مجله مطالعات توسعه اجتماعی ایران، سال پانزدهم/ شماره اول/زمستان ۱۴۰۱
Journal of Iranian Social Development Studies 2023 (Winter), Vol. 15, No. 1

آثار ناشی از شناخت امضای الکترونیک در دفاتر گواهی امضا و مسئولیت اجتماعی آن

رحیم عبدلی[۱]، طیب افشارنیا[۲]، علیرضا رجب زاده اصطهباناتی[۳]

تاریخ دریافت مقاله: ۱۴۰۰/۰۸/۱۸ تاریخ پذیرش مقاله: ۱۴۰۰/۱۱/۰۹

DOI: 10.30495/JISDS.2022.64200.11640

چکیده

دفاتر گواهی امضای الکترونیک به عنوان یک نهاد حقوقی در جهت تامین حقوق برخی از اشخاص اقدام به ثبت و گواهی امضای الکترونیک می‌کنند. دفاتر گواهی امضای الکترونیک در جهت صدور تصادیق امضا و مطابقت آن با اصل، برخی شرایط و ضوابط را رعایت می‌کنند. یکی از مهمترین تعهداتی که دفاتر گواهی امضای الکترونیک به صاحبان امضا می‌دهند. حفظ اسرار و محرمانگی اطلاعات مربوط به شهروندان می‌باشد. یکی از مهمترین مبانی به کار رفته در این تحقیق بررسی مسئولیت صاحبان دفاتر گواهی امضای الکترونیک می‌باشد که جزئیات آن مورد ارزیابی قرار گرفته است.

واژگان کلیدی: دفتر، امضا، الکترونیکی، گواهی، دیجیتال

[۱] دانشجوی مقطع دکتری رشته حقوق خصوصی واحد امارات، دانشگاه آزاد اسلامی، امارات متحده عربی
(Email: abdoli_rahim@yahoo.com)

[۲] استادیار گروه حقوق دانشکده علوم انسانی، واحد تهران غرب، دانشگاه آزاد اسلامی، تهران، ایران. (نویسنده مسئول)
(Email: afsharnia59@gmail.com)

[۳] استادیار دانشگاه غیرانتفاعی رجاء، قزوین، ایران.

مقدمه

گواهی الکترونیکی در مفهوم عام آن عبارت از تصدیق رسمی یک متن، امضا با هر مدرک الکترونیکی دیگر از سوی نهادی است که به موجب" قانون" و با داشتن "تخصص" و" تسلط بر موازین حقوقی" بدین منظور تعیین می‌گردد. در سال‌های اخیر، تصویب پاره ای از مقررات منجر به شکل گیری تصور متفاوتی از گواهی الکترونیکی در کشورمان شده است.

بررسی ضوابط و شرایط ایجاد دفاتر گواهی امضای الکترونیک در حقوق ایران وابسته به نظام‌های حقوقی کشورهای پیشرفته در این رابطه می‌باشد به طوری که در این رابطه می‌توان گفت نظام حقوقی ایران همانند ضوابط جهانی عمل می‌کند. با این حال برخی نواقص و برخی ضعف‌ها در این اقتباس مشاهده می‌گردد.

دفاتر گواهی امضای الکترونیک جهت ارائه تصدیق نامه گواهی امضا باید برخی شرایط و اصول حاکم را رعایت کنند که این اصول حاکم نشان دهنده شناسایی امضا و اعطای اعتبار به آن می‌باشد. در این رابطه کشورهای مختلف طرح‌های متفاوتی دارند که کشور ایران سعی نموده است از تمامی این طرح‌ها به نسبت نیاز خود برخی برداشت‌ها را انجام دهد. در هر حال باید گفت دفاتر گواهی امضای الکترونیک دارای ضوابط و سخت گیری‌های شدیدی می‌باشند به طوری که بعضا در اثر برخی اشتباهات کارکنان این دفاتر مسئولیت حقوقی شامل آنها می‌شود (فدوی لنجوانی، ۱۳۸۵).

شرح وظایف و مسئولیت‌های مراجع گواهی به تفصیل در قوانین و مقررات بیان شده است. قوانین بین‌المللی موجود در خصوص امضای الکترونیک در مورد مقررات مراجع گواهی ساکت هستند و آن را به قوانین ملی واگذار کرده اند. قانون تجارت الکترونیک ایران نیز از مراجع گواهی تحت عنوان «دفاتر خدمات صدور گواهی الکترونیکی» نام برده و باب دوم خود را به آن اختصاص داده است. ماده ۱۳ این قانون مقرر می‌دارد: «دفاتر خدمات صدور گواهی الکترونیکی واحدهایی هستند که برای ارائه خدمات صدور امضای الکترونیکی در کشور تأسیس می‌شوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تایید، ابطال و به روز نگهداری گواهی‌های اصالت (امضای) الکترونیک می‌باشد، ماده ۲۳ نیز بیان می‌کند: «آیین نامه‌ها و ضوابط تأسیس و شرح وظایف این دفاتر توسط سازمان مدیریت و برنامه ریزی کشور و وزارتخانه‌های بازرگانی، ارتباطات و فن آوری اطلاعات، امور اقتصادی و دارایی و دادگستری تهیه و به تصویب هیأت وزیران خواهد رسید که این بخشنامه در سال ۸۶ جهت اجرا ابلاغ شده است. مراجع گواهی امضاء به دلیل نیاز به زیر ساخت‌های فنی، تجهیزات و تأسیسات شبکه ای پیشرفته و استانداردهای ایمنی بالا، هنوز در ایران راه اندازی نشده اند.

بسیاری از کشورها، بین‌سال‌های ۱۹۹۶ تا ۲۰۰۱ میلادی، با استفاده از مقررات بین‌المللی موجود و رهنمون‌های ارائه شده در خصوص امضای الکترونیک مبادرت به قانونگذاری در این زمینه کرده اند. و در حال حاضر می‌توان گفت امضای الکترونیک در اکثر نظام‌های حقوقی مورد پذیرش قرار گرفته است (ملکی، ۱۳۵). در قانون تجارت الکترونیک ایران (مصوب سال ۱۳۸۲)، بحث امضای الکترونیک و شرایط آن مورد توجه قرار گرفته است. کشور ایران نیز در عرصه حاضر، با تصویب قانون تجارت الکترونیکی و تهیه پیش نویس قانون تجارت جدید و پیش بینی اسناد تجاری الکترونیکی در این قانون باید در عرصه جهانی با تقویت قابلیت اتصال به شبکه‌های جهانی و ارائه خدمات حمایتی از تجارت الکترونیکی بیش از پیش عمل نماید.

۱- اثر شناسایی گواهی‌ها و امضاهای الکترونیکی خارجی

یکی از ویژگی‌های مهم تجارت الکترونیکی این است که امکان برقراری ارتباط بین‌تجار کشورهای مختلف از طریق واسطه‌های الکترونیکی وجود دارد. این خصوصیت بین‌المللی قانون تجارت الکترونیکی و لزوم توسعه هماهنگی بین‌کشورها در به کار گیری آن، فرضیه لزوم اعتبار بخشیدن به گواهی و امضای الکترونیکی صادره در کشورهای دیگر را در ذهن مطرح می‌کند.

این موضوع در ماده ۳ قانون تجارت الکترونیکی ایران[۱] و ماده ۴ قانون نمونه امضای الکترونیکی آنسیترال ۲۰۰۱ [۲]مورد اشاره قرار گرفته است. سوالی که در این رابطه به ذهن خطور می‌کند این است که تجار کشورهای مختلف چگونه می‌توانند به گواهی الکترونیکی طرف دیگر که در کشور خودش صادر شده اعتماد کنند. به عنوان مثال وقتی یک تاجر مالزیایی قصد خرید کالا از یک ایرانی را دارد و از او تقاضای گواهی امضای الکترونیکی می‌کند، آیا این گواهی صادره در یک مرکز مبانی ایرانی در کشور مالزی معتبر است. همین مسئله در مورد گواهی‌های صادره توسط کشورهای دیگر نیز که تابعان آنها طرف قرارداد با یک ایرانی هستند، مطرح است.

قاعده کلی در خصوص اعتبار اسناد تنظیمی در کشورهای خارجی در ایران، رعایت اصل رفتار متقابل است. اگر چه شرایطی دیگری نیز لازم است که ماده ۱۲۹۵ قانون مدنی به آن اشاره می‌کند. مطابق این ماده محاکم ایران به اسناد تنظیم شده در کشورهای خارجی همان اعتباری را خواهند داد که آن استاد مطابق قوانین کشوری که در آنجا تنظیم شده دارا می‌باشد مشروط بر اینکه:

اولا- اسناد مزبور به علتی از علل قانونی از اعتبار نیفتاده باشد.

ثانیا- مفاد آن مخالف با قوانین مربوط به نظم عمومی با اخلاق حسنه نباشد.

ثالثا- کشوری که اسناد در آنجا تنظیم شده به موجب قوانین خود با عهود، اسناد تنظیم شده در ایران را نیز معتبر بشناسد.

رابعا- نماینده سیاسی یا کنسولی ایران در کشوری که سند در آنجا تنظیم شده یا نماینده سیاسی با کنسولی کشور مزبور در ایران تصدیق کرده باشد که سند موافق قوانین محلی، تنظیم یافته است.

این ماده حکم کلی در مورد کلیه اسناد تنظیم شده در کشورهای خارجی را بیان می‌کند. اما در مورد گواهی الکترونیکی صادر شده در مراجع صدور گواهی کشورهای دیگر، ماده ۱۸ آیین نامه می‌گوید: «اعتبار و پذیرش گواهی الکترونیکی صادره از مراجع صدور گواهی خارجی، مشروط به توافق دو جانبه بین‌مرکز ریشه کشور و مرجع صدور گواهی کشور خارجی با رعایت اصل شرط عمل متقابل و تصویب شورا خواهد بود."

مطابق این ماده در صورتی گواهی کشورهای دیگر در ایران واجد اعتبار است که سه شرط رعایت گردد: ۱- توافق دو جانبه بین‌مرکز ریشه ایران و مرجع صدور گواهی کشور مورد نظر؛ ۲- رعایت اصل شرط عمل متقابل، ۳- تصویب شورا (مظاهری، ۱۳۸۷).

۲- اثر شناسایی حقوقی و قانونی گواهی امضای الکترونیکی

ناهماهنگی حقوقی و فنی، ریشه اصلی مشکلات در استفاده بین‌المللی از شیوه‌های گواهی و امضای الکترونیکی به شمار می‌آیند. به ویژه زمانی که این شیوه‌ها در صدد جانشینی امضایی هستند که به لحاظ حقوقی معتبر است. ناهماهنگی فنی، همکنشی بین‌سامانه‌های گواهی را مخدوش می‌سازد، ناهماهنگی حقوقی می‌تواند از این امر ناشی شود که قوانین مخلف الزامات متفاوتی را در زمینه استفاده از شیوه‌های گواهی و امضای الکترونیکی تحمیل می‌کنند(همان).

۲-۱- تاثیرات بین‌المللی قوانین داخلی

زمانی که قانون داخلی، معادل‌های الکترونیکی شیوه‌های گواهی بر روی کاغذ را مجاز اعلام می‌کند، معیارهای اعتبار این معادل‌ها ممکن است با یکدیگر هماهنگ نباشند. برای مثال اگر قانون، فقط امضاهای دیجیتالی را به رسمیت بشناسد، سایر ناهماهنگی‌ها در

---

[۱] ماده ۳ :در تفسیر این قانون همیشه باید به خصوصیت بین المللی، ضرورت توسعه هماهنگی بین کشورها در کابرد آن و رعایت لزوم حسن نیت توجه کرد.

[۲] ماده ۴: تفسیر: ۱- در تفسیر این قانن باید منشا بین‌المللی و ضرورت توسعه اعمال یکسان آن و رعایت حسن نیت را مدنظر قرار داد. ۲- مسائل مربوط به موضوعات مشمول این قانون که صریحا در آن حل و فصل نشده اند، باید بر طبق اصول کلی که این قانون بر آن مبتنی است، حل و فصل شوند.

گونه‌های امضای الکترونیکی مورد پذیرش قرار نخواهند گرفت. ناهماهنگی‌ها در معیارهای شناسایی شیوه‌های گواهی شاید مانع استفاده بین‌المللی از آنها نشود ولی هزینه‌ها و دشواری‌های ناشی ضرورت رعایت الزامات تحمیل شده توسط دیگر کشورها خطر کاهش سرعت و کارآمدی (که از امتیازات مبادلات الکترونیکی است) را به دنبال خواهد داشت (مظاهری کوهانستانی، ۱۳۹۳)

۲-۲- موانع بین‌المللی ناشی از دیدگاه‌های داخلی متناقض

دیدگاه‌های فنی خنثی (بی طرف)، به ویژه دیدگاه‌هایی که "معیار قابلیت اعتماد" را مطرح می‌سازند، به طور کلی می‌تواند به حل ناهماهنگی‌های حقوئی یاری رساند. قانون نمونه آنسیترال راجع به تجارت الکترونیکی (قسمت ب بند ۱ ماده ۷) و کنوانسیون سازمان ملل راجع به استفاده از ارتباطات الکترونیکی در قراردادهای بین‌المللی (بند ۳ ماده ۹) از جمله ابزارهای حقوقی بین‌المللی هستند که چنین دیدگاهی را پذیرفته اند. به موجب مقررات اخیر، شیوه گواهی و با امضای الکترونیکی که به طور همزمان شناسایی امضا کننده را ممکن سازد و اراده وی را نسبت به اطلاعات درج شده در ارتباطات الکترونیکی بیان می‌کناد الزامات امضا را در صورتی که معیارهای مختلفی داشته باشد برآورده می‌سازند. شیوه گواهی با امضاء باید اثبات کند که با توجه به تمامی اوضاع و احوال، از جمله هر گونه توافق بین‌فرستنده و گیرنده داده پیام، همچنین موضوعی که داده پیام برای آن تولید با ارسال شده، قابل اعتماد است. در غیر این صورت، این شیوه با امضاء به علاوه باید اثبات کند که به تنهایی یا در پیوند با دیگر عناصر، به اهدافش دست یافته است.

بدون تردید، دیدگاه حداقلی، استفاده بین‌المللی از امضا و شیوه‌های گواهی الکترونیکی را آسان می‌سازد، زیرا هر گونه شیوه یا امضای الکترونیکی در صورتی که به الزامات پیش گفته پاسخ دهد می‌تواند به صورت معتبر برای امضا کردن با گواهی کردن یک قرارداد با یک ارتباط به کار رود. با این همه، دیدگاه حداقلی این نتیجه را در بر دارد که الزامات مورد نظر، باید در آینده مورد تایید قرار گیرد و تضمینی وجود ندارد که دادگاه استفاده از یک شیوه خاص را بپذیرد استفاده بین‌المللی از امضا یا گواهی الکترونیکی، در سیستم هایی که فناوری ویژه‌ای را به رسمیت می‌شناسد یا مورد حمایت قرار می‌دهند، ایجاد مشکل می‌کند. هنگامی که سطح مقررات اداری امضا و گواهی الکترونیکی و یا درجه امنیت حقوقی که قانون به این یا آن شیوه یا قن اعطا می‌کند مطرح است، پیچیدگی موضوع حسب مورد افزایش می‌یابد. دلیل چنین امری بسیار ساده است: زمانی که قانون هیچ گونه ارزش یا اماره حقوقی خاصی برای برخی نمونه‌های امضا با گواهی الکترونیکی نمی شناسد و به پیش بینی معادل‌های کلی با امضای دستی با گواهی‌های کاغذی بسنده می‌کند، خطرات مرتبط با استفاده از امضای الکترونیکی همان هایی خواهد بود که به موجب قوانین جاری در مورد امضای دستی وجود دارد. در مقابل، زمانی که قانون اماره‌های حقوقی قوی تری به امضای الکترونیکی خاص اعطا می‌کند، بار اثبات دلیل از یک طرف معامله به طرف دیگر منتقل می‌شود (محمدزاده، ۱۳۸۵).

ناهماهنگی بین‌قوانین ملی پیرو فناوری خاص، با این خطر همراه است که استفاده از امضای الکترونیکی در تجارت بین‌المللی را مختل سازد به جای آنکه مشوق آن باشد. این امر ممکن است به دو طریق مختلف که به طور تنگاتنگ، به هم پیوسته‌اند رخ دهد.

در وهله اول، در صورتی که امضای الکترونیکی و مراجع خدمات گواهی که آن را گواهی می‌کنند پیرو الزامات فنی و حقوقی متناقض در کشورهای مختلف باشند. اگر امضای الکترونیکی نتواند به طور همزمان الزامات مقرر توسط این کشورها را برآورده سازد، استفاده از آن ممکن است بسیاری از عملیات تجاری بین‌المللی را مختل کند یا مانع آنها شود.

در مرتبه دوم، قانون پیرو فناوری خاص، به ویژه اگر امضای دیجیتالی را برتر بداند خطر مواجهه با مجموعه ای ناهماهنگ از قواعد فنی و الزامات پذیرش متناقض را به دنبال خواهد داشت که استفاده بین‌المللی از امضاهای الکترونیکی را بسیار دشوار خواهد کرد. سیستمی که در آن هر کشور استانداردهای خاص خود را تدوین می‌کند، می‌تواند مانع طرفین برای انعقاد توافق‌های مبتنی بر شناسایی گواهی‌های ضربدری شود. در واقع مشکل مهم حل نشده به ویژه راجع به امضاهای دیجیتالی، شناسایی فرامرزی آنهاست.

گروه کاری امنیت اطلاعات و حریم خصوصی سازمان همکاری‌ها و توسعه اقتصادی یادآور شده است که حتی اگر دیدگاههای پذیرفته شده توسط اکثریت کشورها، تبعیض آمیز به نظر نرسد، تفاوت‌های بین‌الزامات ملی همچنان مشکلات مرتبط با همکنشی را به دنبال خواهد داشت (السان، دوان یامچی، ۱۳۸۳).

۳-۲- آثار شناسایی مراجع خدمات گواهی خارجی

به نظر گروه کاری امنیت تلاش‌ها به ایجاد مراجع خدمات گواهی در سطح ملی متمرکز، معطوف شده است. به همین دلیل ساز و کارهای ناظر بر شناسایی مراجع خدمات گواهی خارجی به طور کلی هنوز توسعه نیافته اند. بنابر این گروه کاری یاد شده این نکته را پذیرفته است که در مقطع کنونی ادامه فعالیت مفید خواهد بود. از آنجا که هر گونه تلاش در این زمینه به طور تنگاتنگی با موضوع کلی تر همکنشی در پیوند قرار دارد، با این مسائل به صورت یکجا برخورد خواهد شد (نوری، ۱۳۸۴).

در برخی موارد، موضوع پذیرش گواهی‌های صادر شده توسط سایر واحدها همانند مانعی بر سر راه همکنشی مطرح شده است. به همین دلیل گروه کاری سازمان همکاری‌ها و توسعه اقتصادی پیشنهاد می‌کند که امکان تدوین مجموعه ای از رویه‌های متناسب با خطوط هدایتگر، برای صدور گواهی هایی که به منظور تصدیق صادر می‌شوند، مورد مطالعه قرار گیرد. کارهایی در این زمینه در بسیاری از مراجع قضایی مختلف در دست انجام است که می‌تواند برای هر گونه ابتکاری از سوی گروه مفید واقع شود(همان).

گروه کاری امنیت اطلاعات و حریم خصوصی سازمان همکاری‌ها و توسعه اقتصادی دریافته است که تقریبا در همه کشورهای عضو این سازمان، مجموعه بزرگی از شیوه‌های گواهی قبلا مورد استفاده قرار گرفته اند. این شیوه‌ها گذر واژه‌ها را از یک طرف و رمزها امضاهای دیجیتالی و زیست سنجی (بیومتریک) را از طرف دیگر در بر می‌گیرد. حسب شیوه مورد استفاده و الزام ناشی از آن، این شیوه‌ها می‌تواند به تنهایی یا به صورت ترکیبی به کار گرفته شود. بسیاری ممکن است این تنوع را مثبت ارزیابی کنند ولی اگر به اطلاعات موجود در پاسخ هایی که به پرسش‌های گروه کاری داده شده مراجعه کنیم، متوجه می‌شویم که دامنه این شیوه‌ها به قدری زیاد است که تامین کننده و کاربر خدمات گواهی کاملا با این خطر مواجه هستند که در جریان انتخاب بین‌شیوه‌های مختلف، از شیوه ای که با نیازهای او همخوانی دارد رو گردان شود. بنابراین به اعتقاد گروه کاری، شاید بهتر باشد یک ابزار مرجع برای ارزیابی شیوه‌های مختلف گواهی در نظر گرفته شود و ویژگی‌های هر یک از این شیوه‌ها با توجه به نحوه پاسخگویی به انتظارات تامین کنندگان و یا کاربران سنجیده شود (مظاهری کوهانستانی، ۱۳۹۳).

تفاوت بین‌سیاست‌های موجود در عرصه بین‌المللی، احتمالا نتیجه ترکیبی از معیارها با درجات مختلف است. برخی کشورها به اعمال الزامات شکلی سختگیرانه و ویژه در زمینه امضا و اسناد گرایش دارند، در حالی که برخی دیگر، بر قصد امضاکننده متمرکز شده‌اند و سطح وسیعی از دلایل را برای اثبات اعتبار امضا مجاز می‌داد. این تفاوت‌های کلی به طور معمول در قوانینی که شیوه‌های گواهی و امضای الکترونیکی را مقرر می‌کنند ظاهر می‌شوند. یکی از سرچشمه‌های اختلاف از درجه متغیر دخالت قوای عمومی در جنبه‌های فنی این شیوه‌ها نشات می‌گیرد. برخی کشورها به ایفای نقش مستقیم در توصیف قواعد قابل اعمال به فناوری‌های جدید تمایل نشان داده اند شاید به این امید که چنین روشی به صنعت داخلی آنها امتیاز قابل رقابتی اعطا کند.

این امکان نیز وجود دارد که سیاست‌های مختلف، فرض‌های متفاوت از تحول فنون گواهی را منعکس کند. سناریوی موسوم به پارادایم گواهی جهانی ایجاب می‌کند که هدف اصلی فنون گواهی، کنترل هویت و ویژگی‌های اشخاصی باشد که هیچ گونه رابطه قبلی بین‌آنها وجود نداشته باشد و به طور مشترک و مستقل از هر گونه توافق قراردادی از یک فن استفاده می‌کنند. از این رو، فن گواهی با امضا، باید هویت با دیگر ویژگی‌های شخصی را در میان تعداد بالقوه نامحدودی از اشخاص و موضوعات تایید کند. این مدل، اهمیت استانداردهای فنی و الزامات عملیاتی مراجع خدمات گواهی را زمانی که ثالث مودر اعتماد دخالت می‌کنند

یادآور می‌شود. سناریوی دیگر که به پارادایم گواهی تایید شده مشهور است توصیه می‌کند که فنون گواهی و امضاء به طور عمده برای کنترل هویت و ویژگی‌های دارنده گواهی را فقط از حیث مجموعه ای تعریف شده از موضوعات و در میان جمعیتی معین از طرف هایی که ممکن است به گواهی اعتماد کنند، تایید کند و به الزامات مشترک استفاده از این فناوری‌ها تن در دهد. در این مدل، تاکید بر شناسایی حقوقی توافقات قراردادی است (احمدیان راد، ۱۳۸۸).

۳- مسئولیت مدنی دفاتر خدمات صدور گواهی الکترونیکی

لازمه توسعه تجارت الکترونیکی و تشویق اشخاص حقیقی و حقوقی به برقراری ارتباطات تجاری به شیوه الکترونیکی این است که افراد در خصوص امنیت این نوع رابطه و جبران خسارت احتمالی که در این زمینه ممکن است وارد شود اطمینان کافی داشته باشند.

به عبارت دیگر از آنجا که حفظ اسرار تجاری یکی از مسائل مهم در تجارت کنونی است و با توجه به اینکه دفاتر خدمات صدور گواهی الکترونیکی از اهمیت بسیار و وظایف پر مخاطره ای برخوردار هستند، و از طرف دیگر فاش شدن امضای الکترونیکی کاربران و با صدور یک گواهی الکترونیکی جعلی علاوه بر تحقق جرم جعل، می‌تواند خسارات بعضا غیر قابل جبرانی را به بار آورد، مسئولیت مدنی این دفاتر و ساز و کار جبران خسارت احتمالی از اهمیت بسیاری برخوردار است. پرسشی که در اینجا به ذهن می‌رسد این است که اگر در جریان صدور یا ایجاد امضا یا صدور گواهی الکترونیکی، خسارتی به یکی از طرفین قرارداد در اثر اهمال یا تقصیر دفاتر وارد شود، جبران خسارت بر عهده کیست؟ آیا مسئولیت به طور مطلق بر عهده دفاتر است با خود صاحبان امضا و طرف‌های اعتماد کننده نیز ممکن است مقصر شناخته شوند (مظاهری کوهانستانی، ۱۳۹۳).

قاعده کلی در باب مسئولیت مدنی این است که هر کس به دیگری زیانی وارد کند، مسئول جبران خسارت است. البته برای این منظور باید سه عنصر اثبات گردد: ۱- ورود ضرر؛ ۲- فعل زیانبار ۳- رابطه سببیت

در مسئولیت قراردادی هم علاوه بر اثبات وجود رابطه قراردادی، باید عدم انجام تعهدات در مهلت معین، توسط زیاندیده اثبات شود. در مورد مسئولیت مدنی در حوزه تجارت الکترونیکی، ماده ۷۸ قانون تجارت الکترونیکی می‌گوید: «هر گاه در بستر مبادلات الکترونیکی در اثر نقص یا ضعف سیستم موسسات خصوصی و دولتی، به جز در نتیجه قطع فیزیکی ارتباط الکترونیکی، خسارتی به اشخاص وارد شود، موسسات مزبور مسئول جبران خسارات وارده می‌باشند، مگر اینکه خسارات وارده ناشی از فعل شخصی افراد باشد، که در این صورت جبران خسارات بر عهده این اشخاص خواهد بود.

همچنین در تبصره ماده ۶ آیین نامه آمده است: «مسئولیت و نحوه پرداخت خسارت بابت ضرر و زیان ناشی از ابطال مرکز میانی به صاحبان امضای الکترونیکی صادر شده از این مرکز و یا به دفاتر ثبت نام باید در دستورالعمل گواهی الکترونیکی مرکز و یا در قرارداد منعقد شده بین‌طرفین قید شده باشد.»

حکم مقرر در ماده ۷۸ قانون تجارت الکترونیکی صرفا در موردی جاری است که به عنوان مثال در سامانه‌های رایانه ای یک مرکز صدور گواهی، ایراد فنی وجود داشته باشد و در اثر این ایراد، ضرری متوجه دیگری گردد، مرکز مربوطه موظف به پرداخت خسارت خواهد بود. این ماده در خصوص موردی که افشای امضای رقمی، تقض حریم خصوصی افراد، افشا اسرار و اطلاعات تجاری، فعالیت‌های متقلبانه حکمی مقرر نکرده است. ماده ۱۸ آیین نامه نیز در واقع حاوی مطلب جدیدی نیست بلکه صرفا الزام به تعیین شرایط مسئولیت و نحوه جبران خسارت در قرارداد پا دستورالعمل مرکز مبانی را ذکر کرده است. بنابر این ملاحظه که علی رغم وظایف گسترده و خطیر این مرکز، قانونگذار به مسئله مهمی چون مسئولتی مدنی توجه نکرده است. به نظر می‌رسد لازم است مقرراتی تصویب شود که به طور دقیق به تبیین مسئولیت مدنی آنها با عنایت به ابعاد فنی و حقوقی این مراجع بپردازد (مظاهری کوهانستانی، ۱۳۹۳).

مسئولیت غیر قراردادی با مدتی در حقوقی کشورهای مختلف ظاهر مختلفی دارد و نمی توان یک لفظ واحد از آن را به عنوان معیار اصلی تلقی مسئولیت غیر قراردادی در نظر گرفت به عنوان مثال، مسئولیت غیر قراردادی در حقوق فرانسه و آلمان با همین اسم وجود دارد در حالی که در حقوق انگلیس مسئولیت غیر قراردادی به عنوان حقوق شبه جرم نامیده می‌شود. هر چند مفهوم شبه جرم و مسئولیت غیر قراردادی پیشرفت‌های بسیاری کرده است و هم اکنون مفهومی که از این اصطلاح افاده می‌شود "مسئولیت بر مبنای تقصیر" را در بر می‌گیرد. به عبارت دیگر مسئولیت بر مبنای تقصیر در بسیاری از سیستم‌های حقوقی همان معنای مسئولیت غیر قراردادی یا شبه جرم را افاده می‌کند. در همین زمینه می‌توان به این نکته نیز اشاره کرد که مسئولیت بدون تقصیر نیز از جمله عناوینی است که این مفهوم شامل آن می‌شود.

در تمام سیستم‌های حقوقی اتحادیه اروپا که انگلستان نیز جزو آن می‌باشد مسئولیت غیر قراردادی با شبه جرم دارای تعریف واحدی می‌باشد. در این زمینه باید گفت که مسئولیت غیر قراردادی در نگاه حقوق کشورهای اروپایی تنها حول یک محور می‌چرخد که آن عبارت است از: یک محدوده حقوقی برای تصمیم گیری در این زمینه که یک شخص آیا می‌تواند بر علیه کسی که با او هیچ ارتباط حقوقی نداشته (اتفاق موجب خسارت باعث ارتباط حقوقی آن‌ها شده باشد) و از عمل او زیانی رسیده، ادعای خسارت کند؟

واژه مسئولیت مدنی که امروزه در حقوق ما تعبیری شایع و متداول است در اصل به خانواده حقوق رومی - ژرمنی تعلق دارد و پس از تصویب قانون مسئولیت مدنی کاربرد بیشتری پیدا کرده است (ره پیک، ۱۳۹۰) و در فقه اسلامی از عناوین ضمان قهری با ضمانات استفاده می‌شود. اما تعاریفی که حقوقدانان از این واژه ارائه داده اند کمابیش یکسان و با تاکید بر اصل «جبران خسارت» است که سابقه فقهی آنرا می‌توان قاعده لاضرر دانست. از جمله گفته شده است مسئولیت مدنی عبارت است از التزام و تعهد قانونی شخص به جبران ضرر و زیانی است که در نتیجه عمل مستند به او به دیگری وارد شده است (باریکلو، ۱۳۸۹). برخی مسئولیت ملتی را به معنای جبران خسارت ناشی از رفتارهای زیان بار دانسته اند و عده ای مسئولیت مدنی را وظیفه ای می‌دانند که بر عهده یک مسئول نهاده شده با زبان‌های وارد آمده به دیگری را جبران کند(ادیب، ۱۳۸۴). این تعاریف همانگونه که گفته شد تنها بر اصل جبران خسارت تکیه داشته و نکات مهم و ضروری دیگری را مدنظر قرار نداده و بدین ترتیب حوزه مسئولیت را پیش از اندازه گسترش می‌دهند. بدیهی است هر ضرری قابل جبران نیست و تحمل برخی زیان‌ها لازمه زندگی اجتماعی است. بنابر این ضرری قابل جبران و موجب مسئولیت است که من غیر حق وارد شده باشد و به همین منظور بایستی در تعریف مسئولیت مدنی فید ناروا بودن به ضرر افزوده شود (غمامی، ۱۳۸۵). از طرفی شخص تنها مسئول جبران خسارتی است که منتسب به وی باشد بنابراین قابلیت انتساب نیز باید به نوعی داخل در تعریف شود.

با توجه به نکات فوق شاید بتوان مسئولیت مدنی را اینگونه تعریف نمود که مسئولیت مدنی عبارت است از الزام و تعهد شخص به جبران ضرر ناروایی که به دیگری وارد نموده و این ضرر عرفا به او منتسب است

مسئولیت مدنی در معنای فوق را به دو شعبه مهم تقسیم کرده اند: ۱- قراردادی ۲- خارج از قرار داد (کاتوزیان، ۱۳۵).

از مسئولیت مدنی خارج از قرارداد به الزامات خارج از قرار داده، «ضمان قهری، و مسئولیت مدنی به معنای اخص» نیز تعبیر می‌شود (قاسم زاده، ۱۳۸۷). مسئولیت قراردادی در نتیجه عدم اجرای قرارداد با اجرای قرارداد به طور ناقص یا تاخیر در اجرای قرارداد و یا عدم رعایت شروط صریح و ضمن عقد به وجود می‌آید، اما مسئولیت خارج از قرار داد که از وقایع حقوقی است در نتیجه ورود ضرر با تسلط بر مال دیگران با استفاده مشروع از اموال یا امتیازات یا خدمات دیگران حاصل می‌گردد (داراب پور، ۱۳۸۷).

۱-۳- فرض مسئولیت مدنی در نقض حقوق اسرار حرفه‌ای

این فرض در جایی پیاده می‌شود که با قراردادی میان صاحب سر تجاری و نقض کننده حق وجود ندارد با قراداد منعقد شده بی‌اعتبار بوده یا اعتبار آن، منقضی شده است. معیار تعیین دادگاه صالح در این فرض را پند سوم ماده ۵ کنوانسیون بروکسل بیان نموده است. مطابق این بند، دادگاه کشور محل وقوع حادثه زیانبار صالح به رسیدگی است. با این حال این معیار از ابهامی مفهومی برخوردار است چرا که مشخص نکرده منظور از محل وقوع حادثه زیانبار، محلی است که خسارت ناشی از نقض حقی بروز پیدا می‌کند یا محلی است که حادثه منشا ورود خسارت، در آنجا اتفاق افتاده است.

نکته مهم در خصوص معیار ارائه شده در کنوانسیون بروکسل یک آن است که اگر خسارات وارد شده به صاحب اسرار تجاری در کشورهای مختلف به وقوع پیوسته باشد، خواهان باید در دادگاه هر کشور بابت همان میزان خسارات وارده طرح دعوی کند و دادگاه آن کشور تنها تا میزان خسارات وارد در آن کشور صالح به رسیدگی است نه همه خسارات. با این حال این معیار در محیط دیجیتالی بسیار مشکل آفرین بوده و می‌تواند بر خلاف حمایت از صاحب حق تلفی شود چرا که با افشای سر تجاری در اینترنت، امکان دسترسی میلیون‌ها کاربر در سراسر جهان فراهم شده و به طور بالقوه ممکن است بخشی از خسارات در هر یک از کشورهای دنیا به وقوع بپیوندد. به دلیل انتقادات وارد بر این معیار، اعضای کنوانسیون بروکسل یک در اصلاحی که به موجب دستورالعمل سال ۲۰۰۱ در این کنوانسیون اعمال کردستان، از رویه کنوانسیون پیشنهادی لاهه تبعیت کرده و مقرر داشتند که دادگاه محل بخشی از خسارات می‌تواند در خصوص کلیه خسارات وارده تصمیم گیری کند. دیوان دادگستری اروپا هم در یکی از آرای خود چنین استدلال کرد که محدود شدن صلاحیت دادگاه محل وقوع خسارت در محیط فیزیکی، قابل اعمال در محیط اینترنتی نیست چرا که محیط اینترنتی، محیطی جهانی و فاقد مرز است و در حکم یک سرزمین محسوب می‌شود. لذا باید از سرزمینی گردن خسارات خودداری کرد چون سرزمینی کردن، با اوصاف محیط فیزیکی سازگار و منطبق است؛ از این رو، اگر صاحب اسرار تجاری در محیط دیجیتالی دچار زیان گردد، دادگاه یکی از کشورهایی که خسارت در آن وارد شده است، می‌تواند به کلیه خسارات حتی در کشورهای دیگر رسیدگی نماید و این از ویژگی‌های خاص این محیط است.

این تفسیر در آرای بسیاری از دادگاههای کشورهای اروپایی راه یافت و دادگاههای ملی این کشورها در برخی آرای خود در زمینه نقض مصادیق مختلف حقوق مالکیت فکری در محیط دیجیتالی، صلاحیت دادگاهها را توسعه دادند (صادقی، ۱۳۸۸).

۲-۳- معیار تعیین دادگاه صالح بر اساس کنوانسیون لاهه

کنوانسیون لاهه، منبع اصلی قواعد بین‌المللی در حوزه حقوق بین‌الملل خصوصی محسوب می‌گردد. این کنوانسیون که نتیجه نشست نخست اعضا در کنفرانس لاهه به سال ۱۹۸۳ بود، با هدف تلاش کشورها برای یکنواخت سازی قواعد حقوق بین‌الملل خصوصی و کاهش تعارضات در زمینه دادگاه صالح و قانون حاکم بر دعاوی بین‌المللی منعقد گردید. در سال ۱۹۹۲، ایالات متحده امریکا پیشنهاد داد تا کنوانسیون پیشنهادی در زمینه شناسایی و صلاحیت آرای محاکم خارجی در زمینه امور مدنی و تجاری تهیه شده و در آن تعارضات راجع به صلاحیت محاکم در دعاوی مالکیت فکری از جمله اسرار تجاری حل گردد. البته این پیشنهاد مورد توجه بسیاری از اعضا قرار نگرفت؛ اما برخی مواد آن، به این حقوق اختصاص یافت که چون این مواد با دعاوی مالکیت فکری از جمله اسرار تجاری در محیط‌های فیزیکی و دیجیتالی ارتباط مستقیم داشته و از آن می‌توان در تعیین دادگاه صالح به رسیدگی بهره برد. این کنوانسیون در ماده ۳ خود مشابه کنوانسیون بروکسل، اصل را در تعیین دادگاه صالح به رسیدگی، بر صلاحیت دادگاه اقامتگاه خوانده دعوی گذارده است.

با این حال ماده ۶ کنوانسیون در مواردی که میان صاحب حق و نقض کننده آن رابطه قراردادی وجود داشته و در فرضی مسئولیت مدنی، قائل به صلاحیت اضافی شده است.

بر اساس ماده ۶ کنوانسیون لاهه، دعاوی ناشی از قرارداد، در دادگاههای کشوری قابل طرح است که اجرای تعهد اصلی ناشی از قرارداد، کالا یا جتا در آنجا صورت پذیرفته است. بنابراین اگر تعهد متعهد در قرارداد با صاحب اسرار تجاری نقض شده باشد. ملاک دادگاهی است که اجرای تعهد اصلی کلا یا جزئا باید در آنجا صورت می‌گرفته است. تفاوت این کنوانسیون با کنوانسیون بروکسل یک در این است که در کنوانسیون لاهه، به اینکه اجرای جزئی یا کلی تعهد تاثیری در صلاحیت محلی دادگاه صالح به رسیدگی ندارد تصریح شده است در حالی که این صراحت از کنوانسیون بروکسل یک بر نمی آید و تردیدهایی در تفسیر بند یک ماده و به جا گذارده است.

صلاحیت دادگاه در فرض وجود قرارداد معتبر در یک مورد استثنا می‌خورد و آن در جایی است که به موجب شرط قراردادی میان صاحب اسرار تجاری و متعهد، طرفین پر دادگاه محل دیگری توافق کرده باشند. در این حالت به استناد ماده ۴ کنوانسیون لاهه، تمامی دعاوی مرتبط با این قرار داد باید در نزد دادگاه منتخب طرح گردد. این موضوع در کنوانسیون پروکسل مورد توجه قرار نگرفته است (کیانی، ۱۳۸۶).

با عنایت به انتقاداتی که به ابهام کنوانسیون بروکسل در خصوص معیار تعیین دادگاه صالح در فرض مسئولیت مدنی وارد شد، کنوانسیون پیشنهاد لاهه، این ابهام را بر طرف ساخته و در بند یک ماده ۱۰ خود تصریح می‌کند که در این فرض، یکی از دو دادگاه کشوری که فعل یا ترک فعل موجد ضرر در آن رخ داده باشد یعنی دادگاه کشور ما زبان یا دادگاه کشور محل ورود زبان، صالح به رسیدگی می‌باشند. بنابر این کنوانسیون حاضر به صاحب اسرار تجاری این اختیار را می‌دهد که در دعوای مدتی خود، یکی از این دو دادگاه را برای احقاق حق برگزینند. البته این اختیار در صورتی است که نظام حقوقی این دو کشور، اصرار تجاری در محیط دیجیتالی را مورد حمایت قرار داده باشند والا خسارت تنها در دادگاه کشوری قابل مطالبه است که اسرار تجاری دیجیتالی را مورد حمایت قرار می‌دهد

اما نکته چالش برانگیز در خصوص معیار فوق آن است که هر چند تا یک ماده ده، معیار تعیین دادگاه صالح را به روشنی بیان داشته است اما اعمال این معیار در عمل و به ویژه در محیط دیجیتالی بسیار دشوار است زیرا احراز اینکه خسارت در کجا ایجاد شده است، غالبا مشکل بوده و می‌تواند باعث بروز اختلاف صلاحیتی میان دادگاههای کشورهای مختلف گردد. از این رو برای رفع این دشواری، چندین راهکار پیشنهاد شد که حتی برخی از این پیشنهادها از سوی محاکم ملی برخی کشورها مورد استناد قرار گرفت و حتی برخی از این پیشنهادها توسط رویه قضایی برخی کشورها خلق گردید.

به چند مورد از این راهکارهای پیشنهادی اشاره می‌شود:

بر اساس راهکار نخست که در رای یکی از محاکم آمریکایی مورد استناد قرار گرفت، برای تشخیص محل وقوع خسارت و به تبع آن تعیین دادگاه محل وقوع خسارت، باید دید عمل زیانبار آیا محل خاصی را هدف قرار داده است یا خیر، به تعبیر دیگر، آیا وب سایت خوانده با حوزه قضایی دادگاه، ارتباط کافی و موثر دارد یا خیر؛ در این صورت، دادگاه محل هدف، صالح به رسیدگی است. دادگاه مقرر داشت که هر چند عمل نقض کننده حق صاحب مالکیت فکری، در کالیفرنیا صورت گرفته و صفحه الکترونیکی در این ایالت نمایش داده شده است اما چون صفحه به ایالت تنسی ارسال شده و در آنجا در دسترس عموم قرار گرفته است، لذا دادگاه تنسی صالح به رسیدگی به این دعوای الکترونیکی است. این راهکار البته با این انتقاد روبرو شد که تعیین هدف ناقض حق در بسیاری از موارد دشوار و غیر ممکن است ضمن آنکه گاه هدف واقعی ناقض حق با آنچه رخ داده در تعارض است برای مثال ناقض حق با هدف افشای اسرار تجاری، قصد دارد مطلب را به یک ایالت بفرستد اما اشتباها آن را به ایالت دیگر ارسال می‌کند، در این حالت باید ملاک را قصد واقعی در نظر گرفت با آنچه در ظاهر اتفاق افتاده است.

راهکار پیشنهادی دیگر در انگلستان مورد استفاده قرار گرفته است، بدین ترتیب که اگر خواهان یعنی صاحب سر تجاری، دعوای خود را هم علیه نقض کننده اصلی و هم علیه ارائه دهنده خدمات اینترنتی که ناقض حق را در افشای سر یا ورود خسارت به

خواهان پاری کرده است، اقامه کرده باشد در صورتی که محل ورود خسارت دقیقا مشخص نباشد می‌توان در دادگاه محل اقامتگاه یا تجارتخانه ارائه دهنده خدمات اینترنتی طرح دعوی نمود. اما این راهکار نیز مورد انتقاد بخری صاحب نظران قرار گرفته است چرا که تنها در قرق محدودی راهگشاست لذا به عنوان راهکار جایگزین این تفسیر را پیشنهاد داده اند که مراد از دادگاه کشوری که در آنجا به خاطر نقض اسرار تجاری خسارت وارد شده است، دادگاه کشوری است که خواهان در آنجا طرح دعوی کرده است

در هر حال، به واسطه جدید بودن بحث، هنوز راهکار مورد اتفاق کشورها ایجاد نشده و راهکارهای ارائه شده با ایراداتی روبرو شده اند. با این حال، صرفنظر از دشواری‌های فوق، یکی از برتری‌های قابل توجه کنوانسیون لاهه نسبت به کنوانسیون بروکسل در فرض مسئولیت مدنی آن است که کنوانسیون لاهه، ایراد کنوانسیون پروکسل را تا حدودی برطرف ساخته است.

طبق کنوانسیون بروکسل، اگر خسارات وارد شده به صاحب اسرار تجاری، در کشورهای مختلف به وقوع پیوسته باشد، خواهان باید در دادگاه هر کشور بابت همان میزان خسارات وارده طرح دعوی کند و دادگاه آن کشور تنها تا میزان خساراتی صالح به رسیدگی است که در آن کشور وارد شده است نه همه خسارات وارده در تمام کشورها بند ۴ ماده ۱۰ کنوانسیون پیشنهادی لاهه با اصلاح نسبی باد سوم ماده : کنوانسیون پروکسل مقرر می‌دارد که اگر خواهان دعوی (در فرض ما، صاحب اسرار تجاری)، در یکی از کشورهای محل ورود خسارت، دارای اقامتگاه معمولی ته موقتی باشد، دادگاه آن کشور صالح است تا علاوه بر خسارات وارد بر خواهان در آن کشور، نسبت به سایر خسارات وارده در کشورهای دیگر نیز رای صادر کند که این اصلاح، گام مهمی در حمایت از صاحبان حقوق مالکیت فکری در اینترنت محسوب می‌شود (رهبری، ۱۳۸۸).

نتیجه‌گیری

امضاهای الکترونیک کاربردهای بالقوه ای در تجارت الکترونیک دارند اما تلاش برای به کار گیری آنها به نحوی که منعکس کننده امضاهای مکتوب باشند احتمال تأثیر ضعیفی دارد، چرا که قیاس مزبور گمراه کننده است. وجود اشخاص ثالث معتمد به عنوان مراجع گواهی کننده امضاهای دیجیتالی، اغلب به وسیله قیاس با نقش مؤسسات مالی در تجارت سنتی توجه می‌شود. با این وجود، چنین قیاسی ظاهرا بر مبنای یک سوءبرداشت از آنچه که موسسات مالی فراهم می‌آورند استوار است، زیرا عناصر مداخله کننده در روابط مبتنی بر اعتماد، ظاهرا سه جانبه هستند. گواهی امضاهای دیجیتالی بیشتر به عنوان ساز و کارهایی برای انضمام یک اجازه به امضاهای دیجیتالی به کار می‌روند تا برای پیوند نام‌ها و هویت‌ها به امضاهای دیجیتالی (چنانچه قیاس با امضاهای مکتوب این نوع را در ما ایجاد می‌کند.) همین ویژگی‌های ترکیبی استفاده از امضاهای دیجیتالی، نه به عنوان محمل هایی برای هویت بلکه به عنوان ساز و کارهایی تلقی می‌گردند که می‌تواند روابط مبتنی بر اعتماد بسته را که تجارت بر آن استوار است، نمایندگی کند. گواهی امضاهای دیجیتالی هویتی و مراجع گواهی کننده مربوطه در توسعه تجارت الکترونیک در مقطع کنونی نقش کمرنگی دارد. به عبارت ساده، این نوع گواهی هویتی برای چنین مقاصدی ضروری نیستند و به نظر می‌رسد بیشتر از اینکه بازار الکترونیک را توسعه بخشند، ظهور آن را به تاخیر می‌اندازند.

گواهی امضاها و مراجع گواهی کنند که ساز و کارهایی برای اداره اجزاء کلید عمومی جفت کلیدها هستند مورد توجه و مباحثه فراوان بوده اند. بر عکس، اداره اجزاء کلید امضاء خصوصی جفت کلیدها توجهی را که شایسته آن بوده است، دریافت نداشته اند. این امر تعجب آور است، زیرا بسیاری اعتقاد دارند که مسائل فنی و حقوقی مرتبط با این اجزاء مهمترند، به ویژه برای امضاهای مکتوب، چرا که این طرف اعتماد کننده است که بار اثبات اصالت آنها را بدوش می‌کشد. با این وجود طرح‌های دولت انگلستان برای امضاهای دیجیتالی دارای مجوز، قرار دادن مسئولیت نقص بر عهده دارند کلید را پیشنهاد می‌کنند. چنین گاهی خطرات مهمی را متوجه مصرف کنندگان می‌سازد، زیرا فناوری موجود برای اداره کلید خصوصی در حال حاضر قادر به تأمین امنیت مورد نیاز برای حمایت از چنین تحولی نیست بر طبق رویکرد اتخاذ شده در قانون نمونه امضاهای الکترونیکی آنسیترال

موقعیت جغرافیایی به هیچ وجه به عنوان عاملی در جهت شناسایی قانونی گواهی‌ها و امضاهای الکترونیکی تلقی نخواهد شد بلکه در عوض باید به مسائل فنی و اینکه گواهی یا امضا به چه میزان از نظر فنی قابل اعتماد است توجه نمود. مفهوم استانداردهای بین‌المللی پذیرفته شده را باید به گونه ای موسع تفسیر نمود به طوری که استانداردهای فنی و تجاری (یعنی استانداردهای پذیرفته شده در بازارهای بین‌المللی) و استانداردها و قواعد اتخاذ شده توسط دولت‌ها و ارگان‌های بین‌دولتی را در بر گیرد این استانداردها ممکن است در قالب الزامات قانونی، توصیه نامه، رهنمود و ... ارائه شده باشد.

منابع و ماخذ

۱. احمدیان راد، حمیده، امضای دیجیتال چیست؟، مجله پیام بانک، شماره ۵۸۹، ۱۳۸۸

۲. باریکلو، علی رضا، مسئولیت مدنی، انتشارات میزان، چاپ سوم ۱۳۸۹

۳. برایان، گلادمن، امضاهای دیجیتالی، گواهی امضاهای الکترونیکی و تجارت الکترونیک، ترجمه محمدرضا ملکی، مجله کانون، سال چهل و هشتم، دوره دوم، شماره ۲۰ فروردین ۱۳۸۵.

۴. داراب پور، مهراب، مسئولیت‌های خارج از قرارداد، انتشارات مجد، چاپ اول ۱۳۸۷

۵. ره پیک، حسن، حقوق مسئولیت مدنی و جبران ها، انتشارات خرسندی، چاپ پانزدهم ۱۳۹۰

۶. رهبری، ابراهیم، حقوق اسرار تجاری، انتشارات سمت، چاپ اول، ۱۳۸۸

۷. ژوردن، پائریس، اصول مسئولیت مدنی، ترجمه مجید ادیب، انتشارات میزان، چاپ دوم ۱۳۸۵

۸. السان، مصطفی، دوان پامچی، امین، ماهیت رایانه ای و جنبه‌های حقوقی امضای دیجیتالی، مجله دیدگاه‌های حقوقی قضایی، شماره ۳۰ و ۳۱، ۱۳۸۳

۹. صادقی، محسن، مطالعه تطبیقی تعیین مرجع صالح رسیدگی به دعاوی حقوقی نقض اسرار تجاری در فضای دیجیتالی، ماهنامه قضاوت، اسفند ۱۳۸۸.

۱۰. غمامی، مجید، قابلیت پیش بینی ضرر در مسئولیت مدنی، انتشارات شرکت سهامی انتشار، چاپ دوم ۱۳۸۸

۱۱. فدوی النجوانی، سلیمان، امضاهای دیجیتالی، گواهی امضای الکترونیکی و تجارت الکترونیک، ترجمه، مجله کانون، سال چهل و هشتم، دوره دوم، شماره ۲۰ فروردین ۱۳۸۵

۱۲. قاسم زاده، مرتضی، الزام‌ها و مسئولیت مدنی بدون قرارداد، انتشارات میزان، چاپ دوم ۱۳۸۷

۱۳. کاتوزیان، ناصر، الزام‌های خارج از قرارداد، انتشارات میزان، چاپ پنجم، ۱۳۸۵

۱۴. کیانی، رضا صفاریان، مریم، فرآیند و الزامات افشای اطلاعات در بازار سرمایه، مجله اقتصادی، سال هفتم، شماره‌های ۷۱ و ۷۲، ۱۳۸۹

۱۵. محمدزاده، محمود، تجارت الکترونیک و امضای الکترونیکی، مجله کاتون، سال چهل و هشتم، دوره دوم، شماره ۱۲، تیر ۱۳۸۵

۱۶. مظاهری کوهانستانی، رسول، مطالعه تطبیقی امضای الکترونیکی در حقوق ایران و مقررات آنسیترال، انتشارات جنگل، چاپ اول، ۱۳۹۳

۱۷. مظاهری، رسول، ناظم، علیرضا، ارزش اثباتی داده پیام و امضای الکترونیکی، مجله نامه مفید، شماره ۷۰، ۱۳۸۷، ص ۸، ص ۱۳۷ ۱۸

۱۸. نوری، سید مسعود، اصول حقوقی تجارت الکترونیک با تاکید بر قانون تجارت الکترونیک ایران، مجله روش شناسی علوم انسانی، شماره ۴، ۱۳۸۶

19. Von bar, Christian, study on property law and non-contractual liability law as they releate to contract law, University of Osnabrick publisher, Hamburg, 2002.

Journal of Iranian Social Development Studies (JISDS)
2023 (Winter), Vol. 15, No. 1

Effects of electronic signature recognition in signature certificate offices and its social responsibility

Rahim Abdoli [1]
PhD student in Private Law, Emirates Branch, Islamic Azad University, United Arab Emirates
Tayeb Afsharnia [2]
Assistant Professor, Department of Law, Faculty of Humanities, West Tehran Branch, Islamic Azad University, Tehran, Iran. (Corresponding Author)
Alireza Rajabzadeh Stahbanani
Assistant Professor of non-profit Rajaa University, Qazvin, Iran

Abstract: *Electronic signature certificate offices, as a legal entity, register and certify electronic signatures in order to secure the rights of some individuals. Electronic signature certificate offices comply with certain terms and conditions in order to issue a signature certificate and conform it to the original. One of the most important responsibilities that e-signature certification offices give to signatories is to maintain the confidentiality and confidentiality of citizen information. One of the most important principles used in this study is to examine the responsibility of the owners of electronic signature certificate offices, the details of which have been evaluated. According to the approach adopted in the law, the sample of non-central electronic signatures, geographical location will not be considered in any way as a factor in the legal identification of electronic certificates and signatures. Instead, pay attention to the technical issues and how technically reliable the certificate or signature is.*

Key words: *Office, Signature, Electronic, Certificate, Digital.*

[1] Email: abdoli_rahim@yahoo.com
[2] Email: afsharnia59@gmail.com (Corresponding Author)