ماهیت رایانه‌ای و جنبه‌های حقوقی امضای دیجیتالی

مصطفی السان*

امین دوان یامچی**

امضای هر شخص به معنی تایید هر نوشته‌ای است که وی تصمیم به پذیرش مفاد آن دارد. در این مقاله آنچه بررسی می‌شود ماهیت رایانه‌ای این تایید و تصدیق در حالتی است که امضا و متن هر دو به هر دلیل به شیوه‌ای الکترونیکی ایجاد شده باشد. بعد از بررسی نحوه شکل‌گیری الکترونیکی یک امضا، به این بحث خواهیم پرداخت که تلقی علم حقوق از امضای دیجیتالی به عنوان پدیده‌ای جدید چیست و اگر علم حقوق آن را مورد شناسایی قرار می‌دهد، چه ضوابطی برای تاثیرگذاری امضای الکترونیکی در نظر می‌گیرد؟

کلید واژه‌ها: تجارت الکترونیکی، استانداردهای امضای دیجیتالی، جنبه‌های حقوقی، ماهیت رایانه‌ای، حقوق تطبیقی و مقررات آنسیترال.

---

* دانشجوی دکتری حقوق خصوصی دانشگاه شهید بهشتی.

** کارشناس مهندسی کامپیوتر.

مقدمه

در تجارت امروز اطمینان از چهار چوب اطلاعات رایانه‌ای نیاز به آشنایی و مهارت حرفه‌ای در هر دو عرصه حقوق و کامپیوتر دارد. آنچه بدیهی است این می‌باشد که این آشنایی به سهولت انجام نمی‌شود. بیگمان مفهوم تاریخی امضا در علم حقوق به عنوان هر نشانه‌ای که در شناسایی شخص گذارنده آن علامت کمک کار است، با مفهومی که در علم کامپیوتر از امضا مدنظر می‌باشد، تفاوت اساسی دارد. در این راستا چاره‌ای جز یکی از دو کار نیست: یا باید امضای دیجیتالی را از نظر علم حقوق نپذیرفت که در این صورت دهکده جهانی تاوان سنگینی خواهد پرداخت. زیرا احتمال عدم شناسایی اکثر قراردادها به دلیل بی‌اعتباری امضای مندرج در آن وجود دارد.

راه حل دیگر این است که امضای دیجیتالی از نظر حقوقی مورد پذیرش باشد. مطمئناً حقوق در این پذیرش بی‌قید و بند عمل نخواهد کرد و تمام ابعاد قضیه از جمله رعایت استانداردها، مناسب بودن نرم افزار بکار رفته، نفوذ ناپذیری سیستم امضا و تمام ضوابط علمی یک امضای صحیح را مد نظر قرار خواهد داد.

پیشرفت روز افزون فناوری رایانه‌ای، به کارگیری آن را در امور تجاری ناگزیر می‌نماید. امضای الکترونیکی نیز از دستاوردهای این پیشرفت است که می‌توان از آن در قراردادهای الکترونیکی استفاده نمود. ارزش اثباتی سند قرار داد حتی اگر به شیوه الکترونیکی صادر شده باشد، ایجاب می‌کند تا ابعاد علمی و ارکان لازم برای تاثیر گذاری یک امضای دیجیتالی به طور دقیق معین شده و تدوین گردد. انجام این مهم بر عهده علوم رایانه‌ای است، زیرا باید به دقت محدوده اعتبار و دایره اطمینان روش‌ها و نرم‌افزارهای امضای دیجیتالی را در گستره شبکه جهانی اینترنت مشخص نموده و قواعد علمی و منسجمی برای نفوذ ناپذیری این تاسیس، که همانطور که گفته خواهد شد مورد پذیرش قانون قرار گرفته، ابداع و معرفی نماید.

به دلیل اهمیت تجارت الکترونیکی و روند افزایش آن در سطح جهانی که پیوستن کشورمان

را به این شیوه مرسوم و تسهیل کننده اقتصادی ایجاب می‌کند. در این مقاله مشترک در صدد بررسی ماهیت رایانه‌ای و جنبه‌های حقوقی امضای دیجیتالی برآمدیم. مطالعه موضوع در دو فصل جداگانه، اولی «ماهیت رایانه‌ای امضای دیجیتالی» و دومی «جنبه‌های حقوقی امضای دیجیتالی» انجام خواهد شد. اما ابتدا لازم است در پیشگفتار به ارایه تعریفی از امضای دیجیتالی بپردازیم. این نکته اضافه شود که سعی شده تا مطلب به ساده‌ترین شکل ممکن بیان شود و لذا اگر در مواردی پیچیدگی خاصی دیده می‌شود به دلیل ماهیت ویژه و علمی موضوع، و امری غیر قابل احتراز می‌باشد.

پیشگفتار

تعریف امضای دیجیتالی

تعاریف متعددی از امضای دیجیتالی به عمل آمده که فقط به ذکر چند تعریف و بررسی آنها اکتفا می‌شود.

۱ـ "امضای دیجیتالی محتوای پیام را تایید و امضا کننده را تصدیق می‌کند. همچنین روشی برای اینکه اثبات شود مدرکی توسط فرستنده خاص ارسال شده فراهم می‌آورد."[۱]

۲ـ در قانون نمونه آنسیترال درباره امضاهای الکترونیکی که در ۵ ژوئیه ۲۰۰۱ به تصویب رسیده، امضای الکترونیکی چنین تعریف شده است:

"امضای الکترونیکی به معنای داده‌ای در شکل الکترونیکی است که به یک داده پیام[1] ضمیمه شده یا جزء همسان، پیوسته و جدا ناپذیری از آن شده است؛ که می‌تواند برای شناسایی امضا کننده آن داده پیام و تایید اطلاعات موجود در داده پیام از سوی امضا کننده به‌کار گرفته شود."[۲]

به موجب این تعریف امضای یک شخص در زیر یک متن در محیط الکترونیکی به هر شکل

---

1. Data Messaga

که باشد نشانگر این است که وی محتوای متن را قبول دارد که این قاعده در مورد اطلاعاتی که به صورت کاغذی هستند نیز صدق میکند.

۳ـ در فرهنگ لغت معروف Baby lon امضای دیجیتالی چنین تعریف شده است: «یک رمز دیجیتالی که می‌تواند به پیام الکترونیکی ارسال شده‌ای ضمیمه شده و به طور کامل ارسال کننده آن را شناسایی نماید. هدف از امضای مکتوب (دستی) این می‌باشد که تعیین کند، آیا شخص ارسال کننده یک پیام واقعاً همان شخص مورد نظر است. یا نه امضای دیجیتالی دارای اهمیت زیادی در تجارت الکترونیکی بوده و یکی از ابزارهایی است که برای توثیق[1] (تعیین هویت طرف معامله) به کار می‌رود.

امضای دیجیتالی در صورتی دارای اعتبار است که قابل جعل نباشد. برای تضمین این حد از اطمینان فناوری‌های رمزگذاری مختلفی وجود دارد».

از مجموع تعاریف فوق استنباط می‌گردد که اگر امضای دیجیتالی با رعایت اصول ایمنی و علمی ایجاد شود، همانند امضای مندرج در "اسناد کاغذی" قابل استفاده و دارای اعتبار قانونی است. در فصل اول به ماهیت رایانه‌ای امضای دیجیتالی پرداخته می‌شود.

1. Authentication

فصل اول: ماهیت رایانه‌ای امضای دیجیتالی

گفتار اول: ماهیت امضای دیجیتالی

اول ـ مفهوم امضای دیجیتالی

همانطور که گفته شد امضای دیجیتالی نوعی رمزگذاری الکترونیکی است که برای مشخص کردن هویت یک پیام یا برای علامت گذاری یک متن بکار می‌رود و نیز در مواردی از طریق امضای مذکور می‌توان اطمینان حاصل کرد که محتوای پیام یا متن توسط فرد دیگری تغییر نخواهد یافت. امضای دیجیتالی به راحتی قابل انتقال است و می‌توان آن را برای انواع پیام‌های کدگذاری شده یا کدگذاری نشده بکار برد.[۳]

دوم ـ مبنای علمی امضای دیجیتالی

امضای دیجیتالی توسط علم رمزگذاری[۱] بوجود آمده است، علم رمزگذاری علمی است که با استفاده از ریاضیات و روش‌های سخت‌افزاری و نرم‌افزاری دیگر، پیامی را به یک متن بی معنی تبدیل می‌نماید و گیرنده دوباره با همان الگوریتم این متن بی معنی را به پیام مورد نظر خویش تبدیل می‌کند.[۴]

امضای دیجیتالی از نوع خاصی از علم رمز گذاری استفاده می‌کند و دو الگوریتم[۲] متفاوت که هر دو مشتق از روش‌های ریاضی هستند را به کار می‌برد. یکی از الگوریتم‌ها برای ایجاد امضای دیجیتالی و تبدیل آن به یک نوع بی معنی یا به عبارتی دیگر برای کدگذاری امضاء و

---

1. Cryptography

۲. الگوریتم: دستورات ساده و قابل فهم کامپیوتر که اجرای پشت سر هم آنها منجر به هدف معینی (برای مثال حل مسأله‌ای) می‌شود. این دستورات گام به گام اجرا می‌شوند و در صورت درست بودن محاسبات در مرحله‌ای خاص به نتیجه می‌رسند. واژه الگوریتم برگرفته از نام ریاضیدانان بزرگ ایرانی "خوارزمی" است.

دیگری برای حصول اطمینان از صحیح بودن امضا و تبدیل پیام به شکل اولیه به کار می‌رود. به این نوع الگوریتم به اصطلاح کلید[۱] گفته می‌شود. الگوریتم اول مخصوص شخص امضا کننده بوده و کلید شخصی[۲] نامیده می‌شود و دومی حالت عمومی داشته و برای حصول اطمینان از صحت امضا به کار می‌رود و به آن به کلید عمومی[۳] گفته می‌شود.

چون همه افراد باید از درستی امضای شخص مورد نظر اطمینان یابند، کلید عمومی باید در اختیار همه افراد قرار گیرد. یکی دیگر از توابع پایه‌ای و مهم تابع هش[۴] می‌باشد که در هر دو کلید عمومی و شخصی بکار می‌رود. تابع هش الگوریتمی است که جایگزین دیجیتالی یا اثر انگشت از نوع هش ایجاد می‌کند که دارای اندازه استانداردی بوده و به صورت یگانه و واحد می‌باشد. هر تغییری در پیام باعث تغییر در جواب الگوریتم هش می‌شود.

با توجه به آنچه گفته شد استفاده از دو فرایند در امضای دیجیتالی ضروری است که یکی توسط امضا کننده و دیگری توسط گیرنده امضای دیجیتالی به کار می‌رود. امضاء کننده از یک الگوریتم هش که در امضای مورد نظر جوابی واحد دارد، استفاده می‌کند لذا در کلید شخصی از همین الگوریتم استفاده می‌شود.

برای حصول اطمینان از صحت امضای دیجیتالی از یک کلید عمومی استفاده می‌شود که این کلید خروجی، الگوریتم هش را که به گیرنده ارسال شده به شکل امضای معمولی تبدیل می‌کند.

برای امضا کردن یک متن یا هر چیز دیگری ابتدا باید امضا کننده محدوده صحت امضا، یعنی اینکه چه چیزی می‌خواهد امضا نماید را تعیین کند. سپس تابع هش در نرم‌افزار امضا

---

1. Key
2. Private Key
3. Puplic Key
۴. Hash Function: محاسبات ریاضی که برای اثبات عدم تغییر یا درستکاری پیام‌های مبادله شده در روابط تجاری الکترونیکی به کار می‌رود.

کننده یک خروجی هش را به امضای دیجیتالی تبدیل می‌کند؛ لذا امضای مورد نظر منحصر به فرد خواهد بود.

برای کدگشایی امضای دیجیتالی باید از الگوریتم هش دیگری همانند الگوریتمی که برای ایجاد امضا به کار رفته استفاده شود. با استفاده از کلید عمومی و یک خروجی هش جدید نمایه[1] کدگشا معین می‌کند که این امضا توسط کلید شخصی مورد نظر ایجاد شده یا توسط کلید دیگری بوجود آمده است. بنابراین نرم‌افزار کدگشا قادر به کدگشایی امضای دیجیتالی در صورت حصول شرایط زیر است:

۱) امضاکننده از یک کلید شخصی مورد نظر که با کلید عمومی رمزگشایی در ارتباط است، استفاده کرده باشد.

۲) الگوریتم هش مربوطه، به کدگشا همان خروجی را بدهد که امضای الگوریتم هش مربوطه به کلید شخصی داده است. علوم رمزگذاری مختلف از الگوریتم‌های متفاوتی برای ایجاد امضای دیجیتالی استفاده می‌کنند؛ ولی این الگوریتم‌ها از بسیاری لحاظ با هم شباهت دارند.

در فرآیند ایجاد و رمزگشایی امضای دیجیتالی، با توجه به آنچه برای امضا کردن ضروری است، قوانین زیر مراعات می‌گردد:

۱) قانون امضاکننده: اگر کلید عمومی و شخصی هر دو توسط امضاکننده ایجاد شده باشد، در آن صورت امضای دیجیتالی انجام شده و ویژگی‌های انحصاری آن را نمی‌توان جعل کرد؛ حتی اگر امضاکننده کنترل کلید شخصی را از دست بدهد، مثلاً فراموش کند که این کلید از چه وسایل و امکاناتی برای رمزگذاری استفاده می‌کند.

۲) قانون پیام: چون امضای دیجیتالی با پیام مربوطه همسان می‌شود و کد واحدی دارند، لذا پیام باید به گونه‌ای باشد که کلید عمومی بتواند آن را رمزگذاری نماید.[۵]

---

1. checksum

گفتار دوم: استانداردهای امضای دیجیتالی

اول ـ طرح گفتار

رمزگذاری و رمزگشایی بوسیله دو کلید متفاوت انجام می‌شود که به یکی از آنها صرفاً شخص امضاکننده دسترسی دارد و کلید شخصی نامیده می‌شود و دیگری در دسترس همگان بوده و کلید عمومی به حساب می‌آید. در خصوص این دو کلید در گفتار اول به تفصیل بحث شد.

امضای دیجیتالی پیام خلاصه شده‌ای است که به وسیله یک کلید شخصی رمزگذاری می‌گردد. گیرنده می‌تواند با استفاده ازکلید عمومی که در اختیار دارد آن را کدگشایی کرده و بخواند.

در ایالات متحده، موسسه ملی استاندارد و تکنولوژی[۱] بین سال‌های ۹۴ـ۱۹۹۱ استانداردی برای امضا دیجیتالی منتشر نمود. در استرالیا نیز در سال ۱۹۹۶ با عنوان "چهار چوب امنیتی کلید عمومی"[۲] به تصویب رسید که مربوط به امضای دیجیتالی بوده و استانداردهای خاصی برای آن در نظر گرفته است.

یکی از مهم‌ترین مواردی که در امضای دیجیتالی باید مدنظر باشد، سری بودن کلید شخصی است که برای این کار از علم رمزگذاری استفاده می‌شود تا کلید مذکور و پشتیبانهای آن به طور سری و مرموز صرفاً در اختیار شخص امضاکننده باشد.[۶]

---

1. National Institute of Standard and Technologhy

2. Public Key Authentiction Framework For Australia

دوم ـ استانداردهای رمزگذاری امضای دیجیتالی

الف ـ امضای PKCS # 7/CMS

یکی از مهم‌ترین استانداردهای رمز گذاری PKCS#7/CMS [۱] می‌باشد که توسط RSA[۲] پیشنهاد شده است. این استاندارد از امنیت بالایی برخوردار است، به گونه‌ای که برای رمز گذاری نامه‌ها[۳]، معاملات[۴]، مبادله الکترونیکی اطلاعات محرمانه[۵] و انتقال کلید شخصی بکار می‌رود.

این استاندارد از ریشه استاندارد CMS می‌باشد که توسط گروه SMIME برای علامات دیجیتالی بوجود آمده بود و به صورت PKCS# 7/CMS تعدادی شکل قابل استفاده را معرفی می‌نماید. این شکل‌ها زمانی به کار گرفته می‌شود که لازم باشد یک شیء رمز گذاری شده، مانند امضای دیجیتالی به پیام اضافه شود.

ب ـ امضای XML

XML و زبانهای وابسته به آن برای تبدیل متن‌ها و پیام‌ها و جمع آوری ساختارهای اطلاعاتی بکار می‌رود. از زبان‌های وابسته به XML می‌توان به XMLSCH اشاره نمود که برای جمع آوری ساختارهای اطلاعاتی به کار گرفته می‌شود. البته هنوز هم XML به عنوان استانداردی برای امضا تصویب نشده و تنها به عنوان یک طرح پیشنهاد شده است.

ج ـ امضای PDF

---

1. Public Key Cryptography Standard /PKCS#7: Cryptographic Message Syntax Standard.

۲. RSA: نوعی رمز گذاری که در سال ۱۹۷۷ در یک پژوهش دسته جمعی توسط رون ریوست، آدی شامیر و لئونارد آدلمن ابداع شد. در روش آر.اس.ای از یک جفت کلید رمزگذاری و رمزگشایی بهره گرفته می‌شود که هر دو کلید از مسیر واحدی کار انتقالی داده را انجام می‌دهند. RSA برگرفته از حرف اول نام مبتکرین این طرح است.

3. S/MIME: Standard (of) /Multipurpose Internet Mail Extensions

4. SET: Secure Electronic Transaction

5. PKCS#12: Personal Information Exchange Syntax Standard

نسخه ۴ آکروبات امکاناتی فراهم کرده که با آن می‌توان امضای دیجیتالی را به متن اضافه نمود؛ البته متن مذکور باید به صورت PDF باشد این موضوع در گفتار سوم به طور مفصل بررسی خواهد شد.[۷]

شکل امضا	ارتباط بین امضای دیجیتالی و داده‌ای که باید امضا شود:	آیا امکان امضای قسمتی از متن وجود دارد؟	داده‌ها باید به چه شکلی باشند تا بتوان آنها را امضا نمود؟	آیا می‌توان برای ایجاد امضای الکترونیکی به‌کار برد؟	آیا می‌توان برای ایجاد متنی به کاربرد که به شیوه دیجیتالی امضا می‌شود؟	آیا می‌توان به عنوان شیوه‌ای برای علامت گذاری داده‌ها به کار گرفت؟
PDF 1.3	امضا با متن ترکیب می‌شود	بلی	فقط PDF	بله البته اگر برای امضا از PKCS#7 استفاده شود.	بله	بله
XML PKCS	داده و امضا به صورت یک بسته واحد ارایه می‌شود	بلی	BLOB	بله	بله	بله
PKCS # 7/CMS	داده امضا به صورت یک بسته ارایه نمی‌شود	خیر	BLOB	بله	بله	خیر

* انواع مختلف متن‌هایی که می‌توان امضاء نمود و شکل امضای دیجیتالی

گفتار سوم: روش‌های امضای دیجیتالی

اول ـ امضای دیجیتالی PDF

یکی از مهمترین نرم افزارهایی که برای امضای دیجیتالی، به ویژه برای کلید عمومی بکار می‌رود Adobe Acrobat می‌باشد. این نرم‌افزار برای رمزگذاری و رمزگشایی از شیوه‌ای استفاده می‌کند که از دو قسمت فیلتر[۱] و زیر فیلتر[۲] تشکیل شده است. فیلتر یک امضا نشانگر وسایلی است که برای استفاده از محتویات لغت نامه رمز گذاری لازم است. زیر فیلتر نشان دهنده شکل‌های استاندارد لغت نامه رمزگذاری می‌باشد.

لغت نامه امضا یکی از ویژگی‌های امضای دیجیتالی در محیط PDF می‌باشد که محلی برای ذخیره کلیدهای عمومی می‌باشد. دو شکل برای ذخیره کردن کلیدهای عمومی در لغت نامه امضا برای PDF وجود دارد، شیوه امضای سطری و PKCS#7.

شیوه امضای سطری[۳] به این صورت می‌باشد که کلیدها و امضاهای کدگذاری شده را مستقیماً به صورت نشانه‌ای در لغت نامه قرار می‌دهد. ولی در روش PKCS#7 امضا و شکل کد گذاری شده علامت‌ها به صورت PKCS#7 درآمده و در لغت نامه ذخیره می‌شود. بنابراین اگر از شیوه اخیر استفاده شود به طور مستقیم می‌توان با بهره‌گیری از کلیدها، امضا را از لغت نامه استخراج نمود. از معایب مهم شیوه مذکور این است که برای هر مورد در PKCS#7 حداقل ۵ تا ۱۰ کیلو بایت حافظه نیاز می‌باشد که مقدار زیادی است.

همانگونه که گفته شد این دو شیوه نشانه‌های مختلفی از امضا را در لغت نامه ذخیره می‌کنند، مثلاً شیوه PKCS#7 نشانه‌های زیر را ذخیره می‌کند:

---

۱. Filter: برنامه یا فرمانی که مانع دسترسی به داده‌ای خاص می‌شود و این امر را منوط به دادن اسم رمز مربوطه می‌نماید.

۲. Sub Filter: شکل استاندارد لغت نامه رمز گذاری، برای نمونه: PKCS، XML یا PDF

3. Raw Signature Format

نوع[1]: نوع لغت نامه امضا

فیلتر: نشان می‌دهد که وسایل دسترسی به امضا در لغت نامه به چه زبانی ساخته شده‌اند.

زیر فیلتر: نشان دهنده فرمت (شیوه‌ای) است که اطلاعات با آن در لغت نامه ذخیره شده‌اند. شیوه امضای سطری نیز نشانه‌های تقریباً مشابهی، با تعدادی اضافات، در لغت نامه ذخیره می‌کند.

رمزگذاری کلید عمومی این امکان را فراهم می‌سازد که گیرنده‌های مختلفی بتوانند متن را رمزگشایی کرده و بخوانند. البته باید توجه داشت که تنها گیرنده هایی که به آنها اجازه داده شده می‌توانند متن را رمزگشایی کنند. اسم و برخی دیگر از خصوصیات استفاده کننده هایی که به آنها اجازه داده شده، متن را بخوانند، به صورت PKCS#7 در آرایه گیرنده‌ها[2] ذخیره می‌شود. البته این مورد با وسایل استاندارد سری تفاوت دارد، زیرا اگر کسی کلمه عبور مرتبط به وسایل استاندارد سری را در اختیار داشته باشد، می‌تواند به تمام جزئیات امضا و حتی کلید شخصی هم دسترسی پیدا کند.[۸]

دوم ـ امضای دیجیتالی Soap

Soap لایه استانداردی از پیام برای تبادل متن‌های XML و یکی از سرویس دهنده‌های مهم XML می‌باشد. در این استاندارد برای امضای دیجیتالی و قواعد آن و شیوه فرستادن و کدگذاری از Soap - DSIG استفاده می‌شود. علاوه بر Soap فناوری‌های دیگر مانند UDDI و WSDl برای انجام این کار وجود دارد، ولی ما در این قسمت فقط به Soap خواهیم پرداخت.

هر پیام در Soap از دو قسمت جداگانه تشکیل یافته است، بسته[3] Soap و رمزگذاری[4] Soap. بسته Soap یک ساختمان داده می‌باشد که می‌توان برای انتقال متن‌های XML از آن

---

1. Type
2. Recipients
3. Envelope
4. Encoding

استفاده کرد. همانطور که گفته شد، Soap فقط متن‌های XML را می‌تواند منتقل نماید، لذا باید این متن به شکل XML درآید که این کار را قسمت رمزگذاری انجام می‌دهد.

در Soap به دو نوع رمزگذاری نیاز است. اولی برای مشخص کردن فرستنده پیام که رمزگذاری پیام نامیده می‌شود و دیگری برای مشخص و جداکردن گیرنده ـ فرستنده پیام که به آن رمزگذاری گیرنده ـ فرستنده گفته می‌شود. رمزگذاری پیام این اطمینان را ایجاد می‌کند که پیام فرستاده شده توسط شخص دیگری به غیر از نویسنده اصلی پیغام تغییر داده نخواهد شد. این کار را می‌توان به راحتی با استفاده از امضای دیجیتالی یا رمز امنیت پیام[۱] انجام داد. البته باید توجه داشت که این رمز هیچ گاه هویت ارسال کننده پیام را مشخص نمی‌کند.

رمزگذاری فرستنده ـ گیرنده هویت واقعی فرستنده و گیرنده پیام را آشکار می‌سازد و لذا ممکن است از این طریق ثابت شود که فرستنده یا گیرنده، شخص واقعی یا مورد نظر نبوده است. همانطور که تشریح شد یکی از روش‌های رمزگذاری Soap امضای دیجیتالی می‌باشد این کار توسط Soap - DSIG انجام می‌شود. بنابراین مهم‌ترین وظیفه Soap - DSIG این است که پیام و امضا را به نحو مناسبی به هم پیوند دهد؛ این عمل را Soap - DSIG به این صورت انجام می‌دهد که یک ساختمان داده برای پیوند متن XML و امضای دیجیتالی ایجاد می‌کند. همین ساختمان داده است[۲] که به دست گیرنده می‌رسد و گیرنده بعد از گرفتن آن و با استفاده از کلید عمومی که در اختیار دارد آن را کدگشایی کرده و معین می‌کند که آیا واقعاً فرستنده پیام همان کسی است که انتظار می‌رود یا اینکه شخص دیگری می‌باشد.[۹]

سوم ـ امضای دیجیتالی Penop

امضای Penop به این صورت عمل می‌کند که امضاهای ایجاد شده توسط امضا کننده را در محل خاصی ذخیره می‌نماید.

---

1. Message Authentication Code
2. Data Structure

در امضای Penop این محل را می‌توان به وسیله نرم افزاهایی مانند Adobe Acrobat مقدار دهی کرد. بعد از آنکه مقدار دهی محل ذخیره امضاها به پایان رسید، زمانی که امضای خاصی به Penop وارد شد، آن را با تمام تصاویر امضاهای موجود مقایسه می‌کند تا مشخص کند که امضای موجود مربوط به چه کسی می‌باشد.

یکی دیگر از قابلیت‌های مهم Penop توانایی تبدیل مستقیم دست نوشته به حروفچینی الکترونیکی می‌باشد. زمانی که یک فرد می‌خواهد متنی را امضا کند از قسمت خاصی از Penop به نام Gravity Prompt استفاده می‌کند؛ این قسمت زمانی که فردی تقاضای امضا میکند از وی سوالات خاصی می‌پرسد تا اینکه مشخص می‌کند امضای مربوط به شخص مورد نظر کدام می‌باشد و اگر امضای وی در محل ذخیره امضاها وجود داشت آن را در زیر متن وی ایجاد می‌کند وگرنه یک پیام خطا فرستاده می‌شود.

برای ایجاد یک مکانیزم سری و مطمئن، امضای دیجیتالی Penop به این صورت طراحی شده که یک ارتباط قوی بین شخص صاحب امضا و امضا و همچنین بین امضا و متن شده ایجاد می‌کند. زمانی که Penop این ارتباط‌های سری را ایجاد می‌کند در واقع یک نشان[1] بیومتریک بین امضا کننده و متن امضا شده ایجاد می‌کند. این نشان درست زمانی که امضا توسط سرویس دهنده گرفته می‌شود به وجود می‌آید. این نشان یک نوع ساختمان داده می‌باشد که تعداد اجزای جدا از هم مربوط به امضا را نشان می‌دهد. همچنین طرز کار و خصوصیات امضا مشابه با مواد زیر را در خود جای بدهد:

- **خصوصیات امضا کننده (اسم، شماره ID)**
- **تاریخ و زمان**
- **سخت‌افزاری که با آن امضا وارد شده است**
- **شکل امضای امضا کننده.**

1.Token

همچنین یک خط داده مربوط به متن مربوطه هم در این ساختمان داده ذخیره می‌شود. این خط داده که نمایه[۱] متن نام دارد، در واقع یک تصویر ریاضی از متن می‌باشد که برای هر متن یگانه می‌باشد و بنابراین اگر متن تغییر کند، این نمایه متن هم تغییر خواهد کرد. Penop برای تطبیق دادن امضایی که به آن وارد می‌شود، در حدود ۹۰ نوع مقایسه و اندازه‌گیری مختلف را انجام می‌دهد تا اینکه معین نماید آیا امضای موجود همان امضایی است که در محل ذخیره امضاها وجود دارد یا نه و این نشان دهنده دقت بالای Penpo نسبت به دیگر سرویس دهنده‌های[۲] امضای دیجیتالی می‌باشد.[۱۰]

فصل دوم ـ جنبه‌های حقوقی امضای دیجیتالی

برای اینکه بتوان اهمیت بررسی ابعاد حقوقی امضای دیجیتالی را شناخت، ابتدا باید این نکته را تشریح نمود که امضا در علم حقوق دارای چه اهمیتی است. نگاهی به ماده ۱۳۰۱ قانون مدنی ایران، ارزش اثباتی امضا را نشان می‌دهد. ماده مذکور مقرر می‌دارد: «امضایی که روی نوشته یا سندی باشد بر ضرر امضا کننده دلیل است.» به این جهت که امضا می‌تواند موجب اعتبار حقوقی سندی باشد که در آن درج شده، ابتدا به بررسی آن می‌پردازیم.

گفتار اول ـ ارزش اثباتی امضای دیجیتالی

امضا به طور کلی برای شناسایی شخص امضا کننده و برای مرتبط ساختن شخص با مندرجات سندی که امضا نموده به کار می‌رود. برای مثال امضا می‌تواند گواه قصد شخص بر تعهد به محتوای قراردادی باشد، یا در اسناد تجاری بیانگر ظهر نویسی یا صدور آن از سوی شخص امضا کننده باشد. چنانچه ماده ۲۲۳ قانون تجارت در صدور برات «امضا یا مهر» برات دهنده را شرط دانسته و ماده ۲۴۶ قانون مذکور، انتقال به موجب ظهرنویسی را صرفاً با امضای

---

1. Checksum
2. Server

ظهر نویس امکان‌پذیر دانسته است.

البته بدیهی است که در کنار امضای دستی که از گذشته رایج بوده، اقسام دیگری از اشکال تایید محتوای نوشته‌ها، نظیر مهر زدن و سوراخ کردن نیز وجود دارد. اهمیت امضا در مورد قراردادهای کتبی که در آنها وجود امضا لازم شناخته شده آشکار می‌گردد، برای مثال نمی‌توان چکی را بدون امضا انتقال داد و حداقل اگر چنین انتقالی صورت گیرد مشمول قانون صدور چک نخواهد بود.

امضاهایی که با دست زده نمی‌شوند و برای نمونه به شکل «پاراف» بوده یا حتی ماشین نویسی می‌شوند، هر چند ماهیتاً امضای الکترونیکی نیستند ولی باید تمام شرایط امضای دستی را داشته باشند. از آنچه گفته شد دو نکته مهم به دست می‌آید:

۱ـ چون هر امضایی می‌تواند تعهد آور باشد، لذا باید امضاکننده در هنگام امضا قصد و رضا و اهلیت داشته باشد و امضای دیجیتالی از این قاعده عمومی استثنا نخواهد بود.

۲ـ هر امضایی که واجد شرایط باشد ـ اعم از دستی یا دیجیتالی ـ به نفع یا بر علیه امضاکننده قابل استناد خواهد بود. لذا اگر امضا کننده دیجیتالی، امضای خویش را انکار نماید، در آن صورت به وسیله شهود یا سایر ادله اثبات دعوا می‌توان صدور امضا از سوی وی را اثبات نمود. همچنین کارشناس فنی رایانه می‌تواند از طریق بررسی کلید شخصی که در گفتار قبل توضیح داده شد، صدور امضا از سوی منکر را اثبات نماید اکنون در صددیم تا با تمسک به اصول و قواعد حقوقی اثبات نماییم که امضای دیجیتالی دارای همان ارزش اثباتی امضای دستی می‌باشد.

الف) اگر امضای دیجیتالی با رعایت نظام اصول علمی و مهندسی الکترونیکی داده‌ها انجام شده باشد، دلیلی بر بی اعتباری آن و لزوم امضای کاغذی و دستی وجود ندارد. زیرا «اصل صحت» ایجاب می‌کند تا هر عملی از سوی هر شخصی صحیح فرض شود مگر اینکه خلاف آن اثبات گردد و در خصوصی امضای دیجیتالی چنین دلیلی نرسیده است.

ب) اگر ادعا شود که امضای دیجیتالی قابل جعل و دستکاری است، در مقابل می‌توان گفت که امضای دستی نیز قابلیت جعل دارد. در واقع حتی امکان جعل امضای دستی به دلیل دسترسی و توانایی هر کس به اعمال نفوذ در آن آسان‌تر از امضای دیجیتالی است.

ج) کمسیون حقوق تجارت بین الملل سازمان ملل متحد (آنسیترال)[1] که می‌توان گفت تمام وقت خود را وقف تصویب قوانینی سودمند در امرتجارت بین الملل نموده است، ماده هفت قانون نمونه درباره تجارت الکترونیکی مصوب ۱۹۹۶ را به بحث «امضا» اختصاص داده و در واقع آن را شناسایی نموده است. ماده ۵ قانون مذکور به تأسیس قاعده‌ای اقدام نموده که در تمام جنبه‌های حقوق تجارت الکترونیکی قابل اعمال است. به موجب این ماده: «اطلاعات نباید صرفاً به این دلیل که به شکل داده پیام هستند فاقد اثر حقوقی، اعتبار و قابلیت اجرایی شناخته شوند»[۱۱]

عقل و عرف نیز به عنوان منابع مهم حقوق خصوصی پشتیبان اعتبار و ارزش اثباتی امضای دیجیتالی است زیرا وقتی عرفاً در جهان به معاملات اینترنتی و رایانه‌ای اقدام می‌شود و امضاهایی برای اهداف مختلف به شیوه‌های گوناگون الکترونیکی انجام می‌شود، باید آن را شیوه‌ای معمول و پسندیده دانست که به دلیل عدم تعارض با اخلاق حسنه و نظم عمومی (ماده ۹۷۵ قانون مدنی ایران) موجبی برای بی اعتباری آن وجود ندارد.

نتیجتاً باید گفت: امضای دیجیتالی در صورتی که واجد شرایط باشد دارای ارزش اثباتی همانند امضای دستی سنتی است. لذا اگر شخص الف به موجب قرار دادی الکترونیکی که در آن امضای متعهد الزامی شناخته شده تعهد به تسلیم تعداد ۱۰۰ دستگاه خودرو با مشخصات معین در مقابل عوض مشخصی به نفع ب نماید و قرار داد را به شیوه دیجیتالی امضا کند، این قرارداد با اثبات صدور امضا از سوی الف بر علیه وی قابل اجرا و دارای تمام آثار حقوقی خواهد بود.

---

1. United Nations Commision on International Trade Law (UNCITRAL)

ماده ۳ قانون نمونه آنسیترال درباره امضای الکترونیکی مصوب ۲۰۰۱[1] نیز صراحتاً اعلام می‌نماید که به جز توافق و تراضی مغایر طرفین هیچ امری نمی‌تواند ارزش حقوقی هر شیوه‌ای که برای امضای الکترونیکی به کار رفته و شرایط مقرر در ماده ۶ را داراست، انکار یا تکذیب نموده و یا نادیده بگیرد. بند ۱ ماده ۶ قانون آنسیترال به صراحت مقرر می‌دارد که هر جا قانون امضای شخصی را لازم بداند و این لزوم در خصوص داده پیام باشد، امضای مذکور می‌تواند به شیوه‌ای الکترونیکی انجام شود. بدیهی است، همانطورکه بند ۳ ماده ۶ قانون مذکور نیز تصریح نموده، امضای دیجیتالی باید دارای شرایط خاصی باشد تا اعتبار حقوقی داشته باشد.[۱۲] این شرایط به طورکامل در فصل اول بررسی شده و نیازی به تکرار آن وجود ندارد.

توجه به میلیونها قرارداد الکترونیکی که در مدت کوتاه در پایگاه‌های مختلف اینترنتی و اغلب ـ مخصوصاً در عقود با تعهدات سنگین ـ(با امضای دیجیتالی منعقد می‌شود، اثباتگر این نکته است که دیگر نمی‌توان گفته نویسنده‌ای را پذیرفت که اظهار داشته: «در عرف تجاری امضای الکترونیکی ضروری نبوده و بر خلاف (امضای عادی) نمی‌تواند دارای اثر حقوقی عمده‌ای باشد زیرا در حقوق انگلیس قرار داد به هر شیوه‌ای قابل امضا نیست.»[۱۳] هر چند نویسنده مذکور بعداً لزوم بازنگری در این زمینه را مطرح نموده ولی با بررسی تطبیقی که درگفتار دوم انجام خواهد شد، روشن می‌گردد که حتی در حقوق انگلیس نیز ارزش اثباتی مشابهی برای امضای دیجیتالی در مقایسه با امضای دستی قایل شده‌اند؛ اگر چه در این خصوص محتاطانه عمل شده است.

سرانجام باید گفت امضای دیجیتالی همانند هر امضای دیگری می‌تواند اثبات گر موارد زیر باشد:[۱۴]

---

1. Uncitral Model Law on Electronic Signatures*

* که از این به بعد به اختصار قانون نمونه آنسیترال نامیده می‌شود.

۱ـ **اسناد**[1] ـ با امضای یک سند، آن سند به امضا کننده مستند و منتسب می‌شود که امضای دیجیتالی نیز می‌تواند دارای این کارکرد باشد.

۲ـ **انجام تشریفات**[2] ـ امضای سند دلالت بر این دارد که تمام تشریفات و آیین‌های لازم برای تهیه آن سند انجام شده که امضای دیجیتالی نیزاثبات گر این وضعیت خواهد بود.

۳ـ **تصدیق** [3] ـ عرفاً و عادتاً امضای هر سند و مدرکی به معنی تصدیق و تایید محتوای آن امضای دیجیتالی قرارداد نیز به مفهوم تایید و گواهی آن محسوب خواهد شد.

۴ـ **لازم لاجرا و دارای اثر حقوقی بودن**[4] ـ امضای اسناد و مدارک بسته به نوع آنها می‌تواند نشانگر لازم الاجرا شدن آن قرارداد یا ایجاد آثار حقوقی برای صرف امضا باشد. برای مثال امضای قرارداد الکترونیکی از سوی مشتری، قبول قرارداد و موجب لازم الاجرا شدن آن و امضای ظهر سندی به شیوه دیجیتالی به معنی دخالت امضا کننده به عنوان ظهر نویس در آن خواهد بود.

گفتار دوم: مطالعه تطبیقی حقوق برخی از کشورها در خصوص امضای دیجیتالی

مطالعه تطبیقی در حقوق داخلی برخی از کشورها نشانگر این است که در اغلب کشورها، امضای الکترونیکی بدون هیچ تردیدی به عنوان یکی از اعمال دارای آثار حقوقی همسان با امضای دستی مورد پذیرش قرار گرفته است. چون در گفتار بعدی به حقوق ایران (با در نظر گرفتن قانون نمونه آنسیترال) خواهیم پرداخت، در اینجا ابتدا به سیستم حقوقی فرانسه به عنوان سیستم حقوقی مشابه ایران و بعداً به قوانین داخلی برخی دیگر از کشورها که در خصوص تجارت الکترونیک و امضای دیجیتالی وضع قانون کرده‌اند، اشاره خواهیم کرد.

---

1. Evidence
2. Ceremony
3. Approval
4. Efficiency

اول ـ حقوق فرانسه

دستور نامه مورخ ۱۳ دسامبر ۱۹۹۹ اروپا در زمینه امضای الکترونیکی به طور کامل در فرانسه پذیرفته شده و مورد تصویب قرار گرفت. این مقرره در فرانسه به عنوان یکی از کشورهای مهد حقوق به اندازه‌ای اهمیت یافته که دستور نامه مذکور با اصلاح ماده ۱۳۱۶ قانون مدنی فرانسه[1] وارد سیستم حقوقی این کشور شده است.

این اصلاح که در ۱۳ مارس ۲۰۰۱ صورت گرفت امضای دیجیتالی که به شیوه‌ای علمی و مطمئن انجام شده باشد را همانند امضای دستی دانسته و به اسناد الکترونیکی ارزش اثباتی برابر با اسناد کاغذی قایل شده است. با تصویب مقرره مذکور که نقطه عطفی در حقوق فرانسه و اتحادیه اروپا به حساب می‌آید، دیگر نیاز به توافق و تراضی بر قابلیت قبول اسناد الکترونیکی وجود ندارد. [۱۵]

تصویب نامه ۱۳ مارس ۲۰۰۱ مقرر می‌دارد: اگر امضای الکترونیکی ضمن فرایندی با دستگاه مطمئن و ایمن انجام شود، قابل استناد می‌باشد. البته اخیراً در فرانسه تصویب نامه ۱۸ آوریل ۲۰۰۲ به جزئیات تجارت الکترونیکی پرداخته است.

قابل ذکر است در فرانسه هنوز قاعده فوق الذکر با استثنایی روبروست؛ برای مثال دفاتر اسناد رسمی ازدواج نمی‌توانند از امضا به شیوه الکترونیکی بهره بگیرند. با این وجود امضای الکترونیکی در قراردادهای خصوصی همواره قابل استفاده خواهد بود.

دوم ـ حقوق ایالات متحده

اولین قانون درباره امضای دیجیتالی در سال ۱۹۹۶ در ایالات یوتای آمریکا به تصویب رسید[2] در ایالات متحده آمریکا، ابتدائاً در سطح ایالتی قانون متحدالشکل معاملات

1. French Civil Code

2. Utah Digital Signature Act 1996

الکترونیکی[۱] و سپس در سطح فدرال قانون امضاهای الکترونیکی در تجارت داخلی و بین المللی[۲] به تصویب رسید. هر دو مقرره بر اعتبار کامل امضای الکترونیکی واجد شرایط در قرار دادهای داخلی و خارجی اشاره دارند.

توجه به امضای الکترونیکی در قراردادها از مشخصه‌های بارز حقوق آمریکا و مقررات تصویب شده در این زمینه می‌باشد که هر چند توسط سایر کشورها را مد نظر داشته‌اند، ولی به طور مفصل به بررسی آن نپرداخته‌اند.

سوم ـ حقوق انگلیس

انگلستان بر خلاف دیگر کشورهای عضو اتحادیه اروپا نظیر آلمان، ایتالیا و لوکزامبورگ، در زمینه تصویب قانونی در خصوص امضای الکترونیکی محتاطانه عمل کرده است.[۱۶] با این وجود سرانجام قانون ارتباطات الکترونیکی پادشاهی متحده[۳] در سال ۲۰۰۰ مورد تصویب قرار گرفت. قانون مذکور گامی به جلو محسوب نمی‌شود. زیرا صرفاً بر این امر تصریح نموده که امضای الکترونیکی باید به عنوان دلیل مورد پذیرش قرار گیرد و این در حالی است که چنین رویه‌ای بدون اینکه نیاز به قانون باشد در حقوق عرفی[۴] اتخاذ شده و دلیل این امر انجام معاملات «بر خط»[۵] در حد بسیار وسیع است.

در زمینه عمل به دستور نامه مورخ ۱۳ دسامبر ۱۹۹۹ اتحادیه اروپا در انگلستان مقررات امضاهای الکترونیکی[۶] در سال ۲۰۰۲ به تصویب رسید و در ۸ مارس ۲۰۰۲ قابلیت اجرایی

---

1. Uniform Electronic Transactions Act [UETA]

2. Electronic Signatures in Global and National Commerce Act [E-Sign]

3. United Kingdom Electronic Communication Act 2000

4. Common Law

5. Online

6. Electronic Signatures Regulations 2002

یافت. مقرره مذکور با حقوق انگلیس در تعارض نیست، زیرا حقوق انگلیس مبتنی بر سیستم حقوقی عرفی است که در عرف تجاری نیز معاملات الکترونیکی به گستردگی انجام می‌شود. این مقرره گامی به جلو بوده و برای شناسایی امضاهای معتبر در سطح بازارهای اینترنتی کاربرد دارد.[۱۷]

چهارم ـ حقوق آلمان

لایحه قانونی امضای الکترونیکی در شانزدهم آگوست ۲۰۰۰ به تصویب کابینه آلمان رسید. بنابر بند ۱ ماده ۱ لایحه مذکور هدف از تصویب آن معرفی شرایط و چهار چوب امضای الکترونیکی است.

به موجب بند ۳ ماده ۲ لایحه، (امضای واجد شرایط الکترونیکی) عبارت است از:

الف ـ امضایی که در هنگام ایجاد از نظر امنیت و اطمینان واجد شرایط باشد.

ب ـ امضای مذکور با دستگاهی مطئن انجام شده باشد.

در ماده ۶ لایحه که مقرره‌ای جالب و جدید است، به منظور بالا بردن اطمینان و امنیت امضای الکترونیکی و قابل استناد بودن آن، سرویس دهنده امضا مکلف شده که اطلاعاتی در خصوص آن ارایه نماید. از جمله متقاضی است باید از این امر آگاه شود که امضای واجد شرایط الکترونیکی از نظر حقوق قراردادها، آثار حقوقی مشابه با امضایی دارد که با دست انجام شده است.

فی‌المجموع لایحه مذکور تمام ابعاد حقوقی امضاهای الکترونیکی و معاملات مبتنی بر آن بررسی نموده و از این لحاظ بر مقررات سایر کشورها که موضوع را به اختصار برگزار کرده‌اند برتری دارد. [۱۸]

پنجم ـ حقوق اسپانیا

لایحه قانونی امضاهای الکترونیکی اسپانیا[1] قبل از دستور نامه مورخ ۱۳ دسامبر ۱۹۹۹ اتحادیه اروپا و در تاریخ هفدهم سپتامبر ۱۹۹۹ به تصویب رسید. به همین دلیل با دستور نامه مذکور هماهنگی کامل ندارد و باید اصلاح شود. ماده ۳ لایحه مذکور امضای الکترونیکی را با در نظر گرفتن قواعد قابل اجرا در خصوص ادله اثبات دعوا قابل استناد و دارای اعتبار حقوقی دانسته است. [۱۹]

ششم ـ حقوق چین

ترجیح معاملات الکترونیکی بر قراردادهای بر حضوری در چین نیز مانند سایر کشورها به دلیل مزایای آن مورد توجه قرار گرفته است. دولت چین نسبت به برداشتن محدودیت‌هایی که در مقابل تجارت آزاد الکترونیکی در آن کشور وجود داشته اقدام نموده که این امر بر اساس توافق آن کشور با ایالات متحده آمریکا و سازمان تجارت جهانی[2] بوده است. [۲۰]

در همین راستا چین در سال ۱۹۹۹ اقدام به تغییر برخی از قوانین خود از جمله در خصوص حقوق قرارداد نموده و در جهت پذیرش امضای الکترونیکی در قراردادهایی که در فضای مجازی شکل می‌گیرند، موسسه فن آوری اطلاعات جدید شانگ‌های[3] با دولت چین در مورد به دست آوردن پروانه سرویس دهی امضا اقدام به انعقاد قرارداد نموده است.

این توافق نامه در ماه ژوئن ۲۰۰۳ امضا شده و قسمتی از پروژه بزرگ دولت در فناوری نامه‌های دستی، امضاهای بیومتریک و امضاهایی است که جایگزین شیوه قدیم می‌شوند. [۲۱]

---

1. Spain's Electronic Signatures Bill (1999)
2. Word Trade Organization (WTO)
3. Shanghai Modern Information Technologhy Institution

هفتم ـ حقوق کانادا

در جهت پیوستن به ساختار جهانی تجارت به شیوه الکترونیکی، کنفرانس یکنواخت سازی قوانین کانادا[۱] اقدام به تصویب قانون متحدالشکل تجارت الکترونیکی[۲] نموده است.

ماده ۸ قانون مذکور به امضای الکترونیکی اختصاص دارد، به موجب بند الف این ماده امضایی که به شکل الکترونیکی صورت گرفته می‌گیرد، سند الکترونیکی را به شخص امضاکننده منتسب می‌نماید، اعم از اینکه امضا در سند مذکور انجام شده یا به آن ضمیمه شده یا به روش علمی دیگری با آن همسان شده باشد.

بنابر بند ب ماده ۸ قانون متحدالشکل تجارت الکترونیکی کانادا، امضای الکترونیکی برای اثبات ماهیت مدرک سند امضا شده و لوازم آن که شامل توافق‌های ضمنی و زمان ایجاد آن مدرک الکترونیکی است، قابل استناد خواهد بود.[۲۲]

هشتم ـ حقوق سنگاپور

این کشور صریحاً روش دوگانه در مقام پذیرش امضای الکترونیکی اتخاذ نموده که از این جهت ماده ۷ قانون نمونه آنسیترال درباره تجارت الکترونیکی را تداعی میکند. به موجب قانون معاملات الکترونیکی سنگاپور[۳] مصوب ۱۹۹۸ فقط امضاهای خاصی دارای ارزش سندیت هستند و آن امضاهایی است که با کلید شخصی مطمئن و قابل اعتمادی زده شده باشد، به گونه‌ای که به راحتی قابل جعل نباشد. [۲۳]

چنانچه ملاحظه می‌شود حقوق سنگاپور بین «امضای الکترونیکی» در مفهوم مطلق آن و «امضای الکترونیکی دارای امنیت»[۴] تفاوت قائل شده است. البته به نظر می‌رسد که تصریح به این تفکیک نیاز نباشد زیرا همانطورکه بررسی شد اگر سیستم امضا از نظر امنیتی دارای اختلال

---

1. Uniform Law Conference of Canada
2. Uniform Electronic Commerec Act
3. Singapore Electronic Transactions Act 1998
4. Secure Electronic Signature

باشد، امضایی که از آن طریق صورت می‌گیرد به دلیل قابلیت جعل آسان سندیت ندارد و اساساً بحث از ماهیت رایانه‌ای امضای دیجیتالی نیز در جهت تسجیل همین واقعیت است.

نهم ـ حقوق فیلیپین

آخرین کشوری که حقوق آن به اختصار در خصوص امضای الکترونیکی مورد بررسی قرار می‌گیرد، کشور فیلیپین به عنوان یکی از کشورهای آسیایی است. البته امکان بررسی حقوق سایر کشورها نیز وجود داشت که برای رعایت اختصار از آن صرف نظر شد.

در کشور فیلیپین قانون موسوم به «قانون تجارت الکترونیک ۲۰۰۰»[۱] در ۲۶ ژوئیه ۱۹۹۹ به تصویب رسیده است.[۲] ماده ۸ قانون مذکور به شناسایی امضاهای دیجیتالی اختصاص دارد که به موجب آن، امضای الکترونیکی در سند الکترونیکی معادل و برابر با امضایی است که شخص در سند مکتوب می‌زند به شرط اینکه ثابت شود امضا از سوی اشخاص ذینفع قابل تغییر نیست.

بند ج ماده مذکور در حکمی جالب مقرر می‌دارد: «برای اشخاصی که قصد متعهد شدن به قراردادی الکترونیکی دارند، اقدام به تهیه و انجام امضای الکترونیکی ضروری است». البته به موجب بند بعدی سایر اشخاص نیز حق دارند که در صحت امضای الکترونیکی تردید نموده و تقاضا نمایند که صاحب امضا، صحت و اعتبار آن را اثبات نماید.[۲۴]

---

1. Electronic Commerce Act of 2000

۲. ماده قانون مذکور تصریح دارد که این قانون باید «قانون تجارت الکترونیک ۲۰۰۰» نامیده شود.

گفتار سوم ـ امضای دیجیتالی در حقوق ایران
با نگاهی به قانون نمونه آنسیترال

بررسی قوانین کشورهای گوناگون در زمینه تجارت الکترونیکی و امضای دیجیتالی بیانگر این نکته مهم است که در دیگر ناچاراً یا با اراده باید در دهکده جهانی عضو شد و در آن با سریع‌ترین وسایل قابل تصور به بهترین و سودآورترین نوع تجارت پرداخت. متاسفانه در این خصوص هم اقدامات لازمه در کشور ما به کندی ـ اگر نگوییم به ندرت ـ صورت می‌گیرد و لذا در این گفتار سعی خواهیم کرد تا موضوع امضای دیجیتالی را در حقوق ایران با در نظر گرفتن قانون نمونه آنسیترال درباره امضای دیجیتالی مصوب سال ۲۰۰۱ و قانون تجارت الکترونیکی[۱] تبیین نماییم. این بررسی را که نیاز به دقت و ظرافت دارد در بندهای چند گانه انجام می‌دهیم.

اول ـ تاثیر بررسی جایگاه حقوقی امضا

این بحث اختصاص به امضای دیجیتالی ندارد ولی بی ارتباط با آن نیز نمی‌باشد. به طور کلی امضا زمانی از نظر حقوقی مورد بررسی قرار می‌گیرد که دارای آثار حقوقی باشد. از اینرو اگر شخص در برگه باطله‌ای تمرین امضا نماید یا در فضای مجازی اقدام به ایجاد امضای بدون دلیل کند، چنین امضایی فاقد اعتبار و اثر حقوقی است. زیرا هیچ حق یا تعهدی برای هیچ شخصی ایجاد نمی‌کند، لذا این نتیجه مهم حاصل می‌شود که هر امضایی از نظر حقوقی سندی را متبادر می‌سازد، برای نمونه امضای دیجیتالی به این دلیل در حقوق مورد بررسی است که فروشنده‌ای

---

۱. این مقاله قبل از تصویب «قانون تجارت الکترونیکی» نگارش یافته است. قانون مذکور سرانجام در تاریخ ۱۳۸۲/۱۰/۱۷، به تصویب مجلس شورای اسلامی رسید. رجوع شود به: روزنامه رسمی، مورخ شنبه یازدهم بهمن ۱۳۸۲، سال ۵۹، شماره ۱۷۱۶۷. در آخرین اصلاحات مقاله حاضر، قبل از چاپ آن تا حدودی به وضعیت امضای دیجیتالی در قانون مذکور پرداخته شده است.

می‌تواند با قراردادن آن در مکان مشخص از قرارداد استاندارد (نمونه)[1] رضایت یا به اصطلاح حقوقی «قبول» خویش را نسبت به آن ابراز دارد. اثر مهم امضا، متعهد شدن به تمام آثار جنبه‌های آن قرارداد از یک طرف و محق شدن به تمام مزایایی است که از امضای قرارداد مذکور از سوی شخص دیگر پدید می‌آید.

به طور کلی «نوشته منتسب به اشخاص در صورتی قابل استناد است که امضا شده باشد. امضا نشان تایید 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». [۲۵]

درستی این عقیده در خصوص اسناد کاغذی کاملاً آشکار است ولی به دلیل اینکه امضای دیجیتالی علی رغم گسترش روز افزون آن هنوز هم رواج کامل ندارد، این نظر را باید مقداری تعدیل نمود. برای مثال هیچ بعید نیست که قراردادی در فضای مجازی با فشار دادن دکمه "Enter"، "Submit" یا "Accept" واقع نشود. زیرا این شیوه در خصوص اسناد الکترونیکی معمول و متعارف است. این تصور وجود دارد که زمانی امضای دیجیتالی و اسناد الکترونیکی به آن اندازه از رواج و امنیت خواهند رسید که دیگر همانند اسناد کاغذی، هیچ سند الکترونیکی بدون امضا اعتبار و اثر حقوقی نخواهد داشت.

دوم ـ آثار حقوقی امضای دیجیتالی در حقوق ایران و قانون آنسیترال

چنانچه در گفتار اول همین فصل بررسی شد، دلیلی بر بی اعتباری امضای دیجیتالی از نظر حقوقی وجود ندارد و اساساً خصوصیتی در امضای دستی وجود ندارد تا آن را بر امضای دیجیتالی که با رعایت تمام موازین علمی انجام (زده) شده، ترجیح دهد.

بر همین اساس ماده ۱۳۰۱ قانون مدنی ایران در اصل و نه به موجب ملاک در خصوص

---

1. Standard Contract

امضای الکترونیکی نیز جاری خواهد بود. لذا باید چنین اظهار داشت: «امضایی که در روی نوشته یا سندی الکترونیکی باشد بر ضرر امضا کننده دلیل است».

بنابراین هیچ مانعی درامضای الکترونیکی هیچ قرارداد، تعهد، مقاوله نامه و توافقنامه‌ای ـ ولو با محتوای استراتژیک و تعهدات سنگین ـ ار نظر حقوق ایران نمی‌تواند وجود داشته باشد.

استاد بزرگوار دکتر کاتوزیان، تقدم نیازها و پیشرفت‌های علمی بر دیدگاه‌های سنتی را در آینده امکان پزیر دانسته‌اند.[۲۶] ولی به جرات می‌توان گفت که این برتری ـ و شاید بهتر است گفته شود "برابری" ـ اسناد تجاری الکترونیکی با اسناد عادی در جهان و با تحلیل فوق الذکر در ایران محقق شده است. واقعیت این است که حتی خشک‌ترین سیستم‌ها دیدگاه خود را با عرف و بنای عمومی تطبیق خواهند داد و ماشین پیشرفت بدون در نظر گرفتن معاندین، عقب مانده‌ها و کسانی که حتی سعی در ممانعت از حرکت آن دارند راه خود را با اتکای به علم و دانش برتر بشری برای تسهیل هر چه بیشتر زندگی بشر خواهد یافت. نمونه کشور هایی که در مقابل امضای دیجیتالی مقاومت می‌کرد و کمتر انعطاف نشان می‌داد دولت انگلستان بود که جنانچه گفته شد بالاخره در مقابل این روند تسلیم و حتی برای آن وضع قاعده نمود.

لذا همانگونه که ماده ۶ قانون نمونه مقرر داشته در هر مورد که به موجب قانون امضای شخصی در سندی لازم باشد، در اسناد و مدارک الکترونیکی این امضا می‌تواند با رعایت اصول امنیتی به شیوه‌ای دیجیتالی انجام شود. این قاعده در حقوق ایران نیز صدق میکند و دلیلی بر خلاف آن وجود ندارد. بعلاوه، ماده ۷ قانون تجارت الکترونیکی به تقلید از ماده ۷ قانون نمونه، تصریح می‌نماید: «هرگاه قانون، وجود امضا را لازم بداند امضای الکترونیکی مکفی است».

بر این اساس می‌توان در خصوص آثار حقوقی امضای دیجیتالی به تاسیس اصلی در حقوق تجارت الکترونیکی اقدام نمود که نه تنها در حقوق ایران بلکه در حقوق تمام کشورها صدق می‌کند. به موجب این قاعده که می‌توان آن را «اصل اتحاد آثار امضا در اسناد کاغذی و الکترونیکی» نامید تمام آثاری که در مورد امضای دستی وجود دارد در امضای دیجیتالی نیز

صدق می‌کند و لذا هر دو می‌توانند مشخص کننده امضا کننده، موجب انتساب سند به وی و نشانگر قابلیت استناد به آن سند به نفع یا به ضرر امضا کننده باشند.

البته این اصل با استثناهایی نیز مواجه است، که به دلیل وارد شدن استثنا به هر اصلی در غالب موراد نمی‌تواند ایراد به مبنای تئوریک آن باشد. به موجب یکی از استثناهای مهم که فقط در حقوق فرانسه ـ که سابقاً بحث شد ـ به آن تصریح شده، امضای دیجیتالی اسناد رسمی امکانپذیر نیست. البته یکی از حقوقدانان انگلیسی، تنظیم سند رسمی الکترونیکی را با رعایت شرایط قانونی مقرر برای سند رسمی نظیر امضا، حضور شهود، توسط ماموران صالح و به موجب قانون صلاحیتدار ـ امکان‌پذیر دانسته ولی سپس با بازگشت به این واقعیت که سند الکترونیکی اطمینان بخش نیست، حداقل وجود یک سند کاغذی را لازم دانسته است.[۲۷]

سوم ـ امضای الکترونیکی اسناد تجاری لازم الاجرا

مساله‌ای که مطرح می‌شود این است که آیا می‌توان اسناد تجاری را به شیوه‌ای الکترونیکی صادر و امضا نمود. قبل از پاسخ به سوال این نکته را باید متذکر شویم که مسلماً اسناد تجاری که در فضای مجازی صادر می‌شوند، حتی اگر عنوان "چک" یا "برات" داشته باشند، به دلیل اینکه کاغذی نیستند دارای ماهیت متفاوتی می‌باشند و از این لحاظ به مساله صرفاً در محدوده فضای مجازی و سیستم الکترونیکی پردازش و انتقال داده‌ها می‌توان پاسخ داد. به طور کلی بررسی پرداخت‌های اینترنتی این نظر را تقویت می‌کند که صدور، امضا مبادله اسناد الکترونیکی فاقد مانع قانونی است. از بعد تاریخی در گذشته از کارتهای اعتباری قابل دستکاری و غیر ایمن در روابط الکترونیکی استفاده می‌شد، ولی عواملی چون عدم قبول این نوع از وسیله پرداخت در معاملات از سوی برخی از تجار اینترنتی به دلیل کسر کارمزد ۲ الی ۳ درصد برای آنها از سوی شرکت‌های عرضه کننده این کارت‌ها و نفوذ یاغیان شبکه (هکرها) در برنامه‌های رمزگذاری شده اینترنت و از آن طریق دست یافتن به شماره کارت اعتباری اشخاص به قصد سوء استفاده

باعث گردید تا شیوه‌های پرداخت پیشرفته‌تری به کار گرفته شود. برای نمونه یکی از روش‌های پرداخت که کارت نرم‌افزار آن را می‌توان از شرکت ای تی ام تهیه نمود، کارت اعتباری بین المللی ماندکس (mondex) می‌باشد. این کارت که از آن برای پرداخت‌های الکترونیکی در ایالات متحده آمریکا، انگلیس و استرالیا به صورت آزمایشی استفاده شده است.[۲۸] با جدیدترین فناوری علمی ساخته شده و مشتری می‌تواند آن را برای خرید از شرکت‌هایی که ماندکس را به عنوان وسیله پرداخت می‌پذیرند، به کار گیرد. برای این منظور مشتری کارت ماندکس را در جایه کارتخوان رایانه شخصی قرار می‌دهد، با این عمل کارت فروشنده در رایانه شخصی او در فرض تایید الکترونیکی قرارداد، مبلغ قابل پرداخت را از کارت خریدار به کارت فروشنده انتقال می‌دهد. به منظور ایمن بودن این فرایند، ماندکس از یک امضای دیجیتالی بدون مشابه که در مدار کارت مشتری تعبیه شده و برای کارت ماندکس طرف مقابل خواناست، بهره می‌گیرد. این ابداع عملاً از جعل و تزویر در امر انتقال اعتبار جلوگیری می‌کند![۲۹] روش مذکور یک شیوه امضا و انتقال الکترونیکی می‌باشد ـ البته امضایی که یک بار برای همیشه زده می‌شود ـ زیرا اعتباری که بنابر فرایند ماندکس به کارت فروشنده افزوده می‌شود از سوی او به همان روش قابل انتقال به دیگران است. تفصیل بحث پرداخت‌های الکترونیکی بیش از آنچه گفته شد، از عهده این نوشته خارج است و در مقاله‌ای جداگانه انجام خواهد گرفت و فقط باید این نکته را متذکر گردید که مسلماً با تکیه بر توان مهندسین مجرب داخلی و علم نرم‌افزار در کشورمان می‌توان روش‌های بهتر و بی عیب‌تری برای انتقال لعتبار در فضاهای مجازی طراحی و ارائه نمود.

در پایان بحث حقوق ایران ماده ۶ قانون تجارت الکترونیکی مورد اشاره قرار می‌گیرد که به عباراتی شیوا بیان می‌دارد: «هرگاه وجود یک نوشته از نظر قانون لازم باشد، «داده پیام» در حکم نوشته است...».

اطلاق این ماده در مواردی که منع صریح و متعارفی باشد در حقوق ایران بدون تردید قابل اعمال و با لحاظ مواد ۷ و ۱۰ ق.ت.ا به امضای دیجیتالی نیز قابل تسری است.

نتیجه‌گیری

نرم‌افزار هایی که برای ایجاد امضای الکترونیکی در فضای مجازی بکار می‌روند باید از نظر علمی در حدی از پیشرفت و اطمینان و عرفا غیر قابل نفوذ نباشند. عدم قابلیت نفوذ به معنی پیشگیری از جعل و دستکاری امضای دیجیتالی است. با این وجود هنوز هم امضاهای دیجیتالی همانند امضاهای دستی می‌تواند توسط اشخاص ناصالحی جعل شوند، لذا قانون گذار باید:

۱ـ مقررات صریحی برای تعیین نرم‌افزاها و سیستم‌های رایانه‌ای که در امضای دیجیتالی مورد استفاده قرار می‌گیرند، مشخص سازد و امضای فاقد آن شرایط را بی‌اعتبار بداند.

۲ـ قانون مجازات به طور صریح به کسانی که با جعل و نفوذ در سیستم شخصی به ارتکاب جرایمی چون کلاهبرداری و خیانت در امانت و جرایم دیگر رایانه‌ای اقدام می‌نمایند، تسری یافته و در مورد این اشخاص نیز اعمال گردد.

در خصوص پذیرش آثار حقوقی برای امضای دیجیتالی:

الف ـ قانون باید به طور صریح «اصل اتحاد آثار امضای دستی و امضای دیجیتالی» را مورد شناسایی قرار دهد و در این خصوص به دور از هر گونه ابهام و سنت گرایی و با در نظر گرفتن متعارف بودن معاملات الکترونیکی وضع قاعده نماید.

ب ـ قانون گذار باید به عنوان پیش قدمی در عرصه تجارت الکترونیکی، صدور و امضای اسناد تجاری لازم الاجرا را به شیوه الکترونیکی مورد شناسایی قرار داده و سازمان خاصی را مسوول مدیریت روند سود آور و جهانی تجارت الکترونیکی و از آن طریق امضای دیجیتالی نماید.

«یادداشت‌ها»

1- Michael Chissick & Alistair Kelman, **Electronic Commerce Law and Practice**, Second Edition, Sweet & Maxwell, London 2000, P. XXX III.

2- **Uncitral Model Law on Electronic Signateres**, in: (Internet) http:// www.Kisa or. Kr/Policy/sub3/dataf/PD-00-07 UNCITRAL. PDF

3- **Definition of Electronic Signature**, in: (Internet)http://searchescurity. Techtarget. com/sdifinition/ "sid14-gci21195J ". html

4- Andrew s. Tanenbaun, **Computer Networks**, Third Edition, Prentice - Hall Interational, Inc. P 587.

5- **Digital Signature Guidelines Tutorial**, Page 3-5 in: (Internet) http:// www.abanet.Org/ scitech / ec isc / dsg 1 tutorial. html

6- Graham Greenleat. and Roger Clarke, **Privacy Implications of Digital Signatures**, Page 2-3. in: (Internet) http://www.anu.edu.au/People/Roger.clarke/DV Digsig.html

7- Diana Berbecaru, Antonio Lioy, Fabio Maino, Daniete Mazzochi and Giantuca Ramumnno. **Towards Concrete Application of Electronic Signature**, Page 3-4 in: (Internet) http://secuity.polito.it/doc/papers/e-sign.pdf

8- Jim Pravctz, **PDF public - Key Digital Signature and Encryption Specification**. Page 1.3 in: (Internet) http://partners.adobe.com/asn/developers/pdfs/tn pp-k pdf-spes. pdf

9- Satoshi Hada, **SOAP Securitey Extensions: Digital Signature**, Page 3-5 in: (Internet) http://www.106.ibm.com/developer works/webservices/Library/WS-soapsec

10- Ian Walden, **Legal Aspects of the Pen Op Signature under English Law**, Page 7-8 in: (Internet) http://www.ecomaus.com/Legal %20 documents /uklegal.pdf

11- **Uncitral Model Law on Electronic Commerece** With additional Article 5 bis as adopted in 1998 and Guide to Enactment , in: (Internet) hpp://www jus.uio.no/im/unelectronic.commece.Model.Law 1996/docc.html.

12- **Uncitral Model Law on Elctronic Signature**; op cit.

13- Susan Singleton, E - **Commerce: APractical Guide to the Law**, Gower Publication, England. Page 71.

14- Digital Signature Guidelines Tutorial, op cit . Page 2.

15- Alexandre Menais, **Electronic Singatures in France**, page 1, 4 in: (internet) http://www.juriscom.net/en/pro/l/ec 20020730.htm.

16- Michael Chissick and Alistair Kelman, op cit , Page 154.

17- Reed Chris, **Internet Law: Text and Materials**, Butterworths, London 2002, Page3- 12.

18- For "**Draft Electronci Signature Law, Germany**" See, (Internet) http://www.iid.de/iukdg/eval/VIBZReferen tentwufenglisch. pdf.

19- **Electronic Signatures Directive**, Page a in: (Internet) htt://216.87.176.marsos/docs/ct-esig-su-eu-html.

20- Paul D.Mckenzie, **Electronic Commerce Law People's Republic of China**, Page 1-3 in; (Internet) http://wwwperkinscoie. com / resource / ecomm / prc. htm

21- Redwood shores, CA, June 23, 2003 (**OTC BB: CICI** - or Internet) http://www.penop,com/press/wventdetail.asp? Newsld=195

22- Uniform Electronic Commerce Act (of Canada), in : (Internet) http://www.law .u.alberta..ca/alri/ulc/current/euecafin.htm.

23- E.U:Electronic Signatures Directive; op cit.

24- Republic of Philippines "**Electronic Commerce Act of 2000**" in: (Internet) http://www.neda.gov.ph/pressRelases/News About RA7872 / signedRA8792. htm#RA

۲۵ـدکتر ناصر کاتوزیان، **اثبات و دلیل اثبات**، جلد اول، چاپ اول نشر میزان، تهران ۱۳۸۰ ص ۲۷۸ ش ۱۷۴.

۲۶ـهمان، ص ۲۸۳-۲۸۲، ش ۱۷۷.

27- David I Bainbridge, **Introduction to Computer Law**, Fourth Edition. Longman. 2000, Page 265.

28- Loshin, Pete & Paul Murphy, **Electronic Commerce: Online Ordering and Digital Money**, Second Edition, Charles River Media Publication, Page, 124.

29- Ishman Mark & Maquet Quincy; **A Consnmer's Analysis of The Electronic Currency System And The Legal Ramitification For A Transacion Gone Awry**, in: (Internet),

http://www.murdoch.edu.eu/elaw/issuesv6n3/ishman63.html-Ik. PP. 4-6.