امضای الکترونیک و جایگاه آن در ادله اثبات دعوی

مرتضی وصالی ناصح[۱]

چکیده:

یکی از عواملی که موجب اعتبار سند می‌شود، صحت انتساب آن به صادرکننده سند است که از طریق مهر یا امضاء صورت می‌گیرد و به عنوان دلیل معتبری برای تحقق اصالت و صحت انتساب آن به صادرکننده محسوب می‌شود. در بستر تجارت الکترونیک، اسناد کاغذی در حال جایگزین شدن با اسناد مبتنی بر داده‌های الکترونیک هستند. بنابراین برای اعتبار و صحت انتساب اسناد مبادلات الکترونیک لازم است یک امضای الکترونیک را جایگزین امضاهای دستی کرد. اگرچه پسوند الکترونیک ممکن است جنبه‌های فنی آن را غالب سازد که مطالعه آن بر عهده علوم رایانه‌ای است، ولی به هر حال امضاء یک تأسیس حقوقی است و از همین رو امضای الکترونیک به عنوان یکی از مباحث حقوقی تجارت الکترونیک مورد توجه علم حقوق قرار می‌گیرد. در این مقاله ضمن تعریف و بیان انواع امضای الکترونیک و بررسی جنبه‌های فنی آن، ارزش اثباتی و جایگاه آن در ادله اثبات دعوی مورد مطالعه قرار گرفته است.

واژگان کلیدی: تجارت الکترونیک، امضای الکترونیک، امضای دیجیتال، رمزنگاری، مراجع گواهی

---

۱ . سردفتر اسناد رسمی ۳۱ همدان و کارشناس ارشد حقوق خصوصی.

مقدمه:

گسترش تجارت الکترونیک مستلزم ایجاد اطمینان و اعتماد عمومی نسبت به این نوع تجارت است و این اطمینان باید از طریق تضمین امنیت و اعتبار تبادل الکترونیک داده‌ها صورت گیرد. یکی از عواملی که باعث اعتبار قرارداد یا هر سند دیگری می‌شود صحت انتساب آن به صادرکننده است که تاکنون از طریق مهر یا امضاء صورت می‌گرفته و دلیل معتبری برای تحقق صحت انتساب صادرکننده بوده است. در قراردادهای الکترونیک نیز اسناد و اطلاعات و داده پیام‌ها باید به امضای شخص صادرکننده برسد تا بتوان صحت انتساب آنها را به وی احراز کرد. بنابراین برای اعتبار و صحت انتساب اسناد قراردادهای الکترونیک لازم است یک امضای الکترونیک تعریف و جایگزین امضاهای دست‌نویس کرد. ارزش اثباتی اسناد قرارداد که به شیوه الکترونیک صادر شده‌اند ایجاب می‌کند تا ابعاد علمی و ارکان لازم برای تأثیرگذاری یک امضای الکترونیک به طور دقیق معین شود. اگرچه این موضوع بیشتر جنبه فنی دارد و برعهده علوم رایانه‌ای است، زیرا باید به دقت محدوده اعتبار و دایره اطمینان روش‌ها و نرم‌افزارهای امضای الکترونیک را مشخص کرده و شرایط و مقررات لازم برای نفوذناپذیری این تأسیس حقوقی که مورد پذیرش قوانین قرار گرفته، ابداع و معرفی نمایند، با وجود این، امضاء یک عمل حقوقی است و به همین جهت فن‌آوری امضای الکترونیک به عنوان یکی از مباحث ماهوی حقوقی تجارت الکترونیک باید از منظر علم حقوق نیزمورد توجه قرار گیرد. در این نوشتار سعی می‌شود ضمن تعریف و آشنایی با امضای الکترونیک جنبه‌های فنی و حقوقی آن مورد بررسی قرار گیرد.

۱ ـ تعریف و تاریخچه امضای الکترونیک

۱ ـ ۱ ـ تعریف امضاء و جایگاه حقوقی آن

«امضاء عبارتست از نوشتن اسم یا اسم خانوادگی (یا هر دو) یا رسم علامت خاصی که نشانه هویت صاحب علامت است، در ذیل اوراق و اسناد عادی یا رسمی که متضمن وقوع معامله یا تعهد یا قرار یا شهادت و مانند آنها است یا بعداً باید روی آن اوراق تعهد یا

معامله‌ای ثبت شود (سفید مهر)»[۱] قانون مدنی تعریفی از امضاء ارائه نکرده است. ماده ۱۳۰۱ قانون مذکور در مورد امضاء مقرر می‌دارد: «امضایی که در روی نوشته یا سندی باشد بر ضرر امضاء کننده دلیل است». بنابراین، اثر مهم امضاء متعهد شدن به تمام آثار جنبه‌های سند یا قراردادی است که امضاء شده باشد.

به طور کلی، نوشته منتسب به اشخاص در صورتی قابل استناد است که امضاء شده باشد. امضاء نشان تأیید اعلام‌های مندرج و پذیرش تعهدهای ناشی از آن است و پیش از آن نوشته را باید طرحی به حساب آورد که موضوع مطالعه و تدبر است و هنوز تصمیم نهایی درباره آن گرفته نشده است.[۲] بنابراین، هر سندی که امضاء می‌شود در واقع اعتبار می‌یابد و می‌توان آن را به شخصی منتسب نمود و وی را به مندرجات آن ملتزم ساخت.

۲ ـ ۱ ـ تاریخچه امضای الکترونیک

اولین بار کانون وکلای ایالات متحده،[۳] در سال ۱۹۹۲ میلادی در خصوص مسائل حقوقی و قانونی امضاء در قراردادهای الکترونیک شروع به کار کرد و در سال ۱۹۹۵ میلادی پیش‌نویس و رهنمودهای امضای دیجیتال[۴] را که در خصوص نحوه امضاء در قراردادهای الکترونیک و زیرساخت‌های آن بود، تهیه کرد. در همان سال اولین قانون در مورد امضای دیجیتال را تصویب کرد که در مورد ایجاد قطعیت و اعتبار قراردادهای الکترونیک و نیز فن‌آوری‌های مربوط به رمزنگاری[۵] و احراز هویت و مراجع گواهی[۶] امضای الکترونیک بود. در سال ۱۹۹۶ میلادی آنسیترال قانون نمونه‌ای در باب تجارت الکترونیک[۷] تدوین کرد که شامل مقرراتی در خصوص امضای الکترونیک بود. در سال ۱۹۹۷ میلادی، اتاق بازرگانی بین‌المللی (ICC)[۸] مبادرت به صدور «راهنمای عمومی برای

---

۱ . محمدجعفر جعفری لنگرودی، **ترمینولوژی حقوق**، ص ۸۱، چ۵، انتشارات گنج دانش، تهران ۱۳۷۰.

۲ . ناصر کاتوزیان، **اثبات و دلیل اثبات**، ج۱، ص ۲۷۸، نشر میزان، تهران ۱۳۸۰.

3. American Bar Association.

4. Digital Signature Guidelines.

5. Cryptograhy.

6.Certification Authorities(CA).

7. Uncitral Model Law on Electronic commerce.

8. International chamber of commerce (ICC).

تجارت بین‌المللی دیجیتال مطمئن»[1] کرده است. اتحادیه اروپا در سال ۱۹۹۹ میلادی، «دستورالعمل امضای الکترونیک»[2] را به تصویب رسانید و در نهایت، گروه کاری آنسیترال در باب تجارت الکترونیک، «قانون نمونه آنسیترال در باب امضای الکترونیک»[3] را تصویب کرد تا به عنوان یک معیار استاندارد و رهنمون برای قانونگذاری‌های ملی مورد استفاده کشورها قرار گیرد.[4]

بسیاری از کشورها، بین سال‌های ۱۹۹۶ تا ۲۰۰۱ میلادی، با استفاده از مقررات بین‌المللی موجود و رهنمون‌های ارائه شده در خصوص امضای الکترونیک مبادرت به قانونگذاری در این زمینه کرده‌اند. و در حال حاضر می‌توان گفت امضای الکترونیک در تمام نظام‌های حقوقی مورد پذیرش قرار گرفته است.[5]

در قانون تجارت الکترونیک ایران (مصوب سال ۱۳۸۲)، بحث امضای الکترونیک و شرایط آن مورد توجه قرار گرفته است که در بخش‌های آتی به تفصیل مورد بررسی واقع می‌گردد.

۳ ـ ۱ ـ تعریف امضای الکترونیک

قانون نمونه آنسیترال در باب امضای الکترونیک[6]، مصوب ۲۰۰۱ میلادی در تعریف امضای الکترونیک مقرر می‌دارد: «امضای الکترونیک، داده‌هایی در شکل الکترونیک است که به یک داده پیام دیگر منضم شده و یا به طور منطقی به آن ضمیمه گردیده و به عنوان وسیله‌ای برای شناسایی امضاءکننده آن داده پیام و تأیید اطلاعات موجود در آن از سوی امضاءکننده به کار گرفته شده است»[7] دستورالعمل امضای الکترونیک اروپا نیز در تعریف امضای الکترونیک بیان می‌کند: «داده‌های الکترونیک که به سایر داده پیام‌های الکترونیک منضم شده یا به نحو منطقی به آنها متصل شده و به عنوان وسیله‌ای برای مستندسازی به کار می‌رود» قانون تجارت الکترونیک ایران نیز در تعریف امضای

1. General Usage for International Digitally Ensured commerce.
2. Electronic Signatures Directive,1999.
3. Uncitral Model Law on Electronic Signatures.
4. Loran Brazel, Electronic Signatures Law and Regulation. P4, Sweet&Maxwell, London2004.
5. ibid,p5.
6. Uncitral Model Law on Electronic signature, Art. 2(a).
7. Uncitral Model Law on Electronic signature, Art. 2(1).

الکترونیک مقرر می‌دارد: «امضای الکترونیک عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده پیام است که برای شناسایی امضاء کننده داده پیام مورد استفاده قرار می‌گیرد.» [۱]

همان‌طور که از تعاریف مذکور پیداست امضای الکترونیک به هر تأییدی اطلاق می‌شود که به صورت الکترونیک ایجاد شده و ممکن است یک علامت، رمز، کلمه، عدد، یک اسم تایپ شده، تصویر دیجیتال یک امضای دست‌نویس، و یا هر نشان الکترونیک اثبات هویت باشد که توسط صادرکننده یا قائم‌مقام وی اتخاذ و به یک قرارداد و یا هر سند دیگری ملحق شده باشد. به عبارت ساده‌تر، امضای الکترونیک یک داده است که به سایر داده‌ها منضم شده و ارتباط امضاء کننده را با داده‌هایی که به آنها منضم شده مشخص می‌کند. باید پذیرفت امضای الکترونیک همانند امضای دست‌نویس دارای آثار حقوقی احراز هویت امضاءکننده سند و التزام وی به مندرجات آن را است.

۲ ـ جنبه‌های فنی امضای الکترونیک

امضای الکترونیک یک پدیده فنی و الکترونیک است و به هر طریقی که صورت گیرد بی‌نیاز از مسائل فنی و تکنولوژیک نیست. نحوه انجام امضاء، انواع، شرایط صحت و کنترل و زیرساخت‌های امضای الکترونیک و فن‌آوری‌های مربوط از جمله مسائل فنی امضای الکترونیک و برعهده علوم رایانه‌ای است. بنابراین پرداختن به مسائل مذکور علاوه بر اینکه از حوصله و توان این مقاله خارج است، مستلزم به کارگیری تعاریف و اصطلاحات علمی و پیچیده‌ای است که در تخصص علوم رایانه‌ای، الکترونیک و ریاضیات است. اما به هر حال از آنجا که امضای الکترونیک یک تأسیس حقوقی است و بخش قابل توجهی از قوانین مربوط به مبادلات الکترونیک را به خود اختصاص داده است، آشنایی اجمالی با آن در حد کلیات ضروری به نظر می‌رسد.

۱ ـ ۲ ـ انواع امضای الکترونیک

از زمان پیدایش فن‌آوری امضای الکترونیک تاکنون روش‌های مختلفی در خصوص چگونگی انجام امضاء از طریق الکترونیک و با توجه به افزایش ضریب امنیت آن معرفی و

---

۱ .ماده ۲ قانون تجارت. ۱، بند ی.

به کار گرفته شده است که مورد اشاره قرار می‌گیرد: [۱]

۱ ـ ۱ ـ ۲ کلمات عبور [۲] ـ یکی از روش‌های ساده و رایج ایجاد ایمنی و اعتبار به کارگیری یک کلمه عبور منحصر به فرد یا استفاده از یک شماره هویت شخصی (PIN) [۳] در انتهای سند است که به طور مخفی به آن منضم می‌شود.

امنیت این روش بسیار پایین است، زیرا کلمات عبور و شماره‌های شخصی افراد به راحتی توسط نفوذگرها شناسایی و به سرقت می‌روند و ممکن است توسط آنها یا دیگران مورد سوءاستفاده قرار گیرد. (مثل آنچه که در مورد کارت‌های اعتباری رخ می‌دهد)

۲ ـ۱ ـ ۲ ـ امضای بیت مپ [۴] ـ این نوع امضاء تصویر اسکن [۵] شده امضای دست‌نویس است که در آن ابتدا فرد بر روی کاغذ امضای خود را پیاده می‌کند و سپس آن را اسکن کرده و می‌تواند تصویر اسکن شده را به عنوان امضاء به هر فایلی که خواست به عنوان امضای الکترونیک منضم کند.

۳ ـ ۱ ـ ۲ ـ قلم نوری [۶] ـ فن‌آوری قلم نوری به این صورت است که هنگامی که فرد با این قلم و بر روی صفحه مخصوصی امضای خود را پیاده می‌کند، دقیقاً همان امضاء در روی صفحه مانیتور رایانه پدیدار می‌شود. یعنی امضای عادی فرد در بیرون از رایانه انجام می‌شود، ولی به همان شکل در صفحه مانیتور رایانه نمودار می‌گردد. این روش اگرچه بسیار ساده است، ولی از امنیت کافی برخوردار نیست و امکان جعل آن زیاد است.

۴ ـ ۱ ـ ۲ـ امضای بیومتریک ـ [۷] این نوع امضاء مبتنی بر ویژگی‌ها و معرف‌های زیست‌شناختی [۸] فرد یعنی خصوصیات رفتاری (مثل نحوه انجام امضای دست‌نویس) و خصوصیات فیزیولوژیک (مثل اثر انگشت) است. در این روش اگرچه ممکن است تا حد

---

1. Lorna Brazel,Electronic Signatures Law and Regulation,p38 to 39.
2. Passwords.
3. Personal Information Number (PIN).
4. Bitmap Signature.
5. Scan.
6. Light Pen.
7. Biometric Signature.
8. Biometric Identifiers.

زیادی بتوان امضاء را منحصر به فرد دانست، ولی مشکل امضای بیومتریک این است که خصیصه‌های فیزیکی و رفتاری افراد با افزایش سن، بیماری و سایر عوامل تغییر می‌کند و به همین دلیل امضای مذکور نیز مصون از اشتباه نیست.[۱]

۵ ـ ۱ ـ ۲ ـ امضای دیجیتال[۲] ـ امضای دیجیتال پیشرفته‌ترین و پرکاربردترین نوع از امضاهای الکترونیک است و به دلیل امنیت بالای آن جایگزین سایر روش‌های موجود شده و بیشتر قانونگذاران ـ از جمله قانونگذار تجارت الکترونیک ایران ـ این شیوه از امضاء را پذیرفته‌اند.[۳] امضای دیجیتال مبتنی بر علم رمزنگاری است و از دو نوع الگوریتم[۴] به نام‌های «کلید عمومی»[۵] و «کلید خصوصی»[۶] استفاده می‌کند.

۲ ـ ۲ ـ فن‌آوری و زیرساخت امضای دیجیتال

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

۱ ـ ۲ ـ ۲ ـ رمزنگاری ـ رمزنگاری علم تغییر شکل دادن نوشته‌ها و اطلاعات است یعنی از طریق آن می‌توان یک متن خوانا را تبدیل به یک متن ناخوانا و غیرقابل فهم کرد. فرآیند رمزگذاری دارای دو مرحله است؛ مرحله اول رمزسازی[۷] یعنی تبدیل یک متن ساده و عادی به یک متن رمزی است. این متن اگر در دسترس همگان هم قرار گیرد غیرقابل فهم است. مرحله دوم رمزگشایی[۸] است یعنی تبدیل متن رمز شده به یک متن عادی که

---

1. Michael Chissick, Alister Kelamn, Electronic Commerce: Law and Practice, p 182, Sweet &Maxwell, London 2002.

2. Digital Signatures.

۳ . از جمله قانون نمونه آنسیترال در باب امضای الکترونیک (مصوب ۲۰۰۱ میلادی) و دستورالعمل امضای الکترونیک اتحادیه اروپا (مصوب ۱۹۹۱ میلادی).

۴ . الگوریتم دستورهای ساده و قابل فهم رایانه است که اجرای متوالی و پشت سر هم آنها منجر به هدف معینی مثل حل یک مسأله می‌گردد. واژه الگوریتم برگرفته از نام ریاضیدان بزرگ ایرانی یعنی خوارزمی است.

5. Public Key.

6. Private Key.

7. Encryption.

8. Decryption.

قابل فهم باشد.[۱]

۲ ـ ۲ ـ ۲ ـ رمزنگاری کلید عمومی ـ[۲] رمزنگاری مبتنی بر کلید عمومی یا رمزنگاری «اسیمتریک»[۳] از دو الگوریتم تشکیل شده است که یکی از آنها برای ایجاد امضای دیجیتال و تبدیل آن به یک متن بی‌معنی استفاده می‌شود و دیگری برای تبدیل متن غیرقابل فهم به شکل اولیه آن به کار می‌رود.[۴] به این دو الگوریتم، اصطلاحاً کلید گفته می‌شود. الگوریتم اول مخصوص شخص امضاءکننده است و کلید شخصی نامیده می‌شود و الگوریتم دوم که برای صحت امضاء و تطبیق و سنجش کلید اختصاصی به کار می‌رود.[۵] در واقع، این دو کلید از نظر ریاضی به هم مرتبط هستند. از بین این جفت کلید یکی برای ایجاد امضای دیجیتال و تبدیل داده‌ها به شکل نامرئی و غیرقابل فهم و کلید دیگر جهت شناسایی امضای دیجیتال و یا برگرداندن پیغام رمزنگاری شده به شکل اولیه آن به کار می‌رود. تجهیزات رایانه‌ای و نرم‌افزاری که از این دو کلید استفاده می‌کنند سیستم رمزنگاری اسیمتریک یا رمزنگاری نامتقارن نامیده می‌شود.[۶]

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

۳ ـ ۲ ـ ۲ ـ نحوه ایجاد یک امضای دیجیتال

برای ایجاد یک امضای دیجیتال، ابتدا امضاءکننده باید از طریق کلید عمومی امضای خود را رمزسازی کرده و سپس آن را ضمیمه پیام داده‌ای کند و برای مخاطب خویش ارسال نماید. مخاطب که اکنون پیام داده‌ای را به همراه امضای دیجیتال منضم شده به آن

---

1. Loran Brazel, Electronic Signatures Law and Regulation, p 49.

2. Public Key Cryptography.

۳ . رمزنگاری اسیمتریک (Asymmetric) یا نامتقارن در مقابل رمزنگاری سیمتریک (Symmetric) یا متقارن به کار برده می‌شود.

۴ . مصطفی السان، امین دوان یامچی، «ماهیت رایانه‌ای و جنبه‌های حقوقی امضای دیجیتالی» مجله دیدگاه‌های حقوقی، ش ۳۰ و ۳۱، بهار ۱۳۸۳، ص ۲۷.

۵ . همان، ص ۲۸.

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

دریافت کرده، باید امضای رمزنگاری شده را که قابل فهم نیست از داده پیام‌ها جداساخته و از طریق کلید عمومی ارسال کننده (که در فهرست عمومی مرجع گواهی امضاء موجود است) پیام را برای وی ارسال می‌کند تا خود ارسال‌کننده (اصل ساز) با کلید خصوصی‌اش آن را رمزگشایی کند. چنانچه نتایج یکسانی حاصل شد، یعنی همان چیزی که امضاء کننده به عنوان امضای دیجیتال برای خود تعریف کرده بود هویدا شد، معلوم می‌شود که اولاً امضای مذکور به نحو صحیحی از سوی امضاءکننده ارسال شده و ثانیاً وی نمی‌تواند ادعا کند که پیام را امضاء نکرده و یا اینکه پیام تغییر یافته است.[1]

بنابراین، به کارگیری امضای دیجیتال شامل دو فرآیند است: مرحله اول ایجاد امضاء توسط ارسال‌کننده پیام توسط کلید خصوصی‌اش است و مرحله بعد نیز شامل فرآیند چک کردن امضای دیجیتال از طریق مراجعه به پیام اصلی و استفاده از کلید عمومی ارسال کننده است.

۳ ـ ۲ ـ مرجع گواهی امضاء[2]

اگرچه استفاده از روش امضای دیجیتال تمامیت سند، محرمانه بودن اطلاعات (در صورت لزوم) و امنیت داده‌ها تضمین می‌شود، اما یک مسأله مهم هنوز باقی است و آن هم تضمین هویت امضاءکننده است. از نظر حقوقی، مهم‌ترین اثر امضاء اثبات رابطه سند با کسی است که امضاء به او نسبت داده شده است. امضای الکترونیک هر چند که از امنیت بالایی هم برخوردار باشد، ولی قادر به تضمین هویت امضاءکننده نیست و این همان مشکل تعیین هویت در سیستم‌های باز است که طرفین یک مبادله در خصوص حقوق تکالیف خود توافقی نکرده و همدیگر را نمی‌شناسند.

ساز و کار احراز و تضمین هویت در فضای سنتی از طریق ثبت اسناد در مرجع ثالثی تحت عنوان دفاتر اسناد رسمی صورت می‌گیرد که با احراز هویت امضاءکنندگان سند و رعایت برخی تشریفات قانونی به اسناد، اعتبار و رسمیت می‌بخشد. در بستر مبادلات الکترونیک نیز وجود چنین مرجع ثالثی برای تعیین هویت امضاءکننده ضروری است. این

1. Edward H.Freeman,J.D,Digital Signatures and Electronic Contracts.PA, Technology Law Journal, 391, 2001.

2. Certification Authority (CA).

مرجع تحت عنوان مرجع گواهی شناخته می‌شود، زیرا از طریق صدور یک گواهی نامه دیجیتال هویت امضاءکننده را تضمین می‌کند.

گواهی‌نامه دیجیتال یک کلید عمومی را برای اشخاص (حقیقی یا حقوقی) تعریف و تصدیق می‌کند. صدور این گواهی‌نامه توسط یک مرجع معتبر و موثق که به آن مرجع گواهی گویند، تأیید می‌گردد. لذا از این طریق اثبات می‌شود که کلید عمومی مذکور فقط مختص یک شخص خاص است.[۱]

شبکه مراجع گواهی و پایگاه‌های داده‌ای و ساختار عملکرد آنها تحت عنوان ساختار کلیدعمومی (PKI)[۲] شناخته به شرح ذیل است:[۳]

۱ ـ تقاضای صدور گواهی امضا از مرجع گواهی توسط ارسال‌کننده پیام داده‌ای

۲ ـ صدور گواهی امضاء پس از احراز هویت و معرفی ارسال‌کننده به کلیدهای عمومی و خصوصی از سوی مرجع گواهی

۳ ـ ارسال پیام داده‌ای همراه با امضای دیجیتال برای مخاطب از طرف ارسال‌کننده

۴ ـ ارسال امضاء به مرجع گواهی برای تصدیق هویت امضاء کننده و اطمینان از صحت آن توسط مخاطب

۵ ـ بررسی صحت و سقم پیام داده‌ای و انتساب آن به ارسال‌کننده توسط مرجع گواهی

۶ ـ ارسال گواهی صحت امضاء از سوی مرجع گواهی برای مخاطب

۷ ـ پاسخ مخاطب به ارسال‌کننده با یک امضای دیجیتال

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

---

1. ibid,p4.
2. Public Key Infrastructure(PKI).
3. Michael Chissik, Alister Kelman, Electronic Commerce: Law and practice.p182.

شرح وظایف و مسئولیت‌های مراجع گواهی به تفصیل در قوانین و مقررات بیان شده است. قوانین بین‌المللی موجود در خصوص امضای الکترونیک در مورد مقررات مراجع گواهی ساکت هستند و آن را به قوانین ملی واگذار کرده‌اند. قانون تجارت الکترونیک ایران نیز از مراجع گواهی تحت عنوان «دفاتر خدمات صدور گواهی الکترونیکی»[1] نام برده و باب دوم خود را به آن اختصاص داده است. ماده ۳۱ این قانون مقرر می‌دارد: «دفاتر خدمات صدور گواهی الکترونیکی واحدهایی هستند که برای ارائه خدمات صدور امضای الکترونیکی در کشور تأسیس می‌شوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به روز نگهداری گواهی‌های اصالت (امضای) الکترونیک می‌باشد» ماده ۳۲ نیز بیان می‌کند: «آیین‌نامه‌ها و ضوابط تأسیس و شرح وظایف این دفاتر توسط سازمان مدیریت و برنامه‌ریزی کشور و وزارت‌خانه‌های بازرگانی، ارتباطات و فن‌آوری اطلاعات، امور اقتصادی و دارایی و دادگستری تهیه و به تصویب هیأت وزیران خواهد رسید» مراجع گواهی امضاء به دلیل نیاز به زیرساخت‌های فنی، تجهیزات و تأسیسات شبکه‌ای پیشرفته و استانداردهای ایمنی بالا، هنوز در ایران راه‌اندازی نشده‌اند.

۳ ـ جنبه‌های حقوقی امضای الکترونیک

اینکه چه چیزی می‌تواند به عنوان امضای الکترونیک استفاده شود یک مسأله حقوقی است، زیرا پردازش فنی اطلاعات یا داده‌ها زمانی می‌تواند به عنوان امضاء به کار گرفته شود که قانون چنین اعتبار و اجازه‌ای به آن داده باشد. بنابراین پس از اینکه علوم رایانه‌ای توانستند یک امضاء از طریق الکترونیک ایجاد کرده و امنیت آن را حداقل به اندازه امضاهای دست‌نویس تأمین کنند، آنگاه نوبت به علم حقوق می‌رسد تا در مورد مسائل حقوقی آن وارد عمل گردد. بنابراین، در مورد امضای الکترونیک ابتدا نگاه‌ها معطوف جنبه‌های اجرایی، فنی و تأمین امنیت آن است و سپس نوبت به جنبه‌های قانونی و حقوقی می‌رسد.

۱ ـ ۳ ـ ماهیت امضای الکترونیک

تا قبل از پیدایش امضای الکترونیک، مهر و امضای دست‌نویس برای انتساب اسناد و

1. Certification Service Provider.

اعمال به اشخاص به کار گرفته می‌شد. و به جز ممنوعیت استفاده از مهر در چک، هر دو از کاربرد و ارزش یکسانی برخوردار هستند. در مورد چک ماده ۳۱۱ قانون تجارت تصریح دارد که چک باید به «امضا»ی صادرکننده برسد. [۱] بنابراین بسیاری از حقوقدان‌ها معتقدند که قانونگذار صدور چک را فقط از طریق امضای صادرکننده پذیرفته است و با توجه به صراحت ماده ۳۱۱ قانون تجارت که از مهر نامی برده نشده، لذا نمی‌توان در صدور چک از مهر استفاده کرد. [۲] زیرا اولاً قانونگذار نمی‌خواسته افراد بی‌سواد چک صادر کنند و ثانیاً ماده ۲۲۳ قانون تجارت در مورد برات، علاوه بر امضاء، مهر را نیز معتبر دانسته، ولی در ماده ۳۱۱ قانون مذکور سخنی از مهر به میان نیامده است. بنابراین، صدور چک فقط با امضاء امکان‌پذیر است و این امضاء هم لزوماً باید دست‌نویس باشد یعنی امضای شخصی که به صورت مهر درآمده نیز برای صدور چک معتبر نیست. [۳] بنابراین، طرح این بحث که امضای الکترونیک در ردیف مهر قرار می‌گیرد یا امضای دست‌نویس در خصوص صدور چک‌های الکترونیک ـ به عنوان یکی از روش‌های پرداخت در قراردادهای الکترونیک ـ اهمیت پیدا می‌کند.

برخی حقوقدان‌ها امضای الکترونیک را در ردیف مهر آورده‌اند، زیرا از نظر ماهیتی با امضای دست‌نویس تفاوت دارد و در مقام مقایسه بیشتر به مهر شباهت دارد. امضای الکترونیک چیزی جز یک سری فرمول‌های ریاضی نیست که از سوی مراجع گواهی امضاء تأیید و در اختیار افراد قرار می‌گیرد و اگرچه تحت عنوان امضاء نام گرفته‌اند، ولی چون توسط شخص ثالثی تولید و به اشخاص اختصاص داده می‌شوند و اشخاص فقط آنها را به شکلی که هستند مورد استفاده قرار می‌دهند، در تحلیل حقوقی در ردیف مهر قرار می‌گیرند. [۴]

---

۱ . ماده ۳۱۱ قانون تجارت بیان می‌کند: «در چک باید محل و تاریخ صدور قید شده و به امضای صادرکننده برسد...»

۲ . حسن حسنی، **حقوق تجارت**، ص ۵۱۷، نشر میزان، تهران ۱۳۷۸ ، امیرحسین فخاری، «جزوه درسی حقوق تجارت ۳»، دانشگاه امام صادق (ع)، نیم‌سال دوم تحصیلی ۸۱ ـ ۱۳۸۰.

۳ . امیرحسین فخاری، «جزوه درسی حقوق تجارت ۳»، دانشگاه امام صادق (ع)، نیم‌سال دوم تحصیلی ۸۱ ـ ۱۳۸۰.

۴ . امیر صادقی‌نشاط، «تحلیل حقوقی جنبه‌هایی از پرداخت الکترونیک»، مجموعه مقالات همایش

طبق ماده ۷ قانون تجارت الکترونیک ایران، «هرگاه قانون، وجود امضاء را لازم بداند، امضای الکترونیک مکفی است» یعنی امضای الکترونیک هر ماهیتی که داشته باشد (مهر، امضاء یا ماهیت دیگر) از نظر قانون جایگزین امضای دست‌نویس با آثار حقوقی مشابه شده است.

۲ ـ ۳ ـ پذیرش قانونی امضای الکترونیک

به موازات گسترش و فراگیری مبادلات الکترونیک، موج قانونگذاری در این زمینه نیز در سال‌های اخیر (بین سال‌های ۱۹۹۶ تا ۲۰۰۱ میلادی) قابل توجه بوده است. بیشتر کشورها که به بسترسازی تقنینی تجارت الکترونیک روی آوردند، یکی از مهم‌ترین موضوعاتی که پیش روی داشتند، پذیرش امضای الکترونیک بود. در حال حاضر، بیشتر این کشورها این نوع امضاء را بدون هیچ تردیدی به عنوان یکی از اعمال دارای آثار حقوقی همسان با امضای دستی مورد پذیرش قرار داده‌اند. در برخی کشورها حتی قوانین و لوایح مستقلی برای امضای الکترونیک وضع شده است. در کشور اسپانیا «لایحه قانونی امضاهای الکترونیک اسپانیا»[1] در سال ۱۹۹۹ میلادی و در آلمان نیز «قانون امضای الکترونیک»[2] در سال ۲۰۰۰ میلادی به تصویب رسیده است. ولی اغلب کشورها امضای الکترونیک را در قوانین مربوط به مبادلات و ارتباطات الکترونیک پیش‌بینی کرده‌اند. اولین قانونگذاری در مورد امضای الکترونیک در «قانون متحد الشکل مبادلات الکترونیک»[3] ایالت «یوتا»ی ایالات متحده به تصویب رسید. سنگاپور در سال ۱۹۹۸ میلادی در «قانون مبادلات الکترونیک سنگاپور»[4] و کانادا نیز در «قانون متحدالشکل تجارت الکترونیک»[5] در سال ۲۰۰۰ میلادی امضای الکترونیک را مورد پذیرش قرار داده‌اند. حتی کشور انگلستان، که نظام حقوقی آن مبتنی بر کامن لا (حقوق عرفی) است نیز ناگزیر از قانونگذاری در این خصوص است. زیرا طبق دستورالعمل شماره ۲۰۰۰/۳۱ اتحادیه اروپا که

بررسی ابعاد حقوقی فن‌آوری اطلاعات، خرداد ۱۳۸۳، ص ۱۷۲.

1. Spain's Electronic Signatures Bill(1999).
2. Electronic Signature Act (2000).
3. Uniform Electronic Transaction Act (1996).
4. Singapore Electronic Transaction Act (1998).
5. Uniform Electronic commerce Act (2000).

ناظر به برخی از جنبه‌های حقوقی تجارت الکترونیک است دولت‌های عضو موظف هستند که نظام‌های حقوقی آنها تشکیل قرارداد از طریق واسطه‌های الکترونیک و سایر مقتضیات آن را تضمین کنند.[۱] در همین راستا کشور انگلستان نیز در سال ۲۰۰۲ میلادی مبادرت به تصویب «مقررات امضاهای الکترونیک»[۲] کرد. در کشور فرانسه نیز اگرچه قانون خاصی در این زمینه تصویب نشده اما به تبعیت از دستورالعمل مذکور ماده ۱۳۱۶ قانون مدنی فرانسه، در سال ۲۰۰۰ میلادی و در راستای پذیرش امضای الکترونیکی و نیز به رسمیت شناختن اسناد الکترونیک به عنوان دلیل معتبر اصلاح گردیده است.

در قوانین و سازمان‌های بین‌المللی نیز، همان‌طور که قبلاً بیان شد دستورالعمل‌ها و رهنمون‌های خویش مقرراتی در خصوص امضای الکترونیک وضع کرده‌اند. از جمله می‌توان به دستورالعمل امضای الکترونیک اتحادیه اروپا، مصوب ۱۹۹۹ میلادی و نیز «قانون نمونه آنسیترال در باب امضای الکترونیک، مصوب ۲۰۰۱ میلادی»، اشاره کرد. کشور ایران نیز در قانون تجارت الکترونیک خویش صریحاً امضای الکترونیک را به رسمیت شناخته است. طبق ماده ۷ قانون مذکور: «هرگاه قانون، وجود امضاء را لازم بداند امضای الکترونیکی مکفی است».

۳ ـ ۳ ـ ارزش اثباتی امضای الکترونیک

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

---

۱. بند یک ماده ۹ دستورالعمل مقرر می‌دارد: «دولت‌های عضو باید تضمین‌کنند که نظامهای حقوقی ایشان تشکیل قرارداد از طریق وسایل الکترونیک را مجاز می‌شمارد. دول عضو به ویژه باید تضمین کنند که مقتضیات قانونی قابل اعمال در روند تشکیل یک قرارداد، هیچ مانعی برای انعقاد قراردادهای الکترونیک ایجاد نمی‌کند و نیز نباید به خاطر اینکه قراردادهای مذکور از طریق وسایل الکترونیک ایجاد شده‌اند، فاقد اعتبار و قابلیت اجرا تلقی کردند.»

2. Electronic Signatures Regulation (2002).

است و همان طور که بیان شد داده پیام‌ها نیز دارای ارزش اثباتی هستند.[۱] اما باید گفت که به طور کلی ارزش اثباتی داده پیام‌ها، با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به کار گرفته شده تعیین می‌شود.[۲] حال چنانچه داده پیام‌های تشکیل‌دهنده امضاء از تمام شرایط فنی لازم برخوردار باشند اعتبار حقوقی و جایگاه آنها در ادله اثبات دعوی همانند جایگاه امضاهای دست‌نویس است و می‌تواند به عنوان دلیل در مقام دعوی یا دفاع در محاکم مورد پذیرش قرار گیرد.

در قانون تجارت الکترونیک ایران از امضایی که تمام شرایط فنی را برخوردار است تحت عنوان «امضای الکترونیکی مطمئن»[۳] نام برده شده است. طبق ماده ۲ قانون مذکور امضای الکترونیکی مطمئن، امضایی است که شرایط ماده ۱۰ همان قانون را داشته باشد. شرایط ماده ۱۰ قانون تجارت ایران نیز برای امضاء و سابقه الکترونیکی مطمئن این است که چنین امضایی باید:

الف) نسبت به امضاءکننده منحصر به فرد باشد.

ب) هویت امضاءکننده داده پیام را معلوم نماید.

ج) به وسیله امضاءکننده و یا تحت اراده انحصاری وی صادر شده باشد.

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

طبق ماده ۱۵ قانون تجارت ایران نسبت به امضایی که با شرایط فوق ایجاد شده است نمی‌توان ادعای انکار و تردید کرد و تنها می‌توان نسبت به آن ادعای جعل کرد. بنابراین، منضم شدن امضای الکترونیک به داده پیام‌ها، آنها را در حکم اسناد رسمی قرار می‌دهد. بنابرآنچه گفته شد، امضای الکترونیک هیچ تفاوتی از حیث آثار حقوقی با سایر امضاهای دستی ندارد بلکه حتی با فراهم شدن زیرساختهای فنی لازم، می‌توان گفت چنین امضایی کمتر در معرض جعل قرار می‌گیرد.

نتیجه‌گیری:

---

۱. مواد ۶ و ۱۲قانون تجارت ایران.

۲. ماده ۱۳ قانون تجارت ایران.

3. Secure/ Enhanced/ Advanced Electronic Signature.

فراگیر شدن تجارت الکترونیک مستلزم تضمین اعتبار و امنیت آن توسط نظام‌های حقوقی است. یکی از مهم‌ترین ابزارهای اعتبار دهی به مبادلات الکترونیک، پذیرش امضای الکترونیک و فراهم کردن مقتضیات فنی آن است. در حال حاضر امضای الکترونیک به عنوان یکی از اعمال دارای آثار حقوقی همسان با امضای دستی مورد پذیرش قانونی نظام‌های حقوقی دنیا (از جمله کشور ایران) قرار گرفته و جایگاه خود را در ادله اثبات دعوی تثبیت کرده است. امضای الکترونیک هیچ تفاوتی از حیث آثار حقوقی با سایر امضاهای دست نویس ندارد یعنی چنانچه امضای الکترونیک از تمام شرایط فنی لازم برخوردار باشد و ایمنی آن توسط علوم رایانه‌ای تضمین گردد، آنگاه از همان اعتبار و جایگاه امضای دست‌نویس در ادله اثبات دعوی برخوردار خواهد بود و می‌تواند به عنوان دلیل در مقام دعوی یا دفاع مورد استناد قرار گیرد.