امضای الکترونیکی
بسترساز کاهش جرم در تجارت الکترونیکی

محمد سریرافراز، دانشجوی کارشناسی ارشد علوم اقتصادی، دانشگاه آزاد اسلامی

فاطمه فهیمی فر، دانشجوی کارشناسی ارشد علوم اقتصادی، دانشگاه آزاد اسلامی

تاریخ دریافت: ۸۸/۸/۵ تاریخ پذیرش: ۸۸/۹/۲۵

از صفحه ۶۴ تا ۷۷

چکیده

تجـارت الکترونیک امروزه به عنوان شـیوه جدیدی از مبادلات تجـاری مبتنی بر داده‌های الکترونیکی، جایگزین روش‌های سـنتی شـده و به سـرعت در حال فراگیر شدن است. امضای الکترونیکی از جمله راهکارهایی است که برای تضمین امنیت و ایجاد اعتبار اسناد و قراردادها و داده‌های الکترونیکی در تجارت الکترونیکی پیش بینی شـده اسـت. طبیعتاً متناسـب با این تغییرات، جرایم مرتبط با امضای سنتی دچار دگرگونی هایی شده و جرایم متناسب با امضای الکترونیکـی مطرح می‌شـود. در مقاله حاضر امنیـت مبادلات در فضای مجازی به عنوان یکی از مهمترین بسـترهای تجارت الکترونیک از دریچه امضای الکترونیکی مورد توجه قرار گرفته است و به‌طور اجمالی به بیان تعریف، مزایا، روش‌ها، قابلیت استنادپذیری این نوع امضا پرداخته شـده اسـت. با توجه به مطالب بیان شـده در مقاله پیش رو به این نتیجه می‌رسیم که امضای الکترونیکی برقرار کننده خدمات امنیتی متعددی بدین شرح است: خدمت امنیتی «تمامیت» را توسط علامتی که بر روی امضای الکترونیکی درج می‌شود برقرار می‌کند و «تصدیق هویت و سندیت و انکار ناپذیری»را با استفاده از گواهی الکترونیکی مورد استفاده در امضای الکترونیکی

و همچنین «محرمانه بودن» را توسط گواهی الکترونیکی و الگوریتم‌های رمزنگاری متقارن و نامتقارن ایجاد می‌کند تا جرایم مرتبط با امضای الکترونیکی به حداقل برسد. روش تحقیق مورد نظر، کتابخانه ای است و با استفاده از منابع روزآمد تهیه شده است.

کلید واژه‌ها:
امضای الکترونیکی، امنیت، تجارت الکترونیکی، رمز نگاری، مرجع گواهی امضا، جرم.

۱- مقدمه

این واقعیت که در تجارت الکترونیک تمام فعالیت‌های تجاری به صورت مجازی صورت می‌گیرد، موجب می‌شود که لزوماً قراردادها و معاملات الکترونیکی از نظر قانون به رسمیت شناخته شوند و از همان اعتبار لازم در فضای غیرالکترونیکی برخوردار باشند.

اصولاً هر عقدی با ایجاب و قبول طرفین آن منعقد می‌شود و فقط آنچه اهمیت دارد این است که متعاملین بتوانند اراده انشایی خود را مبنی بر تشکیل عقد یا انجام معامله به طریقی به یکدیگر منتقل نمایند، به گونه ای که هر یک از طرفین معامله از اراده جدی طرف دیگر اطمینان حاصل نماید. پس همان‌گونه که قصد طرفین ممکن است به صورت کتبی، شفاهی، لفظی یا عملی باشد، می‌توان گفت ایجاب و قبول در یک فضای مجازی و در قابل داده‌های الکترونیکی نیز از نظر حقوقی معتبر و لازم الاجراست؛ اما در تشکیل قراردادهای الکترونیکی و الزام آور دانستن آنها، باید به برخی تفاوت‌ها و ویژگی‌های خاص این‌گونه مبادلات در مقایسه با انواع کلاسیک آنها توجه کرد. یکی از مهمترین مباحث حقوقی تجارت الکترونیکی، بحث امنیت مبادلات الکترونیکی است.

در این مقاله پس از معرفی مختصر این اصول، امضای الکترونیکی را به عنوان عامل ایجاد امنیت در معاملات الکترونیکی به طور مفصل شرح خواهیم داد.

۲- اصول مهم حقوقی تجارت الکترونیکی در جهت کاهش بروز جرم

- اصل لزوم امکان شناسایی پیام‌های ارائه شده در شبکه.
- قاعده اعتبار نظریه وصول در قراردادهای الکترونیکی.
- اصل برابری ادله الکترونیکی با سایر ادله اثبات.
- اصل اختیار حق فسخ حداقل هفت روزه برای مصرف کننده در معامله از راه دور.
- اصل امنیت مبادلات تجارت الکترونیکی به اعتبار امضای الکترونیکی.

موضوع مورد بحث نگارندگان در جهت کاهش جرایم است که به بررسی گسترش تجارت الکترونیک می‌پردازد که این امر مستلزم ایجاد اطمینان و اعتماد عمومی نسبت به این نوع از تجارت است و اینکه این اطمینان باید از طریق تضمین امنیت تبادل داده‌های الکترونیکی صورت گیرد. امنیت تبادل داده‌های الکترونیکی فرایندی است که باید تمام اجزا و عناصر یک مبادله تجاری را به‌طور کامل و مطمئن حفظ کند به‌گونه ای که دریافت کننده پیام داده ای مطمئن شود که اطلاعات رسده توسط همان شخصی که قصد ارسال آن را داشته، فرستاده شده است. علاوه بر این طرفین یک مبادله الکترونیکی باید مطمئن شوند که هیچ گونه دسترسی غیرمجاز و غیرقانونی نسبت به داده‌های الکترونیکی صورت نگرفته است.

یکی از عواملی که باعث اعتبار قرارداد یا هر سند دیگری می‌شود، صحت انتساب آن قرارداد یا سند به صادر کننده است که تاکنون از طریق مهر یا امضا صورت می‌گرفت و دلیل معتبری برای تحقق صحت انتساب صادرکننده بود. در تجارت الکترونیک نیز اسناد، اطلاعات و داده‌های الکترونیکی باید به امضای شخص صادرکننده برسد تا بتوان صحت انتساب آنها را به وی احراز کرد. مسلماً مهر و امضای متداول فعلی که بین عموم و تجار مرسوم است در فضای مجازی کاربردی ندارد، بنابراین متناسب با این محیط الکترونیکی باید یک امضای الکترونیکی را تعریف نموده و جایگزین امضاهای دست نویس کرد. [۱]

۳- امضای الکترونیکی

امضای الکترونیکی به تأییدی اطلاق می‌شود که به صورت الکترونیکی ایجاد شده باشد

و ممکن اســت یک علامت، رمز، کلمه، عدد، یک اســم تایپ شــده، تصویر دیجیتالی شده یک امضای دست نویس و یا هر نشان الکترونیکی اثبات هویت باشد که توسط صادر کننده یا قائم مقام وی اتخاذ شده باشد و به یک قرارداد یا هر سند دیگری ملحق شده باشد.

در قانون تجارت الکترونیکی ایران این تعریف برای امضای الکترونیکی برگزیده شده است:

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

تاکنون انواع مختلفی از امضای الکترونیکی با فناوری‌های متفاوت شناخته شده و به محیط تجارت الکترونیکی معرفی شده است که یکی از ساده ترین آنها عبارتند از:

تصویر اســکن شــده یک امضای دســت نویس، امضــای بیومتریک و امضــای دیجیتال که پیشــرفته تریــن و پرکاربردتریــن نوع از امضاهای الکترونیکی اســت. بنابرایــن با توجه به اهمیــت امضــای دیجیتال و اتخاذ این نوع امضا در بیشــتر قوانیــن مربوطه (از جمله قانون تجــارت الکترونیــک ایران) شــیوه ایجاد آن به طور اجمالی در بند ۳-۳ مورد بررســی قرار می‌گیرد. [۲]

۳-۱ مزایای امضای الکترونیکی

امضای الکترونیکی دارای کارکردهایی اســت که آن را نســبت به امضای دستی قابل قبولتر می‌ســازد، هر چند که همانند فناوری‌های دیگر چنین امضایی صد در صد قابل اعتماد نیســت و اشــتباه‌های انســانی، ذخیره ســازی و پشــتیبانی و خطاپذیری کدهای ریاضی از ضعف‌های احتمالی آن است، ولی این ضعف ها بسیار نادر هستند.

امضای دســتی و ســنتی هر دو به دلایل بسیاری، آســیب پذیر هستند. اول آنکه هیچ روش استانداردی برای ترسیم دقیق آن وجود ندارد و در نتیجه مختلف هستند. این امر تطبیق نمونه امضا را در برخی از موارد با دشواری همراه می‌سازد. به همین دلیل در روابط اقتصادی تجاری مانند بانک‌ها این امضاها در حدود بانکداری تأیید می‌شــوند. دوم آنکه امضای دســتی بسهولت و راحتی قابل جعل اســت ولی امضای الکترونیکی، نســبت این موارد از امنیت و اطمینان بالاتر

و دقیقتری برخوردار است. [۳]

به طور کلی مزایای امضای الکترونیکی مشتمل بر ۶ دسته زیر است:

۳-۱-۱ تضمین تمامیت داده پیام

«تمامیت داده» عبارت از موجودیت کامل و بدون تغییر داده است. اعمال ناشی از تصدی سیستم از قبیل ارسال، ذخیره یا نمایش اطلاعات که به‌طور معمول انجام می‌شود خدشه ای به تمامیت داده وارد نمی کند. (ماده ۲-۸ پیش نویس و ماده ۲-ه قانون تجارت الکترونیکی). این ماده معیار تمامیت داده را حفظ کمال و تغییر نکردن آن می‌داند، برای مثال اعمالی که در اجرای تصدی وظایف شخص ثالث (دفتر خدمات الکترونیکی) برای تأیید و تصدیق داده، از قبیل زمان و تاریخ و شماره و سایر اطلاعات مربوطه نسبت به داده انجام می‌شود، به تمامیت آن لطمه نخواهد زد و اصالت آن را ضایع نمی سازد. روش‌های خاص که سیستم رایانه ای اصل ساز برای آغاز و پایان داده پیام انجام می‌دهد و تا زمانی که آن را ارسال می‌کند باید به عنوان یک پاکت پستی در نظر گرفته شود که برای قرار دادن یک نامه پستی در پاکت و بستن آن و حک تمبر و تاریخ بر روی آن، این کارها صورت می‌گیرد. بنابراین امضای الکترونیکی تمامیت و یکپارچگی داده را تضمین می‌کند به این معنا که به ما اطمینان می‌دهد که اطلاعات به صورت عمدی یا سهوی تغییر نکرده است.

۳-۱-۲ امکان استناد پذیری

استناد پذیری پاسخی به این سؤال است که « چه کسی پیام را ارسال کرده است؟» پاسخ به این سؤال حتی در مواقعی که امضای سنتی دستی مد نظر است، اهمیت بسیاری دارد زیرا امضاهای دستی به خودی خود از نظر قانون کسی را معتمد نمی کند، بلکه استناد پذیری آن باید ثابت شود که این کار تقریباً از طریق دفاتر اسناد رسمی صورت می‌گیرد.

در دنیای دیجیتال، مراجع گواهی امضا (دفاتر خدمات الکترونیکی) که در بند ۳-۳-۱ به آن اشاره خواهیم کرد، استنادپذیری لازم را تأیید می‌کند و این امر به نحوی ناگشودنی، جزئی

از سـند خواهد شـد. به عبارت دیگر امضای الکترونیکی در سایه تأیید و تصدیق دفاتر خدمات الکترونیکی، نقش استناد پذیری به اسناد را نشان می‌دهد.

۳-۱-۳ غیر قابل انکار و تردید

« غیر قابل انکار » به این معنی است که امضا کننده سند نمی تواند وجود یا تمامیت مبادله را انکار کند. فناوری امضای الکترونیکی به واسطه وجود اصل پیام که با پیام خلاصه و رمز شده همراه می‌شـود و همچنین ضمیمه شـدن گواهی دیجیتال، پیام الکترونیکی را غیر قابل انکار و تردید می‌نماید. البته امضای الکترونیکی که به طریق مطمئن ایجاد شـده باشـد تنها قابلیت ادعای جعل را دارد.

۳-۱-۴ دارا بودن مهر - زمان

بیشـتر فناوری‌های اطلاعاتی دارای امکاناتی هسـتند که تاریخ و زمان را ثبت می‌کنند که ایـن مسـئله برای خرید و فـروش الکترونیکی و اعمال حقوقی اهمیت بسـیاری دارد. امضای الکترونیکی که به وسـیله یک مرجع گواهی امضا تأیید شـده است، باید « مهر - زمان » خورده باشد تا به تطبیق کننده و ممیز اجازه بدهد به طور قطع، یقین کند که امضای الکترونیکی دقیقاً در زمان تصدی موجود در گواهی امضا صادر شده است. در واقع فناوری امضای الکترونیکی به شکلی است که دارای مهر - زمان است.

۳-۱-۵ سرعت و دقت

امضای الکترونیکی باعث افزایش سـرعت و دقت خواهد شـد. اسناد و امضای الکترونیکی را می‌توان در چند ثانیه ایجاد کرد و به سراسر دنیا ارسال نمود. در این وضعیت امکان کمتری برای خطا وجود دارد. در مقایسه با امضای سنتی، ماشین بهتر از انسان می‌تواند امضای الکترونیکی را بررسی کند، در نتیجه سرعت و امنیت مبادلات دیجیتال افزوده خواهد شد.

۳-۱-۶ رازداری و محرمانگی

« راز داری و محرمانگی»، یکی دیگر از ویژگی‌های امضای الکترونیکی است. فناوری امضای الکترونیکی این اطمینان را می‌دهد که پیام فقط به وسیله افراد مجاز رؤیت شود، زیرا کلیدی که برای رمز گشایی لازم است فقط در اختیار افراد مجاز است. البته بعد از آنکه پیام رمزگشایی شـد، دیگر هیچ کنترلی وجود نخواهد داشـت، اما دسترسی غیر مجاز در خلال ارسال پیام که بیش از هر زمان دیگری در معرض آسیب است غیر ممکن خواهد شد.

این شش عنصر از اجزای جدانشدنی امضای الکترونیکی است که استفاده از آنها را مطلوبتر و مطمئنتر می‌سازد. اگرچه هنوز مخاطرات، اشتباه، تقلب و سوء استفاده وجود دارد. [۴]

۳-۲ دسته بندی بر مبنای به‌کارگیری و عدم به‌کارگیری رمز نگاری

۳-۲-۱ امضاهای الکترونیکی غیر مبتنی بر رمز نگاری

با توجه به عنوان ذکر شده در این مورد، ویژگی این نوع از امضاهای الکترونیکی عدم استفاده از رمز نگاری در جریان به‌کارگیری آنهاسـت، برای نمونه می‌توان امضاهای رقمی که با اسـکن کردن امضای دستی فرد ایجاد می‌شود و یا امضاهایی که بر اساس معرف‌های «زیست سنجی» سـاخته می‌شـوند_ مانند اثر انگشت، امضاهای دسـتی، الگوی صدایی، الگوی نوشتن و حالت شبکیه چشم _ را نام برد.

۳-۲-۲ امضاهای الکترونیکی مبتنی بر رمز نگاری

رمز نگاری عبارت اسـت از تبدیل داده ها به رمز برای رسـیدن به سـطح مطلوب ایمنی،و در جریان این عمل فرستنده پیغامِ رمز نگاری نشده را به یک متن کد گذاری شده تبدیل می کند و دریافت کننده، این پیغام را به منظور یکی از اهداف زیر به‌کار می‌برد:

۱- تبدیل متنِ کد گذاری شده به شکل اصلی و رمز نگاری نشده آن.

۲- تشخیص هویت فرستنده پیام.

۳- تشخیص تمامیت داده ها یا عدم آن.

۴- ترکیبی از سه مورد بیان شده.

۳-۲-۲-۱روش‌های رمز نگاری

برای متعهد کردن یک شخص به کلمات کلیدی، خود مخترعان روش‌های مختلفی را ابداع کرده اند. روش‌های نامبرده عمدتاً مبتنی بر روش‌های رمز نگاری اســت. از جمله این روش‌ها عبارتند از:

- رمز گذاری و رمز گشایی.
- رمز نگاری متقارن.
- چکیده سازی یا درهم سازی پیام.
- رمزگذاری به شیوه کلید عمومی یا رمزگذاری نامتقارن.
- امضای رقمی و پنهان سازی.
- امضاهای دوگانه.
- امضای چشم بسته.

از میان این نوع از روش‌ها، روش رمز نگاری نا متقارن بهترین شیوه برای استفاده در طراحی امضای الکترونیکی اســت، زیرا این روش کارکردهای یک امضا از جمله تأیید هویت شــخص امضا کننده، امنیت و همچنین کلیت را داراســت. به منظور عملی کردن این رمزنگاری باید از سیستم زیر ساخت کلید عمومی (PKI) استفاده کرد که این شیوه لزوم استفاده از یک مرجع ثالث که همانا دفاتر خدمات الکترونیکی است را ایجاب می‌کند.

در رمزنگاری نامتقارن دو کلید نامتناظر ولی مکمل استفاده می‌شود به طوری که این دو کلید با هم منطبق گشــته و در نهایت عمل امضا تحقق می‌یابد_ کلید، یک فرایند ریاضی کاربردی است که به منظور رمزنگاری و رمزگشایی به کار برده می‌شود_ این دو کلید عبارتنداز: « کلید خصوصــی» کــه فقــط امضا کننده از آن آگاهی دارد و برای ایجاد امضای رقمی و به منظور رمز گشایی از آن استفاده می‌شود، و دیگری « کلید عمومی»، که افراد بیشتری آن را می‌شناسند و از آن برای شناسایی و بررسی اعتبار و درستی امضای رقمی استفاده می‌شود. [۵]

۳-۲-۳ نحوه اجرای یک امضای الکترونیکی مبتنی بر سیستم رمزنگاری نامتقارن

ابتـدای پیـام را با به‌کارگیری نـرم افزار مخصوص، خرد می‌کنیم که با این کار به آن خلاصه پیام می‌گوییم. خلاصه پیام نسبت به پیام کاملاً منحصر بفرد است و به بیانی دیگر می‌توان از آن به خلق "اثر انگشـت الکترونیکی" تعبیر کرد که این عمل پیغام را به شـکل یک ارزش خرد یا نتیجه خرد با اندازه ای استاندارد ایجاد می‌کند. سپس عمل امضا با توجه به خلاصه پیام، با اجرای کلید خصوصی _فرد امضا کننده_ و با اسـتفاده از کلید عمومی _مخاطب_ انجام داده می‌شود و در نهایت این خلاصه پیام امضا شده همراه با اصل پیام ارسال می‌شود. در این شیوه به محرمانگی پیام توجه نمی‌شود به عبارت دیگر فرد ارسال کننده پیام خواهان آن است که بدون هیچ کم و کاستی پیام مورد نظرش ارسال شود. چنانچه فرد خواهان محرمانه بودن خود پیام درهنگام ارسال باشد عمل امضا باید نسبت به کل پیام و بدون ایجاد خلاصه پیام انجام شود.

از طرفی دریافت کننده پیام نیز آن را به‌وسیله نرم افزار خرد می‌کند و ارزش ریاضی آن را که درنتیجه این عمل به‌وجود آمده اسـت، با اثر انگشـت ارسالی مطابقت می‌دهد و چنانچه مشابه بود، صحت محتوای پیام مورد تأیید قرار می‌گیرد و نتیجه به‌دست آمده از این عمل را با کلید خصوصی خود رمزگشایی می‌کند.

۳-۳ امضای الکترونیکی مطمئن

قانون تجارت الکترونیکی امضای الکترونیکی را در دو سـطح مختلف نام برده اسـت: نخست، امضای الکترونیکی ساده و عادی و دوم، امضای الکترونیکی مطمئن.

امضای الکترونیکی ساده، انواع وسیعی را در بر می‌گیرد که برای تعیین ارزش اثباتی امضای الکترونیکی، دخالت قاضی تعیین کننده اسـت و چنانچه نسـبت به آن ادعای شبهه وارد شود، می‌توان پس از اثبات اصالت آن در دادگاه، اعتبار سند رسمی را به آن بخشید.

امضای الکترونیکی مطمئن، از شـیوه مطمئن برای مسـتند سازی استفاده می‌کند و دارای ارزش اثباتی معادل اسـناد رسـمی اسـت. این نوع امضا باید مطابق ماده ۱۰ قانون دارای چهار شرط به قرار زیر باشد:

- منحصر بفرد نسبت به فرد امضا کننده.
- آشکار بودن هویت امضا کننده داده پیام.
- صادر شده توسط شخص امضا کننده و یا به اراده انحصاری وی.
- به شکلی تولید شده و به داده متصل گردد که هر گونه تغییری در داده پیام قابل تشخیص باشد.

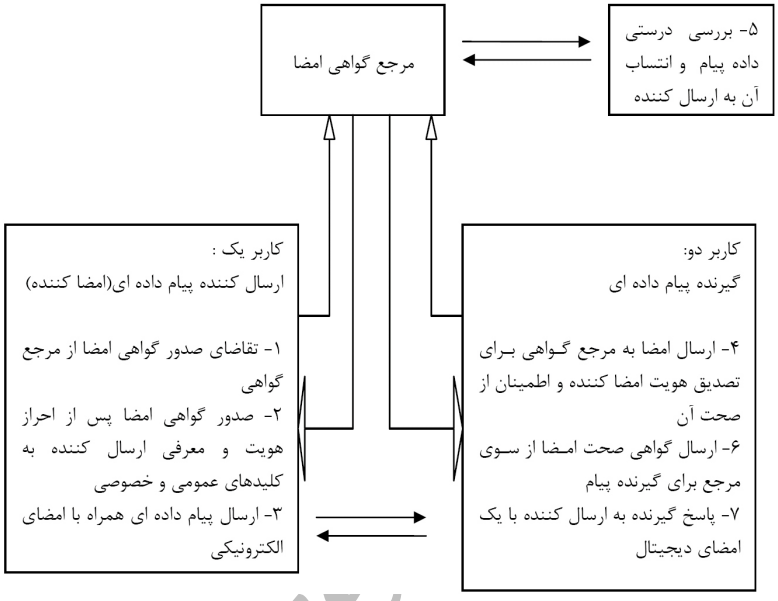
الزام به رعایت این بندهای ماده قانونی مورد نظر، داده پیام را حاوی یک امضای الکترونیکی مطمئن می‌کند و در نتیجه ضرورتی به رسیدگی از سوی مراجع قضایی برای تعیین ارزش اثباتی آن نیست، هر چند می‌توان نسبت به آن ادعای جعل نیز کرد.

با توجه به مطالب بیان شده باید ذکر کنیم که به‌کار بردن امضای الکترونیکی بدون اینکه مراجعی برای فراهم کردن خدمات مستند سازی و اعمال امضای الکترونیکی وجود داشته باشند، امکانپذیر نیست. [۶]

۳-۳-۱ مرجع گواهی امضای الکترونیکی

برای به رسمیت شناخته شدن امضای الکترونیکی از لحاظ قانونی، مرجع گواهی صحت امضای الکترونیکی ایجاد شده است که وظیفه آن کنترل وتأیید هویت صاحب امضا نسبت به منحصر بفرد بودن امضای سند یا پیام ضمیمه شده است. به عبارت دیگر، مرجع مورد نظر باید برای هر امضا یک گواهی تهیه و تنظیم کرده و ضمیمه آن کند، که این گواهینامه هویت امضا کننده و صحت انتساب سند به وی را مورد تأیید قرار می‌دهد. نحوه کار این مراجع به صورت مدل شکل (۱) طراحی شده است. [۷]

مدل (۱): فرایند صدور و بهره گیری از امضای الکترونیکی



۳-۳-۲ ویژگی‌های مرجع گواهی امضای الکترونیکی

- می‌تواند به طور مستقیم یک نهاد دولتی باشد و یا زیر نظر دولت باشد، که این کار برای داشتن ضمانت اجرای قانونی و نیز بالا رفتن درجه اطمینان انجام می‌شود.
- بر مبنای حوزه شمول جغرافیایی در دوسطح ملی و بین المللی قابل انجام است.
- امنیت بالایی را درمورد اطلاعات و اسرار و داده‌های الکترونیکی افراد تضمین می‌کند.
- توانایی نگهداری پرونده ها، سوابق و اطلاعات افراد و ذخیره سازی را دارد.
- مجهز به امکانات و فناوری‌های لازم درتشخیص هویت طرفین تجاری است.

۳-۴ قابلیت استناد امضای الکترونیکی از منظر حقوقی

درمورد استناد به امضای الکترونیکی، تضادی مشاهده می‌شود، به گونه‌ای که فناوری دیجیتال، امکان جعل امضاهای الکترونیکی را درسطحی غیر قابل مقایسه با امضاهای سنتی،

فراهـم آورده اسـت و از طرفـی فناوری دیجیتـال می‌تواند آنچنان ضریـب امنیتی امضاهای الکترونیکی را افزایش دهد که در گذشته نظیر آن وجود نداشته است . [۸]

از منظر حقوقی، امضای الکترونیکی باتوجه به صحت انتسـاب، چگونگی اثبات و به رسمیت شـناختن آن درمحاکم مورد تردید قرار می‌گیرد. با توجه به کلیه امور نباید در مورد پذیرش امضای الکترونیکی همانند امضای سـنتی شـک کرد، زیرا امضا و مهر، روشی است برای احراز صحت انتساب یک عمل، سند و یا قراردادی به هر شخص و یا اشخاص معین، بنابراین از نظر حقوقی جای شبهه ای باقی نمی ماند که چیز دیگری هم بتواند همان اطمینان امضای سنتی را در احراز هویت ایجاد نماید و همان اعتبار قانونی را نیز داشته باشد. به بیانی شیواتر می‌توان بیان کرد که شـکل یا نوع امضا و چگونگی انجام آن مدنظر قانونگذار نیسـت بلکه انتساب سند و یا قرارداد به صاحب آن از منظر قانونی مورد اهمیت است. [۹]

با توجه به مطالب ذکر شده، چنانچه فناوری‌های روزآمد بتوانند اطمینان و اعتماد لازم را در همه زمینه ها برای کاربران اینترنت تضمین کنند و قانونگذار هم آن را بپذیرد و قابل استناد بداند، با توجه به تمام جوانب می‌توان امضای الکترونیکی را در محاکم قابل استناد دانست. [۱۰]

نتیجه گیری

در گذشـته اسـتفاده از شیوه اسناد کاغذی در معاملات تجاری، شیوه ای مرسوم بوده است. استفاده از این شیوه در اذهان حقوقدانان، پدیده‌ای ضروری محسوب می‌شد و علت آن هم اعتبار دلیل اثباتی آن بوده است، اما تجارت الکترونیک این مبنا را تغییر داده و مبنای کاغذی را به مبنای داده‌های الکترونیک مبدل سـاخته اسـت. به عبارت دیگر هرجا سخن از اسناد کتبی می‌شود، در تجارت الکترونیک اسناد الکترونیکی به صورت داده پیام، جایگزین اسناد کاغذی می‌شوند.

همان‌گونه که یک سند کتبی بدون امضای شخص قابلیت استناد ندارد، در تجارت الکترونیک هم اطلاعات باید به امضای شـخص برسـد. با وجود این در تجارت الکترونیک، امضای متداول عرفی نمی تواند مورد اسـتفاده قرار بگیرد، بلکه به عنوان جایگزین آن، امضای الکترونیکی به عنوان یک جریان فنی به عرصه ظهور رسیده است. چنین تغییر رویکردی در این زمینه سبب

شده است متخصصان حوزه جرم شناسی نیز قبل از رسمی شدن امضای الکترونیکی در کشور، اقدامـات لازم را قبـل از هر گـون تخلفی اجرایی نمایند. امضـای الکترونیکی به هر نوع عامل شناسایی الکترونیکی گفته می‌شود که به وسیله رایانه تولید شده و برای تضمین امنیت و ایجاد اعتبار در اسناد، قراردادها و داده‌های الکترونیکی پیش بینی شده است. نوشته‌های الکترونیکی مسائل حقوقی جدیدی را مطرح می کنند که مهمترین آنها اثبات این گونه دادوستدها، درستی محتـوای ذخیره شـده و تعیین هویت طرفین مبادله اسـت، به عبـارت دیگر مهمترین بخش قراردادهای الکترونیک، امضای الکترونیک، بررسی صحت و ارسال امن آن در شبکه است. برای جلوگیری از انکار امضاها، سازمان‌هایی به نام مراجع گواهی امضا به وجود آمده اند که وظیفه تأیید و تصدیق هویت فرد صاحب امضا را بر عهده دارند و از این راه داد و سـتدِ الکترونیکی، با امضای الکترونیکیِ تأیید شـده دارای وجهه قانونی می‌شـود. هویت و اعتبار این مراجع توسط یک مؤسسه قانونی دولتی مورد تأیید قرار می گیرد.

از مزایای امضاهای الکترونیک نسـبت به امضاهای دسـتی می‌توان ایمنی بیشـتر، اسـتناد پذیری دقیقتر، غیر قابل انکار بودن، سرعت و دقت و رازداری را نام برد.

تفاوت‌هـای قانونـیِ موجود در الزامات امضای مکتوب در سیاسـت‌های ملی و بین المللی با ظهور فناوری اطلاعات و ارتباطات نمود بیشـتر ی پیدا می کند. مبادلات افراد در سـطح بین المللی در محیط مجازی باعث می‌شود که الزامات قانونی امضای الکترونیکی از سطح ملی فراتر رفته و رنگ و بویی جهانی را به خود بگیرد، به طوری که اگر هر کشـوری بنا به نظام حقوقی خود، برداشت‌هایی در مورد چگونگی صحت نوشته الکترونیکی و چگونگی شکل گیری امضایِ الکترونیکی داشته باشد، این امر باعث افزایش اختلاف و تنش‌های تجاری و بین المللی می‌شود. لذا با توجه به اهمیت بحث، ضروری اسـت که تمام کشـورها از روند اسـتاندارد سازی امضا به شـکلی واحد اسـتفاده کنند، بنابراین قانونگذار باید مفاهیم ملی امضاهای مکتوب را با توجه به مفاهیم و نقش بین المللی از یک امضای الکترونیکی در دنیای مجازی جهانی، تغییر شکل دهد.

به امید آنکه هر روز شـاهد شـکل گیری بیشتر و گسترده تری از حجم مبادلات الکترونیکی در محیطی ایمن و سریع باشیم.

منابع

۱. نوری، سـید مسـعود (۱۳۸۴) **اصول حقوق تجارت الکترونیـک با تأکید بر قانون تجارت الکترونیک ایران**، فصلنامه حوزه و دانشگاه، سال یازدهم، شماره ۴۴.

۲. ماهنامه بین المللی اقتصادی- تحلیلی تجارت امروز، "امضای دیجیتالی چیسـت؟"، سـال دوم، شماره ۱۱، بهمن ۱۳۸۷.

۳. کریمـی، هـادی (۱۳۸۳) **تجارت در بسـتر مبادلات الکترونیکـی**، خبرنامه حقوق فناوری، شماره ۱۲.

4. "E-signature process management: complexity made simple"; [www.silanis.com]. January 2010.

۵. امنیـت مبادلات الکترونیکـی با نگاهی به امضای الکترونیکـی، خبرنامه حقوق فناوری، شماره۷، آذر ۸۲.

۶. زرکلام، سـتار، "قانون تجارت الکترونیک و الفبای الکترونیکی"، مجموعه مقالات همایش بررسـی جنبه‌های حقوقی فنـاوری اطلاعات، مرکز مطالعات توسـعه قضایی با همکاری شورای عالی اطلاع رسانی کشور، سلسبیل،چاپ اول، ۱۳۸۴.

7. "Electronic signatures: accelerating today's business"; [www.echosign.com]. January 2010.

۸. بختیاروند، مصطفـی(۱۳۸۴) "**مطالعه تطبیقی مقررات حاکم بر داد و سـتدهای الکترونیکی**"، مجموعه مقالات همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، مرکز مطالعات توسعه قضایی با همکاری شورای عالی اطلاع رسانی کشور، سلسبیل، چاپ اول.

۹. بررسـی موانع حقوقی توسـعه خرید و فروش الکترونیکی در ایران، مؤسسـه مطالعات و پژوهش‌های بازرگانی، تیر ۱۳۸۴.

۱۰. کروبـی، محمـد تقـی و اقبـال منوچهر(۱۳۸۴) "**امضـای دیجیتـال در ارتباطات الکترونیکی در پرتو حقوق آلمان**"، ابعاد حقوقی محیط سـایبر در پرتو توسـعه ملی، بقعه، چاپ اول.