اعتبار امضای الکترونیکی با توجه به مقررات داخلی و بین‌المللی

روح‌اله رضایی[۱]

تعریف و تاریخچه امضای الکترونیکی

مبحث اول: تعریف امضا و جایگاه آن در نظام ادله اثبات دعوی

«امضا عبارت است از نوشتن اسم یا اسم خانوادگی (یا هر دو) یا رسم علامت خاصی که نشانه هویت صاحب علامت است، در ذیل اوراق و اسناد عادی یا رسمی که متضمن وقوع معامله یا تعهد یا قرارداد یا شهادت و مانند آن‌ها است یا بعداً باید روی آن اوراق تعهد یا معامله ثبت شود (سفید مهر)».[۱] قانون مدنی از امضا تعریفی ارائه نداده است ولی مادهٔ ۱۳۰۱ همان قانون مقرر می‌دارد: ***«امضایی که در روی نوشته یا سندی باشد بر ضرر امضاکننده دلیل است»*** این ماده یکی از مهم‌ترین آثار امضا یعنی دلیل بودن سند امضاشده به نفع امضاکننده را مورد توجه قرار نداده است و فقط به‌دلیل بودن علیه صاحب امضا اشاره کرده است. بنابراین، اثر مهم امضا همان متعهد شدن صاحب آن به تمام اثرات و جنبه‌های سند یا قراردادی است که امضا شده باشد.

---

۱ . کارشناس ارشد حقوق خصوصی، دانشگاه امام صادق (ع).

به‌طور کلی، نوشته منتسب به اشخاص در صورتی قابل استناد است که امضاشده باشد. امضا، نشان از تأیید اعلام‌های مندرج در سند و پذیرش تعهدهای ناشی از آن است و پیش از آن نوشته را باید طرحی به حساب آورد که موضوع مطالعه و تدبر است و هنوز تصمیم نهایی درباره آن گرفته نشده است.[۲] بنابراین هر سندی که امضا می‌شود، در واقع، اعتبار پیدا می‌کند و می‌توان آن‌را به شخصی منتسب کرد و او را به مندرجات آن ملتزم ساخت.

اگرچه ایجاد حق و تکلیف به‌عنوان مهم‌ترین اثر امضا در اکثر اسناد مورد توجه قرار نگرفته، با این حال، می‌توان از مادۀ ۶۵ ق.ث. (مصوب ۱۳۱۰) آن را استنباط کرد. طبق این ماده «امضای ثبت سند پس از قرائت آن به توسط طرفین معامله یا وکلای آن‌ها دلیل بر رضایت آن‌ها خواهد بود» از این ماده استنباط می‌شود که عدم امضای سند ثبت شده از سوی شخص یا اشخاص ذی‌نفع یا متعهد، مفهومی جز بی‌اعتباری و فقدان هرگونه اثر حقوقی برای آن سند ندارد. طبق مادۀ ۷۰ همان قانون با ثبت سند و طی تشریفات امضا، «سندی که مطابق قوانین به ثبت رسیده رسمی است و تمام محتویات و امضاهای مندرج در آن معتبر خواهد بود مگر این‌که مجعولیت آن سند اثبات شود». پس، امضاکننده نمی‌تواند امضای خود را انکار یا در درستی محتوای سند رسمی تردید کند و فقط می‌تواند جعلیت یا بی‌اعتباری قانونی این دسته از اسناد را اثبات کند. *(مستفاد از مادۀ ۱۲۹۲ ق.م.)*

مبحث دوم: تعریف و مفهوم امضای الکترونیکی

تعاریف مختلفی از امضای الکترونیکی ارائه شده است که به برخی از آن‌ها اشاره می‌شود:

۱. طبق بند "الف" مادۀ ۲ قانون نمونه آنسیترال در باب امضای الکترونیك[۳] *(مصوب سال ۲۰۰۱)*، «امضای الکترونیك، داده‌هایی در شکل الکترونیك است که به یك داده‌پیام دیگر منضم شده و یا به‌طور منطقی به آن ضمیمه گردیده است و به‌عنوان وسیله‌ای برای شناسایی امضاکننده آن داده‌پیام و تأیید اطلاعات موجود در آن از سوی امضاکننده به‌کار گرفته شده است».

۲. دستورالعمل امضای الکترونیك اروپا نیز در تعریف امضای الکترونیکی مقرر می‌دارد: «داده‌های الکترونیك که به سایر داده‌پیام‌های الکترونیك منضم شده یا به‌نحو منطقی به آن‌ها متصل شده و به‌عنوان وسیله‌ای برای مستندسازی به‌کار می‌رود».[۴]

۳. قانون نمونه دفاتر اسناد رسمی ایالات متحده نیز امضای الکترونیکی را این‌گونه تعریف کرده است؛ «هرگونه صدا، علامت یا فرایند الکترونیك است که به مدرك الکترونیکی با لحاظ شرایط علمی ضمیمه یا با آن همسان شده و این امضا از سوی شخصی که قصد پذیرش مدارك را دارد، صورت گرفته و یا به دستور و برای او طراحی شده است» [۵]

۴. قانون نمونه آنسیترال در باب تجارت الکترونیك *(مصوب ۱۹۹۶)* نیز مقرر می‌دارد: «امضای الکترونیکی عبارت است از داده‌های الکترونیکی موجود در یك داده‌پیام منضم‌شده به آن یا داده‌های الکترونیکی که به‌صورت منطقی به یك داده‌پیام متصل هستند و از آن می‌توان برای شناسایی امضاکننده مرتبط با داده‌پیام استفاده کرد و تأیید وی در خصوص اطلاعات موجود در داده‌پیام را نشان داد». [۶]

۵. قانون تجارت الکترونیك ایران نیز که اقتباس مناسبی از قانون نمونه آنسیترال در باب تجارت الکترونیك است، در تعریف امضای الکترونیك بیان می‌کند؛ امضای الکترونیکی عبارت است از «داده‌های الکترونیك که به سایر داده‌پیام‌های الکترونیك منضم شده یا به‌نحو منطقی متصل‌شده به داده‌پیام است که برای شناسایی امضاکننده داده‌پیام مورد استفاده قرار گیرد»[۷] همان‌گونه که از تعاریف مذکور پیدا است امضای الکترونیکی به هر تأییدی اطلاق می‌شود که به‌صورت الکترونیکی ایجاد شده و ممکن است یك علامت، رمز، کلمه، عدد، یك اسم تایپ‌شده، تصویر دیجیتال یك امضای دست‌نویس و یا هر نشان الکترونیکی اثبات هویت باشد که توسط صادرکننده یا قائم‌مقام وی اتخاذ و یك قرارداد و یا هر سند دیگری ملحق شده باشد. به عبارت ساده‌تر، امضای الکترونیك یك داده است که به سایر داده‌ها منضم شده، و ارتباط امضاکننده را با داده‌هایی که به آن‌ها منضم شده،

مشخص می‌کند. باید پذیرفت که امضای الکترونیکی همانند امضای دست‌نویس دارای آثار حقوقی احراز هویت امضاکننده سند و التزام وی به مندرجات آن است.

با توجه به تعاریف فوق از امضای الکترونیکی می‌توان نتیجه گرفت که یك امضای الکترونیکی اولاً، باید بتواند محتوای سند الکترونیکی را به شخص امضاکننده منتسب سازد و ثانیاً، در صورت استفاده از این نوع امضا برای تأیید محتوای مدارك الکترونیکی، امضای الکترونیکی کارکردی همانند امضا در اسناد کاغذی خواهد داشت.

مبحث سوم: تاریخچه پیدایش امضای الکترونیکی

اولین بار کانون وکلای ایالات متحده آمریکا،[۸] در سال ۱۹۹۲م.، در خصوص مسائل حقوقی و قانونی امضا در قراردادهای الکترونیکی شروع به کار کرد و در سال ۱۹۹۵ پیش‌نویس و رهنمودهای امضای دیجیتال[۹] را که در خصوص نحوه امضا در قراردادهای الکترونیکی و زیرساخت‌های آن بود تهیه کرد.[۱۰] در همان سال اولین قانون در مورد امضای دیجیتال را تصویب کرد که در مورد ایجاد قطعیت و اعتبار قراردادهای الکترونیك و نیز فناوری‌های مربوط به رمزنگاری[۱۱] و احراز هویت و مراجع گواهی[۱۲] امضای الکترونیك بود. در سال ۱۹۹۶. آنسیترال، قانون نمونه‌ای در باب تجارت الکترونیك تدوین کرد که شامل مقرراتی در خصوص امضای الکترونیك بود. در سال ۱۹۹۷، اتاق بازرگانی بین‌المللی (ICC)[۱۳] مبادرت به صدور «راهنمای عمومی برای تجارت بین‌المللی دیجیتال مطمئن»[۱۴] کرده است. اتحادیه اروپا در سال ۱۹۹۹ «دستورالعمل امضای الکترونیك»[۱۵] را به تصویب رسانید و نهایتاً گروه کاری آنسیترال در باب تجارت الکترونیك، «قانون نمونه آنسیترال در باب امضای الکترونیك»[۱۶] را تصویب کرد تا به‌عنوان یك معیار استاندارد و رهنمون برای قانونگذاری‌های ملی مورد استفاده کشورها قرار گیرد.[۱۷]

بسیاری از کشورها، بین سال‌های ۱۹۹۶ تا ۲۰۰۱، با استفاده از مقررات بین‌المللی موجود و رهنمون‌های ارائه‌شده در خصوص امضای الکترونیکی مبادرت به قانونگذاری در این زمینه کرده‌اند. در حال حاضر می‌توان گفت امضای الکترونیکی در تمام نظام‌های

حقوقی دنیا مورد پذیرش قرار گرفته است.[۱۸]

بخش دوم

مطالعه تطبیقی جایگاه حقوقی امضای الکترونیکی

مبحث اول: جایگاه امضای الکترونیکی در مقررات بین‌المللی

گفتار اول: قوانین نمونه آنسیترال

۱. اولین سند بین‌المللی که امضای الکترونیك را مورد توجه قرار داد، قانون نمونه آنسیترال در باب تجارت الکترونیك مصوب ۱۹۹۶م. بود.[۱۹] در این قانون، امضای واجد شرایط مطمئنه الکترونیکی و فنی دارای همان آثار و ارزش اثباتی شناخته‌شده امضای سنتی است. یعنی طبق این قانون با امضای الکترونیك نیز اصالت سند و انتساب آن به امضاکننده اثبات می‌شود و وی متعهد به محتوای سند خواهد بود.[۲۰] این قانون مشتمل بر ۱۷ ماده است که مادهٔ ۷ آن به بحث امضای الکترونیك و شرایط آن اختصاص یافته است. با گسترش یافتن تجارت الکترونیك و توجه بیشتر کشورها به آن، امضای الکترونیك نیز به‌عنوان یکی از مهم‌ترین مسائل ماهوی حقوقی آن از اهمیت بیشتری برخوردار شد. از همین رو، گروه کاری تجارت الکترونیك آنسیترال در سال ۲۰۰۱ اقدام به تصویب قانون جداگانه و ویژه‌ای در مورد امضای الکترونیکی و شرایط و احکام آن کرد. این قانون از ۱۲ ماده تشکیل شده و در آن مقررات کامل و دقیقی برای امضای الکترونیکی پیش‌بینی شده است. طبق مادهٔ ۳ قانون مذکور، در صورت داشتن شرایط ایمنی به‌هیچ‌وجه نمی‌توان میان فناوری‌های گوناگون ایجاد امضا تفاوتی قائل شد. بنابراین تمام فناوری‌های مربوط معتبر و دارای آثار حقوقی یکسان خواهند بود. در این قانون، با اشاره به اصل «کارکرد یکسان»[۲۱] هرگونه تفاوت و تبعیض بین امضای دست‌نویس و امضای الکترونیك از میان برداشته شده است. تصویب این قانون اختصاصی برای امضای الکترونیك با هدف ایجاد انگیزه و تمایل در تجار به تجارت الکترونیك و نیز افزایش اطمینان به‌عنوان شرط لازم برای انجام معاملات الکترونیکی صورت گرفته است.

گفتار دوم: اتحادیه اروپا

اتحادیه اروپا نیز در این زمینه اقدام به تصویب دو دستورالعمل کرده است؛ یکی دستورالعمل تجارت الکترونیك [۲۲] و دیگری دستورالعمل امضای الکترونیکی[۲۳] است. این دستورالعمل‌ها برای دول عضو اتحادیه اروپا، لازم‌الاجرا محسوب می‌شود و چنانچه آن‌ها بخواهند در این زمینه اقدام به قانونگذاری کنند باید مفاد دستورالعمل‌های مذکور را لحاظ نمایند. طبق مادۀ ۱۹ دستورالعمل تجارت الکترونیك «دول عضو باید تضمین کنند که انعقاد قراردادهای الکترونیکی در نظام حقوقی آن‌ها مجاز باشد. دول عضو به‌ویژه باید تضمین کنند که مقررات مجری بر قراردادها، در استفاده از قراردادهای الکترونیکی منعی ایجاد نکرده و منجر به فقدان اثر یا اعتبار حقوقی این قراردادها بر مبنای تشکیل آن‌ها با وسایل الکترونیکی نشود».[۲۴]

در دستورالعمل مربوط به امضای الکترونیکی نیز ضمن تعریف امضای مذکور و شرایط فنی لازم برای آن جهت انتساب قطعی به امضاکننده و امکان تشخیص هویت وی از طریق امضا، بر همسان بودن آثار و جایگاه امضای الکترونیك با امضای دست‌نویس در نظام ادله اثبات دعوی تأکید شده است.

مقررات بین‌المللی مذکور با هدف یکسان‌سازی و یکنواخت کردن مقررات ملی سایر کشورها به تصویب رسیده‌اند. بنابراین بسیاری از قانونگذاران ملی مقررات بین‌المللی و استانداردهای ارائه‌شده از سوی سازمان‌های بین‌المللی را در رویه‌های تقنینی خویش لحاظ کرده‌اند؛ از جمله کشور ایران که قانون تجارت الکترونیك مصوب آن، اقتباس مناسبی از قانون نمونه آنسیترال است.

مبحث دوم: جایگاه امضای الکترونیکی در برخی کشورهای پیشرفته

۱. فرانسه

اگرچه دستورالعمل امضای الکترونیکی اروپا برای فرانسه هم لازم‌الاجرا است ولی قانونگذار فرانسه نیز با انجام اصلاحاتی در سال ۲۰۰۰ مفهوم امضای الکترونیکی را وارد قانون مدنی کرده است. مادۀ ۱۳۱۶ قانون مدنی فرانسه در انطباق با دستورالعمل اروپایی

امضای الکترونیکی مصوب ۱۹۹۹ اصلاح شده و امضای الکترونیکی را این‌گونه تعریف می‌کند: «در صورتی که امضای الکترونیکی نیاز باشد این امضا در عمل عبارت است از رویه مطمئنی که شناسایی رابطه امضا را با سندی که منضم به آن است تضمین می‌کند. اصل بر مطمئن بودن این رویه است مگر آنکه دلیل مخالفی در بین باشد. هنگامی که امضای الکترونیکی انجام می‌شود هویت امضاکننده و تمامیت سند را با توجه به شرایط مقرر در مصوبه شورای دولتی تضمین می‌کند»[۲۵] طبق این ماده فرض شده است که امضای الکترونیکی شرایط فنی و قانونی مقرر را دارا بوده و اثبات خلاف این امر علی‌الاصول بر دوش امضاکننده نهاده می‌شود.

۲. کانادا

کانادا در سال ۱۹۹۹ با الهام از قانون نمونه آنسیترال همان سال، «قانون متحدالشکل تجارت الکترونیك»[۲۶] را تصویب کرد که برای تمام ایالات کانادا، لازم‌الاجرا است. در این قانون امضای الکترونیکی نیز مورد توجه قرار گرفته است. طبق مادهٔ ۸ قانون یاد شده، امضای الکترونیکی در صورتی معتبر و دارای آثار حقوقی است که قابلیت‌های خاصی از قبیل مطمئن بودن، ایمن بودن و منحصر به فرد بودن را دارا باشد. بنابراین امضای الکترونیکی در صورتی که با فناوری‌های خاص ایجاد شده یا دارای اوصاف مشخصی باشد، معتبر است.[۲۷] قانون مذکور نیز برای امضاهای الکترونیکی که با رعایت تمام شرایط فنی و قانونی انجام گرفته‌اند، اعتبار یکسانی با امضاهای دست‌نویس قائل شده است.

۳. ایالات متحده آمریکا

در ایالات متحده آمریکا نیز امضای الکترونیکی همانند امضای سنتی الزام‌آور شناخته شده است. اولین قانون درباره امضای الکترونیکی در سال ۱۹۹۶ و در ایالت یوتای آمریکا به تصویب رسیده است.[۲۸] لیکن در سطح فدرال نیز قانون امضاهای الکترونیکی در تجارت داخلی و بین‌المللی[۲۹] در سال ۲۰۰۰ تصویب شده است. در این قانون، امضای الکترونیکی دارای اعتبار و هم‌عرض با امضای دست‌نویس است. مطابق مادهٔ یك قانون مذکور امضای قرارداد یا هر مدرك دیگری مربوط به معاملات الکترونیکی را نمی‌توان با استناد به هیچ

قانون، رویه یا قاعده حقوقی صرفاً به خاطر شکل الکترونیکی آن بی‌اعتبار دانست. قانون متحدالشکل یوتا نیز تصریح دارد که اگر بر طبق قانون، امضای قراردادی الزامی باشد این شرط می‌تواند با وسایل الکترونیکی که مجهز به فناوری تولید امضا هستند، محقق شود.

۴. آلمان

کشور آلمان برخلاف بیشتر کشورها که در قانون تجارت الکترونیك خود به بحث امضای الکترونیك نیز توجه می‌کنند، قانون مجزا و جداگانه‌ای در خصوص امضای الکترونیك تحت عنوان «قانون امضای الکترونیك» [۳۰] مصوب سال ۲۰۰۰، به تصویب رسانده است. در این قانون نیز همانند سایر قوانین مربوط به امضای الکترونیکی و نیز در راستای انطباق با دستورالعمل امضای الکترونیکی اروپا اصل کارکرد یکسان مورد توجه قانونگذار آلمان قرار گرفته است. یعنی امضای الکترونیك با رعایت تمام شرایط فنی و ایمنی مقرر در قانون از همان اعتبار امضای دست‌نویس برخوردار است. بنابراین داده‌پیام‌هایی که امضای الکترونیکی به آن‌ها منضم می‌شوند، معتبر و موجد آثار حقوقی هستند.

۵. انگلستان

کشور انگلستان که نظام حقوقی آن مبتنی بر کامن‌لا (حقوق عرفی) است نیز ناگزیر از قانونگذاری در خصوص تجارت الکترونیك بوده است. طبق دستورالعمل شماره ۲۰۰۰/۳۱ اتحادیه اروپا که ناظر به برخی از جنبه‌های حقوقی تجارت الکترونیك است، دولت‌های عضو موظف هستند که نظام‌های حقوقی آن‌ها تشکیل قرارداد از طریق واسطه‌های الکترونیکی و سایر مقتضیات آن را تضمین کنند. [۳۱] در همین زمینه، کشور انگلستان نیز در سال ۲۰۰۲ مبادرت به تصویب «مقررات امضاهای الکترونیك» [۳۲] کرد.

به موازات گسترش و فراگیری مبادلات الکترونیکی، موج قانونگذاری در این زمینه در سال‌های اخیر (بین ۱۹۹۶ تا ۲۰۰۱) قابل توجه بوده است. بیشتر کشورها که به بسترسازی تقنینی تجارت الکترونیك روی آوردند، یکی از مهم‌ترین موضوعاتی که پیش روی داشتند، پذیرش امضای الکترونیکی بوده است . در حال حاضر، بیشتر کشورها، این نوع امضا را

بدون هیچ تردیدی، به‌عنوان یکی از اعمال دارای آثار حقوقی همسان با امضای دستی مورد پذیرش قرار داده‌اند. [۳۳]

مبحث سوم: جایگاه امضای الکترونیکی در حقوق ایران

کشور ایران نیزدر راستای هماهنگ شدن با مقررات بین‌المللی و سایر کشورها در زمینه قانونگذاری در مورد فناوری‌های نوین ارتباطی، تاکنون اقدام به تصویب قانون تجارت الکترونیك کرده است. قانون مذکور که در واقع، قانون به رسمیت شناختن وسایل ارتباطی نوین و الکترونیك در روابط تجاری و معاملاتی افراد است، اقتباسی از قانون نمونه تجارت الکترونیك آنسیترال است که با حذف و اضافاتی از سوی شورای نگهبان در سال ۱۳۸۳ به تصویب نهایی رسیده است و در حال حاضر، مبنای قانونی تجارت الکترونیك در ایران محسوب می‌شود.

در این قانون، امضای الکترونیك مورد پذیرش قرار گرفته و برخی از شرایط و احکام آن بیان شده است. مادهٔ ۲، امضای الکترونیکی را این‌گونه تعریف کرده است: «عبارت از هر نوع علامت منضم‌شده یا به نحو منطقی متصل شده به داده‌پیام است که برای شناسایی امضاکننده داده‌پیام مورد استفاده قرار می‌گیرد». [۳۴] در این قانون از امضای الکترونیکی مطمئن [۳۵] نام برده شده است و امضای الکترونیکی مطمئن نیز طبق بند "ک" قانون مزبور، هر امضایی الکترونیکی است که شرایط مادهٔ ۱۰ را دارا باشد. مادهٔ ۱۰ قانون تجارت الکترونیك نیز مقرر می‌دارد که امضای الکترونیکی مطمئن باید دارای شرایط ذیل باشد:

الف. نسبت به امضاکننده منحصر به فرد باشد؛

ب. هویت امضاکننده داده‌پیام را معلوم نماید؛

ج. به وسیله امضاکننده و یا تحت اراده انحصاری وی صادر شده باشد؛

د. به نحوی به یك داده‌پیام متصل شود که هر تغییری در آن داده‌پیام، قابل تشخیص و کشف باشد.

مادهٔ ۷ قانون تجارت الکترونیك ایران صراحتاً امضای الکترونیکی را مورد پذیرش قرار

داده و مقرر می‌دارد؛ «هرگاه قانون وجود امضا را لازم بداند امضای الکترونیکی مکفی است». به این ترتیب، می‌بینیم که امضای الکترونیکی در نظام ادله اثبات از همان جایگاه امضای دست‌نویس برخوردار است. همان‌طور که قبلاً هم اشاره شد، قانون تجارت الکترونیك ایران به‌ویژه در آن قسمت که به امضای الکترونیکی ارتباط دارد تا حد زیادی با تقلید از دو قانون نمونه آنسیترال (قانون نمونه تجارت الکترونیك مصوب سال ۱۹۹۶م. و قانون نمونه امضای الکترونیکی مصوب سال ۲۰۰۱) به تصویب رسیده است که در بخش‌های آتی به تفصیل مورد بررسی قرار خواهد گرفت.

بخش سوم

فناوری امضای الکترونیکی

امضای الکترونیکی به‌عنوان یکی از دستاوردهای الکترونیکی مدرن از مبانی علمی و فنی خاصی پیروی می‌کند و باید گفت که امضای الکترونیکی یك پدیده فنی و الکترونیك است و به هر طریقی که صورت گیرد بی‌نیاز از مسائل فنی و تکنولوژیك نیست. نحوه انجام امضا، انواع، شرایط صحت و ایمنی، کنترل و زیرساخت‌های امضای الکترونیك و سایر فناوری‌های مربوط به آن از جمله مسائل فنی آن است که برعهده علوم رایانه‌ای و الکترونیك است. بنابراین، پرداختن به مسائل مذکور علاوه بر اینکه از حوصله و توان این یادداشت خارج است، مستلزم به‌کارگیری تعاریف و اصطلاحات علمی و پیچیده‌ای است که در تخصص علوم رایانه‌ای، الکترونیك و ریاضیات است. اما به هر حال، از آنجا که امضای الکترونیك یك تأسیس حقوقی است و بخش قابل توجهی از قوانین مربوط به مبادلات الکترونیك را به خود اختصاص داده است، آشنایی اجمالی با آن در حد کلیات ضروری به‌نظر می‌رسد.

مبحث اول: انواع امضای الکترونیکی

از زمان پیدایش فناوری امضای الکترونیك تاکنون روش‌های مختلفی در خصوص چگونگی نحوه انجام امضا از طریق الکترونیکی و با توجه به افزایش ضریب امنیت آن

معرفی و به کار گرفته شده است که مورد اشاره قرار می‌گیرد: [۳۶]

۱. کلمات عبور [۳۷]

یکی از روش‌های ساده و رایج ایجاد ایمنی و اعتبار، به‌کارگیری یك کلمه عبور منحصر به فرد با استفاده از یك شماره هویت شخصی (PIN) [۳۸] در انتهای سند است که به‌طور مخفی به آن منضم می‌شود. امنیت این روش بسیار پایین است. زیرا کلمات عبور و شماره‌های شخصی افراد به‌راحتی توسط نفوذگرها[۳۹] شناسایی و به سرقت می‌روند و ممکن است توسط آن‌ها یا دیگران مورد سوءاستفاده قرار گیرند.

۲. امضای بیت‌مپ [۴۰]

این نوع امضا، تصویر اسکن [۴۱] شده امضای دست‌نویس است که در آن ابتدا فرد به روی کاغذ امضای خود را پیاده می‌کند و سپس آن را اسکن‌کرده و می‌توان تصویر اسکن‌شده را به‌عنوان امضا به هر فایلی که خواست به‌عنوان امضای الکترونیکی منضم کند.

۳. قلم نوری [۴۲]

فناوری قلم نوری به این صورت است که هنگامی‌که فرد با این قلم و بر روی صفحه مخصوص امضای خود را پیاده می‌کند، دقیقاً همان امضا در روی صفحه مانیتور رایانه پدیدار می‌شود. یعنی امضای عادی فرد در بیرون از رایانه انجام می‌شود ولی به همان شکل، در صفحه مانیتور، نمودار می‌شود. این روش اگرچه بسیار ساده است ولی از امنیت کافی برخوردار نیست و امکان جعل آن زیاد است.

۴. امضای بیومتریك [۴۳]

این نوع امضا مبتنی بر ویژگی‌ها و معرف‌های زیست‌شناختی فرد، یعنی خصوصیات رفتاری (مثل نحوه انجام امضای دست‌نویس) و خصوصیات فیزیولوژیك (مثل اثر انگشت) است. در این روش، اگرچه ممکن است تا حد زیادی بتوان امضا را منحصر به فرد دانست ولی مشکل امضای بیومتریك این است که خصیصه‌های فیزیکی و رفتار افراد با افزایش

سن، بیماری و سایر عوامل تغییر می‌کند و به همین دلیل امضای مذکور نیز مصون از اشتباه نیست.[۴۴]

۵. امضای دیجیتال [۴۵]

امضای دیجیتال یکی از پیشرفته‌ترین و پرکاربردترین نوع از امضاهای الکترونیك است و به‌دلیل امنیت بالای آن جایگزین سایر روش‌های موجود شده و بیشتر قانونگذاران ـ از جمله قانونگذار تجارت الکترونیك ایران ـ این شیوه از امضا را پذیرفته‌اند.[۴۶] امضای دیجیتال مبتنی بر علم رمزنگاری است و از دو نوع الگوریتم[۴۷] که به نام‌های «کلید عمومی»[۴۸] و «کلید خصوصی»[۴۹] شناخته شده‌اند، استفاده می‌کند. در این قسمت با توجه به اهمیت امضای دیجیتال فناوری و زیرساخت آن مورد دقت و بررسی بیشتری قرار می‌گیرد.

مبحث دوم: زیرساخت فنی امضای دیجیتال

همان‌طور که گفته شد، امضای دیجیتال از طریق علم رمزنگاری ایجاد می‌شود و در واقع، یك فرایند رمزنگاری است و از یك جفت کلید تحت عناوین کلید خصوصی و کلید عمومی تشکیل می‌شود. بنابراین لازم است با این اصطلاحات تا حدودی آشنا شویم:

۱. رمزنگاری [۵۰]

رمزنگاری، علم کدها و رمزها است. علمی است که برای تغییر شکل دادن نوشته‌ها و اطلاعات به‌کار می‌رود. یعنی از طریق رمزنگاری می‌توان یك متن خوانا را تبدیل به متن ناخوانا و غیرقابل فهم کرد. فرایند رمزنگاری دارای دو مرحله است. مرحله اول، رمزسازی[۵۱] یعنی تبدیل یك متن ساده و عادی به یك متن رمزی است. این متن اگر در دسترس همگان هم قرار گیرد، غیرقابل فهم است. مرحله دوم، رمزگشایی[۵۲] است یعنی تبدیل متن رمزشده به یك متن عادی که قابل فهم باشد.[۵۳]

۲. عملیات ایجدسازی «خردسازی» [۵۴]

یکی از فرایندهای مهم و اساسی که در تولید امضای دیجیتال به کار می‌رود فرایند

خردسازی است. فرایند خردسازی، یک فرایند ریاضی است که بر مبنای الگوریتمی، از داده‌پیام، یک «شناسه کوتاه و فشرده»[۵۵] ایجاد می‌کند که «نتیجه خرد»[۵۶] نامیده می‌شود.

این شناسه یا به اصطلاح «نتیجه خرد» در خصوص محتوا و تمامیت سند منحصر به فرد می‌باشد. به‌طوری‌که هرگونه تغییر در داده‌پیام منجر به تغییر شناسه آن می‌گردد و قابل پیگیری است. برای درک بهتر این فرایند، یک مثال ساده می‌زنیم: تصور کنید به ازای هر کاراکتر (عدد یا حرف) در داده‌پیام با استفاده از یک تابع ریاضی، یک عدد اختصاص دهیم. اگر به ازای تک تک حروف و کاراکترهای موجود در داده‌پیام یک عدد اختصاص دهیم، مجموع اعداد به دست آمده، می‌تواند شناسه آن داده‌پیام قرار گیرد. بدیهی است در صورت هرگونه تغییر در داده‌پیام، که مستلزم تغییر حروف یا اضافه کردن حروف و اعداد دیگر باشد، شناسه داده‌پیام اصلی تغییر می‌کند. بنابراین تغییرات قابل پیگیری و کنترل هستند.[۵۷]

شاید بتوان عملیات خردسازی را شبیه حروف «ابجد» در زبان (عربی و) فارسی دانست.

در این فرایند، نرم‌افزار ایجادکننده امضای دیجیتال قادر خواهد بود بر روی مقادیر کوچک‌تری از داده‌ها عمل نماید و در عین حال، دلیل محکمی مبنی بر ارتباط دو طرفه میان پیغام اصلی و شناسه آن فراهم آورد و از این طریق به نحو مطلوبی تضمین می‌شود که از زمان امضا شدن به‌صورت دیجیتال، هیچگونه تغییری در داده‌پیام حاصل نشده است.

۳. رمزنگاری کلید عمومی[۵۸]

رمزنگاری مبتنی بر کلید عمومی یا رمزنگاری «آسیمتریك»[۵۹] از دو الگوریتم تشکیل شده است که یکی از آن‌ها برای ایجاد امضای دیجیتال و تبدیل آن به یك متن بی‌معنی استفاده می‌شود و دیگری برای تبدیل متن غیرقابل فهم به شکل اولیه آن به کار می‌رود.[۶۰] به این دو الگوریتم، اصطلاحاً «کلید» گفته می‌شود.

الگوریتم اول مخصوص شخص امضاکننده است و کلید شخصی[۶۱] نامیده می‌شود و الگوریتم دوم که برای صحت امضا و تطبیق و سنجش کلید اختصاصی به کار می‌رود، کلید عمومی[۶۲] گفته می‌شود.[۶۳] در واقع، این دو کلید از نظر ریاضی به هم مرتبط هستند.

از بین این جفت کلید، یکی برای ایجاد امضای دیجیتال و تبدیل داده‌ها به شکل نامرئی و غیرقابل فهم و کلید دیگر، جهت شناسایی امضای دیجیتال و یا برگرداندن پیغام رمزنگاری‌شده به شکل اولیه آن به کار می‌رود. تجهیزات رایانه‌ای و نرم‌افزاری که از این دو کلید استفاده می‌کنند، سیستم رمزنگاری آسیمتریك یا رمزنگاری نامتقارن نامیده می‌شود.[۶۴]

بنابراین، کلید عمومی، سرّی نیست و می‌تواند در اختیار عموم نیز قرار گیرد. در حالی که کلید خصوصی کاملاً محرمانه بود و تنها در اختیار مالك آن قرار دارد و ضروری است که این کلید پنهان باشد و کس دیگری به آن دسترسی نداشته باشد.

۴. نحوه ایجاد یك امضای دیجیتال

برای ایجاد یك امضای دیجیتال، ابتدا امضاکننده باید از طریق کلید عمومی امضای خود را رمزسازی کرده و سپس آن را ضمیمه پیام‌داده‌ای کند و برای مخاطب خویش ارسال نماید. مخاطب که اکنون پیام‌داده‌ای را به همراه امضای دیجیتال منضم‌شده به آن دریافت کرده باید امضای رمزنگاری‌شده که قابل فهم نیست از داده‌پیام‌ها جدا ساخته و از طریق کلید عمومی ارسال‌کننده (که در فهرست عمومی مرجع گواهی امضا موجود است) پیام را برای وی ارسال می‌کند تا خود ارسال کننده (ی اصل ساز) با کلید خصوصی‌اش آن را رمزگشایی کند، چنانچه نتایج یکسانی حاصل شد، یعنی همان چیزی که امضاکننده به‌عنوان امضای دیجیتال برای خود تعریف کرده بود، هویدا شد، معلوم می‌شود که اولاً امضای مذکور به نحو صحیحی از سوی امضاکننده ارسال شده و ثانیاً او نمی‌تواند ادعا کند که پیام را امضا نکرده و یا اینکه پیام تغییر یافته است.[۶۵]

بنابراین، به‌کارگیری امضای دیجیتال شامل دو فرایند است؛ مرحله اول، ایجاد امضا توسط ارسال کننده پیام توسط کلید خصوصی‌اش است و مرحله بعد نیز شامل فرایند چك کردن امضای دیجیتال از طریق مراجعه به پیام اصلی و استفاده از کلید عمومی ارسال کننده است.

در مرحله اول، نرم افزار رایانه‌ای با انجام فرایند خردسازی داده‌پیام، شناسه مرتبط با آن را تولید می‌کند که این شناسه نسبت به پیغام منحصر به فرد است. سپس با استفاده از این

شناسه و ترکیب آن با کلید خصوصی امضاکننده، یک امضای دیجیتال ایجاد می‌کند که هم نسبت به اطلاعات امضاشده و هم نسبت به کلید خصوصی که برای ایجاد امضا به کار رفته، منحصر به فرد است.

بدین ترتیب، حتی ممکن است، امضای دیجیتال به‌صورت یک جزء مستقل ذخیره یا ارسال شود؛ البته مشروط به آنکه ارتباط مستحکمی میان امضا و پیغام مربوط برقرار باشد.[۶۶]

مبحث سوم: مرجع گواهی امضای الکترونیک[۶۷]

گفتار اول: ماهیت مراجع گواهی

اگرچه استفاده از روش امضای دیجیتال، تمامیت سند، محرمانه بودن اطلاعات (در صورت لزوم) و امنیت داده‌ها تضمین می‌گردد. ولی یك مسئله هنوز باقی است و آن هم تضمین هویت امضاکننده است. از نظر حقوقی مهم‌ترین اثر امضا، اثبات رابطه سند با کسی است که امضا به او نسبت داده شده است. امضای الکترونیکی هر چند هم که از امنیت بالایی برخوردار باشد ولی قادر به تضمین هویت امضاکننده نیست و این، همان مشکل تعیین هویت در سیستم‌های باز است که طرفین یك مبادله در خصوص حقوق و تکالیف خود توافقی نکرده و همدیگر را نمی‌شناسند.[۶۸]

مکانیسم احراز و تضمین هویت در فضای سنتی از طریق ثبت اسناد در مرجع ثالثی تحت عنوان دفاتر اسناد رسمی صورت می‌گیرد که با احراز هویت امضاکنندگان سند و رعایت برخی تشریفات قانونی به اسناد، اعتبار و رسمیت می‌بخشد. در بستر مبادلات الکترونیك نیز وجود چنین مرجع ثالثی برای تعیین هویت امضاکننده ضروری است. این مرجع تحت عنوان مرجع گواهی شناخته می‌شود. زیرا از طریق صدور یك گواهی‌نامه دیجیتال هویت امضاکننده را تضمین می‌کند.

گواهی‌نامه دیجیتال یك کلید عمومی را برای اشخاص (حقیقی یا حقوقی) تعریف و تصدیق می‌کند. صدور این گواهی‌نامه‌ها توسط یك مرجع معتبر و موثق که به آن «مرجع گواهی» گویند، تأیید می‌گردد. لذا از این طریق اثبات می‌شود که کلید عمومی مذکور فقط مختص به یك شخص خاص است.[۶۹]

گفتار دوم : کارکرد ساختار کلید عمومی

شبکه مراجع گواهی و پایگاه‌های داده‌ای و ساختار عملکرد آن‌ها که تحت عنوان ساختار کلید عمومی (PKI) [۷۰] شناخته شده، به‌شرح ذیل است: [۷۱]

۱. تقاضای صدور گواهی امضا از مرجع گواهی توسط ارسال‌کننده پیام‌داده‌ای؛

۲. صدور گواهی امضا پس از احراز هویت و معرفی ارسال کننده به کلیدهای عمومی و خصوصی از سوی مرجع گواهی؛

ارسال پیام‌داده‌ای همراه با امضای دیجیتال برای مخاطب از طرف ارسال کننده؛

۴. ارسال امضا به مرجع گواهی برای تصدیق هویت امضاکننده و اطمینان از صحت آن توسط مخاطب؛

۵. بررسی صحت و سقم پیام‌داده‌ای و انتساب آن به ارسال‌کننده توسط مرجع گواهی؛

۶. ارسال گواهی صحت امضا از سوی مرجع گواهی برای مخاطب؛

۷. پاسخ مخاطب به ارسال‌کننده با یك امضای دیجیتال.

بنابراین، مرجع گواهی تضمین می‌کند که کلید عمومی موجود در فهرست مرجع (که در اختیار عموم است) به‌درستی ایجاد و اعلام شده است. زیرا هویت دارندهٔ کلید خصوصی که منطبق و مرتبط با کلید عمومی است نزد مرجع وجود دارد. در واقع، مرجع گواهی یك کلید خصوصی را به اشخاص تخصیص و آن‌را ثبت و نگهداری می‌کند و کلید مکمل آن یعنی کلید عمومی را در فهرست دارندگان کلید عمومی ثبت و نگهداری کرده و در دسترس عموم قرار می‌دهد.

بنابر آنچه گفته شد، افرادی که در ایجاد و ایمنی امضای دیجیتال مداخله می‌کنند عبارتند از: [۷۲]

۱. امضاکننده اصلی؛ شخصی است که امضای دیجیتال را برای استفاده از آن در تأیید مدرکی ایجاد می‌کند.

۲. مرجع گواهی امضای الکترونیکی؛ این مرجع مکانیسم لازم را برای ایمنی و اطمینان

امضای الکترونیکی فراهم می‌سازد. با گواهی این مرجع، امضاکننده مجاز به استناد به مدارك گواهی‌شده می‌شود و کلیدهای اختصاص‌یافته به او به نام او ذخیره شده و به شخص دیگری تعلق نمی‌گیرد.

۳. طرف اعتماد کننده؛ شخصی است که با بررسی کلید عمومی به اصالت و صحت امضای دیجیتال اعتماد کرده و آن را به‌عنوان معیاری برای تنفیذ تعهد صاحب امضا در قبال خود، می‌پذیرد. این فرد اگرچه در فرایند ایجاد و امنیت امضا نقشی ندارد ولی قبول وی از آن جهت که به امضای دیجیتال اعتبار عملی می‌بخشد، بسیار ارزشمند محسوب می‌شود. زیرا تقریباً در تمام قوانین مراجع به امضای دیجیتال به افراد این اختیار داده شده که از پذیرش امضا و مدارك الکترونیکی در روابط تجاری و مالی خود با دیگران امتناع نموده و امضای دستی و مدارك کاغذی مطالبه کنند که این امر با توجه به مسائل متعددی چون ضعف امنیت و اعتماد در فضای مجازی قابل توجیه است.

شرح وظایف و مسئولیت‌های مراجع گواهی به تفصیل در قوانین و مقررات بیان شده است.[۷۳] قوانین بین‌المللی موجود در خصوص امضای الکترونیك در مورد مقررات گواهی، ساکت‌اند و آن را به قوانین ملی واگذار کرده‌اند. قانون تجارت الکترونیك ایران نیز از مراجع گواهی تحت عنوان «دفاتر خدمات صدور گواهی الکترونیکی»[۷۴] نام برده و باب دوم خود را به آن اختصاص داده است. مادهٔ ۳۱ 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، تأیید، ابطال و به‌روز نگهداری گواهی‌های اصالت امضای الکترونیکی می‌باشد» مادهٔ ۳۲ همین قانون نیز بیان می‌کند: «آیین‌نامه‌ها و ضوابط تأسیس و شرح وظایف این دفاتر توسط سازمان (سابق) مدیریت و برنامه‌ریزی کشور و وزارتخانه‌های بازرگانی، ارتباطات و فناوری اطلاعات، امور اقتصادی و دارایی و دادگستری تهیه و به تصویب هیأت وزیران خواهد رسید». مراجع گواهی‌امضا به‌دلیل نیاز به زیرساخت‌های فنی، تجهیزات و تأسیسات شبکه‌ای پیشرفته و

استانداردهای ایمنی بالا، هنوز در ایران راه‌اندازی نشده‌اند.

بخش چهارم

مسائل حقوقی امضای الکترونیکی

اگرچه امضای الکترونیکی یك پدیده فنی و الکترونیکی و از دستاوردهای علوم رایانه‌ای است و به هر طریقی که صورت پذیرد بی‌نیاز از مسائل فنی و تکنولوژیکی نیست. لیکن امضا، یك تأسیس حقوقی است. و اینکه چه چیزی می‌تواند به‌عنوان امضای الکترونیك استفاده شود یك مسئله حقوقی است. زیرا پردازش فنی اطلاعات یا داده‌ها زمانی می‌توانند به‌عنوان امضا به کار گرفته شوند که قانون چنین اعتبار و اجازه‌ای به آن‌ها داده باشد. بنابراین، پس از اینکه علوم رایانه‌ای توانستند یك امضا از طریق الکترونیك ایجاد کرده و ایمنی آن را حداقل به اندازه امضاهای دست‌نویس تأمین کنند، آنگاه نوبت به علم حقوق می‌رسد تا در مورد مسائل حقوقی ـ قانونی آن وارد عمل گردد. بنابراین در مورد امضای الکترونیك ابتدا نگاه‌ها معطوف به جنبه‌های اجرایی، فنی و تأمین امنیت آن است و سپس نوبت به جنبه‌های قانونی و حقوقی می‌رسد. در این بخش به ماهیت حقوقی امضای الکترونیك، ارزش اثباتی و آثار حقوقی امضای الکترونیکی می‌پردازیم. در این قسمت سعی می‌شود تا موضع قانون تجارت الکترونیك ایران و قوانین مصوب آنسیترال *(قانون نمونه تجارت الکترونیك مصوب سال ۱۹۹۶ و قانون نمونه امضای الکترونیك مصوب سال ۲۰۰۱)* در قبال امضای الکترونیکی مورد بررسی قرار گیرد.

مبحث اول: ماهیت امضای الکترونیکی

تا قبل از پیدایش امضای الکترونیکی، مهر و امضای دست‌نویس برای انتساب اسناد و اعمال به اشخاص به کار گرفته می‌شد و به جز ممنوعیت استفاده از مهر در صدور چك، هر دو از کاربرد و ارزش یکسانی برخوردار هستند. در مورد چك مادهٔ ۳۱۱ ق.ت. تصریح دارد که چك باید به امضای صادر کننده برسد.[۷۵] بنابراین بسیاری از حقوقدان‌ها معتقدند که قانونگذار صدور چك را فقط از طریق امضای صادرکننده پذیرفته است و با توجه به

صراحت مادهٔ ۳۱۱ ق.ت. که از مهر نامی برده نشده است، لذا نمی‌توان در صدور چك از مهر استفاده کرد.[۷۶] زیرا اولاً، قانونگذار نمی‌خواسته افراد بی‌سواد چك صادر کنند و ثانیاً مادهٔ ۲۲۳ ق.ت. در مورد برات، علاوه بر امضا، مهر را نیز معتبر دانسته ولی در مادهٔ ۳۱۱ قانون مذکور سخنی از مهر به میان نیامده است. بنابراین، صدور چك فقط با امضا امکان‌پذیر است و این امضا هم لزوماً باید دست‌نویس باشد.[۷۷] بنابراین، طرح این بحث که امضای الکترونیکی در ردیف مهر قرار می‌گیرد یا امضای دست‌نویس، در خصوص صدور چك‌های الکترونیکی ـ به‌عنوان یکی از ارزش‌های پرداخت در قراردادهای الکترونیکی ـ اهمیت پیدا می‌کند.

برخی از حقوقدان‌ها امضای الکترونیکی را در ردیف مهر آورده‌اند.[۷۸] زیرا از نظر ماهیتی با امضای دست‌نویس تفاوت دارد و در مقام مقایسه بیشتر به مهر شباهت دارد. این دسته از حقوقدانان این‌گونه استدلال می‌کنند؛ امضای الکترونیك چیزی جز یك سری فرمول‌های ریاضی نیست که از سوی مراجع گواهی امضا تأیید و در اختیار افراد قرار می‌گیرد و اگرچه تحت عنوان امضا نام گرفته‌اند ولی چون توسط شخص ثالثی تولید و به اشخاص، اختصاص داده می‌شوند و اشخاص، فقط آن‌ها را به شکلی که هستند، مورد استفاده قرار می‌دهند؛ در تحلیل حقوقی در ردیف مهر قرار دارند.[۷۹]

طبق مادهٔ ۷ قانون تجارت الکترونیك ایران ***«هرگاه قانون، وجود امضا را لازم بداند امضای الکترونیکی مکفی است»*** یعنی امضای الکترونیکی هر ماهیتی داشته باشد (مهر، امضا یا ماهیت دیگری) از نظر قانون، جایگزین امضای دست‌نویس با آثار حقوقی مشابه شده است. بنابراین تفاوتی ندارد که در تحلیل حقوقی آن را در ردیف مهر یا امضا یا هر ماهیتی دیگری قرار دهیم. زیرا ماده مذکور صراحتاً امضای الکترونیکی را هم‌عرض امضاهای مکتوب و دست‌نویس قرار داده است. در نتیجه، تمام آثار امضای الکترونیکی همسان با امضای دست‌نویس است. ولیکن نکته‌ای که باید مورد توجه قرار گیرد این است که در خصوص چك که مقررات خاص قانون تجارت بر آن حاکم است و صدور آن نیاز به

تشریفات ویژه‌ای دارد، نمی‌توان گفت که امضای الکترونیك می‌تواند جایگزین امضای دست‌نویس گردد. اگرچه قانون تجارت وجود امضا را برای صدور چك ضروری دانسته و چك بدون امضا در واقع ارزشی ندارد اما نمی‌توان با استناد به مادۀ ۷ قانون تجارت الکترونیك ایران گفت چون این ماده صراحتاً بیان می‌کند که ***«هرگاه قانون وجود امضا را لازم بداند امضای الکترونیکی مکفی است»***. پس، چون قانون تجارت امضای چك را لازم دانسته لذا امضای الکترونیکی می‌تواند جایگزین امضای دست‌نویس در چك گردد. این امر نیاز به تصریح قانونگذار دارد. مسلماً امضای الکترونیکی فقط بر روی چك‌های الکترونیکی قابل تصور است و در حال حاضر نیز در نظام مالی و بانکی و سیستم‌های پرداخت کشور چنین چك‌هایی تعریف نشده‌اند. ولی بر فرض پیشرفت تجارت الکترونیك در ایران و فراگیر شدن آن، مسلماً، یکی از روش‌های پرداخت از طریق چك‌های الکترونیکی خواهد بود که در آن صورت قانونگذار باید در خصوص چنین چك‌هایی و وجود امضای الکترونیکی آن اقدام به وضع مقررات لازم نماید و تشریفات ویژه آن را در قوانین بیان کند. در نتیجه باید گفت در حال حاضر، امضای الکترونیکی در مورد اسناد تجاری قابل اعمال نیست و فقط در مورد اسناد تجاری الکترونیك غیر از چك و برات و سفته مبنای قانونی دارد. البته پیاده‌سازی فناوری امضای الکترونیکی و تحقق اسناد الکترونیکی نیازمند فراهم آوردن زیرساخت‌های اجرایی، فنی و مدیریتی لازم است که هنوز مقتضیات آن در ایران فراهم نشده است.

مبحث دوم: ارزش اثباتی امضای الکترونیکی

چنانچه امضای الکترونیك بخواهد همانند امضای دست‌نویس در مقام دعوی یا دفاع قابل استناد باشد باید از یك سری شرایط امضای دستی مثل منحصر به فرد بودن، قدرت تعیین هویت و عدم امکان جعل توسط دیگران برخوردار باشد. البته تأمین شرایط مذکور برای امضای الکترونیك، ناظر به مسائل فنی است و چنانچه این نوع امضا با رعایت نظام اصول علمی و مهندسی الکترونیك انجام شده باشد، همانند امضاهای دستی دارای ارزش اثباتی است و از این حیث هیچ تفاوتی با آن‌ها ندارد. امضای الکترونیك یك داده‌پیام است.

طبق مواد ۶ و ۱۲ قانون تجارت الکترونیکی، داده‌پیام‌ها دارای ارزش اثباتی هستند.[۸۰] اما باید گفت که به‌طور کلی ارزش اثباتی داده‌پیام‌ها نیز با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به کار گرفته شده، تعیین می‌شود.[۸۱] حال می‌توان گفت چنانچه داده‌پیام‌های تشکیل‌دهندهٔ امضا از تمام شرایط فنی لازم برخوردار باشند اعتبار حقوقی و جایگاه آن‌ها در نظام ادله اثبات دعوی همانند جایگاه امضاهای دست‌نویس است و می‌تواند به‌عنوان دلیل در مقام دعوی یا دفاع در محاکم مورد پذیرش قرار گیرد.

در قانون نمونه تجارت الکترونیك آنسیترال نیز داده‌پیام‌ها دارای ارزش اثباتی هستند. مادهٔ ۹ قانون مذکور مقرر می‌دارد که در رسیدگی‌های قانونی، هیچ یك از مقررات مربوط به ادله اثبات دعوی به گونه‌ای اعمال نخواهد شد که قابلیت پذیرش یك داده‌پیام به‌عنوان دلیل را صرفاً به علت داده‌پیام بودن آن‌ها نفی کند.[۸۲] مادهٔ مذکور در ادامه بیان می‌دارد که در ارزیابی ارزش اثباتی داده‌پیام، قابل اعتماد بودن روش ایجاد، ذخیره‌سازی یا مبادله آن، روش حفظ تمامیت آن، روش شناساییِ اصل‌ساز آن و هر عامل مرتبط دیگری مورد توجه قرار خواهد گرفت.

در قانون تجارت الکترونیك ایران از امضایی که تمام شرایط فنی را برخوردار است تحت عنوان «امضای الکترونیکی مطمئن»[۸۳] نام برده شده است. طبق مادهٔ ۲ قانون مذکور امضای الکترونیکی مطمئن، امضایی است که شرایط مندرج در مادهٔ ۱۰ همان قانون را داشته باشد. شرایط مادهٔ ۱۰ نیز برای امضا و سابقه الکترونیکی مطمئن این است که چنین امضایی باید:

الف. نسبت به امضاکننده منحصر به فرد باشد؛

ب. هویت امضاکننده داده‌پیام را معلوم نماید؛

ج. به‌وسیله امضاکننده و یا تحت اراده انحصاری وی صادر شده باشد؛

د. به‌نحوی به یك پیام متصل شود که هر تغییری در آن داده‌پیام، قابل تشخیص و کشف باشد.

از قوانین و مقررات مذکور نتیجه می‌شود؛ برای اینکه امضای الکترونیکی از همان اثر و جایگاه امضای دست‌نویس در نظام ادله اثبات دعوی برخوردار باشد باید از تمام شرایط مقرره و مطمئنه‌ای که قانون برای آن در نظر گرفته، برخوردار باشد. طبق مادهٔ ۱۵ قانون تجارت الکترونیك ایران[۸۴] نسبت به امضایی که با شرایط فوق ایجاد شده است نمی‌توان ادعای انکار و تردید کرد و تنها می‌توان نسبت به آن ادعای جعل کرد. بنابراین، منضم شدن امضای الکترونیکی به داده‌پیام‌ها، آن‌ها را در حکم اسناد رسمی قرار می‌دهد. ***(مستفاد از مواد ۱۴ و ۱۵ قانون تجارت الکترونیك ایران).***

بنابر آنچه گفته شد، امضای الکترونیکی هیچ تفاوتی از حیث آثار حقوقی با سایر امضاهای دست‌نویس ندارد. یعنی چنانچه امضای الکترونیك از تمام شرایط فنی لازم برخوردار باشد و ایمنی آن توسط علوم رایانه‌ای تضمین گردد، آنگاه از همان اعتبار و جایگاه امضای دست‌نویس در نظام ادله اثبات دعوی برخوردار خواهد بود و می‌تواند به‌عنوان «دلیل» در مقام دعوی یا دفاع مورد استناد قرار گیرد.

پی‌نوشت:

۱. جعفری لنگرودی، محمدجعفر، ***ترمینولوژی حقوق***، ص. ۸۱، چ. ۵، انتشارات گنج دانش، تهران، ۱۳۷۰.

۲. کاتوزیان، ناصر، ***اثبات و دلیل اثبات***، ج. ۱، ص. ۲۷۸، نشر میزان، تهران ۱۳۸۰.

3. UNCITRAL model law on electronic signature with guide to enactment 2001 , in internt : www.uncitral.org .Art 2.

4. EU Directive on Electronic Signature, Art. 2 (1) in internet : wwww.216.87.76.maros/docs/ct.esig-su-eu.html.

an electronivc signature means data in electronic form which are attached to or logically associated with other electronic ata and which serve as a method of authentication".

5. Model Notary Act, 2002, Art. 14 (7) in internet :
http://www.nationalnotary.org/UserImages/Model_Notary_Act.pdf" 14-7 Electronic Signature.

"Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with an electronic document and executed or adopted by a person with the intent to sign .."

6. Uncitral Model Law on Electronic Commerce, Art. 2 (a) op.cit"... a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and"..

۷. ***قانون تجارت الکترونیك ایران***، پیشین بند ۲.

8 American Bar Association.

9. Digital Signature Guidelines.

10. Lorna Brazell ,Electronic Signiture Law and Regulation , p4 firth edition . sweet &maxwell ,2003.
11. Cryptography.
12. Certification Authorities (CA).
13. International Chamber of Commerce.
14. General Usage for International Digitally Ensured Commerce.
15. Electronic Signature Directive.
16. Uncitral Model Law on Electronic Signature 2001 op.cit.:در پیوست ترجمه قانون فوق آمده است.
17. Lorna Brazel, Electronic Signatures Law and Regulation, p.4, Sweet & Maxwell.
18. Ibid, p.5.
19. Lorna Brazell op cit. p 4.
20. Uncitral Model Law on Electronic Commerce with Guide to Enactment, 1996, op cit. p.36.
21. Equal Treatment.
22. EU Directive on Electronic Commerce, 2000/31/EC in internet : www.dti.gov.uk/industries/ecommunications/ electronic_commerce_directive_0031ec.htm
23. EU Directive on Electronic Signature, 1999 /93/EC /official gournal L13 january .19,2000 op cit.
24. EU Directive on Electronic Commerce op cit . Art 19.
۲۵. زرکلام، ستار، «***قانون تجارت الکترونیکی و امضای الکترونیکی***»، مجموعه مقالات همایش بررسی ابعاد حقوق فناوری اطلاعات، خرداد ۱۳۸۳.
26. Uniform Electronic Commerce Act)of canada) : in internet : www. Law.u.alberta.ca/alri/alc/current/euecafin.htm.
27. Uniform Electronic Commerce Act, Art. 8 op cit.
28. UTAH Digital Signature Act, 1996 op cit .
29. Electronic Signature in Global and National Commerce Act, 2000 in internet : www.whitehouse.gov/omb/memoranda/esign-guidance.pdf.
30. Electronic Signature, Act, 2000 (og Germany) in internet: www.iid.de/iukg/vib2rcfreren.tentwufengh.sh.pdf.
۳۱. ***بند یك مادهٔ ۱۹ دستورالعمل مقرر می‌دارد:*** «دولت‌های عضو باید تضمین کنند که نظام‌های حقوقی ایشان تشکیل قرارداد از طریق وسایل الکترونیك را مجاز می‌شمارد. دول عضو به‌ویژه باید تضمین کنند که مقتضیات قانونی قابل اعمال در روند تشکیل یك قرارداد، هیچ مانعی برای انعقاد قراردادهای الکترونیك ایجاد نمی‌کند و نیز نباید به خاطر اینکه قراردادهای مذکور از طریق وسایل الکترونیك ایجاد شده‌اند، فاقد اعتبار و قابلیت اجرا تلقی گردند». 2000/31/EC
32. Electronic Signatures Regulation, 2002 of (UK) in internet : www.opsi.gov.uk/SI/si2002/20020318.htm.
۳۳. برای مطالعه بیشتر مراجعه شود به

,ornA Brazzel, op cit .,no 006 and more holly وk.towle , Houston law revieiw .e sigature , p 922 and more , in internet :http://www.houstonlawreview.org/archive/downloads/38-3_pdf/HLR38P921.pdf

۳۴. قانون تجارت الکترونیك ایران، پیشین، مادهٔ ۲، بند "ی".
35.Secure/ Enhanced/ Advanced Electronic Signature.
36. Lorna, Brazel, Electronic Signatures Law and Regulation, pp.38-39 op cit.
37. Passwords.
38. Personal Information Number

39. Hackers
40. Bitmap Signature
41. Scan
42. Light Pen
43. Biometric Signature
44. Michael Chissick, Alister Kelman, Electronic Commerce: Law and Practice, p.182, Sweet & Maxwell, London, 2002
45. Digital Signature

۴۶. قانون نمونه آنسیترال در باب امضای الکترونیك (مصوب ۲۰۰۱م) و دستورالعمل امضای الکترونیك اتحادیه اروپا (مصوب ۱۹۹۹م) نیز از همین فناوری استفاده کرده‌اند.

۴۷. الگوریتم دستورات ساده و قابل فهم کامپیوتر است که اجرای متوالی و پشت سر هم آن‌ها منجر به هدف معینی مثل حل یك مسئله می‌شود. واژه الگوریتم برگرفته از نام ریاضیدان بزرگ ایرانی یعنی خوارزمی است.

48. Public Key .
49. Private Key .
50. Cryptography .
51. Encryption .
52. Decryption .
53. Lorna Brazel, Electronic Signature Law and Regulation, p.49 .
54. hashfunction.
55. Message digest.
56. hashresalt.
57. Kurt M.Sunders , practical unternet law for business, p 36, Artech house , boston lomdon 2001.
58. Public Key Cryptography.

۵۹. رمزنگاری آسیمتریك (Asymmetric) یا نامتقارن در مقابل رمزنگاری سیمتریك (Symmetric) یا متقارن به کار برده می‌شود.

۶۰. السان، مصطفی، دوان یامچی، امین، «ماهیت رایانه‌ای و جنبه‌های حقوقی امضای دیجیتال»، مجله دیدگاه‌های حقوقی، شماره‌های ۳۰ و ۳۱، بهار ۱۳۸۳، ص. ۲۷.

61. private key .
62. public key .

۶۳. السان، پیشین، ص. ۲۸.

۶۴. زرکلام، ستار، *«قانون تجارت الکترونیکی و امضای الکترونیکی»*، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، خرداد ۱۳۸۳، ص. ۱۶۰.

65. Edward, H. Freeman, J. D “Digital Signatures and Electronic Contracts”, p.8, Technology Law Journal, No.391, 2001.

۶۶. بختیاروند، مصطفی، پیشین، ص. ۴۹.

67. Certification Authority (CA).

۶۸. زرکلام، ستار، پیشین، ص. ۱۶۱.

69. Edward, H. Freeman, J. D , op cit. ,p 4.
70. Public Key Infrastructures (PKI).
71. Michael Chissik, Alister Kelman, Electronic Commerce, op cit. p.182 .
72. Lorna Brazel, Electronic Signatures Law and Regulations, op. cit .,p.52.

۷۳. مراجعه شود به پیوست، ترجمه قانون آنسیترال در خصوص امضای الکترونیك، مواد ۷ به بعد.

74. Certification Service Provider.

۷۵. ***مادهٔ ۳۱۱ ق. ت بیان می‌کند:*** «در چك باید محل و تاریخ صدور قید شده و به امضای صادر کننده برسد ...».

۷۶. حسنی، حسن، ***حقوق تجارت،*** ص. ۵۱۷، نشر میزان، تهران ۱۳۷۸.

۷۷. درمقابل عده ای از حقوق‌دانان نیز معتقدند که بین مهرو امضای سند تجاری هم ردیفند و به رغم اینکه درمادهٔ ۳۱۱قانون تجارت اسمی از مهر برای چك آورده نشده است، از مهر در چك نیز می‌توان به جای امضا استفاده کرد . این دسته از حقوقدانان این‌گونه استدلال می‌کنند:

اولاً معتبر شناخته شدن مهر برای دریافت چك به‌موجب مادهٔ ۳۱۶ قانون تجارت، بیانگر این معنی است که صدورچك با ممهور نمودن آن به مهر دارنده حساب نیز معتبر است . مادهٔ ۳۱۶ قانون تجارت مقرر می‌دارد : "کسی که وجه چك را دریافت می‌کند، باید ظهر آنرا امضا یا مهر نماید ."

ثانیاً برات که سندی تجاری است به دستور مادهٔ ۲۲۳ قانون تجارت، وقتی به مهر برات‌دهنده ممهور است، با داشتن شرایط اساسی دیگر برای صدور آن معتبر می‌باشد، بنابراین مهر کردن اسناد تجاری به جای امضا نمودن آن موجب اعتبار اسناد مذکورخواهد بود.

ثالثاً طبق بند ۲ مادهٔ ۱۲۹۱ قانون مدنی، ثبوت مهرکردن سند مورد تکذیب یا تردید در دادگاه موجب می‌شود که سند مذبور اعتبار سند رسمی را بیابد.

رابعاً چون به‌موجب بند ا قسمت الف مادهٔ ۳ قانون عملیات بانکیِ بدون ربا مصوب ۱۳۶۲، بانك‌ها می‌توانند تحت عنوان حساب جاری به قبول سپرده مبادرت نمایند و مادهٔ ۴۷ قانون مالیات‌های مستقیم مصوب ۱۳۶۲ در بند یك " برگ قبول شرایط عمومی حساب جاری " را به‌عنوان قرارداد یا سند افتتاح حساب معتبر دانسته است و عرف معمول بانك‌ها این است که مهر ذیل برگ قبول شرایط عمومی را همانند امضا معتبردانسته و مورد عمل قرار می‌دهند، لذا مهر کردن سند، به جای امضا عرفاً در عمل معتبر شناخته می‌شود .

خامساً به‌موجب بند ۲ مادهٔ ۱۲۹۱ و ماه ۱۲۹۳ قانون مدنی و مواد ۲۲۲و ۲۲۳و ۲۲۴ قانون آیین داددسی مصوب ۱۳۷۹،اثر انگشت و مهر معتبر شناخته شده است .

بنا به مراتب چنانچه چك‌های صادره از طرف صاحبان حساب جاری که فاقد سواد هستند، به مهر ممهور شود، مهر آنان به منزله امضا است و معتبر خواهد بود.برای مطالعه بیشتر مراجعه شود به افتخار، جواد، حقوق تجارت ۳، (اسناد تجاری بانکی، خزانه، اوراق قرضه اسناد حمل و نقل) ص. ۱۷۳ انتشارات ققنوس، ۱۳۷۹.

۷۸. صادقی نشاط، امیر، ***«تحلیل حقوقی جنبه‌هایی از پرداخت الکترونیك»***، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، خرداد ۱۳۸۳ ص. ۱۷۰.

۷۹. همان.

۸۰. ***مادهٔ ۶ قانون تجارت الکترونیك ایران مقرر می‌دارد:*** «هرگاه وجود یك نوشته از نظر قانون لازم باشد داده‌پیام در حکم نوشته است ...» مادهٔ ۱۲ همان قانون نیز مقرر می‌دارد: «اسناد و ادله اثبات دعوی ممکن است به‌صورت داده‌پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان بر اساس قواعد ادله موجود،

ارزش اثباتی داده‌پیام را صرفاً به‌دلیل شکل و قالب آن رد کرد».

۸۱. ***مادهٔ ۱۳ قانون تجارت الکترونیك ایران تصریح می‌دارد:*** «به‌طور کلی، ارزش اثباتی داده‌پیام‌ها با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به کار گرفته شده با موضوع و منظور مبادله داده‌پیام تعیین می‌شود».

82. UNCITRAL model law on electronic commerce op cit. Art 9 :" (1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence: (a) on the sole ground that it is a data message; or, (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

83. Secure/ Enhanced/ Advanced Electronic Signature "

۸۴. ***مادهٔ ۱۵ قانون تجارت الکترونیك ایران مقرر می‌دارد:*** «نسبت به داده پیام مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت به داده پیام مزبور وارد و یا ثابت نمود که داده پیام مزبور به جهتی از جهات قانونی از اعتبار افتاده است».

فهرست منابع

۱ ـ فارسی

۱. اسکینی، ربیعا، ***حقوق تجارت (برات، ...)***، چ. اول، انتشارات سمت، ۱۳۷۳.

۲. افتخار، جواد، ***حقوق تجارت ۳ (اسناد تجاری بانکی، خزانه، اوراق قرضه اسناد حمل و نقل)***، انتشارات ققنوس، ۱۳۷۹.

۳. السان، مصطفی، دوان یامچی، امین، ***«ماهیت رایانه‌ای و جنبه‌های حقوقی امضای دیجیتال»***، مجله دیدگاه‌های حقوقی، شماره‌های ۳۰ و ۳۱، بهار ۱۳۸۳.

۴. آهنی، بتول، ***برقراری امنیت در قراردادهای الکترونیك***، نشریه ندای صادق، بهار و تابستان ۱۳۸۲.

۵. بختیاروند، مصطفی، ***مجموعه مقالات همایش ابعاد حقوقی فناوری اطلاعات***، ص. ۲۳۵، چ. اول، سال ۱۳۸۴.

۶. _____، ***بررسی ماهیت حقوقی امضای الکترونیك***، پایان نامه دانشگاه امام صادق (ع)، تابستان ۸۴.

۷. جعفری لنگرودی، محمدجعفر، ***ترمینولوژی حقوق***، چ ۵، انتشارات گنج دانش، تهران، ۱۳۷۰.

۸. _____، ***دایرةالمعارف علوم اسلامی***، ج ۲، تهران، انتشارات گنج دانش، ۱۳۶۰.

۹. _____، ***مکتب‌های حقوقی در حقوق اسلام***، چ. اول، کتابخانه گنج دانش، ۱۳۷۸.

۱۰. _____، ***علم آزاد در گردش ادله اثبات دعوا در حقوق اسلام***، نشریه دانشکده حقوق و علوم سیاسی، شماره ۲۲.

۱۱. زرکلام، ستار، ***امضای الکترونیك و جایگاه آن در نظالم ادله اثبات دعوی***، فصلنامه پژوهشی دانشکده علوم انسانی دانشگاه تربیت مدرس بهار ۱۳۸۲.

۱۲. _____، ***گزارش توجیهی قانون تجارت الکترونیك***، وزارت بازرگانی، سال ۱۳۸۴.

۱۳. _____، ***«قانون تجارت الکترونیکی و امضای الکترونیکی»***، مجموعه مقالات همایش بررسی ابعاد حقوق فناوری اطلاعات، خرداد ۱۳۸۳.

۱۴. صادقی نشاط، امیر، «***تحلیل حقوقی جنبه‌هایی از پرداخت الکترونیک***»، مجموعه مقالات همایش بررسی ابعاد حقوقی فناوری اطلاعات، خرداد ۱۳۸۳.

۱۵. صدرزاده، سیدمحسن، ***ادله اثبات دعوی در حقوق ایران***، مرکز نشردانشگاهی تهران، ۱۳۶۹.

۱۶. قاجارقیونلو، سیامك، ***ادله اثبات دعوی در محیط‌های دیجیتال***، چ. اول، دبیرخانه شورای انفورماتیك، سال ۱۳۷۶.

۱۷. گزارش توجیهی پیش نویش قانون تجارالکارونیك و سیاست تجارت الکترونیك جمهوری اسلامی ایران، وزارت بازرگانی، پاییز ۱۳۸۰ در اینترنت : www.iftiz.org.ir/farsi/farsi-ecgoz.htm.

۲ ـ لاتین

1- Bidgoli,Hossein, Electronic Cemmerce, Academic press, California 2002.

2-Bolgaia Electronic Signature, in internet: www.esd.bg/publications/law/law.e.htm.

3- Brazell,orna ,Electronic Signiture Law and Regulation firth edition , sweet &maxwell ,2003.

4-Canada Uniform Electronic Commerce Act, in internet :
www. Law.u.alberta.ca/alri/alc/current/euecafin.htm

5-code civil ,Dallaoz ed 2003.

6- Edward, H. Freeman, J. D “Digital Signatures and Electronic Contracts”, Technology Law Journal, 2001

Esbin B., Intenet over cable , 1999,1 th edition , newyork -7

8- EU Directive on Electronic Commerce, 2000/31/EC in internet :
www.dti.gov.uk/industries/ecommunications/

9-. EU Directive on Electronic Signature, in internet :
wwww.216.87.76.maros/docs/ct.esig-su-eu.html.

10-Germany. Electronic Signature, Act, 2000, in internet: www.iid.de/iukg/vib2rcfreren.tentwufengh.sh.pdf

11-Holly K. Towle Houston law review , E-signature , see in internet : http://www.houstonlawreview.org/archive/downloads/38-3_pdf/HLR38P921.pdf

12-Kurt M.Sunders , practical iternet law for business, Artech house , boston lomdon 2001

13-Michael Chissick, Alister Kelman, Electronic Commerce: Law and Practice, Sweet & Maxwell, London, 2002

14- Model Notary Act, 2002, in internet : http://www.nationalnotary.org/UserImages/Model_Notary_Act.pdf

electronic_commerce_directive_0031ec.htm

15- R.robinson,E-business london first edition 1999

16-- Sherif, M.H., Protocols for secure Electronic commerceashington, D.c, 1nd edition, 2000.

17- Tapper,Collin,compute law, sweet &maxwell ,2000.

18-. UK. Electronic Signatures Regulation, 2002 of in internet : www.opsi.gov.uk/SI/si2002/20020318.htm.

19-UNCITRAL model law on electronic signature with guide to enactment 2001 , in internet : www.uncitral.org.

20--UNCITRAL model law on electronic commerce with guide to enactment 1998 , in internt : www.jus/im/unelectronic.commerce.model.law.1996/doc.htm.

21-UNCITRAL Convention Providing a Uniform Law For Bills of Exchange and Promissory Notes, 1930, see in internet :
http://www.jus.uio.no/lm/bills.of.exchange.and.promissory.notes.convention.1930/doc.

22- UN Convention on contracts for the international sales of goods -1980 see in internet: www.jus.uio.no/im/un.contracts.international.sale.of.goods.convention.1980.

23- USA Electronic Signature in Global and National Commerce Act, 2000 in

internet : www.whitehouse.gov/omb/memoranda/esign-guidance.pdf.

24 - US Uniform Electronic Transaction Act (UETA) in internet : www.en.wikipedia.org.wiki/uniform-electronic-transaction-act.htm.

25-US UTAH Notarization and Authentication of Documents and Digital Signatures, in internet : http://www.code-co.com/utah/code/04/codetab.htm.

26-www.unidroit.org.

27- http://www.nic.frhttp://www.whatix.com.

28-www.fbe.uwe.ac.uk .

29-http://projects.bus.lsu.edu/independent_study/vdhing1/erp/#Why.