

ماهیت و آثار امضای الکترونیکی در حقوق ایران، مقررات آنسیترال

دکتر رسول مظاهری^۱

علیرضا ناظم^۲

چکیده

امضای الکترونیکی عبارت از داده‌ای الکترونیکی است که به یک داده پیام ضمیمه می‌گردد و موجبات شناسایی شخص و اعلام رضایت وی به مفاد داده پیام را فراهم می‌آورد.

در یک دسته‌بندی، امضای الکترونیکی به لحاظ ارزش اثباتی آن به دو نوع امضای الکترونیکی ساده و امضای الکترونیکی مطمئن منقسم می‌شود.

امضای الکترونیکی ساده مطابق بند «ی» ماده ۲ قانون تجارت الکترونیکی ایران «هر نوع علامت منضم شده و یا به نحو منطقی متصل شده به داده پیام است که برای شناسایی امضا کننده مورد استفاده قرار می‌گیرد». اما امضای الکترونیکی مطمئن بر اساس ماده ۱۰ همان قانون امضایی است که «الف - نسبت به امضا کننده منحصر به فرد باشد، ب - هویت امضا کننده داده پیام را معلوم کند، ج - به وسیله

۱. عضو هیأت علمی گروه حقوق دانشگاه اصفهان.

۲. کارشناس ارشد حقوق خصوصی و سردفتر اسناد رسمی.

امضا کننده و یا تحت اراده انحصاری او صادر شده باشد، - به نحوی به یک داده پیام متصل شود که هر گونه تغییری در آن داده پیام، قابل تشخیص باشد».

مسئله دیگری که در خصوص امضای الکترونیکی مطرح است بررسی ارزش اثباتی امضای الکترونیکی ساده و مطمئن است. امضای الکترونیکی ساده همانند امضای مندرج در اسناد عادی قابل انکار و تردید است، اما امضای الکترونیکی مطمئن به لحاظ ارزش اثباتی مانند امضای مندرج در اسناد رسمی است و صرفاً می توان در مورد آن ادعای جعل مطرح کرد که اثبات آن بر عهده مدعی است.

اصول کلی حقوقی حاکم بر جنبه اثباتی امضای الکترونیکی عبارتند از: اصل پذیرش امضای الکترونیکی، اصل عدم تبعیض بین امضای الکترونیکی ساده و مطمئن، اصل برابری آثار امضای دستی و امضای الکترونیکی، اصل در حکم نوشته بودن داده پیام، اصل اصیل بودن داده پیام.

در حال حاضر تنها امضایی که از آن با نام امضای الکترونیکی مطمئن یاد می شود، امضای رقمی است زیرا این امضا منحصر به فرد بوده امکان شناسایی امضاکننده را فراهم می کند، تحت اراده انحصاری او قرار دارد و هر گونه تغییرات بعدی در داده پیام و امضا از طریق آن قابل کشف است. این موارد دقیقاً ویژگی های امضای الکترونیکی مطمئن در قانون تجارت الکترونیکی و قانون نمونه امضای الکترونیکی آنسیترال (۲۰۰۱) است.

قاعده کلی در مورد امضای الکترونیکی این است که این امضا به لحاظ آثار همانند امضای دستی است و آثار آن عبارتند از: دلالت داشتن بر قصد انشاء، شناسایی فرد، تأیید محتویات سند و دلالت بر انتساب سند به امضاکننده. در این مقاله با بررسی ابعاد حقوقی امضای الکترونیکی چگونگی ایجاد و بهره برداری از آن را مورد بررسی قرار داده آثار حقوقی و تغییرات احتمالی مورد نیاز در مقررات را تحلیل حقوقی کرده ایم.

کلید واژگان: امضای الکترونیکی، امضای رقمی (دیجیتالی)، امضای الکترونیکی مطمئن،

ارزش اثباتی امضای الکترونیکی.

۱- تعریف امضای الکترونیکی^۱

در تعریف امضای الکترونیکی قانونگذاران و حقوقدانان تعابیر متفاوتی دارند. هر کدام بر جنبه‌ی خاصی از آن توجه کرده‌اند؛ بعضی به مسائل فنی و برخی دیگر به جنبه‌های حقوقی آن توجه داشته‌اند. در این جا ابتدا به تعاریفی که از امضای الکترونیکی شده است می‌پردازیم و سپس با بررسی هر يك از آنها تعریف برگزیده خود را ارائه خواهیم کرد.

در بند ۲ ماده ۱۳ پیش نویس قانون تجارت الکترونیکی آمده بود: «امضای الکترونیکی عبارت از هر نوع علامت یا روشی است که به يك داده، منضم شده و برای شناسایی امضاکننده داده مورد استفاده قرار می‌گیرد.» سپس قانونگذار ایران در سال ۱۳۸۲ با کمی تغییر، در «ماده ۲» قانون تجارت الکترونیکی در تعریف امضای الکترونیکی اظهار داشت: «امضای الکترونیکی عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به «داده پیام»^۲ است که برای شناسایی امضاکننده «داده پیام» مورد استفاده قرار می‌گیرد.»

در این تعریف امضای الکترونیکی نوعی «علامت» تعبیر شده است حال آنکه به نظر می‌رسد عبارت مناسب‌تر با فضای مجازی رایانه «داده» است و بهتر بود قانونگذار به جای عبارت «علامت» از «داده» استفاده می‌کرد. البته شاید علت این امر آن باشد که قانونگذار ایران با عنایت به تعریف کهن امضا که هر نوع «علامت یا نوشته» در کتب حقوقدانان تعبیر شده است و این که هنوز عبارت جدید «داده»^۳ وارد ادبیات حقوقی کشور نگردیده، چنین لفظی را استعمال کرده است، اما به هر حال ضروری است اصطلاحات جدید وارد ادبیات حقوقی رایانه‌ای ایران گردد. دومین نکته این است که، قانونگذار تفاوت بین «انضمام امضا و اتصال آن به نحو منطقی» به يك داده پیام را روشن نکرده است. علت این امر می‌تواند تبعیت صرف و ترجمه لفظ به لفظ از منابع خارجی باشد. در متون خارجی

1. Electronic Signature.

2. Data Message.

۳. «داده» به کوچکترین واحد اطلاعات در رایانه می‌گویند.

و از جمله راهنمای تصویب ضمیمه شده به قانون نمونه آنسیترال نیز این تعابیر تعریف نشده‌اند و با توجه به این که مفاهیم این عبارات هنوز آشنای ذهن حقوقدانان نیست، لازم است از طریق تفسیر و آوردن آنها در کتب و مقالات حقوقی کاملاً واضح گردد. ظاهراً منضم شدن اشاره به مواردی دارد که شکل اسکن شده امضای دستی ضمیمه سند و ارسال می‌گردد و اتصال به نحو منطقی، اشاره به سامانه امضا با کلید اختصاصی و محرمانه است که پس از رمزنگاری تنها با کلید عمومی همین تاجر یا با کلید محرمانه مشترک قابل رمزگشایی است که در ظاهر چیزی دیده نمی‌شود ولی منطقاً مرتبط است.

نکته دیگر آن که این تعریف صرفاً به يك جنبه از آثار امضا یعنی «شناسایی امضا کننده» عنایت دارد حال آنکه به نظر می‌رسد با توجه به این که امضا در قرارداد، وسیله ابراز اراده و رضایت طرفین است، اثر اصلی و مهم آن، اعلام رضایت و التزام به مفاد سند است که در این ماده مورد غفلت قرار گرفته است.

در ماده ۲ قانون نمونه آنسیترال (۲۰۰۱) امضای الکترونیکی چنین تعریف شده است: «امضای الکترونیکی عبارت از داده الکترونیکی، منضم شده و یا به صورت منطقی متصل شده به یک داده پیام است و برای تشخیص هویت امضا کننده داده پیام و تأیید وی نسبت به اطلاعات موجود در داده پیام، مورد استفاده قرار می‌گیرد»^۱.

با نگاهی به این تعریف و مقایسه آن با تعریف قانون تجارت الکترونیکی ایران در می‌یابیم که:

۱- قانون آنسیترال امضای الکترونیکی را، «داده» معرفی کرده است بنابراین از تعریف قانون ایران پیشرفته تر است. ۲- قانون آنسیترال به دو کارکرد امضا یعنی؛ شناسایی امضا کننده و رضایت وی به مفاد سند توجه کرده است اما در قانون ایران تنها به شناسایی امضاکننده اشاره شده است. بهتر بود قصد التزام به مفاد سند نیز برای تکمیل تعریف ذکر

1. Art.2“ 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.

می‌گردید زیرا عنصر معنوی امضا در يك قرارداد، قصد التزام طرفین به مفاد سند است و در غیر این صورت امضا از هیچ ارزش حقوقی برخوردار نخواهد بود.

بند «ه» ماده ۲-۱۶۳۳ قانون مدنی ایالت کالیفرنیا چنین مقرر کرده است: «امضای الکترونیکی به معنی صدا، نماد یا فرآیند الکترونیکی است که شخصی آن را می‌پذیرد و ضمیمه مدارک الکترونیکی خود می‌کند». (California Government Code 2001, & 16.5d)

با نگاهی اجمالی به این تعریف و با عنایت به مطالب پیش گفته در می‌یابیم که قانونگذار هیچ گونه عنایتی به جنبه‌های حقوقی امضای الکترونیکی نداشته و صرفاً يك تعریف فنی از امضای الکترونیکی نموده است.

در بند ۷ ماده ۱۴ قانون نمونه دفاتر اسناد رسمی ایالات متحده، امضای الکترونیکی به معنی «هرگونه صدا، علامت یا فرآیند الکترونیکی است که به مدرک الکترونیکی با لحاظ شرایط علمی ضمیمه یا با آن همسان شده و این امضا از سوی شخصی که قصد پذیرش مدارک را دارد، زده شده یا به دستور و برای او طراحی شده است» (Model Notary Act 2002, & 14.7)

همان طور که ملاحظه می‌گردد، تعبیر فوق از امضای الکترونیکی، صرفاً يك تعبیر با رویکرد فنی از آن است. تنها عبارت «قصد پذیرش» تا حدودی دلالت بر جنبه حقوقی امضا دارد.

ماده ۲(۸) قانون ایالت یوتا مقرر می‌دارد: «امضای الکترونیکی عبارت از يك صدا، یا علامت یا فرآیند الکترونیکی است که به يك سند الکترونیکی متصل یا به طور منطقی منضم گردیده است و این کار توسط فردی به قصد امضای يك سند الکترونیکی انجام می‌شود» (UtahCode 1995 & 2.8)

همین تعریف در بند ۸ قسمت دوم قانون متحد الشكل معاملات الکترونیکی تکرار شده است (Uniform Electronic Transaction Act 1999, & 2.8) و همچنین در بند ۵ بخش ۱۰۶ قانون امضای الکترونیکی در قانون تجارت ملی و فرا ملی ایالت متحده نیز ذکر

شده است (ESIGN Act 2000, & 106.5)

در این تعریف نیز قانونگذار می‌توانست به جای عبارت «صدا و علامت» عبارت «داده» را به کار گیرد زیرا «داده» می‌تواند غیر از موارد فوق، موارد دیگری را نیز در برگیرد. نکته مهم آن است که در این تعریف به «قصد امضا» نمودن سند توجه شده است که این تعبیر دیگری از همان مفهوم «قصد التزام» به مفاد سند است.

در جای دیگری آمده است: «امضای الکترونیکی یک داده‌ای به شکل الکترونیکی است که به داده الکترونیکی دیگری متصل یا به نحو منطقی منضم شده و به منظور اثبات اصالت آن به کار می‌رود» (Anonymous 2001, p3).

این تعریف تنها به جنبه اثبات اصالت سند در صورت طرح ادعای جعل در مراجع حقوقی توجه کرده است و به سایر آثار مهم امضا که به آنها اشاره شد، توجهی نکرده است. همچنین در فرهنگ اصطلاحات «دفتر ارتباطات فدرال امریکا»^۱ آمده است: «امضای الکترونیکی یک شیوه فنی است که تضمین اصالت سند یا نامه الکترونیکی و هویت فرستنده پیام را ممکن می‌سازد» (Anonymous 2006).

در «دایره المعارف ویکیپدیا» آمده است: «اصطلاح امضای الکترونیکی عبارت است از یک روش امضای پیام که: پژوهشگاه علوم انسانی و مطالعات فرهنگی

الف) فرد خاصی را به عنوان فرستنده پیام شناسایی و تأیید می‌کند.

ب) رضایت او را نسبت به اطلاعات موجود در پیام نشان می‌دهد.» (Wikipedia 2008).

فرهنگ لغات حقوقی آکسفورد امضای الکترونیکی را چنین تعریف کرده است: «امضای الکترونیکی قسمتی از یک داده است که ملحق یا منضم به سند یا قراردادی است که به طور الکترونیکی و به منظور اثبات اصالت یک ارتباط ارسال شده است.» (Oxford 2001, p169). این تعریف نیز همچون تعاریف سابق جامع نیست و به همه کارکردهای امضا

1. Federal Office Of Communications.

توجهی نکرده است.

ماده ۴-۱۳۱۶ اصلاح قانون مدنی فرانسه مقرر می‌دارد: «امضای الکترونیکی در عمل عبارت از رویه قابل اعتمادی است برای شناسایی که رابطه امضا را با سندی که با آن مرتبط است تضمین می‌کند.» (زرکلام ۱۳۸۴، ص ۱۵۰). این تعریف علی‌رغم آنکه دو کارکرد مهم امضا را مورد توجه قرار می‌دهد، اما «امضای الکترونیکی» را «رویه» می‌نامد حال آنکه امضای الکترونیکی «داده»‌ای است که به يك سند الکترونیکی ملحق می‌گردد. ماده ۱-۲ دستورالعمل اتحادیه اروپا در زمینه امضای الکترونیکی بیان داشته است: «امضای الکترونیکی داده‌ای است به شکل الکترونیکی، که به سایر داده‌های الکترونیکی ضمیمه و یا منطقیاً متصل است و به عنوان روشی برای اثبات هویت به کار می‌رود» (Directive 1999, & 1.2).

از برآیند همه تعاریف ذکر شده می‌توان نکات ذیل را استنباط نمود و در تعریف امضای الکترونیکی مورد توجه قرار داد:

- ۱- امضای الکترونیکی يك داده الکترونیکی است که به يك داده الکترونیکی دیگر (سند یا قرارداد) متصل می‌شود.
- ۲- امضای ذیل سند که توسط خود شخص و یا به دستور او انجام می‌گیرد، برای شناسایی شخص امضا کننده به کار می‌رود.
- ۳- تصدیق محتوای سند و اعطای اثر حقوقی به آن یکی دیگر از کارکردهای امضای الکترونیکی است که باید مورد توجه قرار گیرد.

۴- آخرین و مهم‌ترین نکته این که، امضا به طور مطلق (الکترونیکی یا دستی) باید واجد يك عنصر معنوی به نام «قصد التزام به مفاد سند» باشد. این همان چیزی است که در واقع به يك امضا اثر حقوقی می‌بخشد. در نتیجه، در صورتی که فردی در طول يك فرآیند اقدام به كلیك کردن عبارت «من قبول دارم»^۱ کند بدون این که قصد التزام به مفاد

1. "I agree".

سند داشته باشد، امضا در معنای حقوقی شکل نگرفته است. به عنوان مثال، وقتی يك نفر از طریق پایگاه الکترونیکی يك فروشنده، کالا یا خدماتی را سفارش می‌دهد، آن فرد موظف است اطلاعاتی را که در قسمت‌های مختلف يك فرآیند، که در نهایت منجر به دریافت کالا یا خدمات می‌شود، ارایه دهد. وقتی آن شخص به مرحله آخر می‌رسد و عبارت «من قبول دارم» را کلیک می‌کند. آن فرآیند را با قصد ملحق شدن به سند انجام داده است. یعنی با پذیرفتن این فرآیند، انجام يك «عمل حقوقی» را قصد می‌کند و امضا نشانه آن است.

باتوجه به مطالب بیان شده به نظر می‌رسد می‌توان امضای الکترونیکی را چنین تعریف کرد: امضای الکترونیکی عبارت از داده‌ای است که به قصد التزام به مفاد يك داده پیام به آن ملحق یا منطقیاً به آن منضم شده است و موجبات شناسایی شخص و رضایت وی به مفاد داده پیام را فراهم می‌آورد و بنابراین از اعتبار حقوقی برخوردار است.

۲- انواع امضاهای الکترونیکی

در یک تقسیم بندی دیگر بر اساس ارزش اثباتی و سطح ایمنی فراهم شده، امضای الکترونیکی را به دو دسته ساده و مطمئن تقسیم می‌کنند. این تقسیم بندی در قوانین مختلف از جمله قانون نمونه آنسیترال (۲۰۰۱) و قانون تجارت الکترونیکی ایران بیان شده است.

۲-۱- امضای الکترونیکی ساده

در بند «ی» ماده ۲ قانون تجارت الکترونیکی ایران امضای الکترونیکی بدین گونه تعریف شده است: «امضای الکترونیکی عبارت است 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 می‌گیرد». همچنین بند «الف» ماده ۲ قانون نمونه آنسیترال (۲۰۰۱) نیز در تعریف این امضا آورده است: «امضای الکترونیکی به معنای داده الکترونیکی است که به یک داده پیام منضم، یا به نحو منطقی متصل شده است و برای شناسایی امضا کننده و

تأیید وی در خصوص اطلاعات موجود در داده پیام به کار می‌رود.^۱ شایان ذکر است که عبارت امضای الکترونیکی ساده به صراحت در مقررات فوق‌الذکر نیامده است اما با توجه به نوع مطمئن آن، عنوان امضای الکترونیکی ساده انتخاب شده است.

به نظر می‌رسد، اگر در تعریف قانون ایران همانند قانون نمونه آنسیترال، تأیید امضا کننده نیز از جمله آثار آن ذکر می‌شد، تعریف کامل و دقیق‌تری بود.

۲-۲- امضای الکترونیکی مطمئن^۲

ماده ۱۰ قانون تجارت الکترونیکی ایران که ناظر به بند «ک» ماده ۲ همان قانون است، در تعریف این نوع امضا می‌گوید: «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 کند.
- 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.^۳

همچنین در بند ۳ ماده ۶ قانون نمونه آنسیترال (۲۰۰۱) آمده است: «امضای الکترونیکی

1. Art2(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. Secure Electronic Signature.

3. Art6.3. "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".

قابل اعتماد باید دارای شرایط زیر باشد:

الف - داده ایجاد امضا به همراه مطلبی که در آن امضا مورد استفاده قرار می‌گیرد، مرتبط با شخص امضا کننده باشد و نه فرد دیگری.

ب - داده ایجاد امضا در زمان امضا، تحت کنترل امضا کننده باشد و نه فرد دیگری.

ج - هر گونه تغییری در امضا، بعد از زمان امضا، قابل کشف باشد.

د - در جایی که هدف از امضا حصول اطمینان در خصوص اصالت اطلاعات مرتبط با

امضا است، هر گونه تغییری در اطلاعات بعد از امضا، قابل کشف باشد.»

با مقایسه بندهای این دو ماده با یکدیگر دو نکته به دست می‌آید: اول اینکه بند «ب» ماده ۱۰ قانون تجارت الکترونیکی ایران در قانون نمونه آنسیترال معادلی ندارد. شاید علت این موضوع این است که وجود شرط مندرج در بند «الف» قانون ایران مبنی بر لزوم منحصر به فرد بودن امضا نسبت به امضاکننده، موجبات تعیین هویت او را نیز فراهم می‌کند و دیگر نیازی به ذکر بند «ب» نیست و به همین دلیل قانون نمونه تعیین هویت امضاکننده را از جمله شرایط امضای الکترونیکی بیان نکرده است.

نکته دوم آنکه بند «ج» قانون نمونه آنسیترال نیز در قانون تجارت الکترونیکی ایران معادلی ندارد و به نظر می‌رسد لازم بود این شرط نیز، که در خصوص اطمینان از عدم تغییرات بعدی در امضا است، مورد اشاره قرار می‌گرفت. اما قانونگذار ایران صرفاً اطمینان در خصوص عدم تغییرات بعدی در داده پیام را مورد اشاره قرار داده است.

شایان ذکر است که مقررات ایالات متحده آمریکا هیچ تفاوتی بین امضای الکترونیکی ساده و مطمئن قائل نشده است (E-sign Act 2000) این در حالی است که در دستورالعمل امضای الکترونیکی اتحادیه اروپا نوع دیگری از امضای الکترونیکی به نام «امضای الکترونیکی واجد شرایط»^۱ ذکر شده است و که این امضا در واقع همان امضای الکترونیکی مطمئن است که مبتنی بر گواهی یک مرجع رسمی دولتی باشد. (Directive

1999, Art.2)

این در حالی است که اگرچه در قانون تجارت الکترونیکی ایران نیز این رویکرد مورد لحاظ قرار گرفته است اما در آیین نامه اجرایی ماده ۳۲ این قانون امضای رقمی به عنوان امضای الکترونیکی قابل استفاده در نظر گرفته شده است.

اکنون سوالی که در ذهن مطرح می‌گردد این است که علت تقسیم امضا به انواع ساده و مطمئن در قانون تجارت الکترونیکی ایران و قانون نمونه‌ی آنسیترال (۲۰۰۱) چیست. پاسخ این سوال در بخش بعدی تحت عنوان «اعتبار حقوقی امضای الکترونیکی» آرایه می‌گردد.

۳- اعتبار حقوقی امضای الکترونیکی

یکی از موضوعات اساسی در ارتباط با موضوع حقوقی ارزش اثباتی^۱ آن است. به عبارت دیگر، قابلیت استناد در محاکم در صورت طرح دعوی در دادگاه، علت اصلی پرداختن به جنبه‌های حقوقی مسائل مبتلا به است. اطلاعات ذخیره شده در قالب‌های الکترونیکی ممکن است بنا به دلایل مختلف نگهداری و بازیابی گردند. یکی از این دلایل اقامه دعوی در محاکم است. اگر تاجری که معامله‌ای را در قالب تجارت الکترونیکی انجام داده مجبور به حضور در دعوی به عنوان خواهان یا خواننده شود، مطمئناً اسناد الکترونیکی، نقش بسیار مهمی به عنوان دلیل بر عهده خواهند داشت (Winn, "et, al" 2002, p20.2) پذیرش و ارزش اثباتی این اسناد الکترونیکی بستگی به اعتبار حقوقی امضای مندرج در آن دارد. همچنین اطمینان خاطر در خصوص اعتبار حقوقی امضای الکترونیکی یکی از عوامل اساسی در ارتباط با توسعه تجارت الکترونیکی است چرا که فقدان يك نظام حقوقی منسجم در ارتباط با امضای الکترونیکی امکان انجام معامله به روش الکترونیکی را برای بازرگانان مشکل می‌کند، زیرا قراردادهای تجاری الکترونیکی تحقق نمی‌یابد مگر اینکه امضای الکترونیکی، معتبر و لازم الاجرا باشد (parry and Moor and James 2008, p5) به عبارت دیگر سرعت و اطمینان که از لوازم

1. Evidentiary value.

توسعه تجارت است ایجاب می‌کند که بازرگانان این اطمینان را داشته باشند که در صورت طرح دعوا در دادگاه یا نزد داور، بتوانند به امضای الکترونیکی ذیل قراردادهای یا نامه‌های الکترونیکی استناد کنند و قضات و داوران آن را بپذیرند.

در این بخش به بررسی این موضوع خواهیم پرداخت که آیا به لحاظ قانونی، امضای الکترونیکی در محاکم یا مراجع اداری قابل استناد است. در صورت قابل استناد بودن، از چه میزان ارزش اثباتی برخوردار است؟ آیا بین انواع مختلف امضای الکترونیکی که در قانون به آنها اشاره شده (ساده، مطمئن) به لحاظ ارزش اثباتی وجود دارد؟ آیا امضای دستی و امضای الکترونیکی به لحاظ اثباتی از ارزش حقوقی یکسانی برخوردارند. این فصل از مقاله در صدد پاسخ‌گویی به این سوالات است. برای ورود به این مبحث ابتدا لازم است اصول حقوقی حاکم بر جنبه اثباتی امضای الکترونیکی مورد بررسی قرار گرفته، سپس به جزئیات مطالب بپردازیم.

۳-۱- اصول حقوقی حاکم بر جنبه اثباتی امضای الکترونیکی

۳-۱-۱- اصل پذیرش امضای الکترونیکی^۱

ماده ۱۲ قانون تجارت الکترونیکی مقرر می‌دارد: «اسناد و ادله اثبات دعوی ممکن است به صورت داده پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان بر اساس قواعد ادله موجود، ارزش اثباتی داده پیام را صرفاً به دلیل شکل و قالب آن رد کرد». این اصل در خصوص الزام پذیرش امضای الکترونیکی در محاکم است. به این معنی که قاضی باید امضای الکترونیکی را به عنوان دلیل پذیرفته آن را مورد بررسی قرار دهد، هر چند ممکن است پس از بررسی پرونده، صاحب امضای الکترونیکی قادر به اثبات موضوع دعوا نباشد. اما به هر حال نباید امضا را صرفاً به علت قالب الکترونیکی آن رد کند. این قاعده در ماده ۹ و ۵ قانون نمونه ۱۹۹۶ بیان شده است. بر اساس ماده ۹ «در هر اقدام حقوقی هیچ یک از قواعد اثبات دعوا نباید به گونه‌ای اعمال گردد که منجر به عدم پذیرش داده پیام به

1. Principle of Admissibility.

عنوان دلیل شود: الف - صرفاً به این دلیل که در قالب یک داده پیام است...^۱ و همچنین در ماده ۵ همان قانون آمده است: «اثر حقوقی، اعتبار و قابلیت اجرای اطلاعات نباید صرفاً به علت این که در قالب داده پیام است، مورد انکار قرار گیرد».^۲ همچنین در اکثریت قریب به اتفاق قوانین تجارت الکترونیکی سایر کشورها و دستورالعمل اتحادیه اروپا به عنوان يك اصل کلی مورد پذیرش قرار گرفته است (Alberts and van der hof 1999,p5)

۳-۱-۲- اصل برابری آثار^۳ (امضای دستی و امضای الکترونیکی)

همان طور که در مبحث کارکردهای امضای الکترونیکی مطرح شد، مطابق ماده ۷ قانون تجارت الکترونیکی ایران «هرگاه قانون، وجود امضا را لازم بداند امضای الکترونیکی مکفی است». این اصل در بند يك ماده ۶ قانون نمونه امضای الکترونیکی (۲۰۰۱) و بند يك ماده ۷ قانون نمونه تجارت الکترونیکی (۱۹۹۶) بیان شده است. مطابق این اصل، بین امضای دستی در اسناد کاغذی و امضای الکترونیکی به لحاظ آثار هیچ تفاوتی وجود ندارد.

۳-۱-۳- اصل عدم تبعیض^۴ (بین امضای الکترونیکی ساده و مطمئن)

اصل دیگری که در ارتباط با امضای الکترونیکی در حقوق تجارت الکترونیکی مطرح است قاعده عدم تبعیض بین امضای الکترونیکی ساده و امضای الکترونیکی مطمئن به لحاظ دارا بودن ارزش اثباتی و قابل پذیرش بودن در محاکم است. البته واضح است که ارزش اثباتی این دو نوع امضا با یکدیگر متفاوت است. به عبارت دیگر، همان طور که توضیح داده خواهد شد، ارزش اثباتی امضای الکترونیکی ساده کمتر از امضا مطمئن است اما این به آن معنا نیست که این نوع امضا فاقد ارزش است (Todd 2005,p116). اگرچه

1. Art. 9. Admissibility and evidential weight of data messages 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.

2. Art 5«Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message».

3. Principle of Functional Equivalents.

4. Principle of Non-Discrimination.

این اصل به صراحت در قانون تجارت الکترونیکی و قانون نمونه‌ی امضای الکترونیکی ذکر نشده است، اما از اطلاق ماده ۷ ق.ت.ا. و بند یک ماده ۶ قانون نمونه (۲۰۰۱) و بند یک ماده ۷ قانون نمونه تجارت الکترونیکی (۱۹۹۶) که عبارت «امضای الکترونیکی» را بدون هیچ‌گونه قیدی آورده است، قابل استنباط است. همچنین این قاعده از بند دوم ماده ۵ دستورالعمل اتحادیه اروپا نیز قابل استنباط است (Dumortier, n.d., p33).

۳-۱-۴- اصل در حکم نوشته بودن داده پیام

قبل از توضیح این اصل باید «داده پیام» را تعریف نمود. بند الف ماده ۲ ق.ت.ا. در تعریف داده پیام می‌گوید: «داده پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی نوری و یا فناوری‌های جدید اطلاعات، تولید، دریافت، ذخیره یا پردازش می‌شود». همچنین بند ج ماده ۲ قانون نمونه آنسیترال (۲۰۰۱) در تعریف داده پیام آورده است «داده پیام عبارت از اطلاعات ایجاد، ارسال، دریافت یا ذخیره شده از طریق وسایل نوری یا وسایل مشابه از جمله مبادله الکترونیکی داده‌ها، پست الکترونیکی، تلگراف، تلکس یا تله کپی است که توسط خود فرد شخصاً یا فردی از جانب او تولید می‌شود»^۱

در توضیح این اصل ماده ۶ ق.ت.ا. می‌گوید: «هرگاه وجود یک نوشته از نظر قانون لازم باشد، پیام در حکم نوشته است...». همچنین ماده ۶ قانون نمونه آنسیترال (۱۹۹۶) نیز با همین تعبیر اصل فوق را بیان کرده^۲ با این قید که «اطلاعات محتوی داده پیام برای ارجاعات بعدی قابل دسترسی باشد».

علت وضع این قاعده این است که قانونگذار قصد دارد با این مقرره همان بار اثباتی را برای داده پیام قائل شود که سند مکتوب در قوانین فعلی دارا است (اکبری ۱۳۸۴، ص ۸۲).

1. Art.2(c) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy? and acts either on its own behalf or on behalf of the person it represents "

2. Art.6(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

به عبارت دیگر، مطابق این اصل در صورتی که در قوانین جاری یا رویه قضایی، اطلاعاتی باید به صورت نوشته ارائه شود - یعنی در قالب اسناد کاغذی مکتوب - داده پیام که یک سند الکترونیکی است نیز، قابلیت استناد دارد (Guide to MLEC 1996, p35). در رویه قضایی نیز آرای در خصوص این اصل به شرح ذیل دیده می‌شود:

۱- در پرونده «کارلس سامپر پاسادا علیه جین تاپیاس»^۱ قاضی رای داد که در هر جایی که مقررات الزام می‌کند که اطلاعاتی به صورت نوشته باشد یک نامه‌ی الکترونیکی کافی است، مشروط به این که برای طرفین، امکان دسترسی به آن نامه در زمان بعد از ارسال وجود داشته باشد (Mason 2006).

۲- در پرونده‌ی «رادر علیه شرکت مایکروسافت»^۲ دادگاه اظهار داشت: به قراردادهای الکترونیکی منعقد شده از طریق کلیک کردن، همان اعتباری داده می‌شود که به قراردادهای نوشته (مکتوب) (Mason 2007).

شایان ذکر است مطابق قاعده «ما من عام الا و قد خص»^۳، اصل کلی در حکم نوشته بودن داده پیام نیز مطابق ادامه ماده ۶ ق.ت.ا. با استثنائاتی مواجه است. و موارد استثناء عبارتند از: «الف - اسناد مالکیت اموال غیر منقول ب - فروش مواد دارویی به مصرف‌کنندگان نهایی ج - اعلام، خطر، هشدار و یا عبارات مشابهی که دستور خاصی برای استفاده کالا صادر می‌کند و یا از به کارگیری روش‌های خاصی به صورت فعل یا ترك فعل منع می‌کند.»

بند ۳ ماده ۶ قانون نمونه تجارت الکترونیکی (۱۹۹۶) استثنائات این اصل را به قوانین داخلی کشورها واگذار کرده است، «با این قید که قوانین ملی کشورها حق ندارند استثنائات نامحدود بر این قاعده وضع کنند چرا که در غیر این صورت، امکان اعمال مقررات قانون نمونه فراهم نخواهد شد» (Guide to MLEC 1996, P37).

1. Carlos Samper Pasada v. Jaine Tapias.

2. Rudder v. Microsoft.

۳-۱-۵- اصل اصیل بودن داده پیام

سوالی که در این قسمت مطرح می شود این است که، در صورتی که خواهان یا خواننده به يك سند الکترونیکی به عنوان دلیل استناد کند و این سند مورد انکار یا تردید طرف مقابل (خواننده یا خواهان) واقع شود، آیا طبق قانون آیین دادرسی مدنی در صورت عدم ارایه اصل سند، دادخواست ابطال یا از عداد دلایل خارج خواهد شد؟ به عبارت دیگر در چنین محیطی آیا مفهومی به نام داده پیام اصل و فرع وجود دارد یا خیر؟^۱

ماده ۸ ق.ت.ا. می گوید «هرگاه قانون لازم بداند که اطلاعات به صورت اصل ارایه یا نگهداری شود، این امر با نگهداری و ارائه اطلاعات به صورت داده پیام نیز در صورت وجود شرایط زیر امکان پذیر می باشد:

الف - اطلاعات مورد نظر قابل دسترسی بوده و امکان استفاده در صورت رجوع بعدی فراهم باشد.

ب - داده پیام به همان قالبی (فرمتی) که تولید، ارسال و یا دریافت شده و یا به قالبی که دقیقاً نمایشگر اطلاعاتی باشد که تولید، ارسال و یا دریافت شده نگهداری شود.

ج - اطلاعاتی که مشخص کننده مبدأ، مقصد، زمان ارسال و زمان دریافت داده پیام می باشند نیز در صورت وجود، نگهداری شوند.

د - شرایط دیگری که هر نهاد، سازمان، دستگاه دولتی و یا وزارتخانه در خصوص نگهداری داده پیام مرتبط با حوزه مسئولیت خود مقرر نموده فراهم شده باشد.»

همچنین ماده ۸ قانون نمونه تجارت الکترونیکی (۱۹۹۶) در این زمینه مقرر می دارد:

«۱- هرگاه قانون مقرر کرده باشد که اطلاعاتی در شکل اصلی خود ارائه یا نگهداری شوند داده پیام، اصل محسوب می شود مشروط بر اینکه:

۱. ماده ۹۶ ق.آ.م: «خواهان باید اصل اسنادی که رونوشت آنها را ضمیمه دادخواست کرده است در جلسه دادرسی حاضر نماید. خواننده نیز باید اصل و رونوشت اسنادی را که می خواهد به آنها استناد کند در جلسه دادرسی حاضر نماید... و الا در صورتی که آن سند عادی باشد و مورد انکار و تردید واقع شود، اگر خواننده باشد از عداد دلایل او خارج می شود و اگر خواهان باشد و دادخواست وی مستند به ادله دیگری نباشد در آن خصوص ابطال می گردد».

الف - اطمینان کامل از تمامیت اطلاعات هنگامی که داده پیام برای اولین بار به صورت نهایی تولید شده است وجود داشته باشد.

ب - هرگاه ضرورت ارائه اطلاعات وجود داشته باشد، امکان نشان دادن اطلاعات به کسی که باید به او ارائه شود وجود داشته باشد.

۲- پاراگراف اول اعمال می شود خواه اینکه شرط مقرر در قالب يك تعهد قراردادی باشد یا صرفاً قانون، آثاری را برای اطلاعاتی که به صورت اصل ارائه یا نگهداری نشده بار می کند.

۳- برای اهداف بند فرعی (الف) از بند (۱):

الف - معیار ارزیابی تمامیت داده، حفظ کمال و عدم تغییر در آن خواهد بود. صرف نظر از اضافه کردن هر ظهنویسی (و تأیید) یا تغییری که در جریان معمول ارتباط، ذخیره یا نمایش اطلاعات روی می دهد.

ب - استاندارد قابلیت اعتماد^۲ با توجه به هدفی که از تولید اطلاعات مورد نظر است و سایر اوضاع و احوال، تعیین می شود.»

بنابراین از موارد فوق می توان نتیجه گرفت که داده پیام، اصل و فرع ندارد و همه نسخه ها و کپی ها یکسان هستند و داده پیامی که مستند دعوی قرار گرفته اصل تلقی می شود. از این رو، قانون تجارت الکترونیکی ایران و قانون نمونه تجارت الکترونیکی در صدد این هستند که موانعی را به بهانه اصل نبودن ممکن است در جریان استناد به اسناد الکترونیکی در دعوا مطرح شود بردارند (1996, p37 Guide to MIEC).

۳-۲- ارزش اثباتی داده پیام و امضای الکترونیکی

همان طوری که در مبحث قبل گفته شد یکی از تقسیم بندی های امضای الکترونیکی

۱. مطابق بند ۵ ماده ۲ ق.ت.ا «... اعمال ناشی از تصدی سیستم از قبیل ارسال، ذخیره یا نمایش اطلاعات که به طور معمول انجام می شود، خدشه ای به تمامیت داده پیام وارد نمی کند».

۲. منظور از استاندارد، سطحی از ایمنی است که با توجه به موضوع داده پیام باید رعایت شود. (شرح ماده به ماده لایحه قانونی تجارت الکترونیکی، ۱۳۸۲، ص ۱۹)

که در قوانین نیز به آن اشاره شده، تقسیم بندی امضای الکترونیکی به ساده و مطمئن است. علت این نوع تقسیم در قانون تجارت الکترونیکی ایران و قانون نمونه امضای الکترونیکی (۲۰۰۱) توان اثباتی امضای الکترونیکی است. به عبارت دیگر، قانون بر این اساس که امضای مندرج در یک سند الکترونیکی با کدام يك از این دو نوع امضا مطابقت داشته باشد برای آن ارزش اثباتی قائل است. منظور از ارزش اثباتی، تأثیر قانونی امضای انجام شده در سند در ایجاد اطمینان برای قاضی مبنی بر درستی ادعای شخصی است که به آن استناد می‌کند (شمس. عبدالله ۱۳۸۴، ص ۱۴۸).

توان اثباتی هر يك از امضاهای الکترونیکی ساده و مطمئن را باید در اسناد الکترونیکی مربوطه به طور مجزا بررسی کرد. در کتب حقوق تجارت الکترونیکی، اسناد الکترونیکی را با توجه به نوع امضای مندرج در آن به داده پیام ساده و مطمئن (معتبر) تقسیم می‌کنند. (اکبری، ۱۳۸۴) ما نیز بررسی ارزش اثباتی امضای الکترونیکی را با توجه به همین الگو انجام خواهیم داد.

۳-۲-۱- داده پیام و امضای الکترونیکی مطمئن^۱

طبق مفاد ماده ۱۱ ق.ت.ا، داده پیام مطمئن، داده پیامی است که با امضای مطمئن و با رعایت شرایط يك «سامانه اطلاعاتی مطمئن»^۲ ذخیره شده و به هنگام لزوم در دسترس باشد. امضای الکترونیکی مطمئن همان طوری که قبلاً اشاره شد،^۲ مطابق ماده ۱۰ ق.ت.ا، به امضای الکترونیکی اطلاق می‌شود که «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 يك داده پیام متصل شود که هر تغییری در آن داده پیام قابل تشخیص و کشف باشد».

اما در تعریف سامانه اطلاعاتی مطمئن در بند ح ماده ۲ ق.ت.ا، آمده است: سامانه

1. Secure Data message.

2. Secure Information system.

اطلاعاتی مطمئن، سامانه‌ای است که: «۱- به نحوی معقول در برابر سوء استفاده و نفوذ، محفوظ باشد. ۲- سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد. ۳- به نحوی معقول متناسب با اهمیت کاری که انجام می دهد پیکربندی و سازماندهی شده باشد ۴- موافق با رویه^۱ ایمن باشد».

رویه ایمن وفق بند «ط» همان ماده «رویه ای است برای تطبیق صحت ثبت داده پیام، منشأ و مقصد آن، با تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله محتوا و یا ذخیره سازی داده پیام از يك زمان خاصی. یک رویه ایمن ممکن است با استفاده از الگوریتم‌ها یا کدها، کلمات یا ارقام شناسایی، رمزنگاری، روش‌های تصدیق یا پاسخ برگشت و یا طرق ایمنی مشابه انجام شود.» به طور خلاصه در تعریف داده پیام مطمئن می‌توان گفت: داده پیام مطمئن داده پیامی است که با امضای الکترونیکی مطمئن، امضا شده باشد. در شرایط فعلی امضای رقمی^۲، امضای الکترونیکی مطمئن تلقی می گردد.

و اما در رابطه با ارزش اثباتی داده پیام مطمئن می‌توان گفت قاعده کلی مطابق ماده ۱۳ ق.ت.ا. این است که «ارزش اثباتی داده پیام‌ها با توجه به عوامل مطمئن از جمله تناسب روش‌های ایمنی به کار گرفته شده با موضوع و منظور مبادله داده پیام تعیین می‌شود.»

از عبارات ماده ۱۳ چنین استنباط می‌شود که، قانونگذار بررسی ارزش اثباتی داده پیام مطمئن را به قاضی محول کرده اما بلافاصله در ماده ۱۴ و ۱۵ ارزش اثباتی این نوع داده پیام را صراحتاً معین می‌کند. در نگاه اول به نظر می‌رسد که نوعی تعارض میان این مواد مشاهده می‌شود. زیرا ماده ۱۴ ق.ت.ا. می‌گوید «کلیه داده پیام‌هایی که به طریق مطمئن ایجاد و نگهداری شده‌اند از حیث محتویات و امضای مندرج در آن، تعهدات طرفین یا طرفی که تعهد کرده و کلیه اشخاصی که قائم مقام قانونی آنان محسوب می‌شوند، اجرای مفاد آن و سایر آثار، در حکم اسناد معتبر و قابل استناد در مراجع قضایی و حقوقی است.»

1. Secure Method.

2. Digital Signature.

و در ماده ۱۵ ق.ت.ا. آمده است «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.» از مقایسه این مواد با ماده ۱۲۹۲ ق.م. که می‌گوید «در مقابل اسناد رسمی یا اسنادی که اعتبار اسناد رسمی را دارد، انکار و تردید مسموع نیست و طرف می‌تواند ادعای جعلیت نسبت به اسناد مزبور کند یا ثابت نماید که اسناد مزبور به جهتی از جهات قانونی از اعتبار افتاده است»، چنین استنباط می‌شود که قانونگذار درصدد است داده پیام و سند الکترونیکی مطمئن را به لحاظ ارزش اثباتی (و نه اجرایی) معادل اسناد رسمی قرار دهد هر چند صراحتاً به این مسأله اشاره نکرده و صرفاً عبارت «در حکم اسناد معتبر و قابل استناد» را برای این دسته از اسناد الکترونیکی استعمال کرده است که البته استعمال این عبارت با توجه به مبهم بودن آن مورد ایراد است.

ظاهراً قانونگذار نمی‌خواسته اسناد الکترونیکی مطمئن را به لحاظ همه آثار در حکم اسناد رسمی به حساب آورد؛ از این‌رو، متن پیش‌نویس قانون را که در آن تصریح به «در حکم اسناد رسمی» شده بود تغییر داده است. گویا قانونگذار تنها قصد داشته ارزش استناد به این اسناد الکترونیکی را در محاکم بپذیرد بنابراین تصریح کرده که قابل انکار و تردید نیست.

بنابراین با عنایت به تعارض بدوی ماده ۱۳ با مواد ۱۴ و ۱۵ قانون تجارت الکترونیکی از يك سو، و با مقایسه مواد ۱۴ و ۱۵ قانون مذکور و ماده ۱۲۹۲ قانون مدنی از سوی دیگر، دو سؤال در ذهن مطرح می‌گردد، نخست آنکه اگر قانونگذار در ماده ۱۳ ارزش اثباتی داده پیام را به طور کلی به «عوامل مطمئنه» و قابلیت اطمینان روش‌های ایمنی مورد استفاده واگذار نموده و به عبارت دیگر، تعیین ارزش اثباتی داده پیام الکترونیکی را به عنوان دلیل، به قاضی محول می‌کند، چرا بلافاصله در مواد ۱۴ و ۱۵ ارزش اثباتی داده پیام مطمئن را دقیقاً مشخص کرده است؟ دوم آنکه قانونگذار چگونه و با چه پشتوانه قانونی ارزش اثباتی اسناد رسمی را برای داده پیام مطمئن در نظر گرفته است به عبارت دیگر، چگونه قانونگذار

بدون عنایت به شرایط ماده ۱۲۸۷ قانون مدنی^۱ در رابطه با سند رسمی، این دو نوع سند را از حیث اعتبار استناد معادل یکدیگر دانسته است؟ در پاسخ می‌گوئیم هیچ یک از دو اشکال فوق وارد نیست.

زیرا با مقایسه ماده ۱۳ ق.ت.ا. با مواد ۱۴ و ۱۵ ق.ت.ا. می‌توان گفت: ماده ۱۳ ق.ت.ا. از بند ۲ ماده ۹ قانون نمونه تجارت الکترونیکی (۱۹۹۶) اقتباس شده که در خصوص ارزش و توان اثباتی داده پیام می‌گوید: «...۲. اطلاعات موجود در داده پیام از ارزش اثباتی برخوردار است. در ارزیابی ارزش اثباتی يك داده پیام، باید به قابلیت اطمینان روشی که از طریق آن داده پیام تولید، ذخیره یا ارسال شده توجه کرد، همچنین به قابلیت اطمینان روشی که طی آن تمامیت اطلاعات حفظ شده، و به روشی که از طریق آن هویت ارسال کننده معین می‌شود و به سایر عوامل مرتبط عنایت کرد.»^۲ مطابق این ماده، قانون نمونه تجارت الکترونیکی تعیین ارزش اثباتی داده پیام و امضای الکترونیکی را دقیقاً معین نکرده و این موضوع را با توجه به اوضاع و احوال قضیه بر عهده قاضی پرونده قرار داده است. بنابراین به نظر می‌رسد برای رفع اشکال بدوی می‌توان گفت: با توجه به اینکه ارزش اثباتی داده پیام مطمئن در مواد ۱۴ و ۱۵ ق.ت.ا. معین شده ولی هیچ ماده قانونی به ارزش اثباتی داده پیام عادی (ساده) اشاره نکرده است، ماده ۱۳ ق.ت.ا. منصرف از داده پیام مطمئن بوده، به ارزش اثباتی داده پیام ساده و امضای الکترونیکی ساده اشاره دارد. در واقع به لحاظ اصولی حکم خاص مقرر در مواد ۱۴ و ۱۵ ق.ت.ا. حکم عام ماده ۱۳ ق.ت.ا. را تخصیص می‌زند. بدین معنا که در صورت احراز شرایط ماده ۱۰ قانون تجارت الکترونیکی مبنی بر مطمئن بودن امضای الکترونیکی، قاضی موظف است مطابق مواد ۱۴ و ۱۵ قانون اقدام به

۱. ماده ۱۲۸۷ ق.م. «اسنادی که در اداره ثبت اسناد و املاک یا دفاتر اسناد رسمی و یا در نزد سایر

مأمورین رسمی در حدود صلاحیت آنها و بر طبق مقررات قانونی تنظیم شده باشند رسمی است.»

2. Art.9 (2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

صدور رأی کند.

اما در باره متفاوت یا یکسان بودن داده پیام مطمئن و سند رسمی به لحاظ ارزش اثباتی اگر چه ممکن است اعطای چنین اثری به امضای الکترونیکی مطمئن و داده پیام مطمئن اغراق آمیز به نظر برسد، ولی دقت در ویژگی‌های امضای الکترونیکی مطمئن که ماده ۱۰ قانون تجارت الکترونیکی به آن اشاره دارد، شناسایی چنین اثری را برای این نوع امضا کاملاً توجیه می‌کند (زرکلام ۱۳۸۳، ص ۴۹). چرا که امضای الکترونیکی مطمئن، منحصر به فرد است و منحصر به فرد بودن نسبت به امضا کننده به این معنا است اولاً هیچ فرد دیگری نمی‌تواند چنین امضایی را ایجاد کند و ثانیاً امضا کننده قادر به انکار انتساب امضا به خود نمی‌باشد (شکوری مقدم، ۱۳۸۴، ص ۷۶).

بنابراین با توجه به این نکات، مواد ۱۴ و ۱۵ ق.ت.ا. از این جهت که داده‌های امضای الکترونیکی مطمئن و داده‌های منضم به آن را از حیث برخی آثار در حکم سند رسمی دانسته با منطق حقوقی سازگار است. به علاوه، اگر دلایل الکترونیکی مطمئن را صرفاً از نظر قابلیت استناد و نه از جهت قابلیت اجرا توسط دفاتر اسناد رسمی و اداره ثبت، در حکم سند رسمی بدانیم، این تدبیر مانع از آن خواهد شد که چنین دلیلی به راحتی مورد انکار و تردید قرار گیرد و در نتیجه استنادکننده به دلایل الکترونیکی، هر بار مجبور باشد صحت و اعتبار آن را اثبات کند. امری که نه تنها موجب کاهش دامنه مبادلات و تجارت الکترونیکی می‌شود بلکه موجب اطاله دادرسی و صرف وقت و هزینه خواهد شد (زرکلام ۱۳۸۲، ص ۲۹۹).

برخی در خصوص اعطای اثر اسناد رسمی به داده پیام مطمئن و امضای الکترونیکی مطمئن گفته‌اند: «ماده ۱۵ ق.ت.ا. اثر حقوقی خاصی را برای امضای الکترونیکی مطمئن قائل شده است که با موازین و اصول حقوقی حاکم بر ادله اثبات دعوی مطابقت دارد. زیرا شرایطی که برای امضای الکترونیکی مطمئن در ماده ۱۰ ق.ت.ا. در نظر گرفته شده است، تنها در معتبر شناخته شدن آن امضا موثر است، نه اینکه ارزشی هم سنگ امضایی که نزد

مأمور رسمی دولت انجام شده داشته باشد» (السان، ۱۳۸۵، ص ۱۲۷).

به عبارت دیگر، مقصود از داده پیام و امضای الکترونیکی مطمئن، مدرکی است که قابل انکار و تردید نباشد. در همین راستا برخی حقوقدانان خارجی معتقدند امضای الکترونیکی مطمئن صرفاً آماره‌ای است مبنی بر هویت، تمامیت و رضایت، و تا زمانی معتبر است که خلاف آن اثبات نشده باشد (Todd 2005, p116). همچنین قانون تجارت الکترونیکی سنگاپور، امضای الکترونیکی مطمئن را صرفاً آماره‌ای قانونی تلقی کرده است (Todd 2005, p119).

در راستای بیان ارزش اثباتی امضای الکترونیکی مطمئن و بررسی مواد ۱۴ و ۱۵ ق.ت.ا. در مقایسه با ماده ۱۲۹۲ ق.م. و ارایه نظریه‌ای بینابین می‌توان گفت: اگر چه نحوه ایجاد امضای الکترونیکی مطمئن، که در حال حاضر يك امضای رقمی و مبتنی بر رمزنگاری کلید عمومی است، چنان اعتباری به امضای الکترونیکی مطمئن و داده‌های منضم به آن اعطا می‌کند که نه تنها کلیه آثار مادی امضای دستی از قبیل دوام، اصالت، منحصر به فرد بودن، و تعیین هویت امضا کننده را در آن می‌توان یافت و حتی چنین امضایی با توجه به مسائل فنی، کمتر از امضای دستی بر روی اسناد کاغذی در معرض جعل و تغییرات است، اما مسأله اساسی در ارتباط با اسناد رسمی و برخورداری آن از چنان ارزش اثباتی به علت آن است که قانونگذار «برای پشتیبانی این بخش از قانون ادله اثبات مدنی، به نحوی که بتواند فحواى ماده ۱۲۹۰ ق.م. را در عمل با درجه‌ای معقول و مقبول از اطمینان به ظهور برساند، مجموعه‌ای وسیع از قوانین پشتیبان را وضع کرده است که به طور روشمند برای مستند ساختن اطلاعات در اسناد رسمی عمل می‌کند. مواد مربوط به اسناد رسمی در قانون مدنی، توسط قوانین مفصلی همچون قانون ثبت اسناد و املاک و قوانین مربوط به دفاتر اسناد رسمی و بخشی از آیین دادرسی مدنی پشتیبانی می‌شود و بدون وجود این قوانین پشتیبان، هرگز از چنین قدرت اثباتی در مبادلات اداری، قضایی و حقوقی برخوردار نمی‌شد»

و به منظور تلاش در راستای هماهنگ سازی اسناد کاغذی و الکترونیکی، با توجه به اصول حاکم بر ارزش اثباتی امضای الکترونیکی می توان گفت: با توجه به اصل در حکم نوشته بودن داده پیام و اصل برابری آثار امضای دستی و امضای الکترونیکی و با عنایت به ماده ۴ ق.ت.ا. که می گوید: «در مواقع سکوت و یا ابهام باب اول این قانون، محاکم قضایی باید بر اساس سایر قوانین و رعایت چهار چوب فصول و مواد مندرج در این قانون قضاوت نمایند»، امضا در واقع از ماهیتی یکسان برخوردار است و الکترونیکی یا کاغذی بودن آن تأثیری در مقررات حاکم بر آن ندارد. همچنین سند نیز چه الکترونیکی و چه کاغذی هر دو یکسان بوده به لحاظ ارزش اثباتی همانند یکدیگرند و می توان گفت همان طوری که اسناد کاغذی به عادی و رسمی تقسیم می شوند، اسناد الکترونیکی نیز قابل تقسیم به عادی و رسمی هستند و مقررات یکسانی بر آنها حاکم است و امضای الکترونیکی مطمئن نیز می تواند امضای رسمی تلقی شود مشروط به این که مقررات مربوط به ماده ۱۲۸۷ ق.م. در مورد آن رعایت شده باشد. به عبارت دیگر باید تمام تشریفات مربوط به تنظیم اسناد رسمی شامل تنظیم در نزد مأمور دولتی و با رعایت مقررات و در حیطه اختیارات، نیز در مورد این نوع از اسناد و امضای الکترونیکی رعایت گردد. البته واضح است که قالب و شکل متفاوت اسناد الکترونیکی مستلزم رعایت اصول فنی مربوط به خود است. به عبارت دیگر، همان طوری که اسناد رسمی در دفاتر اسناد رسمی و به شیوه رایج به ثبت می رسند، اسناد الکترونیکی رسمی نیز باید در دفاتر اسناد رسمی الکترونیکی مخصوص به خود و با رعایت مقررات فنی و تخصصی خود به ثبت برسند.

۳-۲-۲- داده پیام و امضای الکترونیکی ساده

همچنان که قبلاً اشاره شد، نوع دیگری از امضای الکترونیکی، امضای الکترونیکی ساده است. در واقع امضای الکترونیکی ساده، آن امضایی است که شرایط امضای الکترونیکی مطمئن را دارا نباشد ولی از مصادیق مفهوم امضای الکترونیکی مقرر در

بند «بی» ماده ۲ ق.ت.ا. و بند «الف» ماده ۲ قانون نمونه امضای الکترونیکی آنسیترال ۲۰۰۱ محسوب می‌شود. در خصوص قابل پذیرش بودن امضای الکترونیکی ساده به عنوان امضا در مبادلات الکترونیکی می‌توان از اطلاق ماده ۷ ق.ت.ا. که می‌گوید: «هرگاه قانون، وجود امضا را لازم بداند امضای الکترونیکی مکفی است» استفاده نمود.^۱

همچنین ماده ۹ قانون نمونه تجارت الکترونیکی آنسیترال ۱۹۹۶ از يك سو مقرر می‌دارد که امضای الکترونیکی اعم از ساده یا مطمئن به این دلیل که به صورت داده پیام است نباید مردود اعلام شود و از سوی دیگر برای امضای الکترونیکی ساده و مطمئن قائل به قدرت اثباتی است که بر اساس قابلیت اطمینان روش ایجاد امضا، نگهداری و ارسال پیام، حفظ تمامیت اطلاعات، هویت ارسال کننده و سایر موارد، ارزیابی می‌شود (MLEC, art 9, 1996). دستورالعمل مورخ ۱۲ دسامبر ۱۹۹۹ اتحادیه اروپا نیز در ماده ۵ خود تحت عنوان «آثار حقوقی امضای الکترونیکی» در بند ۲ کشورهای عضو را موظف می‌سازد که برای امضای الکترونیکی ساده نیز ارزش اثباتی قائل شوند و آنها را از این که چنین امضایی را به دلیل مطمئن نبودن مردود اعلام کنند، منع می‌کند (Directive 1999, art 5). بنابراین هر چند بعضی معتقدند ماده ۷ ق.ت.ا. نمی‌تواند منصرف به امضای الکترونیکی ساده باشد و با توجه به ماده ۱۰ ق.ت.ا.، ماده ۷ صرفاً امضای الکترونیکی مطمئن را مدنظر داشته است (رضایی، ۱۳۸۶، ص ۱۲۶)، اما دلیلی برای توجیه این تبعیض وجود ندارد زیرا می‌توان امضای الکترونیکی ساده را مانند امضای دستی در اسناد عادی مورد استفاده قرار داد. به عبارت دیگر نیازی نیست که در يك ارتباط الکترونیکی حتماً امضای الکترونیکی مطمئن استفاده شود بلکه، امضای الکترونیکی ساده مانند نام شخص در ذیل يك نامه الکترونیکی یا يك امضای اسکن شده در يك سند الکترونیکی نیز، از ارزش اثباتی برخوردار است. البته واضح است که ارزش اثباتی این نوع امضا کمتر از امضای الکترونیکی مطمئن است اما این به آن معنا نیست که ابداً ارزش اثباتی نداشته باشد. این موضوع را تحت

عنوان اصل «عدم تبعیض» در جای خود مورد بررسی قرار دادیم.

در خصوص میزان ارزش اثباتی این نوع امضا، بر خلاف امضای الکترونیکی مطمئن ماده‌ای که صراحتاً اختصاص به این موضوع داشته باشد در قانون تجارت الکترونیکی ایران وجود ندارد. ولی همان طوری که در قسمت قبل گفته شد، از اطلاق ماده ۱۳ ق.ت.ا. می‌توان استنباط کرد که ارزش اثباتی این نوع امضا بستگی به میزان اطمینان روش‌های ایمنی به کار رفته با توجه به اهمیت موضوع و منظور مبادله داده پیام دارد. به عبارت دیگر، برای تعیین ارزش اثباتی امضای الکترونیکی ساده نوعاً دخالت قاضی تعیین کننده است که به اوضاع و احوال هر قضیه توجه کند. البته با توجه به اصل برابری آثار امضای دستی و امضای الکترونیکی و اصل در حکم نوشته بودن داده پیام می‌توان استنباط کرد که داده پیام عادی نیز مانند سند عادی است یعنی همان طوری که امضای دستی عادی در اسناد عادی قابل انکار و تردید است و پس از اثبات اصالت آن در دادگاه، اعتبار سند رسمی را دارا می‌شود (ماده ۱۲۹۱ ق.م.ا)، امضای ساده در داده پیام عادی نیز قابل انکار و تردید است و در صورتی که اصالت آن در دادگاه اثبات گردد اعتبار امضای الکترونیکی مطمئن را می‌یابد. مفهوم مخالف مواد ۱۴ و ۱۵ ق.ت.ا. نیز مؤید همین امر است. به علاوه، مطابق ماده ۴ ق.ت.ا. در هر موردی که ابهام و سکوت در قانون وجود داشته باشد باید به قوانین موضوعه مراجعه کرد و مقایسه امضای دستی عادی و امضای الکترونیکی ساده در آثار و احکام ما را به این نتیجه رهنمون می‌کند.

بنابراین از مطالب فوق چنین استنباط می‌شود که، از نظر ارزش اثباتی داده پیام به دو گروه تقسیم می‌شود؛ یکی داده پیام عادی که به طریق غیر مطمئن و با امضای الکترونیکی ساده ایجاد شده است؛ نسبت به این گونه داده پیام انکار و تردید مسموع است و ارزش اثباتی آن مانند اسناد عادی است. دوم داده پیامی که به طریق مطمئن و با امضای الکترونیکی مطمئن ایجاد شده و از لحاظ محتویات و امضا دارای اعتبار کامل است. یعنی انکار و تردید در مورد آن مسموع نیست و تنها می‌توان ادعای جعل را مطرح

کرد که آن هم نیاز به اثبات دارد.

نتیجه گیری

از مجموع مطالب فوق به دست می آید که، از نظر ارزش اثباتی، داده پیام به دو نوع تقسیم می شود یکی داده پیام عادی که به طریق غیر مطمئن و با امضای الکترونیکی ساده ایجاد شده است: نسبت به این گونه داده پیام انکار و تردید مسموع است و ارزش اثباتی آن مانند اسناد عادی است. دوم داده پیام مطمئن که با امضای الکترونیکی مطمئن ایجاد می شود و از لحاظ ارزش اثباتی (و نه قابلیت اجرا) در حکم سند رسمی است یعنی انکار و تردید در مورد آن مسموع نیست و مدعی تنها می تواند ادعای جعلیت امضا را مطرح کند که آن هم نیاز به اثبات دارد البته سند الکترونیکی مطمئن می تواند به طور کامل (هم از لحاظ ارزش استناد و هم از لحاظ قابلیت اجرا) در حکم اسناد رسمی باشد ولی این مشروط است بر اینکه مقررات مربوط به ماده ۱۲۸۷ ق.م. که لزوم تنظیم این سند و امضای آن را نزد مأمور رسمی و طبق مقررات و در حدود اختیارات وی، را مقرر داشته رعایت شود.

نتیجه دیگری که این مقاله بدان دست یافت این است که قانونگذار ایران در مواد ۱۴ و ۱۵ ق.ت.ا. به دنبال ایجاد يك راهکار جدید قانونی در کنار دفاتر اسناد رسمی برای تولید سند رسمی نبوده است بلکه با هدف توسعه تجارت الکترونیکی، صرفاً يك اماره قانونی را به رسمیت شناخته است. به عبارت دیگر، قانون می گوید سند الکترونیکی حاوی امضای الکترونیکی مطمئن دلالت بر هویت، تمامیت و رضایت امضاکننده به مفاد سند دارد مگر اینکه خلاف آن ثابت شود. مطمئن بودن امضا هم به وسیله کارشناسان رایانه قابل احراز است و در صورت بروز اختلاف و طرح دعوا، قاضی دادگاه چنانچه خود اطلاعات فنی نداشته باشد می تواند از کارشناسان رسمی استعلام کند.

منابع

- اکبری، محسن، (۱۳۸۴)، *بررسی موانع حقوقی توسعه خرید و فروش الکترونیکی در ایران*، تهران، نشر موسسه مطالعات و پژوهش‌های بازرگانی.
- شکوری مقدم، محسن، (۱۳۸۴)، *حقوق تجارت الکترونیکی*، تهران، نشر ذره.
- شمس، عبد الله، (۱۳۸۴)، *آیین دادرسی مدنی (جلد سوم)*، تهران، نشر دراک.
- قاجار، سیامک و ذریانی، حسن و صالح خو، رامین، (۱۳۸۳)، *بررسی کلی نیازهای سیستماتیک نظام قضایی ایران برای تحقق تجارت الکترونیکی*، تهران، مرکز ملی شماره‌گذاری کالا و خدمات ایران.
- السان، مصطفی، (۱۳۸۴)، *ابعاد حقوقی بانکداری الکترونیکی*، مجله پژوهش‌های حقوقی، شماره ۷، ص ۲۰۹-۱۸۵.
- السان، مصطفی، (۱۳۸۵)، *ثبوت اسناد و فناوری اطلاعات، تلاقی سنت و نوآوری*، ماهنامه حقوقی کانون سردفتران و دفتریاران، شماره ۶۴، ص ۱۲۱-۱۴۲.
- زرکلام، ستار، (۱۳۸۲)، *امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوا*، مجله مدرس، شماره ۱، ص ۵۵-۳۳.
- زرکلام، ستار، (۱۳۸۳)، *قانون تجارت الکترونیکی و الفبای الکترونیکی* در مجموعه مقالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضاییه، ص ۲۸۵-۳۰۳، تهران.
- زرکلام، ستار، (۱۳۸۴)، *مقررات حقوق فرانسسه راجع به فضای سایبر*، در سید محمد رضا، صدری و محمد تقی، گروبی، *ابعاد حقوقی محیط سایبر در پرتو توسعه ملی*، ص ۱۵۶-۱۳۱، تهران.
- رضایی، علی، (۱۳۸۶)، *بررسی حقوقی عهدنامه سازمان ملل متحد درباره استفاده از ارتباطات الکترونیکی در قراردادهای بین‌المللی*، پایان نامه کارشناسی ارشد، دانشکده حقوق، دانشگاه شهید بهشتی
- قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی.*
- قانون تجارت الکترونیکی مصوب ۱۳۸۴/۱۰/۱۷*
- قانون مدنی*

Alberts, Babette and Van Der Hof, Simone. (1999). Digital Signature Blindness, analysis of legislative approaches toward electronic authentication, Retrieved 2007 From <http://www.cwis.kub.nl/frw/people/hof/ds.html>

Bahasin, Madan lal. (2006). Electronic Signature: An Analysis of

- European and International Legal Regulation. Retrieved 2008, From www.bath.ac.uk/management/research/papers.html. P.1481-1489
- DIRECTIVE 1999/93/EC of 13 December 1999 on a Community framework For Electronic Signatures. Retrieved 2008, From <http://www.eiropa.eu/geninfo/query/resultaction.jsppage>
- Dumortier, Jos. (n.d.). The European Directive 1999/93/EC on Community Framework For Electronic Signatures. Kluwer Law International. vol 14, p.33-65.
- Mason, Stephen. (2007). Electronic Signatures In Law. London: tottel publishing.
- Mason, Stephen. (2006). Electronic Signature In Practice. Retrived 2008/4/20 From <http://www.law.suffolk.edu/highlights/stuorgs/jht/publications/v6n2/mason.pdf>
- Parry, G.C. and Moore, M. James and Graves, A.P. and Altinoh, O. (2008). Legal Aspects of Electronic Signatures. Retrieved 2008, From <http://www.bath.ac.uk/management/research/papers.html>
- Todd, Paol. (2005). E-Commerce Law. London. Cavendish publishing limited
- Winn, k. Jane and Writht, Benjamin. (2002). The Law of Electronic Commerce. New york: Aspen Law & Business.
- UNCITRAL Model Law On Electronic Commerce with Guide to Enactment. (1996). Retrieved 2007, From <http://www.uncitral.org/english/texts/elecom/ml.html>.
- UNCITRAL Model Law On Electronic Signature with Guide to Enactment. (2001). Retrieved 2008, From <http://www.uncitral.org/english/texts/eletsig/ml-esign.html>

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی