اعتبارحقوقی
امضای الکترونیکی از منظر قانون تجارت الکترونیکی

فاطمه قناد[1]

تاریخ دریافت: ۹۲/۹/۱۲ ..... تاریخ پذیرش: ۹۲/۱۲/۱۵

چکیده

امضای الکترونیکی و اعتبار آن در عرصه های مختلف فناوری های اطلاعات و ارتباطات، یکی از چالشهای مهم در عرصه تجارت الکترونیکی است و در بسیاری از نظامهای حقوقی معاصر، اتخاذ سیاست تقنینی و ایجاد ساز و کارهایی که از یکسو بتواند زمینه بروز، رشد و گسترش بهره برداری از امضای الکترونیکی را فراهم کند و از دیگر سو حافظ امنیت حقوقی و حقوق اجتماعی شهروندان باشد، از برزگترین دغدغه های قانونگذاران به شمار می رود. نظام حقوقی ایران همراستا با پیشرفت های تقنینی بین المللی در این عرصه، مقررات قانون تجارت الکترونیکی را از سال ۱۳۸۲ در اختیار دارد و مقاله حاضر با در نظر گرفتن اهمیت موضوع، مفهوم و ماهیت امضای الکترونیکی و چگونگی اعتبار آن در نظام حقوقی ایران را در پرتو مقررات داخلی، اسناد بین المللی و برخی نظامهای حقوقی خارجی، مورد بررسی قرار می دهد.

واژگان کلیدی:
امضای الکترونیکی، امضای رقومی/دیجیتالی، امضای بایومتریک، تجارت الکترونیکی، فناوری اطلاعات و ارتباطات.

---

۱ - استادیاردانشگاه علم و فرهنگ.

۱- درآمد

«امضای الکترونیکی» از ارکان اساسی تجارت الکترونیکی تلقی می‌شود و ایجاد سازوکاری که در فضای مجازی بتواند، اعتبار حقوقی لازم را برای امضای الکترونیکی ایجاد نماید، یکی از چالشهای بزرگ غالب نظام‌های حقوقی معاصر است. قانونگذاران و نیز بازرگانان در سراسر دنیا، بدنبال ایجاد سازوکارهایی هستند که بتواند به امضای الکترونیکی، اعتباری جهانی ببخشد. حقوق و فناوری هر دو از ابزارهایی هستند که دستیابی به‌این مهم را تسهیل می‌کنند (Brazell, 2009,p.11) و در تعریفی که از امضای الکترونیکی ارائه می‌شود، غالباً هر دو این ابزارها را بکار گرفته‌است. وفق بند ی ماده ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲، امضای الکترونیکی عبارت از هر نوع علامت متصل به داده‌پیام‌است، که برای شناسایی امضاکننده مورداستفاده قرار می‌گیرد (۱) و اگر واجد برخی اوصاف و شرایط قانونی و فنی خاص باشد، امضای الکترونیکی مطمئن نامیده می‌شود و از این نظر با امضای دستنویس، که ذیل اسناد کاغذی درج می‌گردد و در دفاتر اسناد رسمی گواهی می‌شود، تفاوت چندانی ندارد. غالب نظام‌های قانونگذاری، تعریفی از امضا ارائه نداده‌اند. (همان) امضا در لغت به معنای تنفیذ امری‌است و به صورت نوشتن نام، یا علامت خاصی که نمایانگر هویت صاحب علامت‌است، در ذیل اوراق و اسناد متضمن وقوع معامله‌است. (جعفری لنگرودی، ۱۳۷۸، ص. ۸۱) این امضا جزئی از ماهیت معامله نیست، بلکه مؤید شکل آن‌است و باید دارای اوصاف و عملکردهای خاصی باشد. نخست آنکه؛ مشخص کننده هویت امضا کننده باشد و سایر اشخاص امکان استفاده از آن را نداشته باشند. دوم اینکه عمل مثبتی باشد که به مفهوم تصدیق صحت معامله‌است (Brazell, op.cit., p. 12) و چنانچه به گونه‌ای اعمال شود، که موجب اصالت امضا و مدرک باشد و امکان انکار و تکذیب یا تغییر آن وجود نداشته باشد« امضای مسلم‌الصدور» تلقی می‌شود. (جعفری لنگرودی، پیشین)

وجود امضا در ذیل نوشته یا سند، جزیی از شرایط شکلی اعتبار سند‌است و تصدیق صحت و اصالت امضا، به عنوان ابزاری جهت پیشگیری از ادعای انکار یا تردید و حتی جعل تلقی می‌شود. نتیجه چنین فرایندی ایجاد «امضای مسلم‌الصدور»است که هیچگونه دعوای انکار یا تردید، علیه آن مسموع نیست. (قانون آئین دادرسی در امور مدنی، ۱۳۷۹، ماده ۲۲۵) امضای الکترونیکی نیز از این امر مستثنی نیست و برای اینکه واجد آثار حقوقی باشد و صدور آن به مفهوم شناسایی هویت امضاکننده و اصالت امضا و مدرک باشد و عملی مثبت قلمداد شود، باید از یک سلسله شرایط شکلی برخوردار بوده و چون امری مبتنی بر فناوری‌است، از قواعد فنی خاصی نیز تبعیت نماید. هدف از وضع شرایط قانونی برای اعتبار بخشیدن به امضای الکترونیکی و بویژه تولید و صدور امضای الکترونیکی مطمئن، تضمین تمامیت، دوام و امضاپذیری اسناد الکترونیکی‌است. از این رویکرد، اسناد الکترونیکی که

بدین نحو امضا شده‌اند، اعتباری همسان با اسناد کاغذی با امضای دستنویس دارند. هر قدر کارایی سیستم فنی که برای صدور امضای الکترونیکی استفاده می شود، بیشتر باشد، تمامیت، دوام و ارتباط سند با فایلهای امضایی که برای آن ایجاد شده بیشتر است. از این رو امضایی که وفق شروط مقرر در قانون، صادر شود «امضای الکترونیکی مطمئن» نام می‌گیرد و همچون امضای مسلم‌الصدورکه ذیل اسناد کاغذی درج می‌گردد، هیچگونه دعوای انکار یا تردید علیه آن مسموع نبوده و قابل انتساب به صادرکننده‌است. قانون تجارت الکترونیکی ایران از عبارت امضای الکترونیکی بهره جسته‌است تا بتواند فناوری‌های مختلفی را که در حوزه امضای الکترونیکی ابداع می‌شود، مورد استفاده قرار دهد و قانون را با مقتضیات فناوری روز منطبق نماید. به علاوه محدود نشدن موضوع تکنولوژی موجب می‌گردد که رقابت بر سر ایجاد و ابداع روشهای نوین نیز همچنان باقی بماند.(حبیب زاده، ۱۳۹۰،۱۳۰) مفهوم و نیز اعتبار امضای الکترونیکی، اساساً به فناوری‌هایی که برای تولید آن مورد استفاده قرار می‌گیرد، مرتبط است و قانون تنها اوصاف و شرایط معتبر بودن امضا را بیان می‌کند و فناوری خاصی را مورد اشاره قرار نمی‌دهد. (Brazell, op.cit., p. 36) تفاوت امضای الکترونیکی با امضای رقمی در این نکته نهفته‌است. در امضای الکترونیکی هر نماد الکترونیکی که به امضا متصل شود معتبر بوده و می‌توان از کلیه اشکال فناوری‌های الکترونیکی سطح پایین و سطح بالا برای تولید آن بهره گرفت. بعنوان نمونه وقتی بااستفاده از قلم نوری متن یک سند امضا می‌شود(همان، ص. ۳۸)، یا در موردی که شخصی امضای مکتوب خود را در رایانه «تصویربرداری» نموده و آن را به یک نوشته «منضم» می کند، یا حتی در موردی که شخصی نام خود را ذیل یک سند الکترونیکی درج می‌کند(همان)، یک سند با امضای الکترونیکی تولید نموده‌است و لزومی به‌استفاده از فنون رمزنگاری در چنین امضایی وجود ندارد. چنین امضایی اگر چه قابل جعل است، ولی امضای الکترونیکی بااستفاده از فناوری سطح پایین تلقی می‌شود.(همان، صص. ۳۸ ۳۷) در مقابل دو روش مبتنی بر فناوری سطح بالا نیز وجود دارد. نخست، «امضای رقمی» قرار دارد که محدود به فناوری زیرساخت کلیدهای عمومی است و بااستفاده از این فناوری سطح بالا، اسناد «رمزنگاری» و بعبارتی امضا می‌شوند و سپس مورد شناسایی قرار می‌گیرند(Baker,2008, p.p. 248 249) و از آنجا که این رمزنگاری بااستفاده از یک جفت کلید عمومی و اختصاصی صورت می‌پذیرد، «رمزنگاری نا متقارن» نامیده می‌شود(۲). (همان، ص۶۱۷) و دوم «امضای بایومتریک یا مبتنی بر زیست‌سنجی» که بااستفاده از خصوصیات زیستی هر شخص نظیر ویژگیهای شبکیه، عنبیه یا اثر انگشت وی طراحی شده و منحصر به فرداست. وسایلی که برای ثبت ویژگیهای زیستی هر فرد بکار می‌روند، امروز بصورت تجاری خرید و فروش می‌شوند و از طریق آنها، اثر انگشت، ساختار شبکیه و عنبیه چشم، خطوط کف دست، شکل رگها، میزان فشار دست بر روی کاغذ در هنگام امضا، و حتی ترکیب صورت

قابل ثبت و اندازه‌گیری است. این دستگاهها پس از ثبت ویژگیهای زیستی هر شخص، آنرا به اطلاعات عددی تبدیل می‌کنند. به‌این فرایند، «رقمی سازی» گفته می‌شود. این ارقام مبنای شناسایی ویژگیهای زیستی شخص، در مراجعات بعدی قرار می‌گیرد. اشکال این فناوری این است که ویژگیهای جسمی انسان در اثر افزایش سن، بیماری و سایر عوامل تغییر می‌کند. فشار بیش از حد ابزار اندازه‌گیری بر عضو ممکن است باعث صاف شدن عضو و اشکال در تعیین محدوده دقیق آن گردد، یا در مواردی که زخم وجود دارد، اندازه گیری دقیق نخواهد بود. از اینرو ممکن است بواسطه این اندازه گیری غیر دقیق، شخص مجاز را غیر مجاز اعلام کرده و شخص غیرمجاز را تأیید نماید. این خصیصه، نقطه ضعف این روش بشمار می‌رود و از اینرو استفاده از روشهای رمزنگاری برای تولید امضای الکترونیکی مطمئن رایج‌تر است. (Vacca,2012, p،8) بعضی از نظام‌های قانونگذاری نظیر بلژیک، فرانسه، آلمان، ایرلند، فنلاند، نروژ، اسپانیا، سوئد، هلند و پادشاهی متحده انگلستان استفاده از فناوری «زیرساخت کلید عمومی» را شرط صحت امضای الکترونیکی اعلام و بعبارتی امضای رقمی را مورد تأیید قرار داده‌اند، (Brazell,op.cit., pp.28 35) و برخی دیگر همانند ایران، بر فناوری خاصی تأکید نداشته و تنها معیارهای لازم برای اعتبار بخشیدن به امضای الکترونیکی را بیان نموده‌اند که البته مسیری است که به امضای رقمی ختم می‌شود و تحقق آن بااستفاده از فناوری زیر ساخت کلید عمومی امکان‌پذیر است. این ابزار تولیدکننده امضای الکترونیکی مبتنی بر رمزنگاری و متشکل از یک جفت کلید عمومی و اختصاصی است که مکمل یکدیگرند و برای رمزنگاری و رمزگشایی فایل‌های اطلاعاتی الکترونیکی به کار می‌روند. این رمزنگاری امضایی تولید می‌کند که اصطلاحاً، «امضای الکترونیکی مطمئن»، یا «امضای رقمی» نامیده می‌شود. «کلید عمومی» شخص، فاقد وصف محرمانگی بوده و در دنیای تجارت الکترونیکی، در دسترس عموم کاربران قرار می‌گیرد، لیکن «کلید اختصاصی»، «کد رقمی» محرمانه شخص است، که همانند اثر انگشتان وی تلقی شده و باید مورد حفاظت قرار گیرد. (۳) فناوری‌ای که برای رمزنگاری داده‌ها مورد استفاده قرار می‌گیرد، به عملیات هش (hash function) شهرت دارد. این عملیات، اطلاعات را به یک ارزش با اندازه معین تبدیل می‌کند، که ارزش هش (hash value) نامیده می‌شود. الگوریتمی که به هر داده‌پیام اختصاص داده می‌شود، (hash algorythm) منحصر به فرد است. به‌این صورت که برای هر حرف الفبا، یک عدد مشخص و منحصر به فرد تعیین می‌شود و متن، دوباره با این اعداد بازنویسی می‌گردد. سپس کلیه اعداد با هم جمع می‌شوند و حاصل جمع، به عنوان داده‌پیام به آسانی منتقل می‌شود. (کی نیا، ۱۳۸۸، ۱۹ ۲۲) حتی اگر یک حرف، از این متن تغییر کند، متن جدید یک ارزش هش جدید تولید می کند و در نتیجه، حاصل جمع تغییر می کند و جعلی بودن متن معلوم می‌شود. رمزگشایی نیز به‌این صورت است که دریافت کننده، کلید اختصاصی خود یا کلید عمومی فرستنده را (حسب اینکه متن با چه کلیدی

رمزنگاری شده باشد) بکار می‌برد، تا اصالت امضای الکترونیکی فرستنده پدیدار شود. سپس همان الگوریتم هش را بکار می‌برد تا متن رمزنگاری شده، رویت پذیر شود، آنگاه با بهره‌گیری از کلید عمومی فرستنده، متن رویت شده را، رمزگشایی می کند و از این طریق تمامیت و اصالت متن و فرستنده آن، اثبات می‌شود.(Baker, op.cit., p.p. 4 5) به بیان دیگربرای تولید امضای الکترونیکی مطمئن بااستفاده از روش رمزنگاری، امضاکننده، پس از تولید داده‌پیام، اعم از متن، صدا و تصویر، آنرا با کلید اختصاصی خود رمزنگاری نموده و برای مخاطب ارسال می‌نماید. در این مرحله، رمزگشایی داده‌پیام صرفاً از طریق کلید عمومی شخص امضاکننده، که مکمل کلید اختصاصی اوست امکان‌پذیر بوده و با هیچ روش دیگری قابل رمز گشایی نمی‌باشد. ناگفته پیداست، چنانچه کلید اختصاصی امضاکننده در دسترس اشخاص دیگری قرار گیرد، امکان ایجاد اسناد جعلی با امضای دارنده کلید اختصاصی و هر گونه سوءاستفاده وجود دارد و از این رو محافظت از آن بسیار ضروری است. این امر در ماده ۸ قانون نمونه امضای الکترونیکی کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد مصوب سال ۲۰۰۱ و بند ۶ ماده ۹ ویرایش دوم «شیوه‌نامه اتاق بازرگانی بین‌المللی در خصوص تجارت بین‌الملل با استفاده از فناوری‌های رقمی»، مورد اشاره قرار گرفته و دارنده ابزارهای تولید امضا مکلف به مراقبت و نگهداری از ابزارها بوده و در مواردی که احتمال هر گونه سوءاستفاده از ابزارها وجود دارد، باید مراتب را فوراً به کلیه اشخاصی که ممکن است در رابطه با چنین سوءاستفاده‌هایی لطمه ببینند، اعلام نماید، والا مسئول جبران خسارتهای وارده خواهد بود.(۴) از سوی دیگر چنانچه داده‌پیام، با استفاده از کلید عمومی مخاطب، رمزنگاری و برای وی ارسال شود، بازگشایی آن صرفاً از طریق کلید اختصاصی شخص مخاطب امکان‌پذیر بوده و اطلاعات آن برای هیچ کس جز مخاطب قابل درک نمی باشد. خدمات مربوط به کلیدهای مزبور، به موجب ماده ۳۱ قانون تجارت الکترونیکی از طریق «دفاتر خدمات صدور گواهی الکترونیکی» در اختیار درخواست کنندگان قرار می‌گیرد. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به روز نگهداری، گواهی‌های اصالت امضای الکترونیکی می‌باشد. وظیفه اصلی این دفاتر، شناسایی و تأیید هویت امضاکنندگان و اصالت امضای ایشان است، که با ارائه کلیدهای مزبور انجام می‌پذیرد. به عبارت دیگر، با استفاده از این ابزارهای فناورانه، امکان جعل امضای اشخاص، یا دستیابی به متن داده‌پیامهای اختصاصی ایشان در محیط الکترونیکی، جز با دستیابی به کلید اختصاصی آنها وجود ندارد و از این روست که قانونگذار در مواد ۱۰ و ۱۵ قانون تجارت الکترونیکی پس از تبیین کلی شرایط اختصاصی امضای الکترونیکی مطمئن، امضاء داده‌پیام به طرق مذکور را معتبر و سند حاصله را در حکم اسناد معتبر و غیر قابل انکار و تردید دانسته و اگر چه از عباراتی مبهم و غیردقیق استفاده نموده، ولی ارزش اثباتی معادل اسناد رسمی، برای چنین امضایی قایل شده است، و تنها امکان طرح ادعای جعل در خصوص مورد، یا فقدان اعتبار،

به جهات قانونی همچون حجر و فوت دارنده کلید در زمان استفاده از آن، یا ادعای سرقت یا خیانت در امانت و سوءاستفاده از کلید اختصاصی که نزد امین، امانت بوده است، را پیش‌بینی کرده و مسلماً بار اثبات دلیل نیز بر عهده مدعی خواهد بود.

۲- شرایط صحت امضای الکترونیکی

با در نظر گرفتن مفاد ماده ۱۰ قانون تجارت الکترونیکی، یک امضای الکترونیکی باید واجد چند خصیصه عمده باشد(۵).

۱. نسبت به شخص امضا کننده، منحصر بفرد باشد، بدین معنا که توسط هیچ شخص حقیقی یا حقوقی دیگری قابل صدور نبوده، در نتیجه امکان مشابه سازی و موارد جعل آن، بدون استفاده از کلید اختصاصی امضاکننده وجود نداشته باشد. این وصف که مطابق شرایط امضای سنتی است، با بهره‌گیری از فناوری زیرساخت کلید عمومی به آسانی محقق می‌گردد.

۲. هویت امضا کننده داده‌پیام را معلوم نماید. شناسایی هویت امضاکننده داده‌پیام، از مهم‌ترین مباحث تجارت الکترونیکی است. عدم توجه تجار به هویت طرف تجاری ممکن است ایشان را نادانسته در معاملات ممنوعه درگیر و مشمول رسیدگی‌های قضایی قرار دهد.(۶)

۳. بوسیله امضاکننده و یا تحت اراده انحصاری وی صادر شده باشد. این بدان مفهوم است که یا شخص امضاکننده، یا اشخاصی که کلید اختصاصی وی را در اختیار دارند، یا سیستم‌ها و نرم‌افزارهای تحت نظارت و پایش او، امضا را صادر کرده باشند و امضای سنتی نیز بدون در نظر گرفتن قسمت اخیر، عرفاً از چنین شرطی برخوردار است.

تحقق این شرط نیز با بهره‌گیری از فناوری زیرساخت کلید عمومی امکان‌پذیر است، بدین نحو که امضاکننده با استفاده از کلید اختصاصی خود، شخصاً مبادرت به صدور امضا نموده، یا با قراردادن کلید مزبور در اختیار شخص یا سیستم‌ها و نرم‌افزارهایی که تحت کنترل دارد، اراده خود را جهت صدور امضا نمایان می‌سازد. از اینروست که، در بند «ل» ماده ۲ قانون، امضاکننده، اعم از شخص تولیدکننده امضا یا قائم مقام وی می‌باشد و به موجب بند «م» همان ماده، شخص، اعم است از شخص حقیقی و حقوقی و یا سیستم رایانه‌ای تحت نظارت و پایش آنان. بدین ترتیب صدور امضا به صورت خودکار و با استفاده از برنامه نرم‌افزاری یا سیستم رایانه‌ای خودکار، که توسط شخص تنظیم شده است، مورد شناسایی قانونی قرار گرفته است.

۴. آخرین شرط آنکه، امضای الکترونیکی، باید به نحوی تولید و به داده‌پیام متصل شود، که هر گونه تغییر در داده‌پیام، قابل تشخیص و کشف باشد.

تحقق این شرط نیز با تکیه بر زیرساخت کلید عمومی امکان‌پذیر است. امضاکننده با استفاده از کلید

اختصاصی خود، داده‌پیام را رمزنگاری و ارسال می‌نماید. مخاطب صرفاً با استفاده از کلید عمومی شخص امضاکننده، می‌تواند نسبت به رمزگشایی اقدام کرده و داده‌پیام را از حالت یک سلسله نمادها و علائم غیرقابل درک، به اطلاعاتی قابل تشخیص مبدل نماید. مسلماً با استفاده از این فناوری، ایجاد تغییر در داده‌پیام امکان ناپذیر بوده و سالبه به انتفاء موضوع است. صدور امضای الکترونیکی با چهار شرط فوق، مورد حمایت قانونگذار بوده و دارای آثار و نتایجی است که از نظر قانون معتبر و لازم‌الاجراست.

۳- آثار و احکام صدور امضای الکترونیکی

وفق ماده ۷ قانون تجارت الکترونیکی، هر گاه قانون وجود امضا را لازم بداند، امضای الکترونیکی مکفی است. و چنانچه امضای الکترونیکی، واجد کلیه شروط مورد نظر قانونگذار باشد، اعتبار امضای مندرج در ذیل اسناد معتبر را داشته و امکان انکار و تردید در خصوص مورد وجود ندارد و شخص نمی‌تواند منکر انتساب امضا به خود، یا اعلام تردید نسبت به انتساب آن به دیگری باشد. به موجب ماده ۱۵ قانون در خصوص این امضا، صرفاً ادعای جعلیت، یا فقدان اعتبار، به جهات قانونی قابل طرح است، که بار اثبات آن برعهده مدعی خواهد بود.

به علاوه وفق ماده ۱۴ قانون، داده‌پیامی که حاوی چنین امضایی باشد میان طرفین و قائم مقام قانونی آنان معتبر بوده و از حیث اجرای مفاد و سایر آثار، در حکم اسناد معتبر و قابل استناد در مراجع قضایی و حقوقی است.

۴- حقوق مقایسه‌ای

تعریف و شرایط صدور امضای الکترونیکی، در غالب نظام‌های حقوقی و رویه‌های قانونگذاری، از یک الگو تبعیت می‌کند زیرا ساختار فنی به کار گرفته شده جهت ایجاد این امضا، این اشتراک در تعریف و شرایط را موجب می‌شود. به عنوان نمونه، می‌توان به قانون نمونه امضای الکترونیکی کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد در سال (2001UNCITRAL Model Law on Electronic Signature) اشاره کرد. این کنوانسیون آثار حقوقی حاکم بر اسناد کاغذی را بر مکاتبات الکترونیکی بار کرده و یکسان سازی تقنینی در خصوص مورد را ضروری اعلام نموده است.(Charles, 2005، 261) وفق بند الف ماده ۲ این قانون، امضای الکترونیکی عبارت از داده‌های الکترونیکی است که به داده‌پیامهایی که امضاکننده در صدد تأیید و تصدیق آن است، منضم شده باشد، مشروط بر اینکه وفق بند ۳ ماده ۶ قواعد واجد شرایط زیر باشد:

۱) نسبت به امضاکننده منحصر به فرد باشد؛

۲) هویت امضاکننده را شناسایی نماید؛
۳) تحت ارادهٔ انحصاری امضاکننده صادر شده باشد؛
۴) بگونه‌ای به داده‌پیام ملحق شده باشد که هر گونه تغییر بعدی داده‌پیام را آشکار سازد.

اتاق بازرگانی بین‌المللی در شیوه‌نامه تجارت بین‌المللی با استفاده از فناوری رقمی در سال ۲۰۰۱ منتشر نموده‌است و امضای الکترونیکی را به همان سبکی که در ماده ۷ قانون نمونه کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد در خصوص تجارت الکترونیکی مطرح شده بود، واجد اعتبار کرده‌است، لیکن به برخی جنبه‌های جدید امضای الکترونیکی نظیر امضا با استفاده از فناوری زیست‌سنجی نیز توجه نموده و بعضی تعاریف و رویه‌های جدید به منظور تأیید محتوای داده‌پیام و گواهی صحت و اصالت امضای الکترونیکی در آن بیان گردیده‌است. این شیوه‌نامه همانند قوانین نمونه سازمان ملل، فناوری زیرساخت کلید عمومی را برای صدور امضای الکترونیکی مورد تأیید قرار داده، لیکن امکان بکارگیری فناوری‌های دیگر را نیز مدنظر قرار داده‌است. (International Chamber of Commerce Guiding Usage, 2001., Glossary) اگر چه‌این شیوه‌نامه، جنبه الزام آور ندارد ولی بیشتر تشکلهای تجاری بین‌المللی به قواعد آن توجه دارند و دادگاهها نیز در هنگام صدور رأی، عمل به شرایط مقرر در شیوه‌نامه را بعنوان ملاکی برای رفتار متعارف و معقول طرفین دعوا، در نظر می‌گیرند. (Brazel., op.cit., p. 86)

دستورالعمل شماره ۹۹/۹۳ پارلمان و شورای وزیران اتحادیه اروپا در خصوص امضای الکترونیکی نیز حاوی نکات مهمی در زمینه اعتبار امضای الکترونیکی است. (Directive 99/93, op.cit.) بموجب بند یک ماده ۵ این دستورالعمل، در مواردی که امضای الکترونیکی فاقد اوصاف مقرر برای امضای الکترونیکی مطمئن باشد، اعتبار حقوقی آن باید در کنار سایر ادله توسط دادگاه بررسی شود و به صرف عدم احراز شرایط لازم، نباید از سوی دادگاهها رد شود. البته این ایراد به دستورالعمل وارد شده که اصل «بی طرفی فناورانه» را نادیده گرفته و از تمامی امضاهای الکترونیکی صرفه‌نظر از شیوه تولید حمایت ننموده‌است. در عین حال، در مواردی که امضای الکترونیکی، شرایط مد نظر برای صدور امضای الکترونیکی مطمئن را رعایت کرده باشد، باید اعتباری معادل امضای دستنویس داشته باشد که با خصوصیاتی مشابه صادر شده‌است، و در محاکم مورد قبول قرار گیرد. به این اصل «هم ارزی عملکردی» نام نهاده‌اند و اعتبار یکسان امضا در نظام ها ی حقوقی را تضمین می کند. بموجب بند ۲ ماده ۵ دستورالعمل، اعتبار امضای الکترونیکی نباید صرفاً به‌این جهت رد شود که، شکل و قالب الکترونیکی دارد و یا از سوی دفاتر خدمات صدور گواهی الکترونیکی مورد تأیید قرار نگرفته یا با وسایل فنی مطمئنی صادر نشده‌است.

امضای الکترونیکی در ماده ۲ دستورالعمل تعریف شده است و عبارت از داده‌یی الکترونیکی است که به داده‌های الکترونیکی دیگر متصل یا به نحو منطقی مرتبط است و بعنوان روشی برای احراز اصالت بکارمی‌رود. مفهوم امضای الکترونیکی بموجب این تعریف همانند تعریف مندرج در بند ی ماده ۲ قانون تجارت الکترونیکی ایران، بسیار گسترده است، زیرا داده‌یی است که قابلیت اتصال یا همراهی منطق دار، با سایر داده‌های الکترونیکی را دارد و از هیچ ویژگی خاصی برخوردار نیست.

امضای دستنویس نیز چنانچه تصویربرداری شده و از طریق رایانه به داده‌پیام ضمیمه شود و یا اسم فرد که ذیل سند الکترونیکی درج شده باشد، امضای الکترونیکی تلقی می‌شود. (Brazell. op.cit., p. 92)

تعریف ارائه شده در این ماده با تعریف بند الف مادۀ ۲ قانون نمونه امضای الکترونیکی مصوب کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد نیز مطابقت دارد. اینکه امضاهای الکترونیکی بعنوان روشی برای احراز اصالت شخص قابل استفاده باشد، بدین معناست که امضاکننده قصد دارد مندرجات سند را تأیید و آنرا به خود منتسب نماید و در نتیجه اصالت وی از طریق امضای الکترونیکی، قابل احراز است.

شرایط امضای الکترونیکی مطمئن نیز در این دستورالعمل بیان و در قالب چهار شرط اساسی مطرح گردیده است:

۱) نسبت به امضاکننده منحصر بفرد باشد؛

۲) هویت امضاکننده را شناسایی نماید؛

۳) تحت اراده انحصاری امضاکننده صادر شده باشد؛

۴) بگونه‌ای به داده‌پیام مرتبط شده باشد که هر گونه تغییر بعدی داده‌پیام را آشکار سازد.

ملاحظه می‌شود که مجموع شرایط فوق که عیناً در بندهای چهارگانه ماده ۱۰ قانون تجارت الکترونیکی ایران نیز تکرار شده، متضمن بکارگیری فناوری امضاهای رقمی است، زیرا امروزه تنها فناوری است که تحقق کلیه شروط فوق را امکانپذیر می‌سازد و هر گونه تغییر بعدی در داده‌پیام را قابل رویت می‌نماید. از اینرو برای صدور امضای الکترونیکی مطمئن گریزی جز بکارگیری روش امضای رقمی نیست. البته امضایی که بدین نحو تولید می‌شود در صورتی ارزشی معادل امضای دستنویس (که با شرایط و خصوصیات مشابه صادر شده باشد) را دارد که اصالت صادر کننده و صحت انتساب امضا به وی، بموجب یک گواهی معتبر مورد تأیید قرار گرفته باشد. بموجب این دستورالعمل و قانون نمونه امضای الکترونیکی، کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد، گواهی الکترونیکی که صحت صدور امضا و اصالت صادر کننده را تأیید می‌کند، برای اعتبار بخشیدن به امضا کفایت می‌کند.(۷)

ولی چنانچه حاوی شرایط مندرج در دستورالعمل شماره ۹۹/۹۳ پارلمان و شورای وزیران اتحادیه اروپا باشد، گواهی معتبر تلقی می‌شود و برای امضای الکترونیکی اثری مشابه امضای دستنویس که با شرایط و خصوصیات مشابه صادر شده، ایجاد می‌نماید. شرایط صدور گواهی، در ضمیمه یک دستورالعمل بشرح زیر مورد اشاره قرار گرفته‌است و هر گواهی معتبر باید واجد شرایط زیر باشد:

۱- اعلام اینکه گواهی صادره، یک گواهی معتبر و واجد شرایط می‌باشد؛

۲- هویت دفتر خدمات صدور گواهی و محل استقرار آن مشخص باشد؛

۳- نام امضا کننده یا نام مستعاری که با آن شناخته می‌شود؛

۴- منظور از صدور گواهی؛

۵- اطلاعات مربوط به تأیید اصالت امضا، و صحت صدور آن؛

۶- تاریخ شروع و خاتمه اعتبار گواهی صادره؛

۷- شماره شناسایی گواهی؛

۸- امضای الکترونیکی مطمئنی که متعلق به دفتر خدمات صدو رگواهی الکترونیکی‌است، ذیل گواهی صادر شود؛

۹- ذکر اینکه، گواهی صادره در چه فعالیتهایی قابل استفاده‌است، در صورت لزوم؛

۱۰- ارزش مالی تراکنش‌هایی که‌این گواهی در آنها قابل استفاده‌است، در صورت لزوم.

در صورتی که گواهی صادره‌این شرایط حداقلی را در خود جای دهد، میان طرفین معامله و اشخاص ثالثی که به امضای الکترونیکی موضوع گواهی، اطمینان می‌کنند، معتبر و قابل‌استفاده در محاکم قضایی‌است. مقررات این دستورالعمل، عیناً در بسیاری از کشورهای اروپایی نظیر بلژیک، فنلاند، دانمارک، آلمان، هلند، رومانی، سوئد، لهستان، اسپانیا، لوگزامبورگ، ایرلند، مجارستان، جمهوری چک، بلغارستان و پادشاهی متحده انگلستان، اعمال گردیده‌است.(۸)

ممـوجب ماده ۱۷ قانون امضای الکترونیکی کشور روسیه مصوب ۲۰۰۱ (Federal Law on Electronic Digital Signatures, Law of Russian Federation, 2001) نیز، امضای الکترونیکی عبارت از هر علامتی‌است که بوسیله سیستم‌های رمزنگاری تولید امضا و کلید عمومی و اختصاصی، ایجاد شده باشد و محدوده اعتبار آن، منحصر به تعاملات حقوق مدنی و فعالیت‌هایی‌است که در قانون مدنی روسیه بدان اشاره شده‌است مشروط بر اینکه صحت امضا و اصالت صادرکننده آن وفق بند یک ماده ۴ مورد تأیید مراکز رسمی صدور گواهی الکترونیکی قرار گرفته باشد. از این رو امضای الکترونیکی در این کشور، صرفاً در مورد قراردادهای حقوق خصوصی اعتبار دارد و اسنادی که باید به مقامات دولتی تسلیم شوند، بصورت الکترونیکی قابل امضا نیستند. هم‌چنین به موجب ماده ۱۸

قانون آن دسته از اسناد مبتنی بر حقوق مدنی، که نیازمند امضا و تأیید مجدد دولت یا دفاتر اسناد رسمی است، بصورت الکترونیکی قابل امضا نیستند. ملاحظه می‌شود که این کشور اعتبار کاملاً محدودی برای امضای الکترونیکی قائل است. (Baker and McKenzie,2007,p، 12)

حال آنکه در ایران و غالب کشورهای اروپایی و نیز برخی ایالتهای کشور آمریکا(۹) ارزش امضای الکترونیکی مطمئن، معادل امضای دستنویسی است که با شرایط و خصوصیات مشابه صادر شده باشد.

نتیجه:

«امضای الکترونیکی» از ارکان تجارت الکترونیکی است و ایجاد سازوکاری که بتواند، اعتبار حقوقی جهانی برای آن به ارمغان آورد، یکی از چالشهای بزرگ غالب نظام‌های حقوقی معاصر است. تصویب مقررات قانون تجارت الکترونیکی در سال ۱۳۸۲ با این رویکرد صورت پذیرفته است. به موجب این قانون برای آنکه امضای الکترونیکی واجد آثار حقوقی و صدور آن به مفهوم شناسایی هویت امضاکننده و اصالت امضا و مدرک باشد و عملی مثبت قلمداد شود، باید از یک سلسله شرایط شکلی برخوردار بوده و چون امری مبتنی بر فناوری است، از قواعد فنی خاصی نیز تبعیت نماید. هدف از وضع شرایط قانونی برای اعتبار بخشیدن به امضای الکترونیکی و بویژه تولید و صدور امضای الکترونیکی مطمئن، تضمین تمامیت، دوام و امضاپذیری اسناد الکترونیکی است. از این رویکرد، اسناد الکترونیکی که بدین نحو امضا شده‌اند، اعتباری همسان با اسناد کاغذی با امضای دستنویس دارند. هر قدر کارایی سیستم فنی که برای صدور امضای الکترونیکی استفاده شده، بیشتر باشد، تمامیت، دوام و ارتباط سند با فایلهای امضایی که برای آن ایجاد شده بیشتر است. از اینرو امضایی که وفق شروط مقرر در قانون صادر شده باشد «امضای الکترونیکی مطمئن» نام می‌گیرد و همچون امضای مسلم‌الصدورکه ذیل اسناد کاغذی درج می‌گردد، هیچگونه دعوای انکار یا تردید علیه آن مسموع نبوده و قابل انتساب به صادرکننده است. قانون تجارت الکترونیکی ایران از عبارت امضای الکترونیکی بهره جسته است تا بتواند فناوری‌های مختلفی را که در حوزه امضای الکترونیکی ابداع می‌شود، مورد استفاده قرار دهد و قانون را با مقتضیات فناوری روز منطبق نماید. مفهوم و نیز اعتبار امضای الکترونیکی، اساساً به فناوری‌هایی که برای تولید آن مورد استفاده قرار می‌گیرد، مرتبط است و قانون تنها اوصاف و شرایط معتبر بودن امضا را بیان می‌کند و فناوری خاصی را مورد اشاره قرار نمی‌دهد. تفاوت امضای الکترونیکی با امضای رقمی در این نکته نهفته است. در امضای الکترونیکی هر نماد الکترونیکی که به امضا متصل شود معتبر بوده و می‌توان از کلیه اشکال فناوری‌های الکترونیکی سطح پایین و سطح بالا برای تولید آن بهره برد. بعنوان نمونه وقتی با استفاده از قلم نوری متن

یک سند امضا می‌شود، یا در موردی که شخصی امضای مکتوب خود را در رایانه «تصویربرداری» نموده و آن را به یک نوشته «منضم» می کند، یا حتی در موردی که شخصی نام خود را ذیل یک سند الکترونیکی درج می‌کند، یک سند با امضای الکترونیکی تولید نموده‌است و لزومی به‌استفاده از فنون رمزنگاری در چنین امضایی وجود ندارد. چنین امضایی اگر چه قابل جعل است، ولی امضای الکترونیکی بااستفاده از فناوری سطح پایین تلقی می‌شود. در مقابل دو روش مبتنی بر فناوری سطح بالا نیز وجود دارد. امضای بایو متریک و امضای رقومی. بررسی مقررات قانون تجارت الکترونیکی نشان می دهد که قانونگذار با بیان ویژگیهای فنی خاص در مواد مرتبط،استفاده از امضای رقومی را دارای اعتبار معادل با امضای مسلم الصدور در فضای سنتی دانسته‌است و اگرچه اصطلاح امضای الکترونیکی در متن قانون با فراوانی معناداری تکرار شده ولی اعتبار حقوقی آن هیچگاه معادل امضای رقومی در نظر گرفته نشده‌است. لذا کاربران فضای مجازی و جامعه حقوقی برای اینکه از حمایتهای قانونی لازم بهره‌مند گردند باید متناسب با آنچه در نظام حقوقی داخلی همسو با اسناد بین المللی ترسیم شده گام بردارند.

پی نویس ها:

۱– این تعریف، نسبتاً، با تعریف مندرج در بند یک ماده ۲ دستورالعمل شماره ۹۹/۹۳ مصوب ۱۹۹۹ پارلمان و شورای وزیران اتحادیه اروپا در خصوص امضای الکترونیکی و بیشتر با ماده ۷ قانون نمونه کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد در خصوص تجارت الکترونیکی مصوب ۱۹۹۶ و بند الف ماده ۲ قانون نمونه کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد در خصوص امضای الکترونیکی مصوب ۲۰۰۱ مطابقت دارد. تجزیه و تحلیل تعاریف فوق نشان می‌دهد که امضای الکترونیکی، داده‌ای الکترونیکی است که به سایر داده‌های الکترونیکی منضم یا بطور منطقی مرتبط شده و رابطه امضا کننده را با آن داده‌ها مشخص می‌کند. ر.ک، Brazell, L., op.cit., p.p. 77 78

۲- رمزنگاری روشی برای انتقال داده‌ها بگونه‌ای است که محتوای اطلاعات مکتوم مانده و امکان دسترسی و استفاده غیرمجاز از اشخاص ثالث سلب شود. برای رمزنگاری از یک یا چند پارامتر محرمانه که به آن متغیرهای رمزنگاری گفته می‌شود، یا از یک جفت کلید استفاده می‌شود. اگر در رمزنگاری و رمز گشایی از یک کلید خصوصی استفاده شود، رمزنگاری متقارن تلقی می‌شود و اگر یک جفت کلید به نامهای عمومی و اختصاصی مورد استفاده قرار گیرد، رمزنگاری نامتقارن خواهد بود. رمزنگاری متقارن چندان اطمینان بخش نیست زیرا در هر معامله میان افراد مختلف یا حتی یکسان، باید کلید جدیدی ایجاد شود، و امنیت هر کلید فقط برای یکبار استفاده قابل تضمین است، حال آنکه در رمزنگاری نامتقارن، کلید اختصاصی اشخاص همیشه محرمانه باقی می‌ماند. برای اطلاعات بیشتر، ر.ک.،

احمدی باغکی، علیرضا، «پنهان‌سازی اطلاعات» مجله الکترونیکی مرکز اطلاعات و مدارک علمی ایران، دوره چهارم، شماره یک، قابل دسترسی در نشانی اینترنتی،

http://www.irandoc.ac.ir/data/e_j/vol4/ahmadi.htm

3- For more information, see: http://www.itsecurity.com/products

4- For more information, see:

1 UNCITRAL Model Law on Electronic Commerce, op.cit., Article 8

2 International Chamber of Commerce, 2002, "Guiding Usage for Internationally Digitally Exersized Commerce (GUIDEC), Version II, Glossary, Section IX(6)

۵- این اوصاف عیناً در بند ۲ ماده ۲ دستورالعمل شماره ۹۹/۹۳ پارلمان و شورای وزیران اتحادیه اروپا در خصوص امضای الکترونیکی و بند ۳ ماده ۶ قانون نمونه کمیسیون حقوق تجارت بین الملل سازمان ملل متحد در خصوص امضای الکترونیکی مصوب ۲۰۰۱ درج گردیده‌اند. برای اطلاعات بیشتر، ر.ک.،

1. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on Community Framework for Electronic Signatures,available at، http://europa.eu.int/cgi bin/eur lex/udl.pl?REQUEST=Seek DeliverandCOLLECTION=ojandSERVICE=eurlexandLANGUAGE=enandDOCID=2000l013p12andFORMAT=pdf

2. UNCITRAL Model Law on Electronic Signatures (2001), available at، http://www.uncitral.org/pdf/english/texts/electcom/ml elecsig e.pdf

۶- به عنوان نمونه در کشور انگلستان فروش برخی محصولات به کودکان زیر ۱۶ سال غیرقانونی تلقی می‌شود، یا معامله با اتباع کشورهای کوبا، لیبی و ایران برای تجار آمریکایی با موانع قانونی همراه بوده و موجب پیگرد قضایی خواهد بود. به علاوه تبلیغ و بازاریابی برای کودکان و نوجوانان نیز در ماده ۵۷ قانون تجارت الکترونیکی ایران مشروط اعلام شده است.

۷- این گواهی می تواند بصورت رایانامه صادر شود، با این مضمون که: «آقای الف دوست اینجانب و مورد تاییداست. کلید عمومی ایشان ضمیمه این نامه ارسال می‌شود. نامبرده در خصوص اعتبار حقوقی امضای الکترونیکی تحقیق می کند. در صورت امکان با وی همکاری نمایید.»

۸ - برای اطلاعات بیشتر و ملاحظه متن قوانین کشورهای زیر، ر.ک.،

1. Belgian Electronic Documents Act, 2000, Art. 4, p. 111
2 . Bulgarian Law on Electronic Document and Electronic Signature, 2001, Art. 4, 13, 15, `7(2), 24, 30 31, p.p. 111 112
3. Czech Republic، Electronic Signatures Act, 2000, Art. 5(2), 11, p.p. 269 280 and 113
4 . Danish Electronic Signature Law, 2000, Art. 3(1), 1, 15(2), p.p. 113 114
5. Finland، Act on Electronic Signatures, 2003, S. 2(1), 5, 17, 18, p.p. 281 292, and 115 116
6. Germany، Law Covering Framework Conditions for Electronic Signatures, Amending other Regulations, 2001, S.2(8), p.p. 293 326 and 117 119
7. Hungarian Electronic Signatures Act, 2001, Art. 2(f), 3(1), 4(2), 26(2), p.p. 119 120
8 . Irish Electronic Commerce Act, 2000, S. 9, 10(1), 13(2)(b), 14(1), 16(1), 22, 35, p.p. 327 349 and 120
9. Luxembourg Law on Electronic Commerce, 2000, Art. 6 7, 13, 18, 21, p.p. 369 402, and p.p. 123 124
10 . Dutch Electronic Signatures Act, 2003, Art. 15, p. 125
11. Poland، Act on Electronic Signature of 2001, Art. 3 7, 47, p.p. 424 453 and p.p. 125 126
12 . Romanian Law N. 455 on Electronic Signatures, 2001, Ibid, Art. 3 13, 15, 19 20, 24, 31, 36, 41 45, and p.p. 128 129
13 . Swedish Qualified Electronic Signatures Act, 2000, Ibid, S. 2, 17, 7, N. 90 49 6 60, p.p. 131 132
14 . Spain، Law on Electronic Signatures of June 2003, Art. 3 5(2), 7, 15 16, p.p. 479 501
15 . United Kingdom Electronic Communications 2000, Ibid, S. 7, 15 16, p.p. 502 530, and p.p. 132 133

۹ – به عنوان نمونه، وفق بند ۴ ماده ۴ قانون امضای الکترونیکی ایالت فلوریدای آمریکا مصوب ۱۹۹۶، امضای الکترونیکی عبارت از هر نوع حرف، نماد یا علامت است، که با استفاده از وسایل الکترونیکی و نظایر آن و با هدف ایجاد یک نوشته، تولید شده باشد و اگر امضای الکترونیکی به طرزی منطقی، به یک نوشته ضمیمه شود، آن نوشته ممضی به امضای الکترونیکی تلقی می‌گردد. این امضا از اعتباری هم سان با امضای دستی که با شرایط و خصوصیات مشابه صادر می‌شود، برخوردار است. (بند ۵) بموجب بند ۴ ماده ۲ قانون امضای الکترونیکی این ایالت، نوشته مشتمل بر هر نوع دست نوشت، نوشته چاپی، نوشته از طریق ماشین تحریر و سایر طرق و ابزار ایجاد حرف و نماد روی کاغذ، سنگ، چوب و سایر مواد است و هم چنین اطلاعاتی را که بروی واسطه‌های الکترونیکی ایجاد یا ذخیره می‌شود را نیز در بر می‌گیرد.

برای اطلاعات بیشتر، ر.ک.،

Florida Digital Signature Act of 1996, available at، http://www.complaw.com/pgp/digsiglegis.html

فهرست منابع:

1. Baker and McKenzie, 2007, “Legal Alert: Electronic Digital Signature Law” The Russia Practice, avilable at: http://www.bakernet.com/ecommerce/russia e signature alert.doc
2. Baker, S., et al, 2008 “The Limits of Trust Cryptography, Governments and Electronic Commerce”, Kluwer Law International, London
3. Brazell, L., 2009, “Electronic Signature Law and Regulations”, Sweet and Maxwell,
4. Bulgarian Law on Electronic Document and Electronic Signature, 2001
5. Charles,H. Martin, 2005,» The UNCITRAL Electronoc Contracts Convention: Will It Be Used or Avoided?», 17 Pace International Law Rev.
6. Cyber Surfers of Internet Must Beware the Sharks, The Times, 20 May 1995
7. Czech Republic: Electronic Signatures Act, 2000
8. Danish Electronic Signature Law, 2000
9. Digital Signature Act 1997, available at: http://www.mcmc.gov.my/the_law/veiwact.asp?cc =95161999andlg=eandarid=506909
10. Digital Signature Tutorial, available at: http://www.commerce.state.ut.us/digsig/tutorl.htm
11. Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on Community Framework for Electronic Signatures,available at:
http://europa.eu.int/cgi bin/eur lex/udl.pl?REQUEST=Seek DeliverandCOLLECTION=ojandSERVICE=eurlexandLANGUAGE=enandDOCID=2000l013p12andFORMAT=pdf
12. Dutch Electronic Signatures Act, 2003
13. Federal Law on Electronic Digital Signatures, Law of Russian Federation, 2001
14. Finland، Act on Electronic Signatures, 2003
15. Florida Digital Signature Act of 1996, available at: http://www.complaw.com/pgp/digsig-legis.html
16. Germany: Law Covering Framework Conditions for Electronic Signatures, Amending other Regulations, 2001
17. Hungarian Electronic Signatures Act, 2001
18. International Chamber of Commerce, 2002, “Guiding Usage for Internationally Digitally Exersized Commerce (GUIDEC), Version II, Glossary
19. Irish Electronic Commerce Act, 2000
20. Liu, S., et at, 2001, “A Practical Guide to Biometric Security Technology”, avialable at، http://www.computer.org/itpro/homepage/jan_feb/security3.htm
21. Luxembourg Law on Electronic Commerce, 2000
22. Poland، Act on Electronic Signature of 2001
23. Romanian Law N. 455 on Electronic Signatures, 2001
24. Spain، Law on Electronic Signatures of June 2003
25. Swedish Qualified Electronic Signatures Act, 2000
26. UNCITRAL Model Law on Electronic Commerce
27. UNCITRAL Model Law on Electronic Signatures (2001), available at، http://www.uncit-

ral.org/pdf/english/texts/electcom/ml elecsig e.pdf
28. United Kingdom Electronic Communications 2000
29. Vacca, J., 2002, "Biometric Security Solutions", available at، http://www.informit.com

۳۰. حبیب زاده، دکتر طاهر، « مقدمه ای بر حقوق تجارت الکترونیک» چاپ اول، ۱۳۹۰، مرکز پژوهش های مجلس شورای اسلامی.
۳۱. جعفری لنگرودی، دکتر محمد جعفر، «ترمینولوژی حقوق»، چاپ هشتم، سال ۱۳۷۶، کتابخانه گنج دانش
۳۲. جعفری لنگرودی، دکتر محمدجعفر، «مبسوط در ترمینولوژی حقوق»، جلد سوم، چاپ اول، ۱۳۷۸، انتشارات کتابخانه گنج دانش
۳۳. احمدی باغکی، علیرضا، «پنهان‌سازی اطلاعات» مجله الکترونیکی مرکز اطلاعات و مدارک علمی ایران، دوره چهارم، شماره یک، قابل دسترسی در نشانی اینترنتی،
http://www.irandoc.ac.ir/data/e_j/vol4/ahmadi.htm
۳۴. احمدی، علیرضا و همکاران، «رمزنگاری و امنیت تبادل داده»، مجله الکترونیکی مرکز اطلاعات و مدارک علمی ایران، دوره چهارم، شماره یک، قابل دسترسی در نشانی اینترنتی،
http://www.irandoc.ac.ir/data/e_j/vol4/ahmadi.htm
۳۵. فوده، پویا، «کاربرد عامل‌های متحرک در تجارت الکترونیک»، مجله الکترونیکی مرکز اطلاعات و مدارک علمی ایران، دوره چهارم، شماره یک، قابل دسترسی در نشانی اینترنتی،
http://www.irandoc.ac.ir/data/e_j/vol4/ahmadi.htm
۳۶. کی نیا، محمد، « امضای الکترونیک» چاپ اول، ۱۳۸۸، نشر میزان.

تارنما ها:

37. http://www.biometrics.org/html/standards.html
38. http://www.itsecurity.com/products
39. http://www.mycert.org.my/bill/digisgn.thml