

Research Paper

Legal effects of electronic signature and its difference with digital signature

Masoumeh Vaziri Yeganeh ¹, Jamshid Mirzaei ² 

1- Phd student in private Law, Khoramabad Branch, Islamic Azad University, Khoramabad, Iran.

2- Assistant Professor, Department of Law, Khoramabad Branch, Islamic Azad University, Khoramabad, Iran.

Receive:

22 July 2024

Revise:

26 August 2024

Accept:

31 August 2024

Published online:

21 September 2024




Abstract

The increasing growth of the use of Application of communication technology in the world has resulted in new legal rules. In order for the comprehensive interaction of people in the use of this technology and establishing security and public trust, a special judicial system regarding it, in terms of guaranteeing internal and international judicial enforcement. The rules that generally have their own procedural rights in administrative, civil, and criminal lawsuits, and the evidence to prove their lawsuits are also unique in some cases. The increasing tendency to use information technology and the rapid and inevitable expansion of e-commerce at the international level requires the provision of necessary legal mechanisms in this regard. Considering the virtual and immaterial nature of electronic exchanges, one of the most important issues from the point of view of rights is the proof of these exchanges and the identity of the parties. Digital signatures or other mathematical cryptographic techniques that are subsets of electronic signatures make this possible. Today, electric business has opened a new arena in competition due to its speed, efficiency, cost reduction and exploitation of fleeting opportunities, so that it is said that lagging behind this path of development is the result of being isolated in the world economy. will not have In the meantime, many and varied tools have been proposed for the use and application of electronic commerce, and digital signature is one of them.

Keywords:

electronic documents,
electronic signature,
digital signature,
proof of claim,
service offices.


Please cite this article as (APA): Vaziri Yeganeh,M, Mirzaei, J.(2024). Legal effects of electronic signature and its difference with digital signature. *Journal of Business law and economics*, (1) 1, 137-149.

Sponsored by: Institute of Somamos Publications	https://doi.org/10.22034/jble.2024.208264	
Corresponding Author: Jamshid Mirzaei	https://orcid.org/0000-0001-5302-7248	
Email: mirzaei@khoiau.ac.ir	This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License .	



مقاله پژوهشی

آثار حقوقی امضای الکترونیکی و تفاوت آن با امضای دیجیتالی

معصومه وزیر یگانه^۱، جمشید میرزایی^۲ 

۱- دانشجوی دکتری حقوق خصوصی، واحد خرم آباد، دانشگاه آزاد اسلامی، خرم آباد، ایران.

۲- استادیار گروه حقوق، واحد خرم آباد، دانشگاه آزاد اسلامی، خرم آباد، ایران.

<p>چکیده</p> <p>رشد فزاینده کاربرد فناوری اطلاعات در جهان قواعد حقوقی جدیدی در پی داشته است. در جهت تعامل همه جانبه افراد در استفاده از این فناوری و برقراری امنیت و اعتماد عمومی، نظام دادرسی و پرونده‌های در مورد آن، از حیث ضمانت اجرای قضایی داخلی و بین‌المللی شکل گرفته است. قواعدی که عموماً حقوق دادرسی خاص خود را در دعاوی اداری، مدنی و کیفری دارد و ادله اثبات دعوی آن نیز در پاره‌ای از موارد منحصر به فرد است. گرایش روز افزون به استفاده از فناوری اطلاعات و گسترش سریع و ناگزیر تجارت الکترونیک در سطح بین‌المللی، پیش‌بینی ساز و کارهای حقوقی لازم در این خصوص را ایجاب می‌کند. با توجه به ماهیت مجازی و غیر مادی مبادلات الکترونیک یکی از مهمترین مسایل از دید حقوق اثبات این مبادلات و هویت طرفین آن است. امضای دیجیتال یا سایر فنون رمزنگاری ریاضی که زیر مجموعه‌های امضای الکترونیکی هستند چنین امری را ممکن می‌سازد. امروزه تجارت الکترونیکی به دلیل سرعت، کارایی، کاهش هزینه‌ها و بهره‌برداری از فرصت‌های زودگذر، عرصه جدیدی را در رقابت گشوده است تا آن‌جا که گفته می‌شود، عقب افتادن از این مسیر تحول، نتیجه‌ای جز منزوی شدن در عرصه اقتصاد جهانی نخواهد داشت. در این میان کارابزارهای متعدد و متنوعی برای استفاده و بکارگیری تجارت الکترونیکی مطرح شده است که امضای دیجیتالی از جمله آنها به شمار می‌رود.</p>	<p>تاریخ دریافت: ۱۴۰۳/۰۵/۰۱</p> <p>تاریخ بازنگری: ۱۴۰۳/۰۶/۰۵</p> <p>تاریخ پذیرش: ۱۴۰۳/۰۶/۱۰</p> <p>تاریخ انتشار آنلاین: ۱۴۰۳/۰۶/۳۱</p> <p>کلید واژه‌ها: اسناد الکترونیک، امضاء الکترونیکی، امضای دیجیتالی، ادله اثبات دعوی، دفاتر خدمات.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

لطفاً به این مقاله استناد کنید (APA): وزیر یگانه، معصومه؛ میرزایی، جمشید. (۱۴۰۳). آثار حقوقی امضای الکترونیکی و تفاوت آن با امضای دیجیتالی، *دانشنامه حقوق کسب و کار و اقتصاد*، ۱(۱) ۱۳۷-۱۴۹.

	https://doi.org/10.22034/jble.2024.208264	تحت حمایت: موسسه انتشاراتی ساموس
	https://orcid.org/0000-0001-5302-7248	نویسنده مسئول: جمشید میرزایی
	این مقاله تحت شرایط https://creativecommons.org/licenses/by-nc/4.0/deed.fa قابل بازنشر است.	ایمیل: mirzaei@khoiau.ac.ir



مقدمه

ظهور و گسترش پدیده اینترنت و رشد روزافزون تجارت الکترونیکی، تحول در ساختارهای سنتی مرتبط با امور اداری و تجاری را اجتناب‌ناپذیر ساخته است. یکی از رهاوردهای مهم فناوری اطلاعات، تحول در رژیم سنتی ادله اثبات دعوا است. در نظام ادله اثبات دعوی اکثریت مطلق کشورهای جهان، پس از اقرار، دلایل کتبی یا نوشته از اهمیت غیر قابل انکاری برخوردار هستند، به نحوی که بیشترین استفاده را در مقام استناد یا دفاع از دعوا دارند. در واقع، طرح دعوا و اقامه دلایل در زندگی حقوقی ما تا حدود زیادی منوط به ارائه یا صدور یک نوشته کاغذی نظیر کارت شناسایی، فیش حقوقی، رسیدهای پرداخت وجه، قراردادها، اعلامیه‌ها و اخطارها و اظهارنامه‌ها و اسناد تجاری است. فناوری اطلاعات به دلیل ویژگی‌های فنی خود به‌طور محسوس از گردش کاغذ و دلایل کاغذی می‌کاهد. بدیهی است این فناوری قادر به حذف گردش کاغذ نیست، ولی دامنه آن را روز به روز کاهش خواهد داد. در حقوق ثبت و تجارت الکترونیک و به تبع آن مبادلات اسناد و داده‌های تجاری اشخاص باید مطمئن باشند که انتقال‌ها، ایمن و قابل اثبات و مشروع هستند. تنها با این دلگرمی اشخاص می‌توانند در تجارت الکترونیکی فعالیت کنند، زیرا عدم وجود هر یک از خصیصه‌های فوق در انتقال داده‌ها می‌تواند آسیب‌های عمده‌ای به اشخاص حقیقی یا حقوقی وارد کند. اسناد با ارزش قانونی ذخیره می‌شوند بدین منظور که احتمالاً در آینده به دلالت آنها نیاز شود. به‌طور کلی در آرشیو اسناد چهار نکته اساسی وجود دارد که عبارتند از: ایجاد امضاء، اثبات امضای اولیه، ذخیره سازی و ترافک. اگر در مورد اسناد فوق الذکر ترافیکی حاصل شد، باید هویت امضاکننده و صحت امضای وی مجدداً بررسی گردد. یکی از خصوصیات اسناد تجاری الکترونیکی قابلیت حفظ آنها با حجم اندک و برای یک دوره طولانی است و در این مورد امضاهای الکترونیکی نقش مهمی ایفا می‌کنند.

۲- ثبت الکترونیکی

ثبت الکترونیکی، به کارگیری شیوه‌های نوین ارتباط برای تسهیل ثبت اسناد و مدارک است. این فناوری علی‌الاصول برای ثبت تمام اسناد قابل استفاده می‌باشد. با این حال قانون خاص امکان دارد که در جهت حمایت از مصرف‌کننده و یا عوامل دیگر، ثبت الکترونیکی را در مواردی مجاز نداند. 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» در ماده ۳۱ و ۳۲ قانون تجارت الکترونیکی 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. (باقرزاده و همکار، ۱۳۸۸، ۲۵) 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 از «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) ماده ۳ تصریح شده که دفاتر ثبت الکترونیکی، نهادهایی جدای از دفاتر اسناد رسمی به شمار نمی‌آیند و هر سردفتری می‌تواند با گرفتن مجوز و آموزش‌های لازم به یک سردفتر الکترونیکی تبدیل شود. البته دفاتر ثبت اسناد در اقدام به این امر هیچ الزامی ندارند. 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. در اکثر استان های فرانسه ثبت الکترونیکی شروع شده و مقرراتی برای نظام مند کردن آن به تصویب رسیده است. برای مثال در شهر هایی چون مالت، پاریس قوانینی در تجویز «ثبت الکترونیکی» تصویب شده که این دفاتر از جمله به گواهی امضاهای دیجیتالی اقدام می کنند. در پاریس نیز از سال ۲۰۰۲ ثبت الکترونیکی آغاز گردیده و قانون خاصی در این مورد تدوین یافته است. در کشورمان، قانون یا رویه خاصی که به تعریف اصطلاحات راجع به ثبت الکترونیکی پرداخته باشد، وجود ندارد. یکسانی ماهیت و آثار حقوقی ثبت الکترونیکی و سنتی مانع از آن نیست که اصطلاحات در شیوه جدید ثبت اسناد و شرایط اطلاق عنوان «رسمی» به آنها ناشناخته بمانند. ابهام در این مورد، از جهات مختلفی به خصوص از آن جهت که امکان سوء استفاده و برداشت های متناقض را فراهم می نماید دارای ایراد است. (بختیاروند، ۱۳۸۳، ۳۱) برای رسیدن به هدف، چاره ای جز توجه به مقررات خارجی که به طور خاص به این موضوع پرداخته اند، وجود ندارد. در باب چهاردهم قانون نمونه دفاتر اسناد رسمی، اصطلاح «الکترونیک» در بند ۱-۱۴ به «فناوری دارای قابلیت های الکترونیکی، دیجیتالی (رقومی)، مغناطیسی، بی سیم، دیداری (بصری)، الکترومغناطیسی یا موارد مشابه»، تعریف شده است. قسمت اخیر بند با ذکر موارد مشابه، در واقع پیشرفت های آینده را لحاظ نموده و از قید انحصار در این زمینه خودداری کرده است. به منظور تأکید بر وابستگی دفاتر اسناد رسمی فعلی و دفاتر اسناد رسمی الکترونیکی، بند ۲-۱۴ آن را به دفترخانه اسناد رسمی که به عنوان دفتر دارای قابلیت انجام ثبت الکترونیکی به ثبت رسیده، تعریف کرده است.

مطابق با قانون مذکور، مدرک الکترونیکی، در مفهوم عام شامل اطلاعاتی است که با وسایل الکترونیکی ایجاد، تولید، ارسال، ابلاغ، دریافت یا ذخیره شده باشد. همین تعریف، با مقداری توسعه در مفهوم، در بند الف ماده ۲ قانون تجارت الکترونیکی کشورمان برای «داده پیام» ذکر شده است. تعاریف مذکور به گونه ای دیگر دلالت بر قابل استناد بودن مدارکی دارد که وسایل الکترونیکی در مورد آنها به کار گرفته شده است (جمالزاده و همکار، ۱۳۸۶، ۲۴).

دفتر الکترونیکی سوابق ثبت در بند ۴-۱۴ قانون نمونه دفاتر اسناد رسمی تعریف شده است. نظر به اینکه مطابق با بند ۱-۷ قانون مذکور و ماده ۱۹ قانون دفاتر اسناد رسمی و قانون سردفتران و دفتریاران، مصوب ۱۳۵۴/۴/۲۵، دفاتر اسناد رسمی باید دارای دفاتر خاصی برای نگهداری سوابق اسنادی باشند که ثبت می نمایند، پیش بینی این دفاتر برای ثبت الکترونیکی نیز ضروری می باشد. قانون نمونه با لحاظ همین ضرورت، دفتر الکترونیکی سوابق ثبتی را به وسیله ای الکترونیکی که سابقه ای دارای تاریخ و منظم که اعمال ثبتی توسط سردفتر در آن درج می شود، تعریف کرده است. به منظور جلوگیری از هرگونه خدشه به این دفاتر، همانند دفاتر کاغذی، قانون نمونه در جزءهای شش گانه از بند ۴-۱۴ شرایطی را برای آنها مشخص کرده است.

۳- اعتبار و قواعد حقوقی حاکم بر اسناد الکترونیکی

با الکترونیکی شدن ثبت سند، نیاز به اوصافی که برای سند عادی یا رسمی کاغذی که در قوانین ماهوی یا شکلی مقرر است، مرتفع نمی شود. چون سند رسمی الکترونیکی دارای تمام مزایای حمایتی و تضمینی مقرر برای سایر اسناد خواهد بود، لذا تشریفات و معیارهای تنظیم آن به گونه ای رعایت شده باشد که موجب تردید در ایمنی اسناد نگردد (زرکلام، ۱۳۸۲، ۵۴). قوانین و مقررات متعددی این اشکال را که مدارک الکترونیکی دارای اعتبار هستند یا نه، مرتفع ساخته اند. برای مثال در ایالات متحده E-Sign و یوتا که عملاً به قانونی استاندارد در سطح جهانی تبدیل شده، اعتبار یکسانی برای اسناد الکترونیکی در مقایسه با اسناد کاغذی شناخته اند. این روند، با دو قانون نمونه آنسیترال که در سالهای ۱۹۹۶ و ۲۰۰۱ به تصویب رسیده اند، تکمیل گردیده است.



ماده (الف)(۲) ۶۲ قانون امضای دیجیتالی مالزی مصوب ۱۹۹۷ نیز تلویحاً اعتبار داده‌پيامی را که در برای ایجاد سند الکترونیکی به کار می‌رود، تأیید نموده است. به موجب این بند، «جز در مواردی که قانون به گونه‌ای دیگر مقرر داشته باشد، سندی که با امضای دیجیتالی واجد شرایط این قانون تصدیق شده، همانند سندی که به صورت دستی امضاء یا انگشت یا هر علامت دیگری بر آن زده شده، معتبر و تعهدآور است.

در حقوق ایران، مطابق با ماده ۶ قانون تجارت الکترونیکی، هرگاه وجود یک نوشته از نظر قانون لازم باشد، جز در موارد استثنایی و محدود، «داده پیام» در حکم نوشته است. و بنابر ماده ۸، «هرگاه قانون لازم بداند که اطلاعات به صورت اصل ارایه یا نگهداری شود، این امر یا نگهداری و ارایه اطلاعات به صورت داده پیام نیز.. امکان‌پذیر می‌باشد». و بر طبق قسمت اخیر ماده ۹ همان قانون، «جایگزینی اسناد کاغذی به جای «داده پیام» اثری بر حقوق و تعهدات قبلی طرفین نخواهد داشت». و سرانجام، ماده ۱۲ این قانون به گونه‌ای تدوین یافته که هرگونه شک و شبهه‌ای را در باب اعتبار مدارک و اسناد الکترونیکی - به صرف شکل و قالب الکترونیکی آنها مرتفع می‌سازد: «اسناد و ادله اثبات دعوی ممکن است به صورت داده پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان براساس قواعد ادله موجود، ارزش اثباتی «داده پیام» را صرفاً به دلیل شکل و قالب آن رد کرد». البته باید بر این نکته اصرار داشت که هیچ سند، مدرک، سابقه یا امضای الکترونیکی، پیش از طی تشریفات قانونی ثبت، رسمی به شمار نمی‌آید. در این خصوص می‌توان با آرای قضایی استناد کرد که هرچند به دلیل مطرح نبودن اسناد الکترونیکی به طور مستقیم به این دسته از اسناد نپرداخته‌اند؛ اما حاوی قواعد کلی برای نحوه «رسمی» شمردن اسناد می‌باشند (السان، ۱۳۸۴، ۲۵). مطابق با رأی صادره از یکی از محاکم، «جعل چک عادی، جعل سند رسمی محسوب نمی‌شود». هم‌چنین، شورای عالی ثبت ضمن رأی در خصوص ضرورت رسمی و لازم‌الاجرا بودن سند به عنوان شرط لازم برای تقاضای اجرای آن مقرر می‌دارد: «اول؛ ماده اول قانون ۲۲/۶/۲۷ قانون اصلاح بعضی از مواد قانون ثبت و قانون دفاتر اسناد رسمی می‌گوید: «هرکس دستور اجرای اسناد رسمی را مخالف با مفاد سند یا مخالف قانون دانسته یا از جهت دیگری شکایت از دستور اجرای سند رسمی داشته باشد می‌تواند به ترتیب مقرر در آیین دادرسی مدنی اقامه دعوی نماید». موضوع اجرای این ماده موردی است که سند رسمی مسلمی وجود داشته باشد و یا دست کم علم بدیهی به رسمی نبودن سند حاصل نشود. اگر علم بدیهی به رسمی نبودن سند حاصل باشد موردی برای اجرای ماده مزبور نیست. در مانحن فیه با توجه به اینکه قبل از رسیدن به شماره سند و کالتنامه دفتر مزبور منحل شده است با توجه به مواد ۱۲۸۷-۱۲۹۴ قانون مدنی سند و کالتنامه بالبداهه رسمی نیست و ظاهراً موردی برای اعمال ماده یک قانون ۲۲/۶/۲۷ وجود ندارد. دوم؛ به همان استدلال موردی برای اجرای ماده ۹۹ قانون ثبت هم وجود ندارد و چنان است که به استناد سند عادی اجرائیه صادر شده باشد که باید به کنار نهاده شود... جا دارد که در اصلاح قوانین ثبت درباره اختیاراتی صریحاً داده شود تا اسنادی را که بالبداهه (بدون اظهار قضائی) رسمی نبودن آنها مسلم است ملغی الاثر اعلان کنند».

آرای متعددی بیانگر آن هستند که روگرفت غیرمصدق اسناد رسمی، رسمی محسوب نمی‌شوند و جعل آنها، تحریف در اسناد رسمی نیست. برای نمونه، در رأی مقرر شده: «باتوجه به ماده ۲۰ قانون تعزیرات و تعریف قانونی آن، جعل فتوکپی اسناد رسمی و عادی و استفاده از آن جعل جزائی محسوب نمی‌شود لیکن چنانچه فتوکپی اسناد اعم از عادی و رسمی تصدیق شده باشد جعل در آنها و نیز استفاده از آن جرم محسوب می‌شود». نیز، رأی وحدت رویه شماره ۶۳۳۹ - ۲۷ / ۱۳۴۲/۹ اظهار می‌دارد، جعل در فتوکپی یا رونوشت اسناد مصدق ندارد و از مصادیق جعل در سند به معنی و مفهوم مأخوذه قانونی به شمار نمی‌رود. بنابراین، اقدام قانونگذار تجارت الکترونیکی، در قائل شدن آثار و احکام اسناد رسمی برای هرگونه مدرک، سابقه یا امضای الکترونیکی و یا روگرفت آنها - بدون نیاز به گواهی و تصدیق آن «داده پیام‌ها» در مراجع مجاز مایه تعجب و ناشی از عدم دقت در ماهیت و تشریفات لازم برای رسمی بودن سند می‌باشد. (سریر و همکار، ۱۳۸۸، ۱۲)



۴- تفاوت امضای الکترونیکی و امضای دیجیتالی

در وهله اول باید تفاوت میان امضای دیجیتالی 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. از جنبه علمی در تمایز این دو به اختصار می‌توان گفت که امضای دیجیتالی نمودار داده‌ای است که به شکل یک واحد داده، الصاق یا با رمزگذاری منتقل می‌شود و به گیرنده اجازه می‌دهد تا سر منشاء و اصالت آن را تشخیص دهد. این ساختار منطقی مانع از جعل امضا می‌شود. امضای الکترونیکی دارای معنای عام‌تری است و شامل امضای دستی اسکن شده یا اسم شخص که در قسمت انتهایی نامه الکترونیکی قید می‌گردد، نیز می‌شود. برای تامین ایمنی و اصالت امضای الکترونیکی باید از امضای دیجیتالی به عنوان فناوری رمزگذاری استفاده کرد. اطلاق عبارت «امضای دیجیتالی» به فرایند فوق‌الذکر ناشی از مسامحه می‌باشد؛ زیرا هیچ شباهتی بین این نوع از تایید و «امضا» به مفهوم مصطلح آن وجود ندارد. (شهبازی نیا و همکار، ۱۳۸۸، ۲۴).

۵- مزایا و مشکلات امضای دیجیتالی

۵-۱- مزایای امضای دیجیتالی

یکی از خصوصیات اسناد تجاری الکترونیکی قابلیت حفظ آنها با حجم اندک و برای یک دوره طولانی است و در این مورد امضاهای الکترونیکی نقش مهمی ایفا می‌کنند که در بررسی ذیل بدان می‌پردازیم.

۵-۱-۱- نگهداری اسناد الکترونیکی اصیل

اولین بار موسسه استاندارد سازی اتحادیه اروپا دست به یک بررسی گسترده در مورد فعالیت‌های امضای الکترونیکی زد و اولین نتیجه این فعالیت‌ها یک گزارش کارشناسی در مورد استاندارد سازی امضاها در آینده بود. این گزارش تصدیق می‌کند که آرشیوهای ایمن نقش بسیار مهمی در پشتیبانی امضای الکترونیکی بازی می‌کنند. چنانچه ممکن است مدتها بعد از ایجاد امضا برای گواهی یا تعیین هویت به آنها نیاز شود. بنابراین فقط کافی نیست که یک سند در زمان حاضر قابل دسترسی و استناد باشد، بلکه باید برای سال‌های آینده ذخیره شود و قابل استناد گردد. به منظور قابلیت استناد آن باید گواهی‌نامه‌ای که امضاکننده از آن استفاده کرده است در زمان ایجاد امضا معتبر بوده باشد. هر چند که ممکن است مدتی از آن زمان باطل شده یا معلق شده باشد. زمان ایجاد امضا که بوسیله مهرهای زمان نگار ثبت شده‌اند ارزش بسیار مهمی در بایگانی داده‌ها ایفا می‌کنند. زیرا بوسیله این زمان بسیاری از مسایل حقوقی اثبات می‌شود. مثل اهلیت اشخاص در زمان امضای سند و یا اعتبار کلید خصوصی در همان زمان و... تمام اشخاصی که به این آرشیو مراجعه می‌کنند با مراجعه به مهرهای زمان که بر اسناد الصاق شده است از این مورد اطمینان حاصل می‌کنند. (صادقی نشاط، ۱۳۸۳، ۵۸)

در کنار اسناد الکترونیکی، امضاهای الکترونیکی نیز نگهداری می‌شوند، زیرا برای تطبیق اسنادی مطابق با اسناد ذخیره شده در آرشیو داده‌های دیجیتالی امضا قطعاً لازم است. اما این تنها شرط ممکن نیست، زیرا به هر حال داده‌های الکترونیکی تحت تاثیر گذر ایام و تغییرات فرمت‌های برنامه‌ها و بسیاری عوامل دیگر قابلیت خود را از دست داده و از بین می‌روند. بدین منظور این داده‌ها همواره باید به روزرسانی شوند. به روزرسانی این داده‌ها باید همراه با راه‌حلی باشد که مشکلات حقوقی در پی نداشته باشد. مثلاً اگر امضاکننده برای بازسازی امضا و سند سابق خویش سال‌ها بعد با یک کلید خصوصی که به روز رسانی شده امضا و



سند را به روز رسانی کند این یک مثال غیر قابل قبول در دنیای حقوق است، زیرا این یک سند جدید است که با تغییر در داده‌های سند سابق ایجاد شده است. (بختیاروند، ۱۳۸۳، ۱۴)

حتی توافقات طرفین مبادله نیز نمی‌تواند سند و امضای سابق را بدین شکل تغییر دهد. به هر حال این وظیفه علم حقوق نیست که راه‌حلی برای این مشکلات پیدا کند، اما قطعاً این راه‌ها نباید به گونه‌ای باشند که معضلات حقوقی ایجاد کنند. زیرا اولین وظیفه هر علم توسعه آرامش و آسایش انسان‌هاست. اما می‌توان گفت که سرویس دهندگان آرشیوهای الکترونیکی در نگهداری اسناد و امضاهای الکترونیکی وظایف و تعهدات خاصی دارند و از آنجا که نگهداری این امور مهم بدان‌ها واگذار شده است، باید مسئولیت هرگونه آسیب و صدمه ناشی از فعالیت و سیستم آرشیو را به اسناد، امضاها، اشخاص حقیقی و حقوقی که به آنها اعتماد نموده‌اند بپذیرند. در حقیقت این آرشیوها در حفظ و نگهداری داده‌ها تعهد دارند و برای تضمین این امر نیاز به بیمه‌های قوی دارند. در حال حاضر شاید بهترین راه برای حفظ امنیت داده‌ها در بلند مدت تولید امضاهایی با قابلیت ماندگاری طولانی باشد.

۵-۱-۲- نگهداری اسناد الکترونیکی جایگزین

یکی از مزایای مبادله الکترونیکی اسناد تجاری این است که در عین مبادله سریع، داده‌های الکترونیکی قابل چاپ و دریافت در عالم حقیقی تجارت هستند به همین منظور قانون یوتا مقرر می‌دارد: «اگر فرستنده یک سند الکترونیکی از ذخیره یا پرینت بوسیله دریافت‌کننده جلوگیری کند، آن سند علیه دریافت‌کننده سندیت نخواهد داشت». پیش‌نویس لایحه اصلاح قانون تجارت در ماده ۴۱۳ اعلام می‌دارد: «سند تجاری الکترونیکی به دو روش به وجود می‌آید. سند تجاری الکترونیکی اصل و سند جایگزین آن که منظور از سند جایگزین را در ماده ۴۱۴ قانون فوق همان سند پرینت شده می‌داند. به هر حال آنچه مورد بحث است اسنادی است که پس از دریافت از خروجی یک دستگاه الکترونیکی صادر شده‌اند. (عباسی داکانی، ۱۳۸۳، ۱۹)

نگهداری این گونه اسناد به معنای حفاظت عملی آنها برای یک مدت طولانی است. اما به راستی نگهداری این گونه اسناد که بافت الکترونیکی دارند، چگونه است؟ این اسناد کاغذی شامل داده‌های دیجیتالی هستند. پس باید با روشی امضا شده باشند که مناسب با اسناد کاغذی باشد. زیرا داده‌های دیجیتالی در بسیاری موارد بر روی کاغذ نامفهومند و تطبیق آنها دشوار و یا ناممکن است. هر چند که برخی از امضاهای الکترونیکی این خواسته را تامین می‌کنند اما در مقابل، کاستی‌های بسیاری در فضای سایبر دارند که مبادله اسناد را به خطر می‌اندازد. سیستم قانونی فعلی فقط در مورد اسناد کاغذی و ثبت و بایگانی آنها تدوین شده است، در حالی که این یک نیاز روز افزون است که نحوه ثبت و اعتبار بخشی از آنها در دنیای کاغذ به شکل قانونی بیان شود. امروزه تکنولوژی در ایجاد دستگاههایی برای حفظ داده‌های دیجیتالی پس از پرینت گام مهمی برداشته است. فناوری‌های **media sec** سیستم‌هایی را توسعه داده‌اند که در مدارک الکترونیکی که به شکل چاپ شده ظاهر می‌شوند اصالت را به ثبوت می‌رسانند. اما با تمام این موارد باز هم همان روش سنتی برابر با اصل کردن دفاتر اسناد رسمی در صورتی که یک سردفتر برای ایجاد این اسناد نظارت داشته باشد راه حل معتدلانه‌ای به نظر می‌رسد.

۶- معایب امضای دیجیتالی

توجه به توجیه حقوقی سیستم‌های الکترونیکی در امضای اسناد امر بسیار مهمی تلقی می‌شود. بنابر بند ۱۷ ماده ۲ قانون تجارت الکترونیکی ایران از جمله اشخاصی که می‌تواند صاحب امضای الکترونیکی شود، سیستم‌های رایانه‌ای تحت کنترل انسان‌ها هستند. حقیقت این است که امروزه سیستم‌های هوشمند الکترونیکی در فضای تجارت الکترونیک مورد استفاده فراوان واقع



می‌شوند. اما واضح است که با تمام هوشمندی و اطمینان از عملکرد این سیستم همواره نگرانی در مورد آنها وجود دارد. از سویی امروزه مبادلات تجاری سرعت بیشتری به خود گرفته و در دنیای تجاری کسی موفق است که گام‌های بلندتری بردارد. اشخاص حقیقی و حقوقی که داده‌ها و اسناد مهم تجاری خویش را به طور الکترونیکی مبادله می‌کنند اگر همواره در یک نگرانی دائم در مورد سرانجام مبادلات و معاملات تجاری خویش به سر برند، سرانجام راه به جایی نخواهند برد. در سیستم‌های الکترونیکی، نگرانی‌های مزبور بیشتر است. زیرا در صدور امضا بوسیله اشخاص حقیقی یا حقوقی، همواره امضاکننده یک شخص حقیقی هوشمند است که بار مسئولیت عمل خویش را به دوش می‌کشد. اما در سیستم‌های الکترونیکی این امر کمی گیج‌کننده است، به همین دلیل باید شخصی حقیقی در این مساله مسئولیت را بپذیرد. (قاجار قینلو، ۱۳۸۰، ۶۵)

۶-۱-۱- مشکلات حقوقی محتوای اسناد تجاری و امضاء داده‌های دیجیتال

اساساً مشکلات حقوقی در اسناد تجاری در سه موضوع بحث می‌شود. حریم، هویت و غیر قابل اثبات بودن معاملات. از آنجا که فضای سایبر یک فضای عمومی است و نمی‌توان کسی را از دخول به آن منع نمود، همواره وجود عوامل مخل امنیت در آن ناگزیر است. پس نیاز به یک ضریب بالای امنیت دارد تا این ایمنی را در فضای مجازی مزبور اعمال نماید.

۶-۱-۱-۱- جعل هویت

یکی از محدودیت‌های عمده فضای الکترونیکی شناخت هویت اشخاصی است که در فضای فوق مبادله می‌کنند. در بهترین وضعیت یک دستگاه هوشمند بر اساس داده‌های تجربی مشخصات شخصی را تایید می‌کند، اما از اثبات حقیقی هویت وی عاجز است. این مساله باعث جعل هویت در فضای الکترونیکی می‌گردد. بدین معنا که هر کسی می‌تواند با معرفی خود با عنوان شخصی دیگر که مورد نظر طرف مقابل است به داده‌های وی دسترسی پیدا کرده و حریم وی را نقض کند (محمدزاده، ۱۳۸۵، ۵۷).

۶-۱-۲- گمنامی در فضای سایبر

روزانه حجم بالایی از معاملات الکترونیکی به صورت گمنام اعمال می‌گردد. یعنی اشخاص کالا یا خدمتی را به طریق مذکور خریداری کرده و وجه آن را با کارت‌های اعتباری می‌پردازند. در این لاقول برای یکی از طرفین هویت واقعی طرف مقابل از اهمیت چندانی برخوردار نیست و آنچه که از هویت طرف مقابلش به او عرضه می‌شود، فقط یک رمز یا کد انتقالی است. حال سوال این است که آیا گمنامی فوق در مورد امضاها و گواهینامه‌هایی که مرجع صدور گواهینامه برای اشخاص صادر می‌کند، امکان دارد؟ پاسخگویی به این امر مستلزم بررسی حضور اشخاص و مبادلات تجاری آنها در فضا سایبر است. یعنی هرگاه ما بر یک مبادله تجاری الکترونیکی به شکل گمنام صحنه بگذاریم، در واقع موید این امر است که پاسخ سوال فوق مثبت می‌باشد. اما برای پاسخگویی به سوال فوق باید درک صحیحی از مفهوم گمنامی داشته باشیم. گمنامی به معنای مجهول بودن هویت فرد در نظر بعضی از اشخاص است و به معنای ناپیدا بودن نیست، چه بسا که شخصی در میان جمعی حضور داشته، اما ناشناخته باشد در این حالت گفته می‌شود که شخص گمنام است. باید بین درجات گمنامی تمایز قائل شویم، زیرا آثار حقوقی این درجات با یکدیگر متفاوت است: گمنامی را می‌توان به دو دسته تقسیم کرد:



۱) گمنامی مطلق، که موجب می‌شود شخص هیچ گونه رد پای از خود در ارتباطاتش به جای نگذارد، خواه این گمنامی با استفاده از یک نام مستعار باشد، خواه به طریق دیگری صورت گیرد.

۲) نیمه گمنامی، که در این حالت شخص با پشتوانه یک شخص ثالث به صورت گمنام حاضر می‌شود. یعنی در عین حال که در بین افراد خاصی گمنام است، اما هویت واقعی او به وسیله یک شخص ثالث پشتیبانی می‌گردد. (مظاهری و همکار، ۱۳۸۷، ۶۹).

۶-۱-۳- گمنامی در قراردادهای مبادلات تجاری الکترونیکی

حال با توجه به مفاهیم بالا باید دید که آیا می‌توان یک قرارداد تجاری را به طریق گمنام برقرار کرد؟ باید گفت در این حالت هم در ایجاد قرارداد و هم در اجرای قرارداد، مشکلاتی ایجاد می‌شود. بر اساس ماده ۱۹۰ قانون مدنی یکی از شرایط اساسی صحت قراردادها اهلیت است. توجیه انعقاد قرارداد به شکل گمنام، این شرط اساسی را حذف می‌کند. حمایت قانونگذار از حقوق طرفین قرارداد و همچنین اشخاص ثالثی که احتمالاً بازتاب این قرارداد به آنها نیز باز می‌گردد، این امر را منتفی می‌سازد. از طرفی شرایط اساسی صحت قراردادها قواعد آمره‌ایست که نمی‌توان بر خلاف آن توافق نمود. در قراردادهای الکترونیکی تنها شکل ایجاد قرارداد تغییر کرده است و قواعد حاکم بر آن همان قوانین حاکم بر دنیای قراردادهای هستند و اشخاص نمی‌توانند حتی با توافق از آنها تخطی نمایند و ضمانت اجرای تخطی از اهلیت، گاه بطلان و گاه عدم نفوذ قرارداد است.

از طرفی در صورتی که شخص به طور گمنام در قرارداد داخل شود، مسئولیت‌ها و تعهدات ناشی از معاهده بر چه کسی بار می‌گردد؟ در مورد قراردادهای تجاری الکترونیکی نیز الزاماً به همین تجارت حقیقی است. مثلاً اگر یک قرارداد کپی‌رایت به شکل گمنام منعقد گردد، هر کس خود را محق می‌داند که از اثر مزبور استفاده نماید و هیچ مانع قانونی نیز برای این امر وجود نخواهد داشت. با تمام این احوال، شرایطی وجود دارد که تحت آن می‌توان ایجاد قراردادهای گمنام پذیرا شد. گفتیم که گمنامی به دو شکل وجود دارد. گمنامی مطلق و نوعی گمنامی که از به نیمه گمنامی تعبیر شده است. تمام مواردی که در بالا بیان شد حالاتی است که در گمنامی مطلق اتفاق می‌افتد یعنی در شرایطی که یکی از طرفین هیچ رد پای از خود بر جای نمی‌گذارد و بدین ترتیب از منافع قرارداد بهره می‌برد بدون این که الزامات قراردادی را بتوان بر وی مستقر کرد. (قلی‌زاده، ۱۳۹۰، ۵۹) اما در حالت دوم شرایط فرق می‌کند زیرا هویت طرف قرارداد قابلیت اثبات دارد. همانگونه که هیچ مشکلی وجود ندارد اگر قرارداد بواسطه شخص ثالث معتمدی و به حساب طرفی که مایل است گمنام بماند، ایجاد گردد. پس در ایجاد قراردادهای الکترونیکی نیز می‌توان از این امر بهره گرفت. اما از آنجا که تشریفات ایجاد قراردادهای تجاری الکترونیکی در دنیای مجازی متفاوت از همتای آن در عالم حقیقی است شرایط نیز برای آن متفاوت است. قراردادهای صورت قانونی به خود نمی‌گیرند مگر این که خود قرارداد تایید و تصویب و قصد طرفین را نشان دهد یا به وسایلی بتوان به موارد ذکر شده پی برد. این شکل قانونی عموماً به وسیله امضای طرفین بوجود می‌آید. در مبادلات و قراردادهای تجاری الکترونیکی این موقعیت به وسیله امضای الکترونیکی به وجود می‌آید و این مساله ما را بر آن می‌دارد تا گمنامی را در فضای سایبر و تحت امضای الکترونیک بررسی کنیم.

۶-۱-۴- گمنامی در قرارداد امضای الکترونیک

اشخاص برای دریافت کلید خصوصی امضا و گواهینامه معتبر باید از مراجع صدور گواهی، درخواست گواهینامه کنند. مراجع دیگری تحت نظارت این مراجع وجود دارند تحت عنوان مراجع ثبت‌نام که وظیفه احراز هویت و ثبت هویت درخواست کنندگان را دارند. احراز هویت توسط این مراجع به سطح گواهینامه‌های درخواستی بستگی دارد. هر چه گواهینامه‌ها از نظر اهمیت در سطح



بالانتری قرار داشته باشند، سخت‌گیری و دقت بیشتری نسبت به احراز هویت اعمال می‌گردد. پس از احراز هویت بوسیله مرجع ثبت نام، قرارداد امضای الکترونیکی بین مرجع صدور گواهینامه و شخص درخواست‌کننده امضا بسته می‌شود. سوال این است که آیا امکان انعقاد این قرارداد به صورت گمنام وجود دارد یا خیر؟ شاید در نظر اول این طور به نظر بیاید که با وجود مراجع ثبت نام چنین امری منتفی است، اما باید در نظر داشت که مراجع ثبت نام فقط در سطوح بالای گواهینامه اقدامات دقیق و سخت‌گیرانه اعمال می‌کنند و در سطوح پایین تر حتی گاهی ابرازات شخصی درخواست‌کننده برای ثبت نام کفایت می‌کند. همیشه این احتمال وجود دارد که متقاضی صدور گواهینامه، یک هویت مستعار برای خود اعلام کند و با پذیرش این امر از سوی مرجع ثبت نام قرارداد امضای الکترونیکی منعقد گردد. در این حالت چون عمل شخص متقاضی تخطی از قاعده آمره لزوم ابراز حقیقت در زمان ثبت نام می‌باشد، پس قرارداد مذکور باطل و دارنده امضای باطل شده مسئولیت جبران همه خسارات ناشی از عمل خود را نسبت به مراجع صدور گواهینامه و سایر اشخاص که در اثر عمل وی متحمل خسارت شده‌اند بر عهده دارد. پس انعقاد قرارداد امضای الکترونیکی در حالت گمنامی منتفی است. (زرگر، ۱۳۸۶، ۴۷).

۶-۱-۵- گمنامی در گواهینامه‌های الکترونیکی

گواهینامه‌ها داده‌های الکترونیکی هستند که حاکی از هویت اشخاص و گاهی میزان اعتبار و وابستگی آنها به مراجع خاص و نشان دهنده صلاحیت ویژه اشخاص می‌باشند. اغلب اشخاص برای انعقاد قراردادهای تجاری و مبادله اسناد تجاری خود برای این که طرف مقابل خود را بشناسند از مرجع صدور گواهینامه درخواست گواهینامه وی را می‌نمایند تا بدین ترتیب از هویت وی اطمینان حاصل نمایند. واضح است که گواهینامه نمی‌تواند کاملاً مبهم باشد، یعنی هیچ گونه اطلاعاتی از شخص دارنده امضا در خود نداشته باشد یا همه اطلاعات آن مستعار باشد. زیرا این امر نقض غرض است که ماهیت واقعی صدور گواهینامه را زیر سوال می‌برد. اما به نظر می‌رسد اگر تنها نام حقیقی و اطلاعات شخصی وی مستعار باشد در صورتی که خود مرجع گواهینامه بر آن مطلع است ایرادی بر آن وارد نباشد. زیرا اطلاعاتی را که مرجع فوق در حالت عادی مجاز به افشای آن شده است در حالات اضطراری مثلاً در مورد الزام به تعهد ناشی از قرارداد به طریق قانونی ملزم به افشای آن است. پس در این مورد خللی به قرارداد وارد نمی‌کند و این امر در مورد مبادلات اسناد نیز وجود دارد. در مورد ابهامات خاص دیگری که ممکن است در گواهینامه وجود داشته باشد در صورتی که هر شخص ثالث معتمدی آنها را تضمین نماید و با وجود این تضمین قرارداد منعقد شده یا سندی مبادله گردد، شخصی که به اتکای تایید وی عمل حقوقی مزبور انجام شده ضامن صحت مبادله یا قرارداد و سایر مواردی که ناشی از تضمینات وی است، می‌باشد. اما با تمام این احوال توافق طرفین می‌تواند شرایط فوق را از بین ببرد یا اگر قانونگذار امر به تصریح شناسایی کرده باشد دیگر نمی‌توان با یک نام مستعار وارد مبادله یا قرارداد شد. مثلاً ماده ۳۵ قانون تجارت الکترونیکی بیان می‌دارد: «فروشنندگان کالا و ارائه‌کنندگان خدمات بایستی اطلاعات موثر در تصمیم‌گیری مصرف‌کنندگان جهت خرید و یا قبول شرایط را از مان مناسب قبل از عقد در اختیار مصرف‌کنندگان قرار دهند. حداقل اطلاعات لازم شامل موارد زیر است:

۱) هویت تامین‌کننده، نام تجاری که تحت آن نام به فعالیت مشغول است و نشانی وی؛

۲) آدرس الکترونیکی، شماره تلفن و یا هر روشی که مشتری در صورت نیاز بایستی از آن طریق با فروشنده ارتباط برقرار کند. بنابراین فروشنندگان کالا و خدمات، مثل بیمه‌گذاران، الزاماً باید با گواهینامه‌هایی در عرصه سایبر به فعالیت مشغول گردند که تصریح به شناسایی کامل آنها داشته باشد. (ماده ۱۳ قانون تجارت الکترونیکی).



۶-۲- مشکلات حقوقی ناشی از روند امضای دیجیتال

توجه به توجیه حقوقی سیستم‌های الکترونیکی در امضای اسناد امر بسیار مهمی تلقی می‌شود. بنابر بند ۱۷ ماده ۲ قانون تجارت الکترونیکی ایران از جمله اشخاصی که می‌تواند صاحب امضای الکترونیکی شود، سیستم‌های رایانه‌ای تحت کنترل انسان‌ها هستند. حقیقت این است که امروزه سیستم‌های هوشمند الکترونیکی در فضای تجارت الکترونیک مورد استفاده فراوان واقع می‌شوند. اما واضح است که با تمام هوشمندی و اطمینان از عملکرد این سیستم همواره نگرانی در مورد آنها وجود دارد. از سویی امروزه مبادلات تجاری سرعت بیشتری به خود گرفته و در دنیای تجاری کسی موفق است که گام‌های بلندتری بردارد. اشخاص حقیقی و حقوقی که داده‌ها و اسناد مهم تجاری خویش را به طور الکترونیکی مبادله می‌کنند اگر همواره در یک نگرانی دائم در مورد سرانجام مبادلات و معاملات تجاری خویش به سر برند، سرانجام راه به جایی نخواهند برد. در سیستم‌های الکترونیکی، نگرانی‌های مزبور بیشتر است. زیرا در صدور امضا بوسیله اشخاص حقیقی یا حقوقی، همواره امضاکننده یک شخص حقیقی هوشمند است که بار مسئولیت عمل خویش را به دوش می‌کشد. اما در سیستم‌های الکترونیکی این امر کمی گیج‌کننده است، به همین دلیل باید شخصی حقیقی در این مساله مسئولیت را بپذیرد. (السان، ۱۳۸۳، ۲۵)

۶-۲-۱- مسئولیت ناشی از اشکالات سیستم

در سیستم‌هایی که عملاً به طور الکترونیکی از جانب اشخاص حقوقی امضا می‌کنند همواره نگرانی‌های خاصی وجود دارد. در این سیستم‌ها گواهی‌نامه الکترونیکی برای کلیدی که بوسیله سیستم استفاده می‌شود، صادر شده و برای سیستم یا شخص حقوقی صادر نشده است. در این سیستم‌ها همواره شخصی مسئول کنترل وظایف سیستم و حراست از ایمنی آن می‌باشد و حتی نمی‌توان گفت که گواهی‌نامه فوق برای شخص مسئول صادر شده باشد. در صدور گواهی‌نامه‌های اشخاص حقیقی همیشه شخص مالک کلید در امضاها خود مسئول است، اما در اینجا مشکل این است که سیستم را نمی‌توان مسئول در صدور امضاها تلقی کرد. اما بالاخره در هر سازمان باید کسی مسئول نظارت بر دستگاه‌های تولید امضا باشد. این مساله بار سنگینی بر دوش این اشخاص حقیقی خواهد گذاشت، اما در این زمینه می‌توان میزان مسئولیت اشخاص را بر اساس کیفیت دستگاه‌ها ارزیابی نمود تا این مسئولیت قدری محدود تر گردد. یعنی زمانی شخص حقیقی ناظر بر سیستم را مسئول مطلق بدانیم که امنیت دستگاهها و کارایی آنها توسط کارشناسان خبره تامین شده باشد. (شهبازی نیا و همکار، ۱۳۸۸، ۵۷)

۶-۲-۲- مسئولیت ناشی از امضاهای غیر مجاز

کلید خصوصی امضا، نرم‌افزاری است که بر روی یک دستگاه پردازنده ذخیره شده است. فاکتورهای گوناگون ممکن است موجب کپی برداری از کلید یا استفاده غیر قانونی اشخاص غیر مجاز از کلید شود. مثلاً در یک ارتباط نا امن برخط یا در صورت عدم کنترل یا عدم دقت در کنترل کلید این احتمالات به حقیقت نزدیک می‌شوند. حال سوال این است که اگر شخصی با دستیابی به دستگاه به هر طریق از کلید سوءاستفاده کند، مسئولیت این امر به عهده کیست؟ سارق یا سوءاستفاده‌کننده از کلید یا شخص حقیقی ناظر بر سیستم؟ قطعاً نمی‌توان گفت تنها مسئول این امر شخص ناظر بر سیستم است اما آن چه که موضوع را پیچیده می‌کند، این است که کلیدهای خصوصی امضا به ندرت بوسیله دستبرد فیزیکی از دستگاه‌های حامل سرقت می‌شوند، بلکه اغلب سارقین به دنبال فرصت هستند تا در یک ارتباط نا امن یا از لحظه‌های غفلت استفاده کرده و عمل خود را انجام دهند و در اغلب قریب به اتفاق موارد هیچ ردپایی از شخص سارق بر جا نمی‌ماند. چه کسی می‌تواند با اطمینان ابراز کند که سارق در فضای لایتنهای سارقین سایبر، چه کسی است؟ اما به هر حال بهترین راه حل برای بالا بردن ضریب ایمنی در کنترل کلید این است که



شخص ناظر بر سیستم را همانند یک مالک کلید در حفظ کلید خصوصی دستگاه مسئول بدانیم و صد البته این مسئولیت زمانی شکل قانونی دارد که ضریب ایمنی دستگاهها از قبل کنترل شده و در اختیار شخص مزبور قرار گرفته باشد. (حسن پور، ۱۳۸۳، ۵۸).

۷- نتیجه گیری :

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

حقوق ایران همانند بسیاری از کشورهای دنیا ناگزیر از ایجاد راهکارهای حقوقی مناسب برای به رسمیت شناختن فناوری امضای الکترونیکی و امضای دیجیتال است. طرح تجارت الکترونیکی، علی‌رغم کاستیهای قابل توجهش، گام مهمی در این زمینه محسوب می‌شود. این قانون، ضمن تعریف امضای الکترونیکی ساده و مطمئن، جایگاه این امضا و داده‌های منضم به آن را در چارچوب ادله سنتی اثبات دعوا مشخص کرده است.

اما تا زمانی که راهکارهای قانونی مناسب پیش‌بینی نشده‌اند اعتباری که محاکم برای توافقات خصوصی در باب دلایل الکترونیکی خواهند شناخت از اهمیت ویژه‌ای برخوردار خواهد بود. در این خصوص، علی‌رغم محدودیتی که حقوق ایران بر سر راه توافق در باب دلایل ایجاد می‌کند، قراردادهای خصوصی تا جایی که به استفاده از فناوری امضای الکترونیکی به عنوان یکی از طرق اثبات روابط حقوقی مربوط می‌شود اصولاً باید معتبر شمرده شود و محاکم نباید دلایل مرتبط با این گونه توافقات را صرفاً به دلیل قالب انفورماتیکی آن یا ایجادشان در یک محیط الکترونیکی و مجازی مردود بشمارند. البته میزان اعتبار و ارزش حقوقی این دلایل از نظر قضات به نحو انکارناپذیر، بستگی به قابل اطمینان بودن آنها با توجه به روشهای تولید و نگهداری داده‌های مرتبط با امضای الکترونیکی خواهد داشت. اگر این روشها به نحو اطمینان بخش، دوام،

منحصر به فرد بودن، تمامیت و غیر قابل خدشه دار بودن امضای الکترونیکی و داده‌های منضم به آن و نیز هویت طرفین مبادله را تضمین کنند، موجبی نخواهد داشت که دادرسان این داده‌ها را در مقام دعوا یا دفاع نپذیرند. البته تردید نیست که تعیین میزان دلالت امضای الکترونیکی و داده‌های مرتبط با آن، همچنین رفع تعارض احتمالی آنها با دلایل سنتی همواره در اختیار قضات قرار خواهد داشت.

منابع

- ۱-السان، مصطفی، جایگاه امضای دیجیتالی در ثبت اسناد به شیوه الکترونیکی، ماهنامه کانون وکلای مرکز، سال چهل و هفتم، دوره دوم، اسفند ۱۳۸۳، شماره ۵۵
- ۲-باقرزاده، فاطمه و سلیمانی، منصور، امضای دیجیتال و هویت مجازی، فصلنامه ره آورد نور، پاییز ۱۳۸۸، شماره ۲۸
- ۳-بختیاروند، مصطفی، مطالعه تطبیقی مقررات حاکم بر داد و ستدهای الکترونیکی، مجموعه مقالات ۴-همایش بررسی جنبه های حقوقی فناوری اطلاعات، معاونت و توسعه قضایی قوه قضایی، ۱۳۸۳
- ۵-بختیاروند، مصطفی، ماهیت و جایگاه مرکز گواهی ریشه در تراکنش های الکترونیکی، فصلنامه مجلس و راهبرد، تابستان ۱۳۸۶، شماره ۵۵
- ۶-جمالزاده بها آبادی، طیبه، اعتبار و آثار حقوقی اسناد الکترونیکی در قراردادهای بین المللی، پایگاه نشر مقالات حقوقی حق گسترجمالی نیا، خدیجه، ماهیت حقوقی امضای الکترونیکی در اسناد تجاری، مجله علمی تخصصی کانون وکلای دادگستری منطقه فارس دوره سوم، زمستان ۱۳۸۶، شماره ۶
- ۷-جهانگرد محبوب، امیر، رمزنگاری نامتقارن گواهی امضای الکترونیکی معبر تجارت الکترونیک، مجله کانون، مرداد ۱۳۸۹، شماره ۱۰۷
- ۸-حسن پور، محمد مهدی، بررسی ماهیت حقوقی حق امتیاز شرینگ رپ، مجموعه مقالات همایش بررسی جنبه های حقوقی فناوری اطلاعات معاونت حقوقی و توسعه قضایی قوه قضائیه، ۱۳۸۳
- ۹-زرکلام، ستار، امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوا، مجله مدرس علوم انسانی، بهار ۱۳۸۲، شماره ۲۸
- ۱۰-زرگر، محمود، امنیت در تجارت الکترونیکی، فصلنامه مجلس و راهبرد، تابستان ۱۳۸۶، شماره ۵۵
- سریر افراز، محمد و فهیمی فر، فاطمه، امضای الکترونیکی بسترساز کاهش جرم در تجارت الکترونیکی، پاییز ۱۳۸۸، شماره ۸
- ۱۱-شهبازی نیا، مرتضی و عبدلهی، محبوبه، احراز اصالت در اسناد الکترونیکی، مجله مدرس علوم انسانی، زمستان ۱۳۸۸، شماره ۶۳
- ۱۲-صادقی نشاط، امیر، تحلیل حقوقی جنبه‌هایی از پرداخت الکترونیک، مجموعه مقالات همایش بررسی ابعاد حقوقی فن‌آوری اطلاعات، خرداد ۱۳۸۳
- ۱۳-عباسی داکانی، خسرو، گفتاری در باب ضرورت انجام تصدیق امضا در دفاتر اسناد رسمی، ماهنامه حقوقی کانون سردفتران و دفتریاران، ۱۳۸۳، شماره ۵۳
- ۱۴-قاجار قیونلو، سیامک، تجارت الکترونیک و جرائم مرتبط با آن، مجموعه مقالات اولین همایش تخصصی بررسی جرائم رایانه‌ای، تهران معاون آگاهی ناجا، ۱۳۸۰
- ۱۵-قاجار قیونلو، سیامک، امنیت امضای دیجیتالی چگونه حفظ می شود؟، دو ماهنامه بررسی های بازرگانی، اردیبهشت ۱۳۷۸، شماره ۱۴۱
- ۱۶-قلی زاده، احد، تحلیلی بر اعتبار امضا در حقوق تجارت الکترونیکی، دو ماهنامه بررسی های بازرگانی، فروردین و اردیبهشت ۱۳۹۰، شماره ۴۶

- ۱۷- کیانی سرکله، مائده و فکری، یاسر و فیروزخواه، رضا، بررسی امنیت امضای الکترونیکی و مشکلات حقوقی آن، اولین همایش تخصصی علوم، فناوری و سامانه های مهندسی برق، مهرماه ۱۳۹۲، دانشگاه پیام نور استان تهران
- ۱۸- محمدزاده، محمود، تجارت الکترونیک و امضای الکترونیک، ماهنامه کانون سردفتران و دفتریاران، ۱۳۸۵، شماره ۶۲
- ۱۹- مظاهری، رسول و ناظم، علیرضا، ارزش اثباتی داده پیام و امضای الکترونیکی، نشریه نامه مفید، ۱۳۸۷، شماره ۷۰
- ۲۰- مظاهری، رسول و ناظم، علیرضا، ماهیت و آثار امضای الکترونیکی در حقوق ایران و مقررات آنسیترال، مجله کانون وکلا (وابسته به کانون وکلای دادگستری مرکز)، آبان ۱۳۸۷، شماره ۸۶