بررسی تطبیقی تخصیص خطر تراکنش غیرمجاز در بانکداری الکترونیک (نظام حقوقی ایران و آمریکا)

زهرا ایوبی[۱]، مرتضی شهبازی‌نیا[۲]*، محمد عیسائی تفرشی[۳]، حسن بادینی[۴]

۱. دانشجوی دکتری گروه حقوق خصوصی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران
۲. دانشیار گروه حقوق خصوصی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران
۳. استاد گروه حقوق خصوصی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران، ایران
٤. دانشیار حقوق خصوصی دانشکده حقوق و علوم سیاسی، دانشگاه تهران، تهران، ایران

دریافت: ۱۳۹۷/۰۹/۰۵ پذیرش: ۱۳۹۸/۰۳/۲۹

چکیده

از کارکردهای اساسی بانکداری الکترونیک، انتقال وجه به‌عنوان یکی از ابزارهای مهم پرداخت است که در حال حاضر به دلایل گوناگون از گستره فراوانی در حوزه تجارت برخوردار است. با این حال، تقلب و صدور دستورهای پرداخت غیرمجاز به‌کارگیری این ابزار را با تهدید روبرو کرده است. پژوهش حاضر به دنبال یافتن پاسخی مناسب به نحوه تخصیص خطر تراکنش غیرمجاز و بررسی مسؤولیت طرفین معامله در حوزه بانکداری الکترونیکی است که با استفاده از روشی تحلیلی و توصیفی و استنتاج منطقی به بررسی تطبیقی نظام‌های ایران و آمریکا خواهد پرداخت. نتایج پژوهش نشان خواهد داد که تراکنش غیرمجاز بدون اختیار واقعی یا ظاهری مشتری محقق می‌شود؛ مضافاً در مواردی که انتقال بر اساس رویه امنیتی پیشنهادی مشتری باشد غالباً مشتری مسؤول فرض می‌شود. اهداف تخصیص خطر ازجمله کاهش خسارت، ایجاد انگیزه و... را ترکیبی از رویکردهای محتمل تخصیص خطر تأمین می‌کند، بدین نحو که ضمن پذیرش مسؤولیت بانک، تعیین سقف

* نویسنده مسؤول مقاله: Email: Shahbazinia@modares.ac.ir

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

محدود برای مسؤولیت مشتری مانع سهل‌انگاری مشتری در حفظ و نگهداری ابزار دسترسی و کدهای دست‌یابی شود. از دیگر نتایج این تحقیق آن است که نظام حقوقی ایران در این حوزه نوپا است و نیاز به تدوین مقررات جامع وجود دارد و به‌رغم اینکه طبق مقررات اصل بر مسؤولیت بانک است لیکن رویه قضایی مشتری را مسؤول قلمداد می‌کند.

واژگان کلیدی: انتقال الکترونیکی وجوه، تراکنش غیرمجاز، تخصیص خطر، بانک، مشتری.

۱. مقدمه

پرداخت از طریق انتقال الکترونیکی وجوه به‌عنوان چهره نوینی از روش‌های پرداخت به‌طور فزاینده‌ای در حال گسترش است. علی‌رغم سهولت و سرعت در این روش، با توجه به چارچوب قانونی نامشخص استفاده از این روش با خطراتی ازجمله تقلب و سو استفاده روبرو است.

از آنجایی که سابقه بانکداری الکترونیکی در ایران به سال ۱۳۵۰ برمی‌گردد، نظام حقوقی در این حوزه، نهادی نوپا است به‌گونه‌ای که موقعیت طرفین را در وضعیت غیرقابل‌پیش‌بینی قرار می‌دهد. یکی از جنبه‌های اهمیت این موضوع از حیث حقوقی، عدم تعیین موقعیت طرفین در تراکنش‌های غیرمجاز است که منجر به دغدغه و نگرانی‌ها در این حوزه شده است.

در نوشتار حاضر به‌صورت تطبیقی نظام‌های حقوقی آمریکا و ایران را در این باره بررسی می‌کنیم. پس از تبیین مفهوم تراکنش غیرمجاز و بررسی اهداف تخصیص خطر به دنبال پاسخ به این پرسش هستیم که رویکرد نظام حقوقی ایران و آمریکا در تخصیص خطر تراکنش غیرمجاز چیست؟ و نهایتاً مسؤولیت طرفین در تراکنش غیرمجاز چگونه است؟ لذا در مقام پاسخگویی به این مسائل با استفاده از روشی تحلیلی و توصیفی و استنتاج منطقی، پس از تبیین مفهوم انتقال غیرمجاز و

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

رویکردهای مطرح در تخصیص خطر تراکنش غیرمجاز، به بررسی و تحلیل نظام‌های حقوقی ایران و آمریکا در این حوزه پرداخته می‌شود.

۲. مفهوم و معیار تراکنش غیرمجاز

اصطلاح انتقال یا تراکنش الکترونیکی وجوه از حیث فنی به استفاده از رایانه یا وسایل مخابراتی جهت ایجاد یا اجرایی کردن فرآیند پرداخت تعریف می‌شود (جعفری زاده؛ احمدی راد، ۱۳۹۱، ص ۱٦۱-۱٦۰) در ذیل مفهوم و معیارهای تشخیص تراکنش غیرمجاز بررسی می‌شود.

۲-۱. مفهوم تراکنش غیرمجاز

فنّاوری انتقال الکترونیکی وجوه مملو از فرصت‌هایی برای تراکنش غیرمجاز است. تقریباً تمام سیستم‌های انتقال الکترونیکی وجوه قادر به تأیید هویت واقعی دستوردهنده نیستند؛ چراکه هنگام دریافت دستور پرداخت افراد قابل رؤیت نیستند (BROADMAN, 1979, p.254) و احراز دستور از طریق رویه امنیتی صورت می‌گیرد؛ لذا برای تعریف انتقال غیرمجاز الکترونیکی ابتدا باید این مسأله در نظر گرفته شود که موسسه مالی بر چه اساس اقدام به اجرای دستور مشتری می‌کند (Geva, 2003, p. 224). انتقال ممکن است طبق دستور واقعی مشتری یا نماینده وی صورت گیرد؛ در این موقعیت بحثی در خصوص صحت دستور پرداخت وجود ندارد و دستور مجاز محسوب می‌شود؛ لیکن هنگامی‌که انتقال بدون اجازه واقعی مشتری صورت گیرد صحت جواز دستور پرداخت مورد مناقشه و بحث است. در این صورت چند فرض ممکن است مطرح شود.

الف. دستور بر اساس اجازه ظاهری یا صوری مشتری

ب. فقدان اجازه مشتری و منطبق با رویه امنیتی

ج. فقدان اجازه مشتری و عدم انطباق با رویه امنیتی

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

۲-۲. معیار تراکنش غیرمجاز

صدور اجازه از سوی مشتری ممکن است واقعی یا صوری باشد. اجازه واقعی بر اساس ابراز رضایت اصیل به نماینده است (Algudah, 1992, p. 263). درواقع نماینده زمانی اختیار واقعی دارد که اصیل نسبت به ایجاد اختیارات و نمایندگی رضایت داشته باشد. در این مورد میان اینکه رضایت به‌طور صریح[۱] بیان‌شده باشد یا به نحو ضمنی[۲] تفاوتی وجود ندارد. اختیار ظاهری یا صوری مربوط به زمانی است که رابطه نمایندگی میان اصیل و نماینده وجود ندارد و رفتار یا گفتار اصیل به‌گونه‌ای باشد که شخص ثالث استنباط کند که نماینده واجد اختیار است. (مافی؛ کدیور، ۱۳۹۳، ص ۲۷-۲۸) به‌طور مثال اگر مشتری ابزار دسترسی به‌حساب بانکی خود ازجمله کارت‌بانکی، اطلاعات بانکی و... را در اختیار دیگری قرار دهد و وی اقدام به سو استفاده از این ابزار کند (Geva, 2003, p. 230). در چنین حالتی آیا انتقال مجاز است یا خیر؟

۲-۲-۱. نظام حقوقی آمریکا

حقوق آمریکا در ارتباط با تراکنش‌های مصرف‌کننده در بند الف- ۱۲ ماده ۱۶۹۳ قانون فدرال انتقال الکترونیک وجوه،[۳] انتقال غیرمجاز الکترونیکی وجوه را بدین گونه تعریف کرده است: «انتقال الکترونیکی وجهی از حساب مصرف‌کننده[٤] توسط شخصی غیر از مصرف‌کننده یا بدون اجازه واقعی از وی و مصرف‌کننده از این

۱. Express

۲. Implied

۳. The Federal Electronic Fund Transfer Act §1693

٤. مراد از مصرف‌کننده، مشتری است.

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

انتقال نیز بهره‌ای نصیبش نشود». بعلاوه در قانون صداقت در قرض[1] استفاده غیرمجاز از کارت‌های اعتباری را چنین تعریف کرده است: «استفاده از کارت اعتباری توسط شخصی جز دارنده کارت که اجازه واقعی یا صوری از دارنده نداشته باشد و از این استفاده دارنده کارت سودی عایدش نشود»[2] (Algudah, 1992, p. 264) (Rusch, 2008, p. 586). طبق هر دو تعریف فوق هنگامی‌که مشتری از تراکنش سودی نصیبش شود نمی‌تواند ادعای غیرمجاز بودن را مطرح کند؛ لذا انتقال الکترونیکی مجاز نه‌تنها شامل انتقال ارادی می‌شود بلکه شامل معاملاتی نیز می‌شود که مصرف‌کننده برای شخص ثالثی امکان دسترسی به حسابش را فراهم ساخته است؛ بنابراین اگر مصرف‌کننده کارت یا شناسه شخصی خود را به یکی از دوستان یا خویشاوندان خود بدهد و شخص اخیر مبلغی را از حساب بدون رضایت وی خارج سازد، مصرف‌کننده خود باید خسارت ناشی از اختیار اعطایی را بر دوش بکشد. (السان، ۱۳۹۲، ص ۲٦۲-۲٦۳) در پرونده فردریک علیه سیتی بانک[3]، دادگاه رأی داد که تراکنش زمانی غیرمجاز است که علاوه بر اینکه مشتری یا شخص مأذون از سوی وی اقدام به تراکنش نکرده و سودی عایدش نمی‌شود؛ مشتری، با اعطای کارت، رمز عبور یا سایر ابزار دسترسی به مرتکب امکان دست‌یابی به‌حساب خود را فراهم نکرده باشد.

در تراکنش‌های تجاری تجزیه‌وتحلیل انتقال غیرمجاز با بررسی رویه امنیتی آغاز می‌شود. مفهوم رویه امنیتی ازجمله مفاهیم کلیدی در ماده ٤ الف قانون متحدالشکل تجاری آمریکا و بهره‌گیری از آن نیز نقش اساسی در تخصیص خطر ایفا می‌کند

---

۱. The Truth in Lending Act.

۲. U.S.C. 1603(0)

۳. Frederick P. Ognibene, Plaintiff,v. Citibank, N. A. Defendant. December 9, 1981

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

(French, June 1990, p.1426). رویه امنیتی، رویه توافقی بین مؤسسه مالی و مشتری است که برای بررسی و سنجش صحت دستور مشتری و تشخیص خطا در انتقال با محتوای سفارش پرداخت ملاک قرار می‌گیرد (Robert Ludwig, Salvatore Scanio, Joseph Szary, October 2010, p. 109)

بر مبنای قواعد کلی، اصل اصالت ظاهر[۱] و قاعده استاپل[۲] درجایی که اجازه وجود دارد نماینده واجد اختیار فرض می‌شود (Thevenoz, 1990, p. 281)؛ لذا هنگامی‌که اجازه ظاهری وجود دارد دستور مجاز است. لیکن مادام که اجازه وجود ندارد صحت دستور بر اساس رویه امنیتی توافقی فی‌مابین طرفین تعیین می‌شود. (Algudah, 1992, p. 266) در این صورت چند فرض ممکن است پیش می‌آید:

۲-۲-۱-۱. توافق بر رویه پیشنهادی بانک

بانک ملزم به استفاده از رویه امنیتی مناسب و پیشنهاد آن در زمان انعقاد قرارداد به مشتری است. در صورت پذیرش مشتری بررسی دستور پرداخت طبق آن رویه صورت می‌پذیرد. روش امنیتی مورد توافق باید از لحاظ تجاری معقول و متعارف باشد. تشخیص معقول و متعارف بودن به درخواست‌ها، شرایط مشتری، میزان، نوع و مقدار تراکنش‌های مشتری بستگی دارد (Hargitai, 2015, p. 212). در ماده ٤ الف قانون متحدالشکل تجاری آمریکا تعریف و معیار خاصی از رویه امنیتی به عمل نیامده است (Rogers, 2004, p. 477) و مفهوم آن از مجرای رویه قضایی در حال تکامل و غالباً متمرکز بر موارد ذیل است:

الف) شرایط توافقنامه بانک و مشتری

---

۱. Prime Facie

۲. Estoppel

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

ب) آیا روش امنیتی با دستورالعمل‌های بانکی مطابقت دارد یا خیر.
ج) آیا بانک اقدامات امنیتی را در ارتباط با معامله انجام داده است یا خیر. (Salvatore & Ludwig, April 2013, p. 4)

در صورت طرح ادعای تراکنش غیرمجاز، بانک باید اثبات کند که مطابق رویه امنیتی اقدام کرده و دستور منطبق است که در این موقعیت دو حالت ممکن است پیش آید: دستور منطبق با رویه امنیتی باشد یا اینکه منطبق نباشد (Robert Ludwig, Salvatore Scanio, Joseph Szary, 2010, p120,)

۲-۲-۱-۱-۱. دستور منطبق بر رویه امنیتی متعارف تجاری

مطابق قانون متحدالشکل تجاری آمریکا[۱] اگر دستور پرداخت غیرمجاز باشد ممکن است بانک به شرط اثبات موارد ذیل مسؤولیتی نداشته باشد:

۱. توافق بانک و مشتری بر رویه امنیتی
۲. رویه امنیتی مورد توافق تجاری متعارف باشد
۳. اقدام بانک بر مبنای رویه امنیتی
٤. بانک روند انطباق را بر اساس توافقنامه کتبی یا دستورالعمل مشتری بررسی کرده باشد.
٥. حسن نیت بانک در پذیرش دستور پرداخت

در صورت عدم احراز شروط فوق، بانک مسؤول هر تراکنش غیرمجازی تلقی می‌شود. معذلک، حتی باوجود و اثبات شروط مزبور چنانچه محرز شود شخص متقلب، اطلاعات محرمانه را از طریق مشتری، عامل یا نماینده مشتری و یا از منابع تحت کنترل مشتری تحصیل‌نکرده مسؤولیت ضرر به بانک منتقل می‌شود (Salvatore & Ludwig, 2013, p 4).

---

۱. U.C.C. § 4A-202

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

۲-۲-۱-۱-۲. عدم انطباق دستور با رویه امنیتی متعارف تجاری

در فرضی که بانک از رویه امنیتی پیروی نکرده باشد درهرصورت مسؤول تلقی می‌شود. در پرونده شرکت برادفورد علیه بانک تگزاس[1] بابت قصور و سهل‌انگاری بانک در تبعیت از رویه امنیتی که اگر از آن استفاده می‌کرد ممکن بود از خسارت ۸۰۰۰۰۰ دلاری احتراز شود بانک مشتری[2] مسؤول تلقی شد. هرچند که شماره‌حساب اعلامی متعلق به ذینفع نبود و بانک ذینفع[3] متوجه این مسأله نشده بود و این امر خطا و قصور بانک ذینفع بود، اما ازآنجاکه بانک مشتری از رویه امنیتی جهت تشخیص و تأیید دستور پرداخت پیروی نکرده بود سهل‌انگاری بانک مشتری به‌عنوان سبب تراکنش غیرمجاز شناخته شد (Geva, 1997, p. 208)؛ لذا در فرضی که دستور پرداخت منطبق با رویه امنیتی متعارف تجاری نباشد تراکنش غیرمجاز لحاظ می‌شود.

۲-۲-۱-۲. توافق بر رویه امنیتی منتخب مشتری

اگر رویه متعارف ارائه شده از سوی بانک به دلایل گوناگون ازجمله سختی و گران بودن توسط مشتری رد شود و وی به‌صورت کتبی متعهد به پذیرش تمام مسؤولیت های دستور پرداخت ارسالی شود بانک مسؤولیتی در قبال پرداخت‌های غیرمجاز ندارد (Geva, 1997, p. 207).

---

۱. Bradford Trust Co v Texas Am Bank, 790 F 2d 407 (5th cir 1986).

۲. Customer's Bank

۳. Beneficiary Bank

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

۲-۲-۲. نظام حقوقی ایران

نظام حقوقی ایران در حوزه انتقال الکترونیکی وجوه نهادی نوپا است؛ به‌گونه‌ای که مقررات منسجم و نظام‌مندی در این حوزه تدوین‌نشده است معذلک در حوزه تجارت الکترونیک و بانکداری الکترونیکی مقرراتی تبیین شده است؛ لذا برای تحلیل و تبیین روابط بین بانک و مشتری علاوه بر مقررات مذکور به قواعد عمومی حاکم بر قراردادها و قراردادهای بین بانک و مشتریان نیز باید مراجعه کرد.

در هیچ‌یک از مقررات، تعریفی از تراکنش غیرمجاز به عمل نیامده است. لیکن مطابق دستورالعمل صدور دستور پرداخت و انتقال وجه، مؤسسه مالی صادرکننده بایستی دستور پرداخت را پس از تأیید و قبل از قبول، هویت صادرکننده را احراز کند[۱] (جلالی؛ الشریف؛ فصیحی زاده؛ جلالی، ۱۳۹۶، ص ۵۵۱).

بعلاوه مستنبط از دستورالعمل چگونگی شناسایی مشتریان مؤسسات اعتباری، مصوب شورای عالی مبارزه با پول‌شویی موسسه مالی قبل از انجام تراکنش‌های مالی، مکلف به شناسایی مشتری خود و احراز هویت وی است.[۲] لذا هر پرداختی که بدون تأیید و شناسایی مشتری صورت گیرد غیرمجاز و نامعتبر تلقی می‌شود.

نحوه احراز اعتبار دستور پرداخت در قانون تجارت الکترونیک به شرح ذیل مقررشده است:

الف. موافق با رویه ایمن:

---

۱. ماده ۱۲ دستورالعمل صدور دستور پرداخت و انتقال وجه

۲. ماده ۱۱ دستورالعمل چگونگی شناسایی مشتریان ایرانی مؤسسات اعتباری

ماده ۱۳ دستورالعمل چگونگی شناسایی مشتریان خارجی مؤسسات اعتباری

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

چنانچه دستور پرداخت مطابق با رویه ایمن[1] باشد چند حالت قابل‌تصور است:

۱. دستور واقعی مشتری:

«دستور توسط خود مشتری، سیستم اطلاعاتی برنامه‌ریزی‌شده و یا تصدی خودکار از جانب مشتری ارسال شود».

۲. نماینده واقعی:

دستور توسط شخصی ارسال‌شده باشد که از جانب مشتری مجاز به این کار بوده است.

۳. نماینده ظاهری:

«*داده‌پیام* دریافت شده توسط مخاطب از اقدامات شخصی ناشی شده که رابطه‌اش با اصل ساز، یا نمایندگان وی باعث شده تا شخص مذکور به روش مورداستفاده اصل ساز دسترسی یافته و داده‌پیام را به‌مثابه داده‌پیام خود بشناسد».[2]

در هر سه فرض فوق دستور مجاز قلمداد می‌شود؛ لیکن قانون‌گذار در خصوص نمایندگی ظاهری استثنائی مطرح کرده است که در مبحث آتی به آن پرداخته می‌شود.

ب. توافق بر رویه ایمن منتخب مشتری:

مطابق قانون مزبور رویه امنیتی منتخب مشتری بدین گونه تعریف‌شده است که: «چنانچه قبلاً به‌وسیله مشتری روشی معرفی و یا توافق شده باشد که معلوم کند آیا «داده‌پیام» همان است که وی ارسال کرده است.»[3] در این مقرره اگرچه نگارش به نحوی است که در ابتدا فرض می‌شود اگر یکی از دو شرط حاصل شود رویه

---

۱. بند ط ماده ۲ قانون تجارت الکترونیک: رویه‌ای است برای تطبیق صحت ثبت داده‌پیام، منشأ و مقصد آن با تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله، محتوا و یا ذخیره‌سازی داده‌پیام

۲. بند ب ماده ۱۹ قانون تجارت الکترونیک

۳. بند الف ماده ۱۹ قانون تجارت الکترونیک

مورداستفاده رویه منتخب مشتری منظور می‌شود لیکن برای اینکه رویه‌ای، رویه امنیتی منتخب مشتری محسوب شود بایستی هر دو شرط در مقرره فوق را دارا باشد.

در ادامه قانون‌گذار در فروضی که دستور پرداخت از طریق رویه منتخب مشتری یا نمایندگی ظاهری صادرشده باشد؛ لیکن فی‌الواقع از سوی مشتری صادر نشده باشد یا به‌طور اشتباه صادرشده باشد را از حکم دستور مجاز مستثنی کرده، اما حکم آن را بیان نکرده است. در ابتدا چنین دستوراتی را مجاز و منتسب به مشتری قلمداد کرده سپس با ذکر این قید که اگر توسط مشتری ارسال نشده باشد آن را مستثنی کرده و فقط دستوراتی که از سوی مشتری یا نماینده واقعی وی صادرشده باشد مجاز و مؤثر قلمداد شده‌اند. درنتیجه می‌توان چنین استنباط کرد که در تمام حالات مذکور دستور معتبر است مگر اینکه مشتری بتواند اثبات کند که دستور از سوی وی یا نماینده‌اش صادر نشده است و به‌نوعی این مقرره در ارتباط با بار اثبات دعوا مؤثر در مقام است؛ لذا در حقوق ایران اگر دستور مطابق با رویه ایمن باشد و توسط مشتری صادرشده باشد دستور مجاز محسوب می‌شود. در غیر این صورت هرچند دستور مطابق رویه باشد (رویه ایمن یا رویه منتخب مشتری) ولی مشتری بتواند اثبات کند که دستور توسط وی یا نماینده واقعی‌اش صادر نشده غیرمجاز محسوب می‌شود.

۳. تخصیص خطر

تأیید اعتبار الکترونیکی یک وسیله قانونی برای مشروع کردن اقدامات شخص یا نسبت دادن به آن فرد است ولی منجر به شناسایی فرد نمی‌شود. فی‌الواقع شبیه کلید درب است که ورود به ساختمان و سیستم را آسان می‌کند و موجب شناسایی فرد نمی‌شود. در هر پرداختی ممکن است دستوردهنده فرد غیرمجازی باشد که

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

غیرقانونی به ابزار و اطلاعات دسترسی یافته در این موارد پرداخت نسبت به موسسه مالی معتبر شناخته می‌شود چراکه موسسه مالی قادر به تعیین هویت نیست. باوجوداین ممکن است خسارت‌های زیادی به مشتری وارد شود و وی همیشه قادر به حفاظت از خویش نباشد. برعکس تخصیص چنین خسارتی به موسسه مالی احتمال توزیع مؤثر ضرر و خسارت را در پی دارد و موسسه مالی تشویق به استفاده از سیستم و فناوری طراحی‌شده برای تأیید اعتبار بر اساس اطلاعات بیومتریک که شناسایی افراد و دستور پرداخت را آسان‌تر و مطمئن‌تر می‌کند (Geva, 2003, p. 228-229).

در صورت تراکنش غیرمجاز وجوه، بین مشتری و مؤسسه مالی چه کسی مسؤول جبران خسارت است؟ و به چه میزان؟

۳-۱. اهداف

دانش حقوق به دنبال بهره‌گیری از ابزارهای مقبول اقتصادی و استخدام بهترین قاعده از میان قواعد هم‌عرض و جایگزین دیگر در راستای بهینه‌سازی و انعطاف‌پذیری قواعد حقوقی است (الماسی، زمستان ۱۳۹۱، ص ۱۰).

ازآنجاکه هدف اصلی هر مقرره قانونی ایجاد و افزایش اجرای عدالت است (Geva, 2003, p. 210) قواعد مورداستفاده برای تخصیص خطر ضمن در نظر گرفتن شرایط بازار و تنظیم روابط طرفین باید منجر به اجرای عدالت شود. لازمه ارائه ساختار حقوقی مناسب در بدو امر تعیین اهداف است تا راهکار مناسبی بتوان ارائه داد.

۳-۱-۱. ایجاد تعادل بین هزینه‌ها

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

در ارزیابی اهداف موردبررسی برای ایجاد ساختار تخصیص خطر در انتقال الکترونیکی وجوه غیرمجاز، یکی از اهداف موردتوجه ایجاد تعادل فی‌مابین هزینه‌های عملیاتی سیستم انتقال الکترونیکی وجه و امکان اجرای مقررات تخصیص خطر است (Rusch, 2008, p. 590). درعین‌حال چارچوب مقررات باید تعادلی میان منافع افراد درگیر در معامله ایجاد کند (Geva, 2003, p. 210).

اگر مجموع قواعد پیشنهادی بدون افزایش قابل‌توجه در هزینه معامله، منجر به جلوگیری از خسارت بیشتر شود سیستم کارآمدتر و نهایتاً منتج به تسهیل فعالیت اقتصادی می‌شود (Rusch, 2008, p. 590-591).

۳-۱-۲. شفاف‌سازی

هدف دیگر از تعیین تخصیص خطر، شفاف‌سازی است؛ به‌گونه‌ای که استفاده‌کنندگان از سیستم مطلع باشند در معرض چه خطراتی هستند (Rusch, 2008, p. 591-592). درنتیجه تشویق می‌شوند تدابیری برای جلوگیری از ابتلا و تحقق خطر بیاندیشند (Rusch, 2008, p. 593).

۳-۱-۳. کاهش خسارت

قاعده تعیین و تخصیص مسؤولیت در صورتی کارآمد است که طرفین را به اتخاذ تدابیر و اقدامات پیشگیرانه‌ای که برابر با سطح احتیاط مقتضی و لازم باشد سوق دهد که هزینه کل را به حداقل برساند (رحمتی؛ خودکار، ۱۳۹۱، ص ۱۱۶).

۳-۱-۴. ایجاد انگیزه

از لحاظ اقتصادی یکی از اهداف تخصیص خطر کارآیی اقتصادی آن است. این هدف از طرق مختلف قابل تأمین است ازجمله توزیع خطر، درونی کردن هزینه‌های خارجی و بازدارندگی اقتصادی که درواقع با ایجاد انگیزه برای افراد جهت در پیش گرفتن

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

اقدامات احتیاطی که ازنظر هزینه قابل توجیه باشد محقق می‌شود. (بادینی، ۱۳۹۲، ص ۳۹۶)

۳-۱-۵. ایجاد اعتماد و اطمینان برای استفاده از این ابزار

ارتکاب تقلب در حوزه انتقال الکترونیکی وجوه، نه‌تنها خلاف نظم و مصلحت عمومی است، بلکه یک تهدید بالقوه خطرناک، برای کارآیی تجاری این ابزار نیز به شمار می‌رود. همانند هر ابزار تجاری، رواج و شیوع این معاملات قائم به اعتماد کاربران آن است. اگر احتمال سوءاستفاده از ابزار مزبور کاهش نیابد با کاهش کارآمدی اقتصادی، اعتماد به آن نیز رو به افول خواهد نهاد (بنانیاسری، ۱۳۸۵، ص ۳۵۷-۳۵۸).

۳-۲. رویکردهای محتمل در تخصیص خطر تراکنش غیرمجاز

در نظام‌های حقوقی، با توجه اهداف موردنظر، عوامل مختلفی در تعیین مبنای مسؤولیت مدنی موردتوجه قرار می‌گیرد تا قاعده‌ی مطلوب‌تر انتخاب شود (طهماسبی؛ علیپور، ۱۳۹۰، ص ۱۲۹).

در حال حاضر خسارت‌های زیادی در اثر عدم تخصیص خطر مناسب در حوزه بانکداری پرداخت می‌کنیم (Dolan, 2003, p.273.) که منتج از عدم‌حمایت حقوقی مناسب از مصرف‌کننده و عدم پیش‌بینی تبعات متأثر از اعمال رژیم نامناسب است.

برای بهره‌مندی از هر وسیله پرداختی طرفین متحمل هزینه‌هایی می‌شوند که به هزینه معامله منسوب هستند (Robert D. Cooter Edward L. Rubin, 1987, p. 67) یکی از هزینه‌ها، زیان ناشی از خطر تقلب است که نظام حقوقی با توجه به اهداف به دنبال ارائه راهکار تخصیص خطر دراین‌باره است. برای تخصیص تلفات، چارچوب اقتصادی باید لحاظ شود رویکرد اقتصادی مناسب رویکردی است که کارآیی در

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

رسیدن به هدف معین با هزینه کم را دارا باشد (Robert D. Cooter Edward L. Rubin, 1987, p. 67). در ذیل رویکردهای مختلف در تخصیص ریسک و ضرر در انتقال غیرمجاز الکترونیکی وجوه را مطرح و بررسی می‌کنیم.

۳-۲-۱. شخصی که در بهترین موقعیت قرار دارد[۱]

یکی از رویکردها برای تخصیص خطر می‌تواند تحمیل ضرر به شخصی باشد که در موقعیت بهتری در جلوگیری از خطر یا به حداقل رساندن ضرر قرار دارد. (Rusch, 2008, p. 561) این رویکرد می‌تواند یکی از مهم‌ترین و تأثیرگذارترین تدابیر در تخصیص خطر باشد. (Geva, 2003, p. 211)

زیرا گاه زیان‌دیده از این امکان برخوردار است که مانع وقوع زیان شده یا میزان آن را کاهش دهد. (طهماسبی؛ علیپور، ۱۳۹۰، ص ۱۳۱) طبق این رویکرد بانک مسؤول فرض می‌شود چراکه فرصت و توانایی بانک برای پیشگیری از وقوع تقلب بیشتر است؛ زیرا ابزار و اطلاعات بیشتری نسبت به مشتری در اختیار دارد. تنها جایی که ممکن است مشتری بتواند از وقوع تراکنش غیرمجاز جلوگیری کند حفظ ابزار دسترسی و اطلاعات و رمز دستیابی به‌حساب بانکی و اطلاع‌رسانی به بانک در هنگام مفقودی یا سرقت ابزار دسترسی یا وقوع انتقال غیرمجاز است. در غیر این حالات بانک در موقعیت و وضعیت بهتری نسبت به مشتری قرار دارد.

۳-۲-۲. توزیع ضرر

اگر اساس سیاست توزیع گسترده خطر و ضرر باشد قاعده تخصیص خطر برای تراکنش غیرمجاز خیلی ساده بود و بر اساس قاعده توزیع گسترده خطر، ضرر بین دیگر افراد توزیع می‌شد (Rusch, 2008, p. 592). به‌طور مثال بانک می‌تواند

---

۱. Best a voider

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

به‌صورت تخمینی احتمال وقوع تقلب و انتقال غیرمجاز را پیش‌بینی کند و آن را به‌عنوان کارمزد انتقال بر تمام انتقال‌های وجوه توزیع کند.

منطق و اساس توزیع خطر برای بدهی غیرمجاز به‌عنوان هزینه انجام معامله قابل‌قبول است اما منجر به ایجاد انگیزه برای حفظ اطلاعات و رعایت مسائل امنیتی از سوی مشتری و استفاده از رویه مناسب امنیتی و فناوری‌های جدید از سوی بانک و درنتیجه کاهش هزینه‌های عملیاتی سیستم پرداخت نمی‌شود (Rusch, 2008, p 592-593)؛ لذا چنین رویکردی اهداف ایجاد انگیزه و کاهش خسارت در تخصیص خطر را تأمین نمی‌کند.

۳-۲-۳. مسؤولیت محض

مسؤولیت محض، مسؤولیتی است که مبتنی بر وجود یا اثبات تقصیر در عامل زیان یا فعل زیان‌بار نیست صرف ایراد ضرر برای عامل آن ایجاد مسؤولیت می‌کند و جز با اثبات فقدان رابطه سببیت و انتساب ضرر به قوای قاهره معافیت از مسؤولیت ممکن نیست. (بادینی؛ شعبانی کندسری؛ رادپرور،۱۳۹۱، ص ۲۱) در حوزه بانکداری مسؤولیت محض برای مشتری و بانک قابل‌طرح است.

۳-۲-۳-۱. مشتری

چنانچه بر مبنای مسؤولیت محض، مشتری را مسؤول بدانیم منتج به مسائل و زیان‌های عدیده بیشتر می‌شود چراکه بانک خود را مبرا از هرگونه مسؤولیتی فرض می‌کند و تلاشی در جهت اعمال رویه امنیتی مناسب نمی‌کند. از سوی دیگر، مسؤول زیان‌ها باید مؤسسات مالی باشند نه مصرف‌کنندگان؛ زیرا جعل یا تغییر اقلام دستور پرداخت می‌تواند بخش قابل‌توجهی از ثروت یک فرد باشد ولی برای موسسه مالی معمولاً ناچیز است. مضافاً مؤسسه مالی قادر به پیش‌بینی میزان تراکنش‌های

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

غیرمجاز و توزیع ضرر و زیان در میان گروه بزرگی از مصرف‌کنندگان است. البته اگر مشتریان چنین خسارت‌هایی را بیمه کنند متحمل چنین ضررهایی نمی‌شوند (Robert D. Cooter Edward L. Rubin, 1987, p. 71).

۳-۲-۳-۲. بانک

چنانچه بانک مسؤول فرض شود می‌تواند موجب تلاش بیشتر وی در جهت کاهش تلفات و افزایش ایمنی شود (Dolan, 2003, p. 288) و منجر به پیشگیری از خطر می‌شود مگر اینکه فرض شود که مشتری بزهکار باشد که این باعث می‌شود بانک برای شناخت بیشتر مشتری خود انگیزه یابد (Rusch, 2008, p. 593)؛ لیکن در مقابل، منجر به افزایش سهل‌انگاری شدید مشتری و عدم رعایت ایمنی در حفظ ابزار دسترسی و تسهیلات دسترسی به حساب می‌شود که این امر نیز منتهی به افزایش خسارت و هزینه می‌شود.

۳-۲-۴. مسؤولیت محدود

پیش‌بینی مسؤولیت محدود برای یکی از طرفین معامله یکی از رویکردهای مطرح است. این رویکرد در نظام حقوقی آمریکا با مسؤولیت محدود مشتری پیش‌بینی‌شده است.

چنین رویکردی دارای نقاط مثبت و منفی است. ازاین‌جهت که محرک و مشوق بانک و مشتری برای جلوگیری از ایجاد ضرر و خسارت می‌شود رویکرد مناسبی است.

۳-۲-۵. تعیین شخص مقصر

با پذیرش تقصیر به‌عنوان مبنای مسؤولیت، عامل زیان فقط هنگامی در برابر زیان‌دیده مسؤول است که مقصر باشد(طهماسبی؛ علیپور، ۱۳۹۰، ص ۱۳۷). این

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

رویکرد از رویکرد توزیع خطر بسیار پیچیده‌تر است. چراکه باید معیارهایی جهت تشخیص تقصیر و سهل‌انگاری ارائه داد (Robert D. Cooter Edward L. Rubin, 1987, p. 73).

معیار تعیین قاصر؛ می‌تواند عدم رعایت مراقبت معمول باشد که نسبت به مشتری حفظ و رعایت موارد ایمنی نگهداشت ابزار دسترسی و رمز... و برای بانک استفاده از رویه امنیتی مناسب و به کار بردن فناوری‌های جدید جهت حفظ حقوق مشتری است.

این رویکرد ممکن است منجر به تضییع حقوق مشتری شود چراکه مشتری ابزار و اطلاعاتی جهت اثبات ادعای خود در اختیار ندارد. از طرف دیگر برای بانک می‌تواند اثبات قصور و سهل‌انگاری مشتری پیچیده و بغرنج باشد (Thevenoz,, 2015, p. 25).

۳-۲-۶. شخص منتفع

این رویکرد بر مبنای نظریه خطر مطرح می‌شود، مطابق آن ایجادکننده محیط خطرناک منتفع از شیء و فعل زیان‌بار می‌بایست خطر ناشی از آن را نیز تحمل کنند. (بابایی، ۱۳۸۱، ص ٥٦) مع‌هذا، بانک با ارائه خدمات بانکداری الکترونیکی از یک‌سو، بستر خطرناکی را ایجاد کرده و از سوی دیگر، استفاده‌کننده بزرگ این فعالیت‌هاست و باید خطر ناشی از آن را بپذیرد. مبنا قرار دادن چنین رویکردی موجب خواهد شد تا بانک‌ها برای ارتقا سیستم‌های امنیتی خود تلاش بیشتری کند (دیلمی؛ فیروزبخت؛ ۱۳۹٦، ص ۲٥٤).

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

۳-۳. رویکرد نظام‌های حقوقی در تخصیص خطر

در این مبحث رویکرد نظام‌های حقوقی ایران و آمریکا در این حوزه بررسی و تحلیل می‌شود.

۳-۳-۱. نظام حقوقی آمریکا

در حقوق آمریکا در تراکنش‌های مصرف‌کننده سقف مشخصی برای مسؤولیت مشتری در نظر گرفته‌شده است و تنها خطایی که برای مشتری پیش‌بینی‌شده قصور وی در اطلاع‌رسانی سریع به مؤسسه مالی است (Geva, 2003, p. 241).

سه شرط برای اعمال مسؤولیت دارنده کارت برای استفاده غیرمجاز مقررشده است:

۱. کارت به‌کاررفته بایستی کارت اعتباری پذیرفته‌شده باشد.

۲. اطلاع مشتری از حداکثر مسؤولیت

۳. عدم اطلاع‌رسانی مشتری به مؤسسه مالی در خصوص سرقت یا مفقودی کارت و اثبات استفاده از رویه امنیتی مناسب توسط مؤسسه مالی[۱]

در صورت وجود شروط فوق مسؤولیت محدود مشتری به شرح ذیل اعمال می‌شود:

الف. اگر مشتری ظرف دو روز فقدان یا سرقت ابزار دسترسی از زمان رخداد آن ابلاغ کند مسؤولیت مصرف‌کننده ۵۰ دلار یا میزان تراکنش هرکدام کمتر باشد مسؤول است.

در پرونده راسل علیه بانک[۲] دادگاه تصریح کرد که بانک نمی‌تواند از طریق قرارداد مسؤولیت مشتری را بیش از آنچه در قانون مقرر گردیده افزایش دهد. در این

---

۱. U.S.C. § 1633

۲. Russell v. First Am. Bank-Mich., N.A

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

پرونده، مشتری رمز را در حاشیه‌ی کارت بانکی خود یادداشت کرده بود و آن را به دخترش داد. او کارت را گم کرد و مادرش را از این مسأله مطلع کرد. زمانی که مادرش به بانک اطلاع داد مبلغ ۳۱۰ دلار از حساب وی کسر گردیده بود. دادگاه اذعان کرد هیچ کدام از سهل انگاری‌ها و غفلت مشتری در حفظ و نگهداری کارت موجب ممانعت از حق استرداد وجه مصرف کننده نمی‌شود و تنها وظیفه مصرف کننده اعلان در ظرف مهلت مقرر است(Hayhoe, Spring 1995, p. 355) .

ب. اگر مصرف‌کننده در اطلاع‌رسانی ظرف دو روز قصور کند ۵۰۰ دلار یا مبلغ تراکنش غیرمجاز که قبل از اتمام دو روز کاری رخ‌داده است تا ۵۰ دلار به انضمام مبلغ انتقال غیرمجازی که بعد از دو روز کاری و قبل از ابلاغ به موسسه مالی رخ‌داده مسؤول است منوط به اینکه موسسه مالی بتواند اثبات کند که چنین خسارتی در صورت اطلاع از مراتب فقدان یا سرقت ابزار دسترسی محقق نمی‌شد.

ج. اگر مصرف‌کننده از ابلاغ مراتب فقدان یا سرقت ابزار دسترسی ظرف شصت روز کاری از زمان ارسال صورت‌وضعیت دوره‌ای حساب که تحقق تراکنش غیرمجاز را مشخص می‌کند، قصور کند، ممکن است با مسؤولیتی نامحدود مواجه شود. مصرف‌کننده نسبت به مبلغ تراکنش‌های غیرمجاز در ظرف شصت روز تا ۵۰۰ دلار مسؤول است به انضمام تراکنش‌های غیرمجازی که بعد از ٦٠ روز و قبل از ابلاغ به موسسه مالی رخ‌داده است مشروط بر اینکه موسسه مالی اثبات کند در صورت اطلاع انتقال غیرمجاز صورت نمی‌گرفت (Geva, 2003, p. 245).

در پرونده کراسر علیه بانک[1] با خواسته مطالبه خسارت ناشی از برداشت غیرمجاز از کارت دادگاه با این استدلال به نفع بانک رأی داد که خواهان مهلت‌های

---

۱. KRUSER v. BANK OF AMERICA NT SA

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

مقرر در قانون انتقال الکترونیکی وجوه را در خصوص اخطار و گزارش به بانک رعایت نکرده بود. در دسامبر ۱۹۸٦ بیانیه‌ی بانک به کراسر اعلام شد مبنی بر اینکه ۲۰ دلار به‌صورت غیرمجاز برداشت‌شده است. کراسر این موضوع را به بانک اعلام نکرد. در سپتامبر ۱۹۸۷ کراسر بیانیه‌های بانک را برای ماه ژانویه و اوت ۱۹۸۷ دریافت کرد که نشان‌دهنده‌ی چهل‌وهفت مورد برداشت غیرمجاز به مبلغ ۹۰۲۰ دلار با استفاده از کارتش بود.

مسأله مورد مناقشه این بود که آیا عدم اخطار برداشت غیرمجاز ۲۰ دلار در سال ۱۹۸٦ مصرف‌کننده را از مطالبه‌ی خسارت ناشی از برداشت غیرمجاز در سال ۱۹۸۷ منع می‌کند یا خیر.

دادگاه بر اساس مقررات «ای»[۱] و قانون انتقال الکترونیکی وجوه رأی داد که بانک مسؤولیتی ندارد چراکه اخطار ظرف مهلت ٦۰ روز به بانک اعلان نشده است.

از اصول مطرح در مقررات آمریکا، مسؤولیت محدود مشتری در تراکنش غیرمجاز است؛ لیکن این مسؤولیت، محدود به اطلاع‌رسانی وی است بدین معنا که مشتری تا سقف محدودی در برابر انتقال غیرمجاز مسؤول است (Hayhoe, Spring 1995, p. 353)؛ لیکن اگر بانک بتواند اثبات کند که انتقال مجاز بوده به‌طور مثال انتقال از طریق ابزار دسترسی که متعلق به مشتری بوده محقق شده است، بار اثبات به مشتری منتقل می‌شود و وی باید سرقت یا مفقودی کارت را اثبات کند در این صورت مسؤولیت محدود مشتری اعمال می‌شود (Geva, 2003, p. 246-247).

---

۱. Regulation E

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

در خصوص تراکنش‌های تجاری، قانون متحدالشکل تجاری آمریکا[۱] مقرر کرده است چنانچه دستور پرداخت غیرمجاز باشد بانک موظف به بازپرداخت اصل وجه و بهره آن از زمان برداشت غیرمجاز است مشروط به اینکه مشتری در زمان معقولی که نباید از ۹۰ روز تجاوز کند بانک را نسبت به انتقال غیرمجاز مطلع کند. در غیر این صورت مشتری حقی نسبت به بهره بانکی ندارد اما می‌تواند اصل وجه را مطالبه کند.

۳-۳-۲. نظام حقوقی ایران

در حال حاضر روابط مشتری و بانک‌ها غالباً بر اساس قراردادهای تنظیمی از سوی بانک‌ها تبیین می‌شود و بانک‌ها سلب مسؤولیت خود و مسؤولیت مشتری برای هر خسارت احتمالی را در قرارداد می‌گنجانند.

ازآنجاکه این نوع قراردادها الحاقی می‌باشند مشتری حق هیچ‌گونه چانه‌زنی و اعتراضی ندارد و بانک‌ها با تحدید تعهدات خود و افزایش تعهدات مشتری شروط غیرمنصفانه‌ای در قرارداد می‌گنجانند تا منافع خود را بهتر تأمین کنند شروطی که سبب عدم تعادل در تعهدات قراردادی می‌شود. (الهیان؛ الهیان، تابستان ۱۳۹۲، ص ۱۲) اما آیا چنین قراردادی که واجد شروط غیرمنصفانه است از سوی محاکم و اصول حقوقی قابل‌پذیرش است؟ اگرچه اصل حاکمیت اراده در کلیه نظام‌های حقوقی، اصلی محترم و غیرقابل‌انکار است؛ لیکن در مواردی که قرارداد درنتیجه برتری جایگاه معاملاتی یکی از طرفین منعقد شود چنین شروطی بر مبنای مواد ۲۳۲ و ۲۳۳ قانون مدنی، خلاف نظم عمومی، اخلاق حسنه و باطل است. مضافاً در ماده ٤٦ قانون

---

۱. U.C.C. § 4A-204

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

تجارت الکترونیک اعمال شروط غیرمنصفانه به ضرر مصرف‌کننده مؤثر نیست. اگرچه خدمات مالی از فصل حمایت از مصرف‌کننده قانون مزبور مستثنی شده است لیکن این مقرره به‌عنوان اصل حقوقی قابل تسری به تمام قراردادها است. در رویه قضایی نیز اخیراً شاهد عدم پذیرش چنین شروطی هستیم. (منافی، ۱۳۹۵، ص ۱٤۷) لذا شروط قراردادی یک‌طرفه و غیرمنصفانه در قراردادهای بانکی باطل است.

در برخی قوانین و دستورالعمل‌های بانک مرکزی احکامی در ارتباط با جبران خسارت ناشی از فعالیت‌های بانکداری مطرح‌شده است. در ابتدا به بررسی مقررات مذکور و سپس تحلیل رویه قضایی می‌پردازیم.

بر اساس بند ج ماده ۳۵ قانون پولی و بانکی کشور مصوب ۱۳۵۱، هر بانکی در مقابل خساراتی که در اثر عملیات آن متوجه مشتریان می‌شود مسؤول و متعهد جبران خواهد بود. مسؤولیتی که برای بانک مفروض است مسؤولیت محض و صرف اثبات رابطه سببت میان عملیات بانک و خسارت مشتری برای مسؤول شناختن بانک کفایت می‌کند و مشتری ملزم به اثبات تقصیر بانک نیست.

قانون تجارت الکترونیک در خصوص جبران ضرر ناشی از نقص سیستم[1]، مقرر کرده است: «اگر خسارتی در بستر مبادلات الکترونیکی در اثر نقص یا ضعف سیستم مؤسسات خصوصی و دولتی... به اشخاص وارد شود مؤسسات مزبور مسؤول جبران خسارت وارده می‌باشند مگر اینکه خسارت وارده ناشی از فعل شخصی افراد باشد که در این صورت خسارات بر عهده این اشخاص است» (پری، ۱۳۹٦، ص ۱۲۰).

این ماده با تأکید بر مسؤولیت مؤسسات مالی در قبال خسارات ناشی از نقص سامانه، در مواردی که خسارت مستند به فعل افراد باشد، از ایشان رفع مسؤولیت کرده. اگرچه واژه افراد در این ماده قدری ابهام‌برانگیز است و معلوم نیست که

---

۱. ماده ۷۸ قانون تجارت الکترونیک

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

منظور از آن زیان‌دیده است یا اشخاص ثالثی همچون سارقان که با سو استفاده از نقص سامانه سبب ورود ضرر شده‌اند؛ لکن با لحاظ جمله انتهایی ماده که این افراد را ملزم به جبران خسارت می‌داند به نظر می‌رسد برداشت دوم به منطق حقوقی و قصد قانون‌گذار نزدیک‌تر است؛ زیرا اگر تقصیر خود زیان‌دیده سبب بروز خسارت شود از دریافت خسارت محروم می‌شود نه اینکه ملزم به پرداخت خسارت به خود باشد؛ بنابراین طبق ظاهر این ماده اگر شخص ثالثی با سو استفاده از نقص سامانه سبب بروز خسارت شود مؤسسه‌ای که از طریق آن سامانه خدمت‌رسانی می‌کند مسؤول نبوده و مشتری باید به خود وی رجوع کند. (عبدالهی، ۱۳۹۶، ص ۵۵) چنین تفسیری برخلاف اصول حقوقی و حقوق مصرف‌کننده است؛ چراکه حکم این ماده در خصوص رابطه مؤسسه مالی و شخص خاطی و مقصر است که ممکن است مشتری باشد در این صورت مشتری حق مراجعه به بانک را ندارد در غیر این صورت حکم ماده مزبور مشمول مشتری نمی‌شود لذا چنانچه مشتری مسبب ورود ضرر نباشد موسسه مالی در قبال مشتری مسؤول و ملزم به جبران خسارت است و نهایتاً طبق قواعد مسؤولیت مدنی می‌تواند به مسبب و شخص خطاکار مراجعه کند.

حسب ماده ۱۳ دستورالعمل صدور دستور پرداخت و انتقال وجه «چنانچه دستور پرداخت ناقص یا حاوی اطلاعات نادرست باشد، مؤسسه مالی باید از پذیرش و اجرای آن خودداری کند.» مؤسسه مالی مکلف است مفاد دستور پرداخت را از حیث اطلاعات و مفاد بررسی کند. لذا چنانچه مؤسسه مالی به تکلیف مزبور عمل نکند مسؤول خسارت‌های ناشی از آن محسوب می‌شود.

در ماده ۲٤ دستورالعمل شناسایی مشتریان مقررشده است ارائه خدمات به مشتریان به‌منزله تأیید انجام رویه شناسایی مشتری توسط کارکنان ذی‌ربط در مؤسسه اعتباری است و مسؤولیت هرگونه نقص در این زمینه متوجه آن‌ها است.

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

طبق این مقرره مؤسسات مالی مسؤول شناسایی اعتبار و صحت دستور پرداخت هستند؛ لذا در صورت تراکنش غیرمجاز براثر قصور در شناسایی مشتری مؤسسه مالی مسؤول محسوب می‌شود. رویکرد این مقرره تقصیر مفروض بانک است.

به‌موجب آخرین مقرره قانونی[1] «الزامات رمزهای پویا در تراکنش‌های مبتنی بر کارت» در صورت تحمیل خسارت مالی به دارندگان کارت‌های بانکی به دلیل عدم رعایت الزامات مسؤولیت جبران خسارت بر عهده مؤسسه اعتباری است؛ لذا در آخرین مقرره نیز قانون‌گذار با صراحت به مسؤولیت بانک اشاره کرده است.

به‌رغم وجود مقررات فوق و پذیرش مسؤولیت بانک، رویه قضایی حاکی از آن است که دادگاه‌ها مشتری را مسؤول تراکنش‌های غیرمجاز قلمداد می‌کنند.

در دعوای بانک ب علیه آقای الف به خواسته مطالبه مبلغ ٦٨٠/٢٤ یورو[2] دادگاه چنین استدلال کرد که: دلیلی از سوی خوانده در این خصوص که کارت مزبور از سوی شخص یا اشخاصی مورد سوءاستفاده قرارگرفته و نامبرده آن را در اختیار اشخاص دیگری قرار نداده باشد، به دادگاه اقامه و ابراز نگردیده، بنابراین ادعای مطروحه قابل‌اعتنا نبوده و رافع مسؤولیت ایشان در پرداخت وجه مورد برداشت از کارت ارزی در قبال خواهان نیست.

چنین رایی بر خلاف اصول حقوقی است چرا که مشتری در موقعیتی قرار ندارد که بتواند به اسناد و ادله دسترسی داشته باشد مضافاً مشتری تخصص لازم در تحلیل و استفاده از داده‌ها را ندارد و تحمیل بار اثبات به مشتری هزینه گزافی برای مشتری در پی دارد (قنبری، ۱۳۹۱، صص ۱۳۳-۱۳٤). همچنین بانک مدعی این امر که

---

۱. ماده ۵۸ الزامات رمزهای پویا در تراکنش‌های مبتنی بر کارت مصوب شهریور ۱۳۹۷، سند مذکور بر اساس ماده هشتم مقررات ناظر بر فعالیت مرز کاشف توسط شرکت مدیریت امن الکترونیکی کاشف به نمایندگی از بانک مرکزی تهیه و تدوین‌شده است.

2. http://j.ijri.ir

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

دستور معتبر از سوی مشتری صادر شده است لذا طبق قاعده البینه الی المدعی و الیمین علی من انکر باید وجود دستور معتبر و وجود شرایط امنیتی کافی را اثبات کند.

در ادامه نسبت به رأی مزبور تجدیدنظرخواهی شد دادگاه، تجدیدنظر را غیرموجه دانسته با این استدلال که باوجود کارت درید دارنده آن، با شرایط امنیتی عرف بانکداری، وی همچنان که مالک مبلغ اعتبار آن است، مسؤول سوءاستفاده احتمالی از آن نیز محسوب می‌شود.

در پرونده دیگری، آقای الف علیه بانک با خواسته جبران خسارت ناشی از برداشت غیرمجاز از کارتش که توسط سارق و از طریق نصب دوربین جنب دستگاه خودپرداز بانک، رمز را رؤیت و با جعل کارت، وجوهی را از حساب وی برداشت کرده طرح دعوا کرد، دادگاه خسارت را مستند به سارق دانسته و بیان داشت که: «بانک موظف است موارد ایمنی را رعایت کند اما مسؤولیت بیشتر از آن، متوجه او نیست و مصداق حرج است و در چنین موردی، بانک مسؤول نیست زیرا علت قوی‌تر همان سارق است که با نصب دوربین، اطلاعات افراد را سرقت کرده» نهایتاً دادگاه حکم به عدم مسؤولیت بانک صادر کرد (عبدالهی، ۱۳۹٦، ص ٥٦).

رویکرد مقررات ایران مبتنی بر مسؤولیت بانک است؛ لکن رویه قضایی، بدون توجه به ویژگی‌های خاص انتقال الکترونیکی وجوه و در نظر گرفتن موقعیت و شرایط مشتری و عدم توانایی وی در دسترسی به اطلاعات و اثبات قصور بانک در شناسایی صحت دستور و رعایت رویه امنیتی و حفاظت از داده‌ها از رویکرد مسؤولیت محض مشتری پیروی کرده و در یکی از آرا، دادگاه تجدیدنظر بر مبنای نظریه خطر مشتری را منتفع اصلی معاملات بانکی معرفی و وی را مسؤول خسارات قلمداد کرد. درصورتی‌که بانک با ارائه خدمات بانکداری الکترونیکی از یک سو بستر

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

خطرناکی ایجاد کرده و از سوی دیگر منتفع اصلی معاملات بانکی می‌باشند و باید ریسک ناشی از آن را بپذیرند؛ لذا اگرچه در مقررات مسؤولیت بانک قابل استنباط است اما رویه قضایی برعکس این رویکرد عمل کرده است.

نظر به‌مراتب فوق، می‌توان بیان داشت که میان رویکرد نظام حقوقی ایران و آمریکا تفاوت وجود دارد. نظام حقوقی آمریکا میان تراکنش مصرف‌کننده و تراکنش‌های تجاری و مقررات حاکم بر آن‌ها قائل به تفکیک‌شده لیکن در نظام حقوق ایران شاهد چنین امری نیستیم. در ارتباط با مفهوم تراکنش غیرمجاز در تراکنش مصرف‌کننده نظام حقوقی آمریکا سه معیار تبیین کرده: تراکنش توسط شخصی غیر از مشتری، بدون اجازه و اختیار وی به‌گونه‌ای که هیچ بهره‌ای نصیب مشتری نشود. اجازه می‌تواند واقعی (صریح یا ضمنی) و صوری (ظاهری) باشد.

درنتیجه، در حقوق آمریکا در تراکنش‌های مصرف‌کننده هنگامی‌که مشتری یا نماینده وی اعم از واقعی یا ظاهری اقدام به صدور دستور پرداخت کنند دستور مجاز است بعلاوه هنگامی‌که از تراکنش سودی نصیبش شود نمی‌تواند ادعای غیرمجاز بودن را مطرح کند. در تراکنش‌های تجاری نیز درجایی که مشتری یا نماینده وی طبق قواعد نمایندگی اقدام به صدور دستور پرداخت‌کرده باشند تراکنش مجاز محسوب می‌شود. مضافاً نحوه توافق مشتری و بانک بر رویه امنیتی جهت شناسایی صحت دستور می‌تواند در تعیین دستور مجاز مؤثر باشد. اگر طرفین بر رویه امنیتی متعارف تجاری توافق کنند دو فرض ممکن است مطرح شود: ۱) دستور منطبق با رویه امنیتی متعارف موردتوافق باشد درصورتی‌که بانک اثبات کند روش امنیتی به‌کاربرده شده رویه مناسبی بوده است و بانک در پذیرش دستور پرداخت حسن نیت داشته است دستور مجاز محسوب می‌شود ۲) اگر دستور منطبق با رویه نباشد دستور غیرمجاز قلمداد می‌شود. لیکن اگر مشتری در پاسخ به ارائه پیشنهاد رویه امنیتی تجاری متعارف از سوی بانک آن را رد کند و ضمن پذیرش تمام مسؤولیت

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

های رویه امنیتی پیشنهادی خود و دادن تعهد کتبی مبنی بر پذیرش تمام خطرات، در صورت بروز تراکنش غیرمجاز با احراز تمام شروط انتقال مجاز محسوب می‌شود.

در حقوق ایران بدون تفکیک میان تراکنش مصرف‌کننده و تجاری در قانون تجارت الکترونیک مقرر کرده است که اگر دستور مطابق با رویه ایمن باشد و توسط مشتری صادرشده باشد دستور مجاز محسوب می‌شود. در غیر این صورت هرچند دستور مطابق رویه باشد (رویه ایمن یا رویه منتخب مشتری) ولی مشتری یا نماینده واقعی وی صادر نکرده باشند غیرمجاز محسوب می‌شود.

۴. نتیجه

با لحاظ مقررات نظام حقوقی آمریکا و ایران بررسی‌ها نشان می‌دهد که در هر دو نظام حقوقی ایران و آمریکا جهت تشخیص تراکنش غیرمجاز علت و مبنای عملکرد بانک در اجرای دستور پرداخت ملاک است. در هر دو نظام مزبور، پرداخت بر مبنای دستور مشتری یا اجازه واقعی وی مجاز محسوب می‌شود. نظام حقوقی آمریکا ضمن تفکیک میان تراکنش‌های مصرف‌کننده و تجاری، در ارتباط با تراکنش‌های مصرف‌کننده تراکنش بر مبنای اختیار ظاهری مشتری و زمانی که مشتری از تراکنش سودی عایدش می‌شود را مجاز دانسته است. در تراکنش‌های تجاری نیز ضمن پذیرش اجازه صوری، استفاده از رویه امنیتی را معیار کرده بدین نحو که در فرض عدم استفاده از رویه امنیتی تجاری متعارف دستور غیرمجاز محسوب می‌شود و در فرض استفاده از رویه امنیتی دو حالت متصور است: دستور منطبق با رویه امنیتی متعارف موردتوافق باشد درصورتی‌که بانک اثبات کند روش امنیتی به‌کاربرده شده رویه مناسبی بوده است و بانک در پذیرش دستور پرداخت حسن نیت داشته است دستور مجاز محسوب می‌شود ۲. اگر دستور منطبق با رویه نباشد دستور غیرمجاز

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

قلمداد می‌شود. بعلاوه زمانی که مشتری رویه امنیتی بانک را رد کند، رویه خود را پیشنهاد و مسؤولیت آن را به‌صورت کتبی بپذیرد دستور مجاز محسوب می‌شود.

در نظام حقوقی ایران علی‌رغم فقدان مقررات صریح و مدون در حوزه تراکنش الکترونیکی با استناد به مقررات عام در حوزه بانکداری به این نتیجه می‌توان دست‌یافت که در صورت صدور دستور توسط مشتری یا نماینده واقعی وی دستور مجاز محسوب می‌شود. یکی از مسائل اساسی این است که در صورت تراکنش غیرمجاز وجوه، بین مشتری و موسسه مالی چه کسی مسؤول جبران خسارت است؟ هدف اصلی هر مقرره قانونی ایجاد و افزایش اجرای عدالت است و در تخصیص خطر در حوزه بانکداری الکترونیکی قانون‌گذار در پی اهدافی ازجمله: ایجاد تعادل بین هزینه‌ها، شفاف‌سازی، کاهش خسارت، ایجاد انگیزه و اعتماد و اطمینان. برای دست‌یابی به اهداف مزبور معیارهای گوناگونی مطرح گردیده است که می‌توان به توزیع ضرر، شخصی که در بهترین موقعیت قرار دارد، مسؤولیت محض، مسؤولیت محدود، شخص قاصر و منتفع اشاره کرد.

دراین‌ارتباط نظام حقوقی آمریکا در هردو نوع تراکنش، مسؤولیت مشتری را بر مبنای اطلاع‌رسانی یا عدم اطلاع‌رسانی به بانک در خصوص سرقت، گم‌شدن ابزار دسترسی یا برداشت غیرمجاز تعیین کرده است و ترکیبی از رویکرد مسؤولیت محدود و شخصی که در بهترین موقعیت قرار دارد معیار دانسته. اگرچه این رویکرد دارای نقاط قوت ازجمله ایجاد انگیزه برای بانک در راستای افزایش امنیت و بهبود روش امنیتی و کاهش هزینه‌های دادرسی می‌شود لیکن با عدم پیش‌بینی سهل‌انگاری شدید مشتری و مسؤولیت وی، منجر به ایجاد انگیزه برای مشتری نسبت به حفظ ابزار دسترسی و رعایت نکات ایمنی نمی‌شود. در نظام حقوقی ایران، مسؤولیت بانک قابل استنباط است لکن رویه قضایی بدون لحاظ ویژگی خاص تراکنش‌های الکترونیکی و عدم توانایی مشتری در اثبات قصور بانک، مشتری را مسؤول قلمداد

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

کرده است که این امر پیامدهای منفی برای سیستم بانکداری و تجارت ایران در پی خواهد داشت.

لذا ازآنجاکه تراکنش الکترونیکی وجوه به دلیل مزایای متعدد امروزه مورد استقبال تمام نظام‌های بانکی است و بهره‌گیری از آن در تمام عرصه‌ها رو به افزایش است پویایی نظام حقوقی هم‌زمان با نظام فنی بانکداری بسیار حائز اهمیت است. به‌روزرسانی و تدوین قوانین جامع در این حوزه ضروری و اجتناب‌ناپذیر است.

۵. منابع و مآخذ

۵-۱. فارسی

۱. السان، مصطفی، حقوق بانکداری اینترنتی. تهران: پژوهشکده پولی وبانکی بانک مرکزی ایران، ۱۳۹۲.

۲. الماسی، نجاد علی، «تحلیلی اقتصادی ادله اثبات دعوای مدنی»، مجله تحقیقات حقوقی، زمستان ۱۳۹۱.

۳. الهیان، مجتبی؛ الهیان، محمدابراهیم، «شروط غیرمنصفانه در قراردادهای بیمه و آثار آن از منظر فقه و حقوق ایران»، مجله پژوهش‌های فقهی، دوره نهم، تابستان ۱۳۹۲.

۴. بابایی ایرج، «بررسی عنصر خطا در حقوق مسؤولیت مدنی ایران»، مجله پژوهش حقوق و سیاست، دوره ٤، شماره ۷، ۱۳۸۱.

۵. بادینی، حسن، فلسفه مسؤولیت مدنی، تهران: شرکت سهامی انتشار، ۱۳۹۲.

۶. بادینی، حسن؛ شعبانی کندسری، هادی؛ رادپرور، سجاد، «مسؤولیت محض؛ مبانی و مصادیق»، مجله مطالعات حقوق تطبیقی، ۱۳۹۱.

۷. جلالی، مریم؛ الشریف، محمدمهدی؛ فصیحی زاده، علیرضا؛ جلالی، محمود، «کارت بدهی و ارزیابی تعهدات بانک صادرکننده آن در خصوص انتقال وجه؛ مطالعه تطبیقی در حقوق ایران و آمریکا»، مجله مطالعات حقوقی دانشگاه شیراز، دوره نهم، شماره ٤، زمستان ١٣٩٦.
۸. دیلمی، احمد؛ فیروزبخت، فهیمه، «ضمان و مسؤولیت مدنی در انتقال الکترونیکی معتبر و غیرمجاز وجوه»، مجله پژوهش‌های فقهی، دوره ١٣، ١٣٩٦.
۹. رحمتی، پرویز؛ خودکار، رضا، «تحلیل اقتصادی مبانی مسؤولیت مدنی در حوادث دوجانبه»، دو فصلنامه دانش و پژوهش حقوقی، پاییز و زمستان ١٣٩١.
۱۰. روس پی بوکلی؛ گائو ایکس یانگ، «تکامل تدریجی قاعده تقلب در حقوق اعتبارات اسنادی: سفر به گذشته و آینده»، بنانیاسری، ماشاالله، مجله تحقیقات حقوقی،١٣٨٥.
۱۱. طهماسبی، علی؛ علیپور، کوروش، «اثر تقصیر و مسؤولیت محض در ترغیب عامل زیان و زیاندیده به رعایت احتیاط»، مجله حقوقی دادگستری، ١٣٩٠.
۱۲. قنبری؛ حمید، «معکوس نمودن بار اثبات دعوا مبنای مسؤولیت بین بانک و مشتری در بانکداری الکترونیک»، پژوهش‌های پولی و بانکی، ١٣٩١
۱۳. عبدالهی، محبوبه، «تحلیل مسؤولیت حقوقی بانک انتقال‌دهنده در انتقال الکترونیکی وجوه»، دانشنامه حقوق اقتصادی، شماره ١٢، پاییز و زمستان ١٣٩٦.
۱۴. مافی، همایون؛ کدیور، حسام، «بررسی اختیار ظاهری نماینده در حقوق ایران و اسناد بین‌المللی»، مجله حقوق خصوصی، بهار و تابستان ١٣٩٣.
۱۵. منافی، شهرام، «بررسی تطبیق نظریه غیرمنصفانه بودن قراردادها»، دو فصلنامه پژوهشنامه حقوق خصوصی عدالت، دوره ٣، شماره ٥، ١٣٩٥.

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

۱۶. میرزایی پری، امیرعلی، حقوق کارت‌های اعتباری بانکی بین‌المللی، تهران: مجد، ۱۳۹۶.

۵-۲. انگلیسی

17. Algudah, F, the Liabilty of Banks in Electronic Fund Transfer Transactions: A Study in the British and the, 1992.
18. BROADMAN, E, Electronic Fund Transfer Act: Is the Consumer Protected? University of SANFRANCISCO Law Review, 13, 254, Winter 1979.
19. Dolan, J. F Impersonating the Drawer: A Comment on. Canadian Business Law Journal, 38, 288. 2003.
20. French, J. K, Unauthorized and Erroneous Payment Orders. The Business Lawyer, 45, 1426, June 1990.
21. Geva, B, Allocation of Sender Risks in Wire Transfers: The Common Law and UCC Article 4A [Part 1]. Journal of South African Law, 1997.1, 26, 1997.
22. Geva, B. Allocation of Sender Risks in Wire Transfers: The Common Law and UCC Article 4A [Part 2]. Journal of, 1997.2. 1997.
23. Geva, B. Consumer Liability in Unauthorized Electronic. Canadian Business Law Journal, 38, 224, 2003.
24. Hargitai, P. P. (n.d). Florida’s Federal Courts Are on the Verge of Getting It Wrong: UCC Article 4A Displaces Common Law Negligence Actions. The Banking ANKING Law Journal, 212.
25. Hayhoe, R. Comments Fraud, the Consumer, and the Banks: The (un-) Regulation of Electronic Funds Transfer. University of Toronto Faculty of Law Review, 53, Spring 1995.
26. Robert D. Cooter Edward L. Rubin, A Theory of Loss Allocation for Consumer. Texas Law Review, 66:63, 1987.

[DOR: 20.1001.1.22516751.1398.23.3.5.0]

27. Robert W. Ludwig, Jr.Salvatore Scanio, Joseph S. Szary, Malware and Fraudulent Electronic Funds Transfers, Fidelity Law Journal, Vol. XVI, October 2010.
28. Rogers, J. S. The Basic Principle of Loss Allocation for Unauthorized Checks. Boston College Law School, 39, 2004.
29. Rusch, l, Reimagining Payment Systems: Allocation (Vol. 83:2). Chi.Kent L. Rev. 561, 2008.
30. Salvatore Scanio Robert W. Ludwig, Surging, Swift and Liable? Cybercrime and Electronic Payments Fraud Involving Commercial Bank Accounts: Who Bears the Loss? Journal of Intrnet Law, 2013.
31. Thevenoz, L, Error and Fraud in Wholsale Funds Transfers: U. C.C. Article 4A and the Uncitral Harmonization Process. *Alabama Law Review*, 42:2:881. 1990.
32. _____, Consumer liability in case of fraud, *university of oslo*, 25, 2015.

[DOR: 20.1001.1.22516751.1398.23.3.5.0]