

وجوه افتراق و اشتراک سند رسمی و الکترونیک

(تاریخ دریافت ۱۴۰۱/۰۷/۱۵، تاریخ تصویب ۱۴۰۱/۱۲/۱۸)

فاطمه لروند

چکیده

همانطور که در تعریف سند الکترونیک بیان گردید، هر داده یا پیامی که به صورت الکترونیکی از هر دستگاهی که این امکان را دارا باشد ارسال و دریافت شود، با لحاظ شرایط قانونی، قابل استفاده در مقام دعوا و دفاع بوده و در دادگاه قابل استناد است. برخی از کاربران به دلیل نداشتن اطلاعات و آگاهی لازم، بر این تصور هستند که اسناد الکترونیک کاربرد چندانی به هنگام طرح دعاوی حقوقی و دفاع در مقام دعوا نداشته و عملاً قابل انکار هستند. اما این در حالی است که تنها ماهیت این اسناد است که الکترونیکی بوده و حالت پیام دارد؛ گرچه قانون تجارت الکترونیکی (۱۳۸۲) و حتی قانون جرایم رایانه ای (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 فناوری 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. در پی پرداخت به این مطالب به وجوه افتراق و اشتراک سند عادی و الکترونیک نیز پی خواهیم برد.

واژگان کلیدی: ادله اثبات، سند الکترونیک، امضای الکترونیک، اصالت سند

مقدمه

علی رغم گذشت بیش از شصت سال از ظهور رایانه و به ویژه رواج عمومی آن با پیدایش نوع شخصی و علی الخصوص با فراگیر شدن اینترنت در ده پانزده ساله اخیر، هنوز مسائل حقوقی مربوط به اعتبارسنجی اسناد یا سوابق رایانه ای از حوزه بحث های روز حقوقدانان خارج نشده و به جهت گستردگی اهمیت موضوع همچنان حتی در کشور آمریکا که توان و سابقه ای بیش از دیگران در فن آوری اطلاعات دارد، مورد بحث و تحقیق قرار دارد. قانون مدنی طی ماده ۱۲۵۸ ادله اثبات دعوی را در ۵ قسم یعنی اقرار، اسناد کتبی، شهادت، امارات و قسم برشمرده 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 «داده پیام» پرداخته و پس از آنکه آن را در ماده ۲ اینگونه تعریف نموده است: «هرنمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا فن آوری های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می شود»، در مواد بعدی به ارزش آن به عنوان دلیل و معادل نوشته پرداخته و در ماده ۶ مقرر می دارد: «هرگاه یک نوشته از قانون لازم باشد، داده پیام در حکم نوشته است» و در ماده ۱۲ به طور کلی می گوید: «اسناد و ادله ممکن است به صورت داده پیام باشد...». در ماده ۵۰ قانون جرایم رایانه ای نیز بدون آنکه وصف خاصی برای محتوای حافظه رایانه ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده باشد و سیستم رایانه ای یا مخابراتی مربوط به نهوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده ها خدشه وارد نشده باشد، قابل استناد خواهد بود.

اگر قائل به احصاء ادله اثبات دعوی به آنچه قانون مدنی ذکر کرده است باشیم، در آن صورت داده پیام مستقل از اقسام ادله به نحو مذکور نخواهد بود و چیزی از این نظر به آنچه در قانون مزبور آمده است نمی افزاید و تنها شکل ظاهری ادله را در مرحله ارائه بیان می کند. اما اگر احصاء را نپذیریم، در آن صورت اولاً مشمول تعاریف علمی از دلیل که برای احتجاج در مقابل دیگری است خواهد بود و عنوان کلی مذکور در ماده ۱۹۴ قانون آیین دادرسی مدنی

نیز بر آن صدق خواهد کرد، ثانیاً می تواند گونه ای مستقل از دلیل و در کنار ادله پنج گانه قانون مدنی به حساب آید.

اینک بحث در این است که گرچه دلیل یا سند به طور خاص ممکن است به صورت داده پیام باشد، ولی آیا این خود محتوای حافظه رایانه است که دلیل به طور کلی، یا سند به طور خاص یا در حکم آن تلقی می شود یا آنچه چاپ و یا روی صفحه نمایشگر آشکار می گردد؟ آیا محتوای رایانه، «نوشته» محسوب می شود 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» بودن دلیل، که اعم است از آنکه روی کاغذ باشد یا روی پوست یا حامل دیگر. اما آیا تراشه های رایانه را می توان حاملی در ردیف کاغذ یا سایر حامل ها محسوب کرد و محتوای آن را به عنوان نوشته به حساب آورد؟ سوال دیگر این است که آیا سند الکترونیک در حد اطمینان آوری قابل انتساب به صادرکننده آن هست یا خیر؟

عامل سومی نیز برای اعتبار داده پیام در قانون تجارت الکترونیکی به تقلید از قانون نمونه آنسترال در تجارت الکترونیک ذکر شده که عبارت است از تناسب مفاد وهدف از داده پیام با روش های موجب اطمینان و ایمنی سامانه. این ملاک، از نظر علمی قابل بحث است و در حقوق مابه این صورت، حتی در اسناد کاغذی، جای تامل دارد. داده پیام معمولاً در پنج قالب قابل مشاهده است: اطلاعات وبگاه، مفاد شبکه های اجتماعی، پست الکترونیک (رایانامه)، پیام های الکترونیک و ذخیره های رایانه ای در تمام انواع فوق، وظیفه محاکم کشورها خواهد بود که به کمک کارشناسان فنی، میزان مصداق داشتن معیارهای اعتبار ادله اثبات در حقوق خود را در این دلیل نوین احراز کنند و معیارهای اعتبارسنجی را در آنها اعمال نمایند.

بخش اول: نوشته محسوب شدن داده پیام

بند اول: ماهیت داده پیام

اگرچه آن هنگام که محتوای حافظه به روی صفحه نمایش کاغذ منتقل می شود، به صورت نوشته است ولی روشن است که خروجی ها اصالت ندارند و تنها نشانگر محتوای حافظه رایانه هستند. آنچه در حافظه موقت یا دائم ذخیره می شود، به صورت نوشته نیست و صرفاً حاصل

تأثیراتی است که اختلاف ولتاژ برق روی موا نیمه هادی که تراشه ها را تشکیل می دهند باقی می گذارد. درست است که هنگام کار با رایانه، علائم و کلمات انسانی تحت عنوان داده وارد ماشین می شوند، ولی به محض فشارروی کلید، یا هروسیله دیگر، آنچه به داخل دستگاه منتقل می شود جریان های متفاوت برق و نحوه قرار گرفتن آثار آنها در کنارهم است که در هر حرف و علامتی با دیگری تفاوت می کند. لذا آنچه روی تراشه یا دیسکت ذخیره می شود، هیچ شباهتی به ورودی ها ندارد و قابل درک توسط انسان نیست. در این صورت، روشن است که مادام که اطلاعات به صورت ذخیره های الکترونیک باشند، عرفا نمی توانند به عنوان « نوشته » محسوب شوند. بدین ترتیب از یک طرف صفحه چاپ شده یا نمایشگر اصالت ندارند و مستقلا سند محسوب نمی شوند و از طرف دیگر کیفیت موجود در تراشه رایانه هیچ شباهتی به نوشته ندارد. برای رفع معضل اعتباربخشی به این وقایع خارجی، آن هم تحت عنوان یا معادل سند، نمی توان آن را به تفسیرهای گوناگون علمی و قضایی واگذار کرد. ممکن است بعضی، بر مبنای قول به عدم احصای ادله در ماده ۱۲۵۸ قانون مدنی، عنوان مستقلی در ادله برای آن قائل شوند که بیراه نیست. در حقوق کشورها بایستی موضعی شفاف و یکنواخت در این خصوص اتخاذ کنند و ارزش گذاری اثباتی چنین امر مهمی را که مبتلا به جهان امروز است، به تنوع تفسیر و تشتت آرای محاکم نسپارند. به همین سبب قانون گذاران کشورها با روش هایی متناسب با ساختار حقوقی خود و بعضا به صورت اقتباس از برخی نمونه های خارجی یا بین المللی، اقدام به پر کردن خلأ مزبور در قوانین خویش کرده اند. فرانسوی ها آن را در قانون مدنی صراحتا سند نامیده اند و در آمریکا در قانون یوتا از آن به عنوان سوابق الکترونیک یاد کرده اند و در قانون قواعد ادله فدرال در ماده ۱۰۰۱ این نوع دلیل را به همراه سایر موارد به شرح زیر تعریف نموده اند.

نوشته عبارت است از حروف، کلمات، اعداد، با معادل آنها که به هر شکلی ذکر شود. سابقه عبارت است از حروف، کلمات، اعداد یا معادل آنها به هر شکلی که ضبط شده باشد. در بند ۷ ماده ۴ قانون یوتا نیز سابقه الکترونیک اینگونه تعریف شده است: « سابقه ای است که با وسایل الکترونیک ایجاد، تولید، ارسال، ایصال، دریافت یا ذخیره شده باشد ». در تعریف قانون نمونه از داده پیام، طیف نسبتا وسیعی از اطلاعات که به طرق گوناگون الکترونیک، نوری یا

وسایل مشابه تولید، ارسال، دریافت و ذخیره می شوند مانند، و نه محدود به مبادلات استاندارد داده ها بین رایانه ها، پست الکترونیک، تلکس، تلگراف، و غیره، مشمول این عنوان می شوند. 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 داده پیام، در صورتی که استفاده از اطلاعات موجود در آن برای مراجعات بعدی میسر باشد، برآورده خواهد شد. ۲- بند ۱ در هر در موردی که محتوای داده پیام را یک تعهد تشکیل داده یا آنکه قانون صرفاً پی آمدهایی را برای نبود نوشته مقرر کرده باشد، قابل اعمال خواهد بود. ۳- مقررات این ماده در موارد زیر اعمال نمی شود». اما قانون تجارت الکترونیک ایران، ابتدا در ماده ۲ داده پیام را با قدری تفاوت تعریف کرده که علی رغم ابهامات، دایره شمول آن محدودتر است و از این نظر مناسب تر به نظر می رسد: «هر نمادی از واقعه، اطلاعات با مفهوم است که با وسایل الکترونیکی، نوری یا فن آوری های جدید اطلاعات تولید، ارسال، دریافت، ذخیره با پردازش می شود» و سپس در صدر ماده ۶ مقرر می دارد: «هرگاه وجود یک نوشته از نظر قانون لازم باشد، داده پیام در حکم نوشته است.....» و در ادامه استثنائاتی را نیز بیان می کند. نکته ای وجود دارد که می توان آن را به عنوان نقد عبارات هر دو قانون و البته با تفاوت در شدت و ضعف مطرح کرد. در هر دو متن می گوید «هرگاه وجود یک نوشته از نظر قانون لازم باشد، ...» مفهوم این عبارت این است که هرگاه قانون لازم نداند، داده پیام در حکم نوشته نیست و این اعتبار را نخواهد داشت. این در حالی است که نوعاً در اسنادی که مردم صادر می کنند، الزام قانونی وجود ندارد و مردم خودشان برای حفاظت از حقوق خویش اقدام به کتبی کردن تعهدات می کنند. 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 می کند، ولی این طور نیست که همه اسناد با الزام قانونی تنظیم شوند یا قانون گذار کتبی بودن دلیل را لازم دانسته باشد. مسلم است منظور قانون گذار این نبوده که اسناد عادی مردم در صورتی که الکترونیک باشند ولی قانون آن را الزامی ندانسته باشد، نوشته محسوب نمی شوند، 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 اندازه‌های ایراد مزبور تعدیل شده ولی چون در قانون ایران آن قسمت ترجمه شده، ایراد فوق جدی تر است.

۲- ارزیابی ویژگی‌های نوشته در داده پیام سه خاصیت در حد نسبتاً بالایی در نوشته‌های کاغذی وجود دارد:

- اول، ثبات با تغییر ناپذیری محتوای سند. این خاصیت در حدی است که معمولاً تغییرات با 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 استاد کاغذی وجود دارد
- سوم، تفاوت نسخه تکثیر شده با نسخه اصلی این ویژگی امروزه با ظهور دستگاههای نسخه برداری با کیفیت بالا، کمرنگ شده ولی قابل تشخیص است. هر قدر وجود عوامل فوق در سندی قوی تر و اطمینان بخش تر باشد، آن سند از درجه اعتبار بیشتری برخوردار خواهد بود.

بخش دوم: بررسی حقوقی ثبات سند

مقصود، عدم تغییر و محفوظ ماندن تمامیت است. در قانون نمونه آنستیرال از کلمه 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 در خصوص اصالت به معنای دوم، بحث جداگانه‌ای را خواهیم داشت. در حالی که ثبات در اسناد ملموس مانند کاغذی، چوبی، سنگی و امثال آنها راحت‌تر حاصل می‌شود و معمولاً اعمال هر گونه تغییری در آنها اولاً دشوار است و ثانیاً بهتر قابل کشف است، این امر در داده پیام بدون تمهیدات خاص قابل حصول نیست و امکان تغییرات در مندرجات آنها به دفعات و بدون آن که نشانه و اثری از خود 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.

از طرف دیگر، معمولاً استاد کاغذی توسط خود افراد یا تحت نظارت نزدیک آنان تنظیم و مبادله می شوند در حالیکه در داده پیام، اشخاص و تجهیزاتی دخالت دارند که معمولاً همه آنها تحت نظارت و پایش مستقیم صادر کنندگان سند نیستند. بدین ترتیب لازم است ثبات محتوای سند پس از تولید و طی زمان ارسال تا وصول و ذخیره، یا اعمال نمودن روش های فنی اطمینان بخش، به نحو قابل قبولی تأمین شود. گرچه همان طور که نشان خواهیم داد، با تمهیدات لازم فنی، داده پیام می تواند 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 علی رغم روش ها و استانداردهای فنی زیاد، همواره امکان نفوذ عوامل بیگانه به داخل شبکه و تهدیدات نسبت به آن وجود دارد. در حقوق آمریکا، اعتبار سوابق الکترونیک منوط به وجود شرایط ذیل دانسته شده است:

الف- اطمینان بخش و استاندارد بودن تجهیزات رایانه ای

ب- ورود داده ها 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.

بندهای ۱ و 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.

قانون نمونه آنسیترال در بند ۱- الف ماده ۸ تصریح نموده است که هرگاه قانون مقرر کرده باشد اطلاعات به صورت اولیه خود ارائه با نگه داری شوند، این امر در مورد داده پیام در صورتی محقق خواهد شد که تضمینی قابل اعتماد در مورد محفوظ ماندن تمامیت اطلاعات از زمان تولید آن به شکل نهایی، به عنوان داده پیام با عنوان دیگر، وجود داشته باشد. برخی مواد دیگر از جمله بند ب ۱- ماده ۱۰ نیز به نوعی تکرار یا حداقل به دلالت التزامی بازگو کردن همین شرط است: «داده پیام به همان صورتی که تولید، ارسال یا دریافت شده یا به صورتی که بتواند اطلاعات تولید، ارسال با دریافت شده را ارائه نماید نگه داری شده باشد» در مورد بند اخیر، راهنمای آنسیترال نکته ای را متذکر شده است. بدین شرح که منظور از ثبات آن نیست که همواره داده پیام بدون هیچ گونه تغییری ولو آنکه منجر به تغییر در محتوای سند نشود باقی

بماند، ممکن است اسناد به صورت فشرده، باز گردان شده از کدهای اولیه و به صورتی ظاهر متفاوت با حالت اول ذخیره شوند ولی همین که در تمام این موارد امکان بازبازی اطلاعات به شکل اولیه وجود داشته باشد، کفایت خواهد کرد. روشن است که تعیین اینکه چه روش های فنی تضمین های مذکور را تامین می کند، مطلبی نیست که قانون به آن بپردازد بلکه طبیعتا تابع شرایط و مطابق استانداردهای فنی روز است. در مقام قضاء نیز قاضی برای احراز وجود شرایط مزبور، معمولا مورد را به کارشناسان ذیربط ارجاع می دهد مگر آنکه اوضاع و احوال از نظر وی به اندازه کافی روشن باشد با طرفین دعوی در آن اختلافی نداشته باشند. از روش های مطمئن در تأمین شرط عدم تغییر سند الکترونیک، فناوری رمزنگاری است که امضای دیجیتال بر آن مبتنی است. ما در مبحث امضاء به این مطلب خواهیم پرداخت ولی در اینجا این نکته را متذکر می شویم که قابلیت استناد به داده پیام منوط به داشتن امضا نیست و بسیاری از پیام های تجاری بدون امضا به معنای رایج و رمزنگاری است و صرفا با ذکر نام ارسال کننده و نشانی الکترونیک او شناسایی می شوند. 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 به عنوان دلیل (سند) مورد استناد قرار گیرد مانند حساب های بک شرکت که به صورت الکترونیک تهیه و نگهداری شوند.

بخش سوم: بررسی و تحلیل حقوقی دوام سند

یکی دیگر از ویژگی های نوشته آن است که مانند ادله شفاهی زودگذر نیست و برای مدتی به تناسب جنس آن باقی می ماند و در نتیجه این امکان را فراهم می آورد که برای دفعات مکرر به آن مراجعه و در صورت 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 می دارد: «هرگاه قانونا لازم باشد که اطلاعات ارائه شود، امکان ارائه آن به شخصی که لازم است، وجود داشته باشد.»

علاوه بر این ماده ۱۰ قانون مزبور نیز تماما به شرایط لازم برای نگه داری از سند پرداخته است: ۱- هرگاه قانون مقرر داشته باشد که استناد، سوابق با اطلاعات خاصی نگهداری شوند، آن امر با نگه داری داده پیام محقق می شود منوط به آنکه شرایط زیر حاصل شده باشد

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

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

ج - اطلاعاتی که احیاناً وجود داشته است تا مبدأ و مقصد داده پیام و تاریخ و زمان ارسال و دریافت را نشان دهد، نگه داری شده باشد.

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

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

ذخیره کردن در چند حامل مانند دیسکت های متعدد و یا حافظه چند رایانه و ارسال از طریق اشخاص ثالث مانند اداره پست یا سپردن همزمان نزد آن، می تواند صورت هایی برای تأمین شرط دوام داده پیام به شرح فوق باشد.

بند ج نیز استناداردی را برای معرفی خود سند مقرر نموده که عبارت است از اطلاعاتی که مشخصات مبدأ، مقصد، تاریخ و زمان ارسال داده پیام را بیان می کند.

آنستیرال در توضیحات خود، موارد فوق را بالاتر از استاندارد های قوانین ملی در استاد کاغذی می داند اما می توان چنین نظری را نپذیرفت. زیرا اولاً این موارد در اسناد کاغذی نیز معمولاً رعایت می شود و حتی در برخی از اسناد مانند اسناد تجاری، بارنامه و بیمه نامه جزء ضوابط و شرایط قانونی شکل گیری آنها است و عدم رعایت آن ملاحظات ایراد قانونی جدی به همراه دارد، ثانیاً قوانین ملی به لحاظ منطق حقوقی ثبایستی اعتبار هر گونه 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 هر گاه قانون ملی لازم بداند که اسناد و سوابقی نگه داری 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 استاد 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 اطلاعاتی است که به موجب استانداردهای فنی سامانه و به طور خودکار به داده پیام افزوده می شود تا ترتیب ارسال و دریافت آنرا بدهد و از آنجا که توسط طرفین ایجاد نمی شود، سند آنها محسوب نمی گردد و بنابراین مشمول بند ۱ نیز نخواهد بود. ضمن آنکه ممکن است در اوضاع و احوال خاصی، آن موارد فرینهای را برای اثبات امری تشکیل دهند که در آن صورت با کسب نظر از کارشناسان مربوطه برای دادگاه قابل استفاده و استناد خواهد بود.

مقررات ماده ۸ قانون یو تا 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 نگه داری داده پیام مرتبط با حوزه مسئولیت خود مقرر نموده فراهم شده باشد». بند مزبور مانند آن است که طرفین تجاری یک قرارداد برای مبادله اسناد بین خودشان استانداردهای ویژه ای را مقرر کرده باشند، که در آن صورت فیمابین آنان لازم الرعایه خواهد بود. ولی باید گفت در هر حال عدم رعایت این شروط، تنها اثر خاصی را که سازمان با طرفین در مورد سند مزبور در نظر داشته اند (مثلا برای ذکر تاریخ تقاضا یا نوشتن عنوان بخش معینی از یک اداره بزرگ در مکاتبات) منتفی می کند و گرنه تا بدانجا که به ادله اثبات دعوی به طور عام مربوط می شود، همان داده پیام نیز عند الاقتضا قابل استناد خواهد بود.

بخش چهارم: واکاوی حقوقی اصالت در برابر کپی

مقصود از اصالت در اینجا، اصل در برابر کپی است. در محیط رایانه ای می توان به هر تعداد که بخواهیم از یک سند تکثیر کنیم به طوری که هیچ کدام 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 و گرنه آن سند از عداد ادله خارج خواهد شد (م ۹۶ ق آد). مشابه این قاعده در سایر نظامهای حقوقی نیز وجود دارد و در کامن لو از آن به قاعده اصل سند تعبیر می کنند. نقطه نظر دوم مربوط می

شود به استادی که خود آنها مقوم و پدید آورنده یک تعهد هستند مانند اسناد تجاری (مواد ۲۲۳، ۳۰۸ و ۳۱۱ ق، ت) که با صدور آنها یک عمل حقوقی خاص تحقق می پذیرد و همچنین اسنادی که مادام که در دست طلبکار هستند، مدیون نمی تواند ادعای براءت ذمه کند، مانند بارنامه دریایی (بند ۷ ماده ۵۲ ق. د). بارنامه سند مالکیت کالا است و امکان وجود نسخ متعدد یکسان نزد افراد مختلف، تحویل بار را به ارائه دهنده آن مشکل می سازد.

علی رغم 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 با سابقه به معنای خود نوشته با سابقه با هر گونه نسخه متناظری است که برای داشتن همان اثر توسط شخص تولید با صادر کننده موردنظر بوده است. برای ذخیره های الکترونیک اصل به معنای هر گونه چاپ با خروجی دیگری از آن است که توسط چشم قابل خواندن باشد منوط به آن که به طور درست اطلاعات آن را منعکس نماید.

رونوشت به معنای نسخه متناظری است که به طریق ماشینی، عکاسی، شیمیایی، الکترونیک با روش با تکنیک معادل دیگری به درستی اصل را تولید مجدد نماید. ملاحظه می شود که نسخه های مکرر از یک سابق الکترونیک، مشمول هردو عنوان اصل و رونوشت با تعاریف فوق می شوند اما در انگلستان قانون ادله مدنی قاعده عامی را طی مواد ۱ و ۸ در قابلیت جایگزین شدن کپی در دادرسی در صورت فقدان اصل وضع کرده است که اجمالاً می تواند در مسأله اول ما که ادله اثبات است کاربرد داشته باشد. مطابق ماده ۸ مزبور: «هرگاه پذیرش مندرجات یک سند در یک دادرسی مطرح باشد این امر می تواند 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 آنه. مشابه این ترتیب در حقوق آمریکا نیز پذیرفته شده است. 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 نمی شود، 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 پرونده ای حکم بر محکومیت آنان در ادای دین خود بدون تضمین های لازم صادر کند. برخی آرای صادره از محاکم آمریکا و انگلیس مبتنی بر استناد به کپی سند به جای اصل. همگی مستظهر به قرائن قضایی که نقیصه مدارک ارائه شده را جبران می کرده بوده است. به هر حال به لحاظ بر خطر بودن اعتماد به کپی برابر اصل، و نیاز آن به حکم قاضی در هر مورد، عملاً تا کنون این گونه اسناد به صورت الکترونیک رواج نیافته اند و حتی علی رغم اجراشدن طرح های حقوقی - فنی سنگین و ارائه سامانه های ویژه با همکاری سازمان های بین المللی، تجار رغبتی به استفاده از آن سامانه ها نشان نداده اند. شاید به همین سبب بوده باشد که قانون نمونه آنسیترال، آنجا که سند الکترونیک را معادل کاغذی می داند (م ۶)، باز برای کشورها حق تعدیل (رزرو) قائل شده است تا برخی موارد را مستی کنند که بر همین اساس قانون ایران سند مالکیت اموال غیر منقول (و نسخه دارو و هشدارهای ایمنی) را از شمول اعتبار داده پیام 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 بین المللی ۲۰۰۵، 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 کی نظر دارد تا بتواند شمول آن را بر معاهده ۱۹۵۸ نیویورک در شناسایی و اجرای احکام داوری خارجی که ارائه اصل موافقت نامه داوری را لازم می داند، تأمین کند و از طرف دیگر بنا به مقتضیات و ملاحظات عملی، در بند ۲ ماده ۲، اسناد تجاری و بارنامه ها را، از شمول معاهده مستثنی کرده است: « این معاهده در مورد برات، سفته، راه نامه، بارنامه، قبض انبار یا هر گونه سند قابل انتقال با سندی که حامل با ذینفع را برای تحویل کالا با پرداخت مبلغی پول ذی حق می سازد، اعمال نمی شود.»

در واقع می توان گفت عملاً امکان طرح مسأله اصل در برابر کپی در اسناد رایانه ای مشکل، و برآورده ساختن نیاز عملی کاربران در این زمینه با مانع فنی مواجه است و فن آوری اطلاعات نتوانسته به استانداردهای حقوقی پاسخ مناسب دهد. زیرا اولاً نسخه اصل همان است که در ابتدا روی حافظه موقت رایانه تشکیل می گردد و از آن لحظه به بعد آنچه که روی حافظه

جانبی اعم از دیسکت سخت، سی دی و سایر وسایل ذخیره، ارسال و یا چاپ و نمایش داده می شود، همگی کپی محسوب می شوند، و ثانیاً امکان تولید، ارسال و ذخیره مجدد و یا ارسال نسخه های متعدد از نسخه اولیه وجود دارد و نمی توان علی رغم تمهیدات فنی، عاملی قطعی برای جلوگیری از تولید نسخه های مکرر با تمیز آنها از اصل، در حدی که اعتماد تجار و بانک ها را جلب کند، در اختیار کاربران گذارد.

به تعبیر دیگر، حتی در مسأله اول (ادله اثبات)، منطق لزوم ارائه اصل سند توسط مدعی در عالم حقوق همچنان پابرجا است و سطح فن آوری موجود جهان نمی تواند تأمین کننده این استاندارد حقوقی باشد. قوانینی نیز که مقرر می دارند داده پیام با سند الکترونیک به جای سند کاغذی قابل استناد است، مفاد آنها ملازمه یا نفی قاعده اصل سند ندارد مگر آن که حکم صریحی در این زمینه از سوی قانون گذاران 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 نمی تواند رفع کند و به ویژه در مسأله دوم، نیز آنان مطابق قوانین خاص اسناد مشروحه فوق، مادام که اصل را دریافت نکنند معمولاً خطر نمی کنند و پول و کالا را در برابر کپی تحویل نمی دهند. البته می توان گفت در صورتی که تاجری قبلاً با طلب کار در استفاده از سند الکترونیک آن توافق لفظی با عملی کرده باشد حق نخواهد داشت بعداً به عدم اصالت واقعی سند مزبور استناد کند زیرا در واقع از حق ایراد مزبور قبلاً صرف نظر کرده است. در غیر این صورت نمی توان او را ملزم به پذیرش سندی کرد که هیچ اطمینانی در نبود نسخه های مکرر یکسان از آن نزد سایرین وجود ندارد.

بخش پنجم: قابلیت انتساب سند الکترونیک

وقتی سندی معتبر است که بتواند به صادر کننده اش منتسب شود. اثبات این امر محدود به روش خاصی مانند امضا با غیر آن نیست و می تواند با هر دلیلی از ادله پنجگانه اثبات دعوی حاصل گردد. ادله اثبات انتساب را می توان به دو قسم برون سندی و درون سندی طبقه بندی کرد. گروه اول شامل اقرار صادر کننده، گواهی شهود و امارات قضایی یعنی قرائن و اوضاع و احوالی است که قاضی بر اساس آنها قانع می شود سند توسط شخص معینی صادر شده است. اما گروه دوم امضا، مهر، دستخط و هر گونه قرینه ای در درون خود سند را در بر می گیرد.

ضمن آن که در موارد اخیر نیز هرگاه مدعی علیه نسبت به آنها انکار، تردید با 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، علاوه بر ایفای نقش اثبات انتساب سند به صادر کننده، نقشی ماهوی را نیز در به وجود آمدن آن ایفا می نمایند. به طوری که حتی اگر کاملاً محرز باشد که سند توسط خواننده 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 با بارنامه از اینگونه هستند و بدون امضا یا مهر اصلاً به وجود نمی آیند تا بتوان بر اساس آنها طرح دعوی نمود و اثبات انتساب آنها به صادر کننده اثر خاص قانونی را در پی نخواهد داشت. این اسناد، علاوه بر دلیل اثبات دعوی بودن، صدورشان عمل حقوقی محسوب می شود.

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 در حالی که در مرحله دوم، صحت و ایمنی سامانه الکترونیک از مبدأ تا مقصد مورد توجه است. ۱- امضای الکترونیک معمولاً قانون گذاران امضا را تعریف نکرده اند و این امر و مصادیق آن را به عرف واگذار نموده اند. عرف نیز هر گونه علامت دستی، حروف یا ترکیب آن و علامت ها را امضاء محسوب می کند. در برخی کشورها نظیر کشورهای با حقوق عرفی، مهر نیز از انواع امضاء تلقی می شود. ولی در سایر کشورها از جمله ایران، مهر با امضاء ظاهر متفاوت است. به همین سبب ماده ۲۲۳ قانون تجارت می گوید: «برات علاوه بر 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 می شود، 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 فی الواقع امضاء با مهر کرده است. در هر حال، در فضای الکترونیک نیز امضای سند مطرح است منتهی با دو ملاحظه خاص:

یک - ماهیت امضای الکترونیک از جنس همان فضا است به طوری که همراه و جزء سند می شود. در این خصوص ماده ۲ قانون نمونه آنستیرال در امضای الکترونیک در ضمن تعاریف خود چنین می گوید: امضای الکترونیک عبارت است از داده هایی به صورت الکترونیک که

برای تعیین هویت امضاء کننده داده پیام و نشان دادن قبول اطلاعات موجود در آن توسط وی به داده پیام ضمیمه با منطقه همراه می شود.

دو - با عنایت به فن آوری های گوناگون، علاوه بر تفاوت در درجات اطمینان بخشی در صدور سند، گونه هایی از آنها این امکان را نیز فراهم می آورند که هر گونه تغییر پس از صدور در آنها آشکار شود. آنچه با اسکن کردن امضای دستی یک شخص و ذخیره آن در رایانه حاصل می شود، از مصادیق حداقلی امضای الکترونیک است. این گونه امضا تنها این امکان را فراهم می آورد که امضاهای صاحب آن در موارد آنی با آنچه در رایانه ذخیره شده است مقایسه و صحت امضاء توسط کاربر رایانه تأیید شود. این همان کاری است که در بانک ها برای پرداخت چکها رایج است. کلیک کردن روی عباراتی نظیر «قبول دارم» یا «پرداخت شود»، در وبگاه فروشگاه مجازی نیز امضای مشتری محسوب می شود. زیرا این عمل با عنایت به مشخصات وی، نظیر نشانی الکترونیک و شماره کارت پول و رمز آن که به سامانه منتقل می شود، همان خاصیت و عملکرد امضا را در انتساب به شخص معین دارد اما در فن آوری اطلاعات، روش های کامل تری نیز برای امضا ابداع شده است که نه تنها درجه اطمینان زیاد تری را نسبت به امضای دستی در امر اثبات انتساب داده پیام به صادر کننده آن موجب می شود که افزون بر آن، هر گونه تغییر در مندرجات سند پس از صدور آن را نیز برملا می سازد. امضاهای اخیر همگی مبتنی بر فن آوری رمزنگاری و با بهره گیری از فرمول های ریاضی هستند.

به لحاظ قابلیت های بالای اینگونه امضاها بوده است که قوانین کشورها و نیز قوانین نمونه آنستیرال احکام خاصی را در ارتباط با آنها در نظر گرفته اند. در عین حال قوانین مزبور به لحاظ منطق حقوقی، تنها به ذکر اوصاف لازم امضاها الکترونیک برای اعتبار یافتن داده پیام پرداخته اند و نسبت به نوع فن آوری آنها موضع خاصی اتخاذ نکرده اند. ماده ۶ قانون نمونه آنستیرال، شرایطی را برای اعتبار این گونه امضا در نظر گرفته که به اجمال در ماده ۱۰ قانون تجارت الکترونیک ایران تکرار شده است.

علاوه بر امضاهای دیجیتال که ماهیتی برنامه ای دارند، امضاهایی که مبتنی بر 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 با شبکه چشم افراد به داخل رایانه و ذخیره کردن آن، این امکان به وجود می آید تا هر بار که صاحبان از آنها استفاده کنند، با آنچه ذخیره شده مقایسه و در صورت مطابقت، تأیید شود. در زمینه این گونه امضاها نیز ایده ها و روش های فنی متعددی مطرح شده که از سطوح ایمنی و کاربردی متفاوتی برخوردارند. امضاهای اخیر فعلاً بیشتر در تشخیص هویت در مبادی ورودی و امثال آن کاربرد دارند.

بخش ششم: بررسی و تحلیل حقوقی ارزیابی قابلیت ها

بند اول: کفایت امضای الکترونیک

با عنایت به قابلیت های متفاوت امضاهای الکترونیک با ساختارهای گوناگون، برخلاف امضای دستی، طبیعتاً جای این بحث باز می شود که احکام حقوقی آنها چیست؟ قانون نمونه (۱۹۹۶) در ماده ۷ به طور کلی شرایط و کار کردهایی را که یک روش امضا باید داشته باشد تا در ردیف امضای مورد نظر قوانین ملی قرار بگیرد بیان نموده است: ۱- هرگاه قانون امضای شخصی را لازم بداند، آن اقتضاء در صورتی در ارتباط با داده پیام برآورده خواهد شد که الف - روشی استفاده شود که آن شخص و قصد او را برای پذیرش اطلاعات موجود در داده پیام معلوم کند.

ب - روش مزبور با توجه به تمام اوضاع و احوال از جمله توافق های مربوطه، متناسب با مقصودی که برای آن داده پیام تولید با 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 می کند: «امضای الکترونیک در صورتی برای برآورده کردن شرایط مذکور در بند ۱ قابل اعتماد خواهد بود که

الف - داده های تولید امضاء، در متنی که استفاده می شوند به صاحب امضاء مربوط باشند نه شخص دیگر.

ب - داده های تولید امضاء، در زمان امضاء در اختیار صاحب آن باشد به شخص دیگر. ج - هرگونه تغییری در امضای الکترونیک پس از امضاء قابل تشخیص باشد.

د- هرگاه مقصود قانون گذار در امضاء، آن بوده که تأمینی برای عدم تغییر در اطلاعات مرتبط با امضاء به وجود آید، هر گونه تغییری در اطلاعات مزبور پس از امضاء قابل تشخیص باشد.

ماده ۲ دستورالعمل جامعه اروپایی در امضای الکترونیک 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 غیر مطمئن تقسیم بندی کرده احکام خاصی را برای گونه مطمئن در نظر گرفته است: «امضای الکترونیک مطمئن باید دارای شرایط زیر باشد

الف - نسبت به امضا کننده منحصر به فرد باشد.

ب - هویت امضاء کننده داده پیام را معلوم کند.

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

د - به نحوی به یک داده پیام متصل شود که هر تغییری در آن داده پیام قابل تشخیص و کشف باشد. «ایرادی به تمام متون فوق که ظاهراً از هم اقتباس کرده اند، به چشم می خورد. بدین شرح که در تمام آنها بین شرایط خود «امضاء و عمل امضا کردن» خلط شده است. این که هنگام امضا کردن، داده های آن در اختیار صاحب امضا با وکیل او بوده یا نبوده، و به عبارت دیگر به وسیله امضا کننده (صاحب امضا) با 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.

بند دوم: تشخیص هویت امضاء کننده

این امر با عنایت به انواع امضاهایی که در فضای الکترونیک وجود دارد، به صورت های مختلف و البته با ضریب اطمینان های متفاوت قابل تحقق است. در امضاهای با ساختار پیچیده تر، احراز هویت امضاء کننده با ضریب اطمینان بالاتری صورت می پذیرد. امضاهای مبتنی بر زیست سنجی، مانند تحلیل و ذخیره ساختار نقش سر انگشتان یا شبکیه چشم هر شخص در رایانه، علاوه بر آن که ضریب اطمینان بسیار بالایی را موجب می شود، مشکل سوء استفاده از امضا را توسط فرد غیر مجاز را نیز تقریباً منتفی می کند. در این موارد سوء استفاده ممکن است با به کار گیری انگشتان صاحب امضا مثلاً در حال بیماری او صورت گیرد. در فن آوری

رمزنگاری از طریق امضای دیجیتال، و اضافه شدن گواهی مرجع تأیید به آن که مشابه گواهی امضا در دفاتر رسمی است، مقصود فوق بهتر تأمین می شود. در این روش، و البته در نوعی که به آن رمزنگاری نامتقارن می گویند، دو برنامه رایانه ای به عنوان کلیدهای عمومی و خصوصی توسط مرجعی معتبر تولید می شوند و به شخص متقاضی اختصاص می یابند، ضمن آن که سوابق آمر نیز برای صدور گواهی و اعلام مدت اعتبار امضا نگه داری می شود. کلید خصوصی تنها در اختیار صاحب امضا است ولی کلید عمومی مانند شماره تلفن در اختیار همه می تواند باشد و توسط دفتر گواهی در سایت آن نیز برای اطمینان طرفها اعلام می شود. صاحب امضا (الف)، متن نوشته شده را با کلید خصوصی خودش به صورت رمز در می آورد و برای شخص مورد نظر (ب) ارسال می کند. ب متن را به کمک کلید عمومی مربوط به الف، رمزگشایی می نماید. اگر متن مزبور از سوی الف ارسال نشده باشد، رمزگشایی نمی شود و نیز اگر در جریان ارسال تغییری در متن صورت گرفته باشد، آشکار می گردد. البته می توان متن را با کلید عمومی گیرنده رمز و برای او ارسال کرد که در این صورت تنها با کلید خصوصی گیرنده رمزگشایی می شود. روش اخیر، امضای سند توسط صادر کننده محسوب نمی شود ولی این خاصیت را دارد که اگر متن به هر سببی در اختیار شخصی غیر از مخاطب مورد نظر قرار گیرد، قابل بازگشایی نباشد. می توان هر دو کار را برای اطمینان بیشتر به طور توأمان انجام داد که البته روند کار را کند خواهد کرد. آنچه که از فن آوری رمزنگاری می توان تحصیل نمود، حداکثر عبارت از این است که سند ارسال شده با کلیدهای اختصاص داده شده به شخص الف به صورت رمز در آمده است. ولی این امر ملازمه ندارد با اینکه حتما 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 حامل های جانبی رایانه ای ذخیره می شوند، ممکن است توسط اشخاص دیگر به کار گرفته شده باشند. قسمت های الف و ب از بند ۳ ماده ۶ قانون نمونه ۲۰۰۱ از این نکته غافل نبوده و در ضمن ذکر شرایط اطمینان بخش بودن امضاء در حدی که قانون لازم می داند مقرر داشته است:

الف - داده های تولید امضا در زمینه ای که مورد استفاده قرار می گیرند، فقط به امضا کننده و نه شخص دیگر مرتبط شده باشند،

ب - داده های تولید امضا در زمان امضا کردن تحت کنترل امضاء کننده و به شخص دیگر باشند...، و باز در ماده ۸ به وضوح تحت عنوان مراقبت های رفتاری صاحب امضا مقرر می دارد: « هرگاه داده های تولید امضا برای امضایی که اثر قانونی داشته باشند به کار رود، صاحب امضا باید:

الف - مراقبت های معمول را برای جلوگیری از استفاده غیر مجاز از امضا به عمل آورد.

ب- در موارد زیر، بدون تأخیر ناموجه با وسایلی که دفتر گواهی امضا طبق ماده و در اختیار گذارده است با 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 داده های 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 داده های تولید امضای (او) می گردد

ج- در مواردی که گواهی امضا برای پشتیبانی از آن صادر می شود، مراقبت های 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 می شود که علی رغم ذکر مواردی که برای حفظ شرایط انتساب امضای الکترونیک به صاحب آن هست، باز این احتمال داده شده است که شخص غیر مجازی از آن استفاده کرده باشد. لذا قسمت ب را به شرح فوق ذکر نموده و در ادامه نیز اضافه می کند: «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 مراقبت های لازم را انجام داده باشد ولی در عین حال امضای او مورد سوء استفاده دیگران قرار گرفته باشد، نمی توان گفت که سند منتسب به اوست و او به طور مطلق، مسؤول اتفاقاتی

خواهد بود که رخ داده با متعهد در قراردادی است که هرگز منعقد نکرده است. اما قانون تجارت الکترونیک ۱۳۸۲، پس از آنکه در ماده ۱۴ شرط اعتبار داده پیام مطمئن را از نظر تولید و نگهداری توضیح می دهد، در ماده ۱۵ به طور مطلق مقرر می دارد: انبست به داده پیام مطمئن، سوابق الکترونیکی مطمئن و امضای الکترونیکی مطمئن انکار و تردید مسموع نیست و تنها می توان ادعای جعلیت به داده پیام مزبور وارد و با ثابت نمود که داده پیام مزبور به جهتی از جهات قانونی از اعتبار افتاده است. بدین ترتیب احتمال سوء استفاده از امضای صاحب آن بدون تقصیر وی را نادیده گرفته و حتی آثار اسناد رسمی را بر آنها بار کرده است. ضمانت اجرای شدید ماده ۱۵، در هیچ یک از سه قانون نمونه آنسیترا ۱۹۹۶ و ۲۰۰۱ و معاهده ۲۰۰۵ و دستور العمل ۹۳/۱۹۹۹ جامعه اروپا در امضای الکترونیک و قوانین آمریکا دیده نمی شود و حتی در قانون نمونه ۲۰۰۱ به شرح فوق، بر خلاف آن پیش بینی هایی نیز شده است و برخی نویسندگان، به وجود حق انکار برای صاحب امضا در حقوق امریکی تصریح کرده اند. درست است که از نظر فنی، تقریباً امکان مشابه سازی امضای دیجیتالی وجود ندارد و از این حیث انتساب آن توسط دارنده قابل انکار نیست، ولی استعمال کلید خصوصی توسط فرد غیر مجاز کاملاً محتمل و بی ارتباط با سطح فن آوری امضا است. این موضوع، از دیدگاه کیفری نیز قابل بررسی است زیرا سوء استفاده از مهر با کلید خصوصی دیگران امری بعید نیست.

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. 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 با حکم قضائی ابطال شود. رسمیت سند منوط به آن است که مطابق ماده ۱۲۸۷ قانون مدنی صادر گردد، اعم از آن که به صورت 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 می شود و سپس امضای او اخذ می گردد اعم از آن که 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 می توان 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 با 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 فرار می گیرد و اصلاً امضای مطمئن به وجود نمی آید و بدین ترتیب قضیه مزبور از شمول احکام مواد ۱۰ و ۱۵ خارج می شود. علاوه بر این، از ماده ۱۸ قانون نیز می توان استفاده کرد. طبق این ماده: در موارد زیر داده پیام منسوب به اصل ساز است: الف- اگر توسط اصل ساز و یا به وسیله شخصی ارسال شده باشد که از جانب اصل ساز مجاز به این کار بوده است..... مفهوم این بند آن است که اگر اثبات شود داده پیام از سوی اصل ساز با 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: «داده پیامی که بر اساس یکی از شروط زیر ارسال می شود مخاطب حق دارد آن را ارسال شده محسوب کرده و مطابق چنین فرضی (ارسال شده عمل نماید: الف- قبلاً به وسیله اصل ساز روشی معرفی و با توافق شده باشد که معلوم کند آیا داده پیام همان است که اصل ساز ارسال کرده است، ب- داده پیام دریافت شده توسط مخاطب از اقدامات شخصی ناشی شده که رابطه اش با اصل ساز با نمایندگان وی باعث شده تا شخص مذکور به روش مورد استفاده اصل ساز دسترسی یافته و داده پیام را به مثابه داده پیام خود بشناسد.» و در ماده ۲۰ می گوید: «ماده ۱۹ این قانون شامل مواردی نیست که پیام از اصل ساز صادر نشده باشد و یا به طور اشتباه صادر شده باشد.» یکی از مواردی که داده پیام از سوی اصل ساز (صاحب امضا) صادر نشده، موردی است که دیگری بدون اجازه، از امضای الکترونیک او استفاده کرده و داده پیامی را ارسال نموده باشد که در این صورت قابل انکار و تردید خواهد بود.

بند سوم: تناسب مفاد سند با روش های ایمنی

اصولا هدف از امضای سند، پذیرفتن مفاد آن است. در این مورد فرقی نمی کند که نقش سند صرفا محدود به اعلام واقعیتی باشد که مستقل از آن وجود دارد، یا آن که با اقدام به امضاء علاوه بر خلق سند به عنوان 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 مستقیما 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 با سندی باشد بر ضرر امضاء کننده 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 داده پیام، به تناسب روش به کار رفته برای امضا با محتوای سند نیز توجه داشته است؛

هرگاه قانون امضای شخصی را لازم بدانند، آن اقتضا در داده پیام بر آورده خواهد شد اگر:

الف - روشی استفاده شده باشد که آن شخص را شناساند و پذیرش او را نسبت به اطلاعات موجود در داده پیام معلوم نماید.

ب - روش مزبور با عنایت به تمام اوضاع و احوال از جمله توافق مربوط، متناسب با هدفی که داده پیام برای آن تولید یا مبادله گردیده است، قابل اعتماد باشد.

عبارات فوق نشان می دهد که از نظر قانون نمونه، هر امضایی به صرف الکترونیک بودن برای اعتبار داده پیام 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 علی رغم عدم تناسب روش امضا با معامله ای که انجام شده است، طرفین از قبل بر آن روش توافق کرده باشند، آن امضا معتبر خواهد بود. اما 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 داده پیام تناسب نداشته باشد، امضای صورت گرفته

اعتبار نخواهد داشت. در حالی که ممکن است طرفین در ابتدا توافقی بر تناسب مفاد سند با نوع امضا نکرده باشند و ضمناً اختلاف آنان در سایر مسائل باشد. چرا قانون نمونه رأساً و به عنوان یک اصل، اعلام کرده است که اگر تناسب یادشده وجود نداشته باشد، امضا معتبر نخواهد بود و بدین ترتیب اصل سند را بی اعتبار می سازد؟ این ترتیب مستقل از اراده طرفین، گاه به زبان تمام طرف ها و گاه به ضرر برخی از آنان خواهد بود بدون آنکه توجیه حقوقی داشته باشد. البته در تنها در صورتی که در قضیه، شخص ثالثی مانند دولت در اموری مانند مالیات و غیر آن، ذی نفع در بی اعتبار بودن داده پیام باشد، می توان برای مقرر فوق توجیهی یافت، 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 می دارد: «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 می گوید: به طور کلی، ارزش اثباتی داده پیام با توجه به عوامل مطمئن از جمله تناسب روش های ایمنی به کار گرفته شده با موضوع و منظور مبادله داده پیام تعیین می شود. با عنایت به اینکه از جمله روش های ایمنی و از مهم ترین آنها، روش امضا است، اگر تناسبی بین نوع امضا و مفاد سند الکترونیک نباشد، اعتبار سند مخدوش خواهد بود. به هر حال چنین ملاکی در امضاهای غیر الکترونیک معمول نبوده و در قوانین بدان اشاره نشده است. به عبارت دیگر در قانون مدنی با قوانین دیگر، در ایران و سایر کشورها معمول نبوده که قانون گذاران مثلاً از صادر کنندگان چک یا قراردادهای تجاری خواسته باشند در صورتی که ارزش سند از مبلغ معینی بیشتر باشد، روش یا تمهیدات ویژه ای 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 هر حال این تمهیدات با اختیار طرفین قابل اعمال است و دخالت قانون گذار در آن توجیه ندارد.

بله، در یک صورت حکم ماده ۱۳ قابل توجیه و هماهنگی 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 بی اعتباری 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 با سایر ملاحظات ایمنی سامانه در تولید و ارسال باشد. به هر حال این ملاحظات، به عنوان اماره قضائی می تواند برای اعتبار سنجی سند مورد توجه قاضی قرار گیرد ولی قاعده و اصلی همانند آنچه در قوانین مزبور ذکر شده است توجیه حقوقی ندارد.

بخش هفتم: آسیب‌های اعتباردهی به اسناد عادی

این تفاوت در اعتبار اسناد باعث می شود پرونده هایی با موضوع ابطال سند رسمی مالکیت، زمین خواری، فروش مال غیر، فرار از پرداخت های قانونی مانند عوارض و مالیات، تغییر کاربری اراضی و ... روز به روز بیشتر به دستگاه قضایی کشور وارد شوند.

بند اول: فروش یک ملک به چند نفر

یکی از جرائمی که در سال‌های گذشته بسیاری از مردم را متضرر کرده است، فروش یک واحد مسکونی همزمان به به چند نفر است. در این خصوص فروشنده با حضور در بنگاه‌های املاک مکرراً اقدام به تنظیم بیعنامه (که یک نوع سند عادی است) برای یک ملک می کند. در این جرم فرد فروشنده ممکن است در یک روز یک واحد مسکونی را به چند نفر به صورت جداگانه بفروشد و خریدار بی اطلاع از معاملات دیگر او با تحویل گرفتن تنها یک مبایعه‌نامه، میلیون ها تومان پول را به حساب فروشنده قلبی واریز کند. این در حالی است که اگر فرد خریدار برای تنظیم مبایعه نامه به جای مراجعه به بنگاه معاملات املاک به دفاتر اسناد رسمی مراجعه می کرد این کلاهبرداری صورت نمی گرفت. چون با صدور سند رسمی برای یک واحد مسکونی دیگر امکان فروش چند باره آن وجود ندارد و با یک استعلام ساده از ادارات ثبت، مالک واحد مسکونی قابل احراز است.

بند دوم: ضرورت توسعه ثبت رسمی در کشور

با ذکر مثال بالا که مبتلا به جامعه است باید پذیرفت که ریشه بسیاری از اقدامات مجرمانه مثل فروش مال غیر، زمین خواری و ... انجام معاملات غیر رسمی و غیر شفاف است. مثلاً انتقال و تقسیم اراضی مذکور به صورت رسمی و در دفترخانه ها، مستلزم اخذ مجوز لازم از مراجع حامی و ناظر کاربری اراضی کشاورزی و باغ ها و منابع طبیعی است. اما تنظیم مبایعه نامه ها (سند عادی) در خارج از دفترخانه ها بدون مجوزهای مذکور و بی توجه به آن ها صورت

می گیرد. لذا ثبت رسمی معاملات به دلیل ایجاد شفافیت و فراهم کردن قابلیت رهگیری معاملات بهترین راهبرد به منظور حل معضل اسناد عادی است.

بند سوم: پیشگیری از جرائم اقتصادی

علاوه بر این موارد اسناد عادی زمینه فساد اقتصادی و فرار مجرمان را نیز فراهم کرده است. بسیاری از بدهکاران کلان بانکی و نیز کلاهبرداران کلان که مال و پول مردم را تحت پوشش شرکت های لیزینگ، صندوق های تعاونی و... ربوده اند از طریق انتقال عادی املاک، آن ها را نقد کرده و فرار می کنند. اما ثبت اجباری معاملات، سبب شناسایی مالک و امکان ردگیری و پس بینی سابقه معاملات می شود و امکان شناسایی معاملاتی که به قصد فرار از دین انجام می شود را فراهم می کند.

بند چهارم: عدم نیاز به حضور در دادگاه ها

علاوه بر این، ثبت معاملات اموال غیر منقول، ایفای تعهدات طرفین و اجبار آنها به انجام تعهد از طریق اداری و غیر قضایی را ممکن می سازد. در این حالت برای اجبار متعهد به مفاد قرارداد، نیازی به مراجعه به دادگاه و اخذ رای قاضی نیست. مهر سردفتر اسناد برای توسل به قوای قهریه و رسیدن به خواسته کافی است. این ویژگی ثبت رسمی باعث می شود حجم زیادی از ورودی های دادگاه ها کاهش پیدا کند. اما با این که قانونگذار سابقاً سعی کرده بود با اعتبار بخشیدن به اسناد رسمی مردم را به ثبت سند رسمی ترغیب کند، با اعتباردهی مجدد به اسناد عادی باعث شد بسیاری از مردم معاملات خود را در قالب سند عادی تنظیم کنند.

نتیجه گیری

در جمع بندی و نتیجه گیری پایانی مقاله کنونی باید گفت اعتبار محتوای حافظه رایانه، و تعیین جایگاه مشخصی برای آن در میان ادله اثبات دعوی، بدون موضع گیری صریح قانون گذاران قابل تحقق نبود و این مهم نمی توانست به آرا و تفاسیر متنوع دادگاه ها سپرده شود اما مواضع قانون گذاران نیز علی رغم تشابه کلی، به لحاظ طرز تلقی آنها از این پدیده یکسان نیست. برخی از آن به عنوان سوابق الکترونیک (آمریکا)، برخی به عنوان داده پیام (قانون نمونه آنسیترا و ایران و برخی به عنوان سند الکترونیک (فرانسه) از آن نام برده اند ولی همگی کاربرد و جایگاه سند را مستقیماً یا به صورت معادل یا در حکم آن برای این نوع دلیل پذیرفته اند. از میان قانون گذاران، روش فرانسویان به لحاظ آیین تقنین و پیوند این پدیده نوظهور و

احکام آن به بدنه قانونی و فرهنگ حقوقی کشور مدبرانه تر و در عین اختصار، کامل است و می توان در بازمینی 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 آنسیترا ل وارد است. اعتبار سنجی سندهای الکترونیک با محک های 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 می دهد. نکته مهم دیگر، تناسب داشتن مفاد اسناد الکترونیک با شیوه ایمنی به کار گرفته شده در تولید آنها است که گرچه می تواند به عنوان اماره و در اختیار قاضی شناخته شود، ولی نمی تواند 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، بی اعتبار 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 برنامه 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 نسخه ای الکترونیک را ارائه می دهد در حالی که امکان دارد همانند آن در اختیار دیگران نیز باشد. موارد مزبور حاکی از ناتوانی سطح فن آوری روز در پاسخ به استانداردهای دقیق حقوقی است.

منابع و مآخذ

- ۱) آنسیرال (۱۳۹۰)، اعتماد سازی در تجارت الکترونیکی، ترجمه زر کلام ستار، تهران، نشر دانش.
- ۲) اسمدینگاف توماس جی (۱۳۸۷)، قواعد ضروری جهت اعتبار تراکنش های الکترونیکی در عرصه جهانی، ترجمه بختیاروند، مصطفی، مجله حقوقی، ش ۳۸، تهران، مرکز امور حقوقی بین المللی.
- ۳) السان مصطفی وامینی وحید، (۱۳۹۳)، جایگزین بارنامه کاغذی با بارنامه الکترونیکی دریایی، پژوهش نامه بازرگانی، تهران، وزارت بازرگانی.
- ۴) امامی، سین حسن، (۱۳۴۶)، حقوق مدنی، ج ۶، تهران، انتشارات ابوریحان.
- ۵) آهنی، بتول، (۱۳۸۴)، انعقاد و اثبات قراردادهای الکترونیکی، رساله دکتری، دانشکده حقوق و علوم سیاسی دانشگاه تهران
- ۶) جعفری لنگرودی، محمد جعفر، (۱۳۷۲)، ترمینولوژی حقوق، چ ششم، تهران، انتشارات گنج دانش.
- ۷) رضایی، علی، (۱۳۸۷)، حقوق تجارت الکترونیک، چ اول، تهران، نشر میزان.
- ۸) زر کلام، ستار، (۱۳۸۳)، قانون تجارت الکترونیکی و امضای الکترونیکی، مجموعه مقالات همایش بررسی ابعاد حقوق فن آوری اطلاعات.
- ۹) سپاهی، امیر، (۱۳۹۳)، حقوق اسناد، چ اول، تهران، نشر داد گستر.
- ۱۰) فیضی چکاب، غلام نبی، (۱۳۸۹)، اعتبار حقوقی دلیل و امضای الکترونیکی، فصلنامه پژوهش حقوق و سیاست، ش ۳۰، تهران، دانشگاه علامه طباطبائی.
- ۱۱) قناد، فاطمه، (۱۳۸۹)، پیشگیری از سوء استفاده های هویتی در فضای مجازی.
- ۱۲) کاشانی، مومن، نروزی اصفهانی، نوشن، (۱۳۹۰)، زیر ساخت کلید عمومی، تهران، مرکز توسعه تجارت الکترونیکی وزارت بازرگانی.
- ۱۳) کاتوزیان، ناصر، (۱۳۸۷)، اثبات و ادله اثبات، ج ۱، چ پنجم، تهران، نشر میزان.
- ۱۴) مظفر، محمدرضا، اصول الفقه، ج ۲، قم، انتشارات موسسه اسماعیلیان.

