اشاره کرد:زیرساخت های امنیتی ،زیرساخت های فناوری و مخابراتی ،زیرساخت های اقتصادی، فرهنگی و آموزشی وزیرساخت های حقوقی و قانونی.امنیت یکی از زیرساخت های مهم در محیط تجارت الکترونیکی و بانکداری الکترونیکی است. تجربیات زیادی نشان می دهد که بیشتر افراد باتجربه سرمایه گذاری های خود را در محیط ایمن و مورد اعتماد حتی با سود کم به محیطی غیر ایمن با سود زیاد ترجیح می دهند. ریسک ها وتهدیدات مربوط به بانکداری الکترونیکی عبارتند از:دسترسی افراد غیرمجاز به به اطلاعات صاحبان حساب ها ،مشاهده صاحبان حساب به اطلاعاتی بیش از آنچه که مجاز هستند،صاحبان حساب یا دیگران توانایی انجام تراکنشها و اعمال غیر مجاز را داشته باشند،صاحب حساب تراکنشی را انجام دهد اما بعدا منکر آن شود، ویا بانکها انکار کنند که چنین تراکنشی انجام شده است ،حملات ناشی از ویروس ها و سایر کدهای مخرب ،رکوردهای اطلاعاتی در جریان تبادل اطلاعات یا از روی سرویس دهنده بانکهای اطلاعاتی ، به سادگی میتواند توسط افراد غیرمجاز دزدیده شوند، تغییر یابند و یا هر گونه پردازش غیر مجازی روی آنها صورت گیرد،کلمه و رمز عبور در جریان تبادل اطلاعات یا از روی سرویس دهنده به سادگی میتوا ند توسط افراد غیر مجاز (با تدارک دیدن حملات مختلف) دزدیده و جهت انجام حملات تکرار، تراکنش های غیر مجاز مالی و دیگر فعالیتهای غیر مجاز استفاده شوند ،حملهDOS به هر یک از سرور های فوق :ارسال درخواستهای بیش از حد به سرویس دهنده های مورد نظر، در کار آنها اختلال ایجاد کرده و باعث می شود که نتوانند به درخواستهای مجاز پاسخ دهند.

بزرگترین صدمه و آسیب و شکست یک سیستم به واسطه فعالیتهای افراد در سیستم می باشد حال می تواند صدمه افراد عمدی و یا غیرعمدی باشد همچنین اغلب اوقات سیستم ها دچار مشکل می شوند اما همه وضعیت ها باید برای سطح نفوذپذیر بازبینی شود تا بتواند با برنامه ریزی سطح نفوذ پذیر را تجزیه و تحلیل کرد. دستیابی کاربران به فایلهای داده را باید محصور کرد تا فقط با داشتن اختیارات به پردازش قابلیتها یا دستگاههای جانبی یا اعمالی نظیر خواندن،

نوشتن، اجرا کردن و حذف کردن پرداخت.روش کار مراقبت از کارکنان و کاربران غیر مجاز و ایجاد محدودیت درخواندن، کپی کردن، تغییر و یا حتی چاپ می باشد.فقط کاربران مجاز بتوانند اطلاعات ورودی و خروجی و وسایل را دریافت کرده یا آزاد کنند.بازرسی مداوم برای دریافت ورودی ها و خروجی های نفوذپذیر و حساس.روش کار کنترلها این است که جابجایی وسایل یا ارسال و چاپ خروجی ها را کنترل کنند.

اگر پشتیبانی تکنولوژی اطلاعات به صورت متناوب باشد شیوه ها و روشهایی برای ادامه وظایف و کارکردهای اضطراری پیشنهاد می کند. این شیوه ها (تدابیر احتمالی، تدابیر توقف داد و ستد و کسب وکار و پیوستگی تدابیر عملیاتی) باید با گرفتن نسخه پشتیبان، تدابیر بهبود دهنده، با هر سیستم پشتیبانی جامع شامل شبکه ها هماهنگ شود.تدابیر امنیتی باید مطمئن سازند که سیستم های واسطه شناخته شده اند و تدابیر احتمالی برای هر گونه حادثه هماهنگ شده باشد.ایجاد چندین محل برای قرار گرفتن نرم افزار بانکداری الکترونیکی یکپارچه به منظور افزایش قابلیت اعتماد کل سیستم تا در صورت بروز مشکل برای مرکز، مراکز پشتیبان دیگر فعال شده و ادامه فعالیت سیستم بانکداری الکترونیکی میسر شود.ایجاد سایت های پشتیبان و سرورهای مجزا در صورت قطعی شبکه و عدم دسترسی به پایگاه مرکزی برای شعب و استفاده از سیستم های منبع تغذیه بدون وقفه و ایجاد افزونگی های مناسب در خطوط ارتباطی برای مواقع قطعی جریان برق و یا شبکه.طراحی نرم افزار سیستم بانک الکترونیکی برای یک بانک خاص و عدم استفاده از سیستم بانک های کشورهای خارجی مانند FNS و ... که امکان استفاده خرابکارانه از این نرم افزار توسط ارائه دهندگان این محصولات و هکرها وجود خواهد داشت.ایجاد تدابیر مناسب به منظور احراز هویت و تایید مشتریان بانک های الکترونیکی.ایجاد تدابیر مناسب به منظور کنترل صدور مجوزبرای دسترسی به پایگاه های داده ها.ایجاد تدابیر مناسب به منظور حفاظت از یکپارچگی داده ها در معاملات و تراکنش ها در بانکداری الکترونیکی.ایجاد تدابیر و استراتژی های مناسب به منظور حفظ محرمانه بودن اطلاعات کلیدی بانکداری الکترونیکی و عدم استفاده از اطلاعات کلیدی بانک ها توسط مراجع غیرمجاز و سو استفاده و افشای غیر مجاز اطلاعات.استفاده از ابزارهای مناسب تامین امنیت :رمزنگاری کلید عمومی، رمزنگاری کلید خصوصی، زیر ساخت کلید عمومی، امضای دیجیتال و توابع در هم ساز.استفاده از توابع درهم ساز، کارت هوشمند، امضای دیجیتالی، گواهی های دیجیتال از تکنیک های مورد استفاده در ایجاد صحت داده می باشند که از الگوریتم های رمزنگاری نامتقارن و الگوریتم های درهم ساز استفاده می کنند.سازگار بودن عمل احراز هویت و تصدیق اصالت با استراتژی کلی بانک در مورد بانکداری اینترنتی و سرویس های مشتریان در تجارت الکترونیکی و استفاده از چندین فاکتور پیاده سازی جهت تصدیق اصالت و احراز هویت مانند Pin code و روشهای بیومتریک به صورت همزمان و استفاده از معماری لایه به لایه امنیت و سایر کنترل ها جهت کاهش ریسک.استفاده از پروتکلهای SSLو TLS برای حفظ امنیت تراکنش ها و برقراری ارتباطی امن .تشخیص تمام تراکنش ها و سطوح دسترسی مرتبط با برنامه و سرویس های تحت وب مشتری.بررسی و قضاوت در مورد کارایی تکنیک های موجود، کاهش ریسک و تغییر فاکتورهای ریسک برای هر نوع تراکنش و سطوح دسترسی؛ از جمله موارد مهم در راستای امنیت بانکداری الکترونیکی می باشد.

ارائه خدمات پشتیبانی ۲۴ ساعته و ۷ روز هفته باعث می شود خطاهایی از قبیل کوتاهی و ناتوانی در انجام تراکنش با مشتری یا وجود نقص در نرم افزارها و برنامه های بانکداری الکترونیکی، نقص در سخت افزار سرورها و پایگاه داده کاهش یابد. در نتیجه، به شهرت و اعتبار بانک ها لطمه وارد نمی شود و اعتماد مشتریان از دست نمی رود.ایجاد امکانات بازرسی و حسابرسی برای تشخیص تهاجمات، شستشوی پولی، به خطر افتادن رمز عبور، سایر فعالیتهای غیر مجاز و موسسات مالی باید بر روی لایه های چندگانه کنترل برای جلوگیری از کلاهبرداری و حفاظت از اطلاعات مشتریان تکیه کنند.

اگرچه این موارد درصد ارتکاب جرایم کلاهبرداری رایانه ای را به صفر نمی رساند لکن درکاهش چشمگیر آنها موثر خواهد بود وبانک ها نیز میبایست جهت حفظ سرمایه از این امنیت برخوردار شده و آن را ایجاد،حفظ و ارتقا دهند.

مسائل قانونی ،حقوقی وفقهی مسئولیت بانک ها

همانطور که اشاره گردید کلاهبرداری رایانه ای از عمده ترین جرایم رایانه ای هستند که مراجع ذی صلاح مهم ترین دلیل ارتکاب آن را عدم التزام کامل بانک ها به بخشنامه های بانک مرکزی بیان نموده اند.بعنوان مثال، در خصوص جایگزینی رمز پویا با رمز ایستا به هنگام فعالیت مجازی مشتریان بانک ها ،بانک مرکزی جمهوری اسلامی ایران طی بخشنامه شماره ۹۸/۵۱۶۹۱ مورخ ۹۸/۰۲/۲۱ به تمامی بانک ها و موسسات اعتباری اعلام نمود که :«...در خصوص جایگزینی رمز های پویا به جای رمز های ایستا در پرداخت های بدون حضور کارت و با توجه به لزوم ارتقا سطح امنیت پرداخت های مردم و جلوگیری از تضییع حقوق سپرده گذاران ...موارد زیر جهت توجه دقیق و اجرای مفادآن ابلاغ می گردد:

۱) از ابتدای خرداد ماه تامین امنیت مشتریان نظام بانکی در تراکنش های بدون حضور کارت برعهده بانک ها بوده و هرگونه مسئولیت سوء استفاده از حساب های مشتریان به دلیل آسیپ پذیری های امنیتی در سیستم های بانکی مستقیما بر عهده بانک بوده و در این موارد تایید مرجع قضایی برای جبران خسارت مشتریان کفایت می کند.

۲) جایگزینی رمز های پویا به جای رمز های ایستا به عنوان یکی از برنامه های ارتقای سطح امنیتی نظام بانکی مطرح بوده و با توجه به این که امنیت بخش لاینفک هر خدمتی است،نباید هیچ هزینه ای از دارندگان کارت و مشتریان بانکی اخذ شود.

۳) بانک ها می توانند با قبول مسئولیت هرگونه سوء استفاده از مسائل امنیتی و جبران خسارات احتمالی وارد شده به مشتریان،برای تراکنش های کم مقدار(با سقف کمتر از پنج میلیون ریال در روز برای تمام تراکنش ها) و همچنین تراکنش هایی که ذی نفع آن دستگاه های عمومی ـ نظیر صادرکنندگان قبض ـ باشد،استفاده از رمز ایستا را مجاز تلقی نماید.

۴)در صورتی که بانک بتواند راه حل مطمئن دیگری را،که با تایید بانک مرکزی متضمن تایید هویت قوی مشتری پیش از برداشت از حساب مشتری باشد را اجرایی نماید،می تواند از این راهکار به عنوان جایگزین رمز پویا استفاده به عمل آورد.

۵)هرگونه فرایند تامین امنیت پرداخت های بدون حضور کارت باید با انجام هزینه های منطقی و معقول و مطابق با قیمت تمام شده فنی در آن بانک به صورت یک زیرساخت دائمی صورت گرفته و صرفه و صلاح بانک به طور کامل در آن مد نظر قرار گیرد.

۶)به منظور پشتیبانی حداکثری از مشتریان ضرورت دارد امکانات ارائه رمز محدود به استفاده از برنامه های کاربردی گوشی های هوشمند نشده و ارائه آن از طریق سایر ابزار ها نظیر پیامک،پیام رسان های داخلی مجاز و نظایر آن برای مشتریان بانک ها نیز حسب تشخیص بانک فعال گردد.» ونیز در آبان ماه وآذر ماه همان سال نیز بانک مرکزی دراطلاعیه ای با تاکید بربخشنامه های قبلی خود بانک هارا ملزم نموده است که ازدی ماه همان سال رمز پویا را جایگزین رمز ایستا نمایند.لکن شایان ذکراست که در این اطلاعیه ها نیز به مسئولیت بانک ها درقبال عدم اجرای صحیح این اطلاعیه اشاره نشده است.

علیرغم تاکیدات مکرر بانک مرکزی بعنوان مرجع عالی که وظیفه سیاست گذاری و نظارتی در نظام پولی و بانکی کشور را دارد ؛ بانک ها به منظور جذب مشتری و سهولت استفاده از رمز های ایستا برای مشتریان در بادی امر از اجرای کامل این بخشنامه خودداری نموده و آن را اختیاری و منوط به استفاده از برنامه های کابردی گوشی های هوشمند نموده،حال آنکه مطابق بخشنامه اجرای آن اجباری و با توجه به آنکه تمامی مشتریان بانک ها از گوشی های هوشمند برخوردار نبوده بخشنامه اجرای آن را از طرق دیگر پیش بینی نموده بود؛لکن،بانک ها به قصد ترغیب مشتریان برای استفاده از سایر خدمات بانک ارائه رمز پویا را منوط به نصب نرم افزار های بانکی نموده اند که این امر عملا اجرای ناقص بخشنامه فوق بوده و نشانگر مقاومت بانک ها و موسسات مالی و اعتباری در این زمینه بود و به همین سبب بسیاری از مشتریان راغب به استفاده از رمز پویا نبوده و آن را مشقت بار می دانستند. اگرچه امروزه با توجه به بخشنامه های مراجع نظارتی پس از ورود خسارات به مشتریان بانک ها و موسسات مالی و اعتباری لاجرم این امر را اجرا نمودند ؛لکن، همچنان با تعیین محدودیت مبلغ ، عدم تامین امنیت برنامه های کاربردی ارائه کننده رمز پویا ، مجددا ملاحظه می کنیم که این بخشنامه کامل اجرا نشده و همچنان شاهد ورود خسارات به مشتریان از این حوزه هستیم.

حال مسئله این است که با توجه به اینکه بانک ها زمینه را برای اجرای بخشنامه های اینچنینی فراهم ننموده اند اگر از طریق عدم اجرای این بخشنامه خسارتی بر شخصی متصور گردد آیا می توان بانک را مسئول دانست یا خیر؟ برای پاسخ بایستی بیان نمود که:بطور مثال؛مطابق بند های ۱و۳بخشنامه مارالبیان مسئولیت مطلق بانک ها در عدم اجرای مفاد این بخشنامه را بیان نموده است. (خواه بانک آن را اجرا ننماید یا ترتیبی اتخاذ کند که اجرای آن با مشقت فراوانی همراه باشد که نتیجه آن عملا عدم اجرای بخشنامه باشد) و نیز مطابق بخشنامه دادستانی محترم کل کشور که اعلام نموده است که: «دادستان‌های عمومی و انقلاب سراسر کشور ؛با توجه به اینکه به موجب بخشنامه شماره ۹۷/۱۸۶۷۱۷ مورخ ۹۷/۰۶/۰۱ و بندهای ۱ و ۳ بخشنامه شماره ۹۸/۵۱۶۹۱ مورخ ۹۸/۰۲/۲۱ و شماره ۹۸/۱۶۳۵۷۵ مورخ ۹۸/۰۵/۱۴ بانک مرکزی، ارائه خدمات غیر حضوری (نظیر تراکنش‌های بانکی اینترنتی) در بانک‌ها ضرورتاً مستلزم استفاده از رمزهای پویا بوده و از تاریخ ۹۸/۰۳/۰۱ هرگونه استفاده از رمزهای دوم ایستا در تراکنش‌های غیر حضوری ممنوع اعلام و ادامه بکارگیری رمز دوم ایستا از مصادیق آسیب پذیری امنیتی

خدمات بانکی محسوب شده و به عنوان ضمانت اجرا مقرر داشته است که «هر گونه سوءاستفاده از حساب‌های مشتریان به دلیل آسیب پذیری‌های امنیتی (ناشی از عدم اجرای الزامات رمزهای پویا) در سرویس‌های بانکی مستقیما به عهده بانک بوده و در این موارد تأیید مرجع قضایی (دادسرا)، برای جبران خسارت مشتریان کفایت می‌کند.»لذا مقتضی است در پرونده‌های کلاهبرداری رایانه‌ای (برداشت غیرمجاز از حساب‌های بانکی) که پس از الزامی شدن استفاده از رمزهای پویا تشکیل شده است بررسی‌های لازم انجام شود و در صورت احراز انجام تراکنش مجرمانه با رمز دوم ایستا به لحاظ عدم رعایت بخشنامه بانک مرکزی وعدم رفع آسیب پذیری امنیتی، دستور پرداخت خسارت بزه دیده صادر و از طریق سامانه کاشف به بانک متخلف ابلاغ گردد،مسئولیت خسارات وارده به مشتریان برعهده بانک هاباشد وبانک ها خسارات را به مشتریان پرداخت نموده وخود بانک ها به دنبال دریافت خسارت از کلاهبردار باشند.» مشاهده می شود که موارد فوق نمونه ای از بخشنامه ها در راستای الزام بانک ها در جهت امنیت بانکداری مجازی و جلوگیری از ورود خسارت به مشتریان می باشد که جهت حمایت از افراد زیان دیده مسئولیت بانک ها در قبال خسارات وارده مطلق قلمداد شده و بانک ها مطلقا مسئول جبران خسارات وارده به مشتریان در این زمینه می باشند.

بر اساس بند ج ماده ۳۵ قانون پولی و بانکی کشور،هر بانک در مقابل خساراتی که در اثر عملیات آن متوجه مشتریان می شود مسئول و متعهد جبران خواهد بود.بر اساس ظاهر ماده صرف اثبات رابطه سببیت میان عملیات بانک و خسارت مشتری بسنده بوده و نیازی به احراز تقصیر بانک نمی باشد. (میرشکاری ، ۱۳۹۲)

در باب مسئولیت مدنی بانک ها در کلاهبرداری های رایانه ای چون این کلاهبرداری ها در فضای سایبر صورت می پذیرد باید در خصوص مسئولیت بانک ها در فضای سایبر بحث و بررسی نماییم.در فضای سایبر دو دسته بازیگر به عنوان واسطه های اینترنتی با مصادیق رساها(واسطه های الکترونیک که وظیفه شان ایجاد امکان دسترسی به اینترنت برای کاربران و مصرف کنندگان نهایی است)،مدیران سایت و کاربران یا بهره برداران نهایی اینترنت ایفای نقش می کنند که هرکدام برای مسئولیت مبنای مستقلی دارند.شاید در بادی امر به نظر برسد که بر مسئولیت رساها مبنای تقصیر حاکم است چون نقش اینان واسطه صرف است و صرفا در موارد تقصیر مسئول می باشند یعنی چون رساها سبب ورود خسارت می شوند و مباشر آن نیستند و مطابق نظریه مشهور در تسبیب آنچه موجب تحقق مسئولیت است وجود رکن تقصیر است بنابراین مسئولیت ایشان مبتنی بر نظریه تقصیر خواهد بود.علاوه بر آن،ماده۷۸قانون تجارت الکترونیک مصوب ۱۳۸۲ مقرر می دارد:«هرگاه در بستر مبادلات الکترونیکی در اثر نقص یا ضعف سیستم موسسات خصوصی و دولتی،... خساراتی به اشخاص وارد شود موسسات مزبور مسئول جبران خسارت می باشند...» لکن در حقیقت رساها به مثابه پلی هستند که ورود کاربر را به دنیای سایبر ممکن می سازند بدون اینکه نقشی در همراهی او در این فضا داشته باشند.با توجه به این نوع عملکرد،اول و باالذات اصل عدم مسئولیت مدنی این نوع واسطه هاست.لکن مسئولیت این رساها مطابق بند ۴_۳_۵_آیین نامه واحد های ارائه کننده خدمات اطلاع رسانی و اینترنت،مصوب ۱۳۸۰شورای عالی انقلاب فرهنگی تنها در خصوص ایجاد امکان و اعمال برقراری پالایه(فیلترینگ)در شبکه خواهد بود که در صورت عدول از انجام وظایف

یعنی ارتکاب تقصیر مسئول خواهد بود.مدیران و اداره کنندگان سایت(بانک) نیز در صورت عدم رعایت مقررات و ضوابط ایمنی و عدم شناسایی مخرب(کلاهبردار)و عدم امکان جبران زیان،مدیر سایت(بانک) که مقتضی جبران زیان را فراهم کرده است(عدم اجرای بخشنامه) برای تحمل زیان استحقاق بیشتری دارد که مسئولیت مدنی او بر مبنای نظریه تقصیر است ولی باید اشاره نمود که اگر کاربر(مشتری)خود در کلاهبرداری مقصر باشد(ارائه اطلاعات کارت به دیگری) برمبنای نظریه تقصیر بتوان خود را مسئول دانست.(ملکوتی و ساوارایی،۱۳۹۵)

آنچه که در کلاهبرداری رایانه ای مورد کلاهبرداری واقع می شود پول مشتری است،پولی که شخص به بانک سپرده است و ذمه بانک در قبال بازپرداخت آن مدیون شده است و حال اگر آن پول به نحوی از انحا تلف شود ذمه بانک به صورت کلی مشغول و مدیون است و بانک باید در صدد جبران برآید.مسئولیت بانک در قبال مشتری می تواند هم از جنبه قراردادی و هم غیر قراردادی باشد.مطابق موارد بیان شده فوق الذکر که مسئولیت را مبتنی بر تقصیر دانسته است باید بیان نمود که بانک تنها در صورت مقصر بودن مسئول است که این را در رابطه با بانک تنها می توان بر مسئولیت قراردادی تحلیل کرد لکن در مسئولیت غیر قراردادی بهتر است به جای نظریه تقصیر از رابطه استناد عرفی و انتساب برای مسئول دانستن بانک استفاده نمود.لکن بهتر است با توجه به اینکه در ماده ۱ قانون حمایت از مصرف کننده که مصرف کننده را هرشخص حقیقی یا حقوقی که کالا یا خدمتی را خریداری می کند تعریف نموده است مشتریان بانک را نیز مصرف کننده به حساب آورد به ویژه آن که تعریف بند ۲ماده ۱ از مفهوم عرضه کننده که کلیه عرضه کنندگان کالا و خدمات را شامل این عنوان می داند،مشمول خود بانک ها نیز دانست مهم تر آنکه ماده۱۶ این قانون صراحتا موسسات دولتی و بانک ها را ملزم به رعایت مقررات این قانون و جبران خسارت وارده به کلیه مصرف کنندگان کرده است و نیز همانطور که اشاره گردید وفق بند ج ماده۳۵ قانون پولی و بانکی بانک را در هر صورت مسئول دانسته است و ماده ۷۸ قانون تجارت الکترونیک نیز بر این امر تاکید دوچندان کرده است،مسئولیت بانک ها را مسئولیت محض(مسئولیتی است که مبتنی بر وجود یا اثبات تقصیر در عامل زیان یا فعل زیان بار نیست و صرف ایراد ضرر برای عامل آن ایجاد مسئولیت می کند) دانست.(محقق داماد ، ۱۳۹۷)

از طرفی به نظر می رسد که مسئولیت بانک در قبال مشتریان نوعی مسئولیت حرفه ای است که ترکیبی از مسئولیت قراردادی و قانونی بوده و آن را مسئولیت قانونی می نامیم.به علاوه مسئولیت بانک در مقابل مشتری،نوعی مسئولیت محض بوده و صرف استناد خسارت به بانک،موجب مسئولیت اوست.بانک،طبق قرارداد منعقده در مقابل مشتری ملزم به انجام تراکنش به طور صحیح است و برای تحقق این نتیجه،در قبال اعمال تمام کسانی که با وی همکاری می کنند از جمله بانک واسط یا مرکز پایاپای و متصدی خدمات مخابراتی مسئول است که به این امر در سطوح بین المللی نیز در اسناد «راهنمای آنسیترال در خصوص انتقال الکترونیکی وجوه سال۱۹۸۷»و «قانون نمونه انتقال بین المللی آنسیترال سال۱۹۹۴»اشاره شده است.که ایران نیز با تاسی از این اسناد در «دستورالعمل صدور دستور پرداخت و انتقال وجوه مصوب۱۳۸۵» و«مقررات ناظر بر ارائه دهندگان خدمات پرداخت مصوب۱۳۹۰»به این مقررات اشاره نموده است.که همگی آن ها حاکی از آن است که بانک در مقابل مشتری هم دارای رابطه قراردادی است و هم الزامات قانونی برعهده دارد یعنی علاوه بر قرارداد بین بانک و مشتری به موجب مقررات نیز الزاماتی برای بانک ها در نظرگرفته شده است که

بانک به لحاظ حرفه ای ملزم به رعایت آن ها است که بانک بایستی با توجه به تخصص خود کلیه خسارات احتمالی ناشی از خطاهای شغلی خود را پیش بینی نموده و مسئول کلیه زیان های ناشی از اعمال خود باشد که هدف از آن ها حمایت از مشتریان است.قانون گذار بانک را ملزم به انجام صحیح تراکنش و مدیریت صحیح و نگهداری از وجوه مشتری و حفظ امنیت سامانه دانسته و در صورت تخلف از این تکلیف وی را ملزم به جبران خسارت می نماید.مسئولیت بانک در این خصوص نوعی مسئولیت محض است یعنی صرف استناد خسارت به عملیات بانکی برای الزام بانک به جبران،کافی است و اثبات بی تقصیری او یا تقصیر عوامل دیگر موجب رفع مسئولیت بانک نمی شود و تنها عاملی که می تواند بانک را از مسئولیت معاف سازد،اثبات قوه قاهره یا مشارکت زیان دیده در وقوع خسارت است(مستنبط از ماده ۴ قانون عملیات بانکی بدون ربا مصوب۱۳۶۲ که بانک ها را مکلف به بازپرداخت اصل سپرده های مشتریان نموده است و ماده ۳۸موافقت نامه عضویت در ساتنا که اشاره به مسئولیت کامل بانک ذی نفع نموده است)در دعوای مطالبه خسارت علیه بانک مشتری مکلف نیست تعهداتی را که توسط بانک نقض شده اند،توصیف نموده و یا قانونی یا قراردادی بودن آن را تعیین کند بلکه اگر نقض تعهد را به لحاظ موضوعی اثبات نماید کافی است.(عبداللهی ، ۱۳۹۶)

در دعوای میان بانک و مشتری به نظر می رسد که بار اثبات دعوا در امور الکترونیک برعهده بانک قرار داشته باشد(صرف نظر از اینکه بانکی مدعی باشد یا مدعی الیه)چرا که مشتری نسبت به ادله موجود دسترسی ندارد و تمامی اطلاعات نزد بانک می باشد چرا که از نحوه انجام عملیات اطلاعات کامل دارد و اسناد و مدارک عملیات و معاملات مشتریان تماما در دسترس بانک می باشد و حتی اگر مشتری دارای این اطلاعات باشد توان اطلاعات آن ها را ندارد. (قنبری ،۱۳۹۱)

علاوه بر موارد حقوقی و قانونی گفته شده می توان با استناد به قاعده فقهی غرور«هرگاه از شخص عملی صادر گردد که باعث فریب خوردن شخص دیگری بشود و از این رهگذر ضرر و زیانی متوجه او گردد،شخص نخست به موجب این قاعده ضامن است و باید از عهده خسارت وارد برآید.»(محقق داماد،۱۳۹۶)عمل بانک که با ایجاد سیستم مشکل دار یا عدم اجرای مقررات (بخشنامه)مشتری را مبنی بر امنیت شبکه بانکی فریب داده است از نوع غرور عملی«یعنی شخص فریب دهنده با انجام دادن عملی موجب مغرور شدن دیگری می شود.»(قاسم زاده ، ۱۳۷۷)بوده و صدق عرفی اغراء برای مسئولیت بانک کافی است و مطابق قاعده اقدام(هرگاه شخصی با توجه و آگاهی،عملی را انجام دهد که موجب ورود زیان به او گردد اگر وارد کننده زیان،شخص دیگری باشد،مسئول خسارت نخواهد بود یعنی شخص(بانک) با اقدام خود موجب از بین رفتن مال شده است. (محقق داماد ، ۱۳۹۶)بانک علی رغم الزام بانک مرکزی جهت فعال سازی رمز پویا از انجام آن به صورت اجباری نسبت به مشتریان خودداری ورزیده و به صورت عرفی این ترک فعل بانک سبب کلاهبرداری و ورود خسارت به مشتری گردیده است که به نوعی بانک خود با اقدام خود این امر را موجب گردیده است و نیز بنا به نظر فقها از جمله حضرت امام خمینی(ره) که در تحریرالوسیله اعلام نموده اند که سپرده ها(امانات و ودیعه ها) که صاحبان آن ها به بانک می پردازند نزد بانک امانت بوده و بانک مکلف به امانت داری است و در صورت تلف ضامن است.(خمینی (ره)،۱۳۹۲) می توان نظر به مسئولیت بانک ها در قبال خسارات ناشی از کلاهبرداری های رایانه ای داد که مشتری برای جبران خسارات وارده به بانک رجوع نموده و بانک نیز خود حسب مورد به شخص زیان زننده(که ممکن است

شخص ثالث بوده یا کارمند بانک بوده که بانک از باب کارفرمایی مطابق مواد ۱۱ و۱۲ قانون مسئولیت مدنی ضامن باشد)رجوع نماید.

در سایر کشور ها نیز اصل بر مسئولیت مدنی محض بانک ها بوده به طوریکه در انگلستان بنا به مسئولیت اشخاص حرفه ای در قبال مشتریان،لزوم رعایت احتیاط بانک ها در قبال مشتریان،انتظارات خاص از امین در مواردی که بانک ها تراستی حقوقی هستند مسئولیت بانک ها در قبال مشتریان مسئولیت محض خواهد بود. (محقق داماد ،۱۳۹۷)

بحث و نتیجه‌گیری

امروزه پیشرفت جوامع و به ویژه توسعه فناوری‌ها و فضای مجازی سبب گردیده است که همه اشخاص حقیقی و حقوقی چاره ای جز انجام امور مالی خود در بستر شبکه بانکی الکترونیکی نداشته باشند،و این امر سبب شکل‌گیری جرایمی شده که درگذشته نه چندان دور به این شکل وجود نداشته اند؛جرایمی که با شکل و شیوه خاص ارتکاب خود و در عین حال به دلیل تحققشان در ابعاد بسیار متنوع و گسترده، کشورهای مختلف از جمله ایران، به تعریف و تبیین آن‌ها پرداخته اند و قوانین خاصی را نیز برای آنان ایجاد کرده اند .کلاهبرداری کامپیوتری یا رایانه‌ای (Cyber fraud) یکی از این جرایم است که در فضای مجازی ارتکاب می یابد.ارتکاب کلاهبرداری رایانه ای سبب ورود زیان هایی به اشخاص می شود که تعیین تکلیف زیان های وارده به اصل و سود مشتریان تحت عنوان مسئولیت مدنی بانک ها یکی از به روز ترین مسائل حقوقی دنیا به شمار آید.برای ورود به این مباحث به عنوان پیش فرض باید پذیرفت اگر پولی نزد بانکی سپرده شود و از آن پول به هر نحوی استفاده شود چون پول بر ذمه می آید و عینیت ندارد و صرفا اعتبار است،بانک به ذمه مدیون می شود و اگر آن پول تلف شود ذمه بانک کماکان مشغول است؛لذا ید امانی بانک در اینجا کارایی نخواهد داشت و بانک باید درصدد جبران برآید.مبنای مسئولیت بانک ها در قبال مشتریان مسئولیت قراردادی است که در حقوق ایران بر اساس قرارداد خسارت قراردادی بایستی جبران شود.بانک ها مبتنی بر نظریه انتساب مسئول جبران خسارات می باشند مگر اینکه ثابت نمایند قصور یا تقصیر مشتری در تسهیل یا مباشرت در خسارت وارده موثر بوده که در آن صورت صرفا در مقابل آن مشتری معاف از مسئولیت خواهند بود. با توجه به مباحث معنونه و مطروحه می بایست بیان نمود که وفق بند ج ماده ۳۵ قانون پولی و بانکی و مواد ۶۷ و ۷۸ قانون تجارت الکترونیک و ماده۱۳ جرایم رایانه ای و ماده ۴ قانون عملیات بانکی بدون ربا و مستنبط از قانون حمایت از مصرف کنندگان و بخشنامه های صادره از سوی بانک مرکزی و دادستانی کل کشور و سایر آیین نامه ها و دستورالعمل های موجود و قواعد فقهی غرور و اقدام مسئولیت بانک ها،مسئولیت محض بوده و در صورت ورود خسارات بانک ها مکلف به جبران آن خسارات در قبال مشتریان هستند.

امروزه با توجه به قوانین و قواعد فقهی بیان شده می توان حکم به مسئولیت محض بانک ها در قبال خسارات وارده بر مشتریان داد لکن با توجه به اینکه در قوانین به صورت صریح به این موضوع اشاره نشده است ممکن است سبب عروض شبهه در این حکم گردد که برای رفع معضلات پیچیده شرعی و حقوقی می توان پیشنهاد

های ذیل را مطرح نمود:آگاه سازی مردم در خصوص استفاده از بانکداری الکترونیکی و رعایت نکات امنیتی این فضا؛الزام بانک ها به اجرای نص صریح بخشنامه بانک مرکزی و مرقانون ؛ الزام بانک ها به ایجاد فضای امن در بانکداری الکترونیک ؛ استفتاء از مراجع تقلید برای تبیین فقهی مسئله در مورد عدم نیاز به اثبات تقصیر بانک ها برای جبران ضرر مشتریان و مسئولیت محض بانک ها ؛ اصلاح قوانین پولی و بانکی یا بانکداری بدون ربا که به صراحت مسئولیت مسئولیت بانک ها در قبال مشتریان را خارج از ضوابط کلی مسئولیت مدنی به شمار آورد ؛ اصلاح قانون حمایت از مصرف کننده با هدف تبیین رابطه خاص حمایتی مشتریان در قبال بانک.

منابع

۱_ خرم آبادی عبدالصمد ،کلاهبرداری رایانه ای از دیدگاه بین المللی و وضعیت ایران،فصلنامه حقوق دانشکده حقوق و علوم سیاسی،شماره۲، سال ۱۳۸۶

۲_ خمینی(ره)سید روح الله،۱۳۹۲،ترجمه تحریرالوسیله،جلد دوم،موسسه نتظیم و نشر آثار امام خمینی(ره)

۳_ دهخدا علی اکبر، ۱۳۷۷،لغت نامه، تهران، موسسه انتشارات وچاپ دانشگاه تهران

۴_ صفایی سید حسین،۱۳۹۶،مسئولیت مدنی،ویراست سوم،انتشارات سمت

۵_ عبدالهی محبوبه،تحلیل مسئولیت حقوقی بانک انتقال دهنده در انتقال الکترونیکی وجوه،دو فصلنامه دانشنامه حقوق اقتصادی دوره جدید،شماره۱۲،سال بیست و چهارم،پاییز و زمستان ۱۳۹۶

۶_ قاسم زاده سید مرتضی ،رابطه غرور و تقصیر، دیدگاه های حقوقی ،شماره ۱۰ و ۱۱، ۱۳۷۷

۷_ قنبری حمید،معکوس نمودن بار اثبات دعوا مبنای مسئولیت در رابطه بین بانک و مشتری در بانکداری الکترونیکی،پژوهش های پولی_بانکی،شماره۱۲،تابستان ۱۳۹۱

۸_ محقق داماد سیدمصطفی،۱۳۹۶،قواعد فقه بخش مدنی،ویرایش چهارم،مرکز نشر علوم اسلامی

۹_ محقق داماد سید مصطفی_ مرادی یاسر،تحلیل مسئولیت بانک ها در قبال مشتریان؛موانع و راهکار ها،فصلنامه علمی پژوهشی اقتصاد اسلامی،شماره۷۲،سال هجدهم،زمستان ۱۳۹۷

۱۰_ ملکوتی رسول_ساوارایی پرویز،درامدی برمسئولیت مدنی در فضای سایبر،فصلنامه پژوهش حقوق خصوصی،شماره پانزدهم،سال چهارم،تابستان۱۳۹۵

۱۱_ میرشکاری عباس،مسئولیت مدنی بانک ها،فصنامه مطالعات آرای قضایی، دوره دوم،شماره ۱، بهار۱۳۹۲

۱۲_ میرمحمد صادقی حسین،۱۳۹۵،جرایم علیه اموال،ویراست دوم،انتشارات میزان