مقاله

شاپا

مجلهٔ

پژوهشهای حقوقی

فصلنامه علمی ـ ترویجی

شماره ۳۴

هزار و سیصد و نود و هفت ـ تابستان

شهر دانش

مؤسسه مطالعات و پژوهشهای حقوقی

http://jlr.sdil.ac.ir/article_67510.html

قابلیت انتساب ادله الکترونیک

دکتر ایرج بهزادی*

چکیده:

در هزاره سوم تقریباً هیچ امری باقی نمانده که به طور مستقیم یا با واسطه به فناوری‌های نوین اطلاعاتی و ارتباطی، وابسته نباشد. به منظور ایمن‌سازی و اطمینان در تشخیص اصالت امضای الکترونیک، همچنین اثبات رابطه انتساب بین اصل‌ساز و داده‌پیام، متخصصین علوم رایانه‌ای دست به ابداع دو فن در این رشته زده‌اند: اولی، رمزنگاری متقارن یا سایمتریک که دارای کلید واحد تا حدودی اطمینان‌بخش است و امضای الکترونیک با این شیوه قابلیت انتساب به صادرکننده را دارد؛ دومی، رمزنگاری به شیوه نامتقارن است که از یک الگوریتم برای ایجاد دو کلید ریاضی مرتبط و مکمل استفاده می‌شود. این نوع رمزنگاری، سطح مطلوب‌تری از امنیت را برخوردار بوده، احتمال جعل و تحریف در آن وجود ندارد و از حیث قابلیت انتساب به صادرکننده اطمینان‌بخش‌تر است.

به لحاظ قابلیت انتساب در ادله الکترونیک، ضمن بررسی مفهوم امضای الکترونیک، آن را به دو نوع امضای الکترونیکی ساده و مطمئن تقسیم نموده است. امضای الکترونیکی ساده همانند امضای مندرج در اسناد عادی قابل انکار و تردید است اما امضای الکترونیکی مطمئن مانند سند رسمی صرفاً از قابلیت ادعای جعل برخوردار است و هر دو با رعایت شرایط، اصول و قواعدی قابل انتساب به اصل‌ساز هستند.

کلیدواژه‌ها:

دلیل الکترونیک، قابلیت انتساب، امضای الکترونیک، رمزنگاری متقارن، رمزنگاری نامتقارن.

مجلهٔ پژوهشهای حقوقی (فصلنامه علمی - ترویجی)، شمارهٔ ۳۴، تابستان ۱۳۹۷
صفحهٔ ۵۵-۷۰، تاریخ وصول: ۱۳۹۲/۱۰/۰۴، تاریخ پذیرش: ۱۳۹۳/۰۷/۰۸

* دانش‌آموخته دکترای حقوق خصوصی، دانشکده حقوق، دانشگاه آزاد اسلامی واحد تبریز
Email: Dr.behzadi2000365@yahoo.com

مقدمه

در خصوص دلایل و اسناد مطروحه در دعاوی، سندی قابل اتکاست که بتوان علیه شخص یا اشخاص حقیقی و حقوقی به آن استناد نمود و این سند زمانی علیه شخص سندیت دارد که ذیل سند امضاء و یا اثر انگشت باشد؛ بنابراین اصل بر این است که خطوط و عبارات نوشته مربوط به کسی است که ذیل آن را امضاء نموده است، یعنی شرط کامل بودن سند، امضائی است که بتوان آن را به امضاءکننده منتسب کرد؛ بنابراین معنا و مفهوم امضای ذیل سند این است که آن شخص (صاحب امضاء) صحت سند را قبول دارد و به آثار حقوقی و قانونی سند تسلیم است. حال اگر کسی صدور امضاء از ناحیه خود را در ذیل سند پذیرفت، مدلول سند تا اثبات خلاف، علیه او دلیل و حجت است. تعریفی که در خصوص گواهی الکترونیکی در بند (ب) ماده ۲ قانون آنسیترال عنوان گردیده به این شرح است: «گواهی، داده‌پیام یا سند دیگری است که پیوند بین امضاءکننده و امضاء ایجادشده در داده‌پیام را تأیید می‌کند.»

در تعریف گواهی الکترونیکی در بند ۳ از ماده ۲ قانون آلمان، این گواهی را سندی دیجیتالی مشمول یک امضای دیجیتالی معرفی نموده که برای واگذاری کلید امضاء به یک شخص حقیقی مناسب است و ماده ۲ مصوبه امضای الکترونیکی فرانسه نیز این گواهی را به عنوان تأییدیه‌ای که داده‌های مربوط به کنترل امضاء را به شخص معینی منتسب می‌سازد، معرفی می‌کند.[۱]

بحث امضای الکترونیکی در سطح بین‌المللی، اولین 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 کارگروه تجارت الکترونیکی آنسیترال، با امضای الکترونیکی نیز اصالت سند و انتساب آن به امضاءکننده، اثبات و وی متعهد به محتوای سند خواهد بود.[۲] اهمیت موضوع امضاء در تجارت الکترونیک سبب شد تا آنسیترال در سال ۲۰۰۱، قانون نمونه جداگانه‌ای را در مورد امضاءهای الکترونیکی در ۱۲ ماده به تصویب برساند.

---

۱. محمدرضا ملک‌آرا، «قانون قابل اعمال در تجارت الکترونیکی ایران و فرانسه» (پایان‌نامه کارشناسی ارشد، تهران: دانشگاه علامه طباطبائی، ۱۳۸۶)، ۲۳.

2. H.Raymond Anjanette, Electronic Commerce and the New Uncitral Draft *Convention*," *The Computer & Internet Lawyer Journal* 23 (August 2006): 11.

نظر به ضرورت تشخیص انتساب و رابطه دلیل الکترونیک با ایجادکننده آن و به منظور اطمینان از اصیل بودن امضاء، مطالب این مقاله در دو مبحث ارائه می‌شود. مبحث اول شامل تعریف، عناصر و انواع امضای الکترونیک و مبحث دوم انتساب در ادله الکترونیک را دربر می‌گیرد.

۱- تعریف امضای الکترونیک و انواع آن

از آنجایی که موضوع اصلی رابطه انتساب در ادله الکترونیکی را امضاء اصل‌ساز تشکیل می‌دهد، این مبحث به دو قسمت تقسیم می‌شود. قسمت اول شامل تعریف امضای الکترونیک و قسمت دوم انواع امضای الکترونیک را دربر گرفته است.

۱-۱- تعریف امضای الکترونیک

قانون‌گذاران و حقوقدانان تعابیر مختلفی را در تعریف این نوع از امضاء به کار برده‌اند، هرکدام بر جنبه‌های خاصی از این امضاء توجه نموده‌اند. عده‌ایی به مسائل فنی و برخی دیگر به جنبه‌های حقوقی آن توجه کرده‌اند. در بند ۲ ماده ۱۳ پیش‌نویس قانون تجارت الکترونیکی آمده بود: «امضای الکترونیکی عبارت از هر نوع علامت یا روشی است که به یک داده منضم شده، برای شناسایی امضاءکننده داده مورد استفاده قرار می‌گیرد.» ولی ماده ۲ قانون تجارت الکترونیکی مصوب ۱۳۸۲ در تعریف امضای الکترونیکی بیان داشت: «امضای الکترونیکی عبارت از هر نوع علامت منضم‌شده یا به نحو منطقی متصل‌شده به داده‌پیام است که برای شناسایی امضاءکننده داده‌پیام مورد استفاده قرار می‌گیرد». در این تعریف امضای الکترونیکی به نوعی علامت تعبیر شده است در حالی که به نظر می‌رسد با در نظر گرفتن فضای مجازی عبارت مناسب‌تر با فضای رایانه‌ای، واژه «داده‌پیام» است. بهتر آن بود قانون‌گذار ایران به جای عبارت «علامت» از واژه «داده» استفاده می‌کرد. شاید بتوان این‌طور توجیه نمود که قانون‌گذار ایران با عنایت به تعریف قدیمی امضاء که از آن به هر نوع «علامت یا نوشته» در کتب حقوقدانان تعبیر شده است (از جهتی عبارت جدید «داده» وارد ادبیات حقوقی کشور نگردیده)، چنین لفظی را به کار برده است. مطلب قابل توجه اینکه، هرچه سریع‌تر اصطلاحات جدید بایستی وارد ادبیات حقوقی کشور بشوند.

مطلب دیگر اینکه قانون‌گذار ایران تفاوت بین انضمام امضاء و اتصال آن به نحو منطقی به یک داده‌پیام را روشن نکرده است. علت این امر می‌تواند تبعیت صرف و ترجمه لفظ به

لفظ از منابع خارجی باشد. لازم است از طریق تفسیر و بحث در کتب و مقالات حقوقی این تمایز روشن شود.

منظور از منضم شدن امضاء این است که شکل اسکن‌شده امضای دستی ضمیمه سند شده و ارسال می‌شود اما اتصال به نحو منطقی اشاره به سامانه امضاء با کلید اختصاصی و محرمانه دارد که پس از رمزنگاری تنها با کلید عمومی یا با کلید محرمانه مشترک قابل رمزگشایی است که در ظاهر چیزی دیده نمی‌شود، اما منطقاً مرتبط است.[۳]

ماده ۲ قانون نمونه آنسیترال داده‌پیام را این‌طور تعریف کرده است: «امضای الکترونیکی عبارت است از داده الکترونیکی منضم‌شده یا به صورت منطقی متصل‌شده به یک داده‌پیام و برای تشخیص هویت امضاءکننده داده‌پیام و تأیید وی نسبت به اطلاعات موجود در داده‌پیام مورد استفاده قرار می‌گیرد».

در مقایسه این تعریف با تعریفی که قانون‌گذار ایران در قانون تجارت الکترونیکی مصوب ۱۳۸۲ بیان نموده است درمی‌یابیم که:

الف ـ قانون آنسیترال امضای الکترونیکی را داده معرفی کرده است بنابراین از این حیث از قانون تجارت الکترونیکی ایران پیشرفته‌تر است؛

ب ـ قانون آنسیترال به دو کارکرد امضاء یعنی شناسایی امضاءکننده و رضایت وی به مفاد سند توجه کرده است اما در قانون ایران تنها به شناسایی امضاءکننده اشاره شده است. بهتر بود قصد التزام به مفاد سند نیز برای تکمیل تعریف ذکر می‌شد زیرا عنصر معنوی امضاء در یک قرارداد قصد التزام طرفین به مفاد سند است، در غیر این صورت امضاء از ارزش حقوقی برخوردار نخواهد بود.[۴]

فرهنگ لغات حقوقی آکسفورد امضای الکترونیکی را چنین تعریف کرده است: «امضای الکترونیکی قسمتی از یک داده است که ملحق یا منضم به سند قراردادی است که به طور الکترونیکی و به منظور اثبات اصالت یک ارتباط ارسال شده است.»[۵]

این تعریف نیز دارای نقایصی است که به همه ابعاد امضاء توجه ننموده است.

---

۳. رسول مظاهری و علیرضا ناظم، «ماهیت و آثار امضای الکترونیکی در حقوق ایران و مقررات آنسیترال»، *ماهنامه کانون* ۸۶ (۱۳۸۷)، ۱۱۴.

۴. همان، ۹۳.

۵. نک: *آکسفورد*، ۱۶۹.

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

الف ـ امضای الکترونیکی یک داده الکترونیکی است که به یک داده الکترونیکی دیگر متصل می‌شود؛

ب ـ امضای ذیل سند که توسط خود شخص یا به دستور او انجام می‌گیرد برای شناسایی شخص امضاءکننده به کار می‌رود؛

ج ـ تصدیق محتوای سند و اعطای اثر حقوقی به آن، یکی دیگر از کارکردهای امضای الکترونیکی است که باید مورد توجه قرار گیرد؛

د ـ امضاء اعم از اینکه الکترونیکی باشد یا دستی، باید دارای یک عنصر معنوی به نام قصد التزام به مفاد سند باشد. این همان چیزی است که در واقع به یک امضاء اثر حقوقی می‌بخشد در نتیجه در صورتی که یک شخص در طول یک فرایند اقدام به کلیک کردن عبارت «من قبول دارم» کند بدون اینکه قصد التزام به مفاد سند را داشته باشد امضاء در معنای حقوقی آن شکل نگرفته است.

با توجه به مطالب بیان‌شده به نظر می‌رسد می‌توان امضای الکترونیکی را چنین تعریف کرد: امضای الکترونیکی عبارت از داده‌ای است که به قصد التزام به مفاد یک داده‌پیام به آن ملحق یا منطقاً به آن منضم شده است و موجبات شناسایی شخص و رضایت وی به مفاد داده‌پیام را فراهم می‌آورد و از اعتبار حقوقی برخوردار است.[۶]

۱-۲- انواع امضای الکترونیکی

در یک تقسیم‌بندی دیگر بر اساس ارزش اثباتی و سطح ایمنی فراهم‌شده، امضای الکترونیکی را به دو دسته ساده و مطمئن تقسیم می‌کنند. این تقسیم‌بندی در قوانین مختلف از جمله قانون تجارت الکترونیکی مصوب ۱۳۸۲ و قانون نمونه آنسیترال بیان شده است.

با توجه به آنچه آمد، این قسمت به دو بند تقسیم می‌شود شامل: بند اول امضای الکترونیکی ساده و بند دوم امضای الکترونیکی مطمئن است.

۶. مظاهری و ناظم، پیشین، ۹۶.

۱-۲-۱- امضای الکترونیکی ساده

در بند «ی» ماده ۲ قانون تجارت الکترونیکی در تعریف امضای الکترونیکی این‌طور آمده است: «امضای الکترونیکی عبارت است از هر نوع علامت منضم‌شده یا به نحوی منطقی متصل‌شده به داده‌پیام که برای شناسایی امضاءکننده داده‌پیام مورد استفاده قرار می‌گیرد.»

قانون نمونه آنسیترال ۲۰۰۱ در بند الف ماده ۲ امضای الکترونیکی را تعریف کرده است. با دقت در دو تعریف مزبور گرچه تصریحی به امضای الکترونیک ساده نکرده است اما با توجه به تعریف امضای الکترونیکی مطمئن در جای دیگر قانون مزبور، کشف می‌شود که منظور مقنن از تعریف فوق امضای الکترونیکی ساده می‌باشد. به نظر می‌رسد، اگر در تعریف قانون ایران همانند قانون نمونه آنسیترال، تأیید امضاءکننده نیز از جمله آثار آن ذکر می‌شد تعریف کامل‌تر و دقیق‌تری بود.

آنچه از تعریف امضای الکترونیکی ساده برمی‌آید؛ این امضاء دارای وصف انحصاری نسبت به اصل‌ساز نیست و تحت اراده صرف ایشان ایجاد نمی‌شود، بنابراین چنانچه توسط هر شخص ثالثی تغییراتی در آن به وجود آید، قابل تشخیص نخواهد بود. مطلب دیگر آنکه در این نوع از امضاء، هویت صادرکننده آن به وسیله امضاء معلوم نمی‌شود. با جمع اوصاف مزبور سطح اطمینانی که از این امضاء وجود دارد بسیار ضعیف است. همین امر متخصصین این دسته از علوم را به فکر ایجاد نوع امضای دیگری انداخته است که دارای اطمینان بیشتری باشد.

۱-۲-۲- امضای الکترونیکی مطمئن

ماده ۱۰ قانون تجارت الکترونیکی ایران که ناظر به بند «ک» ماده ۲ همان قانون است در تعریف این نوع امضاء بیان داشته است: «امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد:

الف ـ نسبت به امضاءکننده منحصربه‌فرد باشد؛

ب ـ هویت امضاءکننده داده‌پیام را معلوم کند؛

ج ـ به وسیله امضاءکننده یا تحت اراده انحصاری وی صادر شده باشد؛

د ـ به نحوی به یک داده‌پیام متصل شود که هر تغییری در آن داده‌پیام قابل تشخیص و کشف باشد.»

از جهتی در بند ۳ ماده ۶ قانون نمونه آنسیترال ۲۰۰۱ نیز شرایط امضای مطمئن چنین ذکر شده است:

الف ـ داده ایجاد امضاء به همراه مطلبی که در آن مورد استفاده قرار می‌گیرد، مرتبط با شخص امضاءکننده باشد نه فرد دیگری؛

ب ـ داده ایجاد امضاء، در زمان امضاء تحت کنترل امضاءکننده باشد نه فرد دیگری؛

ج ـ هرگونه تغییری در امضاء بعد از زمان امضاء قابل کشف باشد؛

د ـ در جایی که هدف از امضاء حصول اطمینان در خصوص اصالت اطلاعات مرتبط با امضاست هرگونه تغییری در اطلاعات بعد از امضاء قابل کشف باشد.»

از بررسی این دو ماده نکات زیر به دست می‌آید:

اول اینکه بند «ب» ماده ۱۰ قانون تجارت الکترونیکی ایران در قانون نمونه آنسیترال معادلی ندارد. شاید علت این موضوع، وجود شرط مندرج در بند «الف» قانون ایران مبنی بر لزوم منحصربه‌فرد بودن امضاء نسبت به امضاءکننده، موجبات تعیین هویت او را نیز فراهم می‌کند و دیگر نیازی به بند «ب» نیست و به همین دلیل قانون نمونه آنسیترال تعیین هویت امضاءکننده را از جمله شرایط امضای الکترونیکی بیان نکرده است.

نکته دوم اینکه بند «ج» قانون نمونه آنسیترال نیز در قانون تجارت الکترونیک ایران معادلی ندارد و به نظر می‌رسد لازم بود این شرط که در خصوص اطمینان از عدم تغییرات بعدی در امضاست، مورد اشاره قرار می‌گرفت؛ اما قانون‌گذار ایران صرفاً اطمینان در خصوص عدم تغییرات بعدی در داده‌پیام را مورد اشاره قرار داده است.[۷]

۲- انتساب در ادله الکترونیک

آنچه که در ادله الکترونیک سبب انتساب آنها به اصل‌ساز می‌باشد عبارت از اثبات رابطه‌ای است که دلیل را توسط ایجادکننده آن (اصل‌ساز) خلق نموده است. به عبارتی دیگر در ادله الکترونیک با استفاده از امضای الکترونیک داده‌پیام به اصل‌ساز منتسب می‌شود. چگونگی ایجاد این نوع از امضاء با امضای سنتی فرق دارد اما کارکردی که این دو نوع امضاء دارند با یکدیگر مشترک هستند. سند الکترونیکی حاوی امضای الکترونیکی دلالت بر هویت، تمامیت و رضایت امضاءکننده به مفاد سند دارد.

در محیط کاغذی امضاء در شکل سنتی سه نقش را ایفاء می‌کند: نقش اول، شناساندن هویت صاحب آن است؛ نقش دوم، عبارت از فراهم نمودن اطمینان برای دادرسی است چون

۷. همان، ۹۸.

شخص در عمل امضاء دخالت داشته است می‌توان به عنوان دلیل به آن استناد جست؛ نقش سوم بین امضاءکننده و محتوای سند پیوند برقرار می‌کند و رابطه انتساب را اثبات می‌کند.[۸]

امضای منتسب‌الیه رکن سند عادی است، امضاء زیر سند و معمولاً در خود سند درج می‌شود. امضای سنتی به مفهوم اعم هرگونه علامت انحصاری شخصی است که زیر نوشته ترسیم یا گذاشته شده و دلالت بر هویت امضاءکننده و تأیید متن نوشته توسط ایشان می‌نماید. لذا امضاء می‌تواند به وسیله دست در سند ترسیم شده (امضاء به معنای اخصّ) و یا به وسیله دیگر نقش بسته و یا منحصراً مهر یا اثر انگشت باشد. اگرچه امضاء، مهر یا اثر انگشت رکن سند عادی است، اما قانون‌گذار در مواردی نوشته بدون امضاء را نیز سند دانسته است (مانند دفاتر تجاری بازرگانان، ماده ۱۴ قانون تجارت و ماده ۱۲۹۷ قانون مدنی) در غیر مواردی که قانون استثناء کرده امضاء رکن سند عادی است، در نتیجه با در نظر گرفتن این استثناء هر نوشته درخور استنادی که هریک از شرایط سند رسمی را نداشته باشد اما دارای امضای منتسب‌الیه باشد سند عادی شمرده می‌شود.[۹]

در انتساب اسناد و ادله الکترونیک مطلب قابل ذکر این است که امضای سند به منزله آگاهی و اطلاع داشتن از مفاد سند بوده و اینکه صادرکننده همان کسی است که سند به ایشان منتسب است و امضای شخص منتسب‌الیه به منزله تأیید و پذیرفتن مفاد سند توسط ایشان است. هرچند که سند سفید باشد ظاهر این‌طور تلقی خواهد شد که ابتدا مفاد و محتویات سند مکتوب شده و سپس امضاء شده است و چنین سندی به امضاءکننده سند، منتسب خواهد شد. اسنادی که افراد امضاء می‌کنند نوشته‌های عادی هستند که در روابط حقوقی خود به کار می‌برند.[۱۰]

بند ب ماده ۴۸ قانون برنامه پنجم توسعه اجتماعی اقتصادی و فرهنگی جمهوری اسلامی ایران (۱۳۸۹) برای معادل‌سازی کارکردی سند الکترونیکی با سند کاغذی، قابلیت انتساب در سند الکترونیکی را ضروری دانسته است: «سند الکترونیکی در حکم سند کاغذی است، مشروط بر آنکه اصالت صدور و تمامیت آن محرز باشد.» این ماده از برنامه پنجم از یک سو

---

۸. کمیسیون تجارت بین‌الملل سازمان ملل متحد (آنسیترال)، اعتمادسازی در تجارت الکترونیکی، *مسائل حقوقی مرتبط با استفاده بین‌المللی از شیوه‌های گواهی امضای الکترونیکی*، ترجمه ستار زرکلام (تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۰)، ۳۴.

۹. عبدالله شمس، *ادله اثبات دعوا، حقوق ماهوی و شکلی* (تهران: انتشارات دراک، ۱۳۹۰)، چاپ دوازدهم، ۹۱.

۱۰. سید حسن امامی، *حقوق مدنی* (تهران: انتشارات اسلامیه، ۱۳۷۸)، جلد ششم، چاپ دوازدهم، ۱۸۶.

مکمل ماده ۶ قانون تجارت الکترونیکی است، بر اساس آن «هرگاه وجود یک نوشته از نظر قانون لازم باشد، داده‌پیام در حکم نوشته است مگر در موارد زیر ...» و از سوی دیگر تکمیل‌کننده ماده ۱۰ آن قانون است، زیرا آنچه که در ماده ۱۰ آمده، ناظر به امضای الکترونیکی است و حکم صریحی در مورد شرایط و الزامات نوشته الکترونیکی مطمئن، در قانون تجارت الکترونیکی وجود ندارد. منظور از قابلیت انتساب یعنی، امکان تعیین هویت صادرکننده یا به عبارت دیگر احراز اصالت آن.[۱۱]

نظر به اهمیت موضوع، مطالب این مبحث در سه قسمت بیان می‌شود. قسمت اول شامل انتساب امضای ساده، قسمت دوم انتساب امضاء در رمزنگاری متقارن و قسمت سوم انتساب امضاء در رمزنگاری به شیوه نامتقارن را توضیح می‌دهد.

۲-۱- انتساب امضای ساده

موضوع شایان ذکر اینکه نباید تصور کنیم امضای الکترونیکی که موضوع نوشته الکترونیکی را دربر می‌گیرد، همانند امضای دستی و فیزیکی است که بر روی نوشته کاغذی نقش می‌بندد، اگر این‌طور تصور شود که امضای الکترونیکی با امضای دستی از این حیث دارای وجه مشترک باشند، پیامدهای غیرمنطقی را به دنبال خواهد داشت و نتیجه این خواهد شد که سند عادی الکترونیکی بلافاصله با یک امضای الکترونیکی همراه شود، بلافاصله موجودیت خود را کسب کرده و از این لحظه امضاء ایجاد می‌شود، در حالی که واقعیت مطلب غیر از این خواهد بود. چنین برداشتی از موضوع تمام اهمیت قالب کاغذی را در سازوکار نوشته سنتی انکار می‌نماید. نوشته کاغذی در حقیقت این تضمین را ایجاد می‌کند که امضای روی آن دلیل الحاق امضاءکننده به محتوای سند است، زیرا امضاء و محتوای سند در یک قالب واحد قرار دارند. این روند کارکرد تمامیت سند را از طریق ماهیت مادی کاغذ تضمین می‌کند.[۱۲]

امضای الکترونیکی امری انتزاعی است که در فضای غیرکاغذی و محیط مجازی به وجود می‌آید و این امکان برای هر شخصی می‌تواند وجود داشته باشد. این وصف باعث ایجاد

---

۱۱. ستار زرکلام، «چالش‌های حقوقی نگهداری مطمئن از سوابق الکترونیکی بانکی»، *مجله حقوق بانکی* ۱ (بهار و تابستان ۱۳۹۱)، ۱۹.

۱۲. زویه لیان دوبلفون، *حقوق تجارت الکترونیک*، ترجمه ستار زرکلام (تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۰)، چاپ دوم، ۱۶۶.

ناهمگونی خواهد شد و امکان اثبات رابطه انتساب را با دشواری مواجه خواهد کرد. لذا ضرورت شناسایی بدون چون و چرای امضای الکترونیکی و سازمان‌دهی روشی برای کنترل مبدأ این امضاءها احساس می‌شود، بدین‌منظور سیستم گواهی که برای معتبر بودن اسناد الکترونیکی توسط اشخاص ثالث نسبت به معاملات باید صورت پذیرد، پیش‌بینی شده است که از آن با عنوان مرجع گواهی امضای الکترونیکی یاد می‌شود که توسط شخص ثالثی به غیر از طرفین موضوع معامله ایفای نقش می‌کند. ایجاد نوشته الکترونیکی که دارای ارزش سند عادی باشد ممکن نخواهد بود مگر آنکه عناصر تشکیل‌دهنده سند با عبور از کنترل شخص ثالث (مرجع گواهی امضای‌الکترونیکی) یا عناصری که امکان کنترل گواهی را فراهم سازد، وجود داشته باشد.

استفاده از امضای الکترونیکی اغلب با مشکلاتی مواجه می‌شود و دارای ایراداتی است که باید در رفع این مشکلات و ایرادات تلاش کرد. یکی از عمده‌ترین این ایرادها در کاربرد این امضاءها این است که ممکن است ابزار تولید امضاء در مکانی امن نگهداری نشود یا به نحوی از انحاء مورد خدشه و آسیب قرار گیرد و این مسئله ناشی از حالتی خواهد بود که نماینده امضاءکننده کار خود را به دقت انجام نداده باشد از مشکلات دیگر اینکه ممکن است سلسله‌مراتب امضای واقعی که توسط مرجع خدمات گواهی انجام می‌شود قابل اعتماد نباشد، به عنوان مثال چنانچه کلید امضاءکننده یا کلید مرجع خدمات گواهی مفقود شود و در دسترس اشخاص غیرمجاز قرار گیرد و توسط این افراد مورد سوءاستفاده قرار گیرد.[۱۳]

برای اینکه امضای الکترونیکی به اصل‌ساز منتسب شود و از اعتبار لازم برخوردار باشد بایستی به گونه‌ای عمل شود که «تدابیر معقول را برای ممانعت از هرگونه استفاده غیرمجاز از داده‌های مرتبط با تولید امضاء به عمل آورد.»

با رعایت مراتب و قواعد لازم که ویژگی منحصربه‌فرد ادله و اسناد الکترونیک است باید به گونه‌ای عمل کرد که عدم اعتماد در امضاءهای الکترونیکی از بین برود و استنادکننده بدون هرگونه شک و شبهه‌ای بتواند در صورت لزوم، امضاء را به اصل‌ساز منتسب کند.

۱۳. کمیسیون تجارت بین‌الملل سازمان ملل متحد، پیشین، ۱۸۶.

قوانین ملی اغلب مقرر می‌کنند که امضاءکننده متعهد است زمانی که احتمال داده می‌شود، محرمانگی داده‌های تولید امضاء از بین رفته برود، در هر اوضاع و احوالی، ابطال گواهی را از مرجع خدمات گواهی درخواست کند.[۱۴]

در چنین حالتی در قوانین مربوط به این کشورها، گواهی که به نفع یا به ضرر صادرکننده به وجود آمده، ارزش حقوقی نداشته و مورد استناد قرار نمی‌گیرد و چنین سند الکترونیکی به عنوان دلیل شنیده نمی‌شود و قابلیت انتساب چنین امضایی در این شرایط امکان‌پذیر نمی‌باشد.

۲-۲- انتساب امضاء در رمزنگاری متقارن

امروزه از پیام‌های الکترونیکی در حوزه‌های مهم نظیر تجارت و بازاریابی الکترونیکی استفاده می‌شود، در نتیجه باید مکانیسم‌های مهمی برای احراز هویت پدیدآورندگان سوابق الکترونیکی در نظر گرفت، از جمله بهره‌گیری از فناوری رمزنگاری.[۱۵]

ابتدا باید روشن کرد رمزنگاری در اسناد الکترونیکی چه معنایی دارد و کاربرد آن در کجاست. تعریف رمزنگاری این‌گونه است که هر نوع نرم‌افزار یا سخت‌افزار که با استفاده از توافق‌های محرمانه مورد استفاده قرار گرفته باشد و هدف از آن تبدیل اطلاعات یا علامت‌های روشن به علامت‌های غیرقابل فهم برای اشخاص ثالث بوده و یا انجام این عملیات به صورت وارونه و در راستای تبدیل علامت‌های غیرهوشمند به اطلاعات و علامت‌های قابل فهم باشد و مورد استفاده نیز واقع شود. فن رمزنگاری از زمانی که الگوریتم‌های کلید عمومی رایج شد و این الگوریتم‌ها به شیوه‌های مبتنی بر مالکیت کلید اختصاصی توسط دو شخص ذی‌نفع در مبادلات الکترونیکی جایگزین شد، بسیار متحول شده است.[۱۶]

پیام ممکن است به وسیله نرم‌افزار رمزنگاری شود، به عنوان مثال PGP[۱۷] عنوان نرم‌افزاری است که برای رمزنگاری مورد استفاده قرار می‌گیرد. بخشی از آن برای کلیدهای متقارن و بخش دیگری از آن برای کلیدهای غیرمتقارن به کار می‌رود.

---

۱۴. قانون تجارت الکترونیک آرژانتین، ماده ۲۵.

۱۵. امیرحسین جلالی فراهانی، *درآمدی بر آیین دادرسی کیفری جرایم سایبری* (تهران: خرسندی، ۱۳۸۹)، چاپ اول، ۱۱۰.

۱۶. دوبلفون، پیشین، ۱۷۲.

17. Pretty Good Privacy.

در رمزنگاری متقارن باید یک کلید رمز مشترک بین دو طرف تعریف گردد. چون کلید رمز باید کاملاً محرمانه باقی بماند. برای ایجاد و رد و بدل کردن کلید رمز مشترک باید از کانالی استفاده شود که کاملاً امن بوده و اطمینان‌بخش باشد و یا اینکه می‌توان از کلیدهای رمزنگاری نامتقارن استفاده کرد. نیاز به وجود یک کلید رمز به ازای هر دو نفر درگیر در رمزنگاری متقارن موجب بروز مشکلاتی در مدیریت کلیدهای رمز می‌شود.

با رعایت تمامی شرایط لازم که در استفاده از شیوه رمزنگاری متقارن وجود دارد باید سعی کرد تمامیت اسناد و ادله الکترونیک محفوظ بماند و میزان اطمینان‌بخشی اسناد مزبور هرچه بیشتر نزد دادرس در دعاوی ارتقاء یابد. با این وضعیت اطمینان‌بخش و ایجاد محیط امن در شیوه رمزنگاری متقارن می‌توان، ادله الکترونیک و اسناد مربوطه را به ایجادکننده سند (اصل‌ساز) نسبت داد و در این حالت می‌توان گفت شیوه انتساب ادله الکترونیک با مشکلی مواجه نخواهد شد.

۲-۳- انتساب امضاء در رمزنگاری به شیوه نامتقارن

در رمزنگاری وجود اطلاعات یا ارسال شدن پیام به هیچ‌وجه مخفی نمی‌باشد، بلکه ذخیره اطلاعات یا ارسال داده‌پیام مشخص است اما تنها افراد خاصی می‌توانند اطلاعات اصلی را بازیابی کنند، با این تفاوت که در پنهان‌کاری، اصل وجود اطلاعات یا ارسال پیام، محرمانه و مخفی نگاه داشته می‌شود و غیر از ارسال‌کننده و طرف دریافت‌کننده کسی از ارسال پیام آگاه نمی‌شود. تغییرات رمزنگاری در محتویات یک متن حرف به حرف و گاهی اوقات بیت به بیت می‌باشد و هدف از آن تغییر محتوای یک متن می‌باشد.

رمزنگاری نامتقارن در ابتدا با هدف حل مشکل انتقال کلید در روش متقارن در قالب پروتکل تبادل کلید (دیفی ـ هلمن) پیشنهاد شد. در این نوع از رمزنگاری به جای یک کلید مشترک از یک زوج کلیدی به نام‌های کلید عمومی و کلید اختصاصی استفاده می‌شود.

کلید خصوصی تنها در اختیار دارنده آن قرار دارد و امنیت رمزنگاری به محرمانه بودن کلید خصوصی بستگی دارد. کلید عمومی در اختیار کلیه کسانی که با دارنده آن در ارتباط باشند قرار داده می‌شود. هم‌زمان با گذر زمان به غیر از مشکل انتقال کلید در روش متقارن، کاربردهای متعددی برای این نوع از رمزنگاری در نظر گرفته شده است. در سیستم‌های رمزنگاری نامتقارن، بسته به کاربرد و پروتکل مورد نظر، گاهی اوقات از کلید عمومی برای

رمزگشایی و از کلید خصوصی برای رمزگذاری و بعضی اوقات برعکس عمل می‌شود، یعنی از کلید خصوصی برای رمزگشایی و از کلید عمومی برای رمزگذاری استفاده می‌شود.

دو کلید عمومی و خصوصی با یکدیگر متفاوت هستند و با استفاده از روابط خاص ریاضی محاسبه می‌شوند رابطه ریاضی بین این دو کلید به گونه‌ای است که کشف کلید خصوصی با در اختیار داشتن کلید عمومی به طور عملی ناممکن است.

پیشرفته‌ترین رمزنگاری که بیشترین استفاده را نیز دارد بهره‌برداری از کلیدهای نامتقارن است. الگوریتم رمزنگاری نامتقارن بر تولید کلیدهای دوگانه استوار است، هر عاملی یک کلید عمومی و یک کلید اختصاصی در اختیار ایشان است که ارتباط این دو از طریق رابطه‌های ریاضی است و تعداد مبادی آن به قدری زیاد است که به دلیلی ویژگی رشدیابنده و پیچیدگی ایجادشده در آن با ترکیب‌های احتمالی، پیدا کردن کلید اختصاصی از روی کلید عمومی غیرممکن است.

در مقابل آن داده رمزنگاری‌شده به کمک کلید اختصاصی، می‌تواند با استفاده از کلید عمومی و بالعکس رمزگشایی شود.

از آنجایی که در رمزنگاری نامتقارن کلید اختصاصی به طور سرّی و محرمانه باقی خواهد ماند این امر باعث می‌شود آن آسیب‌پذیری که در رمزنگاری متقارن وجود داشت در اینجا ظاهر نشود. پیام‌های الکترونیکی نوعی سند و دلیل الکترونیکی محسوب می‌شوند و حاوی یک سری اطلاعات و مفاهیم بوده که این اطلاعات نزد دادگاه دارای اعتبار هستند و از سوی فرستنده به گیرنده ارسال می‌شوند. آنچه در اینجا باید تأمین شود، دو کارکرد می‌باشد، اول محرمانگی محتوای داده‌پیام؛ دوم شناسایی فرستنده آن باید لحاظ شود.

مطلب دیگر اینکه پیام نباید در نتیجه انتقال بر روی شبکه‌ها دستخوش تغییر قرار گیرد یا توسط ثالث مورد تجسس واقع شود به عبارت دیگر تمامیت سند و پیام باید تحت کنترل همیشگی باشد.[۱۸]

همیشه این احتمال وجود دارد که پیام توسط شخص ثالثی ارسال شود که دارای سوءنیت هم باشد. علت این امر نیز به واسطه وجود کلید عمومی است که برای همگان قابل دسترس است. برای اینکه بتوانیم از چنین عملی جلوگیری کنیم، پیام باید از طریق نرم‌افزاری ارسال شود که با امضای فرستنده همراه باشد و این امضاء با کلید عمومی ایجاد شده باشد.

۱۸. دوبلفون، پیشین، ۱۶۹.

ابزاری که باعث می‌شود تمامیت یک پیام تضمین شود، عبارت است از تبدیل آن پیام به یک چکیده. این امر نتیجه اطلاعات طولی ثابتی است که به کمک الگوریتم کوچک‌کننده (خردکننده اطلاعات) به دست می‌آید. مقایسه این رد پا در آغاز و پایان، تمامیت پیام را تضمین می‌کند، زیرا کمترین تفاوت در اطلاعات ارائه‌شده منجر به اثرات متفاوت می‌شود؛ بنابراین ضرورتی ندارد که چکیده‌ها خیلی سنگین باشند.[۱۹]

با حفظ تمامیت یک پیام که از طریق رمزنگاری نامتقارن امکان‌پذیر است و به لحاظ محرمانگی بیشتر، این نوع امضاءها که از طریق این نوع رمزنگاری انجام می‌پذیرد، دارای اثر اطمینان‌بخشی بیشتری بوده و امکان انتساب آن به اصل‌ساز راحت‌تر و مقبول‌تر است.

نتیجه

طرفین دعوا می‌توانند نسبت به اصالت مدارک تولیدی رایانه و مدارک حاصل برنامه انسان از حیث مخدوش یا جعلی بودن ایراد وارد کنند یا ممکن است طرفین به صحت و اصالت مدارک تولیدی رایانه از حیث غیرقابل اعتماد بودن آنها ایراد وارد نمایند یا اینکه ممکن است طرفین به مدارک حاصل برنامه انسان از حیث هویت مؤلف آن ایراد وارد کنند.

اظهار انکار و تردید فقط نسبت به اسناد عادی الکترونیکی ممکن است و اسناد مطمئن به موجب ماده ۱۵ قانون تجارت الکترونیک، قابل انکار و تردید نیستند. منظور از انکار، اعلام رد تعلق خط، امضاء، مهر و یا اثر انگشت سند غیر رسمی به منتسب‌الیه توسط خود وی می‌باشد. منظور از تردید، عدم پذیرش انتساب خط، امضاء، مهر و یا اثر انگشت سند غیر رسمی به منتسب‌الیه توسط شخص دیگر است که در دلایل الکترونیکی به صورت رد انتساب امضای الکترونیکی ذیل سند تحقق می‌یابد. لازم به ذکر است که اگر شرایط مذکور در مواد ۱۸ و ۱۹ در مورد اماره قانونی انتساب داده‌پیام به اصل‌ساز محقق باشد، نمی‌توان در مورد آن، انکار و تردید کرد.

ادعای جعل هم در مورد ادله الکترونیکی عادی و هم در مورد ادله الکترونیکی مطمئن می‌تواند مطرح شود. از آنجا که جعل نوعی ادعاست، باید توسط ادعاکننده اثبات شود.

گاه مدعی جعل، انتساب سند به خود را قبول دارد اما مدعی است که مطالب مندرج در سند بعد از امضاء یا ارسال به دریافت‌کننده تغییر کرده است. اگرچه تغییر سند الکترونیکی از

۱۹. همان، ۱۷۰.

خود اثر فیزیکی باقی نمی‌گذارد، اما می‌توان آن را با استفاده از برخی روش‌های فنی اثبات نمود. به عنوان مثال در صورتی که در سند مورد اختلاف، از فناوری امضای دیجیتال استفاده شده باشد، در صورتی که امضاء مورد جعل قرار گیرد به راحتی می‌توان از طریق استفاده از فناوری «خرد کردن» آن را تشخیص داد.

بنابراین با توجه به مطالب مذکور پیشنهادهای ذیل ارائه می‌گردد:

۱- با عنایت به گستردگی جهانی مخابرات و ارتباطات رایانه‌ای، ادله الکترونیکی نیز در ابعاد بین‌المللی و فرامرزی خودنمایی کرده است. بدین‌ترتیب برای حل مسائل و مشکلات ماهوی و شکلی ناشی از این‌گونه ادله، ضرورت هماهنگی بین‌المللی کشورها در جهت استفاده بهینه از آنها احساس می‌شود؛

۲- از آنجایی که دولت‌ها همواره باید نیازهای آینده شهروندان خود را در نظر داشته باشند و چند گام جلوتر از آنها حرکت کنند، پیشنهاد می‌شود دولت‌ها با سرمایه‌گذاری علمی و مادی در زمینه موضوعی فضای سایبر و علوم فناوری اطلاعات پیشگام باشند؛

۳- دولت امکانات کافی را برای ارائه خدمات صدور گواهی الکترونیکی شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و نگهداری گواهی اصالت امضای الکترونیکی از طریق تأسیس دفاتر خدمات صدور گواهی الکترونیکی در کشور تأمین نماید. اگر چنین سازوکاری در کشور اجرا شود رهگیری و بازیابی و احراز اصالت و قابلیت انتساب در اسناد الکترونیکی بسیار آسان خواهد گردید.

فهرست منابع

الف) منابع فارسی

امامی، سید حسن. *حقوق مدنی*. جلد ششم. چاپ دوازدهم. تهران: انتشارات اسلامیه، ۱۳۸۷.

جلالی فراهانی، امیرحسین. *درآمدی بر آیین دادرسی کیفری جرایم سایبری*. چاپ اول. تهران: نشر خرسندی، ۱۳۸۹.

دوبلفون، زویه لیان. *حقوق تجارت الکترونیک*. چاپ دوم. ترجمه ستار زرکلام. تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۰.

زرکلام، ستار. «چالش‌های حقوقی نگهداری مطمئن از سوابق الکترونیکی بانکی». *مجله حقوق بانکی* ۱ (بهار و تابستان ۱۳۹۱): ۲۴-۵.

شمس، عبدالله. *ادله اثبات دعوا، حقوق ماهوی و شکلی*. چاپ دوازدهم. تهران: انتشارات دراک، ۱۳۹۰.

کمیسیون تجارت بین‌الملل سازمان ملل متحد (آنسیترال). *اعتمادسازی در تجارت الکترونیکی، مسائل حقوقی مرتبط با استفاده بین‌المللی از شیوه‌های گواهی امضای الکترونیکی*. ترجمه ستار زرکلام. تهران: مؤسسه مطالعات و پژوهشهای حقوقی شهر دانش، ۱۳۹۰.

مظاهری، رسول، و علیرضا ناظم. «ماهیت و آثار امضای الکترونیکی در حقوق ایران و مقررات آنسیترال». *ماهنامه کانون* ۸۶ (۱۳۸۷): ۱۱۷-۸۹.

ملک‌آرا، محمدرضا. «قانون قابل اعمال در تجارت الکترونیکی ایران و فرانسه». پایان‌نامه کارشناسی ارشد، تهران: دانشکده حقوق و علوم سیاسی دانشگاه علامه طباطبائی، ۱۳۸۶.

ب) منابع انگلیسی

Anjanette, H.Raymond. "Electronic Commerce and the New Uncitral Draft *Convention*." *The Computer & Internet Lawyer Journal* 23 (August 2006): 9-16.

Argentina, Lev de Firma Digital (2001) Article 25 (c).

The Oxford English Dictionary. Oxford: University Press, 2007.

Feature Assignment in Electronic Evidence

Dr. Iraj Behzadi
Graduated Ph.D. of Private Law, School of Law, Islamic Azad University, Tabriz, Iran
Email: Dr.behzadi2000365@yahoo.com

Almost nothing remains of the third millennium, directly or through the new information and communication technologies is associated. In order to secure and ensure the authenticity of electronic signatures in the diagnosis, also prove the relationship between the instrument and data assignment message, the computer sciences experts to develop two technologies in this field. A symmetric encryption or single key that has been saymtryk and was somewhat reassuring, electronic signature feature of this approach is attributable to the issuer. The latter is asymmetric cryptographic techniques; the two keys are mathematically related and complementary to an algorithm used. This type of encryption has a greater level of security enjoyed, there is no possibility of falsification and distortion, attributable to the issuer in terms of functionality is more reassuring.
In terms of capacity allocation electronic evidence, while the concept of electronic signatures, it is divided into two types of electronic signature, simple and reliable. As a simple electronic signature to sign documents contained in normal, it is an undeniable question. But sure the electronic signature as certificate, merely alleged capabilities of forgery and both terms in compliance with the principles and rules of construction are attributable to original creator.

Keywords: Electronic Evidence, Feature Assignment, Electronic Signatures, Symmetric Encryption, Asymmetric Encryption.

ISSN 1682-9220

Journal of LEGAL RESEARCH

VOL. XVII, No. 2 2018-2

S. D. I. L.
The S.D. Institute of Law
Research & Study