امضاء الکترونیک و مسائل حقوقی آن

طهمورث افشاری و لیلا وهابی

مقدمه

در کاربرد مبادله الکترونیک داده ها به عنوان بخشی از فعالیت کسب و کار و بازرگانی، پذیرش قانونی مبادله الکترونیک موضوع مهمی است. قبول امضای الکترونیک و رسانه های الکترونیک به عنوان سند در محاکم قضایی، پیش شرط هرگونه کاربرد تجاری این فناوری است. بنابراین، لازم است قوانین موثری وضع شود تا طرحهای مختلف بتوانند معاملات خود را به صورت الکترونیک انجام دهند و در جایی که لازم است، قوانین و مقررات نیز جهت انطباق با این شیوه به منظور اعتبار سندهای الکترونیک باید تغییر کند؛ چرا که در حال حاضر منظور از سند اطلاعات نوشته و امضاء شده به روی کاغذ است . در صورتی که با تجارت الکترونیکی وتجارت ازنوع بدون کاغذواسناد الکترونیک روبرو باشیم که اخیراتمام مراحل تجاری درمعاملات واداری دراداره هاوسازملنهاازطریق رایانه هاوبه صورت الکترونیکی انجام می گیرد؛بنابراین برای صحت انتساب اسناد مبادلات الکترونیک لازم است یک امضای الکترونیک را جایگزین امضاهای سنتی گردد.

امضاءالکترونیک برخلاف امضاءسنتی که فقط دارای یک بعد حقوقی می باشد؛دارای دوبعد فنی وحقوقی است . پس امضاءالکترونیک به عنوان یکی از مباحث حقوقی تجارت الکترونیک مورد توجه علم حقوق قرار گرفته است. در این مقاله ضمن تعریف و بیان انواع امضای الکترونیک و بررسی جنبه‌های فنی آن، ومواردیگری که درزیرشاهد آن هستیم مورد مطالعه قرار گرفته است.

امروزه مهمترین نیازتجارت الکترونیک و دولت الکترونیک تامین امنیت آن است و در این مکان اطـلاع رسانی سریع و مناسب از یک سو و جلب مشارکت بخش خصوصی از سویی دیگر ؛ساده ترین راه دسـتیابی به این مهم است.

دنیای دیجیتال و فضای سایبر؛نیازمندیهای امنیتی خاص خود را می طلبد و اینکه بتوانیم هویت واقعی اشخاص را در چنین محیطی تشخیص دهیم از جمله مهمترین نیاز هاست. با استفاده از امضای دیجیتالی می توان هویت واقعی افراد را در دنیای دیجیتالی فضای سایبر تشخیص داد.تامین امنیتE_mail ها و وب سایت ها در هنگام تبادل اطلاعات مهم از جمله بیشترین موارد کاربرد امضای دیجیتالی است.

امضای دیجیتالی امضایی است که ثابت می کند نامه الکترونیکی دریافتی را به طور حتم خود فرستنده نوشته و فرستاده و تا به دست گیرنده برسد؛تغییری نکرده است. چون در صورت دستکاری نامه الکترونیکی که امضای دیجیتالی دارد؛امضا دیگر اعتبار نخواهد داشت و گیرنده متوجه تغییر و دستکاری در برنامه می شود .

کلاوس پتراشنور[۱] یکی از طرفداران امضاهای دیجیتالی است او می گوید: این امضاها مثل رمزنویسی است. از طریق امضای دیجیتالی می توانید اطلاعات را قفل کنید و مطمئن شویدکه کس دیگری به آن دسترسی پیدا نمی کند .این اطمینان تضمین شده است[۲].

وب سایت های اینترنتی که این قفلهای مطمئن را در اختیار دارند به راحتی قابل تشخیص اند. وقتی وارد این سایتها می شوید یک کلید زرد رنگ کوچک در سمت چپ صفحه می بینید این یعنی اینکه اطلاعاتی که فرستنده ارسال می کند قفل شده به گیرنده میرسندواطلاعات را کس دیگری نمی تواند بخواند و یا تغییر بدهد.گیرنده نیز برنامه مخصوصی در اختیتار دارد که قفل اطلاعات فرستاده شده را باز می کند.

در مورد ضریب اطمینان این امضاها باید بیان نمود که هر روش مطمئنی دست کم تا مدت زمان مشخصی مطمئن است تا زمانی که قفل هک نشده ؛اطلاعات محفوظ می ماند البته هرکسی نتوانسته این نوع قفل ها را که در خرید های اینترنتی از آن استفاده می شود را باز کند؛اما صد درصد نمی توان مطمئن بود[۳].

باید بدانیم که برگزاری این نمایشگاه گام بلندی در افزایش آگاهی کارشناسان و متخصصین در مورد این فناوری نوین می باشد چرا که مشکل مهم ما این است که متاسفانه اطلاعات بسیاری از مدیران و

۱. claus peterschnorr
۲. www.hamshahri.net
۳. www.hamshahri.ir

کارشناسان فن آوری اطلاعات در این رابطه کمتر از حداقل است.از طرفی دیگرهمان طور که هنگـامی کـه اینترنت وارد کشور شد هیچ تردیدی نسبت به آن وجود نداشـت و جانـداختن فرهنـگ اسـتفاده از مـدت زیادی را طلب کردپس با توجه به جدید بودن این تکنولوژی در ایران و مقایسه آن با اینترنت ؛باید در نظـر گرفت که جا انداختن فرهنگ استفاده از امضای دیجیتالی سـخت تـر از اینترنـت اسـت چـرا کـه امـضای دیجیتالی به غلط میان مردم معرفی شده است.

راهکارها و پیشنهادات که در این زمینه وجود دارد عبارتند از:

_ افزایش آگاهی مدیران و کارشناسان فن آوری اطلاعات در این رابطه

_ بالابردن سطح اطلاعات و آگاهی مردم از خدمات الکترونیک و جاانداختن فرهنـگ اسـتفاده ازآن در میان مردم

_ افزایش فعالیت بخش خصوصی در گسترش بهره گیری از امضای دیجیتالی و تلاش بخش خصوصی برای تصویب دولت الکترونیک در راستای خدمات رسانی هر جه بهتر و سریع تر به مردم.

تاریخچه امضای الکترونیک

اولین بار کانون وکلای ایالات متحده، در سال ۱۹۹۲ میلادی در خصوص مسائل حقوقی و قانونی امضاء در قراردادهای الکترونیک شروع به کار کـرد و در سـال ۱۹۹۵ مـیلادی پـیش‌نـویس و رهنمودهـای امـضای دیجیتال را که در خصوص نحوه امضاء در قراردادهای الکترونیک و زیرساخت‌های آن بـود، تهیـه کـرد. در همان سال اولین قانون در مورد امضای دیجیتـال را تـصویب کـرد کـه در مـورد ایجـاد قطعیـت و اعتبـار قراردادهای الکترونیک و نیز فن‌آوری‌های مربوط بـه رمزنگـاری و احـراز هویـت و مراجـع گـواهی امـضای الکترونیک بود. در سال ۱۹۹۶ میلادی آنسیترال قانون نمونه‌ای در باب تجارت الکترونیک تدوین کـرد کـه شامل مقرراتی در خصوص امضای الکترونیک بـود. در سـال ۱۹۹۷ مـیلادی، اتـاق بازرگـانی بـین‌المللـی مبادرت به صدور «راهنمای عمومی برای تجارت بین‌المللی دیجیتال مطمئن» کرده است. اتحادیه اروپا در سال ۱۹۹۹ میلادی، «دستورالعمل امضای الکترونیـک» را بـه تـصویب رسـانید و در نهایـت، گـروه کـاری آنسیترال در باب تجارت الکترونیک، «قانون نمونه آنسیترال در باب امضای الکترونیک» را تصویب کـرد تـا به عنوان یک معیار استاندارد و رهنمون برای قانونگذاری‌های ملی مورد استفاده کشورها قرار گیرد. بسیاری از کشورها، بین سال‌های ۱۹۹۶ تا ۲۰۰۱ میلادی، با استفاده از مقررات بین‌المللی موجود و رهنمـون‌هـای

ارائه شده در خصوص امضای الکترونیک مبادرت به قانونگذاری در این زمینه کـرده‌انـد. و در حـال حاضـر می‌توان گفت امضای الکترونیک در تمام نظام‌های حقوقی مورد پذیرش قرار گرفته است. در قانون تجـارت 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.

جایگاه امضا در نظام سنتی ثبت اسناد

باتوجه به قانون مدنی داریم: «امضایی که در روی نوشته یا سندی باشد بر ضرر امضا کننده دلیل است»[۱] ، مقنن در این ماده به یکی از مهمترین آثار امضا، یعنی دلیل بودن سند امـضا شـده بـه نفـع امـضا کننـده توجهی نداشته است. به طور کلی «نوشته منتسب به اشخاص در صورتی قابل استناد است که امـضا شـده باشد. امضا نشان تایید اعلامهای مندرج در سند و پذیرش تعهدهای ناشی از آن است و پیش از آن نوشـته را باید طرحی به حساب آورد که موضوع مطالعه و تدبر است و هنوز تصمیم نهایی درباره آن گرفتـه نـشده است».

اگرچه ایجاد حق و تکلیف به عنوان مهمترین اثر امـضا در اکثـر اسـناد، مـورد توجـه حقوقـدانان قـرار نگرفته، با این‌حال می‌توان از ماده ۶۵ قانون ثبت اسناد و امـلاک (مـصوب ۱۳۱۰ بـا اصـلاحات و الحاقـات بعدی) آن را استنباط کرد. به موجب این ماده، «امضای ثبت سند پس از قرائت آن به‌توسط طرفین معامله یا وکلای آنها دلیل بر رضایت آنها خواهد بود». از ماده مذکور استنباط می‌شود که عدم امضای سـند ثبـت شده از سوی شخص یا اشخاص ذینفع و یا متعهد، مفهومی جز بی‌اعتباری و فقدان هـر گونـه اثـر حقـوقی برای آن سند ندارد.

با ثبت سند و طی تشریفات امضا، «سندی که مطابق قـوانین بـه ثبـت رسـیده رسـمی اسـت و تمـام محتویات و امضاهای مندرج در آن معتبر خواهد بود مگر اینکه مجعولیت آن سند اثبات شـود»[۲]. بنـابراین امضا کننده نمی‌تواند امضای خود را انکار یا در درستی محتوای سند رسمی تردید کنـد و فقـط مـی‌توانـد جعلیت یا بی‌اعتباری قانونی این دسته از اسناد را اثبات نماید[۳].

[۱] . ماده ۱۳۰۱ قانون مدنی
[۲] . ماده ۷۰ قانون ثبت اسنادواملاک
[۳] . ماده ۱۲۹۲ قانون مدنی

تصدیق صحت امضا، در نظام سنتی ثبت اسناد از جمله وظایفی است که بر عهده مسوولین دفاتر نهاده شده[1] و در قانون دفاتر اسناد رسمی و کانون سردفتران و دفتریاران، دفتری به نـام «دفتـر گـواهی امـضا» پیش‌بینی شده که بنابر ماده ۲۰ قانون ثبت اسنادواملاک: «دفتری است کـه منحـصراً مخـصوص تـصدیق امضا ذیل نوشته‌های عادی است و نوشته تصدیق امضا شده با توجه به ماده ۳۷۵ (قـانون) آئـین دادرسـی مدنی مسلم‌الصدور شناخته می‌شود». به نظر می‌رسد، «دفاتر خدمات صدور گواهی الکترونیکی» مذکور در باب دوم قانون تجارت الکترونیکی[2]به این دفاتر شباهت زیادی دارند.

جایگاه امضای دیجیتالی در ثبت اسناد به شیوه الکترونیکی

در اسناد مکتوب، امضا، نشان تایید تعهدات قبول شده در آن سند به شـمار مـی‌آیـد. از آن جهـت کـه در تجارت الکترونیکی «مدارک الکترونیکی» دارای جایگاهی همانند اسناد مکتوب هستند، لـذا امـضا در ایـن مدارک نیز علی‌الاصول دارای همان ارزش اثباتی می‌باشد. در ثبـت الکترونیکـی اسـناد و مـدارک، چگونـه می‌توان از امضای دیجیتالی بهره گرفت و بهترین مرجع برای تصدی امور گواهی امضای الکترونیکی و ثبت اسناد الکترونیکی کجاست. بررسی موضوع همواره با مبنا قرار دادن این ایده انجام شده که تخلف از رویه و قوانین موجود در زمینه ثبت اسناد و گـواهی امـضا دارای آثـار زیانبـاری ـ از حیـث حقـوقی، اجتمـاعی و اقتصادی ـ خواهد بود و از این حیث، اساساً امضا و مدارک الکترونیکی خصوصیتی ندارند که موجب تغییـر مرجع ثبت و گواهی آنها شود.

امضای دیجیتال[3]

نگاهی علمی و فنی

امضای دیجیتالی به این معناست که طرف مصرف کننده و طرف تجاری بتوانند از امنیت ارتبـاط و برنامـه ها با استفاده از PKL[4] بهره برداری کنند.امضای دیجیتالی به عنوان یکی از دستاوردهای الکترونیکی مدرن از مبانی علمی خاصی پیروی می‌کند. اگرچه این جنبه از امضای مذکور در نوشته‌های علمـی مـورد توجـه

[1] . قانون ثبت اسنادو املاک ماده ٤٩ بند٣
[2] . ماده های ٣١و٣٢قانون تجارت الکترونیکی

[3]. Digital sign
[4]. public key Infrastructure

قرار گرفته، ولی آثار حقوقی آن به‌دقت تحلیل نشده است. اهمیت این مسایل به حدی می‌باشد که می‌توان جنبه‌های دیگر را با مبنا قرار دادن آن مورد بررسی قرار داد.

امضاهای دیجیتالی با رمزگذاری معروف به رمزگذاری کلید عمومی ایمن می‌شوند. رمزگذاری کلید عمومی بر الگوریتمی مبتنی است که از طریق دو نوع رمز متفاوت معروف به «کلید» ایجاد شده و کلیدهای مذکور برای رمزگذاری و رمزگشایی داده‌پیام مورد استفاده قرار می‌گیرد. کلید رمزگذاری به «کلید خصوصی» معروف بوده و دارنده کلید به عنوان صاحب امضا ملزم به حفظ و عدم افشای آن می‌باشد. اما از آن جهت که همه افراد باید از درستی امضای شخص اطمینان یابند، کلید عمومی باید در دسترس همگان باشد. هر امضای دیجیتالی که ایجاد می‌شود، نسبت به دارنده آن بی‌همتاست و استفاده از الگوریتمهای مختلف برای رمزگذاری امضاهای متفاوت موجب تمایز امضای افراد از همدیگر می‌شود.

افرادی که در ایجاد و ایمنی امضای دیجیتالی مداخله می‌کنند، را ـ بر حسب مورد ـ می‌توان به شرح زیر برشمرد.:

الف . امضا کننده اصلی. به مفهوم شخصی که امضای دیجیتالی را برای استفاده از آن در تایید مدرکی ایجاد می‌کند.

ب . دفتر خدمات گواهی. مکانیسم لازم را برای ایمنی و اطمینان امضا فراهم می‌سازد. با گواهی این مرجع، امضا کننده مجاز به استناد به مدارک گواهی شده می‌شود و کلیدهای اختصاص یافته به او به نام او ذخیره شده و به شخص دیگری تعلق نمی‌گیرد.

ج . دفاتر ثبت. بر خلاف مورد قبل که ایمنی و اطمینان امضا را از جنبه فنی تامین می‌کند، سردفتر به عنوان شخص ثالث قابل اعتماد به تصدیق مدارک و تایید هویت امضا کننده اقدام می‌کند. به طور کلی، اطلاعات تهیه شده توسط دفاتر خدمات گواهی از جمله عواملی است که زمینه اعتماد سردفتر را به امضای ایجاد شده فراهم می‌سازد، اگرچه او نیز موظف است تا بررسیهای متعارف را به عمل آورد. البته امکان دارد که به دلیل عدم پیش‌بینی در قانون و رویه عملی، این دفاتر در برخی از کشورها تشکیل نشده باشند که آثار منفی آن را بعدها بررسی خواهیم کرد.

د. طرف اعتماد کننده. شخصی است که با بررسی کلید عمومی به اصالت و صحت امضای دیجیتالی اعتماد کرده و آن را به عنوان معیاری برای تنفیذ تعهد صاحب امضا در قبال خود می‌پذیرد. این فرد اگرچه در فرایند ایجاد و امنیت امضا نقشی ندارد، ولی قبول وی از آن جهت که به امضای دیجیتالی اعتبار عملی

می‌بخشد، بسیار ارزشمند محسوب می‌شود، زیرا تقریباً در تمام قوانین راجع به امضای دیجیتالی بـه افـراد این اختیار داده شده که از پذیرش امضا و مدارک الکترونیکی در روابـط تجـاری و مـالی خـود بـا دیگـران امتناع نموده و امضای دستی و مدارک کاغذی مطالبه کنند که این امر با توجه به مـسایل متعـددی چـون ضعف امنیت و اعتماد در فضای مجازی قابل توجیه است.

آنچه به اختصار درباره جنبه‌های علمی و فنی امضاهای دیجیتالی ذکر شده، نشان می‌دهـد کـه حـذف دفاتر ثبت اسناد از ساختار شکل‌گیری، ایمنی و تصدیق این گونه از امضاها تا چه حد می‌تواند زیانبار باشد: اگرچه نام «امضا» برای هر دو نوع امضای دستی و دیجیتالی به کار می‌رود، اما در تفـاوت مـاهوی ایـن دو نباید تردید کرد. امضای دستی نشان می‌دهد کـه شـخص آن سـند را تنفیـذ نمـوده، حـال آنکـه امـضای دیجیتالی مدرک معین دلالت بر به کارگیری کلید خصوصی متعلق به فرد معین برای رمزگـذاری آن دارد، که در صورت فقدان تصدیق محضری نشانگر چیزی جز عدم تغییر داده‌پیـام بعـد از ایجـاد ان نیـست. بـه عبارت دیگر بدون وجود سابقه ثبتی و مدارک دقیق علمی، امضای دیجیتالی هیچ دلالتی بـر دخالـت یـک فرد در محتوای سندی که امضا در آن به کار گرفته شده، ندارد.

بدون دخالت دفاتر اسناد رسمی ـ یا هر ارگان دیگر کـه بـه اصـول سـنتی ثبـت اسـناد احتـرام بگـذارد ـ اشکالات دیگری نیز بروز می‌کند که آثار آن به مراتب بدتر و وسـیع‌تـر از مـوارد بالاسـت: فقـدان سـابقه و بایگانی مطمئن مدارک، وجود گواهی برای همیشه، امکان اختصاص کلید خصوصی یـک شـخص بـه فـرد دیگر به دلیل بی‌اطلاعی از این امر یا اشتباه، افشای رمزگذاری یا بی‌اعتباری استانداردهای آن، تغییـر غیـر مشروع رمز و.. از مشکلات فنی و علمی می‌باشد.

امنیت بر روی اینترنت

ما اکنون در حال سپری کردن عصر اطلاعات هستیم. تعداد افراد و تجارتهایی که هر روز به اینترنت ملحق می شوند به طور بی سابقه ای در حال رشد است. در حالیکه هـر روز دسترسـی بـه اینترنـت آسـان تـر و سرعت آن سریعتر می شود و قیمت آن ارزانتر می شود, بسیاری از افراد میزان زیادی از وقـت خـود را بـر روی اینترنت به تبادل اطلاعات و همچنین به تبادلات مـالی میپردازنـد. در حالیکـه اینترنـت یـک شـبکه اطلاعاتی بازاست. هرکسی می تواند از اینترنت استفاده کنـد و در نتیجـه هـر کـسی میتوانـد از آن بـرای استخراج اطلاعات از مناطق آسیب پذیر، برای مقاصد سودجویانه و غیر قانونی استفاده کنـد. اگـر اینترنـت

بخواهد به منبعی برای استفاده اهداف تجاری و انتقال اطلاعات تبدیل شود مطمئنا به یک بنیاد و موسسه امنیت هم نیاز دارد.استفاده از شبکه های کامپیوتری و اینترنت , خطرات امنیتی متعددی را به همراه دارد. برای همین سیستم عامل های لینوکس برنامه های متعددی را برای تامین امنیت سیستم هـا و ارتباطـات ارائه می دهد.

استراق سمع

در این نوع حمله غیرفعال , اطلاعات تغییر نمی یابند ولی محرمانگی آنها از دست می رود. بطور مثال اگـر بخواهید اطلاعات خود را بصورت متن عادی و رمز نشده به سیستم های راه دور ارسال کنید آنگاه ممکـن است این اطلاعات توسط افراد غیرمجاز دریافت شـوند . دسـتبرد اطلاعـات ممکـن اسـت در مکـان هـای مختلفی همانند شبکه های محلی , سوئیچ های انتقال داده ها و یا شبکه اینترنت انجام شود . هـم اکنـون نرم افزارهای مختلفی برای دریافت اطلاعات مختلف از روی یک شبکه محلـی وجـود دارد و ویـروس هـا و حمله کنندگان نیز می توانند اطلاعات انتقال یافته بر روی یـک شـبکه عمـومی را دریافـت نماینـد. بـرای جلوگیری از این مشکل امنیتی از تکنیک های رمزنگاری متقارن و نامتقارن داده ها استفاده می شود.

تغییر اطلاعات

در این نوع حمله فعال , اطلاعات در حین انتقال به مقصد مورد حمله قرار می گیرد و جامعیت داده هـا از دست می رود. حمله کننده با دریافت اطلاعات آنها را تغییـر مـی دهـد و یـا آنهـا را بـا اطلاعـات دیگـری جایگزین می کند. مقصد نیز این مسئله را تشخیص نداده و داده ها را استفاده می نماید. برای جلوگیری از این نوع حمله از توابع درهم ساز یا هش استفاده می شود.

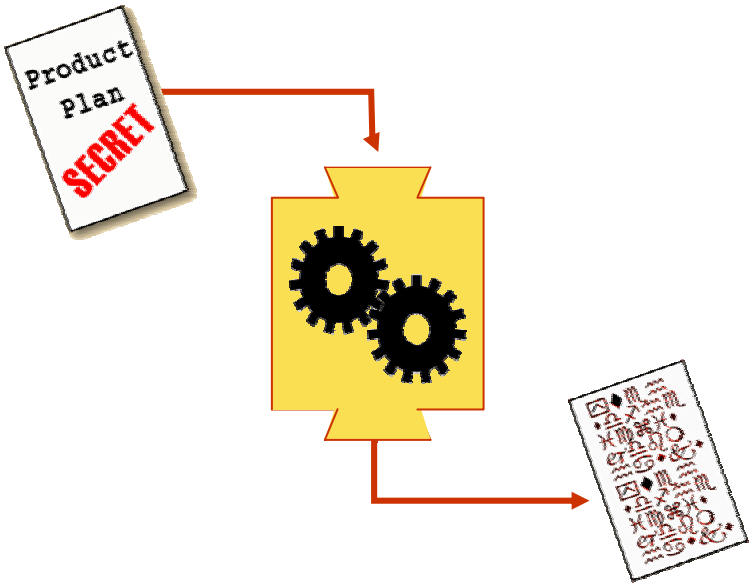
جعل هویت

در این نوع حمله فعال , شخص حمله کننده خود را به عنوان یک کـاربر مجـاز بـه سیـستم هـای محلـی معرفی می کند و بدین ترتیب از سرویس های مختلف شبکه محلی استفاده می کند . بـرای جلـوگیری از این نوع حملات و فراهم کردن احراز هویت کاربران و نرم افزارها از امضاء دیجیتالی استفاده می شود. عدم سرویس دهی در این روش، حمله کنندگان از ارائه سرویس های یک موسـسه جلـوگیری مـی نماینـد. راه

اندازی این نوع حملات راحت می باشد و اغلب از روش های جعل هویت و نیز ارسال مقادیر زیادی از بسته های IP انجام می گیرد. این حملات به اختصار DOS نامیده می شوند و جزء حملات فعال هستند. با استفاده از دیواره های آتش شبکه خطر این حملات می توان کاهش داد.

رمز نگاری داده ها

رمزنگاری فرآیندی است که در طی آن، داده ها از فرم عادی خود خارج و به صورتی تبدیل می شوند که بدون داشتن اطلاعات لازم (کلید رمزگشائی) خواندن آنها تقریبا غیر ممکن می باشد. بنابراین در این روش با رمز نمودن داده ها از دسترسی افراد غیرمجاز به داده ها جلوگیری شده و محرمانگی داده ها بدست می آید. در این روش ابتدا در مبدا عمل رمز نگاری انجام شده و سپس رمز شده داده ها به مقصد ارسال می گردند. حمله کننده ای که استراق سمع میکند و بسته های داده ها را در حین انتقال از شبکه دریافت می کند، رمز شده داده ها را به دست می آورد که برای او قابل استفاده نیست . دریافت کننده داده ها در مقصد هم داده رمز شده را دریافت می نماید ولی او بدلیل اینکه، اطلاعات رمز گشائی داده ها را دارد می تواند داده ها را رمز گشائی نموده و استفاده کند. برای رمزنگاری داده ها دو روش متقارن و نامتقارن وجود دارد . ایده رمزنگاری متقارن از سالها پیش وجود داشته است و مسئله جدیدی نیست ولی رمزنگاری نامتقارن از اصول ریاضی و الگوریتم های پیچیده ای استفاده می کند و روش جدیدی در رمزنگاری داده ها بشمار می آید. در ادامه به بررسی کامل هر دو روش خواهیم پرداخت.



رمزنگاری متقارن داده ها

در این روش رمزنگاری، ترکیبی از جابجایی و جایگزینی داده ها در مراحل متعدد انجام می شوند تا پیچیدگی لازم بر روی داده ها بوجود آید. همچنین برای انجام عملیات رمزنگاری، یک کلید مشترک و محرمانه بین فرستنده و گیرنده استفاده می شود. در این روش داده ها در مبدا با کلید مشترک رمز شده و به مقصد ارسال می گردند و در مقصد نیز داده ها با کلید مشترک رمز گشائی می شوند. در رمزنگاری متقارن فرض بر این است که حمله کننده از الگوریتم رمزنگاری مطلع است و تنها بر محرمانگی کلید رمزنگاری مشترک تکیه می شود. بطور کلی هرچه طول کلید بیشتر باشد مدت زمان بیشتری برای شکستن رمز داده ها صرف می گردد و امنیت بیشتری بدست می آید. با توجه به قدرت پردازش فعلی , انتخاب کلیدهای با طول بیشتر از ۱۲۸ بیت مناسب بنظر می رسد. همچنین کلید های رمزنگاری مدتی پس از استفاده باید تعویض شوند و کلیدهای جدید نیز حتی الامکان باید بصورت تصادفی انتخاب گردند تا حداکثر امنیت بدست آید. الگوریتم های رمزنگاری متقارن بدو دسته الگوریتم های بلاکی و جریانی , داده ها بیت به بیت رمزنگاری یا رمزگشائی می شوند. الگوریتم های جریانی سریعتر از بلاکی هستند. الگوریتم هائی همانند DES بلاکی و الگوریتم هائی همانند RC۴ جریانی می باشند. البته لازم به ذکر است که رمزنگاری متقارن، احراز هویت را نیز فراهم می آورد. بطور مثال در صورتی که داده رمزشده ای دریافت شد با توجه به کلید مورد استفاده می توان از هویت شخص ارسال کننده داده نیز مطمئن شد زیرا این کلید ها محرمانه فرض می شوند. رمزنگاری متقارن از کارایی مطلوبی برخوردار است و تاخیر کمی را در عملیات رمزنگاری و رمزگشائی داده ها فراهم می آورد. بنابراین از آن می توان برای رمزنگاری حجم بزرگی از داده ها استفاده نمود. از این نوع رمزنگاری در پروتکل های امنیتی محیط باسیم و بی سیم بطور گسترده استفاده می شود. الگوریتم هایی همانند RC۴,IDEA,DES,۳DESو . . . از الگوریتم های متقارن می باشند.

رمزنگاری نا متقارن

رمزنگاری نامتقارن یا رمزنگاری کلید عمومی، بزرگترین و شاید تنهاترین انقلاب موجود در تاریخ رمزنگاری است . در الگوریتم این روش،به جای جایگشت و جایگزینی داده ها، از توابع ریاضی استفاده می شود و بجای یک کلید محرمانه مشترک، یک کلید عمومی و یک کلید خصوصی ایجاد و کلید عمومی در اختیار

همه و کلید خصوصی تنها در دسترس کاربر قرار مـی گیـرد. بـرای محرمـانگی کلیـدهای خـصوصی، رمـز عبوری برای دسترسی پایگاه داده کلید خصوصی در نظر گرفته می شود. مفهوم رمزنگاری کلیـد عمـومی، در پی تلاش برای حل دو مشکل توزیع کلید به روشـی امـن و امـضاء دیجیتـالی بوجـود آمـده و دارای دو خاصیت مهم و اساسی زیر می باشد :

۱- طور محاسباتی محاسبه کلید رمزگشائی از کلید رمزگذاری غیر ممکن است. ۲- هر دو کلید خـصوصی و عمومی را می توان برای رمزنگاری استفاده نمود . البته برای رمزگشائی نیز باید کلید دیگر استفاده کـرد. در این روش رمزنگاری، ابتدا کلید عمومی مقصد به روش معتبری فراهم شده و سپس داده ها توسط کلید عمومی مقصد رمزنگاری و به آن ارسال می گردند. حمله کننده بین مسیر مبداء و مقصد مـی توانـد کلیـد عمومی مقصد را به راحتی به دست بیاورد ولی با این کلید قادر به رمزگشائی داده ها نخواهد بود. در مقصد داده ها توسط کلید خصوصی رمزگشائی و استفاده می شوند. توجـه داشـته باشـید کـه عکـس ایـن روش محرمانگی داده ها را بوجود نمی آورد زیرا در صورتی که داده ها ابتـدا توسـط کلیـد خـصوصی رمزنگـاری شوند و سپس منتقل گردند چون همه افراد کلید عمومی را می دانند بنابراین همه مـی تواننـد داده هـای رمز شده را رمزگشائی نمایند و محرمانگی داده ها از دست می رود. برای بدست آوردن کلیـد عمـومی بـه روشی معتبر می توان از گواهی های دیجیتالی استفاده نمود. در مقایسه با رمزنگاری متقـارن ایـن روش از محاسبات پیچیده و زمانگیری استفاده می نماید و لذا برای رمزنگاری حجم زیادی از داده ها بکار نمی رود. اغلب از این نوع رمزنگاری، برای ارسال مقـادیر کمـی از داده هـا، هماننـد کلیـد هـای رمزنگـاری متقـارن استفاده می شود. متداول ترین الگوریتم برای رمزنگاری کلید عمومی الگوریتم RSA است[۱].

امضای دیجیتالی از دید برنامه نویسی

در یک امضای دیجیتالی سه دسته اطلاعات وجود دارد:

هویت تولید کننده نرم افزار، هویت منبع تایید کننده (سازمانی که امضاء را صادر کرده) و یک عـدد رمـز برای تایید این مطلب که محتویات نرم افزار دستکاری نشده است.

اگر می خواهید برای وب محتویات فعال بنویسید باید یک گواهینامه کد تعیین اعتبار برای خود دست و پا کنید تا بتوانید برای نرم افزار های خود امضای دیجیتالی بگیرید. اگر فقط بـرای اینترنـت برنامـه مـی

[۱] . الگوریتم RSA توسط سه نفربه نام های رایوست،شامیر،وآدلمن بوجود آمده است.

نویسید نیازی به این مراحل ندارید چون سطح امنیتی در آنها معمولا پایین است و نیازی به امضای دیجیتالی وجود ندارد.اگر صرفاً برای شرکت خود نرم افزار می نویسید می توانید از گواهینامه آن استفاده کنید. اما توصیه می شود خودتان هم این گواهینامه را بگیرید.با آن که شرکت های متعددی برای صدور گواهینامه کد تعیین اعتبار وجود دارند، میکروسافت شرکت Verisign را توصیه می کند. برای کسب اطلاعات بیشتر می توانید به سایت وب این شرکت مراجعه کنید[1].

هزینه دریافت این گواهینامه ۲۰ دلار در سال و مراحل انجام آن بسیار ساده است:

۱- در سایت این شرکت، یک فرم پر کنید و در آن اطلاعات خواسته شده (از جمله اطلاعات مربوط به کارت اعتباری) را وارد کنید.

۲- شرکت Verisign کد شناسایی شما را با پست الکترونیک برایتان ارسال خواهد کرد.

۳- به صفحه نصب گواهینامه رفته و کد شناسایی خود را وارد کنید. این کار باید در همان کامپیوتری که توسط آن کد شناسایی را گرفته اید، انجام شود.

۴-گواهینامه به کامپیوتر شما فرستاده خواهد شد.

علت استفاده از یک امضای دیجیتال چیست ؟

اجازه دهید برای پاسخ به سوال فوق ، سوالات دیگری را مطرح کنیم !

برای تشخیص و تائید هویت فرد ارسال کننده یک نامه الکترونیکی از چه مکانیزمهائی استفاده می شود؟

فرض کنید یک نامه الکترونیکی را از یکی از دوستان خود دریافت داشته اید که از شما درخواست خاصی را می نماید، پس از مطالعه پیام برای شما دو سوال متفاوت مطرح می گردد :

الف) آیا این نامه را واقعا" وی ارسال نموده است ؟

ب)آیا محتوای نامه ارسالی واقعی است و وی دقیقا" همین درخواست را داشته است ؟

آیا وجود هر نامه الکترونیکی در صندوق پستی ، نشاندهنده صحت محتوا و تائید هویت فرد ارسال کننده آن است ؟

سوءاستفاده از آدرس های Email برای مهاجمان و ویروس ها به امری متداول تبدیل شده است و با توجه به نحوه عملکرد آنان در برخی موارد شناسائی هویت فرد ارسال کننده یک پیام بسیار مشکل و

[1].http://www.verisign.com/developers/index.html

گاها" غیرممکن است . تشخیص غیرجعلی بودن نامه های الکترونیکی در فعالیت های تجـاری و بازرگـانی دارای اهمیت فراوانی است .

یک نامه الکترونیکی شامل یک امضای دیجیتال، نشاندهنده این موضوع است که محتوای پیام از زمان ارسال تا زمانی که به دست شما رسیده است ، تغییر نکـرده اسـت . در صـورت بـروز هـر گونـه تغییـر در محتوای نامه ، امضای دیجیتال همراه آن از درجه اعتبار ساقط می شود .

انواع امضای الکترونیک

از زمان پیدایش فن‌آوری امضای الکترونیک تاکنون روش‌های مختلفی در خصوص چگونگی انجام امـضاء از طریق الکترونیک و با توجه به افزایش ضریب امنیت آن معرفی و به کار گرفته شده است کـه مـورد اشـاره قرار می‌گیرد:

کلمات عبور

یکی از روش‌های ساده و رایج ایجاد ایمنی و اعتبار به کارگیری یک کلمه عبور منحصر به فرد یا اسـتفاده از یک شماره هویت شخصی در انتهای سند است که به طور مخفی به آن منضم می‌شود.امنیت ایـن روش بسیار پایین است، زیرا کلمات عبور و شماره‌های شخصی افراد به راحتی توسط نفوذگرهـا شناسـایی و بـه سرقت می‌روند و ممکن است توسط آنها یا دیگران مورد سوءاستفاده قرار گیرد. (مثـل آنچـه کـه در مـورد کارت‌های اعتباری رخ می‌دهد)

امضای بیت مپ

این نوع امضاء تصویر اسکن شده امضای دست‌نویس است که در آن ابتدا فرد بر روی کاغذ امضای خـود را پیاده می‌کند و سپس آن را اسکن کرده و می‌تواند تصویر اسکن شده را به عنوان امضاء بـه هـر فـایلی کـه خواست به عنوان امضای الکترونیک منضم کند.

قلم نور

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.

امضای بیومتریک

این نوع امضاء مبتنی بر ویژگی‌ها و معرف‌های زیست‌شناختی فرد یعنی خصوصیات رفتاری (مثل نحوه انجام امضای دست‌نویس) و خصوصیات فیزیولوژیک (مثل اثر انگشت) است. در این روش اگرچه ممکن است تا حد 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.

امضای دیجیتال

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. امضای دیجیتال مبتنی بر علم رمزنگاری است و از دو نوع الگوریتم به نام‌های «کلید عمومی» و «کلید خصوصی»استفاده می‌کند.

امضاهای دیجیتال از طریق رمزنگاری ایجاد و شناخته می‌شوند. همانطور که گفتیم رمزنگاری شاخه‌ای از ریاضیات کاربردی است که موضوع آن تبدیل پیغام‌ها به شکل و صورتی است که در حالت عادی قابل فهم و خواندن نباشد، عکس این عملیات (یعنی قابل فهم کردن پیغام رمزنگاری شده) نیز با استفاده از این شاخه ریاضیات کاربردی امکان‌پذیر است. رمزنگاری مبتنی بر کلید عمومی، روشی است که در ایجاد امضاهای دیجیتال به کار می‌رود: در این نوع رمزنگاری از الگوریتمی استفاده می‌شود که شامل دو کلید متفاوت است؛ این دو کلید در عین حال از نظر ریاضی با هم مرتبط هستند. از بین این جفت کلید ، یک کلید برای ایجاد امضای دیجیتال و یا تبدیل داده‌ها به شکلی 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 اغلب «سیستم رمزنگاری نا متقارن » نامیده می‌شوند.

دو کلید مکملی که از آنها در سیستم رمزنگاری نا متقارن استفاده می‌شود، کلید خصوصی - که صرفاً امضا کننده از آن مطلع است و برای ایجاد امضای دیجیتال به کار می‌رود- و کلید عمومی - که معمولاً افراد بیشتری آن را می‌شناسند و جهت شناسایی و بررسی اصالت و اعتبار امضای دیجیتال مورد استفاده قرار می‌گیرد- نامیده می‌شوند. اگر در اثر روابط گسترده امضا کننده با دیگران، اشخاص زیادی به شناسایی و بررسی اعتبار امضای دیجیتال امضا کننده نیاز داشته باشند، کلید عمومی باید بین تمامی آنها توزیع (و برای آنها ارسال) شود و یا در دسترس آنها باشد مثلاً از طریق درج در یک دفترچه راهنما یا فهرست برخط که براحتی قابل دسترسی باشد. علیرغم ارتباط ریاضی کلیدهای این جفت کلید، در صورتی که سیستم رمزنگاری نامتقارن به صورتی ایمن طراحی و اجرا شده باشد، پی بردن به کلید خصوصی از طریق علم به کلید عمومی امری ناممکن خواهد بود. بنابراین، اگرچه ممکن است افراد بسیاری از کلید عمومی امضا کننده آگاه بوده و آن را جهت شناسایی امضای وی به کار گیرند، این افراد نمی‌توانند کلید خصوصی مشارالیه را کشف نمود. و برای جعل امضای دیجیتال وی از آن استفاده کنند.[1]

آنسیترال

کمیسیون سازمان ملل در خصوص تجارت بین‌الملل در سال ۱۹۶۶ با هدف یکنواخت نمودن حقوق تجارت بین‌المللی به وجود آمد. بخشی از فعالیتهای این سازمان به توسعه قوانین نمونه و اسناد استاندارد جهت تسهیل روابط تجاری بین‌المللی اختصاص دارد. قانون نمونه برای داوری تجاری بین‌المللی، قواعد داوری آنسیترال، قانون نمونه در انتقال اعتبار بین‌المللی و کنوانسیون دین در مورد بیع بین‌المللی کالا در شمار مهمترین قوانین نمونه آنسیترال قرار دارند.

اتحادیه اروپا

اتحادیه اروپا تاکنون، مبادرت به وضع دستورالعمل‌های متعدد در زمینه تجارت الکترونیکی نموده است. دستورالعمل ۱۹۹۷ که بیانگر خط مشی قانونگذاری راجع به تجارت الکترونیکی است، این امر را تضمین

[1]. http://www.notary.ir/Magazine۵۹/Mag۵۹۰۵.htm

می‌کند که در بازار داخلی مانعی برای تجارت الکترونیکی وجود نخواهد داشت. تضمین مذکور در دستورالعملهای بعدی اتحادیه اروپا نیز مورد تأکید قرار می‌گیرد. از جمله می‌توان از دستور العمل تجارت الکترونیکی که می‌خواهد پاسخگوی مهمترین مسائل مرتبط با صلاحیت انعقاد قراردادها و مسؤولیت واسطه‌ها باشد و دستورالعمل امضاء الکترونیکی که امضاء الکترونیکی را به عنوان جایگزین امضاء دستی می‌پذیرد، نام برد.

از دیگر اقدامات اتحادیه اروپا در زمینه وضع قواعد برای تجارت الکترونیکی، دستورالعمل فروش راه دور است که در قراردادهای انعقاد یافته از طریق الکترونیکی حمایتهای قابل توجهی را از مشتری به عمل می‌آورد. دستورالعملهای اتحادیه اروپا از کشورهای عضو می‌خواهد تا قوانین خود را با اتحادیه هماهنگ نمایند. قوانین داخلی یک کشور تنها برای همان کشور به عنوان منبع حقوق دارای اعتبار است، اما، هنگامی که موضوع وضع قانون در خصوص پدیده‌ها و فن آوریهای نوین باشد. کشورهای مختلف از تجارب یکدیگر بهره می‌گیرند.

قوانین داخلی کشورها

در سال ۱۹۹۶ گروه کاری آنسیترال در خصوص تجارت الکترونیکی مبادرت به ارائه یک قانون نمونه در این زمینه کرد که در بردارنده قواعدی راجع به تجارت الکترونیکی بود و سعی داشت قواعد حقوقی را با فن‌آوریهای نوین سازگار نماید.

تلاشهای کمیسیون سازمان ملل، قانون نمونه آنسیترال نتوانست به هدف خود که ایجاد یک نظام هماهنگ بین الملل است نایل شود. زیرا، ارائه این قانون هنگامی صورت گرفت که بسیاری از کشورهای پیشرفته، از قبل مبادرت به وضع قوانینی در قلمرو تجارت الکترونیکی کرده بودند که کاملاً متفاوت با قواعد آنسیترال بود. بعید به نظر می‌رسد که کشورهای مذکور بخواهند قوانین داخلی خود را به منظور هماهنگی با آنسیترال جرح و تعدیل نمایند.

طی سالهای اخیر و با درک اهمیت ویژه تجارت الکترونیکی کشورها در صدد برآمده‌اند تا به وضع قانون در این زمینه بپردازند. در سال ۱۹۹۵ نخستین قانون امضای دیجیتال در ایالت یوتای امریکا به تصویب رسید. کره جنوبی در سال ۱۹۹۶؛ آلمان، مالزی، استونی، ایتالیا، برزیل در سال ۱۹۹۷؛ سنگاپور، سوئد، کانادا، لوکزامبورگ در سال ۱۹۹۸؛ استرالیا، فنلاند، کلمبیا، نیوزیلند در سال ۱۹۹۹؛ ترکیه،

هنگ‌کنگ، تایلند، مالت، ایرلند، سوئیس، فرانسه در سال ۲۰۰۰؛ آرژانتین، بلژیک، نروژ، مجارستان، تونس، ونزوئلا در سال ۲۰۰۱؛ ژاپن، لیتوانی، رومانی، روسیه در سال ۲۰۰۲ از جمله کشورهایی می‌باشند که مبادرت به انشاء قانون در خصوص تجارت الکترونیکی نموده‌اند. قوانینی که در کشورهای عضو اتحادیه اروپا به تصویب رسیده است، در راستای اجرای دستورالعملهای اتحادیه اروپاست. مع هذا این قوانین ترجمه صرف مصوبات اتحادیه نیستند و عموماً گامی فراتر برداشته‌اند.

در حقوق کشور ما لایحه توجیهی قانون تجارت الکترونیکی برای نخستین بار در سال ۱۳۷۸ توسط گروه کاری حقوقی کمیته ملی ادیفاکت ارائه گردید و شورای عالی اطلاع‌رسانی در سال ۱۳۸۰ سیاست تجارت الکترونیکی را که از طریق وزارت بازرگانی تدوین شده بود. به تصویب رسانید. هم اکنون نیز پیش‌نویس قانون تجارت الکترونیکی به مجلس شورای اسلامی تقدیم شده است. این پیش‌نویس که عمدتاً ملهم از قانون نمونه آنسیترال می‌باشد، نیازمند تحلیل حقوقی است و جا دارد که ضوابط آن با موازین حقوقی ما سازگار شود. بعبارت دیگر باید روشن گردد که این ضوابط تا چه حد قابل پذیرش می‌باشند و در چه مواردی اصلاح و تغییر قوانین پیشین ضروری است

اسناد و مقررات بین‌المللی

بحث امضای الکترونیکی در سطح بین‌المللی، نخستین بار درباره تجارت الکترونیکی در سال ۱۹۹۶ مطرح گردید[۱]. در این ماده، امضای واجد شرایط الکترونیکی دارای همان آثار و ارزش اثباتی شناخته شده که امضای سنتی داراست. بنابر گزارش گروه کاری تجارت الکترونیکی آنسیترال با امضای الکترونیکی نیز اصالت سند و انتساب آن به امضا کننده اثبات و وی متعهد به محتوای سند خواهد بود. اهمیت موضوع امضا در تجارت الکترونیکی سبب شده تا آنسیترال در سال ۲۰۰۱ قانون نمونه جداگانه‌ای درباره امضاهای الکترونیکی در ۱۲ ماده به تصویب رساند.

بنابر ماده ۳ قانون نمونه (۲۰۰۱)، در صورت داشتن شرایط ایمنی به هیچ وجه نمی‌توان میان فناوریهای گوناگون ایجاد امضا تفاوت قایل شد و تمام آنها معتبر و دارای آثار حقوقی یکسان خواهند بود. شناسایی اصل «کارکرد یکسان» در این ماده از آن جهت دارای اهمیت است که هیچ تردیدی در عدم امکان تبعیض میان امضای دستی (مکتوب) و الکترونیکی باقی نمی‌گذارد. در ماده ۶ شرایطی برای اعتبار

[۱] . ماده ۷قانون نمونه آنسیترال

امضای الکترونیکی ذکر شده و در مواد ۸ و ۹ وظایفی بر دوش امضا کننده و دفاتر صدور گواهی الکترونیکی نهاده شده است .ماده ۱۲ قانون مذکور نکته جالبی مطرح می‌سازد و آن «به رسمیت شناختن گواهی‌ها و امضاهای الکترونیکی (صادره در) خارج» می‌باشد. مطابق این ماده، در تعیین آثار حقوقی برای گواهی یا امضای الکترونیکی نباید به حوزه جغرافیایی محل صدور امضا یا مرکز امور تجاری امضا کننده توجه شود و هر امضایی در صورت داشتن شرایط، علی‌الاصول معتبر خواهد بود.

در گزارش سازمان ملل متحد درباره تجارت الکترونیکی و توسعه تصویب قوانین و مقررات مناسب، از جمله درباره امضای الکترونیکی، شرط انجام و اعتبار معاملات الکترونیکی محسوب شده است. پذیرش امضای الکترونیکی دارای دو فایده مهم تمایل تجار به تجارت الکترونیکی و افزایش اطمینان به عنوان شرط لازم برای انجام معاملات الکترونیکی خواهد بود. و همین فواید آنسیترال را به تصویب قانون نمونه برای امضای الکترونیکی وادار ساخته است.

در اتحادیه اروپا، دستورالعمل اروپایی امضاهای الکترونیکی و دستورالعمل تجارت الکترونیکی را باید مبنای قانونی اعتبار امضاهای الکترونیکی دانست. این مقررات ،آمره و پیوستن دولتهای عضو اتحادیه اروپا به آنها اجباری می‌باشد. ماده ۲ دستورالعمل امضاهای الکترونیکی ضمن تعریف آن، با قید چهار شرط انتساب قطعی به امضا کننده، امکان تشخیص هویت وی از طریق امضا، کنترل امضا کننده بر آن و همسانی امضا و متن، «امضای الکترونیکی پیشرفته»را محقق دانسته است. در دستورالعمل تجارت الکترونیکی، ماده (۱۹) واژه‌های «مکتوب» و «امضا» را به طور کامل تشریح نمی‌کند. به موجب این بند، «دولت‌های عضو باید تضمین نمایند که انعقاد قرارداد الکترونیکی در نظام حقوقی آنها مجاز باشد. دولتهای عضو به‌ویژه باید تضمین دهند که مقررات مجری بر قراردادها، در استفاده از قراردادهای الکترونیکی منعی ایجاد نکرده و منجر به فقدان اثر یا اعتبار حقوقی این قراردادها بر مبنای تشکیل آنها با وسایل الکترونیکی نشود».

به طور ضمنی از ماده ۹ دستورالعمل چنین استنباط می‌شود که دولتهای عضو مجاز نیستند تا استفاده از نوشته قلم و کاغذی را برای تشکیل قراردادها اجباری نمایند. البته چنانچه گفته شد، استثنائاتی بر این اصل وارد شده است. ماده ۹ از این نظر که دولتهای عضو را از تحمیل الزامات علمی و فنی خاص به عنوان شرایط شکلی امضا منع نمی‌کند، دارای اشکال می‌باشد. بنابراین بعید نیست که برخی از دولتهای عضو اتحادیه اروپا فقط امضاهای الکترونیکی از نوع مشخص را قابل قبول بدانند؛ این در

حالی است که کشورهای دیگر به تبعیت از یوتا و قانون نمونه آنسیترال دیدگاه موسعی در این مورد خواهند داشت. اتخاذ تدابیر گوناگون در کشورهای اروپایی در این زمینه محتمل و نتیجتاً مانع از هماهنگی حقوق این کشورها به عنوان هدف غایی خواهد بود.

مطالعه تطبیقی جایگاه امضای الکترونیکی

این بررسی از آن جهت ضرورت دارد که بیانگر پذیرش امضای الکترونیکی در اکثر کشورها و تمایل به توسعه، ایمنی و اعتبار بخشیدن به آن می‌باشد. برای رعایت اختصار به ترتیب اسناد و مقررات بین‌المللی، حقوق آمریکا، کانادا، فرانسه و ایران مطالعه شده و از پرداختن به حقوق دیگر کشورها خودداری می‌شود.

حقوق آمریکا

اخیراً در ایالات متحده، امضای الکترونیکی همانند امضای سنتی الزام‌آور شناخته شده است. با این‌حال قانون به چگونگی تحقق آن اشاره نکرده یا حداقل احتیاطاتی که برای اعتبار و ایمنی فرایند امضا لازم می‌باشد، به‌دقت بررسی نشده‌اند. از بعد تاریخی، اولین قانون درباره امضای دیجیتالی به سال ۱۹۹۶ در ایالت یوتای آمریکا به تصویب رسید. در سطح فدرال، قانون امضاهای الکترونیکی در تجارت داخلی و بین‌المللی در ۳۰ ژوئن ۲۰۰۰ تصویب شده و از اول اکتبر همان سال قابلیت اجرایی یافت. این قانون راهبردی به امضای الکترونیکی اعتبار می‌بخشد. قانون مذکور حقوق و رویه قضایی ۵۰ ایالت آمریکا را از پذیرش امضای مکتوب به عنوان قاعده آمره به قبول امضای الکترونیکی و به‌رسمیت شناختن آن در کلیه دعاوی و محاکم تعدیل نموده است.

ماده (۱) (الف) ۱۰۱ مقرر می‌دارد، امضا، قرارداد یا هر مدرک دیگری مربوط به معاملات الکترونیکی را نمی‌توان با استناد به هیچ قانون، رویه یا قاعده حقوقی به صرف شکل الکترونیکی آن بی‌اعتبار دانست. قانون متحدالشکل معاملات الکترونیکی (یوتا) مصوب ۱۹۹۹ نیز تصریح دارد که اگر بر طبق قانون، امضای قراردادی الزامی باشد، این شرط شکلی می‌تواند با وسایل الکترونیکی که مجهز به فناوری تولید امضا هستند، محقق شود؛ مشروط بر اینکه قصد امضا محرز باشد. البته یوتا امکان امضای دیجیتالی وصیت‌نامه و قراردادهای امانی را به موجب بخش (۱) (ب) ۳ از این عموم خارج و غیر ممکن دانسته است. از حیث

قایل شدن اعتبار برای امضاهای الکترونیکی انجام شده در خارج از ایالات متحده، E-Sign در بخش (ح) ۱۰۱ به این امر پاسخ مثبت می‌دهد.

به لحاظ ماهوی، یوتا با طرح بحث «قصد امضا» به عنوان شرط اعتبار آن، گامی بلند در مقایسه با دستورالعمل تجارت الکترونیکی، دستورالعمل امضاهای الکترونیکی اروپا و قوانین نمونه آنسیترال برداشته است. دلیل این امر تفسیر موسع قانون متحدالشکل تجاری از مفهوم امضا می‌باشد؛ به گونه‌ای که حروف‌چینی ماشینی و شیوه علامت‌گذاری را که امکان دارد به اندازه امضاهای دستی قابل اعتماد نباشد، در بر می‌گیرد. نکته مهم دیگر در یوتا این است که شرکتها و موسسات را مجاز ساخته تا با توجه به اوضاع و احوال، تصدیق یا ثبت امضاهای الکترونیکی را شرط پذیرش آن بدانند. اعطای این اختیار به‌ویژه از لحاظ کاهش مخاطرات تجاری دارای اهمیت فوق‌العاده‌ای می‌باشد.

حقوق کانادا

در جهت پیوستن به ساختار جهانی تجارت به شیوه الکترونیکی، کنفرانس یکنواخت سازی قوانین کانادا در ۳۰ سپتامبر ۱۹۹۹، به تقلید از قانون نمونه (۱۹۹۶) قانون متحدالشکل تجارت الکترونیکی (یوکا) را تصویب کرد. قانون مذکور در اکثر ایالات کانادا با اصلاحات اندکی مورد پذیرش قرار گرفته است. البته ایالت کِبِک، قانونی با عنوان «قانونی در پایه‌ریزی چهارچوب حقوقی برای فناوری اطلاعات» تصویب کرده که بسیار کاملتر از یوکا می‌باشد.

اگرچه از آن جهت که مقنن، بی‌نظیر، مطمئن و ایمن بودن را از شرایط امضای دستی به شمار نیاورده و از این لحاظ، علی‌الاصول نباید قید و بند خاصی را به امضاهای الکترونیکی تحمیل کرد. با این وجود یوکا تصریح دارد که در برخی از موارد، از جمله به موجب مقررات، ممکن است تصریح شود که امضاهای الکترونیکی باید قابلیت‌های خاصی داشته باشند تا معتبر شناخته شوند. بند ب ماده ۸ یوکا به‌نوعی این قید را خاطر نشان می‌سازد.

بر خلاف یوکا، در کانادا برخی از قوانین خاص راجع به تجارت الکترونیکی مقرر می‌دارند که امضاهای دیجیتالی تنها در صورتی که با فناوریهای خاص ایجاد یا دارای اوصاف مشخصی باشند، معتبرند و اغلب داده‌پیامها و مدارکی که استانداردهای خاصی را از حیث امضا داشته باشند، قابل استناد می‌دانند. چهره‌ای از این طرز تفکر را می‌توان در «قانون حمایت از اطلاعات شخصی و مدارک الکترونیکی»، مصوب

۲۰۰۰مشاهده نمود که استفاده از «امضای الکترونیکی مطمئن» را الزامی می‌داند. در بخش ۴۸ قانون مذکور شرایطی برای امضای مذکور بیان شده است. یوکا، معالاسف، همانند اکثر اسناد موجود در سطح جهانی از ادله و چگونگی اثبات صحت امضاهای الکترونیکی، حمایت حقوقی و قضایی از شخص دارای حسن‌نیت و اعتماد کننده به امضای الکترونیکی و نحوه گواهی امضا و مدرک الکترونیکی، سخنی به میان نمی‌آورد. بنابراین شاید بتوان به طرفین حق داد تا در روابط تجاری الکترونیکی خویش قید و بندهایی برای پذیرش امضای الکترونیکی پیش‌بینی کرده و آن را به اطلاق قبول نکنند.

حقوق فرانسه

در ۱۳ مارس ۲۰۰۰، پارلمان فرانسه، قانونی را برای پذیرش امضای الکترونیکی تصویب و از طریق آن مفهوم امضای الکترونیکی را وارد قانون مدنی فرانسه (ق.م.ف) کرد. این قانون به‌سرعت قابلیت اجرایی یافت. علاوه بر آن، دستورالعمل امضاهای الکترونیکی اروپا در فرانسه به تصویب رسیده است. ماده ۱۳۱۶ ق.م.ف به موجب اصلاحات مذکور بیشتر به قواعد ماهوی امضای الکترونیکی می‌پردازد. به موجب بند ۳ این ماده «.. با اثبات صدور امضا از سوی شخص معین، قرارداد (توافق) دارای ارزش و اعتبار مساوی با معادل کاغذی آن خواهد بود»(بند ۳ ماده ۱۳۱۶) علاوه بر تشخیص هویت امضا کننده، امضای معتبر بیانگر تنفیذ مدرک از سوی شخص اخیر و اثبات‌گر دخالت ارادی او در تنظیم محتوای سند است (بند ۴ ماده ۱۳۱۶) بند اخیر تصریح دارد که امضا، اعلام قصد شخص بر التزام به قرارداد به‌شمار می‌آید.

نکته مهم امکان انتساب امضا به شخص و فعل ارادی امضا کننده به هنگام قبول تعهد است، بنابراین با لحاظ بند ۴ ماده ۱۳۱۶ ق.م.ف چنین فرض می‌شود که امضا شرایط فنی و قانونی مقرر در مقررات خاص را دارا بوده و اثبات خلاف این امر، علی‌الاصول بر دوش امضا کننده (مدعی) نهاده می‌شود. باید یادآوری نمود که در فرانسه هنوز پذیرش امضای الکترونیکی در پاره‌ای موارد با محدودیتهایی روبروست. برای مثال دفاتر ثبت اسناد رسمی و ازدواج نمی‌توانند از این نوع امضا استفاده کنند. با این وجود امضای الکترونیکی در قراردادهای خصوصی همواره قابل استفاده خواهد بود.

حقوق ایران

در حقوق ایران می‌توان از مقررات قانون اسناد و املاک، قانون مدنی و قانون آئین دادرسی مدنی در استنباط احکام مربوط به «امضای دیجیتالی» استفاده نمود. البته قبل از هر چیز باید این امر بررسی شود که آیا این امضاها، اساساً مورد قبول قانونگذار ایرانی قرار گرفته‌اند یا نه. زیرا، اعمال مقرراتی که با وجود ارتباط به اسناد و مدارک و امضای ذیل آنها، هیچ اشاره‌ای به مدارک و امضای الکترونیکی نکرده‌اند، بر امضا و مدارک الکترونیکی نیازمند دلیل است. قانون مهمی که می‌توان قواعدی را درباره امضا و مدارک الکترونیکی از آن استنباط نمود، قانون تجارت الکترونیکی می‌باشد.

این قانون ـ به‌ویژه در آن قسمت که به امضای الکترونیکی ارتباط دارد ـ تا حدود زیادی با تقلید از دو قانون نمونه آنسیترال (۱۹۹۶ و ۲۰۰۱) به تصویب رسیده است. امضای الکترونیکی در بند (ی) ماده ۲ و «امضای الکترونیکی مطمئن» در بند (ک) همان ماده تعریف شده، که در گفتار اول به بررسی این بند و تعاریف پرداخته‌ایم. از این جهت که امضای دیجیتالی ـ همانند امضای دستی ـ وجود سند و مدارکی را متبادر می‌سازد و بدون آن فاقد هر گونه اثر حقوقی است و به این دلیل که امضای دیجیتالی را تنها می‌توان بر روی مدارک الکترونیکی ـ و نه کاغذی ـ انجام داد، ضرورت دارد که مفهوم «مدارک الکترونیکی» بررسی شود.

قانون تجارت الکترونیک تعریفی از «مدرک الکترونیکی»به دست نمی‌دهد و تنها در بند (الف) ماده ۲ در تعریف «داده‌پیام» چنین مقرر می‌دارد: «هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فناوری جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود». بدون آنکه بخواهیم وارد بحث مدرک الکترونیکی شویم، باید افزود که ق.ت.ا همواره از ایمنی و اطمینان سیستم‌های اطلاعاتی و رایانه‌ای سخن به میان می‌آورد. این تصریح فی‌نفسه دارای اهمیت است . زیرا بدون ایمنی و اطمینان، داده‌پیام و امضای الکترونیکی از هر نظر فاقد اعتبار خواهد بود. بنابراین، چنانچه قانون مذکور نیز به حق تصریح دارد، قابلیت پذیرش مدارک الکترونیکی و به تبع آن امضای دیجیتالی نیازمند وجود رکن اساسی «اطمینان و ایمنی» می‌باشد. به همین دلیل است که ق.ت.ا از موجودیت کامل و بدون تغییر داده‌پیام به مفهوم عدم خدشه به تمامیت داده‌پیام در جریان اعمال تصدی سیستم از قبیل ارسال، ذخیره یا نمایش اطلاعات، سخن به میان می‌آورد (بند هـ ماده ۲) یا در بندهای (ح) و (ط) به‌ترتیب «سیستم‌های اطلاعاتی ایمن» و «رویه ایمن»را تعریف می‌کند؛ اگرچه، شایسته‌تر آن بود که این مفاهیم مهم از بحث صِرف تعریف خارج و به طور ماهوی بررسی می‌گردید.

بنابر آنچه گفته شد، داشتن «امضا و سابقه الکترونیکی مطمئن» مذکور در مواد ۱۰ و ۱۱ ق.ت.ا نیازمند وجود تمام شرایط و ارکان فوق‌الذکر می‌باشد. ق.ت.ا در بیان شرایط امضای الکترونیکی مطمئن چنین مقرر می‌دارد: «..الف. نسبت به امضا کننده منحصر به فرد باشد.

ب. هویت امضا کننده داده‌پیام را معلوم نماید.

ج. به وسیله امضا کننده و یا تحت اراده انحصاری وی صادر شده باشد.

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

چنانچه در گفتار بعد خواهیم دید، قانون تجارت الکترونیکی در مواد ۱۶ــ۱۲ در مقام بیان «پذیرش ارزش اثباتی و آثار سابقه و امضای الکترونیکی مطمئن» بسیار فراتر از آنچه که فی‌الواقع باید می‌بود، برای این موارد ارزش اثباتی قایل و دچار همان اشتباه و افراطی شده که مطابق نظر انجمن ملی دفاتر اسناد رسمی ایالات متحده، در قوانین راجع به امضای دیجیتالی اکثر ایالات این کشور، مصادیق متعدد دیده می‌شود.

۳ مشکلات حقوقی و عملی ناشی از ظهور سیستم دیجیتالی امضا

متاسفانه، اساسی‌ترین مشکل حقوقی و عملی استفاده از امضای دیجیتالی برای تصدیق مدارک الکترونیکی مربوط به انواع مختلف معاملات و وقایع، ناشی از همین قوانین و مقررات است. تدوین کنندگان قوانین راجع به تجارت الکترونیکی و امضای دیجیتالی، این اصل مهم را فراموش کرده‌اند که صدور هر نوع «گواهی» و «تصدیق» امضایی که تایید آن به مفهوم پذیرش محتوای اسناد است، نیازمند مشاوره با سازمان یا نهادهای تخصصی راجع به ثبت اسناد، گواهی امضا و تصدیق مدارک می‌باشد.

قانونگذاری خودسرانه و توجه به ابعاد علمی و فنی تجارت الکترونیکی بدون نگاه به جنبه‌های شکلی و قواعد ماهوی ادله اثبات دعوی با این اشکال اساسی روبروست که نمی‌توان با پیش‌بینی کلیه ضوابط علمی و ایمن‌سازی سیستم‌های رایانه‌ای و اطلاعاتی، عدم خدشه و نفوذناپذیری امضا و مدارک الکترونیکی تضمین نمود: هر روز روش نوینی در دانش الکترونیک و رایانه پدیدار می‌شود و چه بسا قبل از احاطه و ضابطه‌مند نمودن آن توسط قانون‌نویسان، هکرها، سارقان حرفه‌ای و کلاهبرداری اینترنتی دست یافته و بساط «بی‌اعتمادی» را که مهمترین مانع در راه گسترش تجارت الکترونیکی به شمار می‌آید، بگسترند.

اشکال مهم دیگر قانونگذاری غیر تخصصی ـ حداقل در زمینه امضا و سابقه الکترونیکی ـ این است که معلوم نیست بار سنگین اثبات مسایل عمده و متنوعی که در جریان تولید، ارسال، دریافت، افشا و استفاده و

سوءاستفاده از امضا و سابقه الکترنیکی ناشی می‌شود را بر دوش چه کسی می‌نهد. قانون تجارت الکترونیکی از این حیث سرآمد مقررات موجود در سطح کشورها محسوب می‌شود. ادعای عدم امکان انکار و تردید نسبت به داده‌پیام مطمئن و سوابق الکترونیکی مطمئن در ماده ۱۵ و ارایه راه‌حل منحصر «ادعای جعلیت» یا «بی‌اعتباری قانونی» آنها در واقع مقایسه این مدارک با اسناد رسمی و تکرار محتوای ماده ۱۲۹۲ ق.م ـ که اختصاص به اسناد رسمی دارد ـ نقض تمام اصول و قواعد موجود در خصوص اسناد رسمی به شمار می‌آید؛ زیرا هیچ مرجع رسمی مسوولیت ارایه، بازرسی و کنترل این دسته از خدمات را بر عهده نگرفته است.

ماده ۳۱ ق.ت.ا در باب دفاتر خدمات صدور گواهی الکترونیکی نیز نمی‌تواند مستمسکی برای توجیه این اشتباه بزرگ باشد، چرا که، اولاً: صراحت ماده حکایت از آن دارد که دفاتر مذکور تنها برای ارایه خدمات صدور امضای الکترونیکی تاسیس می‌شوند و ثانیاً: عدم استفاده از خدمات این دفاتر، به دلیل عدم تصریح قانون و اینکه ماده مذکور بعد از مواد ۱۲ـ ۱۶ ق.ت.ا و در باب جداگانه‌ای آمده است، مانع از پذیرش مدارک و امضای الکترونیکی به آن وسعت که مواد اخیر مقرر می‌دارند، نخواهد بود.

بنابراین بحران غیر منتظره، به مفهوم آثار منفی ناشی از تصور عدم نیاز به مراجعه به سردفتر اسناد رسمی یا هر مقام ذیصلاح قانونی برای گواهی و تصدیق مدارک الکترونیکی ـ آن گونه که مدنظر انجمن ملی دفاتر اسناد رسمی آمریکا بوده ـ در کشور ما نیز در حال وقوع است و باید هر چه سریعتر چاره‌ای اندیشید. در ادامه این گفتار با تبیین مشکلات و چالش‌های ناشی از پیدایش امضای الکترونیکی، به ارایه راهکار در این زمینه نیز خواهیم پرداخت.

نقض حقوق مصرف کننده

قانون تجارت الکترونیکی مقررات بالنسبه قابل توجهی (مواد ۲۳ تا ۴۹) را به «حمایت از مصرف کننده» اختصاص داده است. در بند ب ماده ۳۳ از لزوم مشخص شدن هویت تامین کننده سخن به میان آمده و تشریفات دیگر در ماده مذکور و دیگر مواد برای شفافیت رابطه و جلوگیری از تقلب و کلاهبرداری ذکر شده، با این حال هیچ تضمینی برای تحقق آنها مد نظر نبوده است. وفقط مقرر شده است که «اطلاعات اعلامی و تاییدیه اطلاعات اعلامی به مصرف کننده باید در واسطی بادوام، روشن و صریح بوده و در زمان

مناسب و با وسایل مناسب ارتباطی در مدت معین و بر اساس لـزوم حـسن نیـت در معـاملات و از جملـه ضرورت رعایت افراد ناتوان و کودکان ارایه شود»[1]. حال آنکـه ارایـه اطلاعـات در واسـطی بـادوام، هماننـد دیسک، فلاپی و.. مانع از کلاهبرداری و تقلب نخواهد بود[2].

مساله از جنبه دیگر نیز قابل بررسی است:

امضای دیجیتالی مصرف کننده نباید در معرض نفوذ و سوء استفاده دیگران باشـد، اشـخاص ضـعیف و کم‌توان باید قبل از معامله الکترونیکی از هر نظر توجیه شده و نسبت به ابعاد معامله اطلاع یابنـد و همـین مسایل ضرورت ثبت حداقل امضای طرف مقابل را به عنوان شخصی که مدام در عرصه تجارت فعال اسـت، نزد سردفتر قابل اعتماد توجیه می‌نماید.

اصول حاکم

در زمینه ثبت امضای الکترونیکی، در وهله اول، سه اصل مهم را باید مدنظر قرار داد:

اصل۱ . استفاده از تجربه ارزشمند سایر کشورها و رویه عملی شکل گرفته در دفاتر ثبت اسـناد آنهـا از جهت کاهش هزینه مطالعاتی و اجرایی ثبت الکترونیکی، امری است کـه بایـد ـ البتـه بـا رعایـت ضـوابط، معیارها و اوصاف خاص سیستم ثبتی کشور ـ آن را پذیرفت. در این راستا، بررسی و پژوهش عمیـق مـورد نیاز است و ترجمه صرف قوانین و مقررات داخلی دیگر کشورها عامل همان مشکلاتی خواهـد بـود کـه در برخی از قوانین داخلی ملاحظه می‌شود.

اصل۲. بحث از ثبت الکترونیکی، اگرچه بسیار جدید می‌باشد، به گونه‌ای که عملاً نمـی‌تـوان سـابقه‌ای بیش از ۵ سال برای آن تصور نمود؛ با این‌حال به هیچ وجه نباید آن را ناقض اصـول و قواعـد ثبتـی ایجـاد شده در طول سالهای مختلف دانست. در مقدمه توجیهی قانون نمونه دفاتر اسناد رسمی آمریکا نیز تاکیـد شده که، «اگرچه فناوری در حال تحول و تکامل است، اما متاسـفانه ماهیـت انـسانهایی کـه آن را بـه کـار می‌گیرند، چنین نیست. هر آئینی ـ خواه کاغذی یا الکترونیکی ـ برای ثبت اسناد و امضا، مـستلزم حـضور فیزیکی امضا کننده در یک دفترخانه اسناد رسمی واجد شرایط و صالح است. بر خلاف تصور عمـوم، ثبـت الکترونیکی نباید به عنوان عامل «ریشه‌کنی» ثبت رسمی (در حوزه تجارت الکترونیکی) محـسوب گـردد».

[1] . ماده ۳۵قانون تجارت الکترونیکی
[2] . ماده ۲قانون تجارت الکترونیکی بند ق

بر همین اساس در مقدمه مذکور تصریح شده که تمامی تعاریف و اصطلاحات مقرر در قانون در هر دو نوع ثبت کاغذی و الکترونیکی به کار گرفته خواهد شد کـه شـامل تـصدیق و گـواهی، امـضا، شـهادت و تمـام مفاهیم تخصصی مربوط می‌باشد.

در حقوق کشورمان، تمام اصول و قواعد مربوط به تشریفات ثبت امضا، ارزش اثبـاتی آن و.. مـذکور در قوانین ثبت اسناد و املاک، قانون دفاتر اسناد رسمی، آئین دادرسی مدنی، قانون مدنی و سـایر مقـررات در مورد امضای الکترونیکی نیز اجرا خواهد شد. لذا هر قانون و رویه‌ای برای ثبت الکترونیکی در آینده باید بـا مبنا قرار دادن این اصل شکل گیرد.

اصل ۳ . در مورد امضای الکترونیکی، ترجیح هر یک از فناوریهای ایجاد امضا، بدون لحاظ جنبه ایمنـی و اطمینان آن، از هر نظر بی‌اعتبار است: دفاتر ثبت الکترونیکی باید در صورت احراز صدور و ایجـاد امـضا و کلید خصوصی به نام متقاضی، نسبت به ثبت و طی تشریفات لازم اقدام نمایند. علی‌الاصـول نمـی‌تـوان بـا توصیف فناوری خاص به عنوان شیوه مقبول در ایجاد و رمزگذاری خاص، به نفع شرکت یـا شـخص مالـک آن تبلیغ نمود و باید در مقام پذیرش یا رد امضا کیفیت و ضوابط علمی و فنی را لحاظ کرد.

تشریفات ثبت امضای الکترونیکی

چنانچه گفته شد، اعمال تشریفات ثبت امضای الکترونیکی نیازمند استقرار دفاتر ثبت الکترونیکی می‌باشد. این دفاتر باید در ثبـت امـضای الکترونیکـی ضـوابطی را رعایـت نماینـد کـه بـه اختـصار ذکـر مـی‌شـود.

۱. حضور شخص امضا کننده و تشخیص هویت او از سوی سردفتر. در این مورد قبلاً توضیح داده شد. عدم تصریح مستقیم به این شرط به عنوان رکن امکان صدور تصدیق امضا بیشتر ناشی از آن است که گـویی از نظر قانونگذار این شرط به قدری بدیهی بوده که ذکر آن غیر لازم و فقدان آن (عدم حـضور شـخص امـضا کننده نزد سردفتر برای تصدیق امضا) موجب بی‌اعتباری چنین تصدیقی بوده است. فقط باید ایـن نکتـه را افزود که حضور وی برای امضای اسناد و مدارک الکترونیکی نیست، چرا که فـرض بـر ایـن مـی‌باشـد کـه امضای مذکور یک‌بار توسط او در «دفتر صدور امضای الکترونیکی» ایجاد شده اسـت. حـضور امـضا کننـده برای این است که امضای مذکور ثبت شده و صحت صدور آن از سوی درخواست کننده ثبت از این طریـق قابل اثبات باشد.

در مورد این بند، دو ایراد قابل تصور است که ضمن طرح به پاسخ آن نیز می‌پردازیم:

الف . اگر فناوری ارتباط تا اندازه‌ای پیشرفته باشد که نیازی به حضور امضا کننده نزد سردفتر وجود نداشته باشد، آیا می‌توان باز هم او را اجبار به حضور نمود؟ به عبارت دیگر، اصل مذکور قابل تخصیص می‌باشد یا نه؟در پاسخ باید گفت که اگرچه این نوع از فناوری هم‌اکنون موجود نیست؛ اما در صورت تحقق آن نیازی به حضور امضا کننده در دفتر ثبت الکترونیکی نخواهد بود و سردفتر ضمن ارتباط دیداری ـ شنیداری زنده با امضا کننده الکترونیکی، هویت او را تشخیص خواهد داد.

ب. دوگانگی «مرجع ایجاد امضای دیجیتالی» و «مرجع ثبت امضای الکترونیکی» بدعتی جدید است و می‌توان به راحتی این دو را در یک سازمان متمرکز ساخت. در پاسخ، ضمن منتفی ندانستن این تدبیر، باید توضیح داد که دو کارکرد فوق از لحاظ فنی با هم تفاوت بسیار دارند؛ به گونه‌ای که ایجاد، نگهداری و به‌روز رسانی امضای الکترونیکی بحثی است متعلق به علم الکترونیک و رایانه، حال آنکه ثبت آن ـ به لحاظ ضرورت رعایت اصول و قواعد مقبول حقوق و رویه ثبتی ـ جنبه حقوقی دارد. البته دایر کردن دفاتر صدور امضای الکترونیکی و ثبت الکترونیکی در کنار هم راه آسانی برای حل این مشکل خواهد بود. حتی امکان ادغام این دو نهاد نیز وجود دارد، بدین صورت که برای مثال سردفتر حقوقدان بوده و دفتریار از میان متخصصین نرم‌افزار انتخاب شود و هر دو کار در یک دفتر انجام گیرد.

۲ بررسی صلاحیت مرجع صدور امضا. شخص ثالث و مورد اعتمادی که داده مربوط به امضای ایجاد شده برای افراد را در اختیار دارد، ممکن است در آینده قابل اعتماد نبوده و یا اطلاعات لازم برای تصدیق امضا همانند داده مربوطه امکان دارد که در آینده در دسترس نباشد. بنابراین دفتر ثبت الکترونیکی باید احتیاط متعارف را به عمل آورده و اطمینان یابد که نرم‌افزار مورد استفاده برای ایجاد امضای دیجیتالی به‌روز بوده و به هنگام تقاضای تصدیق / ثبت امضا از سوی متقاضی از اعتبار نیفتاده باشد[۱]. لذا دفتر ثبت الکترونیکی در این زمینه باید دو نکته مهم را بررسی نماید:

۱ کلیدها/ رمزهایی که برای ایجاد امضا به کار می‌روند، باید تنها برای مدت مشخصی دارای اعتبار باشند تا از این طریق از افشای آنها به دلیل گذشت زمان و تغییر استانداردهای رمزگذاری یا سایر خطرات جلوگیری شود. رویه معمول در مراکز ایجاد امضا، تعیین طول عمریک یا حداکثر دوساله و مبتنی بر ۱۰۲۴ بیت [Bit] داده از نوع کلید آر.اِس.اِی می‌باشد.

[۱] . قانون نمونه دفاتر اسناد رسمی آمریکا بند۲تا۱۶

۲ مرجعی که امضا را صادر (ایجاد) می‌کند، باید فی‌الواقع موجود باشد: دفتر ثبت الکترونیکی، بی‌نیاز از این نوع مراکز نخواهد بود و به نظر می‌رسد که بتوان «دفاتر خدمات صدور گواهی الکترونیکی» را با مقداری تعدیل و شفافیت از حیث وظایف و مسوولیتها برای انجام این امور مهیا کرد. به منظور تشخیص صلاحیت مرجع صدور امضا، باید مراجع (دفاتر) مشخصی برای این امر ـ به موجب قانون و تحت نظارت سازمان مشخص ـ تاسیس و از حیث رعایت اصول علمی و قوانین و مقررات مورد بازرسی و نظارت قرار گیرند. تعدیل ماده ۱۳ ق.ت.ا، از آن جهت ضروریست که حوزه عملکرد دفاتر خدمات صدور گواهی الکترونیکی را بسیار موسع تعیین کرده که این امر چنانچه بررسی شد، منجر به مشکلات عمده‌ای از جمله مداخله در اموری می‌شود که در صلاحیت دفاتر اسناد رسمی قرار دارد. بنابراین دفاتر خدمات صدور گواهی الکترونیکی را باید به عنوان دفاتر صدور امضا معرفی کرد و بر این اساس وظایف آنها را، فقط در «تولید، صدور، ذخیره، ارسال، ابطال و به‌روز نگهداری امضاهای الکترونیکی» که ق.ت.ا نیز بیان داشته، منحصر نمود.

دفاتر صدور امضا به شرح فوق، حق تایید گواهی‌های صادره از سوی خود را ندارند و این مورد از جمله مسایلی است که در حوزه صلاحیت دفاتر اسناد رسمی قرار می‌گیرد. همچنین دفتر صدور امضا باید در صورت صلاحدید فنی (از جمله افشای کلید خصوصی، تقاضای دارنده امضا و..) اقدام به ابطال امضای دیجیتالی ایجاد شده نمایند. با توجه به امکان ابطال امضا از سوی مرجع اخیر، سردفتر باید قبل از ثبت و تصدیق امضای الکترونیکی، از نزدیکترین دفتر صدور امضا (که به صورت شبکه‌ای با سایر دفاتر صدور امضا از حیث اطلاعات به‌روز در ارتباط می‌باشد)، نسبت به استعلام لازم از حیث تعلق امضا به متقاضی و ابطال یا عدم ابطال آن به عمل آورد.

۳. بررسی سلامت عقلانی، داشتن سمت و آزادی اراده متقاضی ثبت امضا. متقاضی ثبت (تصدیق) امضا، در واقع می‌خواهد تا از امضای ایجاد شده به شرح مذکور در بند فوق، برای پذیرش محتوای مدرک الکترونیکی استفاده نماید: این امر به مفهوم متعهد شدن وی به محتوای آن سند است و لذا باید همانند اسناد کاغذی قصد انجام عمل حقوقی در فرد متقاضی احراز شود. در قانون ثبت[۱]، از جمله برای ثبت سند قبل از احراز «هویت اصحاب معامله» مجازات اداری از یک تا سه سال انفصال از خدمات دولتی پیش‌بینی شده که اعمال آن در مورد ثبت امضای الکترونیکی نیز منتفی نخواهد بود.

[۱] . ماده ۱۰۲ قانون ثبت اسنا د واملاک

نتیجه‌گیری

در صورت تحقق تجارت الکترونیکی، بحث ایمنی از یک سو و مدل ساختن دعاوی از سوی دیگر مطرح خواهد بود. در بخش اول ایجاد و ثبت امضای دیجیتالی و در سوی دوم ثبت الکترونیکی اسناد و مدارک الکترونیکی راهگشای بسیاری از مشکلات قابل تصور در این عرصه می‌باشد. در مورد ثبت الکترونیکی امضا و مدارک، نکته مهم «اعتماد» به سردفتر و تلاش در جهت رسیدن به استانداردهای روز پیشرفت می‌باشد. مورد اخیر آنقدر اهمیت دارد که بدون آن نمی‌توان امکان ثبت الکترونیکی کارآمد و اصولی را تصور نمود.

هر اقدامی در واگذاری ثبت به شرح فوق به سازمان جدید و یا اشخاصی که هیچ تخصصی در امور ثبتی ندارند، به دلیل ناآشنایی آنها به اصول و قواعد ثبت محکوم به شکست خواهد بود: ثبت امضا و مدارک الکترونیکی از همان قواعد و اصولی تبعیت می‌کند که در مورد سایر اسناد و امضاها (کاغذی و دستی) جاریست و بر خلاف نظر عده‌ای، نمی‌توان تحولات فناوری را مستمسک نقض اصول و قواعد قرار داد. قبل از هر چیز باید با تصویب قانون مناسب «ثبت الکترونیکی» را به رسمیت شناخت و تعدادی از دفاتر اسناد رسمی موجود را بعد از آموزشهای لازم به این امر اختصاص داد. امکان ثبت به هر دو شیوه الکترونیکی و کاغذی در این دفاتر بهترین دلیل برای عدم عدول از اصول و قواعد موجود می‌باشد. دفتر ثبت الکترونیکی در عین اینکه می‌تواند امضای دیجیتالی را ثبت و از سند ثبتی پشتوانه الکترونیکی تهیه کند؛ قادر خواهد بود که به امور روزمره و عادی خود نیز پرداخته و برای مثال معاملات ملکی را نیز ثبت نماید.

این ادعا که پذیرش ایجاد مراکز صدور امضا و ثبت الکترونیکی، به طور جداگانه منجر به تشریفاتی و پیچیده‌تر شدن معاملات الکترونیکی و در نتیجه عدم گرایش به آن می‌شود نیز، محکوم به بی‌اعتباریست. نمی‌توان برای رسیدن به سرعت و ارزانی مشکلات عمده‌ای را از حیث تقلب، کلاهبرداری و سوء استفاده در فضای مجازی ایجاد نموده و اثبات مسایل را سخت کرد. در عین حال با وضع مقررات دقیق این امکان وجود دارد که صدور و ثبت امضای الکترونیکی در یک مرجع (دفتر) و در حداقل زمان ممکن انجام شود. ایجاد تعادل میان فلسفه گسترش تجارت الکترونیکی و ایمنی و

اطمینان آن بهترین گزینه است که با ثبت الکترونیکی امضا و مدارک به‌راحتی می‌توان بدان دست یافت.

منابع:

http://www.hamshahri.net

http://www.isna.ir

http://www.hamshahrionline.ir

iran-eng.com

http://www.iranbar.com

http://atalebi.com/articles/show.asp?ID=۴۴۶

http://www.iranssl.com/?tabid=۷۳

http://www.sgnec.net/Articledet-f.asp?number=۶۷

http://www.notary.ir/Magazine/Magazine۵۹/Mag۵۹۰۵.htm

http://www.verisign.com/developers/index.html

http://www.mefa.ir/newsdetail-fa-۴۸.html