

جایگاه امضای دیجیتالی در ثبت اسناد به شیوه الکترونیکی

نویسنده: مصطفی السان^۱

چکیده

در اسناد مکتوب، امضاء نشان تأیید تعهدات قبول شده در آن سند به شمار می‌آید. از آن جهت که در تجارت الکترونیکی «مدارک الکترونیکی» دارای جایگاهی همانند اسناد مکتوب هستند، لذا امضا در این مدارک نیز علی‌الاصول دارای همان ارزش اثباتی می‌باشد. در این مقاله، با تکیه بر تجربه کشورهای پیشرفته و مطالعه در قوانین و مقررات به این مساله پرداخته می‌شود که در ثبت الکترونیکی اسناد مدارک، چگونه 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 گواهی امضا دارای آثار زیانباری - از حیث حقوقی، اجتماعی و

۱. دانشجوی دوره دکتری حقوق خصوصی، دانشکده حقوق دانشگاه شهید بهشتی.

اقتصادی - خواهد بود و از این حیث، اساساً امضا و مدارک الکترونیکی خصوصیتی ندارند که موجب تغییر مرجع ثبت و گواهی آنها شود. واژگان کلیدی: امضای دیجیتالی، ثبت الکترونیکی، حقوق تطبیقی، قانون تجارت الکترونیکی، قانون نمونه آنسیترال و قانون نمونه دفاتر اسناد رسمی آمریکا.

مقدمه

ظهور و گسترش وسایل نوین ارتباط که ویژگی بارز آنها «سرعت» و «تنوع» روابط بود، تنها زمانی منجر به معرفی و توسعه «تجارت الکترونیکی» شد که کاملترین شیوه ارتباط الکترونیکی، یعنی «اینترنت» ابداع و معرفی گردید. اینترنت در حقیقت هر دو ویژگی سرعت و تنوع را باهم ارایه می‌نمود و از سوی دیگر موجب «ارزانی» روابط معاملاتی نیز می‌گردید. این تحولات اگرچه در مدتی کمتر از یک قرن روی داد؛ با اینحال - بنابر سنت زندگی آدمهای خوب و بد در کنار هم - همواره روابط الکترونیکی در معرض اختلال، تقلب، کلاهبرداری و اعمال خرابکارانه دیگر قرار داشت. فناوری نوظهور، دیگر با مساله «وجود» روبرو نبود، بلکه باید حیات و پذیرش خود را در دهکده جهانی «استمرار» بخشید.

بر همین اساس، بحث ایمنی و اعتماد از همان ابتدای ظهور اینترنت مطرح و موضوع بحث و تحقیق متخصصان بود. روشهای مختلف رمزگذاری^۱ و امضای دیجیتالی^۲ با همین تفکر ایجاد و گسترش یافته و بعدها در قوانین داخلی و مقررات بین‌المللی ارزیابی و مورد حمایت قرار گرفتند.

توسعه تجارت الکترونیکی، علاوه بر ایمنی، فناوری دیگری را اقتضا می‌کرد و آن - اگرچه بسیار دیرتر از شیوه‌های ایمنی مطرح گردید - ثبت الکترونیکی^۳ گواهی دیجیتالی^۱

1. Encryption.

2. Digital Signature.

3. Electronic Notarization.

امضاها و مدارک الکترونیکی بود. بحث از ثبت و گواهی الکترونیکی بعد از سال 1996 مطرح و تاکنون به طور کامل وارد رویه بین‌المللی نشده است؛ با این حال برخی از کشورها قوانین و مقرراتی برای توسعه و ضابطه‌مند کردن آن تصویب کرده‌اند.

در این مقاله ما به پیوند امضا و ثبت الکترونیکی خواهیم پرداخت. بنابراین آنچه بیشتر مبنا خواهد بود، جایگاه امضا و گواهی دیجیتالی است و این امر مورد بررسی قرار خواهد گرفت که چگونه فرایند امضا و متن الکترونیکی را می‌توان دارای آثار حقوقی همانند امضا و مدارک کاغذی / سنتی دانست. بعد از بررسی مختصر قوانین و مقررات موجود (مطالعه تطبیقی (به مسایل و مشکلات امضا و گواهی دیجیتالی نیز خواهیم پرداخت. بنابراین، مباحث مقاله در گفتارهای جداگانه به شرح زیر بررسی می‌شود.

۱. کلیات

۲. مطالعه تطبیقی جایگاه امضای دیجیتالی

۳. مشکلات حقوقی ناشی از ظهور سیستم دیجیتالی امضا

در تمام مباحث، بررسی بر مبنای مسایل راجع به ثبت و گواهی الکترونیکی خواهد بود.

۱- کلیات

اگرچه ثبت الکترونیکی، بیشتر برای ثبت معاملات الکترونیکی - به ویژه اینترنتی - به کار می‌رود؛ با این وجود این امر به مفهوم عدم امکان استفاده از آن در معاملات عادی نیست. بنابراین می‌توان از مدارک کاغذی روگرفت الکترونیکی تهیه و با رعایت تشریفات ثبت کرد. البته بدیهی است که طرفین به ندرت طی این تشریفات را می‌پذیرند و با امکان ثبت به شیوه سنتی ترجیح می‌دهند که از روشهای نوظهور احتراز نمایند. به دلیل کاربرد ثبت الکترونیکی در معاملات اینترنتی، لازم است تا مفهوم تجارت الکترونیکی، امضای دیجیتالی و ثبت الکترونیکی به اختصار تشریح شده و جایگاه امضا در سیستم

سنتی ثبت اسناد مشخص گردد.

۱ - ۱. مفهوم تجارت الکترونیکی

پیدایش «فناوری اطلاعات و ارتباطات»^۱ را باید یک انقلاب نامید که منجر به گشایش «باب جدیدی در اقتصاد»^۲ شده است. تجارت الکترونیکی یکی از مهمترین نتایج این انقلاب و از نمودهای بارز آن به شمار می‌آید و مفهوم آن به قدری پویا، در حال تحول و گسترده می‌باشد که ارایه تعریفی جامع و مختصر از آن امکان‌پذیر نیست. چنانچه قانون تجارت الکترونیکی (ق.ت.ا) مصوب ۱۳۸۲ نیز تعریفی در این مورد ارایه نکرده است. با این وجود، برخی از مؤسسات به ارایه تعریف نسبتاً گویایی در این زمینه پرداخته‌اند. سازمان تجارت جهانی^۳ در اعلامیه مورخ ۲۵ سپتامبر ۱۹۹۸ تجارت الکترونیکی، آن را چنین تعریف می‌کند:

«تولید، توزیع، بازاریابی، فروش یا تسلیم کالاها و خدمات از طریق وسایل الکترونیکی» (گزارش سازمان تجارت جهانی). این سازمان گسترش تجارت الکترونیکی را نوید بخش هزینه پایین معاملات و تولیدی، تسهیل انعقاد قراردادها و تشدید رقابت دانسته که به نوبه خود، منجر به کاهش قیمت‌ها، افزایش کیفیت و تنوع تولیدات و نهایتاً منجر به پیشرفت و رفاه بیشتر خواهد شد.^۴

کمیسیون حقوق تجارت بین‌الملل سازمان ملل متحد (آنسیترال)^۵ در تفسیر ماده ۱ قانون نمونه (۱۹۹۶)^۶ و در تشریح واژه «تجاری»، این اصطلاح را شامل معاملات راجع

1. Information Communication Technology [ICT]

2. New Economic Paradigm.

3. **E-Commerce and Development Report**, United Nations, New York & Geneva 2001.p.xvii.

4. World Trade Organization [WTO].

5. Bacchetta, M., et al. **Electronic Commerce and the Role of the WTO**, World Trade Organization Special Studies 2, Geneva: World Trade Organization, 1998.p.15.

6. United Nations Commission on International Trade Law [UNCITRAL].

7. UNCITRAL Model Law on Electronic Commerce 1996.

به تهیه، مبادله و توزیع کالا، نمایندگی تجاری، حق‌العمل کاری، اجاره، بهره‌برداری از معادن، مشاوره، مهندسی، صدور پروانه، سرمایه‌گذاری، امور مالی، بانکی، بیمه، موافقت‌نامه‌های استخراج یا واگذاری منابع، قراردادهای مشارکت و سایر مشارکت‌های صنعتی و تجاری و حل و نقل کالا یا مسافر از طریق هوا، دریا، راه‌آهن و جاده دانسته است.

بنابراین، هر عمل حقوقی که به نوعی در انجام آن از وسایل الکترونیکی ارتباط استفاده شود را باید «معامله الکترونیکی» و توسعه و استقرار این روند را منجر به «تجارت الکترونیکی» دانست. وقتی به حجم معاملات مذکور توجه نماییم، اهمیت ایمنی فضای مجازی و لزوم معرفی فناوری امضای دیجیتال و ثبت الکترونیکی مطمئن بیشتر آشکار می‌گردد.

۲ - ۱. مفهوم امضای دیجیتال

در وهله اول باید تفاوت میان امضای دیجیتال و الکترونیکی را شناخت: اگرچه به کار بردن هر کدام از این اصطلاحات به جای دیگری تعبیر بر مسامحه شده و عرفاً با ایرادی روبرو نیست.^۱ از جنبه علمی در تمایز این دو به اختصار می‌توان گفت که امضای دیجیتال نمودار داده‌ای است که به شکل یک واحد داده، الصاق یا با رمزگذاری منتقل می‌شود و به گیرنده اجازه می‌دهد تا سرمنشأ و اصالت آن را تشخیص دهد. این ساختار منطقی مانع از جعل امضا می‌شود. امضای الکترونیکی دارای معنای عام‌تری است و شامل امضای دستی‌سکن شده یا اسم شخص که در قسمت انتهایی نامه الکترونیکی قید می‌گردد، نیز می‌شود. برای تأمین ایمنی و اصالت امضای الکترونیکی باید از امضای

1. Digital Signature Guidelines, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, Information Security Committee Electronic Commerce and Information Technology Division Section of Science and Technology American Bar Association 1996. page.3.

دیجیتالی به عنوان فناوری رمزگذاری - از جمله تابع هَش^۱ - استفاده کرد.^۱ بنابراین دو نکته مهم را در رابطه با امضای الکترونیکی و دیجیتالی باید ذکر کرد:

یک. اطلاق عبارت «امضای دیجیتالی» به فرایند فوق‌الذکر ناشی از مسامحه می‌باشد؛ زیرا هیچ شباهتی بین این نوع از تأیید و «امضا» به مفهوم مصطلح آن وجود ندارد.

دو. امضای الکترونیکی به شرح فوق و با تعاریفی که در زیر می‌آید، تنها در صورتی دارای اعتبار است که با فرایند امضای دیجیتالی همراه باشد.^۲ به همین دلیل در عنوان تحقیق حاضر از عبارت «امضای دیجیتالی» استفاده شده است. لذا در هر جا که امضای الکترونیکی به کار رود نیز، باید مفهوم آن را بر همین مبنا تحلیل کرد.

تعاریف متعددی از امضای الکترونیکی ارایه شده که به ذکر برخی از آنها اکتفا می‌شود. در بند الف ماده^۲ قانون نمونه آنسیترال درباره امضاهای الکترونیکی^۴ که در ۵

۱. Hash Function [تابعی برگشت پذیر که داده وارده را به صورت یک رمز بی‌همتا درمی‌آورد. نیز اگر به عنوان امضای دیجیتالی به کار رود، موجب شناسایی قریب‌بسته و ایمنی محتوای پیام می‌گردد.]
[منبع: فرهنگ لغت Babylon]

2. Berbecaru, et al, Toward Concrete Application of Electronic Signature 2002.

۳. ماده ۱۰ قانون تجارت الکترونیکی، بحث از «امضای الکترونیکی مطمئن» را مطرح ساخته است که به نظر نمی‌رسد، راهی برای حصول این اطمینان جز از طریق رمزگذاری امضا [امضای دیجیتالی] وجود داشته باشد. به طور کلی در رویه موجود حرکت بدین سوی است که امضای الکترونیکی فاقد رمزگذاری از حیث اثباتی مورد پذیرش نباشد یا ارزش اثباتی بسیار کمتری در مقایسه با امضای دیجیتالی داشته باشد، زیرا: ۱. صدور آن از سوی هر شخص برای خود او وجود دارد. ۲. هیچ تضمینی برای اینکه امضای مذکور منحصر به فرد باشد، وجود ندارد. (برای مثال در امضای نامه الکترونیکی در سایت یا هو، هیچ وقت نمی‌توان مدعی شد که امضای مشابهی در سایت دیگر توسط شخص دیگر - مورد استفاده قرار نمی‌گیرد). ۳. امضای الکترونیکی، لزوماً خط داده به مفهوم علمی آن نیست و چنانکه بررسی شد، می‌تواند امضای دستی اسکن شده باشد؛ بدیهی است که این تدبیر با امضایی که عملاً با محاسبات دقیق علمی و ریاضی ایجاد شده متفاوت است؛ یا حداقل از لحاظ حقوقی ارزش اثباتی آن دو یکسان نیست. شاید به همین دلایل است که در قوانین اکثر کشورها و قانون نمونه (۲۰۰۱) میان امضای الکترونیکی به مفهوم عام و امضای الکترونیکی مطمئن (و به تعبیر قانون برخی از کشورها، پیشرفته: Advanced) قایل به تمایز شده‌اند.

4. UNCITRAL Model Law on Electronic Signatures 2001.

ژوئیه ۲۰۰۱ به تصویب رسیده، امضای الکترونیکی چنین تعریف شده است: «داده‌ای در شکل الکترونیکی که به یک داده‌پیام^۱ ضمیمه، یا جزء همسان، پیوسته و جدا ناپذیری از آن شده و می‌تواند برای شناسایی امضا کننده آن داده‌پیام و تأیید اطلاعات موجود در داده‌پیام از سوی امضا کننده به کار گرفته می‌شود».

در بند ۷ ماده ۱۴ قانون نمونه دفاتر اسناد رسمی^۲ ایالات متحده، امضای الکترونیکی به معنی «هر گونه صدا، علامت یا فرایند الکترونیکی است که به مدرک الکترونیکی با لحاظ شرایط علمی ضمیمه یا با آن همسان شده و این امضا از سوی شخصی که قصد پذیرش مدارک را دارد، زده شده یا به دستور و برای او طراحی شده است». تعریف مذکور، در واقع تکرار مفهومی می‌باشد که بند ۸ ماده ۲ قانون متحدالشکل معاملات الکترونیکی^۳ از امضای الکترونیکی به دست می‌دهد.

در بند (ی) ماده ۲ق.ت.ا، امضای الکترونیکی «عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به «داده‌پیام» است که برای شناسایی امضا کننده «داده‌پیام» مورد استفاده قرار می‌گیرد». بند (ک) ماده ۲ و ماده ۱۰ قانون مذکور نیز شرایطی برای «امضا و سابقه الکترونیکی مطمئن» در نظر گرفته است.

تعاریف ذکر شده از امضای الکترونیکی، تقریباً مشابهند و از آنها می‌توان استنباط کرد که امضای مذکور باید به گونه‌ای باشد که بتوان موارد زیر را از طریق آن اثبات نمود:
یک. اسناد.^۴ با امضای الکترونیکی یک سند، محتوای آن به شخص امضا کننده منتسب می‌شود و لذا له و علیه او قابل استناد است.

دو. انجام تشریفات.^۵ امضای دیجیتالی یک سند الکترونیکی حاکی از انجام تمام

1.Data Message.

2.Model Notary Act 2002.

3.Uniform Electronic Transaction Act [UETA].

4.Evidence.

5.Ceremony.

تشریفات مقرر قانونی برای تنظیم آن است.

سه . تصدیق^۱ در صورت استفاده از امضای دیجیتالی برای تأیید محتوای مدارک الکترونیکی، این نوع امضا کارکردی همانند امضا در اسناد کاغذی خواهد داشت.

چهار . داشتن آثار حقوقی. امضای الکترونیکی دارای تمام آثار حقوقی مقرر برای امضای سنتی می‌باشد. چنانچه در ماده ۷ قانون نمونه (۱۹۹۶) و ماده ۳ قانون نمونه (۲۰۰۱)، «اصل اتحاد آثار امضا و مدارک الکترونیکی و سنتی» مورد تأکید قرار گرفته است.

۳- ۱. مفهوم ثبت الکترونیکی

چنانچه گفته شد، ثبت الکترونیکی مفهومی نسبتاً نوظهور به شمار می‌آید. با توجه به همین امر و عدم اقدام به تأسیس دفاتر ثبت الکترونیکی در کشورمان، برای یافتن مفهوم این عبارت باید به حقوق و رویه کشورهای پیشگام در این زمینه مراجعه کرد. البته «دفاتر خدمات صدور گواهی الکترونیکی»^۲ در ماده ۳۱ و ۳۲ ق.ت.ا پیش‌بینی شده و می‌توان از ملاک آن برای دفاتر ثبت الکترونیکی نیز استفاده نمود. به موجب ماده ۳۱ «دفاتر خدمات صدور گواهی الکترونیکی واحدهایی هستند که برای ارائه خدمات صدور امضای الکترونیکی در کشور تأسیس می‌شوند. این خدمات شامل تولید، صدور، ذخیره، ارسال، تأیید، ابطال و به‌روز نگهداری گواهی‌های اصالت (امضای) الکترونیکی می‌باشد».

در ایالات متحده، قانون نمونه دفاتر اسناد رسمی، ماده ۳ را به بحث در مورد «دفاتر ثبت الکترونیکی» اختصاص داده است. این ماده به طور مفصل - از بخش ۱۴ تا ۲۳ - تمام مفاهیم مربوط به ثبت الکترونیکی را لحاظ نموده و اصول و قواعد حاکم بر این نهاد جدید را تشریح می‌کند. در مقدمه توجیهی (تفسیر)^۳ ماده ۳ تصریح شده که دفاتر ثبت الکترونیکی، نهادهایی جدای از دفاتر اسناد رسمی به شمار نمی‌آیند و هر سردفتری

- 1.Approval.
- 2.Certification service Provider.
- 3.Comment.

می‌تواند با گرفتن مجوز و آموزشهای لازم به یک «سردفتر الکترونیکی»^۱ تبدیل شود. البته دفاتر ثبت اسناد در اقدام به این امر هیچ الزامی ندارند.^۲

در بند ۲ بخش ۱۴ قانون مذکور، دفتر ثبت الکترونیکی چنین تعریف شده است: «دفتر ثبت اسنادی که به حکم مرجع صالح دارای قابلیت انجام امور دفاتر ثبت الکترونیکی مطابق با مقررات مربوط، شناخته می‌شود». بنابر بخش ۱۵ تنها افرادی صلاحیت افتتاح دفاتر ثبت الکترونیکی را دارند که آموزشهای لازم را دیده و در امتحان مربوطه پذیرفته شده باشند.^۳ اگرچه تفصیل این بحث از موضوع مقاله حاضر خارج است، ولی به اختصار می‌توان گفت که در اکثر ایالات آمریکا ثبت الکترونیکی شروع شده و مقرراتی برای نظام‌مند کردن آن به تصویب رسیده است. برای مثال در ایالت‌های فلوریدا، کُلرادو و یوتا قوانینی در تجویز «ثبت الکترونیکی» تصویب شده که این دفاتر از جمله به گواهی امضاهای دیجیتالی اقدام می‌کنند.^۴ در آریزونا نیز از سال ۲۰۰۲ ثبت الکترونیکی آغاز شده و قانون خاصی در این مورد تدوین یافته است.

از آن جهت که امضا، در تنظیم و ثبت اسناد دارای اهمیت زیادی است، نخست باید جایگاه آن را در نظام سنتی ثبت اسناد شناخته و سپس به مفهوم و کارکرد آن در ثبت الکترونیکی بپردازیم.

۴ - ۱. جایگاه امضا در نظام سنتی ثبت اسناد

مطابق ماده ۱۳۰۱ قانون مدنی، «امضایی که در روی نوشته یا سندی باشد بر ضرر امضا کننده دلیل است» مقنن در این ماده به یکی از مهمترین آثار امضا، یعنی دلیل بودن سند امضا شده به نفع امضا کننده توجهی نداشته است. به طور کلی «نوشته منتسب به

1. Electronic Notary.

2. The Model Notary Act, September 1, 2002. Published As A Public Service by the National Notary Association. P. 75.

3. Op cit, p. 80.

4. Leff, Laurence Lefflaurence, **Notaries and Electronic Notarization**, Western Illinois University 2002.p.3.

اشخاص در صورتی قابل استناد است که امضا شده باشد. امضا نشان تأیید اعلامیه‌های مندرج در سند 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»^۱.

اگرچه ایجاد حق و تکلیف به عنوان مهمترین اثر امضا در اکثر اسناد، مورد توجه حقوقدانان قرار نگرفته، با این حال می‌توان از ماده ۶۵ قانون ثبت اسناد و املاک (مصوب ۱۳۱۰ با اصلاحات و الحاقات بعدی) آن را استنباط کرد. به موجب این ماده، «امضای ثبت سند پس از قرائت آن به توسط طرفین معامله یا وکلای آنها دلیل بر رضایت آنها خواهد بود». از ماده مذکور استنباط می‌شود که عدم امضای سند ثبت شده از سوی شخص یا اشخاص ذینفع و یا متعهد، مفهومی جز بی‌اعتباری و فقدان هر گونه اثر حقوقی برای آن سند ندارد.

با ثبت سند و طی تشریفات امضا، «سندی که مطابق قوانین به ثبت رسیده رسمی است و تمام محتویات و امضاهای مندرج در آن معتبر خواهد بود مگر اینکه مجعولیت آن سند اثبات شود» (ماده ۷۰ ق.ث). بنابراین امضا کننده نمی‌تواند امضای خود را انکار یا در درستی محتوای سند رسمی تردید کند و فقط می‌تواند جعلیت یا بی‌اعتباری قانونی این دسته از اسناد را اثبات نماید (ماده ۱۲۹۲ ق.م).

تصدیق صحت امضا، در نظام سنتی ثبت اسناد از جمله وظایفی است که بر عهده مسؤولین دفاتر نهاده شده (بند ۳ ماده ۴۹ ق.ث) و در قانون دفاتر اسناد رسمی و کانون سردفتران و دفترباران، دفتری به نام «دفتر گواهی امضا» پیش‌بینی شده که بنابر ماده ۲۰ قانون اخیر، «دفتری است که منحصراً مخصوص تصدیق امضا ذیل نوشته‌های عادی است و نوشته تصدیق امضا شده با توجه به ماده ۳۷۵ (قانون) آئین دادرسی مدنی مسلم‌الصدور شناخته می‌شود». به نظر می‌رسد، «دفاتر خدمات صدور گواهی الکترونیکی»

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

مذکور در باب دوم قانون تجارت الکترونیکی (مواد ۳۱ و ۳۲) به این دفاتر شباهت زیادی دارند و تطبیق آنها در گفتارهای آینده خالی از فایده نخواهد بود.

۲. 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.

۱ - ۲. اسناد و مقررات بین‌المللی

بحث امضای الکترونیکی در سطح بین‌المللی، نخستین بار در ماده ۷ قانون نمونه آنسیترال درباره تجارت الکترونیکی به سال ۱۹۹۶ مطرح گردید. 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^۱ 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»^۲ 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 امضای

1. UNCITRAL Working Group on Electronic Commerce UNCITRAL model Law on Electronic Commerce With Guide to Enactment 1996.p.36.

2. Equal Treatment.

الکترونیکی ذکر شده و در مواد ۸ و ۹ وظایفی بر دوش امضا کننده^۱ و دفاتر صدور گواهی الکترونیکی نهاده شده است. ماده ۱۲ قانون مذکور نکته جالبی مطرح می‌سازد و آن «به رسمیت شناختن گواهی‌ها و امضاها الکترونیکی (صادره در) خارج»^۲ 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^۳ 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.^۴ و همین فواید آنسیترال را به تصویب قانون نمونه برای امضای الکترونیکی و ادار ساخته است.

در اتحادیه اروپا، دستورالعمل اروپایی امضاها الکترونیکی^۵ و دستورالعمل تجارت الکترونیکی^۶ را باید مبنای قانونی اعتبار امضاها الکترونیکی دانست. این مقررات، امره و پیوستن دولتهای عضو اتحادیه اروپا به آنها اجباری می‌باشد. ماده ۲ دستورالعمل امضاها 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

1. Signatory.

2. Recognition of Foreign Certification and Electronic Signatures.

3. E-Commerce and Development Report, Op cit, p.115.

4. Smedinghoff, T.J. and Bro, R.H. "Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce," **The John Marshall Journal of Computer & Information**, Vol 17, 1999.p.723 .

5. Directive on Electronic Signatures Directive 1999.

6. Directive 2000/3/EC of the European Parliament and Council of 8 June 2000 on certain aspects of information society services, in particular electronic commerce, in the Internal Market.

متن (داده‌پیام)، «امضای الکترونیکی پیشرفته»^۱ 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 قراردادهای، در استفاده از قراردادهای الکترونیکی معنی ایجاد نکرده و منجر به فقدان اثر یا اعتبار حقوقی این قراردادهای 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 قراردادهای 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.^۲ 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.^۳ اتخاذ تدابیر گوناگون در کشورهای اروپایی در این زمینه محتمل و نتیجتاً مانع از هماهنگی حقوق این کشورها به عنوان هدف غایی خواهد بود.

۲-۲. حقوق آمریکا

اخیراً در ایالات متحده، امضای الکترونیکی همانند امضای سنتی الزام‌آور شناخته شده است. با این حال قانون به چگونگی تحقق آن اشاره نکرده یا حداقل احتیاطاتی که برای

1. Advanced Electronic Signature.

2. Ramberg, Christina Hultmark. The E-commerce Directive and Formation of Contract in a Comparative perspective, 1 *Global Jurist.*, Iss.2, art. 3, 2001. p.8.

3. Winn, J.K., *Idaho Law Review Symposium: on Uniform Electronic Transaction Act The Emperor's New Clothes: The Shocking Truth about Digital Signatures and Internet Commerce* 2001.

اعتبار و ایمنی فرایند امضا لازم می‌باشد، به دقت بررسی نشده‌اند.^۱ از بعد تاریخی، اولین قانون درباره امضای دیجیتالی به سال ۱۹۹۶ در ایالت یوتای آمریکا به تصویب رسید.^۲ در سطح فدرال، قانون امضاهای الکترونیکی در تجارت داخلی و بین‌المللی^۳ 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 امره به قبول امضای الکترونیکی و به رسمیت 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^۴ از مفهوم امضا می‌باشد؛ به گونه‌ای که حروف چینی ماشینی و شیوه علامت‌گذاری

1. Broderick Martha A., J.D. Electronic Signatures: They're Legal, Now What? Appears in Internet Research: Networking Applications and Policy, 2001, 11(5). P.1.

2. UTAH Digital Signature Act 1996.

3. Electronic Signature in Global and National Commerce Act [E-sign].

4. Uniform Commercial code [UCC].

را که امکان دارد به اندازه امضاهای دستی قابل اعتماد نباشد، در بر می‌گیرد.^۱ نکته مهم دیگر در یوتا این است که شرکتها و مؤسسات 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.

۳ - ۲. حقوق کانادا

در جهت پیوستن به ساختار جهانی تجارت به شیوه الکترونیکی، کنفرانس یکنواخت سازی قوانین کانادا^۲ در ۳۰ سپتامبر ۱۹۹۹، به تقلید از قانون نمونه (۱۹۹۶) قانون متحدالشکل تجارت الکترونیکی (یوکا)^۳ را تصویب کرد. قانون مذکور در اکثر ایالات کانادا با اصلاحات اندکی مورد پذیرش قرار گرفته است. البته ایالت کیپک، قانونی با عنوان «قانونی در پایه‌ریزی چهارچوب حقوقی برای فناوری اطلاعات»^۴ تصویب کرده که بسیار کاملتر از یوکا می‌باشد.^۵

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

1. Boss A, The Uniform Electronic Transaction Act in a Global Environment, *Idaho Law Review*, vol. 37, 2001. P. 38.

2. Uniform Law Conference of Canada.

3. Uniform Electronic Commerce Act [UECA] 1999.

4. An Act to Establish a Legal Framework for Information Technology 2001.

5. Freedman, Bradley J. Electronic Contracts Under Canadian Law - A Practical Guide, *Manitoba Law Journal*, Vol 28 NO 1, 2002. p.3.

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»،^۱ مصوب ۲۰۰۰ مشاهده نمود که استفاده از «امضای الکترونیکی مطمئن» را الزامی می‌داند. در بخش ۴۸ قانون مذکور شرایطی برای امضای مذکور بیان شده است. یوکا، مع‌الأسف، همانند اکثر اسناد موجود در سطح جهانی از ادله و چگونگی اثبات صحت امضاهای الکترونیکی، حمایت حقوقی و قضایی از شخص دارای حسن نیت 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.

۴ - ۲. حقوق فرانسه

در ۱۳ مارس ۲۰۰۰، پارلمان فرانسه، قانونی^۲ را برای پذیرش امضای الکترونیکی تصویب و از طریق آن مفهوم امضای الکترونیکی را وارد قانون مدنی فرانسه (ق.م.ف) کرد. این قانون به سرعت 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

1. Canadian Personal Information Protection and Electronic Documents Act 2000.

2. Law adapting evidence to information technology and relating to electronic signature, March 13, 2000. [loi portant adaptation du droit de la prevue aux technologies de l'information et relative à la signature electronique].

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 به شمار می‌آید.^۱

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.^۲

۵-۲. 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 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 - به‌ویژه در آن قسمت که به امضای الکترونیکی ارتباط دارد - 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)

1. Birnbaum-Sarcy, Laurence & Darques Florence. **Electronic Signature Comparison Between French & U.S. Law**, International Business Law Journal, April 2001. P.2.
2. Menais, Alexandre. **Electronic Signatures in France 2002**, p.3.

همان ماده تعریف شده، که در گفتار اول به بررسی این بند و تعاریف پرداخته‌ایم. از این جهت که امضای دیجیتالی - همانند امضای دستی - 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 - و نه کاغذی - انجام داد، ضرورت دارد که مفهوم «مدارک الکترونیکی» بررسی شود.

ق.ت.ا تعریفی از «مدارک الکترونیکی»^۱ 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 مدارک 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 ه ماده ۲) یا در بندهای (ح) و (ط) به ترتیب «سیستم‌های اطلاعاتی ایمن»^۲ و «رویه ایمن»^۳ را تعریف می‌کند؛ اگرچه، شایسته‌تر آن بود که این مفاهیم مهم از بحث صرف 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

1. Electronic Evidence.
2. Secure Information System.
3. Secure Method.

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 ۱۶-۱۲ در مقام بیان «پذیرش ارزش اثباتی و آثار سابقه و امضای الکترونیکی مطمئن» بسیار فراتر از آنچه که فی الواقع باید می‌بود، برای این موارد ارزش اثباتی قایل و دچار همان اشتباه و افراطی شده که مطابق نظر انجمن ملی دفاتر اسناد رسمی^۱ ایالات متحده، در قوانین راجع به امضای دیجیتالی اکثر ایالات این کشور، مصادیق متعدد دیده می‌شود.^۲

۳. مشکلات حقوقی و عملی ناشی از ظهور سیستم دیجیتالی امضا

۱- ۳. طرح بحث

دو گفتار قبل، در واقع تلاش برای تبیین مفهوم امضای دیجیتالی و جایگاه آن در حقوق مدرن بود. دیدیم که چگونه اکثر کشورهای دنیا این مفهوم را وارد حقوق داخلی خود کرده و قوانین خاصی را درباره آن تصویب نموده‌اند. در همین جا باید گفت که متأسفانه، 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 تأیید آن به مفهوم پذیرش محتوای اسناد است، نیازمند مشاوری با سازمان یا نهادهای تخصصی راجع به ثبت اسناد، گواهی امضا و تصدیق مدارک می‌باشد.

1. National Notary Association [NNA].

۲. گزارش انجمن ملی دفاتر اسناد رسمی، نگاهی به قوانین مربوط به امضای دیجیتالی و ثبت رسمی اسناد، ترجمه مصطفی‌السان، ماهنامه کانون سردفتران و دفتریاران، سال ۴۷، دوره دوم، شماره ۵۱، تیر و مرداد ۱۳۸۳.

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 - حداقل در زمینه امضا و سابقه الکترونیکی - 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 الکترونیکی 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. - که اختصاص به اسناد رسمی دارد - نقض تمام اصول و قواعد موجود در خصوص اسناد رسمی به شمار می‌آید؛ زیرا هیچ مرجع رسمی مسؤولیت 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 تأسیس می‌شوند و ثانیاً: عدم استفاده از خدمات این دفاتر، به دلیل عدم تصریح قانون و اینکه ماده مذکور بعد از مواد ۱۲-۱۶ 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 - آن گونه که مدنظر انجمن ملی دفاتر اسناد رسمی آمریکا بوده - 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.

۲ - ۳. مسایل علمی و فنی

امضای دیجیتالی به عنوان یکی از دستاوردهای الکترونیکی مدرن از مبانی علمی خاصی پیروی می‌کند. اگرچه این جنبه از امضای مذکور در نوشته‌های علمی مورد توجه قرار گرفته، ولی آثار حقوقی آن به دقت 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^۱ ایمن می‌شوند. رمزگذاری کلید عمومی بر الگوریتمی مبتنی است که از طریق دو نوع رمز متفاوت معروف به «کلید»^۲ ایجاد شده و کلیدهای مذکور برای رمزگذاری و رمزگشایی داده‌پیام مورد استفاده قرار می‌گیرد. کلید رمزگذاری به «کلید خصوصی»^۳ 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.^۴

افرادی که در ایجاد و ایمنی امضای دیجیتالی مداخله می‌کنند، را - بر حسب مورد -

1. Public Key Encryption.

2. Key.

3. Private Key.

4. Lekkas, Dimitris & Gritzalis, Dimitris, Cumulative Notarization for Long - Term Preservation of Digital Signatures, **Computer & Security Information** 2004. P.415.

می‌توان به شرح زیر برشمرد.

الف. امضا کننده اصلی.^۱ به مفهوم شخصی که امضای دیجیتالی را برای استفاده از آن در تأیید مدرکی ایجاد می‌کند.

ب. دفتر خدمات گواهی.^۲ 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 تأمین می‌کند، سردفتر به عنوان شخص ثالث قابل اعتماد به تصدیق مدارک و تأیید 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 اعبار عملی می‌بخشد، بسیار ارزشمند محسوب می‌شود، زیرا تقریباً در تمام قوانین راجع به امضای دیجیتالی به افراد این اختیار داده شده که از پذیرش امضا و مدارک الکترونیکی در روابط تجاری و مالی خود با دیگران امتناع نموده و امضای دستی و مدارک کاغذی مطالبه کنند که این امر با توجه به مسایل متعددی چون ضعف امنیت و اعتماد در فضای مجازی قابل توجیه است.

آنچه به اختصار درباره جنبه‌های علمی و فنی امضاها دیجیتالی ذکر شده، نشان

1. Initial Signer.

2. Certification Service Provider [CSP].

می‌دهد که حذف 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 تفاوت ماهوی این دو نباید تردید کرد. امضای دستی نشان می‌دهد که شخص آن سند را تنفیذ نموده، حال آنکه امضای دیجیتالی مدرک معین دلالت بر به کارگیری کلید خصوصی متعلق به فرد معین برای رمزگذاری آن دارد، که در صورت فقدان تصدیق محضری نشانگر چیزی جز عدم تغییر داده‌پیام بعد از ایجاد آن نیست. به عبارت دیگر بدون وجود سابقه ثبتی و مدارک دقیق علمی، امضای دیجیتالی هیچ دلالتی بر دخالت یک فرد در محتوای سندی که امضا در آن به کار گرفته شده، ندارد.^۱

بدون دخالت دفاتر اسناد رسمی - یا هر ارگان دیگر که به اصول سنتی ثبت اسناد احترام بگذارد - اشکالات دیگری نیز بروز می‌کند که آثار آن به مراتب بدتر و وسیع‌تر از موارد بالاست: فقدان سابقه و بایگانی مطمئن مدارک، وجود گواهی برای همیشه، امکان اختصاص کلید خصوصی یک شخص به فرد دیگر به دلیل بی‌اطلاعی از این امر یا اشتباه، افشای رمزگذاری یا بی‌اعتباری استانداردهای آن، تغییر غیر مشروع رمز و . از مشکلات فنی و علمی می‌باشد که بررسی تفصیلی آنها از موضوع این مقاله و تخصص نویسنده خارج است. در فرازهای بعدی به مسایل حقوقی ناشی از عدم دخالت مرجع ثبتی در جریان ایجاد و ایمنی امضاهای الکترونیکی - که چنانچه گفته شد، بیشتر از ابعاد علمی و فنی ناشی می‌شود - خواهیم پرداخت.

۳ - ۳. مسایل حقوقی ناشی از امضای دیجیتالی

شمارش این مسایل به دلیل تعدد و روزافزونی آنها بسیار دشوار است. فقدان مرجع ثبت و نظارت بر امضای دیجیتالی از جمله منجر به مسایل حقوقی به شرح زیر می‌باشد.

1. Gladman , Brian, Elison, Carl and Bohm, Nicholas. **Digital Signatures, Certificates & Electronic Commerce**, Version 1.1, revised 8th June 1999, Digital Signatures, Certificates and Electronic Commerce.p.10.

۳-۳-۱. گمنامی^۱

از آن جهت که در قوانین داخلی کشورها (راجع به امضای الکترونیکی)، از جمله کشورمان، حضور امضا کننده نزد سردفتر واجد شرایط به منظور ثبت امضا پیش‌بینی نشده، بنابراین نیازی به طی تشریفات مقرر در قانون ثبت برای تشخیص هویت امضا کننده وجود ندارد و همین امر امکان صدور امضا از سوی اشخاصی را که فی‌الواقع وجود ندارد (افراد خیالی)^۲ افزایش می‌دهد. نتیجه این امر آشکار است: امضا کننده می‌تواند از این طریق حقوق و تعهداتی برای خویش در قرارداد با دیگران ایجاد نماید، حال آنکه تعهدات وی به دلیل فقدان شخصیت حقیقی برای او قابل گریز می‌باشد. اگرچه این وضعیت در حقوق ایالات متحده با تصویب قانون نمونه دفاتر اسناد رسمی در حال تغییر است؛ اما قانون تجارت الکترونیکی در این مورد پیش‌بینی مداخله دفاتر اسناد رسمی را ننموده و از این لحاظ دارای ایراد اساسی می‌باشد.

به لحاظ تطبیق، میان مقررات داخلی از یک طرف و این مقررات و حقوق آمریکا از سوی دیگر باید افزود که به موجب ماده ۸۶ ق.ت، «در صورتی که تقاضای ثبت سندی بشود تحصیل اطمینان از هویت متعاملین یا طرفی که تعهد کرده به عهده صاحب دفتر است و اگر مشارالیه شخصاً آنها را نشناسد باید بر طبق مواد این قانون رفتار نماید و در صورت تخلف مشمول ماده ۱۰۲ این قانون خواهد بود». ماده ۱۰۲ نیز ناظر به ماده ۱۰۱ می‌باشد که در آن برای متخلف مجازات اداری از یک تا سه سال انفصال از خدمت دولتی تعیین شده است. همچنین، بنابر ماده ۵۰ ق.ت، «هرگاه مسؤول دفتر در هویت متعاملین یا طرفی که تعهد می‌کند تردید داشته باشد، باید هر دو نفر از اشخاص معروف و معتمد حضوراً هویت آنان را تصدیق نموده و مسؤول دفتر مراتب را در دفتر ثبت و به امضای شهود رسانیده و این نکته را در خود اسناد قید نماید».

ماده ۱۰ ق.ت.ا، در بیان شرایط امضای الکترونیکی مطمئن، معلوم نمی‌کند که

1. Anonymity.
2. Fictions Person.

احراز این شرایط با چه مرجعی است: اگرچه امضا فی نفسه می تواند، نسبت به امضا کننده منحصر به فرد بوده و به وسیله امضا کننده و یا تحت اراده انحصاری وی صادر شده باشد (بند الف و ج ماده ۱۰)؛ اما هیچ تضمینی برای اینکه هویتی که امضای دیجیتالی برای امضا کننده معلوم می کند، همان هویت واقعی او باشد، وجود ندارد و باید تشخیص این امر را به مرجعی صالح سپرد.

در حقوق آمریکا عدم تصریح یوتا به نقش دفاتر اسناد رسمی در ثبت الکترونیکی و در نتیجه تصویب قوانین خاصی در ایالات آمریکا که به موجب آن نیازی به حضور امضا کننده دیجیتالی در دفاتر اسناد وجود نداشت، به شدت مورد انتقاد حقوقدانان و دست‌اندرکاران ثبت اسناد قرار گرفت.^۱ به گونه‌ای که انجمن ملی دفاتر اسناد رسمی آمریکا آن را نوعی دستبرد غیر رسمی^۲ به حوزه کاری خود محسوب داشت.^۳ در نتیجه سمینارها و نشست‌های متعددی در تبیین ابعاد قضیه و چاره‌اندیشی برای مساله برگزار گردید.^۴ مخالفان در تبیین روندی که به غلط شکل گرفته بود معتقدند، اینکه E-Sign به عنوان قانون فدرال و قوانین و مقررات داخلی برخی از ایالات به اشخاص - به صراحت یا به طور ضمنی - اجازه می‌دهند تا گواهی دیجیتالی را از یک مرجع مجاز برای صدور گواهی اخذ کرده و از آن برای ایجاد امضاهای دیجیتالی ثبت شده، بی‌هیچ محدودیتی و بدون بهره گرفتن از خدمات صدور گواهی دفاتر اسناد رسمی، استفاده نمایند، امکان سوء استفاده اشخاص را از طریق استفاده از هویت دیگران (سرقت هویت) و گمنامی فراهم

1. Thaw, Deborah M. *the Notary Public and its Impact in 21st Century*, A Presentation at the NACO/ NACRC Annual Conference, 2000.p.4; Valera, Milton, G. *In Notarization, There is no Substitute for Personal Appearance-Despite Technology*, A Presentation to the Property 2000.p.4.

2. Verbal Misappropriation.

3. *A Position on Misleading Usage of Notary Terms In the Electronic Age* A Position Statement from the National Notary Association 2001.p.1.

۴. در بیشتر موارد این سمینارها به ابتکار انجمن ملی دفاتر اسناد رسمی آمریکا برگزار شده است. تعدادی از مقالات ارایه شده در آن سمینارها در تحقیق حاضر مورد استفاده قرار گرفته و در فهرست منابع معرفی شده‌اند.

می‌سازد.

تلاشهای جمعی و فردی انجام شده، سرانجام تا حدودی، به ثمر نشست. چرا که بند

۳- ۱۶ ماده ۳ قانون نمونه دفاتر اسناد رسمی، برای جلوگیری از گمنامی مقرر می‌دارد:

«دفترخانه ثبت الکترونیکی نباید اقدام به ثبت الکترونیکی نماید، در صورتی که امضا

کننده مدرک الکترونیکی:

۱. به هنگام ثبت، نزد سردفتر اسناد رسمی حاضر نشده باشد.

۲. هویت وی برای شخص سردفتر نامعلوم بوده و دلایل متقنی برای احراز هویت او

از سوی سردفتر موجود نباشد.

۳. قراینی باشد که بر اساس آن سردفتر در اینکه آیا امضا کننده به آثار حقوقی آنچه

درخواست ثبت آن را دارد، آگاه است یا نه، تردید نماید.

۴. از نظر سردفتر، اراده آزاد او (امضا کننده) احراز نشود».

دفاتر خدمات صدور گواهی الکترونیکی مذکور در قانون تجارت الکترونیکی، اختیار و

صلاحیت بررسی هیچکدام از موارد فوق را دارا نمی‌باشند. این امر مفهومی جز دامن زدن

به گمنامی، بی‌هویتی و سرقت هویت در روابط الکترونیکی ندارد. آثار نامطلوب روند

مذکور عبارت از، امکان جعل، کلاهبرداری، خیانت در امانت و سایر جرایم در فضای

مجازی است، حال آنکه با تمسک به ثبت الکترونیکی و تشریفات که بخشی از آن ذکر

گردید، می‌توان از بسیاری از مشکلات کاست.

۲ - ۳ - ۳. نقض حقوق مصرف کننده

قانون تجارت الکترونیکی مقررات بالنسبه قابل توجهی (مواد ۲۳ تا ۴۹) را به «حمایت

از مصرف کننده»^۱ اختصاص داده است. در بند ب ماده ۳۳ از لزوم مشخص شدن هویت

تأمین 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 مدنظر نبوده است. فقط در ماده ۳۵ ق.ت.ا مقرر شده، «اطلاعات اعلامی و تأییدیه 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 لزوم حسن نیت در معاملات و از جمله ضرورت رعایت افراد ناتوان و کودکان ارایه شود». حال آنکه ارایه اطلاعات در واسطی بادوام، همانند دیسک، فلاپی و ..بند) ق (ماده ۲ ق.ت.ا (مانع از کلاهبرداری و تقلب نخواهد بود.

مساله از جنبه دیگر نیز قابل بررسی است: امضای دیجیتالی مصرف کننده نباید در معرض نفوذ و سوء استفاده دیگران باشد، اشخاص ضعیف و کم‌توان باید قبل از معامله الکترونیکی از هر نظر توجیه شده و نسبت به ابعاد معامله اطلاع یابند و همین مسایل ضرورت ثبت حداقل امضای طرف مقابل را به عنوان شخصی که مدام در عرصه تجارت فعال است، نزد سردفتر قابل اعتماد توجیه می‌نماید.

۳-۳-۳. امضای دیجیتالی و ثبت الکترونیکی

از آن جهت که اعتبار امضای دیجیتالی و ثبت الکترونیکی در قانون داخلی شناسایی شده، که از جمله شامل امضاهایی می‌شود که در اسناد و مدارک الکترونیکی به کار می‌رود، لذا باید دفاتر اسناد رسمی و ادارات ثبت اسناد و املاک به عنوان مراجع صالح در کشورمان برای طی تشریفات و اعمال این شیوه از ثبت آماده شوند. ماده ۶ ق.ت.ا، در پذیرش مدارک الکترونیکی مقرر می‌دارد: «هرگاه وجود یک نوشته از نظر قانون لازم باشد، «داده‌پیام» در حکم نوشته است. «..ماده بعدی نیز در جهت پذیرش امضای الکترونیکی چنین تدوین شده، «هرگاه قانون وجود امضا را لازم بداند، امضای الکترونیکی مکفی است».

متأسفانه قانون فوق به بررسی دقیق شرایط و ضوابط پذیرش امضا و مدارک الکترونیکی نپرداخته و به همین دلیل باید مقررات و رویه لازم برای این امر در کشورمان وضع شده و شکل گیرد. دفاتر اسناد رسمی نیز از جمله مراجعی هستند که باید به دلیل کارکرد و قابلیت و وظایف قدیمی خود در روند ثبت اسناد و امضای الکترونیکی مداخله

نمایند. بدیهی است که این موضوع نیازمند تصویب قانون، طی تشریفات و ایجاد زیرساخت‌های مورد نیاز می‌باشد. در این مقاله، اگرچه به دلیل نا آشنایی حقوق کشورمان با مفاهیم امضای دیجیتالی، گواهی و ثبت الکترونیکی، بیشتر به جنبه‌های نظری موضوع پرداخته شد، با این حال نحوه ثبت الکترونیکی امضا در مقام عمل نیز به اختصار مورد بررسی قرار می‌گیرد. البته ذکر این نکته اهمیت دارد که بحث تفصیلی موضوع نیازمند پرداختن به مساله «ثبت الکترونیکی» به مفهوم عام است که بررسی آن از چهارچوب این مقاله خارج می‌باشد.

۱-۳-۳-۳. اصول حاکم

در زمینه ثبت امضای الکترونیکی، در وهله اول، سه اصل مهم را باید مدنظر قرار داد: یک. استفاده از تجربه ارزشمند سایر کشورها و رویه عملی شکل گرفته در دفاتر ثبت اسناد آنها از جهت کاهش هزینه مطالعاتی و اجرایی ثبت الکترونیکی، امری است که باید - البته با رعایت ضوابط، معیارها و اوصاف خاص سیستم ثبتی کشور - آن را پذیرفت. در این راستا، بررسی و پژوهش عمیق مورد نیاز است و ترجمه صرف قوانین و مقررات داخلی دیگر کشورها عامل همان مشکلاتی خواهد بود که در برخی از قوانین داخلی ملاحظه می‌شود.

دو. بحث از ثبت الکترونیکی، اگرچه بسیار جدید می‌باشد، به گونه‌ای که عملاً نمی‌توان سابقه‌ای بیش از ۵ سال برای آن تصور نمود؛ با این حال به هیچ وجه نباید آن را ناقص اصول و قواعد ثبتی ایجاد شده در طول سالهای مختلف دانست. در مقدمه توجیهی قانون نمونه دفاتر اسناد رسمی آمریکا^۱ نیز تأکید شده که، «اگرچه فناوری در حال تحول و تکامل است، اما متأسفانه ماهیت انسانهایی که آن را به کار می‌گیرند، چنین نیست. هر آئینی - خواه کاغذی یا الکترونیکی - برای ثبت اسناد و امضا، مستلزم حضور فیزیکی امضا کننده در یک دفترخانه اسناد رسمی واجد شرایط و صالح است. بر خلاف تصور عموم،

1. The Model Notary Act, Op cit, p.75.

ثبت الکترونیکی نباید به عنوان عامل «ریشه‌کنی» ثبت رسمی (در حوزه تجارت الکترونیکی (محسوب گردد». 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 که شامل تصدیق و گواهی، امضا، شهادت و تمام مفاهیم تخصصی مربوط می‌باشد.

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

سه . در مورد امضای الکترونیکی، ترجیح هر یک از فناوریهای ایجاد امضا، بدون لحاظ جنبه ایمنی و اطمینان آن، از هر نظر بی‌اعتبار است. دفاتر ثبت الکترونیکی باید در صورت احراز صدور و ایجاد امضا و کلید خصوصی به نام متقاضی، نسبت به ثبت و طی تشریفات لازم اقدام نمایند. علی‌الاصول نمی‌توان با توصیف فناوری خاص به عنوان شیوه مقبول در ایجاد و رمزگذاری خاص، به نفع شرکت یا شخص مالک آن تبلیغ نمود و باید در مقام پذیرش یا رد امضا کیفیت و ضوابط علمی و فنی را لحاظ کرد.

۲-۳-۳. تشریفات ثبت امضای الکترونیکی

چنانچه گفته شد، اعمال تشریفات ثبت امضای الکترونیکی نیازمند استقرار دفاتر ثبت الکترونیکی می‌باشد. این دفاتر باید در ثبت امضای الکترونیکی ضوابطی را رعایت نمایند که به اختصار ذکر می‌شود.

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 گویی از نظر قانونگذار این شرط به قدری بدیهی بوده که ذکر آن غیر لازم و فقدان آن (عدم حضور شخص امضا کننده نزد سردفتر برای تصدیق

امضا (موجب بی اعتباری چنین تصدیقی بوده است. فقط باید این نکته را افزود که حضور وی برای امضای اسناد و مدارک الکترونیکی نیست، چرا که فرض بر این می باشد که امضای مذکور یکبار توسط او در «دفتر صدور امضای الکترونیکی» ایجاد شده است. حضور امضا کننده برای این است که امضای مذکور ثبت شده و صحت صدور آن از سوی درخواست کننده ثبت از این طریق قابل اثبات باشد.

در مورد این بند، دو ایراد قابل تصور است که ضمن طرح به پاسخ آن نیز می پردازیم: الف. اگر فناوری ارتباط تا اندازه ای پیشرفته باشد که نیازی به حضور امضا کننده نزد سردفتر وجود نداشته باشد، آیا می توان باز هم او را اجبار به حضور نمود؟ به عبارت دیگر، اصل مذکور قابل تخصیص می باشد یا نه؟

در پاسخ باید گفت که اگرچه این نوع از فناوری هم اکنون موجود نیست؛ اما در صورت تحقق آن نیازی به حضور امضا کننده در دفتر ثبت الکترونیکی نخواهد بود و سردفتر ضمن ارتباط دیداری - 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 می توان 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 گونه ای که ایجاد، نگهداری و به روز رسانی امضای الکترونیکی بحثی است متعلق به علم الکترونیک و رایانه، حال آنکه ثبت آن - به لحاظ ضرورت رعایت اصول و قواعد مقبول حقوق و رویه ثبتی - 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 نرم افزار 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 به‌هنگام تقاضای تصدیق / ثبت امضا از سوی متقاضی از اعتبار نیفتاده باشد (بند ۲ - ۱۶ قانون نمونه دفاتر اسناد رسمی آمریکا). (لذا دفتر ثبت الکترونیکی در این زمینه باید دو نکته مهم را بررسی نماید:

یک. 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 عمر^۱ یک یا حداکثر دوساله و مبتنی بر ۱۰۲۴ بیت [Bit] داده از نوع کلید آر.اس.آی^۲ می‌باشد.^۳

دو. 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 مسؤولیتها برای انجام این امور مهیا کرد. به منظور تشخیص صلاحیت مرجع صدور امضا، باید مراجع (دفاتر) مشخصی برای این امر - به موجب قانون و تحت نظارت سازمان مشخص - تأسیس 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

1. Lifespan.

۲. RSA. نوعی فناوری رمزگذاری معمول که بر الگوریتم ریاضی مبتنی است و از هر دو کلید عمومی و خصوصی برای رمزگذاری / رمزگشایی بهره می‌گیرد. نام این روش برگرفته از حرف اول نام مبدعین آن. یعنی ریوست، شامیر و آدلمن، Rivest, Shamir Adelman می‌باشد. منبع: فرهنگ لغت Babylon

3. Lekkas & Gritzalis, Op cit, p.414.

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 مسائلی 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 ماده ۱۰۲ قانون ثبت، 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.

نتیجه‌گیری

توجه به مبانی و زیرساخت‌ها شرط نخست ورود در دنیای تجارت الکترونیکی و پیشرفت در آن حوزه به شمار می‌آید. قانون تجارت الکترونیکی را - علی‌رغم پاره‌ای از ایرادات و نواقص - باید نقطه شروع این روند محسوب داشت. تجربه دیگر کشورها نشان می‌دهد که در صورت تحقق تجارت الکترونیکی، بحث ایمنی از یک سو و مدلل 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 نآشنایی 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 ثقل، 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 به راحتی می توان بدان دست یافت.

فهرست منابع

کاتوزیان، ناصر . اثبات و دلیل اثبات، جلد اول، چاپ اول، نشر میزان، تهران ۱۳۸۰.
گزارش انجمن ملی دفاتر اسناد رسمی، نگاهی به قوانین مربوط به امضای دیجیتالی و
ثبت رسمی اسناد، ترجمه مصطفی السان، ماهنامه کانون سردفتران و دفتریاران، سال
۴۷، دوره دوم، شماره ۵۱، تیر و مرداد ۱۳۸۳.

قانون تجارت الکترونیکی، مصوب ۱۳۸۲/۱۰/۱۷، روزنامه رسمی ۱۳۸۲/۱۱/۱۱ -
سال ۵۹، شماره ۱۷۱۶۷.

قانون ثبت اسناد و املاک، مصوب ۱۳۱۰/۱۲/۲۶ با اصلاحات و الحاقات بعدی، به
نقل از مجموعه قوانین و مقررات ثبتی، تدوین جهانگیر منصور، چاپ اول، نشر دیدار،
تهران ۱۳۸۲.

قانون دفاتر اسناد رسمی و کانون سردفتران و دفتریاران، مصوب ۱۳۵۴/۴/۲۵، به
نقل از مجموعه قوانین و مقررات ثبتی، تدوین جهانگیر منصور، چاپ اول، نشر دیدار،
تهران ۱۳۸۲.

Bacchetta, M., et al. **Electronic Commerce and the Role of the WTO**, World Trade Organization Special Studies 2, Geneva: World Trade Organization, 1998.

Berbecaru and et al, **Toward Concrete Application of Electronic Signature** 2002. http://security.polito.it/doc/papers/e_sign.pdf

Birnbaum-Sarcy, Laurence & Darques Florence. **Electronic Signature Comparison Between French & U.S. Law**, International Business Law Journal, April 2001.

Boss A, The Uniform Electronic Transaction Act in a Global Environment, **Idaho Law Review**, Vol. 37, 2001.

Broderick Martha A., J.D. Electronic Signatures: They're Legal, Now What? Appears in Internet Research: **Networking Applications and Policy**, 2001, 11(5), 423-434.

Gladman, Brian, Ellison, Carl and Bohm, Nicholas. **Digital Signatures, Certificates & Electronic Commerce**, Version 1.1, revised 8th June 1999, Digital Signatures, Certificates and Electronic Commerce. <http://jya.com/bg/digsig.pdf>

Freedman, Bradley J. Electronic Contracts Under Canadian Law-A Practical Guide, **Manitoba Law Journal**, Vol 28 NO 1, 2002.
http://www.umanitoba.ca/faculties/law/Journal/back_issues/articles/28_1_freedman.pdf

Leff, Laurence LeffLaurence, **Notaries and Electronic Notarization**, Western Illinois University 2002
<http://www.oasis-open.org/committees/download.php/4541/enotarization.pdf>

Lekkas, Dimitris & Gritzalis, Dimitris. Cumulative Notarization for Long-Term Preservation of Digital Signatures, **Computer & Security Information** 2004.

Menais, Alexandre. **Electronic Signatures in France 2002**, Available at: <http://www.juriscom.net/en/pro/1/ec20020730.htm>

Ramberg, Christina Hultmark. The E-commerce Directive and Formation of Contract in a Comparative Perspective, 1 **Global Jurist**, Iss. 2, art. 3 (2001), Available at:
<http://www.bepress.com/gj/advances/voll/iss2/art3>.

Smedinghoff, T. J. and Bro, R.H. (1999), "Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce," **The John Marshall Journal of Computer & Information**, Vol 17, pp. 723-768.

Thaw, Deborah M. the Notary Public and its Impact in 21st Century, A Presentation at the NACO/NACRC Annual Conference, 2000. Available at:
www.nationalnotary.org/userimages/notaryofficeandimpact.pdf

Valera, Milton G. **A Presentation To The Multi State Digital Signature Summit**, National Notary Association, Chatsworth, California Marines' Memorial Club & Hotel San Francisco, California Friday, August 11, 2000

Valera, Milton G. In Notarization, There is no Substitute for Personal Appearance—Despite Technology, A Presentation to the Property
www.nationalnotary.org/userimages/inNotarization.pdf

Winn, J. K., **Idaho Law Review Symposium: on Uniform Electronic Transaction Act The Emperor's New Clothes: The Shocking Truth about Digital Signatures and Internet Commerce** at: <http://www.smu.edu/~jwiztn/shocking-truth.html>

A Position on Digital Signature Laws and Notarization, a Position Statement From The National Notary Association
www.nationalnotary.org/userimages/digitalSignature.pdf

A Position on Misleading Usage of Notary Terms in the Electronic Age A Position Statement from the National Notary Association 2001.
www.nationalnotary.org/userimages/Notary_Terms.pdf

Digital Signature Guidelines, **Legal Infrastructure for Certification Authorities and Secure Electronic Commerce**, Information Security Committee Electronic Commerce and Information Technology Division Section of Science and Technology American Bar Association 1996. www.abanet.org/scitech/ec/isc/dsg.pdf

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (**Directive on electronic commerce**). Available at: www.europea.oeu.int/ISPO/ecommerce/legal/documents/200031ec_en.pdf.

Directive 1999/93/Ec Of 13 December 1999 On a Community Framework For Electronic Signatures , A Copy of **Electronic Signatures Directive** is Available At: www.europa.eu.int/information_society/topics/ebusiness/ecommerce/8epolicy_elaw/law_ecommerce/legal/index_en.htm .

Electronic Signature in Global and National Commerce Act [E-sign]. Effective October. 1,2000. Available at: <http://fwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106-cong-bills&docid=f:s761enr.txt.pdf>.

E-Commerce and Development Report, United Nations, New York & Geneva 2001. Available at: www.commercenet.org/documentos/UNCTAD%20Report%20on%20e-commerce%202002.pdf.

Electronic and Digital Signatures, State Archives Department, Minnesota Historical Society March 2004, Version 4 Page 1

Electronic Records Management Guidelines Electronic and Digital Signatures 2000.

The Model Notary Act, September 1, 2002. Published As A Public Service by the National Notary Association. Available at:
http://www.nationalnotary.org/UserImages/Model_Notary_Act.pdf

UNCITRAL Model Law On Electronic Commerce With Guide to Enactment 1996 , Available at:
www.uncitral.org/english/texts/electcom/ecommerceindex.htm.

UNCITRAL Model Law on Electronic Signatures 2001, Available at:
www.uncitral.org/english/texts/electcom/ml-electsig-e.pdf.

Uniform Electronic Transactions Act [UETA], Approved By National Conference Of Commissioners On Uniform State Laws (NCCUSL) On July 23, 1999. Available at:
www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm .

Uniform Law Conference of Canada, **Uniform Electronic Commerce Act [UECA]**, August 1999, Available at:
www.law.ualberta.ca/alri/ulc/eindex.htm.