سال دوازدهم، شماره ۳۰، پاییز ۱۳۸۹، ویژه نامه هفته پژوهش ۱۳۸۸

اعتبار حقوقی دلیل و امضای الکترونیکی
(مرور اجمالی برخی منابع ملی و بین المللی)

دکتر غلام نبی فیضی چکاب **legalfayz@gmail.com**

استادیار دانشکده حقوق و علوم سیاسی دانشگاه علامه طباطبایی

تاریخ دریافت مقاله: ۱۳۸۹/۳/۲۲ تاریخ پذیرش نهایی: ۱۳۸۹/۸/۱۹

چکیده

اسناد و قراردادهای الکترونیکی مبتنی بر داده های الکترونیکی هستند. هنگام رسیدگی به اختلافات و حل و فصل دعاوی ناشی از این اسناد و مدارک، باید به داده ها واطلاعات مربوط به آنها مراجعه نمود. این اطلاعات و اسناد در سیستم‌های رایانه ای ذخیره و نگهداری می شوند و گاه هرگز روی کاغذ چاپ نمی شوند. آیا این اسناد را می توان به منزله دلیل به دادگاه ارائه داد ؟ ارزش اثباتی این دلایل به چه میزان است ؟ باتوجه به احتمال انکار و تردید یا ادعای جعل از سوی شخصی که دلیل علیه او ارائه شده است، احراز صحت و اصالت اسناد و انتساب آنها به صادر کننده و همچنین احراز هویت طرفین، مباحثی هستند که تعیین تکلیف آنها ضروری است.

باید توجه داشت که پذیرش نوع اسناد و دلایل الکترونیکی، به معنای ایجاد اعتبار قانونی برای تمام اسناد و اطلاعات الکترونیکی نیست، بلکه اسنادی محکمه پسند محسوب می شوند که از شرایطی که قانون برای آنها مقرر کرده، برخوردار باشند. باتوجه به ویژگی فضای رایانه ای که در آن امکان دستکاری، تغییر، نسخه برداری و حذف اطلاعات الکترونیکی فراهم است، طبیعی است که دادرس درخصوص اعتبار این اسناد با احتیاط بسیار رفتار کرده، در حالت عادی، آنها را حداکثر به منزله قرینه‌ای بر مدعا بینگارد. لذا در این نوشتار سعی شده است اعتبار ادله و امضای الکترونیکی با توجه به مقررات داخلی و بین المللی بررسی گردد.

واژه‌های کلیدی: ادله الکترونیکی، امضای الکترونیکی، امضای الکترونیکی مطمئن، دفاتر خدمات صدور گواهی الکترونیکی، قانون نمونه آنسیترال.

مقدمه

پذیرش اعتبار قراردادهای الکترونیکی فرع بر شناسایی قانونی ادله و اسناد الکترونیکی است. از سوی دیگر و در مرحله اثباتی وجود امضای الکترونیکی در فضای سایبر، لازمه اعتبار اسناد و مدارک الکترونیکی است. لذا در این نوشتار مطالب مربوطه در سه مبحث به شرح زیر ارائه می-گردد: در مبحث نخست به مسأله "پذیرش قانونی دلایل الکترونیکی" پرداخته و در مبحث دوم "شرایط اعتبار دلایل الکترونیکی" را بررسی می نماییم. در مبحث سوم امضای الکترونیکی را اجمالا" مطالعه نموده، پس از بیان پذیرش و اعتبار امضای الکترونیکی در قوانین و مقررات، به مباحث مربوط به مفهوم و انواع امضای الکترونیکی و ضوابط تحقق امضای الکترونیکی مطمئن و نیز مستندسازی این امضاها خواهیم پرداخت.

مبحث اول: پذیرش دلایل الکترونیکی در قوانین

این مبحث را در سه گفتار بررسی می کنیم. ابتدا پذیرش ادله الکترونیکی را در قوانین ایران مطالعه می کنیم(گفتار اول). سپس به بررسی موضوع در مقررات بین المللی می‌پردازیم (گفتار دوم) و در خاتمه این مبحث ارزش اثباتی دلایل الکترونیکی در حقوق ایالات متحده آمریکا را، به عنوان یکی از منابع ملی خارجی، مورد توجه قرارخواهیم داد (گفتار سوم).

گفتار اول: حقوق ایران

قانون مدنی ایران از دلیل تعریفی ارائه نداده است، ولی به موجب ماده ۱۹۴ قانون آیین دادرسی مدنی سال ۱۳۷۹: «دلیل عبارت از امری است که اصحاب دعوا برای اثبات یا دفاع از دعوا به آن استناد می نمایند». و ماده ۱۲۵۸ قانون مدنی نیز بدون ارائه تعریف دلیل، ادله اثبات دعوا را، شامل: اقرار، اسناد کتبی، شهادت، سوگند و اماره می‌داند. به نظر می‌رسد که دلایل مذکور در ماده ۱۲۵۸جنبه حصری دارند و امری که به عنوان دلیل ارائه می شود، باید مشمول تعریف یکی از ادله اثبات دعوا که در قانون آمده قرار گیرد. این ادله می‌توانند به دو شکل سنتی یا الکترونیکی عرضه شوند. فناوری های نوین اطلاعاتی و ارتباطی، از جمله کامپیوتر و اینترنت امکان ارائه دلایل مرتبط با وقایع و اعمال حقوقی در شکل های جدید، از جمله به صورت الکترونیکی را فراهم کرده-اند(دبلفون، ۱۳۸۸: ۱۷۷).

ماده ۱۲ قانون تجارت الکترونیکی ایران، اصل لزوم پذیرش دلایل الکترونیکی از سوی محاکم و ادارات را مورد تصریح قرار داده است:«اسناد و ادله اثبات ممکن است به صورت داده پیام باشد و در هیچ محکمه یا اداره دولتی نمی توان بر اساس قواعد ادله موجود، ارزش اثباتی داده پیام را صرفا" به دلیل شکل و قالب آن رد کرد.

عبارت«ادله اثبات دعوا»در این ماده، ظاهرا" به این معناست که تمامی دلایل پنجگانه موضوع ماده ۱۲۵۸ قانون مدنی چنانچه به صورت داده پیام باشند، باید مورد پذیرش قرار گیرند (نک: همان:۱۷۸-۱۸۰).

گفتار دوم: مقررات بین المللی

۱.قانون نمونه آنسیترال ۱۹۹۶.[1]

کمیسیون حقوق تجارت بین الملل سازمان ملل از سال ۱۹۸۶ تلاش خود را برای شناسایی قانونی دلیل الکترونیکی آغاز کرد و سرانجام در سال ۱۹۹۶ با تصویب قانون نمونه تجارت الکترونیکی ـ از جمله ـ اعتبار و ارزش اثباتی داده پیام‌ها را پذیرفته است. ماده ۹ این قانون زیر عنوان پذیرش و ارزش اثباتی داده پیامها مقرر می‌دارد:

"۱- در هیچ رسیدگی قضایی، هیچ یک از مقررات ادله اثبات دعوی به گونه ای اعمال نخواهد شد که ارزش اثباتی داده پیام به منزله دلیل را صرفا" به علل زیر رد کند:

الف) به دلیل داده پیام بودن آن؛ یا

ب) هرگاه داده پیام بهترین دلیلی بوده است که شخص اقامه کننده آن به طور معقول و متعارف می توانسته به دست آورد، به این دلیل که به شکل اصلی خود نیست.

۲- اطلاعاتی که به شکل داده پیام ارائه می‌شوند، دارای ارزش اثباتی خواهند بود[2]..."

---

1. UNCITRAL Model Law on Electronic Commerce، 1996; Available at :www.uncitral.org

2. **Article 9** . Admissibility and evidential weight of data messages:

(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.

هدف از وضع ماده مذکور ممانعت از رد پذیرش داده پیام، در مقابل دلیل، به صرف ماهیت الکترونیکی آن است، لیکن در بیان مقصود به‌جای استفاده از عبارت«قابلیت پذیرش» از عبارت«ارزش اثباتی»استفاده شده که تاحدی نامناسب به نظر می‌رسد، زیرا اولین تردید محاکم در مواجهه با دلیل الکترونیکی«قابل پذیرش»بودن و انطباق آن با ضوابط حاکم بر دلایل است و مسأله«ارزش اثباتی»امری ثانونی است که پس از پذیرش یک دلیل مطرح می شود. اگرشرایط پذیرش داده پیام در مقام دلیل نیز بیان می‌گردید، مناسبتر بود (آهنی، ۱۳۸۲: ۱۳۰).

گفتار سوم: حقوق خارجی

در ایالات متحده آمریکا نیز قوانین و مقررات راجع به قراردادها و ارتباطات الکترونیکی، اصل شناسایی و اعتبار حقوقی ارتباطات الکترونیکی را پذیرفته اند. آخرین قانون مدون ایالات متحده؛ یعنی‌ای ساین[1]، که با دامنه شمولی عام، مقدم بر قوانین ایالتی است، درخصوص هرگونه معامله بین ایالات، مقرر می دارد: «اثر حقوقی، اعتبار و یا قابلیت اجرایی امضای قرارداد و یا دیگر سوابق مرتبط با چنین معامله ای نباید تنها به دلیل آنکه به شکل الکترونیکی است، انکار شود.»

بند (الف) ماده ۷ قانون یوتا[2] نیز در این زمینه مقرر می‌دارد که«تأثیر قانونی یا قابلیت اجرای سند یا امضا را صرفا" به دلیل شکل الکترونیکی آن نمی‌توان رد کرد»[3]. همچنین ماده ۱۳ این قانون مقرر کرده است که«در جریان رسیدگی به دعاوی، اعتبار سند یا امضا به منزله دلیل را صرفا" به علت شکل الکترونیکی آن نمی توان رد کرد.»[4]

مبحث دوم: شرایط اعتبار دلایل الکترونیکی در قوانین

به طور کلی، پذیرفتن اسناد و دلایل الکترونیکی به منزله دلیل، منوط به ایجاد قناعت وجدان در دادرس رسیدگی کننده به دعاوی است. بنا بر این، قوانین مربوط به تجارت الکترونیکی، پذیرش

---

(2) Information in the form of a data message shall be given due evidential weight …

1. Electronic Signature in Global and National Commerce Act , U.S, 2000 -E – Sign.

2 .Uniform Electronic Transactions Act,U.S,1999 - UETA

3. **SECTION 7**. LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS.
(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

4. **SECTION 13.** ADMISSIBILITY IN EVIDENCE. In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

ارزش اثباتی معادل اسناد کاغذی برای اسناد الکترونیکی را منوط به تحقق شرایطی کرده اند. ابتدا این موضوع را در حقوق ایران بررسی می نماییم(گفتار اول). سپس شرایط لازم برای اعتبار ادله الکترونیکی را از دید منابع بین المللی مورد ملاحظه قرار خواهیم داد(گفتار دوم).

گفتار اول: حقوق ایران

مواد ۱۴ تا ۱۶ قانون تجارت الکترونیکی به ارزش اثباتی داده پیام و امضای الکترونیکی اختصاص یافته است. ماده ۱۳ این قانون که از بند ۲ ماده ۱۹ قانون نمونه آنسیترال اقتباس شده است، مقرر می‌دارد:

« به طور کلی، ارزش اثباتی داده پیام‌ها با توجه به عوامل مطمئنه، از جمله تناسب روشهای ایمنی به کار گرفته شده با موضوع و منظور مبادله داده پیام تعیین می‌شود.»

در نتیجه، تشخیص درجه ارزش اثباتی داده پیام به دادگاه واگذار شده است که اماره‌های قضایی در این باب سهم نخستین را دارند.

ماده ۱۳ اصلی را مقرر کرده است که بر اساس آن تعیین و تشخیص ارزش اثباتی داده پیام به دادرس واگذار شده است. با این حال، دادرس باید باتوجه به عوامل مطمئنه، از جمله تناسب روش های ایمنی به کار گرفته شده با موضوع و منظور مبادله داده پیام در این زمینه تصمیم بگیرد. مقنن در ماده ۱۴ و ۱۵ پا را فراتر گذاشته و برای داده پیام تحت شرایط خاص، ارزشی معادل اسناد قایل شده است. مطابق ماده ۱۴ " کلیه داده پیامهایی که به طریق مطمئن ایجاد و نگهداری شده اند، از حیث محتویات و امضای مندرج در آن، تعهدات طرفین یا طرفی که تعهد کرده و کلیه اشخاصی که قائم مقام قانونی آنان محسوب می شوند، اجرای مفاد آن و سایر آثار، در حکم اسناد معتبر و قابل استناد در مراجع قضایی و حقوقی است." و طبق ماده ۱۵ "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 اثبات نمود که داده پیام مزبور به جهتی از جهات از اعتبار افتاده است." مطالبی که در ماده ۱۵ درخصوص ارزش اثباتی امضای الکترونیکی ذکر شده است، در قانون نمونه آنسیترال و عهدنامه ۲۰۰۵ ملاحظه نمی‌شود (برای توضیح بیشتر رک: دبلفون، ۱۳۸۸: ۱۸۹- ۱۹۰).

چنانکه ملاحظه می‌شود، این دو ماده برای داده پیام مطمئن ارزشی معادل سند، قایل شده‌اند.

از جمله مسائلی که ارزش اثباتی داده پیام را تا حد اسناد رسمی بالا می برد، حفظ تمامیت داده پیام و تولید و ذخیره داده پیام به صورت مطمئن است. ماده ۱۱ قانون تجارت الکترونیکی ایران می گوید: "سابقه الکترونیکی مطمئن عبارت است از داده پیامی که با رعایت شرایط یک سیستم اطلاعاتی مطمئن ذخیره شده و به هنگام لزوم در دسترس و قابل درک است." و شرایط سیستم اطلاعاتی مطمئن در بند (ح) ماده ۲ قانون تجارت الکترونیکی ایران بدین گونه احصا شده است:

۱ـ به نحوی معقول در برابر سوء استفاده و نفوذ محفوظ باشد؛

۲ـ سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد؛

۳ـ به نحوی معقول، متناسب با اهمیت کاری که انجام می دهد، پیکربندی و سازماندهی شده باشد؛

۴ـ موافق با رویه ایمن[1] باشد.

رویه ایمن در بند (ط) ماده ۲ این قانون، چنین تعریف شده است: رویه ایمن، رویه‌ای است برای تطبیق صحت ثبت داده پیام منشا و مقصد آن با تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله محتوا یا ذخیره سازی داده پیام از یک زمان خاص. یک رویه ایمن ممکن است با استفاده از الگوریتم یا کدها ـ کلمات یا ارقام شناسایی رمزنگاری، روش‌های تصدیق یا پاسخ برگشت و یا طرق ایمن مشابه انجام شود.[2]

لذا اگر روش تطبیق صحت ثبت رعایت شود؛ به نحوی که هرگونه خطا یا تغییر در محتوا یا مبادله را مشخص کند و در برابر سوء استفاده و نفوذ محفوظ باشد و سطح معقولی از دسترسی را داشته باشد و در عین حال متناسب با اهمیت کاری اش تولید و سازماندهی شده باشد، در واقع این داده پیام تمامیتش حفظ شده است و از لحاظ ارزش اثباتی و آثار مطابق با ماده ۱۴ قانون تجارت الکترونیکی ایران همسنگ ارزش اسناد رسمی است و انکار و تردید نسبت به آن جایز نیست و فقط می توان ادعای جعلیت داده پیام مربوطه را نمود.

---

1. secure method.

۲. همان‌طور که ملاحظه می‌شود، تبیین بیشتر رویه ایمن متضمن مباحث فنی و اجرایی بوده، از حوصله این نوشتار خارج است. برای اطلاع بیشتر، رک: رضایی، علی .(۱۳۸۷). **حقوق تجارت الکترونیکی**، صص۱٤٥-۱٤٦.

گفتار دوم: مقررات بین المللی

از میان قوانین بین المللی، بند دوم ماده ۹ قانون نمونه آنسیترال معیارهایی را برای تعیین ارزش اثباتی داده پیام ارائه کرده است:

«۲- اطلاعات موجود به شکل داده پیام از ارزش اثباتی مناسب برخوردار خواهد شد. در ارزیابی ارزش اثباتی داده پیام، قابل اعتماد بودن روش ایجاد، ذخیره سازی یا مبادله آن، روش حفظ تمامیت آن، روش شناسایی اصل ساز آن و هر عامل مرتبط دیگر، مورد توجه قرار خواهد گرفت».

هر چند مواد ۸ و ۹ قانون نمونه آنسیترال ۱۹۹۶ که در بارهٔ تمامیت و غیر قابل تغییر بودن داده پیام هستند، تقریبا" مأخذ مواد پیش گفته قانون تجارت الکترونیکی ایران هستند، اما عهدنامه ۲۰۰۵ به نحو بهتری به این موضوع توجه کرده است.

در قسمت های (a) و (b) بند ۵ ماده ۹ این عهدنامه چنین قید شده است: ملاک و مناط حفظ تمامیت داده پیام، غیرقابل تغییر و کاملا" دست نخورده ماندن اطلاعات مندرجه است، در عین حال، رعایت استاندارد و ضرورتهایی که داده پیام باتوجه به آن هدف تولید شده، الزامی است. چنین داده پیامی که قابلیت دسترسی بعدی را دارد، به عنوان سند نوشته در دادگاهها به کار گرفته خواهد شد (شفقت،۱۳۸۶: ۳۳).

مبحث سوم: امضای الکترونیکی

آنچه درباره دلایل الکترونیکی گفته شد، عمدتا" درباره امضای الکترونیکی صادق است. با این حال باتوجه به کارکرد متفاوت امضای الکترونیکی در مقایسه با سایر داده پیام های متضمن دلیل و نیز نحوه ایجاد و مستند سازی آن؛ از یک سو اصل پذیرش امضای الکترونیکی(گفتار اول) و از سوی دیگر، مفهوم و انواع امضای الکترونیکی(گفتارهای دوم وسوم) و سرانجام شیوهٔ مستند سازی امضای الکترونیکی(گفتارچهارم) نیاز به بررسی جداگانه دارد.

گفتار اول: پذیرش امضای الکترونیکی در قوانین

به موازات گسترش و فراگیری مبادلات الکترونیکی، موج قانونگذاری در این زمینه نیز در سالهای بین ۱۹۹۶ تا ۲۰۰۱ میلادی قابل توجه بوده است. بیشتر کشورها که به بستر سازی تقنینی تجارت الکترونیکی روی آوردند، یکی از مهمترین موضوعهایی که پیش رو داشتند، پذیرش امضای

الکترونیکی بود. در حال حاضر، بیشتر این کشورها این نوع امضا را بدون هیچ تردیدی به عنوان یکی از اعمال دارای آثار حقوقی همسان با امضای دستی پذیرفته‌اند؛ به‌طوری‌که در برخی از کشورها حتی قوانین مستقلی برای امضای الکترونیکی وضع شده است[۱] (اکبری، ۱۳۸۷: ۷۶).

۱) قانون تجارت الکترونیکی ایران:

در حقوق ایران امضای الکترونیکی به رسمیت شناخته شده، لیکن هنوز قانون مستقلی برای آن وضع نشده است. قانون تجارت الکترونیکی مصوب ۱۳۸۲ در مواد متعدد به امضای الکترونیکی تصریح نموده است. با توجه به بندهای "ی" و"ک" ماده ۲ و مادتین ۷ و ۱۰ این قانون، تردیدی دراعتبار امضای الکترونیکی وجود ندارد. طبق ماده ۷ مرقوم:"هرگاه قانون وجود امضا را لازم بداند، امضای الکترونیکی مکفی است." درماده ۱۰ این قانون نیز شرایط لازم برای امضای الکترونیکی مطمئن احصا گردیده است. این قانون تا حدود زیادی با تقلید از دو قانون نمونه آنسیترال ۱۹۹۶ و ۲۰۰۱ میلادی به تصویب رسیده است. در این مورد متعاقبا" توضیحات بیشتری ارائه خواهد شد.

۲) مقررات بین المللی:

الف-قانون نمونه آنسیترال ۲۰۰۱[2]:

ماده ۳ آنسیترال ۲۰۰۱، زیر عنوان برخورد یکسان با فناوری های مربوط به امضا بیان می دارد: هیچ بخشی از این قانون، جز ماده ۵، به صورتی اعمال نخواهد شد که یک روش ایجاد امضاهای الکترونیکی را که شرایط ماده (۱) ۶ را داشته یا به طریق دیگری شرایط قانونی قابل اعمال را دارد، حذف، محدود یا فاقد اثر قانونی کند[۳].

---

۱. در این رابطه از جمله می توان به فرمان شماره ۲۷۲-۲۰۰۱ مصوب ۳۰ مارس ۲۰۰۱ در فرانسه به منظور اجرای بند ٤ ماده ۱۳۱٦ ق.م در ارتباط با امضای الکترونیک و تصویب اولین قانون امضای دیجیتال در ایالات یوتای آمریکا در سال ۱۹۹۵ و تصویب قانون امضای دیجیتال مالزی در سال ۱۹۹۷ و غیره اشاره نمود.

2 . UNCITRAL Model Law on Electronic Signatures (2001) ,

Available at : www.uncitral.org .

3. **Article 3** . Equal treatment of signature technologies

Nothing in this Law , except article 5 , shall be applied so as to exclude , restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in article 6 , paragraph I , or otherwise meets the requirements of applicable law .

بند۱ماده۶ مقرر می‌دارد: در مواردی که قانون امضای شخصی را لازم می‌داند، وجود امضا در ارتباط با یک داده پیام هنگامی محقق خواهد شد که امضای الکترونیکی به کار رفته باتوجه به اوضاع و احوال برای هدفی که داده پیام به خاطر آن ایجاد یا منتقل شده است، به اندازه کافی قابل اعتماد باشد[1].

ب-عهدنامه ۲۰۰۵[2]:

بند ۳ ماده ۹ عهدنامه ۲۰۰۵ امضای الکترونیکی را در ارتباطات الکترونیکی به شرط تحقق شرایطی که در ادامه این بند ذکر می نماید، به رسمیت شناخته است. بند ۳ ماده ۹ مقرر داشته است:«در مواردی که قانون مقرر می دارد که ارتباط یا قرارداد باید توسط شخص امضا شود یا آثار فقدان امضا را بیان می کند، این شرط از طریق ارتباط الکترونیکی محقق می شود، اگر:...»

۳) حقوق خارجی:

الف- دستورالعمل تجارت الکترونیکی اروپا[3]

در این دستورالعمل، صراحتا" به مسأله امضای الکترونیکی پرداخته نشده است، اما تلویحا" از ماده ۹ آن می توان چنین استنباط نمود که دولتهای عضو مجاز نیستند، استفاده از نوشته و امضای سنتی (کاغذی) را برای انعقاد قراردادها اجباری نمایند؛هر چند که جواز استفاده از مکتوب و امضای الکترونیکی، در این دستورالعمل، به طور مطلق قابل اجرا نیست و درعمل، انتقال اموال غیر منقول، قراردادهای منعقد شده با دخالت محاکم، مقامات عمومی یا دفاتر اسناد رسمی، قرارداد کفالت و

1. **Article 6** . compliance with a requirement for a signature

(1) where the law requires a signature of a person , that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated , in the light of all the circumstances , including any relevant agreement .

2.United Nations Convention on the Use of Electronic Communications in International Contracts , Adopted by the General Assembly on 23 November 2005 . Available at: www.uncitral.org

3. Directive 2000/31/ EC of the European Parliament and of the Council of June 2000 on Certain Electronic Commerce .
Available at : www. europa.oeu.int

قراردادهای مشمول حقوق خانواده، از جمله موارد خارج از عموم ماده ۹ هستند(هولتمارک رامبرگ،۱۳۸۵: ۱۷۲).

متن ماده ۹ بدین شرح است: دولتهای عضو باید جواز انعقاد قرارداد الکترونیکی را در نظام حقوقیشان تضمین کنند، به ویژه اینکه مقررات جاری بر قراردادها، در استفاده از قراردادهای الکترونیکی منعی ایجاد نکرده، به فقدان اثر یا اعتبار حقوقی این قراردادها بر مبنای تشکیل آنها با وسایل الکترونیکی منجر نشود.

گفتار دوم: مفهوم امضای الکترونیکی

۱) امضای الکترونیکی در قوانین:

هر چند بسیاری از نظامهای حقوقی تعریف مشخصی از امضا ارائه نمی کنند، لیکن اساسا" مشخصات ارائه شده برای امضای سنتی در این نظامها وجود یک نوشته را ضروری می‌داند. قانون مدنی ایران در ماده ۱۳۰۱ خود بدون تعریف امضا مقرر می دارد: «امضایی که روی نوشته یا سندی باشد، بر ضرر امضا کننده دلیل است». از سوی دیگر، مطابق تعریف برخی از حقوقدانان، امضا عبارت است از نوشتن نام یا نام خانوادگی یا هر دو یا ترسیم علامت خاصی که نشانه هویت صاحب علامت است در زیر اوراق و سندهای عادی یا رسمی متضمن وقوع معامله، تعهد، اقرار، گواهی و مانند آنها، یا اینکه بعدها باید روی آن اوراق تعهد یا معامله‌ای ثبت شود (سفید مهر)(زرکلام، ۱۳۸۴: ۲۸۸).

در حقوق فرانسه، آمریکا و انگلیس نیز تعریف مشابهی از امضا ارائه شده است، ولی در فضای الکترونیکی که نوشته ها تجسم بیرونی و مادی ندارند و تبادل اطلاعات در محیطی مجازی صورت می گیرد، تجدید نظر در مفهوم امضا نیز ضرورت خواهد داشت. در این مفهوم، یک رمز، پیام یا هر روش غیر مادی می تواند در شرایطی دارای ارزش اثباتی امضا به مفهوم سنتی آن باشد. امضای الکترونیکی به مفهوم عام کلمه عبارت است از یک رمز مستقل و محرمانه که به وسیله آن تعیین هویت فرستنده و الحاق او به سندی که محتوای داده را تشکیل می دهد، ممکن می‌شود(همانجا).

بحث امضای الکترونیکی در سطح بین المللی، نخستین بار در ماده ۷ قانون نمونه آنسیترال ۱۹۹۶ مطرح گردید. در این ماده، امضای واجد شرایط الکترونیکی دارای همان آثار و ارزش اثباتی امضای سنتی شناخته شد. بنابر گزارش کار گروه تجارت الکترونیکی آنسیترال، با امضای الکترونیکی نیز، اصالت سند و انتساب آن به امضا کننده اثبات می‌شود و وی متعهد به محتوای

سند، خواهد بود (Anjanette H.Raymond,2006:11). اهمیت موضوع امضا در تجارت الکترونیکی سبب شد تا آنسیترال در سال ۲۰۰۱، قانون نمونه جداگانه‌ای را درباره امضاهای الکترونیکی، در ۱۲ ماده تصویب کند.

از امضای الکترونیکی به مفهوم اخص، تعاریف متعددی شده است که به بررسی برخی از آنها خواهیم پرداخت، اما پس از آشنایی با مفهوم امضای الکترونیکی، این سؤال مطرح می‌شود که آیا صرف هر امضایی در محیط الکترونیکی، معتبر تلقی شده و یا ضوابط و معیارهایی در این خصوص باید مراعات گردد؟ لذا پس از بیان مفهوم امضای الکترونیکی در قوانین مختلف، انواع امضا و در واقع، معیارهای لازم برای اعتبار امضاهای الکترونیکی در آن قانون هم بیان خواهد شد.

الف ـ قانون تجارت الکترونیکی ایران

بند (ی) ماده ۲ قانون تجارت الکترونیکی کشورمان در مفهوم امضای الکترونیکی بیان می‌دارد:

« امضای الکترونیکی عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده پیام است که برای شناسایی امضا کننده داده پیام مورد استفاده قرار می گیرد».

طبق آنچه در متن قانون تجارت الکترونیکی کشورمان نیز پذیرفته شده، تعریف فوق، تعریف امضای الکترونیکی«ساده»یا«عادی»است و نوع دیگر امضا، امضای الکترونیکی «مطمئن»است که مطابق ماده ۱۰ همین قانون به شرح زیر معرفی شده است:

امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد:

الف) نسبت به امضا کننده منحصر به فرد باشد؛

ب) هویت امضا کننده داده پیام را معلوم نماید؛

ج) به وسیله امضا کننده و یا تحت اراده انحصاری وی صادر شده باشد؛

د) به نحوی به یک داده پیام متصل شود که هر تغییری در آن داده پیام قابل تشخیص و کشف باشد».

«ملاحظه می شود که به موجب این سند، برای اینکه یک امضای الکترونیکی مطمئن تلقی شود، باید از چهار خصوصیت برخوردار باشد:

نخست آنکه این امضا باید نسبت به امضا کننده، منحصر به فرد باشد. با پیش بینی این شرط، قانونگذار جنبه اسنادی امضای الکترونکی را مد نظر داشته که می تواند به عنوان مدرکی علیه و یا له امضا کننده، استفاده شود. تعیین هویت امضا کننده نیز یکی دیگر از شرایط امضای الکترونیکی

است که در بند ب و به عنوان شرط دوم، مورد توجه قرار گرفته است. بدیهی است که اساسی‌ترین کارکرد امضا همین است. صدور از طرف امضا کننده و یا تحت اراده انحصاری وی، شرط سومی است که ماده ۱۰ به آن اشاره کرده است، و در نهایت، اتصال به داده پیام به نحوی که هرگونه تغییری قابل کشف باشد، به عنوان شرط چهارم ذکر شده است» (زرکلام،۱۳۸۴: ۱۵۴).

با در نظر گرفتن این ماده و ماده ۷ که ذکر آن گذشت، یکی دیگر از نقایص قانون تجارت الکترونیکی کشورمان رخ می نماید، زیرا در ماده ۷، قانونگذار، با آوردن عبارت مطلق«امضای الکترونیکی»مبادرت به بیان این قاعده نموده است که در مواردی که قانون، امضا را الزامی بداند، امضای الکترونیکی، مکفی است. بنابراین، باتوجه به مقید نبودن امضای الکترونیکی، چنین استنباط می شود که حتی امضای الکترونیکی ساده و بدون دارا بودن شرایط مقرر در ماده ۱۰ همین قانون، کارکردی همسان با امضای دستی در محیط واقعی را دارد، در حالی‌که چنین نیست و اطلاق موجود در ماده ۷، باتوجه به ماده ۱۰ نفی شده است.

ب ـ مقررات بین المللی

۱. قانون نمونه آنسیترال ۱۹۹۶

ماده ۷ قانون نمونه آنسیترال ۱۹۹۶ بدون پرداختن به تعریف امضای الکترونیکی در مورد شرایط پذیرش امضای الکترونیکی اعلام می دارد:

«۱. چنانچه قانون امضای برخی اشخاص را ضروری بداند، این ضرورت از طریق داده پیام تأمین می شود، اگر:

الف) چنانچه شیوه‌ای که برای تعیین هویت شخص مورد نظر به کار گرفته شده، به گونه‌ای باشد که این شخص اطلاعات مندرج در داده پیام را تأیید کند؛

ب) اگر اطمینان حاصل شود این شیوه باتوجه به موضوعی که داده پیام برای آن ایجاد شده یا انتقال یافته، با در نظر گرفتن تمامی اوضاع و احوال، از جمله هرگونه توافق در این زمینه، کفایت می‌کند.

۲. بند (۱) زمانی اعمال می‌شود که ضرورت مورد نظر یک تعهد باشد و یا اینکه قانون برای فقدان امضا آثاری بشناسد».

۲. قانون نمونه آنسیترال ۲۰۰۱

در ماده ۲ قانون نمونه آنسیترال ۲۰۰۱، زیر عنوان تعاریف چنین آمده است: "در این قانون:

الف) امضای الکترونیکی عبارت است از داده های الکترونیکی موجود در یک داده پیام، منضم شده به آن یا داده های الکترونیکی که به صورت منطقی به یک داده پیام متصلند و از آن می توان برای شناسایی امضا کننده داده پیام استفاده کرد و تأیید وی درخصوص اطلاعات موجود در داده پیام را نشان داد."[1] و در ماده۶ ذیل عنوان رعایت شرط وجود امضا بیان می‌دارد:

۱. در مواردی که قانون امضای شخصی را لازم می‌داند، وجود امضا در ارتباط با یک داده پیام هنگامی محقق خواهد شد که امضای الکترونیکی به کار رفته باتوجه به اوضاع و احوال برای هدفی که داده پیام به خاطر آن ایجاد یا منتقل شده است، به اندازه کافی قابل اعتماد باشد.

۲. صرف نظر از این که شرط مذکور به شکل یک تکلیف قانونی باشد یا آنکه قانون صرفا" عواقبی را برای نبود امضا پیش بینی کرده باشد، پاراگراف ۱ اعمال خواهد شد.

۳. زمانی امضای الکترونیکی برای تحقق شرط مورد اشاره در پاراگراف۱ قابل اعتماد خواهد بود که:

الف) داده های تشکیل دهنده امضا تحت شرایط به کارگیری آنها به امضا کننده مرتبط باشد.

ب) داده‌های تشکیل دهنده امضا، در زمان امضا کردن، صرفا" تحت کنترل امضا کننده باشد، نه شخص دیگر؛

ج) هرگونه تغییر درخصوص امضای الکترونیکی که پس از امضا کردن ایجاد شده است، قابل کشف باشد؛

د) در مواردی که هدف از شرط قانونی وجود امضای الکترونیکی، تضمین تمامیت اطلاعاتی است که امضا با آن مرتبط است، هرگونه تغییر ایجاد شده در اطلاعات مذکور پس از امضا کردن قابل کشف باشد.[2]

---

1. **Article 2**. Definitions
For the purposes of this Law:
(a) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message

2. **Article 6.** Compliance with a requirement for a signature**:**
(1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or

۳. عهدنامه ۲۰۰۵

این عهدنامه بدون ارائه تعریفی از امضای الکترونیکی در بند ۳ ماده ۹ خود، به منظور تحقق شرایط قانونی امضا، از طریق ارتباط الکترونیکی، تصریح نموده است:

"در مواردی که قانون مقرر می‌دارد که ارتباط یا قرارداد باید توسط شخصی امضا شود یا آثار فقدان امضا را بیان می کند، این شرط از طریق ارتباط الکترونیکی محقق می‌شود، اگر:

الف) ارتباط الکترونیکی، متضمن روشی باشد که برای تعیین هویت طرف و معلوم کردن قصد او درخصوص اطلاعات، به‌کار می‌رود؛

ب) روشی که به‌کار گرفته شده، یا:

۱. برای هدفی که ارتباط الکترونیکی، برای آن تولید یا اعلام شده از حیث جمیع شرایط، از جمله هرگونه توافق مربوطه، مطمئن و مناسب باشد؛ یا:

۲. در عمل اثبات شده باشد که کارکردهای موصوف در بند (الف) فوق را به تنهایی یا به همراه دلیل دیگر دارا است".[1]

---

communicated, in the light of all the circumstances, including any relevant agreement.

2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:

(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;

(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

(d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

قانون نمونه آنسیترال درخصوص امضاهای الکترونیکی .(۲۰۰۱). ترجمه مصطفی بختیاروند، **خبرنامه انفورماتیک**، تهران، ش ۸۸، مهر ۱۳۸۲: ٤٦ ـ ٤٧).

1. **Article 9**

From requirements:

3. Where the law requires that a communication or a contract should be signed by a party , or provides consequences for the absence of a signature , that requirement is met in relation to an electronic communication if :

این مقرره که بیان می دارد چنین ارتباطات الکترونیکی باید به درستی و با روش هـایی مطمـئن، هویت طرفین قرارداد را شناسایی کند، شبیه ماده ۷ (۱) قانون نمونه ۱۹۹۶ آنسیترال اسـت. در پـیش نویس عهدنامه، ماده ۹ این‌گونه تنظیم شده بود کـه عـلاوه بـر اسـتفاده از روش مطمـئن، بـه منظـور تحقق امضا، امضا کننده نیز باید آن ارتباط را تأیید می کرد کـه در جریـان تـصویب نهـایی از مـتن عهدنامه حذف گردید و بدین گونه تغییر یافت که تنها باید بر«قصد شخص در ارتباط بـا»اطلاعـاتی که در ارتباطات الکترونیکی مندرج است، دلالت نماید.

این بند که برگرفته از ماده ۷ قانون نمونه ۱۹۹۶ اسـت، شـرایط عمـومی لازم را کـه بـه موجـب آنها، ارتباط الکترونیکی، تمامی ارزش و اعتبار یک امضای دست نویس را داراست، بیان می‌کند و بر دو کارکرد اصلی امضا، تأکید دارد:

یکی آنکه، امضای الکترونیکی، باید هویـت اصـل سـاز ارتبـاط الکترونیکـی را مـشخص کنـد؛ دیگر آنکه، تأیید کند که اصل ساز، محتوای سند را پذیرفته است، یا به بیان دیگر، این داده، توسـط همان اصل ساز، امضا شده است.

بند ب نیز روش قابل انعطافی را پذیرفته که به موجب آن، احراز هویت امضا کننده و انتـساب امـضا بـه وی، باید به موجب روشی صورت گیرد که قابل اعتماد ومطمئن بوده، برای هدفی که ارتباط برای آن، تولید یـا ابـلاغ شده، مناسب باشد. لذا از منظر عهدنامه، در مواردی که قانون، امضا را شرط تحقق رابطه یا قرارداد می داند، ارتباط الکترونیکی این امر را برآورده می کند؛ مشروط بر آنکه، امضا، هویت و قـصد اصـل سـاز را مـشخص نمـوده و روشی که برای امضا، به‌کار گرفته شده، باتوجه به توافق طـرفین و یـا اوضـاع و احـوال قـضیه، مطمـئن و مناسـب باشد(رضایی،۱۳۷۸: ۱۴۷-۱۴۸).

ج) حقوق خارجی

۱. قانون متحدالشکل معاملات الکترونیکی یوتا (ایالات متحده امریکا)[1]

(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication ; and

(b) The method used is rather :

(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated , in the light of all the circumstances , including any relevant agreement ; or

(ii) Proven in fact to have fulfilled the functions described in subparagraph (a) above , by itself or together with further evidence .

1. Uniform Electronic Transactions Act,U.S,1999 - UETA

در حقوق امریکا نیز، یوتا با امضای الکترونیکی به‌طور تشریفاتی برخورد نکرده است.[۱] و تصریح دارد که اگر به موجب قانون، امضای قراردادی الزامی باشد، این شرط شکلی می تواند با وسایل الکترونیکی مجهز به فناوری تولید امضا محقق شود؛ مشروط به اینکه قصد امضا محرز باشد.»(هولتمارگ رامبرگ، ۱۳۸۵ :۱۶۶)چنانکه پیشتر اشاره شد، در بخش ۷ (د) یوتا چنین آمده است:«اگر قانون در موردی، امضا را لازم بداند، امضای الکترونیکی حایز شرایط قانونی است.»[۲]

و بخش ۸ (۲) بیان می دارد:«امضای الکترونیکی به معنای صدای الکترونیکی، رمز یا فرایندی است که به یک مدرک، الصاق یا به طور منطقی با آن همسان شده و این الصاق یا همسانی از سوی شخصی با قصد امضای آن مدرک انجام گرفته است.»

«می‌توان گفت در مقایسه با دستورالعمل تجارت الکترونیکی و دستورالعمل امضاهای الکترونیکی اروپا، یوتا با ارائه معیار«قصد امضا»، گامی فراتر برداشته است.

دلیل این امر، تفسیر موسع قانون متحدالشکل تجاری از مفهوم امضاست؛ به گونه ای که حروف چینی ماشینی و شیوه علامت گذاری را که امکان دارد به اندازه امضاهای دستی قابل اعتماد نباشد، دربر می‌گیرد.

نکته مهم دیگر در یوتا این است که شرکت ها و مؤسسات را مجاز ساخته تا باتوجه به اوضاع و احوال، تصدیق یا ثبت امضاهای الکترونیکی را شرط پذیرش آن بدانند. اعطای این اختیار، به ویژه از لحاظ کاهش مخاطرات تجاری، دارای اهمیت فوق العاده‌ای است»(همانجا)؛ ضمن اینکه بر اساس تأکید یوتا بر قصد امضا، شخصی که امکان انعقاد قرارداد را در یک پایگاه اینترنتی فراهم می‌سازد، مکلف است از شیوه غیر مبهمی در پایگاهش استفاده کرده، طرف مقابل را که با کلیک بر روی دکمه‌ای خاص یا وارد کردن رمز عبور یا اجرای امضای دیجیتالی، خود را متعهد و ملتزم می

---

۱. بررسی قانون ای ساین ایالات متحده آمریکا نیز نشان می دهد که همچون یوتا، این قانون نیز معیار قصد امضا را برای اعتبار امضاهای الکترونیکی مطرح نموده است(به نقل از علی رضایی، پیشین: ۱۵۲).

2. **SECTION 7**. LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS.
(d) If a law requires a signature, an electronic signature satisfies the law.
شایان ذکر است که بخش سوم یوتا، شرط مکتوب بودن و داشتن امضای الکترونیکی را در مورد وصیت نامه ها، متمم وصیت نامه ها و تراستهای مبتنی بر وصیت، نمی پذیرد.

سازد، به بهترین شکل ممکن توجیه کند .

اگر به موجب قانون، امضای معامله‌ای الزامی باشد، این تعهد درصورتی محقق می گردد که قصد قبول تعهد و امضا در پایگاه اینترنتی به اثبات برسد؛ حتی اگر قانون چنین الزامی نداشته باشد، طراحی پایگاه به شرح فوق به مصلحت خواهد بود؛ بنابراین، تنظیم قرارداد را می‌توان بدین شیوه اثبات کرد که شخصی با رعایت تشریفات مشخص شده در پایگاه اینترنتی، صریحا" قصد التزام خویش را ابراز داشته است(هولتمارگ رامبرگ، ۱۳۸۵: ۱۷۱-۱۷۲).

۲. دستورالعمل امضاهای الکترونیکی اروپا:[1]

در ماده ۲ این دستورالعمل چنین آمده است:

امضای الکترونیکی داده ای به شکل الکترونیکی است که به داده پیام الصاق یا به نحو منطقی با آن همسان شده، روشی برای تصدیق و گواهی قلمداد می‌شود؛

۲. امضای الکترونیکی پیشرفته، به معنای هر امضای الکترونیکی است که واجد شرایط زیر باشد:

الف) بدون هیچ تردیدی به امضا کننده منتسب باشد؛

ب) با آن بتوان امضا کننده را شناسایی کرد؛

ج) ایجاد آن به وسیله دستگاههایی صورت گیرد که امضا کننده توان کنترل شخصی بر آن داشته باشد؛

د) به گونه‌ای با داده پیام همسان گردد که هر گونه تغییری در داده، بعد از امضا، قابل تشخیص باشد.

ملاحظه می‌شود که در دستورالعمل اروپایی امضاهای الکترونیکی ـ برخلاف آنسیترال ۱۹۹۶ و یوتا ـ به قصد امضا اشاره‌ای نشده است. مواد مربوط به امضای الکترونیکی پیشرفته (مطمئن) در دستورالعمل مذکور بر شناسایی امضا کننده از طریق تصریح به ملاحظات فنی مبتنی است؛ به گونه ای که از این طریق، شخص امضا کننده تعیین شود.

گفتار سوم: انواع امضای الکترونیکی

۱) دسته بندی بر مبنای به‌کارگیری یا عدم به‌کارگیری رمز نگاری

باتوجه به تعریفهای عام ارائه شده از امضای الکترونیکی، شگردها و ساز و کارهای مختلفی در محدوده این تعریف قرار می گیرند که آنها را می توان به دو دسته تقسیم کرد.

الف) امضاهای الکترونیکی مبتنی بر رمز نگاری:[1]

1. Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures . Available at : http://europa.eu

رمز نگاری شاخه ای از ریاضیات کاربردی است که موضوع آن تبدیل داده ها به رمز برای رسیدن به ایمنی مطلوب است. در جریان رمز نگاری، فرستنده، پیغام رمز نگاری نشده را به یک متن کد گذاری شده تبدیل می کند. دریافت کننده پیغام رمز نگاری را برای یکی از اهدافهای زیر به کار می برد:

(۱) تبدیل متن کد گذاری شده به شکل اصلی و رمز نگاری نشده آن؛

(۲) تشخیص هویت فرستنده پیغام؛

(۳) تشخیص تمامیت داده ها یا عدم آن؛

(۴) ترکیبی از سه مورد یاد شده.

ب) امضاهای الکترونیکی بدون رمز نگاری:

همان‌گونه که از عنوان این امضاها بر می‌آید، وجه تمایز آنها با دسته نخست، استفاده نکردن از رمز نگاری در جریان به کارگیری آنهاست. یکی از مصداقهای این نوع امضا، امضاهای رقمی یا دیجیتالی[۲] است که با اسکن کردن امضای دستی (سنتی) فرد ایجاد می‌شوند. فردی که می‌خواهد سندی الکترونیکی را امضا کند، از تصویر امضای خود استفاده می کند. یکی دیگر از این امضاها ساز و کارهای مبتنی بر «معرفهای زیست سنجی»اند.[۳] در این ساز و کارها، از ویژگی منحصر به فردی برای معرفی و شناسایی امضا کننده استفاده می شود از جمله مهمترین معرفهای زیست سنجی عبارتند از: اثر انگشت، امضاهای دستی، الگوی صدایی، الگوی نوشتن و حالت شبکیه چشم.

۲)دسته بندی بر مبنای سطح ایمنی فراهم شده

چنانکه ملاحظه خواهد شد، تعریفهای ارائه شده از امضای الکترونیکی به گونه ای تنظیم شده اند که همه شگردهایی را که کارکردهای امضای سنتی را ارائه می کنند، دربر می گیرند. در حقیقت، در این تعریفها نوعی بی طرفی فناورانه[4] اتخاذ شده و هیچ یک از ساز و کارهای تولید امضای

1. Cryptography
2. digital signature
3. Biometric identifiers
4. Technological neutrality

الکترونیکی بر دیگری برتری داده نشده است. دلیل این بی طرفی، توجه به گونه گونی روشهای تولید امضای الکترونیکی و پیشرفت های سریعی است که در این زمینه رخ می‌دهد.

با وجود این، در قوانین مختلف، معمولا" پس از ارائه تعریفی کلی از امضای الکترونیکی، نوع خاصی از این امضا ذکر شده که امتیازهای ویژه ای برای آن در نظر گرفته شده است؛ یعنی، امضای الکترونیکی پیشرفته[1] یا امضای الکترونیکی[2] ایمن. علت این امر، آگاهی از این واقعیت است که همه امضاهای الکترونیکی از نظر حقوقی، سطح یکسانی از امنیت را فراهم نمی آورند. برای نمونه، آوردن نام نویسنده در پایان یک پیغام الکترونیکی در قلمرو تعریف عام امضای الکترونیکی قرار می گیرد، ولی هیچ تضمینی درخصوص حفظ پیغام الکترونیکی، دربر ندارد.

شایستهٔ یادآوری است که اکنون فقط امضای رقمی یا دیجیتال، شرایط امضای الکترونیکی پیشرفته، ایمن (یا به تعبیر قانون تجارت الکترونیکی ایران، امضای الکترونیکی مطمئن) را که در قوانین مختلف ذکر شده است، در بردارد (بختیاروند، ۱۳۸۳: ۳۷۲-۳۷۳).

بنابراین، می توان گفت، امضای الکترونیکی مطمئن، به لحاظ فنی یک امضای دیجیتال، یا یک فرایند تجاری معقول است که طرفین آن را به رسمیت شناخته‌اند. لذا در یک تقسیم بندی، امضاهای الکترونیکی به دو نوع«ساده»یا«عادی»و«مطمئن»تقسیم می شوند. درک تمایز و تفاوت بین امضای الکترونیکی از امضای دیجیتال ـ که در واقع یکی از انواع امضای الکترونیکی مطمئن است ـ حایز فواید بسیاری است؛ به گونه‌ای که بسیاری از کشورها، برای جلوگیری از بروز مشکل، برای هر کدام از این اصلاحات، تعریف جداگانه‌ای ارائه نموده‌اند.

از جنبه علمی در تمایز این دو، به اختصار می‌توان گفت که امضای الکترونیکی، اصطلاح جامع و گسترده‌ای است که می تواند هر علامتی را که تصویر دیجیتالی شده یک امضای کاغذی باشد، در برگیرد و یا حتی یک اسم درج شده در زیر یک سند یا آدرس قید شده در بالا یا پایین یک نامه الکترونیکی را شامل شود (Edward H.Freeman.,2004:9)

از این جهت، امضای الکترونیکی، هیچ‌گونه تضمینی از صحت اصالت سند و هویت امضا کننده بدست نداده و حتی در صورتی که در سند، تغییری حاصل شده باشد، آن را نشان نمی دهد، در حالی که امضای دیجیتالی، نوع خاصی از امضای الکترونیکی است و امروزه به عنوان یکی از ایمن ترین و مطمئن ترین امضاهای الکترونیکی به حساب می آید. بنابراین، امضای الکترونیکی

1. Advanced electronic signature

2. Secure electronic signature

دارای معنای عامتری است و شامل امضای دستی اسکن شده یا اسم شخصی که در قسمت انتهایی نامه الکترونیکی قید می گردد، نیز می‌شود (رضایی،۱۳۸۷: ۱۲۱-۱۳۹).

در تعریف امضای دیجیتال گفته شده است که این امضا یک فرایند رمزنگاری (cryptography) است و به معنای رمز کردن پیام، با کلید خصوصی و رمز گشایی آن با کلید عمومی است. در این روش، طرفین بجای در اختیار داشتن یک کلید مشترک، هرکدام یک جفت کلید دارند. این جفت کلیدها که کلید عمومی[1] و کلید خصوصی[2] نامیده می شوند، با یکدیگر قرینه و جفت هستند. کلید عمومی، سری نبوده، می تواند در اختیار همه مردم از جمله طرف معامله قرار گیرد، اما کلید خصوصی کاملا" محرمانه و تنها در اختیار مالک آن است. از آنجا که کلید خصوصی از کلید عمومی قابل استنباط نیست، می‌توان از یک کلید برای رمز نگاری و از کلید دیگر برای رمز گشایی استفاده کرد. این امضا، شاخه ای از ریاضی کاربردی است که ابتدا، پیام را به شکل نامفهوم، تبدیل و سپس آن را به شکلی که قابل فهم باشد، در می‌آورد. بدیهی است که کلیدهای عمومی و خصوصی به کارگرفته شده در این نوع از امضا، فیزیکی نبوده، بلکه به صورت اعداد هستند که توسط سخت افزارها و نرم افزارهای خاصی، ایجاد می شوند. از لحاظ تخصصی، به فرایندی که طی آن، نرم افزارها و سخت افزارهای رایانه‌ای، با استفاده از این دو نوع کلید، مبادرت به رمزنگاری و رمزگشایی می کنند،«رمز نگاری نامتقارن»یا زمز نگاری کلید عمومی[3] گفته می‌شود. یکی دیگر از فن آوری های امضای الکترونیکی، که البته از درجه اطمینان کمتری نسبت به امضای دیجیتالی، برخوردار بوده و کاربرد آن محدودتر است، استفاده از فن آوری«بیومتریک»است. در این روش شخص با استفاده از خودکار مخصوص بر روی صفحه نمایش رایانه و یا یک صفحه دیجیتالی، امضا می کند. امضای وی توسط رایانه، پردازش شده، به صورت مقدارهای عددی، ذخیره می گردد که می‌تواند به ارتباط الکترونیکی اضافه شده و به عنوان مدرک شناسایی آن شخص تلقی می‌شود. در این روش از قبل، نمونه امضا از شخص گرفته شده و ذخیره می‌شود و توسط روش بیومتریک، پردازش و سپس برای شناسایی و تشخیص هویت و انتساب امضا به امضاکننده، مورد استفاده می گردد (همان: ۱۴۵ ـ ۱۴۶).

گفتار چهارم: مستند سازی امضای الکترونیکی و دفاتر خدمات صدور گواهی الکترونیکی

۱- مراجع تأیید و صدور گواهی الکترونیکی

1. public key(
2. private key
3. Asymmetric cryptography

تأیید و احراز هویت، یکی از مسائل بسیار مهم در تجارت الکترونیکی و قراردادهای منعقده در فضای مجازی محسوب می‌شود. هویت در لفظ؛ یعنی حقیقت شیء یا شخصی که مشتمل بر صفات جوهری او باشد. هویت ویژگی قابل تشخیص یا شخصیت یک فرد است. تأیید هویت روندی است که بر آن اساس اثبات می‌شود که بعضی از ویژگیهای منتخب یک موجود در دنیای واقعی به آن موجود تعلق دارد. برای مثال، توپوگرافی منحصر به فرد صورت هر فردی، نشان دهنده آن شخص با مشخصات خاص دارای هویت ویژه ای است.

در زمینه سیستمهای اطلاعاتی، تأیید هویت روز به روز مهمتر می‌شود و اهمیت خاصی پیدا می‌کند، چون معاملات تجاری و مبادلات اجتماعی رو به فزونی است و عدم حضور فیزیکی کامل، همواره به نشانه های هویتی منحصر به فرد و قابل اثبات نیاز دارد. در مورد سیستم‌های اطلاعاتی و الکترونیکی، نام و نشانی از مهمترین ویژگیهای قابل تشخیص است. اصولا" هویت افراد در معاملات حایز اهمیت است و در معاملات روزمره، افراد از طریق اوراق شناسایی مانند شناسنامه و گواهینامه رانندگی مبادرت به احراز هویت نموده، امضای افراد نیز برای تأیید مندرجات یک سند به رسمیت شناخته می‌شود، ولی در هر صورت امکان دارد که هویت افراد مورد توجه قرار گیرد و یا نسبت به اصالت و صحت انتساب اسناد به امضا کندگان آنها تردید شود.

دفاتر اسناد رسمی در ایران، وظیفه تأیید هویت و امضای افراد را به عهده دارند و صحت انتساب اسناد را به صادرکنندگان آنها تأیید می کنند. در محیط مجازی نیز احتمال بروز این مسائل و تردید و انکار نسبت به سند طرف و یا ادعای جعل و انکار نسبت به امضای متعاملین وجود خواهد داشت (راد اخلاقی، ۱۳۸۷: ۱۲۵).

با استفاده از روش امضای دیجیتال یا امضای مبتنی بر رمز نگاری نامتقارن، تمامیت سند، محرمانه بودن اطلاعات (در صورت لزوم) و امنیت داده ها تضمین می شود؛ اما یک مسأله مهم حل نشده باقی می ماند و آن تضمین هویت امضا کننده است. در واقع، به لحاظ حقوقی، مهمترین اثر امضا، اثبات رابطه سند با کسی است که امضا به او نسبت داده شده است.

امضای الکترونیکی مطمئن یا دیجیتال به تنهایی قادر به تضمین هویت امضا کننده نیست. آنجا که طرفین یک رابطه حقوقی تجار بزرگ بین المللی یا شرکت های چند ملیتی هستند، این مشکل کمتر بروز می کند؛ زیرا طرفین یکدیگر را به خوبی می شناسند و از توانایی های مالی و فنی و انسانی یکدیگر به خوبی آگاه هستند. در این گونه موارد، صرف مبادله داده های رمز نگاری شده برای اثبات وجود رابطه حقوقی و محتوای آن کفایت می کند. همچنین در مواردی که طرفین

مبادله الکترونیکی قبل از ورود به محیط الکترونیکی درخصوص نحوه انجام این مبادلات و حقوق و تکالیف خود یا روند ایجاد امضای الکترونیکی توافق می کنند و هویت هر یک از طرفین برای طرف دیگر آشکار است، مشکل تعیین هویت اساسا" فرصت بروز نمی یابد. برای مثال، در عملیات بانکی از طریق کارت های بانکی الکترونیکی معمولا" مشتری با حضور در بانک، ضمن ارائه مدارک لازم برای تعیین هویت، قراردادی را که بانک درخصوص نحوه استفاده از کارت بانکی و مسائل حقوقی مرتبط با آن، از جمله دلیل انجام عملیات بانکی تهیه کرده، امضا می‌کند. در این گونه موارد، امضای الکترونیکی می‌تواند مبنایی برای سیستم پرداخت الکترونیکی باشد. در این سیستم دارنده کارت، فروشنده و بانک های عضو که مبادله را پردازش می کنند، یک امضای دیجیتال یا الکترونیکی در دست دارند که هویت و صلاحیت وی را درون سیستم تضمین می کند، اما مشکل تعیین هویت در سیستم های باز که طرفین از پیش درخصوص حقوق و تکالیف خود توافق نکرده‌اند و همدیگر را نمی شناسند، همچنان باقی است. برای مثال، در معاملات از طریق شاهراه های اطلاعاتی (اینترنت) که در یک طرف آن تجار، شرکت ها و مؤسسات تجاری و خدماتی و در طرف دیگر، عمدتا" مصرف کنندگان قرار دارند، تضمین هویت امضا کنندگان ضرورت دارد. از این‌رو، از زمانی که فناوری امضای الکترونیکی مطرح شده است، یکی از دغدغه های اصلی قانون گذاری ملی و سازمان های تجاری بین المللی و اتاق های بازرگانی، این است که مرجع ثالثی، اعتبار پیام را از طریق تعیین هویت امضا کننده دیجیتال تضمین کند.

این مرجع ثالث اصطلاحا"«دفاتر خدمات صدور گواهی الکترونیکی»یا «دفاتر مطمئن خدمات الکترونیکی»یا«مراجع گواهی»نامیده می شوند. عملکرد این دفاتر با عملکرد دفاتر اسناد رسمی در محیط سنتی و اسناد کاغذی قابل مقایسه است. به عبارت دیگر، همان طور که دفاتر اساد رسمی با احراز هویت امضا کنندگان سند و طی تشریفات قانونی به نوشته سندیت و رسمیت می بخشند، «دفاتر گواهی الکترونیکی»نیز هویت امضا کننده را تضمین می کنند و در نتیجه، به اطلاعات الکترونیکی سندیت می دهند. در واقع، گواهی دیجیتال که توسط دفاتر خدمات الکترونیکی صادر می شود، هویت امضا کننده را از طریق کنترل رابطه بین کلید عمومی و دارنده کلید خصوصی مربوط تضمین می کند. به عبارت دقیقتر، امضای دیجیتال دارای دو جزء متفاوت، اما از نظر ریاضی مرتبط است. کلید خصوصی که در اختیار صاحب امتیاز است و کلید عمومی که در فهرست مراجع گواهی قرار دارد. این مرجع تضمین می کند که کلید عمومی مندرج در فهرست به درستی اعلام و ایجاد شده است؛ زیرا هویت دارنده کلید خصوصی که منطبق با کلید عمومی است، نزد

مراجع گواهی وجود دارد. برای اطمینان از اینکه داده پیام از سوی کسی که ادعا می کند، صادر شده، وجود کلید عمومی ضروری است. در واقع، مرجع گواهی دو وظیفه مهم دارد: اول، تخصیص یک کلید خصوصی به دارنده و ثبت آن به عنوان یک مستند اطلاعاتی؛ و دوم نگهداری کلید مکمل آن به نام کلید عمومی و در دسترس قرار دادن فهرست نام دارندگان کلید عمومی از طریق سیستم درون خطی و بانکهای اطلاعاتی ویژه (دبلفون، ۱۳۸۸ :۲۲۲-۲۲۴).

۲- دفاتر خدمات صدور گواهی الکترونیکی

قانون تجارت الکترونیکی ایران، بدون اینکه تعریفی از گواهی الکترونیکی ارائه دهد، باب دوم خود را به «دفاتر خدمات صدور گواهی الکترونیکی»اختصاص داده و با تعریف این دفاتر (ماده ۳۱)، ضوابط تأسیس و شرح وظایف آنها را به آیین نامه موکول کرده است (ماده ۳۲).

بر اساس ماده ۳۱ این قانون:«دفاتر خدمات صدور گواهی الکترونیکی، واحدهایی هستند که برای ارائه خدمات صدور امضای الکترونیکی در کشور تاسیس می شوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به روز نگهداری گواهی های اصالت (امضای) الکترونیکی است».

آیین نامه موضوع ماده ۳۲ قانون تجارت الکترونیکی تحت شماره ۹۸۹۸۶/ت ۵۳۱۸۱۹ در تاریخ ۱۳۸۶/۶/۱۱ به تصویب هیأت وزیران رسیده است. ماده ۱ آیین نامه که به تعارف اختصاص یافته، در بند (ج) خود گواهی الکترونیکی را چنین تعریف کرده است:

«داده الکترونیکی حاوی اطلاعاتی در مورد مرکز صادر کننده گواهی، مالک گواهی، تاریخ صدور و انقضا، کلید عمومی مالک و یک شماره سریال است که توسط مرکز میانی تولید شده؛ به گونه ای که هر شخصی می تواند به صحت ارتباط بین کلید عمومی و مالک آن اعتماد کند».

در این ماده، سایر مفاهیم مرتبط با گواهی امضای الکترونیکی، شامل:«ایجاد امضای الکترونیکی»،«داده وارسی امضای الکترونیکی»،«زوج کلید یا داده های ایجاد و وارسی امضای الکترونیکی»،«طرف اعتماد کننده»،«مهر زمانی»،«مخزن»،«تجهیزات ایجاد و وارسی امضای الکترونیکی»،«سیاست های گواهی»،«دستورالعمل گواهی»و«زیر ساخت کلید عمومی»تعریف شده است.

ماده ۴ این آیین نامه سه سطح مختلف برای دفاتر خدمات صدور گواهی الکترونیکی موضوع ماده ۳۱ قانون، تعیین کرده است:

«الف) مرکز دولتی صدورگواهی الکترونیکی ریشه که با کسب مجوز از شورای سیاست گذاری گواهی الکترونیکی (موضوع ماده ۲ آیین نامه) فعالیت می‌نماید؛

ب) مرکز صدور گواهی الکترونیکی میانی که با کسب مجوز از یک مرکز ریشه، مبادرت به صدور گواهی الکترونیکی نموده، سایر خدمات مربوط به امضای الکترونیکی را انجام می‌دهد.

پ) دفتر ثبت نام گواهی الکترونیکی که با کسب مجوز از حداقل یک مرکز میانی نسبت به ثبت و انتقال درخواست متقاضیان درخصوص صدور و لغو گواهی ها و سایر امور مربوط به ضوابط و دستورالعمل های صادره از سوی مراکز میانی که تعهد همکاری با آنها امضا نموده است، اقدام می‌نماید».

با مطالعه سایر مواد آیین نامه، مشخص می شود که شورای سیاست گذاری گواهی الکترونیکی با ترکیب مقرر در ماده ۲ آیین نامه وجود دارد. این شورا عمدتا" سیاست گذاری زیر ساخت کلید عمومی کشور و ارائه آن به شورای عالی فناوری اطلاعات کشور برای تصویب، نظارت بر فعالیت و عملکرد مراکز میانی و ریشه و تصویب استانداردها، رویه ها و دستورالعمل های اجرایی گواهی الکترونیکی را به عهده دارد.

باتوجه به ماده ۵ آیین نامه، مراکز ریشه اجرای سیاست ها و دستورالعمل های شورای سیاست گذاری گواهی الکترونیکی و صدور مجوز برای مراکز میانی و لغو آنها درصورت تخلف و نیز نظارت بر عملکرد مراکز میانی را عهده دار هستند. بر خلاف شورای سیاست گذاری گواهی الکترونیکی و مراکز ریشه که به اعمال حاکمیت می پردازند و در نتیجه دولتی هستند، مرکز میانی می تواند حسب مورد از سوی دستگاههای دولتی یا بخش غیر دولتی (خصوصی یا تعاونی) ایجاد شود.

برابر ماده ۸ آیین نامه مراکز میانی دارای وظایف زیر هستند:

الف) بررسی صلاحیت و صدور مجوز برای دفاتر ثبت نام؛

ب) تضمین ارائه خدمات صدور و لغو گواهی ها به صورت مطمئن؛

پ) تضمین ارائه خدمات تأیید صدور گواهی ها به صورت سریع و مطمئن؛

ت) تضمین محرمانه بودن داده های مربوط به امضا در فرآیند ایجاد این داده ها برای جلوگیری از شبیه سازی گواهی ها؛

ث) حصول اطمینان نسبت به موارد زیر:

۱) در لحظه صدور گواهی الکترونیکی، اطلاعات مندرج در گواهی ها صحیح باشند.

۲) در هنگام صدور گواهی الکترونیکی، امضا کننده مشخص شده در گواهی، داده‌های ایجاد و وارسی امضای الکترونیکی را دریافت نموده، داده ایجاد امضای الکترونیکی تحت کنترل انحصاری وی باشد.

۳) کلیه اطلاعات مرتبط با گواهی الکترونیکی را تا مدت زمان تعیین شده در دستورالعمل گواهی به صورت الکترونیکی حفظ نماید.

۴) تاریخ و ساعت صدور و لغو یک گواهی به دقت تعیین شده و قابل تشخیص باشد.

۵) عدم کپی یا ذخیره داده ایجاد امضای الکترونیکی متقاضیان را تضمین نماید.

۶) گواهی قابل دسترسی برای عموم نباشد، جز در مواردی که صاحبان گواهی ها رضایت خود را اعلام کرده اند یا نوع گواهی انتشار عمومی را ایجاب کند.

۷) در صورت امکان مرکز میانی و با دریافت درخواست دفتر ثبت نام، یک مهر زمانی به داده های الکترونیکی منضم شود...»

مطابق ماده۱۳ آیین نامه وظایف دفاتر ثبت نام گواهی الکترونیکی که به طور مستقیم با درخواست کنندگان گواهی الکترونیکی سر و کار خواهند داشت، عبارتند از:

«الف) انجام عملیات مطابق با دستورالعمل گواهی مرکز میانی مربوط؛

ب) احراز و تصدیق مدارک ارائه شده متقاضی دریافت خدمات گواهی؛

پ) ارسال درخواست متقاضی همراه با مدارک مربوطه به مرکز میانی مربوط؛

ت) دریافت گواهی صادر شده از مرکز میانی مربوطه و تحویل به متقاضی».

به علاوه، بر اساس ماده ۱۵ آیین نامه، دفاتر ثبت نام گواهی الکترونیکی مکلفند هنگام ثبت نام متقاضی گواهی الکترونیکی، امضای شخصی را برای وارسی صحت اطلاعات ارائه شده (املایی و محتوایی) اخذ نموده، وی را از نحوه و شرایط طرح و پیگیری دعوا مطابق سیاست ها و دستورالعمل های مراکز گواهی میانی آگاه سازند.

ماده ۱۸ آیین نامه به گواهی های امضای الکترونیکی صادر شده در خارج از کشور پرداخته، مقرر می‌دارد: «اعتبار و پذیرش گواهی الکترونیکی صادره از مراجع صدور گواهی خارجی، مشروط به توافق دو جانبه بین مرکز ریشه کشور و مرجع صدور گواهی کشور خارجی با رعایت اصل شرط عمل متقابل و تصویب شورا (شورای سیاست گذاری گواهی الکترونیکی) خواهد بود».

از جمله ایرادات وارده به ماده ۱۸ فوق الذکر این است که در صورت توافق بین مرجع صدور گواهی خارجی و مرکز ریشه کشور، دیگر جایی برای رعایت شرط عمل متقابل نخواهد بود. در حقیقت، از دید حقوق

بین الملل عمومی، عمل متقابل زمانی ملاک رفتار یک کشور در مقابل کشور دیگر قرار می گیرد که بین آن دو توافق و قراردادی در زمینه موضوعی خاص موجود نباشد. در صورت وجود قرارداد باید به مفاد قرارداد عمل شود و موضوع عمل متقابل منتفی خواهد بود (همان: ۲۲۲-۲۲۷).

۳) موضع قانون نمونه آنسیترال ۲۰۰۱

بند (ه) ماده ۲ قانون نمونه آنسیترال درخصوص امضاهای الکترونیکی، دفاتر ارائه خدمات گواهی الکترونیکی را چنین تعریف نموده است: «شخصی که گواهی صادر می کند و ممکن است دیگر خدمات مرتبط با امضاهای الکترونیکی را ارائه دهد».

ماده ۹ این قانون نمونه، در مورد خدماتی که توسط دفاتر ارائه دهند. خدمات گواهی امضا، انجام می‌شوند، مراتب زیر را مقرر نموده است:

۱. در مواردی که ارائه دهنده خدمات صدور گواهی خدماتی را برای حمایت از امضای الکترونیکی ارائه می‌دهد که از آن می توان به عنوان امضایی با آثار قانونی استفاده کرد، وی باید:

الف) مطابق اظهاراتی که درخصوص سیاست ها و رویه هایش بیان کرده است، عمل کند؛

ب) مراقبت معقولی برای تضمین صحت و کامل بودن همه آثار فیزیکی صورت دهد که به وسیله او ایجاد شده و طی چرخه حیاتی گواهی با آن مرتبط هستند یا در گواهی گنجانده شده‌اند؛

ج) تجهیزاتی را که به صورت معقولی قابل دسترسی است، فراهم کند تا طرف اعتماد کننده با استفاده از آن بتواند موارد زیر را تشخیص دهد:

۱. هویت ارائه دهنده خدمات صدور گواهی؛

۲. امضا کننده‌ای که در گواهی معرفی شده است، در زمان صدور گواهی یا پیش از آن معتبر باشد.

د) تجهیزاتی را که به صورت معقولی قابل دسترسی است، فراهم کند تا طرف اعتماد کننده بتواند با استفاده از آن، در موارد ضروری، از طریق گواهی یا به صورتی دیگر موارد زیر را تشخیص دهد:

۱) روش به کار رفته برای شناسایی امضا کننده؛

۲) هرگونه محدودیت درخصوص هدف یا فایده‌ای که داده‌های تشکیل دهنده امضا یا گواهی ممکن است برای آن به کار رود؛

۳) اعتبار داده های تشکیل دهنده امضا و عدم آسیب دیدگی آنها.

۴) هرگونه محدودیت درخصوص چارچوب یا قلمرو مسؤولیت اعلام شده به وسیله ارائه دهنده خدمات صدور گواهی؛

۵) وجود یا نبود تجهیزاتی برای اطلاع رسانی به وسیله امضا کننده بر مبنای بند (ب) از پاراگراف (۱) ماده ۸

۶) ارائه یا عدم ارائه بموقع خدمات فسخ.

هـ) در مواردی که خدماتی بر مبنای زیر پاراگراف (۵) (د) ارائه می شود، تجهیزاتی برای امضا کننده برای اطلاع رسانی بر مبنای بخش (ب) از بند (۱) ماده ۸ فراهم است و در مواردی که خدماتی بر مبنای زیر پاراگراف (۶) (د) ارائه می شود، در دسترس باشد و خدمات فسخ بموقع را تضمین کند؛

و) از سیستم ها، تشریفات و منابع انسانی قابل اعتماد در اجرای خدمات خود بهره گیرد.

۲. عواقب قانونی قصور در رعایت شرایط پاراگراف (۱) بر عهده ارائه کننده خدمات صدور گواهی خواهد بود (ترجمه قانون نمونه آنسیترال ۲۰۰۱، پیشین: ۴۷).

نتیجه گیری

یکی از رهاوردهای مهم فناوری اطلاعات، تحول در نظام سنتی ادله اثبات دعواست. در اکثر کشورهای جهان، دلایل کتبی یا نوشته پس از اقرار اهمیت انکارناپذیری دارند، اما فناوری اطلاعات به دلیل ویژگیهای فنی خود به طور محسوس از گردش کاغذ و دلایل کاغذی می کاهد. در نتیجه، اطلاعات مهمی که می تواند در رسیدگی به اختلافها و حل و فصل دعاوی سودمند واقع شود، در سیستم رایانه ای نگهداری شده یا به شکلی نگهداری می شود که فقط با رایانه می توان به آنها دسترسی پیدا نمود.

حجم چشمگیری از اطلاعات ذخیره شده در رایانه نیز هرگز روی کاغذ چاپ نمی‌شود. این واقعیت ما را با این پرسش مهم روبه‌رو می کند که آیا اسناد الکترونیکی را می توان به منزله دلیل در دادگاه ارائه کرد؟ با اندکی تأمل، بی تردید پاسخ مثبت خواهد بود، زیرا عدم پذیرش و شناسایی دلایل الکترونیکی نتیجه‌ای جز بلاتکلیفی قراردادها و عدم حل و فصل اختلافها و سرانجام بی رغبتی بازرگانان به انجام داد و ستدهای الکترونیکی نخواهد داشت. بنابراین، در قوانین و منابع ملی و بین المللی مختلف، اعتبار و ارزش اثباتی پیغامهای الکترونیکی پذیرفته شده است.

باید توجه داشت که پذیرش این اسناد به منزله دلیل منوط به قناعت وجدان دادرس رسیدگی کننده به دعاوی است و پذیرش ارزش اثباتی معادل اسناد کاغذی برای اسناد الکترونیکی، به تحقق شرایطی مانند تغییر ناپذیری و ثبات و دوام منوط شده است.

امضای الکترونیکی نیز به عنوان داده های الکترونیکی ای تعریف شده که به یک داده پیام پیوند خورده تا از آن برای شناسایی امضا کننده داده پیام و نیز تأیید وی درخصوص اطلاعات موجود در داده پیام، استفاده شود.

امضاهای الکترونیکی بر اساس دسته بندی بر مبنای به کارگیری یا عدم به کارگیری رمز نگاری و نیز بر مبنای سطح ایمنی فراهم شده تقسیم بندی می شوند. در راستای اقدامات تقنینی درخصوص تسهیل و ایمن سازی داد و ستدهای الکترونیکی، می توان به تأسیس دفاتر خدمات صدور گواهی الکترونیکی نیز اشاره نمود. عملکرد این دفاتر با عملکرد دفاتر اسناد رسمی در محیط اسناد کاغذی قیاس پذیر است. به بیان دیگر، همان‌گونه که دفاتراسناد رسمی با احراز هویت امضا کنندگان سند و گذراندن تشریفات قانونی به آن نوشته رسمیت می بخشند، دفاتر گواهی الکترونیکی نیز هویت امضا کنندگان را تضمین کرده، در نتیجه، به اطلاعات الکترونیکی سندیت می دهند.

در ایران، تصویب قانون تجارت الکترونیکی و برخی آیین نامه های اجرایی آن، از قبیل آیین نامه ماده **۳۲**، و تعیین چهارچوب های حقوقی امضای الکترونیکی، و پذیرش قانونی ادله الکترونیکی و ارزش اثباتی آن، گام مهمی برای عملی ساختن مفاهیمی، همچون: تجارت الکترونیکی، دولت الکترونیکی، بانکداری الکترونیکی وغیره تلقی می‌شود، لیکن هنوز تا بهره برداری عملی و عمومی و همه جانبه از ادله الکترونیکی و امضای الکترونیکی مطمئن راه طولانی باقی است.

همتم بدرقه راه کن ای طایر قدس　　که دراز است ره مقصد و من نو سفرم

فهرست منابع

الف) کتب فارسی و ترجمه ها:

- دبلفون، پرفسور زویه لینان .(۱۳۸۸). **حقوق تجارت الکترونیک**، ترجمه و تحقیق دکتر ستار زرکلام، تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، چاپ نخست.
- رضایی، علی .(۱۳۸۷). **حقوق تجارت الکترونیکی**، تهران: نشر میزان، چاپ اول.
- هولتمارک رامبرگ، کریستینا .(۱۳۸۵). «دستورالعمل تجارت الکترونیکی و تشکیل قرارداد در چشم اندازی تطبیقی»، ترجمه مصطفی السان، **مجله تخصصی دانشگاه علوم اسلامی رضوی**، ش۲۰، ویژه حقوق، سال ششم، تابستان.

ب) مقالات فارسی

- بختیاروند، مصطفی .(۱۳۸۴). **مطالعه تطبیقی مقررات حاکم بر داد و ستدهای الکترونیکی**، در مجموعه مقاله های همایش بررسی جنبه های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، چاپ نخست، نشر سلسبیل.
- زرکلام، ستار .(۱۳۸۴). **قانون تجارت الکترونیکی و الفبای الکترونیکی**، در مجموعه مقاله‌های همایش بررسی جنبه های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضائیه، چاپ نخست، نشر سلسبیل.
- قانون نمونه تجارت الکترونیکی آنسیترال .(۱۹۹۶). ترجمه مصطفی بختیاروند، **خبرنامه انفورماتیک**، تهران: ش ۸۹، دی ۱۳۸۲.
- قانون نمونه آنسیترال درخصوص امضاهای الکترونیکی .(۲۰۰۱). ترجمه مصطفی بختیاروند، **خبرنامه انفورماتیک**، تهران: ش ۸۸، مهر ۱۳۸۲.

ج) پایان نامه‌ها

- آهنی، بتول .(۱۳۸۲). **انعقاد و اثبات قراردادهای الکترونیکی**، رساله دکتری حقوق خصوصی، راهنمایی دکتر گودرز افتخار جهرمی، دانشکده حقوق دانشگاه تهران.
- راداخلاقی، مهرداد .(۱۳۸۷). **اعتبار قراردادهای الکترونیکی (با امضای دیجیتال) در حقوق ایران**، پایان نامه کارشناسی ارشد حقوق خصوصی، به راهنمایی دکتر سیدهادی حسینی، دانشکده حقوق دانشگاه آزاد اسلامی، واحد تهران مرکزی، تیرماه.
- شفقت، عبرت علی .(۱۳۸۶). **زمان و مکان وقوع عقد در تجارت الکترونیک (حقوق ایران و قوانین نمونه آنسیترال)**، پایان نامه کارشناسی ارشد حقوق خصوصی، به راهنمایی دکتر غلام نبی فیضی چکاب، دانشکده حقوق و علوم سیاسی دانشگاه علامه طباطبایی، بهمن ماه.
- علی اکبری، علی جان .(۱۳۸۷). **جنبه های حقوقی امضای الکترونیکی با تکیه بر قوانین کشورهای مختلف**، پایان نامه کارشناسی ارشد اقتصاد و تجارت الکترونیک، به راهنمایی دکتر اسدالله فرزین وش، دانشکده اقتصاد دانشگاه تهران، مردادماه.

د) مقالات لاتین

- Anjanette H.Raymond ,Electronic commerce and the new UNCITRAL Draft Convention , the computer & Internet lawyer , vol. 23, no. 8. August 2006.

- Edward H. Freeman , J. D. , Digital Signatures and Electronic Contracts, INFORMATION SYSTEMS SECURITY, MAY, June 2004.

هـ) قوانین خارجی، قوانین نمونه و اسناد بین المللی

- Electronic Signature in Global and National Commerce Act , U.S, 2000 [E – Sign]
- Uniform Commercial Information Transactions Act,U.S,1999,[UCITA]
- Uniform Electronic Transactions Act,U.S,1999,[UETA]
- Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures. Available at: http://europa.eu
- Directive 2000/31/ EC of the European Parliament and of the Council of June 2000 on Certain Electronic Commerce.
- Available at: www. europa.oeu.int
- Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce 1996 .
- UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 ; Available at: www.uncitral.org.
- UNCITRAL Model Law on Electronic Signatures (2001) ,
- Available at: www.uncitral.org.
- United Nations Convention on the Use of Electronic Communications in International Contracts , Adopted by the General Assembly on 23 November 2005. Available at: www.uncitral.org.