فصل‌نامه مطالعاتی در مدیریت بانکی و بانکداری اسلامی

مؤسسه عالی آموزش بانکداری ایران
زمستان ۱۴۰۲، دوره ۹، شماره ۲۵، صفحه ۷۹-۵۶

چالش‌های احراز هویت دربانکداری الکترونیکی با تاکید برخطرپول‌شویی

کوروش جعفر پور*[۱]
صدیقه هجینی نژاد[۲]

چکیده

اجرای بانکداری الکترونیکی علی‌رغم مزایای فراوان، با چالش‌های زیادی روبروست. در این مقاله چگونگی تحقق قرارداد، احرازهویت، امضای الکترونیکی و قابلیت استناد امضا به‌عنوان داده پیام از یک طرف و مخاطرات جعل هویت و تسهیل پول‌شویی از طرف دیگر با مطالعه مقررات داخلی و بین المللی و روش تحلیلی، توصیفی بررسی شده است. نتیجه این بررسی نشان می‌دهد که قرارداد الکترونیکی با توجه به آزادی تعیین روش انعقاد قرارداد و تجویز قانون تجارت الکترونیکی، قابل تحقق است و امضای بیومتریک و امضای دیجیتالی نه‌تنها کارآمد و مطمئن است بلکه می‌تواند جبران‌کننده ناتوانی اقشار محروم از ارائه اسناد هویتی و اقامتی در راستای مقررات مبارزه با پول‌شویی باشد؛ ضمن اینکه احراز هویت الکترونیکی با کمک هوش مصنوعی باعث شناسایی رفتارهای متقلبانه و مانع وقوع پول‌شویی می‌شود. در پایان پیشنهاد می‌گردد سیستم یکپارچه اطلاعاتی بین بانک‌ها و سازمان‌های متولی هویت مانند ثبت احوال، ثبت شرکت‌ها، ثبت اسناد و دستگاه قضایی از حیث احکام صادره در خصوص هویت اشخاص مانند محجوریت و ورشکستگی و انحلال برقرار شود تا با اطمینان ازصحت داده‌ها، زمینه ارائه خدمات مطمئن آنلاین و متعاقباً دفاع از داده‌های الکترونیکی به‌عنوان سند در محاکم قضایی فراهم شود.

واژه‌های کلیدی: امضای الکترونیکی، احراز هویت، امضای بیومتریک، بانکداری الکترونیکی، پول‌شویی.

طبقه‌بندی JEL: K15، G21،E50، E59 و G23.

---

۱. کوروش جعفر پور، استادیار دانشکده حقوق دانشگاه آزاد اسلامی واحد تهران جنوب، تهران، ایران (نویسنده مسئول)؛ Kouroshjafarpour@gmail.com

۲. صدیقه هجینی نژاد ، دانشجوی دکتری حقوق خصوصی دانشکده حقوق دانشگاه آزاد اسلامی واحد تهران جنوب، تهران؛ ایران؛ hajini12@gmail.com

مقدمه

دردهه ۱۹۷۰ دسترسی برخط به حساب مشتریان بانکی با انتقال آنی اطلاعات از طریق بکارگیری پایانه در جلوی باجه فراهم شد، اما نرم افزارها کماکان یکپارچه نبودند. دردهه ۱۹۸۰ با دسترسی مشتریان به حساب‌هایشان از طریق تلفن، دستگاه خودپرداز، کارت هوشمند، امکان عملیات دریافت و پرداخت به‌صورت الکترونیکی فراهم شد، اما یکپارچگی و تعامل در خطوط مخابراتی مطمئن و پروتکل‌های ارتباطی لازم برای اتصال مشتری به شعب سایر بانک‌ها وجود نداشت. بعدها با گسترش شبکه اینترنت و قابلیت دسترسی و استفاده از فناوری‌های پیشرفته نرم‌افزاری و سخت‌افزاری مبتنی‌بر شبکه مخابرات برای تبادل منابع و اطلاعات‌مالی به‌صورت الکترونیکی، دیگر نیازی به حضور فیزیکی مشتری نبود. این امر با رشد روزافزون تجارت الکترونیکی در زمینه‌های مختلف از جمله عرضه اینترنتی کالا توسط تولیدکننده به مصرف‌کننده[1]، تجارت بین بنگاه‌ها[2]، حراج آنلاین کالای مازاد توسط مردم[3]، ارائه اینترنتی نیاز مصرف‌کنندگان به تجار[4]، خرید اینترنتی مایحتاج دستگاه اداری و دولتی به‌صورت آنلاین[5]، معاملات اینترنتی بین دستگاه‌های دولتی (G2G)، معاملات اینترنتی دولت با تجار (G2B) و معاملات آنلاین بین دولت و مصرف‌کنندگان (G2C) همگام شد. پرواضح است تحقق این موارد و توسعه تجارت الکترونیکی در تمام این زمینه‌ها بدون توسعه بانکداری الکترونیکی میسر نبود، اما اجرای بانکداری الکترونیکی با چالش‌های زیادی مواجه شد. تصویب مقرراتی مانند قانون تجارت الکترونیکی مصوب ۱۳۸۲، قانون آزادی اطلاعات مصوب ۱۳۸۵، قوانین مرتبط با مالکیت فکری، قانون جرایم رایانه‌ای مصوب ۱۳۸۸، تصویب‌نامه‌های ۱۳۸۳/۱۰/۹ و اصلاحی ۱۳۸۳/۱۱/۲۸، تصویب‌نامه مورخ ۱۳۸۴/۴/۵ در مورد برنامه جامع تجارت الکترونیک، آیین‌نامه اجرایی ماده ۴۸ قانون تجارت الکترونیک مصوب ۱۳۸۴/۵/۲ کمک شایانی به رفع برخی ابهامات نمود اما همچنان چالش‌های زیادی از حیث احراز هویت الکترونیکی و آثار آن روی تحقق قرارداد الکترونیکی و نحوه اخذ امضای الکترونیکی و ارزش اثباتی آن وجود داشت. شکل‌گیری جرایمی مانند پول‌شویی و تدوین مقررات بین‌المللی با تاکید بر احراز هویت دقیق و شناسایی هویت مشتری به‌عنوان الزام و اصلاح قانون مبارزه با پول‌شویی ایران در سال ۱۳۹۷ با الگو گرفتن از

---

1. Business-to-Consumer (B2C)
2. Business-to-Business (B2B)
3. Consumer to Consumer (C2C)
4. Consumer to Business (C2B)
5. Business to Administer (G2G)

استانداردهای چهل توصیه FATF موجب گردید به‌دلیل غیرحضوری بودن خدمات در بانکداری الکترونیکی دغدغه تسهیل پول‌شویی و عدم تحقق احراز هویت دقیق نیز به چالش‌ها اضافه شود. در مطالعه سوابق تحقیق مشاهده گردید زرکلام (۱۳۸۲) به جایگاه امضای الکترونیکی درنظام ادله اثبات دعوا پرداخت و سجادی و جعفری (۱۳۹۸) موضوع مسئولیت مدنی ناشی از امضای الکترونیکی را مطرح نمودند و صادقی و ناصر (۱۳۹۹)، مخاطرات حقوقی امضای الکترونیکی و الزامات قانونی پیشگیری از آن را بررسی کردند که نتایج آن در پژوهش حاضر مورد توجه قرار گرفته است. اسدی (۱۳۹۷) جایگاه امضای دیجیتال در ثبت اسناد به‌شیوه الکترونیکی را مطرح و همکاری دفاتر اسناد رسمی و ادارات ثبت اسناد و املاک در انجام تشریفات امضای دیجیتال را پیشنهاد نمود. مافی و ناصر (۱۴۰۰) به واکاوی مکانیسم احراز اهلیت متعاملین در پیاده‌سازی قراردادهای هوشمند پرداختند. همین‌طور پیروی و جعفری (۱۳۸۸) روش‌های فنی احراز هویت در تجارت الکترونیک را مطرح و مدل یکپارچه‌سازی تأیید هویت به‌کمک شاخص بیومتریک و RFID را ارائه دادند. اصغری و همکاران (۱۳۹۲) برای امنیت احراز هویت در تجارت الکترونیک، روش ارائه شده توسط ASVS را مطرح نمودند. باتوجه به اینکه درخصوص چالش‌های موضوع این مقاله که مبتنی بر احراز هویت هستند و علی‌الخصوص اینکه آیا احراز هویت الکترونیکی ممکن است منجر به تسهیل پول‌شویی شود یا بالعکس از حیث شناسایی رفتارهای متقلبانه می‌تواند مانع پول‌شویی گردد تاکنون تحقیقی مشاهده نگردیده است. در این مقاله سعی شد با مطالعه آخرین مقررات مرتبط و استفاده از روش استدلالی و تحلیلی‌وتوصیفی، چالش‌های مذکور با محوریت احراز هویت بررسی و پیشنهاداتی ارائه شود. به این منظور ابتدا موضوع تحقق قرارداد، امضای قرارداد و احراز هویت طرفین مورد تحلیل قرار گرفته و سپس با استفاده از نتایج این دو قسمت به موضوع رابطه پول‌شویی و بانکداری الکترونیکی به‌دلیل احتمال عدم احراز هویت دقیق پرداخته می‌شود و در قسمت‌های پایانی مقاله، موضوع ارزش اثباتی امضای الکترونیکی و خلاء مقررات در بحث جرم‌انگاری برخی اعمال به‌منظورحمایت از بانکداری الکترونیکی مطرح می‌شود تا چالش احراز هویت در بانکداری الکترونیکی از نقطه شروع قرارداد تا مرحله اثبات مورد تحلیل قرار گیرد.

۱-تحقق قرارداد الکترونیکی

باتوجه به اینکه قرارداد الکترونیکی حسب ماده ۳۰ قانون تجارت الکترونیکی تابع قواعد حاکم بر قراردادهاست ازاین‌رو در این قسمت به‌اختصار نحوه تحقق قرارداد الکترونیکی مورد تحلیل قرار

می‌گیرد. دسترسی به شبکه جهانی اینترنت و گسترش ارتباطات الکترونیک بین افراد وسازمان‌های مختلف، بستری مناسب برای تنظیم قرارداد الکترونیکی جهت برقراری مراودات تجاری و اقتصادی فراهم‌کرده‌است (امیرحسنی، ۱۴۰۰). خصوصیت اساسی قرارداد الکترونیکی این است که باید با واسطه الکترونیکی و یا در محیط الکترونیکی بدون حضور فیزیکی متقابل طرفین منعقد گردد (الدسوقی، ۲۰۰۳). با این وصف، قرارداد الکترونیکی را می‌توان از مجموعه قراردادهای از راه دور موضوع بند«ص» ماده ۲ قانون تجارت الکترونیکی دانست و به‌سبب سرعت مبادله اطلاعات در محیط اینترنت آن را قرارداد آنی شمرد. بنابراین نحوه اعلام اراده، زمان و مکان تشکیل قرارداد از حیث قانون حاکم بر قرارداد الکترونیکی اهمیت زیادی دارد. در حقوق ایران، لزوم تبعیت از شکل معینی از تشریفات، از شروط صحت قرارداد نمی‌باشد (کاتوزیان، ۱۳۶۴) کمااینکه حسب ماده ۱۹۱ قانون مدنی«عقد محقق می‌شود به قصد انشاء به شرط مقرون بودن به چیزی که دلالت بر قصد کند» بنابراین طرفین در انتخاب نحوه اعلام اراده آزاد هستند و روش الکترونیکی هم یک نوع نحوه انعقاد قرارداد است با این تفاوت که اراده بشکل داده پیام اعلام و با استفاده از روش‌های الکترونیکی ارسال و پذیرش می‌شود. در واقع اصل رضایی بودن قراردادها، امکان توافق طرفین بر تعیین شکل معینی برای انعقاد قرارداد را فراهم می‌کند، زیرا حسب ماده ۱۰ ق.م «قراردادهای خصوصی نسبت به کسانی که آن را منعقد نموده‌اند در صورتی که مخالف صریح قانون نباشد نافذ است» با توجه به اینکه آزادی طرفین در روش اعلام اراده ممکن است زمینه سوءاستفاده از اعتماد متعاملین و مشکل اثبات بیان اراده را به‌همراه داشته باشد، ازاین‌رو قانون‌گذار برای حفظ نظم عمومی، اخلاق حسنه و تعادل منافع و مصالح اقتصادی اشخاص در روابط حقوقی، انعقاد بعضی از قراردادها را منوط به طی تشریفات خاصی نموده است. در عرصه بین‌المللی، تشریفات خاصی که از رضایی بودن قراردادهای الکترونیکی بکاهد وضع نشده است کمااینکه ماده ۵ قانون نمونه آنسیترال[1] تصریح دارد که «اطلاعات نباید به‌صرف این که به‌شکل داده پیام است، انکار شود». در این راستا ماده ۹ دستورالعمل اتحادیه اروپا[2] از کشورهای عضو خواسته که مانعی در انعقاد و استفاده از قرارداد الکترونیکی که طبق ضوابط حاکم بر قراردادها در سیستم‌های حقوقی تنظیم شده است، بوجود نیاورند و به‌صرف استفاده از شیوه‌های الکترونیکی، این قراردادها را بی‌اثر و فاقد اعتبار ندانند.

---

1. http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005 Convention.html.

2. Official Journal L 178 , 17/07/2000 P. 0001 - 0016

با توجه به اینکه تشکیل قرارداد مستلزم اتصال ایجاب و قبول در زمان نفوذ آن است، لذا زمان و مکان اتصال ایجاب و قبول از حیث قانون و احکام حاکم بر آن اهمیت زیادی دارد. درخصوص تعیین زمان قرارداد در نظام‌های حقوقی معاصر چهار راهکار عمده شناخته شده است که عبارتند از: زمان اعلام قبول، زمان ارسال قبول، زمان وصول قبول و زمان مطلع شدن ایجاب‌کننده. در حقوق ایران، ماده ۱۹۱ قانون مدنی، بیشتر با مفهوم وسیع اعلام قبول مطابقت دارد (قاسم زاده، ۱۳۸۵). دکتر شهیدی و دکتر صفایی از اساتید حقوق مدنی علی‌رغم پذیرش مبنای نظریه اعلام قبول، نظریه ارسال قبولی را بیشتر در وجهه منطقی و عملی دانسته (صفایی، ۱۳۸۶) و (شهیدی، ۱۳۷۷: ۱۶۴) و ارسال قبولی را زمان انعقاد قرارداد می‌دانند. درعرصه معاملات تجاری بین‌المللی، زمان مطلع شدن ایجاب‌کننده به‌طور ضمنی معمول نمی‌باشد و زمان انعقاد قرارداد تابع زمان ارسال و یا وصول قبول به محل ایجاب‌کننده است اعم از اینکه مطلع شود یا نشود. به‌عنوان مثال در کنوانسیون بیع بین‌المللی برای نفوذ و اعتبار ایجاب، اطلاع مخاطب لازم نیست و صرف رسیدن ایجاب به مخاطب برای نفوذ و اعتبار آن کافی است(صفایی، ۱۳۹۹). در قراردادهای الکترونیکی گرچه زمان و مکان ارسال داده پیام حسب ماده ۳۰ قانون تجارت الکترونیکی تابع قواعد عمومی حاکم بر قراردادهاست، ولی با توجه به روش‌های ارتباطی و مقررات خاصی که قانون‌گذار به‌صراحت در فصل چهارم قانون تجارت الکترونیکی پیش‌بینی نموده و صراحتا اشاره‌ای به زمان انعقاد قرارداد ندارد، می‌توان گفت که زمان انعقاد قرارداد الکترونیکی وابسته به ارسال و وصول داده پیام در سیستم طرفین است اعم از اینکه مطلع شوند یا نشوند. در واقع با وصول داده پیام به سیستم مخاطب، اطلاع مالک سیستم مفروض تلقی شده و عذر عدم‌اطلاع قابل پذیرش نیست؛ ضمن اینکه اعتبار ارسال داده پیام منوط به این است که داده به سیستم اطلاعاتی خارج از کنترل اصل‌ساز یا قائم مقام وی وارد شود یعنی لحظه وصول قبول الکترونیکی، زمان انعقاد قرارداد تلقی می‌شود. توالی ایجاب و قبول در قرارداد غیرالکترونیکی اهمیت دارد و نویسندگانی از جمله شیخ انصاری معتقدند «عقد و قرارداد، مرکب از ایجاب و قبول و متکی به متعاقدان و به‌منزله یک کلام است که بخشی از آن به بخش دیگر ارتباط دارد. پس فاصله‌ای که هیأت اتصالی عقد را از بین ببرد، مضر به قرارداد است. ازاین‌رو، اگر فاصله بین ایجاب و قبول خیلی طولانی باشد در این صورت قرارداد صدق نمی‌کند، معیار و قانون این موالات و عدم‌فاصله به‌عهده عرف است» (هادوی، ۱۳۸۸). در قرارداد الکترونیکی این توالی ایجاب و

قبول بستگی به روش ارتباط الکترونیکی و درجه تقارن زمانی قبول نسبت به ایجاب دارد[۱] که عرف تجارت الکترونیکی تلقی می‌شود.

درخصوص مکان تحقق قرارداد الکترونیکی، علی‌رغم اینکه طرفین در محیط مجازی به‌طور عموم دارای محل و یا نشانی وب سایت و یا عضو سیستم پست الکترونیکی می‌باشند ولی به‌علت قابلیت تغییر سریع آن، نمی‌توان مکان مجازی اعم از آدرس وب سایت و یا آدرس پست الکترونیکی را به‌عنوان مکان انعقاد قرارداد الکترونیکی معتبر دانست؛ زیرا تعیین مکان انعقاد قرارداد باید دارای ویژگی‌های حقیقی و یا حکمی باشد تا آثار ناشی از این رابطه از لحاظ تشخیص دادگاه صالح و یا نحوه اجرای تعهدات ناشی از قرارداد و یا تعیین قوانین حاکم بر قرارداد و حل‌وفصل اختلافات ناشی از آن قابل احراز باشد. ماده ۲۹ قانون تجارت الکترونیکی، مکان تحقق ایجاب و قبول در قرارداد الکترونیکی را به این صورت تعیین نموده است که اگر محل استقرار سیستم اطلاعاتی ارسال داده با محل استقرار سیستم اطلاعاتی برای دریافت همان داده یکی باشد، همان مکان محل تنظیم قرارداد است، درغیر این صورت قانون‌گذار سه گزینه را پیش‌بینی نموده است:

گزینه اول، اگر طرفین توافق دیگری نکرده باشند، محل ارسال داده پیام، محل تجاری یا کاری اصل‌ساز و محل دریافت داده پیام می‌تواند محل تجاری یا کاری مخاطب محسوب شود.

گزینه دوم، در صورت تعدد محل تجاری و یا کاری اصل‌ساز، نزدیک‌ترین محل به اصل معامله مناط اعتبار برای محل ارسال داده است وگرنه محل اصلی شرکت همانا محل تجاری یا کاری تلقی می‌شود.

گزینه سوم، درصورتی‌که اصل‌ساز ویا مخاطب فاقد محل تجاری یا کاری باشند، اقامتگاه قانونی آنان ملاک خواهد بود. بنابراین مکان انعقاد قرارداد الکترونیکی طبق نظریه ارسال و یا وصول قبول، به‌ترتیب در گزینه‌های توافق طرفین، محل تجاری و یا کاری، محل اصلی شرکت و اقامتگاه قانونی می‌باشد (فیضی چکاپ، ۱۳۸۳).

ممکن است برنامه رایانه‌ای به طور مستقل و خودکار اقدام به انجام تراکنشی‌کند که متضمن ایجاب و قبول بدون دخالت انسان باشد (داده پیام به‌طور هوشمند تولید و با ارسال داده، اراده کاربر را منتقل‌کند)، در اینجا دخالت انسان مثل نامه، فاکس، تلکس، ایمیل، وب‌سایت صرفاً جنبه ناقل بودن

---

۱. این تقارن اصولا در شبکه باز اینترنتی (صفحه وب سایت) به‌شکل فوری و متوالی انجام می‌گیرد. ولی در واسطه پست الکترونیکی به‌طور معمول نسبت این تقارن نیاز به فواصل زمانی دارد.

داشته و سیستم به‌عنوان شخص به رسمیت شناخته می‌شود. بنابراین با توجه به اینکه توافق اولیه اولی بر این گزینه‌ها می‌باشد و قانون‌گذار اجازه توافق خلاف گزینه‌های مندرج در ماده ۲۹ قانون تجارت الکترونیکی را داده است، بانک می‌تواند در شرایط اعلامی اولیه محل استقرار سیستم اطلاعاتی بانک را به‌عنوان مبنای تعیین زمان ارسال و دریافت داده پیام و ملاک تحقق قرارداد تعیین نماید. بدیهی است در صورت عدم درج این شرط و عدم حصول توافق، سه گزینه بالا نقش تعیین‌کننده‌ای در تعیین زمان و مکان انعقاد قرارداد خواهد داشت.

۲- احراز هویت و امضا قرارداد الکترونیکی

اگرچه تجارت الکترونیکی باعث ارتباط سریع و ارزان طرفین و سهولت جمع‌آوری و نگهداری اطلاعات می‌گردد اما امنیت نقش مهمی دارد و باید در رفع مشکلات امنیتی هم پاسخ‌گو باشد (ابراهیمی سروعلیا، ۱۳۹۵: ۲). در شبکه‌های بسته مانند سوئیفت که اعضای آن مشخص است تبادل داده امنیت بالایی دارد چون هویت اعضا قابل احراز هست اما در شبکه‌های جهانی که عمومی هستند امنیت مبادلات و هویت مبادله‌کنندگان اهمیت بیشتری دارد. همین‌طور حمایت از حقوقی مانند فناوری تولید، علایم تجاری، نام‌های معروف و مهم، طرح‌ها و مدل‌ها و علائم موضوع تصدیق‌نامه‌ها (حق امتیاز) یا حق تولید، که تحت حمایت کنوانسیون‌های بین‌المللی‌اند (اصغری واسکندری،۱۳۹۸)، نیازمند حفظ امنیت اطلاعات است. حتی حفظ حقوق اسرار تجاری علی‌رغم پیشینه‌ای طولانی به‌دلیل مسایلی چون گمنامی، سرقت شخصیت، وجود شخصیت دیجیتالی و نفوذ هکرها در عصر فناوری اطلاعات با ابهامات روبه‌رو است (داراب پور و السان وخشنودی، ۱۳۹۸) بنابراین احراز هویت نقش مهمی در حفظ امنیت اطلاعات، اسرار تجاری و جلوگیری از جرایم مربوطه دارد. به‌عنوان نمونه، تحقیقی برای پیدا کردن بهترین روش احراز هویت با رعایت محرمانگی و یکپارچگی اطلاعات در شش بانک فعال در امارات نشان داد که ارتقای روش‌های احراز هویت باعث کاهش خطرات می‌شود و سیستم شناسایی مؤثر باعث جلوگیری از ضرر مالی و خسارات ناشی از کلاهبرداری، سرقت و افشای اطلاعات می‌شود (بنی هنیا و همکاران[1]، ۲۰۲۳). علاوه‌بر احراز هویت، بکارگیری ابزارهای الکترونیکی و نظارت دقیق‌تر بر تراکنش داده پیام‌های الکترونیکی نیز باعث کاهش چشمگیر تدلیس و کلاهبرداری و نقض مقررات می‌گردد (کری، ۲۰۱۳). برای ممانعت از دستبرد سارقین کامپیوتری در فضای الکترونیکی که همواره مترصد خواندن مستندات می‌باشند،

1. Bani-Hania et al

لازم است این اسناد به‌صورت رمز درآمده و امضای دیجیتالی شود، امضای دیجیتالی تضمین‌کننده اصالت، کامل بودن و عدم وجود خدشه می‌باشد (سجادی وجعفری، ۱۳۹۸). با توجه به اینکه پرداخت دیجیتال سالانه ۱۲/۷ درصد رشد داشته، بنابراین پیش‌بینی شد تا پایان سال ۲۰۲۰ عدد تراکنش‌ها به ۷۲۶ میلیارد تراکنش برسد و ۶۰ درصد کل جهان را در بر گیرد. این آمار اهمیت سیستم ID دیجیتال (شناسایی دیجیتال) را به‌عنوان روشی متکی بر شناسه دیجیتال (CDD[1]) برای اطمینان از عدم وقوع خطرات پول‌شویی و شناسایی روابط و معاملات پرخطر نشان می‌دهد[2]. در عرصه بانکداری الکترونیکی نیز تهدیدها و حملاتی مانند فیشینگ، سرقت هویت، پول‌شویی باعث شد بانک‌ها در جستجوی بهترین روش احراز هویت باشند. در واقع احراز هویت، فرآیندی است که طی آن ارسال‌کننده یا دریافت‌کننده اطلاعات، مطمئن می‌شود طرف مقابل همانی هست که ادعا می‌کند؛ به‌نوعی تا اعتمادی ایجاد نشود، تبادل اطلاعات صورت نمی‌گیرد. این فرآیند می‌تواند بسیار ساده یا بسیار پیچیده و دشوار باشد. ساده‌ترین راهکار احراز هویت، استفاده ازکلید احراز هویت متنی به‌عنوان پسورد یا رمز عبور است که علاوه‌بر آن استفاده از ابزار فیزیکی که باید در زمان احراز هویت همراه فرد باشد مانندکارت شناسایی نیز رایج است. همین‌طور بعضی از خصوصیات بیومتریک شامل چهره (اندازه‌گیری فاصله بین نقاط خاصی روی صورت) اثر انگشت (اندازه‌گیری فاصله بین خطوط روی انگشت) صدا (اندازه‌گیری الگوی صوتی در گفتار انسانی برای عبارات از پیش تعیین‌شده) هم عامل احراز هویت زیست‌سنجی هستند. در برخی موارد جایی که شخص آنجاست، مانند یک ترمینال کامپیوتری که از طریق آن وارد شده‌اند یا شماره تلفن شهر یا کشوری که از آنجا تماس گرفته‌اند مبنایی برای احراز هویت قرار می‌گیرد. در عین حال تأیید هویت اشخاص توسط شاخص بیومتریک و به‌کمک شناسایی از طریق امواج رادیویی (RFID) در هر مکان و زمان قابل انجام است و باعث می‌شود علاوه‌بر اینکه تعاملات الکترونیکی در فضایی امن صورت گیرد و از تکرار موارد معمول مانند تایپ کردن رمز عبور و اطلاعات شخصی پیشگیری شود، اساسا پایگاه داده‌ای متمرکز ایجاد می‌کند که قابلیت جستجو و بروزرسانی دارد (پیروی وجعفری، ۱۳۸۸). همین‌طور راه‌حل مبتنی بر کارت هوشمند برخلاف راه‌حل توکن تجاری (که در آن کلیدها اغلب توسط سازنده توکن درخارج از کشور تولید می‌شوند) به‌طور قابل توجهی امکان کنترل کلید توسط مؤسسه مالی را از طریق مدیریت حوزه

1. Customer Due Diligence (شناسایی دقیق مشتری)
2. Guidance on Digital ID 2020

قضایی ملی فراهم می‌کند (هیلتگن، ۲۰۰۶). راه‌حل‌های احراز هویت موبایل نیز قابل توجه است اما حملات پیچیده‌تر کلاینت پلتفرم در آینده قابل پیش‌بینی می‌باشد.[1]

قانون نمونه آنسیترال (امضای‌الکترونیکی) به موضوع احراز هویت امضاکننده داده پیام و امکان تأیید قصد امضاکننده مبنی‌بر تأیید پرداخت و معیارهای عملی برای اطمینان به امضا، ارائه و ارتباط بین اطمینان فنی از امضا و اثر حقوقی آن و رابطه امضای الکترونیک با امضای دیجیتال را مطرح می‌نماید (امضای دیجیتالی نوعی از امضای الکترونیکی است که پیشرفته و قابل اطمینان بوده و ارزش اثباتی بالایی دارد). در کشورهایی که هر دو قانون نمونه را پذیرفته‌اند امضای دیجیتالی ارزش اثباتی دارد و در کشورهایی که فقط قانون تجارت الکترونیکی را پذیرفته‌اند امضایی ارزش دارد که شرایط ماده ۷ قانون را داشته باشد، حتی اگر دیجیتال باشد. ماده ۷ مقرر می‌دارد چنانچه در داده پیام روش مطمئنی اتخاذ شود که اولا هویت امضاکننده را نشان‌دهد و ثانیا قصد وی مبنی‌بر تأیید محتوی داده پیام را تأیید کند در این صورت داده پیام مزبور به منزله امضا شده تلقی می‌شود (شیروی، ۱۴۰۰) .

در قانون تجارت الکترونیکی ایران، امضای الکترونیکی هر نوع علامت منضم‌شده یا متصل‌شده به داده پیام از قبیل اسم، رمز، کلمه، عدد، تصویر دیجیتالی از امضای دستی و هر نشان الکترونیکی است که به سند منضم و یا ملحق شده باشد و ارتباط امضاکننده با داده را مشخص نماید. انواع امضاهای الکترونیکی عبارتند از: ۱- وارد کردن اسم، علامت و یا هر نوع نشانه در ذیل سند الکترونیکی مثل نوشتن نام و نام‌خانوادگی و یا هر علامت دیگر در ذیل نامه الکترونیکی ۲- وارد کردن تصویر اسکن شده امضای دستی به سند الکترونیکی ۳- وارد کردن تصویر امضای دستی به سند الکترونیکی از طریق قلم نوری (فرد روی صفحه رایانه‌ای امضا می‌کند و تصویر آن عینا در رایانه نمایش داده شود) ۴- امضای بیومتریک که بر ویژگی زیست‌شناختی فرد از قبیل اثر انگشت، شکل گوش، چشم، نحوه امضا) مبتنی است ۵- استفاده از رمز هویت شخصی که با کلمه عبور منضم می‌شود ۶- امضای دیجیتال که با استفاده از کلید عمومی و کلید خصوصی صورت گیرد (همان، ۱۴۰۰).

امضای الکترونیکی به دو گروه باینری و دیجیتالی به‌معنای عام تقسیم می‌گردد؛ امضای باینری صورت ساده از امضای الکترونیکی است که در خریدوفروش‌های اینترنتی، انجام معاملات فاقد حساسیت و در دادرسی الکترونیکی مورد استفاده قرار می‌گیرد. امضای دیجیتالی در معنای عام به دو

1. https://www.researchgate.net/publication.pag1

نوع بیومتریکی و دیجیتالی در معنای خاص تقسیم می‌شود. نوع بیومتریکی در نظام حقوقی ایران ازجمله ثبت الکترونیکی اسناد، ثبت مالکیت‌های فکری و انجام معاملات مورد پذیرش قرارگرفته است. نوع دیجیتالی آن در نظام حقوقی امریکا به‌عنوان ابزار انعقاد قراردادهای هوشمند در نظام نوین مبادلاتی به‌کار می‌رود (صادقی و ناصر، ۱۳۹۹)، زیرا امضای دیجیتالی به‌دلیل برخورداری از فناوری رمزنگاری دادها و کلیدهای عمومی و خصوصی جهت تضمین و تصدیق هویت استفاده‌کننده، منجر به تضمین صحت تراکنش‌های داده پیام‌های الکترونیکی می‌گردد، ازاینرو انکار محتوای چنین امضایی امکان‌پذیر نیست. به‌دلیل وجود چنین ضریب امنیتی امروزه بسیاری از تجار در مبادلات از این نوع امضا استفاده نموده و حتی استفاده از آن به‌عنوان یکی از شرایط ایجاد اعتماد مابین طرفین معامله در عرف مبادلات تلقی می‌گردد. به‌عبارت دیگر به‌دلیل اینکه کاربران این نوع امضاها دارای بانک‌های اطلاعاتی مطمئن در نظام حقوقی کشورهای متبوع خود هستند، وجود چنین امضایی در مبادلات آن‌ها به‌طور کامل مبین دقیق هویت آن‌ها می‌باشد. شاید شاخص‌ترین ویژگی این نوع از امضای الکترونیکی نسبت به سایر گونه‌ها تضمین و شناسایی دقیق هویت افراد و رمزگذاری مدارک است. درکانادا، بریتانیا، استرالیا و نیوزیلند نیز امضای دیجیتال را پذیرفتند اما اینکه کدام امضا کامل‌تر است مربوط به متخصصین است نه مقنن. در کشورهای تابع حقوق رم همچون ایتالیا، آرژانتین و آلمان نوع فناوری برای امضای الکترونیکی مورد شناسایی مقنن قرارگرفته و شرایط کامل معاملات الکترونیک اعم از موانع و محدودیت‌ها مشخص‌گردیده است. اما گسترش روزافزون روش‌های تجارت الکترونیک باعث شده که قانون‌گذاری همه جانبه به‌دلیل احتمال اشتباه میسر نباشد. بنابراین پرداختن به تمام مسائل و جزئیات راجع به تجارت الکترونیک در قانون امکان‌پذیر نیست و اشکالات و نواقص معاملات الکترونیک با تکیه بر تجربه دیگر کشورها و یا تجربه داخلی با رویه قضایی، عرف تجاری داخلی و بین‌المللی قابل رفع است کمااینکه حقوق ایران و فرانسه به این سو گرایش دارند. درمواد ۱۰ و ۱۱ قانون تجارت الکترونیکی ایران، امضا و سابقه الکترونیک مطمئن تعریف و آثار حقوقی آن بیان‌شده، لکن فناوری خاصی به رسمیت شناخته نشده است؛ چون رسمیت بخشیدن به یک فناوری مشخص به‌عنوان مبنا و نمونه می‌تواند منجر به کنار گذاشتن سایر روش‌ها شود.

۳- وضعیت پول‌شویی در بانکداری الکترونیکی

با توجه به اینکه طبق مقررات بین‌المللی از جمله توصیه شماره ده FATF [1] و ماده ۷ قانون مبارزه با پول‌شویی ایران، احراز هویت مشتری نقش مهمی در مبارزه با پول‌شویی دارد ازاین‌رو ممکن است تصور شود که بانکداری الکترونیکی به‌دلیل عدم حضور مشتری باعث تسهیل پول‌شویی می‌شود، درصورتی‌که احراز هویت الکترونیکی نه‌تنها زمینه‌ساز پول‌شویی نیست بلکه روش‌های مبتنی‌بر هوش مصنوعی غیرتحلیلی و روش‌های خودکار و دسته‌بندی[2] مانند شبکه‌های عصبی مصنوعی می‌تواند با شناسائی الگوهای رفتاری سوابق مشتری و تطبیق آن با الگوهای تمیز، نسبت به بررسی رفتارهای متقلبانه مشتری پرداخته و مخاطرات پول‌شویی در بانکداری الکترونیکی را مورد شناسائی قرار دهد و به‌همین دلیل توصیه ۱۶ مقررات FATF به نقل و انتقالات الکترونیکی پرداخته و با الزام به پیش‌بینی اطلاعات فرستنده و ذینفع موجبات شفافیت بیشتر را فراهم کرده است (ارجمندنژاد و مهجوریان، ۲۰۱۳). در برخی موارد روش‌های هوشمند بدون ناظر[3]، استانداردی برای تأیید امنیتی برنامه‌های کاربردی مبتنی بر وب ASVS[4] ارائه نموده است که امنیت احراز هویت الکترونیکی را با در نظر گرفتن نیازمندی‌های امنیتی ارائه شده توسط ASVS در فازهای چرخه حیات تولید برنامه‌های تجارت الکترونیکی مطرح می‌کند (اصغری و قلی زاده ومدیری، ۱۳۹۲). درهرصورت اگر با شناسائی الگوی حاکم بر تبادلات مالی نسبت به شناسائی الگوی مبادلات مجاز اقدام شود در صورت مشاهده رفتار خارج از الگو، سیستم هوشمند می‌تواند با صدور اخطار لازم، مانع وقوع برخی از مخاطرات پول‌شویی در بانکداری الکترونیکی شود. به‌منظور پیاده‌سازی نظام اجرایی الکترونیک قوی با شبکه متمرکز و هوشمند لازم است در نخستین گام شاخص‌ها و پارامترهایی برای بررسی عملکرد و ارزیابی مشتری تعریف شود. شاخص‌هایی مانند قابلیت اعتماد، مقاومت، زمان پاسخ، کیفیت خدمات، قابلیت تحمل خطا و انعطاف‌پذیری به‌عنوان زبان مشترک کارشناسان و مدیران در سامانه‌ها دیده شود. این نظام با بهره‌گیری از تلفیق هوش مصنوعی و نظرات فردی مبتنی‌بر خبرگی همگام با پیشرفت‌های دنیا و منطبق با بافت اقتصادی و نوع گردش پول هر کشور عمل می‌کند و قابلیت اجرا

1. Financial Action Task Force
2. classification
3. Unsupervised Intelligent learners
4. Application Security Verification Standard

با الگوریتم روش‌های یادگیری هوشمند بدون ناظر[1] و روش‌های یادگیری هوشمند با ناظر[2] را به‌طور همزمان دارد (گوگردچیان و صادقی عمروآبادی وشهبازی، ۱۳۹۰).

با توجه به اینکه در بانکداری الکترونیک، ارتباط با کاربر با استفاده ازروش‌های الکترونیکی و بدون ارتباط مستقیم انسانی انجام می‌شود و شناخت مستقیمی در مورد کاربر به‌دست نمی‌آید، به همین دلیل توسعه و گسترش تشکیلات سازمان‌یافته‌ی پول‌شویی همزمان با پیدایش بانکداری الکترونیک تا حدودی نگران‌کننده است. شناسایی و احراز هویت مشتری از حیث مقررات مبارزه با پول‌شویی در خدمات پایه، به‌دلیل حساسیت و شرایط خاصی که دارند و اینکه می‌توانند پایه سایر خدمات بانکی محسوب شوند مورد تأکید مؤکد قرارگرفته و به همین دلیل، قانونگذار ایران درسال ۱۳۹۸ ارائه خدمات پایه به ارباب‌رجوع را به‌صورت غیرحضوری ممنوع نمود[3]، اما ضرورت ارائه غیرحضوری خدمات پایه موجب شد تا هیات وزیران در مصوبه ۱۳۹۹/۱۱/۲۹، ارائه خدمات پایه غیرحضوری را با رعایت دستورالعمل مصوب شورای عالی مقابله و پیشگیری از جرائم پول‌شویی و تامین مالی تروریسم مجاز نماید. دستورالعمل مورد نظر در تاریخ ۱۴۰۰/۱۲/۲۴ توسط شورا تصویب و براساس آن خدمات پایه غیرحضوری منوط به احراز هویت الکترونیکی گردید. در واقع احراز هویت الکترونیکی جایگزین احراز هویت حضوری شد و ابزارهای زیست‌سنجی (بیومتریک) مانند امضای دیجیتال، اثرانگشت، تصاویرعنبیه، تشخیص صدا، هندسه دست، الگوی تایپ و نظایر آن وسیله شناسایی و احراز هویت قرارگرفت. همین‌طور عامل مالکیت (مانندکارت بانکی یا برنامه موبایل) و عامل دانستنی (مانند رمزکارت بانکی یا رمز پویا) به‌عنوان عوامل ثبت هویت قلمداد شدند. بااین‌حال برخی خدمات پایه حساس و پرریسک مانند افتتاح حساب جاری، اعطای تسهیلات تجاری و صدور ضمانت‌نامه تجاری کماکان منوط به مراجعه حضوری مشتری اعلام شد. با توجه به اینکه جامعه بین‌المللی ترکیبی از کشورها و رابطه‌های گوناگون است، جریان صحیح این رابطه‌ها طلب می‌کند قاعده‌هایی حاکم باشد و حقوقی مخصوص آن جامعه و متمایز از حقوق داخلی یکایک کشورها، برای مطالعه آن قاعده‌ها وجود داشته باشد (سلجوقی، ۱۳۹۸). به‌عنوان نمونه در صنعت بانکداری، بانک‌ها در برخی کشورها اقدام به تقسیم‌بندی حساب‌ها کرده‌اند به این صورت که برخی حساب‌ها صرفاً به‌صورت حضوری افتتاح شده اما کارتی به مشتری داده نمی‌شود و مشتری می‌تواند حداقل کارکرد از

---

1. Unsupervised
2. Supervised

۳. تبصره ۳ ماده ۹۱ آیین‌نامه اجرائی ماده ۱۴ الحاقی قانون مبارزه با پولشویی مصوب ۱۳۹۸.

حیث مانده و سقف برداشت، واریز و انتقال را داشته باشد. در برخی حساب‌ها، مشتری اجازه افتتاح به‌صورت غیرحضوری و نقل و انتقال الکترونیکی وجه را دارد اما محدودیت‌های آن‌ها کمتر از دسته اول هست. دسته سوم شامل حساب‌هایی است که هیچ محدودیت واریز و برداشت و مانده مبلغ ندارند مانند تمام حساب هایی که در نظام بانکی کشور وجود دارد (مهجوریان، ۱۴۰۱)؛ اما حساسیت خاص مقررات مبارزه با پول‌شویی و فراملی بودن جرم پول‌شویی ایجاب می‌کند که مقررات واحدی برای کلیه کشورها تنظیم شود تا وحدت رویه صورت گیرد. به‌همین منظور در راستای مبارزه با پول‌شویی، سازمان‌های بین‌المللی اقدام به تدوین مقررات یکسانی ازجمله توصیه‌های **FATF** نمودند که بر لزوم شناسایی مشتری و اخذ مستندات شناسایی تاکید دارد. حتی در نقل‌وانتقالات الکترونیکی داخل‌کشور نیز، مؤسسه مالی که صادرکننده دستور پرداخت مکلف شده است از وجود اطلاعات مربوط به فرستنده و ذینفع اطمینان حاصل نموده و اگر به‌دلیل محدودیت‌های فنی، امکان نگهداری اطلاعات برون‌مرزی در نقل و انتقال داخلی میسر نبود باید سوابق اطلاعات دریافتی ازمؤسسه مالی واسطه، حداقل به‌مدت ۵ سال نگهداری شود (ارجمند نژاد و مهجوریان، ۲۰۱۳). این تکالیف نشان می‌دهد که احراز هویت، اخذ اطلاعات و مستندات لازم در خصوص شغل و اقامتگاه مشتری و نگهداری آن، نقش بسزایی در جلوگیری از پول‌شویی دارد. به‌همین دلیل در مقررات مبارزه با پول‌شویی و توصیه‌های **FATF** تاکید شده است که مشتری باید مدارک هویتی، شغلی و اقامتگاه خود را به بانک ارائه دهد تا بتواند خدمات بانکی دریافت نماید (فصل پنجم آیین‌نامه مبارزه با پول‌شویی و توصیه ۱۰ گروه **FATF**)، اما ممکن است برخی اقشار محروم به‌دلایل مختلف قادر به ارائه مدارک و مستندات مورد نیاز همچون اسناد احراز هویت یا احراز اقامتگاه و شغل نباشند و به‌همین دلیل از دریافت خدمات بانکی محروم گردند. حسب راهنمای شناسه دیجیتال۲۰۲۰ در دنیا، ۱/۷ میلیارد بزرگسال بدون بانک در سراسر جهان وجود دارند که ۲۶ درصد آنان کمبود اسناد را مانع اصلی دریافت خدمات بانکی می‌دانند. شناسه دیجیتال و احراز هویت الکترونیکی می‌تواند به افراد بدون هویت سنتی اجازه دسترسی به خدمات مالی بدهد و بهبود شمول مالی داشته باشند. در واقع شناسه دیجیتال قابل اعتماد می‌تواند شناسایی افراد در بخش مالی را آسان‌تر، ارزان‌تر و ایمن‌تر نموده و به الزامات نظارت بر تراکنش‌ها کمک کند.[1] همین‌طور با استفاده از روش‌های احراز هویت الکترونیکی از جمله شناسایی بیومتریک می‌توان برای افراد فاقد مدارک هویتی، حساب‌های با کارکرد محدودتر در نظر گرفت تا هم نیازهای مالی آنان برطرف شود و هم الزامات شناسایی مشتری

1. Guidance on Digital ID 2020

سهل‌گیرانه باشد تا ریسکی متوجه بانک نشود. بنابراین احراز هویت الکترونیکی نه تنها باعث تسهیل پول‌شویی نمی‌شود بلکه موجب حفظ مشتریان توانمند ازحیث ارائه خدمات سهل، راحت و سریع شده و به مشتریان ضعیف و محرومی که به‌دلیل فقدان مدارک شناسایی قادر به ارائه مستندات نیستند نیز کمک می‌نماید؛ از جمله مشتریانی که نیازمند حداقل یک حساب بانکی برای دریافت کمک‌های مالی از قبیل یارانه و غیره می‌باشند اما قادر به ارائه مستندات شغلی و اقامتی نیستند. این مهم در نسخه تکمیلی **FATF** دیده شده است[1].

٤- ارزش اثباتی اسناد الکترونیکی

صرف‌نظر از چگونگی اخذ امضا در بانکداری الکترونیکی، اساسا سندیت امضا به‌عنوان داده پیام در سطح ملی و بین‌المللی با توجه به ماهیت مجازی و غیرمادی مبادلات، اهمیت زیادی دارد. در ایران براساس قانون تجارت الکترونیکی داده پیام به‌جز اسناد مالکیت غیرمنقول، مواد دارویی، هشدارهای خاص کالاها، جایگاهی همانند اسناد مکتوب داشته و امضای آن دارای ارزش اثباتی است. به‌همین منظور دفاتر ثبت الکترونیکی در صورت احراز صدور امضا از سوی متقاضی، نسبت به ثبت طی تشریفات اقدام می‌نمایند و داده پیام مطمئن در صورت رعایت موارد فوق، درحکم سندرسمی بوده و قابل انکار و تردید نمی‌باشد. درهرصورت ادله الکترونیکی، اصولا به‌عنوان ادله اثبات می‌توانند سند یا اماره محسوب شوند (میرشکاری و علایی،۱۳۹۹: ۲). برخی امضاها مطمئن و برخی غیرمطمئن هستند؛ امضای غیرمطمئن در صورتی سندیت دارد که یا توسط صادرکننده تأیید شود یا حداقل انکار نشود و یا با قرائن و امارات، انتساب آن به صادرکننده مسجل گردد. مطابق ماده ۱۰ قانون تجارت الکترونیکی، امضای مطمئن باید نسبت به امضاکننده منحصربه‌فرد بوده و هویت امضاکننده داده پیام را معلوم نماید به‌نحوی‌که به داده‌پیام متصل‌شده و هر تغییری در آن قابل تشخیص و کشف باشد. برای ایجاد امضای الکترونیکی مطمئن از فناوری‌های مبتنی‌بر رمزنگاری استفاده می‌شود که یا به‌شیوه متقارن است یعنی رمز و کلید واحد برای رمزگشایی و رمزنگاری از سوی طرفین تعریف شود یا به شیوه غیرمتقارن است یعنی از دو کلید عمومی و خصوصی برای رمزنگاری و رمزگشایی استفاده شود. اگر با کلید عمومی رمزنگاری شود با کلیدخصوصی فقط باز می‌شود و اگر با کلیدخصوصی رمزنگاری شود فقط با عمومی باز می‌شود. شیوه متقارن دارای اشکالاتی است ازجمله اینکه باید برای

---

1. https://www.fatf-gafi.org/en/publications/Fatfgeneral/Financial-inclusion-cdd-2017.html.

هر شرکت به تعداد تجار کلید صادر شود و کلید باید به روش مطمئن ارسال شود تا به دست سارقان نیفتد. به‌همین دلیل برای مشتریان اتفاقی و غیردائمی کاربرد ندارد. امضای دیجیتالی یا سایر فنون رمزنگاری ریاضی زیر مجموعه امضای الکترونیکی قابل اثبات هستند (زرکلام، ۱۳۸۲). در شیوه هاش[1] به دلیل عبور سند از پردازش‌های ریاضی یک الگوریتم (شکل فشرده دیجیتال یک سند الکترونیک که چکیده یا ارزش هاش نامیده می‌شود)، ارزش منحصر به فرد سند به آن متصل و ارسال می‌شود به‌گونه‌ای که دریافت‌کننده با کلید خصوصی ارزش هاش را رمزگشایی می‌کند. اگر ارزش هاش ارسالی با دریافتی یکی باشد سند مطمئن محسوب شده و جعلی نمی‌باشد. این شیوه هم اشکالاتی دارد چون کلید عمومی و خصوصی، صرفا اصالت سند را تأیید می‌کند و هویت ارسال‌کننده را تأیید نمی‌کند زیرا ممکن است فرد جعلی در سایت جعلی کلید عمومی و خصوصی تعریف کند (شیروی، ۱۴۰۰). به‌منظور تایید هویت صاحب کلید عمومی، دفاتر خدمات صدور گواهی الکترونیکی یا مقامات گواهی‌کننده در ماده ۳۱ قانون تجارت الکترونیکی ایران پیش‌بینی شده است که گواهی صادره طبق ماده ۱۹ آیین‌نامه اجرایی مصوب ۱۳۸۶، در صورت تقاضای صاحب گواهی یا تخطی صاحب گواهی، یا احراز اشتباه در صدور گواهی، یا اشتباه متقاضی و یا احراز عدم رضایت صاحب آن و افشای کلید خصوصی نزد افراد غیرمجاز باطل می‌شود (همان منبع، ۱۴۰۰). حتی گواهی صادره از مراجع خارجی نیز در صورت توافق مرکز ریشه و مرجع خارجی و رعایت اصل شرط عمل متقابل و تصویب شورا قابل پذیرش است. بنابراین در بانکداری الکترونیک، امضای مشتری ذیل قرارداد الکترونیکی در صورت رعایت موارد فوق، دارای ارزش اثباتی هم‌ردیف اسناد رسمی بوده و قابلیت انکار و تردید ندارد. درخصوص قانون حاکم بر شکل سند، قانون محل تنظیم، بنابه مصلحت دولت محل تنظیم سند از یک طرف و منافع خصوصی افراد از طرف دیگر مبنا قرار گرفته است (الماسی، ۱۴۰۰: ۲۹۹). یکی از اسناد الکترونیکی در سیستم بانکی، اسناد تجاری است که برخی عقیده دارند به‌عنوان وسیله پرداخت نقشی نظیر پول دارند (اسکینی،۱۳۹: ۸) و برخی عقیده دارند معرف طلبی به سررسید مدت کم هستند (ستوده تهرانی،۱۳۷۵: ۱۳). درهرصورت به جهت ایجاد وحدت رویه در بین کشورها کنوانسیون ژنو تشکیل شده است. دولت ایران علی‌رغم اینکه به کنوانسیون ژنو راجع به برات و سفته و چک ملحق نگردیده است، اما مختصر بودن قانون تجارت ایران و فراوانی موارد سکوت و اجمال، حقوقدانان را ناگزیر نموده است که در موارد عدیده برای تفسیر قانون تجارت به متون مزبور استناد نمایند (کاویانی، ۱۳۹۳: ۴۲). این کنوانسیون مقررات متحدالشکلی را تعریف نموده

1. Hash

است اما خطر وقوع پول‌شویی منجر به ایجاد کنوانسیون‌های مختلفی در این خصوص گردید که بحث احراز هویت و امضای الکترونیکی در چک الکترونیکی نیز از این قاعده مستثنی نیست. چک الکترونیکی یک ابزار نوین پرداخت، متشکل از امنیت، سرعت و دارای فرآیند بازدهی تمام تراکنش‌های الکترونیکی همگون و توام با زیرساخت قانونی گسترش‌یافته صحیح است که قابلیت جایگزینی با چک‌های کاغذی در فرآیندهای تجاری را دارد (زنگباری، ۱۳۹۱: ۲۱۶). درهرصورت شناسایی دقیق صادرکننده و دارنده چک و ظهرنویسان چک، مستلزم ثبت اطلاعات و امضای دقیق آنان می‌باشد که مقررات مبارزه با پول‌شویی در این خصوص کمک‌کننده است. قانون اصلاحی قانون صدور چک در سال ۱۳۹۷ و لزوم ثبت اطلاعات دقیق دارندگان چک در سامانه صیاد یکی از مواردی است که کمک بزرگی به شناسایی مشتری در راستای ردیابی وجوه و احراز هویت دارندگان چک می‌نماید.

در آمریکا ثبت الکترونیکی اسناد معاملات بین طرفین و رسمیت بخشیدن به آن‌ها منوط به شناسایی دقیق هویت متعاملین و وجود شاخص‌های قانونی جهت ثبت معاملات می‌باشد که استفاده از امضاهای الکترونیکی دیجیتالی یکی از امارات تحقق هدف مذکور است. ماده ۱۲ کنوانسیون ملل (ارتباطات الکترونیکی)[1] انعقاد قرارداد از طریق نمایندگی هوشمند را برای طرفینی پیش‌بینی نموده که محل تجاری آنان درکشورهای مختلف قرار دارد، در واقع احراز اهلیت متعاملین در قراردادهای هوشمند با استفاده از امضای دیجیتالی صورت می‌گیرد (مافی و ناصر، ۱۴۰۰)؛ کما اینکه در قانون نمونه دفاتر اسناد رسمی امریکا (حسب بند ۲-۱۶) دفتر ثبت الکترونیکی باید احتیاط متعارف را به‌عمل آورده و اطمینان یابد که نرم‌افزار مورد استفاده برای ایجاد امضای دیجیتالی به‌روز بوده و به هنگام تقاضای تصدیق، ثبت امضا از سوی متقاضی از اعتبار نیفتاده باشد (اسدی، ۱۳۹۷). درکانادا قانون متحدالشکل تجارت الکترونیکی (۱۹۹۹) براساس قانون نمونه آنسیترال تنظیم و داده پیام همانند نوشته اعتبار دارد و انعقاد قرارداد توسط نمایندگی هوشمند مورد شناسایی قرارگرفته است.

۵-خلاء مقرراتی

افزایش دامنه بانکداری الکترونیکی مستلزم بازنگری مقررات و سیاست‌های اقتصادی به‌ویژه هماهنگی بیشتر در سطح بین‌المللی است (نصولی واسچیچتر، ۲۰۰۲: ۱). احراز هویت الکترونیکی نیاز به زیرساخت‌های فنی و حمایت قانونی دارد که نبود هر کدام می‌تواند مانع محسوب شود. با

---

۱. این کنوانسیون در ۲۰۱۳ لازم‌الاجرا شد، کشور ایران علی‌رغم امضا هنوز ملحق نشده است.

توجه به اینکه موانع بانکداری الکترونیک در چهار دسته موانع حرفه‌ای و فنی، قانونی و اجتماعی، استراتژیک و مالی و اقتصادی قابل طبقه‌بندی است، تحقیق بین صد نفر از کارشناسان E-Banking نشان داده که به‌جز موانع مالی و اقتصادی سایر موارد، مانع اصلی محسوب می‌شوند (علینژاد ساروکولی، ۲۰۱۲). ازاینرو می‌توان مشکلات فنی احراز هویت و اخذ امضای الکترونیکی در بانکداری الکترونیکی را جزو موانع فنی و قانونی به‌حساب آورد. به‌عنوان نمونه براساس مطالعه میدانی در بانک انصار، ۳۹ عامل متمایز و مؤثر در توسعه بانکداری الکترونیک بدست آمده که پس از تحلیل، عوامل مدیریتی، فناوری به‌عنوان عوامل اصلی شناخته شده و عواملی مانند عدم ایجاد تغییرات مناسب در سیستم پرداخت و کمبود بودجه برای تجهیزات فنی به‌عنوان عوامل کم اهمیت شناخته شده است (خوش هیکل و غریب، ۱۳۹۵). صرف‌نظر از عوامل فنی، اساساً وقتی روابط بانکی از مرزها فراتر می‌رود، تمسک به مقررات موجود برای مدیریت و نظام‌مندکردن آن کفایت نمی‌کند و تنظیم مقررات دقیق راجع به بانکداری الکترونیکی در داخل کشور و همکاری با دیگر کشورها در گسترش ایمن این شیوه از بانکداری و تدوین مقررات تسهیل‌کننده ضرورت دارد (السان و علی دادی، ۱۳۸۸). مقررات راجع‌به بانکداری الکترونیکی باید علاوه‌بر شفافیت، مقتدرانه و توام با ضمانت اجرا باشد به‌گونه‌ای که علاوه‌بر استفاده از فناوری‌های‌جدید و ایمن‌سازی فرآیند با وضع مجازات‌های دقیق و بازدارنده، مجرمان را از اخلال در نظام بانکی منع نمایند. مطالعه تطبیقی پژوهش انجام‌شده توسط پژوهشکده پولی‌وبانکی ایران در سال ۱۳۸۸ بر مبنای حقوق کشورهای امریکا و انگلیس و مقررات آنسیترال و در میان کشورهای اسلامی نشان می‌دهد کشور مالزی به‌عنوان پیشگام در بانکداری اینترنتی اسلامی می‌باشد (همان منبع، ۱۳۸۸). قواعد حاکم بر این نوع از بانکداری در مالزی به‌موجب مقرراتی ازجمله قانون موسسات بانکی‌ومالی مصوب ۱۹۸۹[1]، قانون بانکداری‌اسلامی مصوب ۱۹۸۳[2]، راهبرد حداقلی بانک مرکزی در مقررات راجع‌به ارائه خدمات بانکی اینترنتی از سوی موسسات مصوب ۲۰۰۰[3]، لایحه حمایت از داده‌های شخصی مصوب ۱۹۹۸[4] و قانون جرایم رایانه‌ای مصوب ۱۹۹۷[5] مشخص شده است. اندیشمندان مالزی با تأکید بر اینکه دین اسلام حامی

1. Banking and Financial Institution ACT 1989 (BAFIA)
2. Islamic Banking ACT 1983.
3. The Central Banks of Malaysia Minimum Guidelines on the Provision of Internet Banking, Services. Which was issued in MAY 2000
4. Personal Data Protection Bill 1998
5. Computer Crimes ACT (1997-Supp2000)

نوآوری‌وابتکار بوده و از این حیث در میان تمام ادیان و مذاهب سرآمد می‌باشد مانعی برای معاملات الکترونیکی نیافته‌اند (جاواهیتا و نورریحان، ۲۰۰۳) و سعی در توسعه بانکداری الکترونیکی داشتند.

مقررات مالزی حاوی نکات مهمی است که می‌تواند در تدوین مقررات بانکداری الکترونیکی ایران مورد توجه قرارگیرد؛ از جمله می‌توان به مواردی مانند راهبرد بانکداری برخط، محرمانگی معاملات بانکی در فضای اینترنت، همچنین مسئولیت مدنی برای عامل افشای اطلاعات محرمانه در جهت صیانت از حریم خصوصی و جرم‌انگاری موارد نقض و پیشگیری از نفوذ افراد غیرمجاز به سیستم اطلاعاتی و کشف فوری چنین افعالی اشاره نمود (السان و علی دادی، ۱۳۸۸). مقررات ایران ازجمله قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۳/۵ همه موارد ازجمله رمزگیری و جعل هویت را پوشش نمی‌دهد. اگرچه برخی از مواد قانون جرایم رایانه‌ای با تفسیر قابل انطباق است اما پیشنهاد می‌شود برای حمایت از گسترش بانکداری الکترونیکی صراحتا جرم انگاری شود و مقررات با استانداردهای جهانی همگام‌سازی شود. به‌عنوان نمونه به‌جای تحمیل عواقب سهل‌انگاری مشتری در حفظ رمز خود به بانک‌ها [۱] بهتر است طبق قاعده اقدام، مسئولیت عواقب عملکرد هر شخص متوجه خودش باشد. در واقع باید بین بی‌احتیاطی نظام بانکی با بی‌احتیاطی مشتری تفکیک قائل شد. علاوه‌بر لزوم ایجاد هماهنگی بین مقررات کشورها، مشکلات داخلی سازمانی (مانند ضعف تشکیلات منسجم بین بانکی، مطلوب نبودن پهنای باند و پایین بودن ضریب نفوذ اینترنت) و مشکلات انسانی (مانند کمبود نیروهای متخصص و مجرب توسعه بانکداری الکترونیکی، فقدان سخت‌افزار مانند گران‌بودن نظام بانکداری‌الکترونیک، عدم امکان خرید به‌دلیل تحریم‌ها و مشکل ارتباط با شبکه‌های جهانی) از دیگر چالش‌های بانکداری الکترونیکی محسوب می‌شود که در این مقاله مجال پرداختن به آن‌ها نیست و هرکدام تحقیقی مستقل می‌طلبد. بدیهی است مزایایی بانکداری الکترونیکی ازجمله بالا رفتن کیفیت و سرعت خدمات بانکی، کاهش ترافیک و آلودگی هوا، کاهش هزینه چاپ اسکناس، نهایتاً افزایش رضایت‌مندی مشتریان وکاهش فساد اداری در حدی اهمیت دارد که رفع کامل مشکلات جهت ورود به این عرصه را اجتناب‌ناپذیر می‌نماید (تقی نتاج و دیرمینا، ۱۳۹۰) و جا دارد تحقیقات بیشتری دراین‌خصوص صورت گیرد.

---

۱. بخشنامه مورخ ۱۳۹۸/۰۲/۲۲ بانک مرکزی که عواقب ناشی از سهل‌انگاری مشتری در حفظ رمز خود را متوجه بانک‌ها نمود، نمونه عینی از این مقررات است.

جمع‌بندی و نتیجه‌گیری

با توجه به اینکه توسعه فناوری‌ها منجر به توسعه تجارت الکترونیکی شده و توسعه تجارت الکترونیکی بدون توسعه بانکداری الکترونیکی و تغییر روش‌های پرداخت میسر نیست و نظر به اینکه اجرای بانکداری الکترونیکی با مخاطرات و چالش‌های زیادی در زمینه احراز هویت مواجه است، ازاین‌رو دراین مقاله چالش‌های بانکداری الکترونیکی با محوریت احراز هویت مشتری مورد بررسی قرار گرفته و پیشنهاداتی ارائه می‌شود.

اولین چالش، موضوع احراز تحقق قرارداد الکترونیکی است. با توجه به اینکه ارائه هر خدمتی در بانک نیازمند تحقق قراردادی بین بانک و مشتری است، لذا می‌توان گفت به استناد اصل رضایی بودن قرارداد و اصل صحت، مانعی برای تنظیم قرارداد به‌صورت الکترونیکی وجود ندارد. ضمن اینکه قانون تجارت الکترونیکی ایران و قانون نمونه آنسیترال نیز چنین قراردادی را معتبر دانسته است با این توضیح که زمان ارسال قبول الکترونیکی به‌عنوان زمان انعقاد قرارداد محسوب شده و مکان تنظیم قرارداد نیز تابع محل توافق طرفین است که می‌تواند محل ارسال داده پیام، محل تجاری یا کاری اصل‌ساز یا مخاطب باشد. درصورت عدم حصول توافق یا فقدان موارد فوق، اقامتگاه طرفین ملاک قرار گیرد. بنابراین بانک می‌تواند در قرارداد الکترونیکی شرطی مبنی‌بر تعیین محل سیستم بانک به‌عنوان محل تنظیم قرارداد درج نماید و زمان ارسال داده پیام به سیستم مشتری را زمان تنظیم قرارداد تعیین نماید.

چالش دوم انتخاب بهترین روش احراز هویت و امضا برای حفظ امنیت اطلاعات و جلوگیری از سرقت شخصیت، سرقت اینترنتی، جعل هویت و کلاهبرداری است که مقایسه بین روش‌های مختلف احراز هویت و معایب و محاسن روش‌ها نشان داد که احراز هویت بیومتریک مطمئن‌تر، کم هزینه‌تر و مناسب‌تر است؛ ضمن اینکه استفاده از امضای دیجیتالی، بکاربردن کلید عمومی و خصوصی و رمزنگاری و همین طور شیوه هاش نیز می‌تواند اطمینان بخش باشد و چه بسا مخاطرات جعل هویت و کلاهبرداری را کاهش دهد.

چالش سوم تأثیر بانکداری الکترونیکی روی تسهیل وقوع پدیده پول‌شویی است که بررسی نشان داد احراز هویت الکترونیکی قوی نه تنها موجب تسهیل پول‌شویی نمی‌شود بلکه با شبکه متمرکز و تلفیق هوش مصنوعی می‌تواند با شناسایی الگوهای رفتاری مشتری و تطبیق آن با الگوهای تمیز نسبت به شناسایی رفتارهای متقلبانه مشتری و کشف موارد پول‌شویی اقدام نماید، همین‌طور روش احراز هویت الکترونیکی ازطریق شناسایی بیومتریک می‌تواند مانع جبران‌کننده محرومیت اقشار

محروم جامعه از خدمات بانکی باشد، اشخاصی که قادر به ارائه مستندات احراز هویت، اقامتگاه و شغل نیستند اما نیازمند خدمات بانکی هستند می‌توانند با احراز هویت بیومتریک خدمات بانکی محدودی را دریافت نمایند. این موضوع در نسخه ۲۰۱۷ مکمل **FATF** آمده و در راهنمای شناسه دیجیتال ۲۰۲۰ نیز مورد تاکید قرار گرفته است. در مقررات ایران به‌دلیل دغدغه مخاطرات پول‌شویی و عدم امکان شناسایی مشتری در خدمات بانکی غیرحضوری ابتدا ارائه خدمات پایه به ارباب‌رجوع به‌صورت غیرحضوری ممنوع شد، اما ضرورت این امر موجب شد تا هیات وزیران در سال ۱۳۹۹ اجازه ارائه خدمات پایه غیرحضوری با رعایت دستورالعمل مصوب شورای عالی مقابله و پیشگیری از جرائم پول‌شویی و تامین مالی تروریسم را مصوب نماید و این شورا نیز متعاقباً طی دستورالعمل سال۱۴۰۰ ارائه خدمات بانکی الکترونیکی را در صورت احراز هویت الکترونیکی با استفاده از ابزارهای زیست‌سنجی (بیومتریک)، عامل مالکیت (مانند کارت بانکی یا برنامه موبایل) و عامل دانستنی (مانند رمز کارت بانکی یا رمز پویا) به‌عنوان عوامل ثبت هویت مجاز اعلام نمود. لکن خدمات دارای حساسیت بالا مانند افتتاح حساب جاری، اعطای تسهیلات تجاری، صدورضمانت‌نامه تجاری کماکان نیازمند مراجعه حضوری اعلام شد؛ چراکه مخاطرات پولشویی و جعل‌اسناد الکترونیکی همچنان وجود دارد و لازم است اقدامات مؤثری از حیث تدارک سخت‌افزار، نرم‌افزار، سیستم اطلاعاتی یکپارچه بین نهادهای متولی شناسایی از قبیل ثبت احوال، ثبت اسناد و املاک و ثبت شرکت‌ها ایجاد گردد و احکام صادره از سوی محاکم دادگستری درخصوص محجوریت اشخاص حقیقی و ورشکستگی و انحلال شرکت‌ها در اختیار سازمان‌های متولی ثبت اطلاعات هویتی اشخاص حقیقی و حقوقی قرارگیرد تا امکان احراز هویت دقیق الکترونیکی فراهم شود تا بانک‌ها بتوانند با دسترسی به سامانه‌های مربوط، از صحت و سقم دیتاهای هویتی مطمئن شده و سیستم به‌صورت خودکار با استعلام و تایید هویت مشتری بدون نیاز به حضور وی، خدمات پایه الکترونیکی ارائه نمایند.

در چالش چهارم ارزش اثباتی مستندات الکترونیکی بررسی و مشخص می‌شود که در امریکا امضای دیجیتالی به‌دلیل برخورداری از فناوری رمزنگاری داده‌ها و کلید عمومی و خصوصی، مطمئن‌ترین امضا تلقی می‌شود. در اروپا و ایران نیز مقرراتی مبنی‌بر اعتبار بخشی به امضای الکترونیکی و امکان انعقاد قرارداد از طریق داده پیام وجود دارد و امضای دیجیتالی تضمین‌کننده اصالت امضا است، ضمن اینکه داده پیام مطمئن در حکم سندرسمی بوده و قابل انکار و تردید نمی‌باشد و تنها ادعای جعل قابلیت طرح دارد. بدیهی است احراز هویت الکترونیکی مستلزم توسعه

فناوری‌ها و ایجاد شبکه یکپارچه بانکی قابل اتصال به سایر دستگاه‌های متولی ثبت اطلاعات هویتی اشخاص اعم از حقیقی و حقوقی است که اصالت هویت امضاکننده سند، اصالت اسناد الکترونیکی و اعتبار آن‌ها قابل احراز باشد، کمااینکه برای راه‌اندازی چک الکترونیکی نیز باید بستر لازم برای امضای الکترونیکی و احراز هویت فراهم باشد. همین‌طور دستگاه‌های خارج از بانک از قبیل محاکم قضایی و ثبتی امکان مشاهده، کنترل و رسیدگی به سند الکترونیکی را داشته باشند. بنابراین پیش‌بینی سیستم یکپارچه در کلیه دستگاه‌ها و نهادها ازجمله دادگستری برای قبول داده پیام به‌عنوان سند مورد نیاز است.

درپایان، بررسی مقررات بانکداری الکترونیکی نشان می‌دهد قانون تجارت الکترونیکی و قانون جرایم رایانه‌ای مصوب ۱۳۸۸/۳/۵ همه موارد از جمله رمزگیری و جعل هویت را پوشش نمی‌دهد. اگرچه برخی از مواد قانون جرایم رایانه‌ای با تفسیر قابل انطباق است اما پیشنهاد می‌شود برای حمایت ازگسترش بانکداری الکترونیکی صراحتا جرم‌انگاری شود و مقررات با استانداردهای جهانی همگام‌سازی شود.

منابع و مآخذ

الف. فارسی

ابراهیمی‌سروعلیا، فاطمه (۱۳۹۵). تجارت الکترونیک درایران، مزایا، معایب و موانع. ***سومین‌کنفرانس ملی علوم مدیریت نوین و برنامه‌ریزی پایدار ایران.***

اسدی،بهنام (۱۳۹۷). جایگاه امضای‌دیجیتالی در ثبت اسناد به شیوه الکترونیکی، ***مجله پژوهش‌های حقوقی قانون‌یار***، ۱(۳).

اسکینی، ربیعا (۱۳۹۰). ***حقوق تجارت***. تهران: نشر سمت.

اصغری، خدیجه؛ قلی‌زاده، بهروز و مدیری، ناصر (۱۳۹۲). ارائه‌روشی برای بهبود احراز هویت در تجارت الکترونیک. ***اولین کنفرانس ملی‌نوآوری در مهندسی‌کامپیوتر و فنآوری اطلاعات***، تنکابن. https://civlica.com/doc/26306

اصغری‌آقمشهدی، فخرالدین و اسکندری فرشته (۱۳۹۸). ***مطابقت حقوقی کالا با قرارداد در کنوانسیون بیع بین‌المللی کالا (وین ۱۹۸۰) و حقوق‌ایران***. چاپ ۸، منتشره در کتاب حقوق‌مدنی تطبیقی، تهران: نشردانشگاه تهران.

السان، مصطفی و علی‌دادی، محسن (۱۳۸۸). ***جنبه‌های حقوقی بانکداری اینترنتی***. تهران: نشر پژوهشکده پولی و بانکی، بانک مرکزی.

الماسی، نجادعلی (۱۴۰۰). ***حقوق بین‌الملل خصوصی***. تهران: نشر میزان.

امیرحسنی، کامران (۱۴۰۰). واکاوی تجارت الکترونیک بر رفتار بانکداری و حسابداری در صنعت تجارت الکترونیک. ***مجله رهیافتی در مدیریت بازرگانی***، ۵(۱).

پیروی، نرگس و جعفری، شهرام (۱۳۸۸). طرح مدل یکپارچه‌سازی تأیید هویت به کمک شاخص بیومتریک و RFID جهت شرکت در تعاملات الکترونیکی. ***همایش کنفرانس شهر الکترونیک جهاد دانشگاهی***، دوره۲.

تقی‌نتاج، غلامحسن و داوردیر، مینا (۱۳۹۰). چرخه عمر بانکداری نوین و مولفه‌های فناوری در ایران. ***بیست‌ودومین همایش بانکداری اسلامی مؤسسه عالی آموزش بانکداری ایران***.

خوش‌هیکل، مسعود و غریب، ایمان (۱۳۹۵). شناسایی موانع توسعه بانکداری الکترونیک. ***مطالعات مدیریت کسب و کار هوشمند***، ۴(۱۶)، ۱۴۵-۱۲۳.

داراب پور، مهراب؛ السان، مصطفی و خشنودی، رضا (۱۳۹۸). ***حقوق تجارت بین‌الملل***. کتاب پنجم، تهران: نشر گنج‌دانش.

زرکلام، ستار (۱۳۸۲) **امضای‌الکترونیکی و جایگاه آن درنظام ادله اثبات دعوا**، تهران: نشر مدرس‌علوم انسانی، ۷(۱).

زنگباری، ناصر (۱۳۹۱). ***حقوق بانکی***. جلد۱، تهران: نشر روزبهان.

ستوده تهرانی، حسن (۱۳۷۵). ***حقوق تجارت***. جلد۳، تهران: نشر دادگستر.

سجادی، مونا و جعفری، جمیله (۱۳۹۸). امضای‌الکترونیکی‌درحقوق‌ایران‌ومسئولیت مدنی‌ناشی‌از آن. ***پنجمین همایش ملی حقوق تحولات مسئولیت مدنی در نظام حقوقی ایران***. https://civilica.com/doc/94079

سلجوقی، محمود (۱۳۹۸). ***بایسته‌های حقوق بین الملل خصوصی***. تهران: نشر میزان.

شهیدی، مهدی (۱۳۷۷). ***تشکیل قراردادها و تعهدات***. تهران: نشر حقوقدان.

شیروی، عبدالحسین (۱۴۰۰). ***حقوق تجارت بین‌الملل***. ویراست ۴، تهران: نشر سمت.

صادقی، محسن و ناصر، مهدی (۱۳۹). خطرات حقوقی امضای الکترونیکی و الزامات قانونی پیشگیری از آن‌ها: مطالعه تطبیقی در حقوق ایران و امریکا. ***فصلنامه پژوهشنامه بازرگانی***، (۹۶).

صفایی، حسین (۱۳۹۹). ***حقوق بیع بین‌المللی***. چاپ۹، تهران: نشر دانشگاه تهران.

صفایی، سید حسین (۱۳۸۶). ***دوره مقدماتی حقوق مدنی***. جلد۲، چاپ ۵، تهران: میزان.

فیضی چکاب، غلام نبی (۱۳۸۳). لحظه انعقاد قرارداد از رهگذر واسطه های الکترونیکی، ***مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات***.

قاسم زاده، سید مرتضی (۱۳۸۵). ***حقوق مدنی، اصول قراردادها و تعهدات***. چاپ۲، تهران: نشر دادگستر.

کاتوزیان، ناصر (۱۳۶۴). ***حقوق مدنی،قواعد عمومی قراردادها***. جلد۱، چاپ۱، تهران: نشرمیزان.

کاویانی، کورش (۱۳۹۳). ***حقوق اسنادتجاری***. چاپ۶، تهران: نشر میزان.

گوگردچیان، احمد؛ صادقی‌عمروآبادی، بهروز و شهبازی، نجفعلی (۱۳۹۰). بانکداری الکترونیک و تأثیر آن بر پدیده پول‌شویی. ***مجموعه مقالات ۲۲ همایش بانکداری اسلامی مؤسسه الی آموزش بانکداری ایران***.

مافی، همایون و ناصر، مهدی (۱۴۰۰) واکاوی مکانیسم احراز اهلیت تعاملین در پیاده‌سازی قراردادهای هوشمند در حقوق ایران. ***مجله پژوهشنامه بازرگانی***، ۲۵(۹۸).

مهجوریان، فاطمه (۱۴۰۱). شمول مالی و مبارزه با پول‌شویی، ***روزنامه دنیای اقتصاد***، شماره ۵۶۶۸، شماره خبر ۳۹۴۲۸۱۱،

مهجوریان قمی، فاطمه (۱۳۹۵). ***متدولوژی ارزیابی تطبیق فنی با توصیه‌های گروه ویژه اقدام مالی و کارآمدی نظام مبارزه با پولشویی و تامین‌مالی‌تروریسم***. چاپ اول، تهران: نشر بانک مرکزی.

میرشکاری، عباس و علایی، صابر (۱۴۰۰). ماهیت‌داده پیام‌الکترونیکی‌به‌عنوان‌ادله اثبات دعوا. ***فصلنامه تحقیقات حقوقی دانشگاه شهید بهشتی***، ۲۴(۹۶).

هادوی‌تهرانی، مهدی (۱۳۸۸). ***شرایط عقود و قراردادهای جدیددر فقه‌اسلامی***. چاپ اول، تهران: نشر پژوهشکده پولی‌وبانکی بانک مرکزی.

ب. عربی

الدسوقی، ابواللیل (۲۰۰۳). ***الجوانب القانونیه للتعاملات الاکترونیه***. الکویت: طبع مجلس النشر العلمی بجامعه الکویت.

ج. انگلیسی

Alinezhad Sarokolaei, M., Rahimipoor, A., Nadimi, S., & Taheri, M. (2012)..***Procedia-Social and Behavioral Sciences***, 62(2012), 1100–1106.

Bani-Hania, A., Majdalweieha, M., & AlShamsia, A. (2019). Online Authentication Methods Used in Banks and Attacks Against These methods. ***Procedia Computer Science***, (151), 1052-1059.

Hiltgen, A., Kramp, T,. & Weigold, T. (2006). Secure Internet banking authentication. ***IEEE Security & Privacy***, 4(2), 21-29.

Jawahitha S. Ab., Hamid, N.R., & Ishak M.M., M. (2003). Internet banking: A comparative analysis of legal and regulatory framework in Malaysia. ***Arab Law Quarterly***, 18(3/4), 291-308.

Nsouli, S.M., & Schaechter, A. (2002). Challenges of the"E-Banking Revolution. ***INTERNATIONAL MONETARY FUND Magazin***, 39(3), 48-51.

Stephanie, C. (2013). Washington`s Electronic Signature Act: An Anachronism In The New Millennium, ***Washington Law Review***, 88(2), 559-589