اعتبارسنجی اسناد الکترونیک

امیر صادقی نشاط *

(تارخ دریافت: ۱۳۹۳/۹/۱ – تاریخ پذیرش: ۱۳۹۳/۱۱/۲)

چکیده

گرچه قانون تجارت الکترونیکی (۱۳۸۲) و حتی قانون جرایم رایانه‌ای (۱۳۸۹) اصل اعتبار اسناد الکترونیک را تأیید کرده و مشکلی از این لحاظ در استناد به اینگونه ادله نیست، ولی در عین حال این مطلب از چند جهت قابل بررسی است. اول، از نظر ماهیت و در نتیجه حوزه شمول عنوان سندیت به آنها، دوم به لحاظ کم و کیف مواد قانونی مربوط و نقاط قوت و ضعف آنها. سوم، ناتوانی سطح فن‌آوری در پاسخ‌گویی به استانداردهای دقیق حقوقی در اصالت سند در برابر کپی .مقاله حاضر به هر سه مطلب فوق خواهد پرداخت و پیشنهادهایی را نیز برای اصلاح قانون ارائه خواهد داد.

کلید واژگان: ادله اثبات، سند الکترونیک، امضای الکترونیک، اصالت سند.

---

* دانشیار گروه حقوق دانشگاه تهران asneshat@ut.ac.ir

مقدمه

- ماهیت سند الکترونیک

علی‌رغم گذشت بیش از شصت سال از ظهور رایانه و به‌ویژه رواج عمومی آن با پیدایش نوع شخصی و علی‌الخصوص با فراگیر شدن اینترنت در ده پانزده ساله اخیر، هنوز مسائل حقوقی مربوط به عتبار سنجی اسناد یا سوابق رایانه‌ای از حوزه بحث‌های روز حقوق‌دانان خارج نشده و به جهت گستردگی و اهمیت موضوع همچنان حتی در کشور آمریکا که توان و سابقه‌ای بیش از دیگران در فن‌آوری اطلاعات دارد، مورد بحث و تحقیق قرار دارد (Federal Bar Association, 2014).

قانون مدنی طی ماده ۱۲۵۸ ادله اثبات دعوی را در ۵ قسم یعنی اقرار، اسناد کتبی، شهادت، امارات و قسم برشمرده[1] و در ماده ۱۲۸۴ سند را چنین تعریف کرده است: «سند عبارت است از هر نوشته که در مقام دعوی یا دفاع قابل استناد باشد». مواد بعدی در بیان احکام، ارزش و جایگاه سند است. قانون تجارت الکترونیکی نیز در مواد ۶ تا ۱۲ به جایگاه و ارزش اثباتی ادله الکترونیک در قالب «داده‌پیام» پرداخته و پس از آنکه آن را در ماده ۲ اینگونه تعریف نموده است: «هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فن‌آوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود»، در مواد بعدی به ارزش آن به‌عنوان دلیل و معادل نوشته پرداخته و در ماده ۶ مقرر می‌دارد: «هرگاه یک نوشته از نظر قانون لازم باشد، داده‌پیام در حکم نوشته است» و در ماده ۱۲ به‌طور کلی می‌گوید: «اسناد و ادله ممکن است به صورت داده پیام باشد...». در ماده ۵۰ قانون جرایم رایانه‌ای نیز بدون آنکه وصف خاصی برای محتوای حافظه رایانه در نظر بگیرد آن را با وجود شرایطی قابل استناد یعنی دلیل شناخته است: «چنانچه داده‌ای رایانه‌ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده باشد و سیستم رایانه‌ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشده باشد، قابل استناد خواهد بود».

اگر قائل به احصاء ادله اثبات دعوی به آنچه قانون مدنی ذکر کرده است باشیم (فیضی چکاب، ص ۱۷۶)، در آن صورت داده پیام مستقل از اقسام ادله به نحو مذکور نخواهد بود و

۱. برخی بیان قانون مدنی را احصاء نمی‌دانند (جعفری لنگرودی، ۱۳۷۲، ص ۳۰۹)، برخی بدون اظهار نظر در این خصوص، در شرح خود از قانون مدنی پیروی کرده‌اند (امامی، ج ۶، ۱۳۴۶، ص ۲۲).

چیزی از این نظر به آنچه در قانون مزبور آمده است نمی‌افزاید و تنها شکل ظاهری ادله را در مرحله ارائه بیان می‌کند. اما اگر احصاء را نپذیریم، در آن صورت اولاً مشمول تعاریف علمی از دلیل که برای احتجاج در مقابل دیگری است (مظفر، محمدرضا، ج۲، ص۱۲) خواهد بود و عنوان کلی مذکور در ماده ۱۹۴ قانون آیین دادرسی مدنی نیز بر آن صدق خواهد کرد، و ثانیاً می‌تواند گونه‌ای مستقل از دلیل و در کنار ادله پنج‌گانه قانون مدنی به حساب آید.

اینک بحث در این است که گرچه دلیل یا سند به‌طور خاص ممکن است به صورت داده‌پیام باشد، ولی آیا این خود محتوای حافظه رایانه است که دلیل به‌طور کلی، یا سند به طور خاص یا در حکم آن تلقی می‌شود یا آنچه چاپ و یا روی صفحه نمایشگر آشکار می‌گردد؟ آیا محتوای رایانه، «نوشته» محسوب می‌شود تا مشمول تعریف قانونی و عرفی از سند و احکام آن بشود یا آنکه ولو دلیل باشد، سند نیست؟

آنچه در تعریف قانون مدنی ملاک سندیت قرار گرفته عبارت است از «مکتوب» و «قابل استناد»[1] بودن دلیل[2]، که اعم است از آنکه روی کاغذ باشد یا روی پوست یا حامل دیگر. امّا آیا تراشه‌های رایانه را می‌توان حاملی در ردیف کاغذ یا سایر حامل‌ها محسوب کرد و محتوای آن را به‌عنوان نوشته به حساب آورد؟ سؤال دیگر این است که آیا سند الکترونیک در حد اطمینان‌آوری قابل انتساب به صادر کننده آن هست یا خیر؟

عامل سومی نیز برای اعتبار داده‌پیام در قانون تجارت الکترونیکی به تقلید از قانون نمونه آنسیترال در تجارت الکترونیک (UNCITRAL Model Law on Electronic Commerce-1996) ذکر شده که عبارت است از تناسب مفاد و هدف از داده‌پیام با روش‌های موجب اطمینان و ایمنی سامانه. این ملاک، از نظر علمی قابل بحث است و در حقوق ما به این صورت، حتی در اسناد کاغذی، جای تأمل دارد.

داده‌پیام معمولاً در پنج قالب قابل مشاهده است: اطلاعات وبگاه، مفاد شبکه‌های اجتماعی، پست الکترونیک (رایانامه)، پیام‌های الکترونیک و ذخیره‌های رایانه‌ای (Pendleton, Hon Alan, 2013, P.1). در تمام انواع فوق، وظیفه محاکم کشورها خواهد بود که به کمک کارشناسان

---

۱. برخی بزرگان نوشته و امضا داشتن را ارکان سند ذکر کرده‌اند (کاتوزیان، ج۱، ۱۳۸۷، ص ۲۷۷).

۲. اینجا ما از مباحث مربوط به دلالت سند که تفاوتی در نوع الکترونیک با غیر آن نیست، فارغیم. بنا بر این، در بحث قابلیت استناد، صرفاً به امور شکلی و قابلیت انتساب سند الکترونیک به صادرکننده آن، اکتفا خواهیم کرد.

فنی، میزان مصداق داشتن معیارهای اعتبار ادله اثبات در حقوق خود را در این دلیل نوین احراز کنند و معیارهای اعتبار سنجی را در آنها اعمال نمایند.

مبحث اول- نوشته محسوب شدن داده‌پیام

۱- ماهیت داده‌پیام

اگرچه آن هنگام که محتوای حافظه به روی صفحه نمایش یا کاغذ منتقل می‌شود، به صورت نوشته است ولی روشن است که آن خروجی‌ها اصالت ندارند و تنها نشانگر محتوای حافظه رایانه هستند. آنچه در حافظه موقت (RAM) یا دائم ذخیره می‌شود، به‌صورت نوشته نیست و صرفاً حاصل تأثیراتی است که اختلاف ولتاژ برق روی مواد نیمه هادی که تراشه‌ها را تشکیل می‌دهند باقی می‌گذارد. درست است که هنگام کار با رایانه، علائم و کلمات انسانی تحت عنوان داده (DATA) وارد ماشین می‌شوند، ولی به محض فشار روی کلید، یا هر وسیله دیگر، آنچه به داخل دستگاه منتقل می‌شود جریان‌های متفاوت برق و نحوه قرارگرفتن آثار آنها در کنار هم است که در هر حرف و علامتی با دیگری تفاوت می‌کند[۱]. لذا آنچه روی تراشه یا دیسکت ذخیره می‌شود، هیچ شباهتی به ورودی‌ها ندارد و قابل درک توسط انسان نیست. در این صورت، روشن است که مادام که اطلاعات به صورت ذخیره‌های الکترونیک باشند، عرفاً نمی‌توانند به عنوان «نوشته» محسوب شوند.

بدین ترتیب از یک طرف صفحه چاپ شده یا نمایشگر اصالت ندارند و مستقلاً سند محسوب نمی‌شوند و از طرف دیگر کیفیت موجود در تراشه رایانه هیچ شباهتی به نوشته ندارد. برای رفع معضل اعتبار بخشی به این وقایع خارجی، آنهم تحت عنوان یا معادل سند، نمی‌توان آن را به تفسیرهای گوناگون علمی و قضایی واگذار کرد. ممکن است بعضی، بر مبنای قول به عدم احصای ادله در ماده ۱۲۵۸ ق‌م، عنوان مستقلی در ادله برای آن قائل شوند که بیراه نیست[۲]. حقوق کشورها بایستی موضعی شفاف و یکنواخت در این خصوص اتخاذ کنند و ارزش‌گذاری اثباتی چنین امر

---

۱. در برنامه نویسی از آنها به ۰ و ۱ تعبیر می‌کنند ولی بدیهی است که در تراشه رایانه اینگونه نیست. هر علامتی که وارد رایانه می‌شود ترکیبی از وجود و عدم برق است که هر کدام یک Bit و ترکیب آنها یک Byte را تشکیل می‌دهد که اختصاص به همان علامت وارد شده به رایانه دارد.

۲. در اسناد بین‌المللی نظیر قانون نمونه آنسیترال از آن به عنوان دلیل الکترونیک (Electronic evidence) تعبیر شده که اعم از سند (Document/Deed/Writing) و غیر آن است.

مهمی را که مبتلابه جهان امروز است، به تنوع تفسیر و تشتت آرای محاکم نسپارند. به همین سبب قانون‌گذاران کشورها با روش‌هایی متناسب با ساختار حقوقی خود و بعضاً به صورت اقتباس از برخی نمونه‌های خارجی یا بین‌المللی، اقدام به پر کردن خلأ مزبور در قوانین خویش کرده‌اند. فرانسوی‌ها آن را در قانون مدنی صراحتاً سند نامیده‌اند و در آمریکا در قانون یوتا (Uniform Electronic Transactions Act-1996) از آن به عنوان سوابق الکترونیک (Electronic record) یاد کرده‌اند و در قانون قواعد ادله فدرال (Federal Rules of Evidence -2014) در ماده ۱۰۰۱ این نوع دلیل را به همراه سایر موارد به شرح زیر تعریف نموده‌اند:

نوشته(Writing) عبارت است از حروف، کلمات، اعداد، یا معادل آنها که به هر شکلی ذکر شود.

سابقه (Recording) عبارت است از حروف، کلمات، اعداد یا معادل آنها به هر شکلی که ضبط شده باشد. در بند۷ ماده ۲ قانون یوتا نیز سابقه الکترونیک اینگونه تعریف شده است: «سابقه‌ای است که با وسایل الکترونیک ایجاد، تولید، ارسال، ایصال، دریافت یا ذخیره شده باشد».

در تعریف قانون نمونه از داده‌پیام، طیف نسبتاً وسیعی از اطلاعات که به طرق گوناگون الکترونیک، نوری یا وسایل مشابه تولید، ارسال، دریافت و ذخیره می‌شوند مانند، و نه محدود به مبادلات استاندارد داده‌ها بین رایانه‌ها ، پست الکترونیک، تلکس، تلگراف، و غیره، مشمول این عنوان می‌شوند.

پس از تعریف فوق، قانون نمونه در بند ۱ ماده ۶ چنین مقرر داشته است: «۱- هرگاه قانون لازم بداند که اطلاعاتی به صورت کتبی باشد، آن اقتضاء در داده‌پیام، درصورتی‌که استفاده از اطلاعات موجود در آن برای مراجعات بعدی میسر باشد، برآورده خواهد شد. ۲- بند ۱ در هر دو موردی که محتوای داده‌پیام را یک تعهد تشکیل داده یا آنکه قانون صرفاً پی‌آمدهایی را برای نبود نوشته مقرر کرده باشد، قابل اعمال خواهد بود. ۳- مقررات این ماده در موارد زیر اعمال نمی‌شود [...]».

اما قانون تجارت الکترونیک ایران، ابتدا در ماده ۲ داده‌پیام را با قدری تفاوت تعریف کرده که علی‌رغم ابهامات، دایره شمول آن محدودتر است و از این نظر مناسب‌تر به‌نظر می‌رسد: «هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری یا

فن‌آوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود» و سپس در صدر ماده ۶ مقرر می‌دارد: «هرگاه وجود یک نوشته از نظر قانون لازم باشد، داده‌پیام در حکم نوشته است...» و در ادامه استثنائاتی را نیز بیان می‌کند.

نکته‌ای وجود دارد که می‌توان آن را به‌عنوان نقد عبارات هر دو قانون و البته با تفاوت در شدت و ضعف مطرح کرد. در هر دو متن می‌گوید «هرگاه وجود یک نوشته از نظر قانون لازم باشد، ...». مفهوم این عبارت این است که هرگاه قانون لازم نداند، داده‌پیام در حکم نوشته نیست و این اعتبار را نخواهد داشت. این در حالی است که نوعاً در اسنادی که مردم صادر می‌کنند، الزام قانونی وجود ندارد و مردم خودشان برای حفاظت از حقوق خویش اقدام به کتبی کردن تعهدات می‌کنند. درست است که در برخی موارد نظیر رانندگی، این قانون است که وجود سندی به نام گواهینامه را که کتبی است لازم دانسته است و یا در امثال چک و سفته، کتبی بودن را جزء شرایط ماهوی آنها ذکر می‌کند، ولی این‌طور نیست که همه اسناد با الزام قانونی تنظیم شوند یا قانون‌گذار کتبی بودن دلیل را لازم دانسته باشد.

مسلماً منظور قانون‌گذار این نبوده است که اسناد عادی مردم درصورتی‌که الکترونیک باشند ولی قانون آن را الزامی ندانسته باشد، نوشته محسوب نمی‌شوند، ولی به هر حال ظاهر عبارات ذکر شده دارای چنین مفهومی هست. البته در قانون نمونه، با اضافه شدن بند ۲ به ماده ۶ تا اندازه‌ای ایراد مزبور تعدیل شده ولی چون در قانون ایران آن قسمت ترجمه نشده، ایراد فوق جدی‌تر است.

۲- ارزیابی ویژگی‌های نوشته در داده‌پیام

سه خاصیت در حد نسبتاً بالایی در نوشته‌های کاغذی وجود دارد:

اول، ثبات یا تغییر ناپذیری محتوای سند. این خاصیت در حدی است که معمولاً تغییرات یا تراشیدگی در سند آشکار می‌شود.

دوم، بقا و دوام دلیل برای مراجعات بعدی. این ویژگی نیز متناسب با جنس کاغذ و شرایط نگه‌داری، برای مدت‌های طولانی برای اسناد کاغذی وجود دارد.

سوم، تفاوت نسخه تکثیر شده با نسخه اصلی. این ویژگی امروزه با ظهور دستگاه‌های نسخه‌برداری با کیفیت بالا، کمرنگ شده ولی قابل تشخیص است.

هر قدر وجود عوامل فوق در سندی قوی‌تر و اطمینان بخش‌تر باشد، آن سند از درجه اعتبار بیشتری برخوردار خواهد بود.

۱-۲- ثبات سند

مقصود، عدم تغییر و محفوظ ماندن تمامیت (Integrity)است. در قانون نمونه آنسیترال از کلمه (Originality) استفاده شده است. کلمه مزبور در هر دو معنای مزبور، و نیز اصل در برابر کپی استعمال می‌شود. از آنجا که مقصود قانون نمونه و ما در این مبحث همان معنای اول است، لذا برای جلوگیری از خلط مطالب، از اصطلاح «ثبات» استفاده می‌کنیم و درخصوص اصالت به معنای دوم، بحث جداگانه‌ای را خواهیم داشت.

درحالی‌که ثبات در اسناد ملموس مانند کاغذی، چوبی، سنگی و امثال آنها راحت‌تر حاصل می‌شود و معمولاً اعمال هرگونه تغییری در آنها اولاً دشوار است و ثانیاً بهتر قابل کشف است، این امر در داده‌پیام بدون تمهیدات خاص قابل حصول نیست و امکان تغییرات در مندرجات آنها به دفعات و بدون آن‌که نشانه و اثری ازخود باقی بگذارند، وجود دارد. ایمنی سامانه‌ها در برابر تغییرات از سوی اشخاص بیگانه نیز همواره از مسائل اصلی و نگرانی‌های مطرح در ارائه خدمات به ویژه آنهایی بوده است که مانند بانک‌داری از حساسیت فراوان برخوردارند (Gkoutzinis, P. 150).

از طرف دیگر، معمولاً اسناد کاغذی توسط خود افراد یا تحت نظارت نزدیک آنان تنظیم و مبادله می‌شوند در حالیکه در داده‌پیام، اشخاص و تجهیزاتی دخالت دارند که معمولاً همه آنها تحت نظارت و پایش مستقیم صادرکنندگان سند نیستند. بدین‌ترتیب لازم است ثبات محتوای سند پس از تولید و طی زمان ارسال تا وصول و ذخیره، با اعمال نمودن روش‌های فنّی اطمینان‌بخش، به نحو قابل قبولی تأمین شود (Stephen Mason,2014).

گرچه، همان‌طور که نشان خواهیم داد، با تمهیدات لازم فنی، داده‌پیام می‌تواند حتی از ضریب اطمینان بالاتری نسبت به اسناد کاغذی برخوردار باشد. ولی در هر حال هروقت سخن از شبکه باشد، ایمنی آن قطعی نیست و علی‌رغم روش‌ها و استانداردهای فنی زیاد، همواره امکان نفوذ عوامل بیگانه به داخل شبکه و تهدیدات نسبت به آن وجود دارد (Tanenbaum, pp. 772-805).

در حقوق آمریکا, اعتبار سوابق الکترونیک منوط به وجود شرایط ذیل دانسته شده است:

الف- اطمینان‌بخش و استاندارد بودن تجهیزات رایانه‌ای.

ب- ورود داده‌ها به سامانه مطابق روال معمول تجارت و در زمانی نزدیک به واقعه توسط افرادی که از آن اطلاع دارند.

ج- چاپ شدن نسخه کاغذی به روشی اطمینان بخش (Reed, 2007 p.216).

بندهای ۱و ۲ ماده ۱۳۱۶ قانون مدنی فرانسه نیز، لزوم وجود اطمینان در صدور و ثبات سند را صرف نظر از قالب آن مورد توجه قرار داده است[1].

---

۱. تدبیری در قانون‌گذاری فرانسه در خصوص اعتبار بخشی به اسناد الکترونیک به‌کار رفته است که می‌تواند به‌عنوان روشی مناسب در تقنین مورد استفاده قرار گیرد. قانون‌گذار مزبور به جای آنکه تعداد زیادی مواد با اصطلاحات فنی نامأنوس برای جامعه حقوقی و عامه مردم تصویب کند، تنها به اضافه کردن بندهای مختصری به شرح زیر به مواد موجود قانون مدنی در مبحث اسناد، اکتفا نموده است و بدین ترتیب اولاً خلأ قانونی را مرتفع کرده و ثانیاً زمینه درک و جذب آسان این پدیده نو را در فرهنگ حقوقی جامعه خویش فراهم ساخته است.

«ماده ۱۳۱۶- دلیل کتبی صرف نظر از قالب یا روش انتقال آن، از مجموعه‌ای حروف، نشانه‌ها، ارقام یا هر نماد یا علامت قابل درک دیگر تشکیل می‌شود.

۱- نوشته الکترونیک همانند نوشته کاغذی به عنوان دلیل پذیرفته می‌شود، منوط به آنکه بتواند شخصی را که نوشته توسط وی صادر شده است بشناساند و در شرایطی ایجاد و نگه‌داری شود که تمامیت آن تضمین گردد.

۲- هنگامی‌که قانون اصول دیگری را مقرر نداشته است و در صورت نبود تراضی معتبر طرفین برخلاف آن، دادرس با توسل به شیوه‌های گوناگون و صرف‌نظر از قالب دلایل، تعارض ادله کتبی را با شناسایی کردن دلیلی که مقرون به صحت است، حل خواهد نمود.

۳- نوشته الکترونیک ارزش اثباتی نوشته دستی را دارا است.

۴- امضای لازم برای یک عمل حقوقی، هویت امضاکننده و رضایت طرفین را به تعهدات ناشی از عمل حقوقی روشن می‌کند و چنانچه امضا توسط یک مرجع رسمی گواهی شود، به سند اصالت داده می‌شود.

هرگاه امضا به صورت الکترونیک باشد، متضمن روشی مطمئن برای شناسایی و به نحوی خواهد بود که ارتباط آن را با سند مربوط تضمین کند. فرض بر مطمئن بودن امضا خواهد بود تا زمانی که خلاف آن اثبات شود و هرگاه یک امضای الکترونیک انجام شود، در صورتی که ضوابط مرجع دولتی رعایت شده باشد، هویت امضاکننده و تمامیت سند تأمین می‌گردد.

ماده ۱۳۱۷- سند رسمی سندی است که توسط مأمورین رسمی که حق تنظیم آنرا دارند، در مکانی که سند در آنجا تنظیم می‌گردد و با رعایت تشریفات قانونی تنظیم می‌شود. این سند ممکن است الکترونیک باشد منوط به آنکه حسب شرایط مقرر تنظیم و حفاظت شود».

قانون امضای الکترونیک کشور مزبور نیز مطلب جدید قابل توجهی به آنچه قانون مدنی مقرر داشته نیافزوده است (Birnbaum & Darques, 2001, P.2)

بجا بود در کشور ما نیز که دارای حقوق نوشته و مشابه فرانسه در این مورد است، به ترتیب فوق عمل می‌شد و این‌همه مواد (۶ تا ۲۵) با ایرادهای علمی و اصطلاحات نامأنوس فنی تحت عنوان قانون مستقل تصویب نمی‌شد. ضمن اینکه تفصیل فعلی نیز، که بعضاً ورود به جنبه‌های موضوعی و خارج از شأن قانون محسوب می‌شود، عملاً هیچ نیازی را در موارد ارجاع به کارشناسان در پرونده‌های مطروحه نزد قضات برطرف نمی‌کند و علی‌القاعده کارشناسان مطابق استانداردهای فنی مربوط

قانون نمونه آنسیترال در بند ۱- الف ماده ۸، تصریح نموده است که هرگاه قانون مقرر کرده باشد اطّلاعات به صورت اولیه خود ارائه یا نگه‌داری شوند، این امر در مورد داده‌پیام در صورتی محقق خواهد شد که تضمینی قابل اعتماد در مورد محفوظ ماندن تمامیت اطّلاعات از زمان تولید آن به شکل نهایی، به عنوان داده‌پیام یا عنوان دیگر، وجود داشته باشد. برخی مواد دیگر ازجمله بند ب -۱ ماده ۱۰ نیز به نوعی تکرار یا حداقل به دلالت التزامی بازگو کردن همین شرط است: «داده‌پیام به همان صورتی که تولید، ارسال یا دریافت شده یا به صورتی که بتواند اطلاعات تولید، ارسال یا دریافت شده را ارائه نماید نگه‌داری شده باشد».

در مورد بند اخیر، راهنمای آنسیترال نکته‌ای را متذکر شده است. بدین شرح که منظور از ثبات آن نیست که همواره داده‌پیام بدون هیچ‌گونه تغییری ولو آنکه منجر به تغییر در محتوای سند نشود باقی بماند. ممکن است اسناد به صورت فشرده، بازگردان شده از کدهای اولیه و به صورتی ظاهراً متفاوت با حالت اول ذخیره شوند ولی همین‌که در تمام این موارد امکان بازیابی اطّلاعات به شکل اولیه وجود داشته باشد، کفایت خواهد کرد (Guide of MLEC, p.42).

روشن است که تعیین اینکه چه روش‌های فنّی تضمین‌های مذکور را تامین می‌کند، مطلبی نیست که قانون به آن بپردازد بلکه طبیعتاً تابع شرایط و مطابق استانداردهای فنی روز است. در مقام قضاء نیز قاضی برای احراز وجود شرایط مزبور، معمولاً مورد را به کارشناسان ذیربط ارجاع می‌دهد مگر آنکه اوضاع و احوال از نظر وی به اندازه کافی روشن باشد یا طرفین دعوی در آن اختلافی نداشته باشند.

از روشهای مطمئن در تأمین شرط عدم تغییر سند الکترونیک، فناوری رمزنگاری است که امضای دیجیتال بر آن مبتنی است. ما در مبحث امضا، به این مطلب خواهیم پرداخت ولی در اینجا این نکته را متذکر می‌شویم که قابلیت استناد به داده‌پیام منوط به داشتن امضا نیست و

به کار خود، اعم از آن‌که در قانون چیزی در آن موارد ذکر شده یا نشده باشد، نظر می‌دهند. ترتیب موجود در قانون تجارت الکترونیک از قوانین و مقررات کشورهای کامن لو و اسناد بین‌المللی تحت تأثیر آن کشورها و البته با دخل و تصرفاتی اقتباس شده است. در کشورهای با حقوق عرفی که فاقد قوانین مدون و قدیمی در زمینه ادله اثبات دعوی بوده‌اند، به ناچار برای مواردی جدید و مورد نیاز مانند سند الکترونیک، قانون جدید وضع می‌کنند و معمولاً عبارات قانونی آنها مفصل است. همین کشورها نیز معمولاً بانیان و تدوین کنندگان اصلی اسناد بین‌المللی نظیر قانون نمونه آنسیترال هستند که از باب مثال در تجارت الکترونیک به عنوان الگو برای کشورها تدوین شده است. بدین ترتیب جا دارد هنگام اقتباس کشورها از این قوانین، حقوق‌دانان خبره آنان با عنایت به فرهنگ حقوقی خود و قوانین خویش به نحو مناسب تنها موارد نیاز و خلأ قانونی را از آن منابع اقتباس کنند و بی‌جهت حجم قوانین خویش را نیافزایند و عبارات و اصطلاحات نامأنوس فنی را در قانونی که برای ادله اثبات دعوی است، نیاورند.

بسیاری از پیام‌های تجاری بدون امضا به معنای رایج و رمزنگاری است و صرفاً با ذکر نام ارسال کننده و نشانی الکترونیک او شناسایی می‌شوند. البته این را نیز باید اضافه کرد که سند الکترونیک تنها در ارتباطات مطرح نیست و محتوای حافظه یک رایانه بدون آنکه به جایی ارسال شده باشد ممکن است به‌عنوان دلیل (سند) مورد استناد قرار گیرد مانند حساب‌های یک شرکت که به صورت الکترونیک تهیه و نگه‌داری شوند.

۲-۲- دوام سند

دومین ویژگی نوشته آن است که مانند ادله شفاهی زودگذر نیست و برای مدتی به تناسب جنس آن باقی می‌ماند و در نتیجه این امکان را فراهم می‌آورد که برای دفعات مکرر به آن مراجعه و درصورت نیاز به مراجع دولتی و قضایی ارائه شود.

بند ب- ۱ ماده ۸ قانون نمونه در این مورد، در ضمن ذکر شرایط اصالت اطلاعات الکترونیک، مقرر می‌دارد: «هرگاه قانوناً لازم باشد که اطّلاعات ارائه شود، امکان ارائه آن به شخصی که لازم است، وجود داشته باشد». علاوه‌بر این ماده ۱۰ قانون مزبور نیز تماماً به شرایط لازم برای نگه‌داری از سند پرداخته است: «۱- هرگاه قانون مقرر داشته باشد که اسناد، سوابق یا اطلاعات خاصی نگه‌داری شوند، آن امر با نگه‌داری داده‌پیام محقق می‌شود منوط به آنکه شرایط زیر حاصل شده باشد:

الف- اطلاعات موجود در داده‌پیام قابل دسترسی باشد به نحوی که در مراجعات بعدی بتوان از آن استفاده کرد.

ب- داده‌پیام به همان صورتی که تولید، ارسال یا دریافت شده است یا به صورتی که بتواند اطلاعات تولید، ارسال یا دریافت شده را ارائه نماید، نگه‌داری شده باشد.

ج- اطّلاعاتی که احیاناً وجود داشته است تا مبدأ و مقصد داده‌پیام و تاریخ و زمان ارسال و دریافت را نشان دهد، نگه‌داری شده باشد.

۲- تکلیف به نگه‌داری اسناد، سوابق یا اطلاعات مطابق با بند ۱، شامل اطلاعاتی که هدف از آنها فراهم نمودن امکان ارسال یا وصول پیام است نمی‌شود.

۳- هرگاه شرایط مذکور در بند ۱ با استفاده از خدمات شخص دیگر تأمین شود نیز کفایت خواهد نمود منوط به آن‌که شرایط مذکور در بخش‌های الف و ب و ج بند ۱ حاصل شده باشد».

ذخیره کردن در چند حامل مانند دیسکت‌های متعدد و یا حافظه چند رایانه و ارسال از طریق اشخاص ثالث مانند اداره پست یا سپردن همزمان نزد آن، می‌تواند صورت‌هایی برای تأمین شرط دوام داده‌پیام به شرح فوق باشد.

بند ج نیز استانداردی را برای معرفی خود سند مقرر نموده که عبارت است از اطلاعاتی که مشخصات مبدأ، مقصد، تاریخ و زمان ارسال داده‌پیام را بیان می‌کند.

آنسیترال در توضیحات خود، موارد فوق را بالاتر از استانداردهای قوانین ملی در اسناد کاغذی می‌داند (Guide of MLEC, p.42). اما می‌توان چنین نظری را نپذیرفت. زیرا اولاً این موارد در اسناد کاغذی نیز معمولاً رعایت می‌شود و حتی در برخی از اسناد مانند اسناد تجاری، بارنامه و بیمه‌نامه جزء ضوابط و شرایط قانونی شکل‌گیری آنها است و عدم رعایت آن ملاحظات ایراد قانونی جدی به همراه دارد، ثانیاً قوانین ملی به‌لحاظ منطق حقوقی نبایستی اعتبار هرگونه سندی را منوط به رعایت ضوابطی مانند تاریخ صدور، وصول و امثال آن بنمایند تا بدین ترتیب دارندگان اسناد را از استناد به آنها در حدودی که دلالت دارند، محروم سازند. بنابراین بهتر است بگوییم که ماده ۱۰ قانون نمونه نیز تنها در این مقام بوده است که بگوید هرگاه قانون ملی لازم بداند که اسناد و سوابقی نگه‌داری شوند، آن مقصود با وجود شرایط مذکور، حاصل خواهد شد. بدین ترتیب اگر در قانون کشوری وجود برخی شرایط مذکور در بند ج، در تمام اسناد کاغذی لازم نباشد، رعایت آنها در شکل الکترونیک آن اسناد نیز ضروری نخواهد بود.

در مورد بند ۲ نیز باید گفت با عنایت به مفاد قسمت ج از بند ۱، آن بند تنها ناظر به اطّلاعاتی است که به موجب استانداردهای فنّی سامانه و به طور خودکار به داده‌پیام افزوده می‌شود تا ترتیب ارسال و دریافت آنرا بدهد و از آنجا که توسط طرفین ایجاد نمی‌شود، سند آنها محسوب نمی‌گردد و بنابراین مشمول بند ۱ نیز نخواهد بود. ضمن آنکه ممکن است در اوضاع واحوال خاصی، آن موارد قرینه‌ای را برای اثبات امری تشکیل دهند که در آن صورت با کسب نظر از کارشناسان مربوط، برای دادگاه قابل استفاده و استناد خواهد بود.

مقررات ماده ۸ ق‌ت‌ا نیز در این زمینه مشابه قانون نمونه است و تنها در بند (د) به عنوان شرط نهایی اضافه کرده است: «شرایط دیگری که هر نهاد، سازمان، دستگاه دولتی و یا وزارتخانه در خصوص نگه‌داری داده‌پیام مرتبط با حوزه مسؤولیت خود مقرر نموده فراهم شده باشد».

بند مزبور مانند آن است که طرفین تجاری یک قرارداد برای مبادله اسناد بین خودشان استانداردهای ویژه‌ای را مقرر کرده باشند، که در آن صورت فیمابین آنان لازم‌الرعایه خواهد بود. ولی باید گفت در هر حال عدم رعایت این شروط، تنها «اثر خاصی» را که سازمان یا طرفین در مورد سند مزبور در نظر داشته‌اند (مثلاً برای ذکر تاریخ تقاضا یا نوشتن عنوان بخش معینی از یک اداره بزرگ در مکاتبات) منتفی می‌کند وگرنه تا بدانجا که به ادله اثبات دعوی به‌طور عام مربوط می‌شود، همان داده‌پیام نیز عندالاقتضا قابل استناد خواهد بود.

۳-۲- اصالت در برابر کپی

مقصود از اصالت (Originality) در اینجا، اصل در برابر کپی است. در محیط رایانه‌ای می‌توان به هر تعداد که بخواهیم از یک سند تکثیر کنیم به‌طوری که هیچ‌کدام با دیگری تفاوت نداشته باشند.

این موضوع از دو نقطه نظر قابل توجه است. یکی از نظر ادله اثبات دعوی و رسیدگی به دعاوی است که طرفی که علیه او سندی ابراز شده حق دارد اصل آن را مطالبه کند وگرنه آن سند از عداد ادله خارج خواهد شد (م ۹۶ ق‌آدم). مشابه این قاعده در سایر نظامهای حقوقی نیز وجود دارد و در کامن لو از آن به قاعده اصل سند(Original Document Rule) تعبیر می‌کنند (Black Law Dictionary).

نقطه نظر دوم مربوط می‌شود به اسنادی که خود آنها مقوم و پدیدآورنده یک تعهد هستند مانند اسناد تجاری (مواد ۲۲۳، ۳۰۸ و ۳۱۱ ق‌ت) که با صدور آنها یک عمل حقوقی خاص تحقق می‌پذیرد و همچنین اسنادی که مادام که در دست طلبکار هستند، مدیون نمی‌تواند ادعای برائت ذمه کند، مانند بارنامه دریایی (بند ۷ ماده ۵۲ ق‌د). بارنامه سند مالکیت کالا است و امکان وجود نسخ متعدد یکسان نزد افراد مختلف، تحویل بار را به ارائه دهنده آن مشکل می‌سازد (ماده ۶۴ ق‌د، و السان و امینی، ۱۳۹۳، ص۷۱).

علی‌رغم اهمیت این مطلب، قانون نمونه به آن نپرداخته و قانون ایران نیز در آن ساکت است. در قانون فرانسه نیز اشاره خاصی به این مطلب نشده، در ماده ۱۰۰۱ قانون قواعد ادله فدرال آمریکا، در ضمن تعاریف، به این امر توجه شده ولی پس از آن مشکلی را رفع نکرده است.

اصل یک نوشته یا سابقه به معنای خود نوشته یا سابقه یا هرگونه نسخه متناظری (Counterpart)است که برای داشتن همان اثر توسط شخص تولید یا صادر کننده موردنظر بوده است. برای ذخیره‌های الکترونیک اصل به معنای هرگونه چاپ یا خروجی دیگری از آن است که توسط چشم قابل خواندن باشد منوط به آن‌که به‌طور درست اطلاعات آن را منعکس نماید... .

رونوشت (Duplicate) به معنای نسخه متناظری است که به طریق ماشینی، عکاسی، شیمیایی، الکترونیک یا روش یا تکنیک معادل دیگری به درستی اصل را تولید مجدد نماید.

ملاحظه می‌شود که نسخه‌های مکرر از یک سابق الکترونیک، مشمول هردو عنوان اصل و رونوشت با تعاریف فوق می‌شوند.

اما در انگلستان قانون ادله مدنی(Civil Evidence Act -1995) قاعده عامی را طی مواد ۱ و ۸ در قابلیت جایگزین شدن کپی در دادرسی در صورت فقدان اصل وضع کرده است (Reed, ibid, p. 215) که اجمالاً می‌تواند در مسأله اول ما که ادله اثبات است کاربرد داشته باشد. مطابق ماده ۸ مزبور: «۱- هرگاه پذیرش مندرجات یک سند در یک دادرسی مطرح باشد این امر می‌تواند به یکی از دو روش زیر اثبات و حسب نظر دادگاه اصالت آن تأیید شود:

الف- با ابراز آن سند، ب- چنانچه سند موجود نباشد با ارائه کپی از تمام یا بخش مهم آن».

مشابه این ترتیب در حقوق آمریکا نیز پذیرفته شده است (Goode, 2010, PP.6o-61).

روشن است که در مسأله دوم حتی راهبرد قانون انگلستان به نحوی نیست که قبل از رأی دادگاه در محکومیت مدیون سند تجاری که اصل آن مفقود شده یا متصدی حملی که اصل بارنامه دریایی صادره توسط او به وی ارائه نمی‌شود، افراد مزبور خطر کنند و در برابر کپی اسناد که ممکن است متعدد و در اختیار چندین نفر باشند، پول یا کالا تحویل دهند. دادگاه نیز به راحتی قادر نخواهد بود در هر پرونده‌ای حکم بر محکومیت آنان در ادای دیون خود بدون تضمین‌های لازم صادر کند. برخی آرای صادره از محاکم آمریکا و انگلیس مبتنی‌بر استناد به کپی سند به جای اصل (آهنی، ص ۱۹۷-۱۹۴). همگی مستظهر به قرائن قضایی که نقیصه مدارک ارائه شده را جبران می‌کرده بوده است.

به هر حال به لحاظ پر خطر بودن اعتماد به کپی برابر اصل، و نیاز آن به حکم قاضی در هر مورد، عملاً تا کنون این‌گونه اسناد به‌صورت الکترونیک رواج نیافته‌اند و حتی علی‌رغم اجرا

شدن طرح‌های حقوقی- فنی سنگین و ارائه سامانه‌های ویژه با همکاری سازمان‌های بین‌المللی، تجار رغبتی به استفاده از آن سامانه‌ها نشان نداده‌اند[۱].

شاید به همین سبب بوده باشد که قانون نمونه آنسیترال، آنجا که سند الکترونیک را معادل کاغذی می‌داند (م ۶)، باز برای کشورها حق تعدیل (رزرو) قائل شده است تا برخی موارد را مستثنی کنند که بر همین اساس قانون ایران سند مالکیت اموال غیر منقول (و نسخه دارو و هشدارهای ایمنی) را از شمول اعتبار داده‌پیام خارج ساخته است (م ۶) ولی مسأله اصالت سند همچنان مغفول باقی مانده است.

اما معاهده ۲۰۰۵ ملل متحد در استفاده از ارتباطات الکترونیک در قراردادهای بین‌المللی (UN Convention on the Use of Electronic Communications in International Contracts – 2005)، موضعی خاص و عملاً دوگانه اتخاذ کرده است. زیرا از یک طرف در بند ۴ ماده ۹ به کفایت نسخه الکترونیک به عنوان اصل در برابر کپی نظر دارد تا بتواند شمول آن را بر معاهده ۱۹۵۸ نیویورک در شناسایی و اجرای احکام داوری خارجی که ارائه اصل موافقت‌نامه داوری را لازم می‌داند، تأمین کند و از طرف دیگر بنا به مقتضیات و ملاحظات عملی، در بند ۲ ماده ۲، اسناد تجاری و بارنامه‌ها را، از شمول معاهده مستثنی کرده است: « این معاهده در مورد برات، سفته، راه‌نامه، بارنامه، قبض انبار یا هرگونه سند قابل انتقال یا سندی که حامل یا ذی‌نفع را برای تحویل کالا یا پرداخت مبلغی پول ذی‌حق می‌سازد، اعمال نمی‌شود».

در واقع می‌توان گفت عملاً امکان طرح مسأله اصل در برابر کپی در اسناد رایانه‌ای مشکل، و برآورده ساختن نیاز عملی کاربران در این زمینه با مانع فنی مواجه است و فن‌آوری اطلاعات نتوانسته به استانداردهای حقوقی پاسخ مناسب دهد. زیرا اولاً نسخه اصل همان است که در ابتدا روی حافظه موقت رایانه تشکیل می‌گردد و از آن لحظه به بعد آنچه که روی حافظه جانبی اعم از دیسکت سخت، سی‌دی و سایر وسایل ذخیره، ارسال و یا چاپ و نمایش داده می‌شود، همگی کپی محسوب می‌شوند، و ثانیاً امکان تولید، ارسال و ذخیره مجدد و یا ارسال نسخه‌های متعدد از نسخه اولیه وجود دارد و نمی‌توان علی‌رغم تمهیدات فنی، عاملی قطعی برای جلوگیری از تولید نسخه‌های مکرر یا تمیز آنها از اصل، در حدی که اعتماد تجار و بانک‌ها را جلب کند، در اختیار کاربران گذارد.

---

۱. سامانه‌های بارنامه دریایی الکترونیک تحت عناوین باز (CMI) و بسته (Bolero) نمونه‌های تلاش‌های مزبور هستند (Todd, 2002, PP.810-811).

به تعبیر دیگر، حتی در مسأله اول (ادله اثبات)، منطق لزوم ارائه اصل سند توسط مدعی در عالم حقوق همچنان پابرجا است و سطح فن‌آوری موجود جهان نمی‌تواند تأمین کننده این استاندارد حقوقی باشد. قوانینی نیز که مقرر می‌دارند داده‌پیام یا سند الکترونیک به جای سند کاغذی قابل استناد است، مفاد آنها ملازمه با نفی قاعده اصل سند ندارد مگر آن‌که حکم صریحی در این زمینه از سوی قانون‌گذاران ملی وضع شود که نمونه آن از قانون ادله انگلیس نقل شد که آن نیز عملاً منوط به نظر دادگاه در هر پرونده است و در رویه تجار مشکلی را نمی‌تواند رفع کند و به‌ویژه در مسأله دوم، نیز آنان مطابق قوانین خاص اسناد مشروحه فوق، مادام که اصل را دریافت نکنند معمولاً خطر نمی‌کنند و پول و کالا را در برابر کپی تحویل نمی‌دهند.

البته می‌توان گفت در صورتی که تاجری قبلاً با طلب‌کار در استفاده از سند الکترونیک آن توافق لفظی یا عملی کرده باشد حق نخواهد داشت بعداً به عدم اصالت واقعی سند مزبور استناد کند زیرا در واقع از حق ایراد مزبور قبلاً صرف‌نظر کرده است. در غیر این‌صورت نمی‌توان او را ملزم به پذیرش سندی کرد که هیچ اطمینانی در نبود نسخه‌های مکرر یکسان از آن نزد سایرین وجود ندارد.

مبحث دوم- قابلیت انتساب سند الکترونیک

وقتی سندی معتبر است که بتواند به صادرکننده‌اش منتسب شود. اثبات این امر محدود به روش خاصی مانند امضا یا غیر آن نیست[1] و می‌تواند با هر دلیلی از ادله پنجگانه اثبات دعوی حاصل گردد. ادله اثبات انتساب را می‌توان به دو قسم برون سندی و درون سندی طبقه‌بندی کرد.

---

۱. در تعریف سند درماده ۱۲۸۴ ق‌م، قید امضا یا مهر نیست بنابراین گرچه نوعاً امضا یا مهر بهترین وسیله برای انتساب سند به صادرکننده و وجود اراده او برای آن در مواردی که نیاز به اراده هست محسوب می‌شود، ولی انحصاری در این خصوص نیست و به هر طریقی که با توجه به قرائن بتوان صدور سند را اثبات نمود، نوشته سندیت خواهد داشت. البته در مواردی که به شرح مذکور در متن، وجود امضا موضوعیت دارد و بدون آن سند خاص به وجود نمی‌آید، امضا لازم خواهد بود.

قانون متحدالشکل تراکنش‌های اطلاعات رایانه‌ای آمریکا (The Uniform Computer Information Transactions Act-UCITA) به جای تأکید بر امضا، بر یک سامانه مطمئن برای ثبت تراکنش‌ها تأکید کرده است (سپاهی، امیر، ۱۳۹۳، ص ۱۷۲). در معاهده ۲۰۰۵ نیز اثری از لزوم امضا برای اعتبار ارتباط به چشم نمی‌خورد (رضایی، همان، ص ۱۲۷).

گروه اول شامل اقرار صادرکننده، گواهی شهود و امارات قضایی یعنی قرائن و اوضاع و احوالی است که قاضی بر اساس آنها قانع می‌شود سند توسط شخص معینی صادر شده است. اما گروه دوم امضا، مهر، دستخط و هرگونه قرینه‌ای در درون خود سند را در بر می‌گیرد. ضمن آن‌که در موارد اخیر نیز هرگاه مدعی‌علیه نسبت به آنها انکار، تردید یا ادعای جعل نماید، باز باید برای اثبات انتساب به وی، از ادله بیرونی مانند نظریه کارشناسی کمک گرفته شود.

قبلاً اشاره کردیم که گاه امضا یا مهر، علاوه‌بر ایفای نقش اثبات انتساب سند به صادرکننده، نقشی ماهوی را نیز در به وجود آمدن آن ایفا می‌نمایند. به‌طوری که حتی اگر کاملاً محرز باشد که سند توسط خوانده دعوی تنظیم و تسلیم خواهان شده است، ولی به سبب آنکه فاقد امضا یا مهر است، اعتبار و اثر خاص قانونی آن سند را ندارد. اسناد تجاری یا بارنامه از اینگونه هستند و بدون امضا یا مهر اصلاً به‌وجود نمی‌آیند تا بتوان بر اساس آنها طرح دعوی نمود و اثبات انتساب آنها به صادرکننده اثر خاص قانونی را در پی نخواهد داشت. این اسناد، علاوه‌بر دلیل اثبات دعوی بودن، صدورشان عمل حقوقی محسوب می‌شود.

انتساب سند در مبادلات الکترونیک در دو مرحله قابل بررسی است، اول مرحله تنظیم و امضاء سند و دوم مرحله ارسال تا وصول آن. در مرحله اول بحث امضای الکترونیک مطرح است درحالی‌که در مرحله دوم، صحت و ایمنی سامانه الکترونیک از مبدأ تا مقصد مورد توجه است.

۱- امضای الکترونیک

معمولاً قانون‌گذاران امضا را تعریف نکرده‌اند و این امر و مصادیق آن را به عرف واگذار نموده‌اند. عرف نیز هرگونه علامت دستی، حروف یا ترکیب آن و علامت‌ها را امضاء محسوب می‌کند. در برخی کشورها نظیر کشورهای با حقوق عرفی، مهر نیز از انواع امضاء تلقی می‌شود (Reed, p. 208). ولی در سایر کشورها از جمله ایران، مهر با امضا، ظاهراً متفاوت است. به همین سبب ماده ۲۲۳ قانون تجارت می‌گوید: «برات علاوه‌بر امضا یا مهر برات دهنده باید دارای شرایط ذیل باشد». در بند ۲ ماده ۱۲۹۱ قانون مدنی نیز در مواردی که اعتبار سند معادل اسناد رسمی می‌شود، مهر و امضا را جداگانه و متفاوت ذکر و در عین حال دارای اثر یکسان دانسته است «... هرگاه در محکمه ثابت شود که سند مزبور را طرفی که آن را تکذیب یا تردید کرده فی‌الواقع امضاء یا مهر کرده است».

در هرحال، در فضای الکترونیک نیز امضای سند مطرح است منتهی با دو ملاحظه خاص:

یک- ماهیت امضای الکترونیک از جنس همان فضا است به‌طوری که همراه و جزء سند می‌شود. در این خصوص ماده ۲ قانون نمونه آنسیترال در امضای الکترونیک (UNCITRAL Model law on Electronic Signatures -2001)، در ضمن تعاریف خود چنین می‌گوید: «امضای الکترونیک عبارت است از داده‌هایی به صورت الکترونیک که برای تعیین هویت امضاءکننده داده‌پیام و نشان دادن قبول اطلاعات موجود در آن توسط وی به داده‌پیام ضمیمه یا منطقاً همراه می‌شود».

دو- با عنایت به فن‌آوری‌های گوناگون، علاوه‌بر تفاوت در درجات اطمینان‌بخشی در صدور سند، گونه‌هایی از آنها این امکان را نیز فراهم می‌آورند که هرگونه تغییر پس از صدور در آنها آشکار شود.

آنچه با اسکن کردن امضای دستی یک شخص و ذخیره آن در رایانه حاصل می‌شود، از مصادیق حداقلی امضای الکترونیک است. این گونه امضا تنها این امکان را فراهم می‌آورد که امضاهای صاحب آن در موارد آتی با آنچه در رایانه ذخیره شده است مقایسه و صحت امضاء توسط کاربر رایانه تأیید شود. این همان کاری است که در بانک‌ها برای پرداخت چک‌ها رایج است.

کلیک کردن روی عباراتی نظیر «قبول دارم» یا «پرداخت شود» در وبگاه فروشگاه مجازی نیز امضای مشتری محسوب می‌شود. زیرا این عمل با عنایت به مشخصات وی، نظیر نشانی الکترونیک و شماره کارت پول و رمز آن که به سامانه منتقل می‌شود، همان خاصیت و عملکرد امضا را در انتساب به شخص معین دارد.

امّا در فن‌آوری اطلاعات، روش‌های کامل‌تری نیز برای امضا[1] ابداع شده است که نه تنها درجه اطمینان زیادتری را نسبت به امضای دستی در امر اثبات انتساب داده‌پیام به صادرکننده آن موجب می‌شود که افزون بر آن، هرگونه تغییر در مندرجات سند پس از صدور آنرا نیز برملا می‌سازد.

---

۱. گرچه حسب مشهور «امضا» خوانده می شوند, ولی در واقع بیشتر مشابه «مهر» هستند لذا «مهر الکترونیک» عنوان مناسب‌تری برای آنها بود. زیرا همه آنها برنامه‌هایی رایانه‌ای و ذخیره‌شده در ابزار جانبی رایانه می‌باشند که توسط سازمانی مستقل تولید و به شخص متقاضی اختصاص داده می‌شوند و او پس از تهیه کردن متن سند, آن برنامه را به آن اضافه یا منضم می‌کند و بدین وسیله متن را به صورت رمز درآورده به خود نسبت می‌دهد.

امضاهای اخیر همگی مبتنی‌بر فن‌آوری رمزنگاری و با بهره‌گیری از فرمول‌های ریاضی هستند (Carlson, Crilly & Rutledge, pp. 594-601). به لحاظ قابلیت‌های بالای اینگونه امضائات بوده است که قوانین کشورها و نیز قوانین نمونه آنسیترال احکام خاصی را در ارتباط با آنها در نظر گرفته‌اند. در عین حال قوانین مزبور به لحاظ منطق حقوقی، تنها به ذکر اوصاف لازم امضائات الکترونیک برای اعتبار یافتن داده‌پیام پرداخته‌اند و نسبت به نوع فن‌آوری آنها موضع خاصی اتخاذ نکرده‌اند.

ماده ۶ قانون نمونه آنسیترال، شرایطی را برای اعتبار این‌گونه امضا درنظر گرفته که به اجمال در ماده ۱۰ قانون تجارت الکترونیک ایران تکرار شده است.

علاوه‌بر امضاهای دیجیتال که ماهیتی برنامه‌ای دارند، امضاهایی که مبتنی‌بر زیست سنجی هستند نیز به همراه برنامه و از طریق رایانه کاربردی شده و از جایگاه بالایی از نظر اطمینان بخشی برخوردار هستند. با انتقال ساختار خطوط سرانگشتان یا شبکیه چشم افراد به داخل رایانه و ذخیره کردن آن، این امکان به وجود می‌آید تا هر بار که صاحبان از آنها استفاده کنند، با آنچه ذخیره شده مقایسه و درصورت مطابقت، تأیید شود. در زمینه این‌گونه امضاها نیز ایده‌ها و روش‌های فنی متعددی مطرح شده که از سطوح ایمنی و کاربردی متفاوتی برخوردارند(Tait & Solms, pp. 175-182). امضاهای اخیر فعلاً بیشتر در تشخیص هویت در مبادی ورودی و امثال آن کاربرد دارند.

۳- ارزیابی قابلیت‌ها

۱-۲- کفایت امضای الکترونیک

با عنایت به قابلیت‌های متفاوت امضاهای الکترونیک با ساختارهای گوناگون، برخلاف امضای دستی، طبیعتاً جای این بحث باز می‌شود که احکام حقوقی آنها چیست؟

قانون نمونه (۱۹۹۶) در ماده ۷ به طور کلی شرایط و کارکردهایی را که یک روش امضا باید داشته باشد تا در ردیف امضای مورد نظر قوانین ملّی قرار بگیرد بیان نموده است: «۱- هرگاه قانون امضای شخصی را لازم بداند، آن اقتضاء در صورتی در ارتباط با داده‌پیام برآورده خواهد شد که:

الف- روشی استفاده شود که آن شخص و قصد او را برای پذیرش اطّلاعات موجود در داده‌پیام معلوم کند.

ب- روش مزبور با توجه به تمام اوضاع و احوال از جمله توافق‌های مربوطه، متناسب با مقصودی که برای آن داده‌پیام تولید یا ارسال شده است اطمینان بخش باشد».

ماده ۶ قانون نمونه ۲۰۰۱ در امضای الکترونیک نیز پس از عبارات مشابه فوق در بند ۱، در بند ۳ اضافه می‌کند: «امضای الکترونیک درصورتی برای برآورده کردن شرایط مذکور در بند ۱ قابل اعتماد خواهد بود که:

الف- داده‌های تولید امضاء، در متنی که استفاده می‌شوند به صاحب امضاء مربوط باشند نه شخص دیگر.

ب- داده‌های تولید امضاء، در زمان امضاء در اختیار صاحب آن باشد نه شخص دیگر.

ج- هرگونه تغییری در امضای الکترونیک پس از امضاء قابل تشخیص باشد.

د- هرگاه مقصود قانون‌گذار در امضاء، آن بوده که تأمینی برای عدم تغییر در اطّلاعات مرتبط با امضاء به وجود آید، هرگونه تغییری در اطلاعات مزبور پس از امضاء قابل تشخیص باشد».

ماده ۲ دستورالعمل جامعه اروپایی در امضای الکترونیک (EU Directive for electronic signatures -1999/93/EC) نیز مشابه شرایط فوق را ذکر کرده است.

قانون تجارت الکترونیک ایران ابتدا طی ماده ۷ به طور کلی مقرر کرده است: «هرگاه قانون وجود امضا را لازم بداند امضای الکترونیک مکفی است» و سپس در ماده ۱۰ آنرا به دو نوع مطمئن و غیرمطمئن تقسیم‌بندی کرده احکام خاصی را برای گونه مطمئن در نظر گرفته است: «امضای الکترونیک مطمئن باید دارای شرایط زیر باشد:

الف- نسبت به امضاکننده منحصر به فرد باشد.

ب- هویت امضاءکننده داده‌پیام را معلوم کند.

ج- به‌وسیله امضاءکننده 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».

ایرادی به تمام متون فوق که ظاهراً از هم اقتباس کرده‌اند، به چشم می‌خورد. بدین شرح که در تمام آنها بین شرایط خود «امضا» و عمل «امضاکردن» خلط شده است. این‌که هنگام امضا کردن، داده‌های آن در اختیار صاحب امضا یا وکیل او بوده یا نبوده، و به‌عبارت دیگر

به‌وسیله امضاکننده (صاحب امضا) یا تحت اراده انحصاری وی صادر شده باشد، مربوط به شرایط خود امضا نیست و باید جداگانه در ارتباط با اعتبار سندی که دارای آن امضا هست، مطرح شود. به این مطلب به مناسبت دیگری با تفصیل بیشتر خواهیم پرداخت.

۲-۲- تشخیص هویت امضاءکننده

این امر با عنایت به انواع امضاهایی که در فضای الکترونیک وجود دارد، به صورت‌های مختلف و البته با ضریب اطمینان‌های متفاوت قابل تحقق است.

در امضاهای با ساختار پیچیده‌تر، احراز هویت امضاءکننده با ضریب اطمینان بالاتری صورت می‌پذیرد. امضاهای مبتنی بر زیست سنجی، مانند تحلیل و ذخیره ساختار نقش سر انگشتان یا شبکیه چشم هر شخص در رایانه، علاوه‌بر آن‌که ضریب اطمینان بسیار بالایی را موجب می‌شود، مشکل سوءاستفاده از امضا را توسط فرد غیر مجاز را نیز تقریباً منتفی می‌کند. در این موارد سوء استفاده ممکن است با به کار گیری انگشتان صاحب امضا مثلاً در حال بیماری او صورت گیرد.

در فن‌آوری رمزنگاری از طریق امضای دیجیتال، و اضافه شدن گواهی مرجع تأیید به آن[1] که مشابه گواهی امضا در دفاتر رسمی است (فیضی چکاب، صص ۱۹۷-۱۹۴)، مقصود فوق بهتر تأمین می‌شود. در این روش، و البته در نوعی که به آن رمزنگاری نامتقارن (Asymmetric encryption) می‌گویند، دو برنامه رایانه‌ای به‌عنوان کلیدهای عمومی و خصوصی توسط مرجعی معتبر تولید می‌شوند و به شخص متقاضی اختصاص می‌یابند، ضمن آن‌که سوابق امر نیز برای صدور گواهی و اعلام مدت اعتبار امضا نگه‌داری می‌شود.

کلید خصوصی تنها در اختیار صاحب امضا است ولی کلید عمومی مانند شماره تلفن در اختیار همه می‌تواند باشد و توسط دفتر گواهی در سایت آن نیز برای اطمینان طرف‌ها اعلام می‌شود. صاحب امضا (الف)، متن نوشته شده را با کلید خصوصی خودش به صورت رمز درمی‌آورد و برای شخص مورد نظر (ب) ارسال می‌کند. ب متن را به کمک کلید عمومی مربوط به الف، رمزگشایی می‌نماید. اگر متن مزبور از سوی الف ارسال نشده باشد، رمز گشایی

۱. در گواهی‌نامه موارد زیر ذکر می‌شود: نام مرجع صدور، نام صاحب امضا، نوع گواهی ناظر به محدودیت‌های آن، دوره اعتبار, و شرایط گواهی مثلاً قابل استفاده بودن برای چند سند (زرکلام، ۱۳۸۳). ضمناً برای شناخت تفصیلی از مقررات صدور گواهی و مراجع مختلف صدور و مسؤولین اجرایی و نظارتی آن ر ک به سپاهی، همان، صص ۱۲۴-۶۷.

نمی‌شود و نیز اگر در جریان ارسال تغییری در متن صورت گرفته باشد، آشکار می‌گردد. البته می‌توان متن را با کلید عمومی گیرنده رمز و برای او ارسال کرد که در این صورت تنها با کلید خصوصی گیرنده رمزگشایی می‌شود. روش اخیر، امضای سند توسط صادرکننده محسوب نمی‌شود ولی این خاصیت را دارد که اگر متن به هر سببی در اختیار شخصی غیر از مخاطب مورد نظر قرار گیرد، قابل بازگشایی نباشد. می‌توان هردو کار را برای اطمینان بیشتر به طور توأمان انجام داد که البته روند کار را کند خواهد کرد.

آنچه که از فن‌آوری رمزنگاری می‌توان تحصیل نمود، حداکثر عبارت از این است که سند ارسال شده با کلیدهای اختصاص داده شده به شخص الف به صورت رمز درآمده است. ولی این امر ملازمه ندارد با اینکه حتماً کلید مزبور توسط صاحب آن نیز به کار رفته باشد. زیرا همانطور که ممکن است مهر لاستیکی متعلق به شخصی، توسط افراد غیر مجاز مورد استفاده قرار گرفته باشد، کلیدهای فوق نیز که روی حامل‌های جانبی رایانه‌ای ذخیره می‌شوند، ممکن است توسط اشخاص دیگر به کار گرفته شده باشند.

قسمت‌های الف و ب از بند ۳ ماده ۶ قانون نمونه ۲۰۰۱ از این نکته غافل نبوده و در ضمن ذکر شرایط اطمینان‌بخش بودن امضاء در حدی که قانون لازم می‌داند مقرر داشته است: «الف- داده‌های تولید امضا در زمینه‌ای که مورد استفاده قرار می‌گیرند، فقط به امضاکننده و نه شخص دیگر مرتبط شده باشند، ب- داده‌های تولید امضا در زمان امضا کردن تحت کنترل امضاءکننده و نه شخص دیگر باشند... »، و باز در ماده ۸ به وضوح تحت عنوان مراقبت‌های رفتاری صاحب امضا مقرر می‌دارد:

«۱- هرگاه داده‌های تولید امضا برای امضایی که اثر قانونی داشته باشند به کار رود، صاحب امضا باید:

الف- مراقبت‌های معمول را برای جلوگیری از استفاده غیرمجاز از امضا به عمل آورد.

ب- در موارد زیر، بدون تأخیر ناموجه با وسایلی که دفتر گواهی امضا طبق ماده ۹ در اختیار گذارده است یا به هر طریق معقول دیگری به هر شخصی که صاحب امضا ممکن است به نحو متعارف احتمال دهد که به امضای الکترونیک اعتماد کند یا خدماتی را در حمایت از امضای مزبور ارائه نماید، اطلاع دهد:

۱- صاحب امضا بداند که داده‌های تولید امضاء (توسط دیگران) مورد استفاده قرار گرفته است.

۲- وجود اوضاع و احوالی که برای صاحب امضا معلوم باشد منجر به وجود خطر اساسی در استفاده دیگران از داده‌های تولید امضای (او) می‌گردد.

ج- در مواردی که گواهی امضا برای پشتیبانی از آن صادر می‌شود، مراقبت‌های معقولی که برای تأمین صحت و کامل بودن تمام اطلاعات مرتبط با گواهی که در طول عمر آن در آن هست یا باید باشد, توسط صاحب امضا به عمل آید... ».

ملاحظه می‌شود که علی‌رغم ذکر مواردی که برای حفظ شرایط انتساب امضای الکترونیک به صاحب آن هست، باز این احتمال داده شده است که شخص غیرمجازی از آن استفاده کرده باشد. لذا قسمت ب را به شرح فوق ذکر نموده و در ادامه نیز اضافه می‌کند: «د- صاحب امضاء مسؤول عواقب حقوقی ناشی از کوتاهی خود در رعایت ضوابط مذکور در بند ۱ است». مفهوم مخالف این بند این است که هرگاه کوتاهی نکرده و در حد متعارف و معقول مراقبت‌های لازم را انجام داده باشد ولی در عین حال امضای او مورد سوءاستفاده دیگران قرار گرفته باشد، نمی‌توان گفت که سند منتسب به اوست و او به‌طور مطلق، مسؤول اتفاقاتی خواهد بود که رخ داده یا متعهد در قراردادی است که هرگز منعقد نکرده است.

اما قانون تجارت الکترونیک ۱۳۸۲، پس از آنکه در ماده ۱۴ شرط اعتبار داده‌پیام مطمئن را از نظر تولید و نگه‌داری توضیح می‌دهد، در ماده ۱۵ به‌طور مطلق مقرر می‌دارد: «نسبت به داده‌پیام مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن انکار و تردید مسموع نیست و تنها می‌توان ادعای جعلیت به داده‌پیام مزبور وارد و یا ثابت نمود که داده‌پیام مزبور به جهتی از جهات قانونی از اعتبار افتاده است». بدین‌ترتیب احتمال سوء استفاده از امضای صاحب آن بدون تقصیر وی را نادیده گرفته و حتی آثار اسناد رسمی را بر آنها بار کرده است (فیضی چکاب، ص ۱۸۰).

ضمانت اجرای شدید ماده ۱۵، در هیچ‌یک از سه قانون نمونه آنسیترال ۱۹۹۶ و ۲۰۰۱ و معاهده ۲۰۰۵ و دستورالعمل ۱۹۹۹/۹۳ جامعه اروپا در امضای الکترونیک و قوانین امریکا دیده نمی‌شود و حتی در قانون نمونه ۲۰۰۱ به شرح فوق، بر خلاف آن پیش‌بینی‌هایی نیز شده است و برخی نویسندگان، به وجود حق انکار برای صاحب امضا در حقوق امریک تصریح کرده‌اند (توماس جی. اسمدینگاف، ص ۲۸۱)[۱]. درست است که از نظر فنی، تقریباً امکان مشابه سازی

۱. در سایر کشورها نیز به این نکته توجه شده و در هیچ کدام حق انکار در شرایط مزبور از صاحب امضا سلب نشده است (آنسیترال، اعتماد سازی در تجارت الکترونیک، صص ۱۰۳-۹۵).

امضای دیجیتال وجود ندارد و از این حیث انتساب آن توسط دارنده قابل انکار نیست (کاشانی و نوروزی، ۱۳۹۰، ص ۷۵)، ولی استعمال کلید خصوصی توسط فرد غیر مجاز کاملاً محتمل و بی‌ارتباط با سطح فن‌آوری امضا است. این موضوع، از دیدگاه کیفری نیز قابل بررسی است زیرا سوءاستفاده از مهر یا کلید خصوصی دیگران امری بعید نیست (قناد، ۱۳۸۹، پیشگیری از سوءاستفاده‌های هویتی در فضای مجازی).

حمایت ماده ۱۵ از سند الکترونیک مطمئن، مناسب با اسناد رسمی و اسنادی است که صحت آنها با اقرار یا نزد محکمه اثبات شده باشد (قم ۱۲۹۲-۱۲۹۱). «رسمیت» و «اعتبار» دو مفهوم متفاوتند. هر سند معتبری رسمی نیست ولی هر سند رسمی را قانون معتبر شناخته است مگر آنکه به طریق قانونی یا حکم قضائی ابطال شود. رسمیت سند منوط به آن است که مطابق ماده ۱۲۸۷ قانون مدنی صادر گردد، اعم از آن‌که به‌صورت دستی یا الکترونیک باشد و اگر شرایط مزبور را نداشته باشد، رسمی نیست ولو معتبر باشد.

در اسناد تنظیمی در دفاتر اسناد رسمی، ابتدا هویت امضا کننده به کمک اسناد معتبر احراز می‌شود و سپس امضای او اخذ می‌گردد اعم از آن‌که امضای اخذ شده امضای معمول او باشد یا امضایی جدید که در هر حال معتبر و دارای اثر یکسان با امضای معمول او خواهد بود. این در حالی است که در امضای الکترونیک از راه دور این پایش میسر نیست و ممکن است شخص الف از امضای ب استفاده کرده باشد. البته برای تعدیل حکم ماده ۱۵ می‌توان از شرایطی که برای آن در ماده ۱۰ ذکر شده استفاده کرد و صغرای قضیه را زیر سؤال برد. به این ترتیب که چون یکی از شرایط امضای مطمئن آن است که توسط صاحب آن یا تحت اراده انحصاری وی صادر شده باشد، در موردی که در وجود این شرط تردید است، یکی از شرایط اطمینان منتفی است و اصلاً وصف مطمئن بودن امضای مزبور از ابتدا و در مرحله صدور مورد مناقشه و تردید قرار می‌گیرد و اصلاً امضای مطمئن به وجود نمی‌آید و بدین ترتیب قضیه مزبور از شمول احکام مواد ۱۰ و ۱۵ خارج می‌شود. علاوه بر این، از ماده ۱۸ قانون نیز می‌توان استفاده کرد. طبق این ماده: «در موارد زیر داده‌پیام منسوب به اصل‌ساز است: الف- اگر توسط اصل‌ساز و یا به وسیله شخصی ارسال شده باشد که از جانب اصل‌ساز مجاز به این کار بوده است...». مفهوم این بند آن است که اگر اثبات شود داده‌پیام از سوی اصل‌ساز یا شخص مجاز از طرف او «ارسال» نشده است، منسوب به او نیست و از این جهت اعتبار ندارد و بنابراین قابل انکار و تردید نیز خواهد بود.

راه دیگر، جمع مواد ۱۹ و ۲۰ است. بدین شرح که طبق ماده ۱۹: «داده‌پیامی که بر اساس یکی از شروط زیر ارسال می‌شود مخاطب حق دارد آن را ارسال شده محسوب کرده و مطابق چنین فرضی (ارسال‌شده) عمل نماید: الف- قبلاً به وسیله اصل‌ساز روشی معرفی و یا توافق شده باشد که معلوم کند آیا داده‌پیام همان است که اصل‌ساز ارسال کرده است، ب- داده‌پیام دریافت شده توسط مخاطب از اقدامات شخصی ناشی شده که رابطه‌اش با اصل‌ساز یا نمایندگان وی باعث شده تا شخص مذکور به روش مورد استفاده اصل‌ساز دسترسی یافته و داده‌پیام را به مثابه داده‌پیام خود بشناسد.» و در ماده ۲۰ می‌گوید: «ماده ۱۹ این قانون شامل مواردی نیست که پیام از اصل‌ساز صادر نشده باشد و یا به‌طور اشتباه صادر شده باشد». یکی از مواردی که داده‌پیام از سوی اصل‌ساز (صاحب امضا) صادر نشده، موردی است که دیگری بدون اجازه، از امضای الکترونیک او استفاده کرده و داده‌پیامی را ارسال نموده باشد که در این صورت قابل انکار و تردید خواهد بود.

مبحث سوم- تناسب مفاد سند با روش‌های ایمنی

اصولاً هدف از امضای سند، پذیرفتن مفاد آن است. در این مورد فرقی نمی‌کند که نقش سند صرفاً محدود به اعلام واقعیتی باشد که مستقل از آن وجود دارد، یا آن‌که با اقدام به امضا، علاوه بر خلق سند به‌عنوان دلیل، یک عمل حقوقی نیز انشاء شود مانند اسناد تجاری.

پذیرش محتوای سند به وسیله امضای آن، آنقدر نزد عرف روشن است که قانون مدنی لازم ندیده مستقیماً به آن اشاره کند و فقط به احکام و آثار سند پرداخته و حداکثر در ماده ۱۳۰۱ مقرر داشته است: «امضایی که در روی نوشته یا سندی باشد بر ضرر امضاءکننده دلیل است». در واقع، اصل بر آن است که امضا برای پذیرش محتوای سند است و لذا تنها خلاف آن نیاز به اثبات دارد.

اما قانون نمونه ۱۹۹۶ در بخش ب بند ۱ ماده ۷ در اعتبار سنجی داده‌پیام، به تناسب روش به کار رفته برای امضا با محتوای سند نیز توجه داشته است:

«۱- هرگاه قانون امضای شخصی را لازم بداند، آن اقتضا در داده‌پیام برآورده خواهد شد اگر: الف- روشی استفاده شده باشد که آن شخص را بشناساند و پذیرش او را نسبت به اطلاعات موجود در داده‌پیام معلوم نماید. ب- روش مزبور با عنایت به تمام اوضاع و احوال از

جمله توافق مربوط، متناسب با هدفی که داده‌پیام برای آن تولید یا مبادله گردیده است، قابل اعتماد باشد».

عبارات فوق نشان می‌دهد که از نظر قانون نمونه، هر امضایی به صرف الکترونیک بودن برای اعتبار داده‌پیام کافی نیست و وجود تناسب بین روش امضا و مفاد سند نیز لازم است. موارد فوق در بند ۳ ماده ۹ معاهده ۲۰۰۵ نیز تکرار شده است.

تعیین مصداق شرایط فوق با نظر عرف خواهد بود و بنا به اوضاع و احوال در هر مورد، قضات با استفاده از نظر کارشناسان آنرا احراز خواهند کرد.

روشن است که هرگاه علی‌رغم عدم تناسب روش امضا با معامله‌ای که انجام شده است، طرفین از قبل بر آن روش توافق کرده باشند، آن امضا معتبر خواهد بود. امّا ایراد به ملاک مذکور وقتی خواهد بود که چنین توافق قبلی وجود نداشته باشد. بدین شرح که مطابق قانون نمونه، چنانچه با توجه به اوضاع و احوال و در نبود توافق طرفین، نوع امضا با هدف داده‌پیام تناسب نداشته باشد، امضای صورت گرفته اعتبار نخواهد داشت. درحالی‌که ممکن است طرفین در ابتدا توافقی بر تناسب مفاد سند با نوع امضا نکرده باشند و ضمناًاختلاف آنان در سایر مسائل باشد. چرا قانون نمونه رأساً و به‌عنوان یک «اصل» اعلام کرده است که اگر تناسب یادشده وجود نداشته باشد، امضا معتبر نخواهد بود و بدین ترتیب اصل سند را بی‌اعتبار می‌سازد؟ این ترتیب مستقل از اراده طرفین، گاه به زیان تمام طرف‌ها و گاه به ضرر برخی از آنان خواهد بود بدون آنکه توجیه حقوقی داشته باشد.

البته در تنها درصورتی که در قضیه، شخص ثالثی مانند دولت در اموری مانند مالیات و غیر آن، ذی‌نفع در بی‌اعتبار بودن داده‌پیام باشد، می‌توان برای مقرره فوق توجیهی یافت (رضایی، همان، ص ۱۵۱)، ولی به هر حال همان مورد نیز قطعی نیست و قابلیت رسیدگی و احراز توسط دادگاه را خواهد داشت.

اما در قانون تجارت الکترونیک ایران این ایراد شدیدتر است. زیرا علاوه بر ملاحظه فوق، از یک طرف در ماده ۷ به نحو مطلق اعلام می‌دارد: «هرگاه قانون وجود امضا را لازم بداند امضای الکترونیکی مکفی است» یعنی قید و شرطی از نظر تناسب نوع امضا با مفاد سند قائل نشده و از طرف دیگر در ماده ۱۳ می‌گوید: «به‌طور کلی، ارزش اثباتی داده پیام با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به کار گرفته شده با موضوع و منظور مبادله داده

پیام تعیین می‌شود». با عنایت به اینکه از جمله روش‌های ایمنی و از مهم‌ترین آنها، روش امضا است، اگر تناسبی بین نوع امضا و مفاد سند الکترونیک نباشد، اعتبار سند مخدوش خواهد بود.

به هرحال چنین ملاکی در امضاهای غیر الکترونیک معمول نبوده و در قوانین بدان اشاره نشده است. به‌عبارت دیگر در قانون مدنی یا قوانین دیگر، در ایران و سایر کشورها معمول نبوده که قانون‌گذاران مثلاً از صادرکنندگان چک یا قراردادهای تجاری خواسته باشند درصورتی که ارزش سند از مبلغ معینی بیشتر باشد، روش یا تمهیدات ویژه‌ای در امضای خود معمول دارند. اگرچه ممکن است بنا به خواست متعهدله، علاوه بر امضای دستی، اثر انگشت نیز اخذ یا گواهی رسمی امضا نیز مطالبه شود. به هرحال این تمهیدات با اختیار طرفین قابل اعمال است و دخالت قانون‌گذار در آن توجیه ندارد.

بله، در یک صورت حکم ماده ۱۳ قابل توجیه و هماهنگ با حکم موضوع در سایر اسناد خواهد بود. آن صورت عبارت از وضعیتی است که سندی مورد تردید متعهد باشد و یکی از ادله او برای بی‌اعتباری سند، به همراه سایر ادله و قرائن یا اصل عملی، قرینه عدم تناسب عرفی یا روال معمول بین طرفین در خصوص مفاد سند با روش امضا یا سایر ملاحظات ایمنی سامانه در تولید و ارسال باشد. به هر حال این ملاحظات، به‌عنوان اماره قضائی می‌تواند برای اعتبارسنجی سند مورد توجه قاضی قرار گیرد ولی قاعده و اصلی همانند آنچه در قوانین مزبور ذکر شده است توجیه حقوقی ندارد.

مبحث چهارم- جایگاه سند الکترونیک در روابط اشخاص

این نکته مهمی است که باید روشن شود. آیا با وجود اعتبار قانونی داده‌پیام، طرف‌های روابط حقوقی ملزم به پذیرش چنین گونه‌ای از مبادلات هستند و در هر حال مفاد آنها بر روابط اشخاص حاکم است؟

قوانین نمونه و تجارت الکترونیکی ایران در این زمینه ساکتند ولی یوتای آمریکا و معاهده ۲۰۰۵ ملل متحد در ارتباطات بین‌الملل در این خصوص دارای حکم مشخص هستند.

در حالی که ماده ۷ یوتا تأکید می‌کند که امضای الکترونیک و قرارداد الکترونیک صرفاً به لحاظ نوع آنها قابل انکار نیستند، و هر گاه قانون وجود نوشته‌ای را لازم بداند سوابق الکترونیک کفایت می‌کند، در عین حال ماده ۵ تصریح می‌کند که قانون مزبور تنها بر

معاملاتی حاکم خواهد بود که طرف‌ها بر استفاده از این روش توافق کرده باشند ولو آن‌که این توافق از رفتار آنان استنباط شود.

تقریباً مشابه همین ترتیب در ماده ۸ معاهده ۲۰۰۵ نیز آمده است.

اما حکم قضیه در حقوق ایران چیست؟ پاسخ نخست آن است که چون احکام قانون تجارت الکترونیک به صورت آمره و بیان حکم داده‌پیام به طور مطلق بیان شده و منوط به توافق اشخاص نگردیده است، همانند احکام قانون مدنی در ادله اثبات دعوی بوده و بر روابط اشخاص در اعمال حقوقی و نیز در وقایع حقوقی حاکم است.

پاسخ دوم آن است که مقررات یوتای آمریکا و ق‌تا ایران در عمل فرق زیادی ندارند. زیرا در هر دو، چنانچه طرف‌ها از داده‌پیام (سابقه الکترونیک) استفاده کرده باشند، در آن صورت عملاً اعتبار آن را پذیرفته‌اند ولی اگر استفاده نکرده باشند، در آن صورت قضیه سالبه به انتفای موضوع خواهد بود. زیرا داده‌پیامی وجود نداشته است تا به آن ملتزم باشند. اما اگر یک طرف اراده خود را با داده‌پیام و طرف دیگر به وسیله دیگری اعلان کرده باشد، در آن صورت در آمریکا، ظاهراً، ارسال کننده به پذیرش مفاد آن ملتزم شده است ولی در التزام طرف دیگر تردید است، درحالی‌که در ایران هردو طرف به اعتبار آن ملتزم هستند زیرا شرط توافق در قانون نیامده است.

نتیجه‌گیری

اعتبار محتوای حافظه رایانه، و تعیین جایگاه مشخصی برای آن در میان ادله اثبات دعوی، بدون موضع‌گیری صریح قانون‌گذاران قابل تحقق نبود و این مهم نمی‌توانست به آرا و تفاسیر متنوع دادگاه‌ها سپرده شود.

اما مواضع قانون‌گذاران نیز علی‌رغم تشابه کلی، به لحاظ طرز تلقی آنها از این پدیده یکسان نیست. برخی از آن به عنوان سوابق الکترونیک (آمریکا)، برخی به عنوان داده‌پیام (قانون نمونه آنسیترال و ایران) و برخی به عنوان سند الکترونیک (فرانسه) از آن نام برده‌اند ولی همگی کاربرد و جایگاه سند را مستقیماً یا به صورت معادل یا در حکم آن برای این نوع دلیل پذیرفته‌اند.

از میان قانون‌گذاران، روش فرانسویان به لحاظ آیین تقنین و پیوند این پدیده نوظهور و احکام آن به بدنه قانونی و فرهنگ حقوقی کشور مدبرانه‌تر و در عین اختصار، کامل است و

می‌توان در بازبینی قانون تجارت الکترونیک، که دارای عناوین نامتجانس حقوقی است (گرچه قدم اول در این راه بوده و لذا قابل تقدیر است)، از روش مزبور بهره گرفت و ایرادهای علمی و تقنینی آن را زدود.

ایرادهای متعدد حقوقی به قوانین اعم از قانون تجارت الکترونیکی ایران و سایر کشورها و نیز قوانین نمونه آنسیترال وارد است. اعتبار سنجی سندهای الکترونیک با محک‌های میزان ثبات پذیری، دوام و قابلیت انتساب آنها با توجه به مقررات وضع شده در خصوص امضاهای مطمئن نقایص قوانین را در برخی موارد مهم نشان می‌دهد. نکته مهم دیگر، تناسب داشتن مفاد اسناد الکترونیک با شیوه ایمنی به کار گرفته شده در تولید آنها است که گرچه می‌تواند به‌عنوان اماره و در اختیار قاضی شناخته شود، ولی نمی‌تواند به عنوان یک اصل در قوانین ذکر گردد که حتی با عدم اختلاف طرفین دعوی در آن زمینه، قانون آن را به صورت حکم آمره، بی‌اعتبار بشناسد.

مسأله لزوم ارائه اصل سند به عنوان دلیل اثبات به ویژه در مواردی مانند اسناد تجاری که اصل آن مقوم تعهد نیز هست، و یا در بارنامه دریایی که بدون ارائه اصل امکان تحویل کالا نیست، خلأیی را موجب شده است که علیرغم تصریح قوانین به اعتبار نسخه الکترونیک به جای کاغذی، عملاً باقی مانده و تجار به حسب معمول تمایل ندارند با خطر کردن، پول یا کالا را به اشخاصی تحویل دهند که نسخه‌ای الکترونیک را ارائه می‌دهد در حالی که امکان دارد همانند آن در اختیار دیگران نیز باشد. موارد مزبور حاکی از ناتوانی سطح فن‌آوری روز در پاسخ به استانداردهای دقیق حقوقی است.

منابع

فارسی و عربی

- قانون مدنی
- قانون تجارت
- قانون آئین دادرسی مدنی
- قانون تجارت الکترونیکی
- آنسیترال (۱۳۹۰)، "اعتمادسازی در تجارت الکترونیکی"، ترجمه زرکلام ستار، تهران، نشر دانش.
- اسمدینگاف توماس جی (۱۳۸۷)،"قواعد ضروری جهت اعتبار تراکنش‌های الکترونیکی در عرصه جهانی"، ترجمه بختیاروند
مصطفی، مجله حقوقی، ش ۳۸، تهران، مرکز امور حقوقی بین المللی.
-السان مصطفی و امینی وحید، (۱۳۹۳)، "جایگزین بارنامه کاغذی با بارنامه الکترونیکی دریایی"، پژوهش‌نامه
بازرگانی، تهران، وزارت بازرگانی.
- امامی سید حسن، (۱۳۴۶)، *حقوق مدنی*، ج ۶، تهران، انتشارات ابوریحان.
-آهنی بتول، (۱۳۸۴)، *انعقاد و اثبات قراردادهای الکترونیکی*، رساله دکتری، دانشکده حقوق و علوم سیاسی
دانشگاه تهران.
- جعفری لنگرودی محمدجعفر، (۱۳۷۲)، *ترمینولوژی حقوق*،چ ششم، تهران، انتشارات گنج دانش.
- رضائی علی ،(۱۳۸۷)، *حقوق تجارت الکترونیک*، چ اول، تهران، نشر میزان.
- زرکلام ستار، (۱۳۸۳)، "قانون تجارت الکترونیکی و امضای الکترونیکی"، مجموعه مقالات همایش بررسی ابعاد حقوق فن آوری اطلاعات، در www.wikipg.com.
- سپاهی امیر، (۱۳۹۳)، *حقوق اسناد*،چ اول ، تهران، نشر دادگستر.
- فیضی چکاب غلامنبی، (۱۳۸۹)، "اعتبار حقوقی دلیل و امضای الکترونیکی"، فصلنامه پژوهش حقوق و سیاست، ش ۳۰، تهران، دانشگاه علامه طباطبائی.

- قناد فاطمه، (۱۳۸۹)، "پیشگیری از سوءاستفاده‌های هویتی در فضای مجازی"، در www.academia.edu.

-کاشانی مؤمن - نوروزی اصفهانی نوشین، (۱۳۹۰)، "زیرساخت کلید عمومی"، تهران، مرکز توسعه تجارت الکترونیکی وزارت بازرگانی.

- کاتوزیان ناصر، (۱۳۸۷)، *اثبات و ادله اثبات*، ج۱، چ پنجم ، تهران، نشر میزان.

- مظفر محمد رضا، *اصول الفقه*، ج ۲، قم، انتشارات مؤسسه اسماعیلیان.

لاتین

-Birnbaum-Sarcy Laurence & Darques Florence (2001), 'La signature électronique Comparaison entre les législations française et américaine ', www.signelec.com.

-Black Henry Campbell (1983), *Black Law Dictionary*, West Publishing Co.

-Carlson A. B., Crilly P.B. & Rutledge J.C. (2002), *Communication Systems*, Mc Graw Hill, Boston.

-Federal Bar Association (2014), www. Fedbar.org/litigation/march/27/2014.

-Goode Steven (2010), 'The Admissibility of Electronic Evidence, The Review of Litigation', Vol. 29:1, the University of Texas.

-EU E Commerce, EC/2000/31 .

-Gkoutzinis Apostolos Ath (2006), *Internet Banking and the Law in Europe*, Cambridge University press.

-French Civil Law.

-Pendleton Hon Alan (2013), 'Admissibility of Electronic Evidence', www.mnbenchbar.com

-Reed Chris & Angel John (2007) , *Computer Law*, 6th Edition, Oxford University.

-Stephen Mason (2014), 'Electronic Evidence', www.infolaw.co.uk/newsletter/2014/electronic-evidence.

-Tanenbaum Anderson S. (2002), *Computer Networks*, Vrije Universiteit, Amesterdam.

-Tait Bobby & Salms Basie von (2006), *Biometrically Based Electronic Signatures for a Public Networked Environment*, University of Johannsburg.

-UNCITRAL Model Law on Electronic Commerce (1996).

-UNCITRAL Model Law on Electronic Commerce with Guide to Enactment (1996).

-UNCITRAL Model Law on Electronic Signature (2001).

-UN Convention on the Use of Electronic Communications in International Contracts (2005).

-Uniform Law Commission, www.uniformlaws.org

-US Uniform Computer Information Transactions Act (1999).

-US Uniform Electronic Transactions Act (1999).

-US Federal Rules of Evidence (2014).

-Todd Paul (2002), *international Trade*, Sweet & Maxwell, London.