Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

مروری کوتاه به اصالت اسناد و ادله الکترونیک در نظام حقوقی ایران

فتح ا... رحیمی[۱]
زهره حسین میخچی[۲]

تاریخ دریافت: ۹۶/۱/۲۰
تاریخ پذیرش: ۹۶/۵/۱۸

چکیده:

با گسترش حوزه فناوری اطلاعات در تمام ابعاد زندگی بشر حوزه‌های مختلفی از جمله نظام حقوقی تحت تأثیر فناوری‌های نوین اطلاعاتی و ارتباطاتی قرار گرفته، به طوری که داده پیام‌ها از این پس می‌توانند به موجب مقررات فصل دوم قانون تجارت الکترونیک ارزش اثباتی یافته و به عنوان ادله اثبات در محاکم و ادارات دولتی پذیرفته شوند. همچنین از حیث محتوی و امضاء و یا اجرای مفاد و سایر آثار مربوطه، داده پیام بموجب ماده ۱۴ قانون مزبور در حکم اسناد معتبر و قابل استناد در مراجع قضاوتی محسوب شوند. در اسناد الکترونیکی، تحقق مفهوم اصل سند با وجود نسخی که بی واسطه و به طور مستقیم توسط صادرکننده سند ایجاد شده، محل تأمل است. در فضای سایبر به دلیل شیوع عواملی نظیر انکار، تغییر، جعل و دستکاری اسناد و مدارک، اعلام هویت جعلی و .... بحث ارزش اثباتی و همچنین جمع آوری، حفظ تمامیت، اصالت و اعتبار داده پیام و ... برای ارائه در رسیدگی‌های قضایی منجر به چالش‌هایی ازجمله چگونگی عملکرد مجریان قانون در مواجهه با داده پیام‌ها ویا پرونده‌های مرتبط با فضای سایبر شده است، بنابراین صحت انتساب داده پیام به اشخاص ذینفع و صادر کننده و تصدیق آن از سوی مرجع صالح رسمی، محتاج نقد و بررسی است.

کلمات‌کلیدی: دلیل، سند، استناد پذیری، داده پیام، جعل، انکار.

۱- دکتری حقوق بین الملل، استادیار دانشگاه آزاد اسلامی واحد تهران شمال، نویسنده مسئول
رایانامه: Email: rahimif_law@yahoo.com
۲- کارشناس ارشد حقوق خصوصی دانشگاه آزاد اسلامی واحد تهران شمال،

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

❐ مقدمه

در دادرسی‌های الکترونیکی مهم‌ترین بخش فرایند رسیدگی، ناظر به ادله اثبات دعوا است. چرا که دلایل الکترونیکی به شکل داده پیام، انعکاس متفاوتی از سایر دلایل غیر مجازی دارند و به علت دارا بودن ویژگی‌های منحصر به فرد، مستلزم قواعد و تدابیر جدیدی می‌باشند بود. قانون تجارت الکترونیکی مصوب ۱۷/۱۰/۸۲ در مواد ۶ تا ۱۲ خود به جایگاه و ارزش اثباتی ادله الکترونیک در قالب «داده پیام» پرداخته و پس از آنکه آنرا در ماده ۲ تعریف نموده، در ماده ۶ داده پیام را در حکم نوشته، ارزشگذاری کرده است. از آنجا که «نوشته» از بین سایر ادله، تنها در صورت و شکل سند می‌تواند متبلور شود، لذا مسائل حقوقی عدیده ای مرتبط با اعتبار سنجی اینگونه اسناد بین حقوقدانان مطرح می‌شود؛ مثلاً آیا سند الکترونیک در حد اطمینان آوری قابل انتساب به صادرکننده آن می‌باشد یا خیر؟ تشخیص اصل سند از کپی آن و ارائه اصل آن در محاکم، همچنین حفظ اصالت و تمامیت این اسناد الکترونیکی و اینکه تعرض به اصالت این چنین اسناد، چگونه است؟ از مواردی است که تحلیل‌ها و دیدگاه‌های متفاوتی درباره آن‌ها مطرح است.

با مداقه در مواد ۱۴، ۱۵ ... قانون مذکور مبرهن است که قانونگذار کاربرد و جایگاه سند را به صورت معادل یا در حکم آن برای این نوع دلیل پذیرفته و در فصل دوم زیر عنوان «انتساب داده پیام» احکام خاصی را مقرر نموده است؛ کما اینکه در ماده ۲۱ این قانون به نوعی درصدد تفکیک اصل داده پیام از رونوشت (پرینت) آن است؛ در اینصورت، هرگاه قانون لازم بداند که اطلاعات به صورت اصل ارائه یا نگهداری شود، این امر یا نگهداری و ارائه اطلاعات به صورت داده پیام در صورت وجود شرایط ماده ۸ قانون امکان پذیر می‌شود؛ بنابراین، در این مقاله آنچه که محور کار است بررسی و تحلیل جنبه‌های شکلی ادله الکترونیک از قبیل ارزش اثباتی دلایل الکترونیکی و مستند سازی آن‌ها، حفظ اصالت و تمامیت داده پیام، توقیف داده‌ها و سیستم‌های رایانه ای و... می‌باشد که از ابعاد حقوقی، واجد اهمیت ویژه ای برخوردارند.

❐ ۱. دلیل الکترونیک

دلیل در ماده ۱۹۴ ق. آ.د. م عبارت از «امری است که اصحاب دعوا برای اثبات یا دفاع از ادعا به آن استناد می‌کنند» و در اصطلاح حقوق جزا، عبارت است از «هروسیله قانونی که مقام قضایی را در کشف حقیقت و حصول اقناع وجدانی و اتخاذ تصمیم یاری بخشد.» (آشوری، ۱۳۸۸، ص ۲۳۰).

در معنی رایج و مصطلح، دلیل الکترونیک عبارت است از هر داده پیامی که اصحاب دعوا برای اثبات یا دفاع از مدعای خود به آن استناد می‌کنند (شهبازی نیا، عبداللهی ۱۳۸۹، ص ۱۹۴). به موجب ماده ۲ قانون تجارت الکترونیک «داده پیام هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری یا فناوری‌های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود»، بنابراین هر ابزاری ناشی از فناوری اطلاعات اعم از تلگرام، تلکس، ابزارهای نوری و امثالهم جزو منابع دلیل الکترونیک محسوب می‌شوند؛ لذا با مداقه در تعریف ادله الکترونیک، محرز است که

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

«داده پیام»[۳] عنصر اصلی دلائل الکترونیکی می‌باشد.

بموجب ماده ۱۲۵۸ قانون مدنی ادله اثبات دعوی به ۵ دسته یعنی اقرار، اسناد کتبی، شهادت، امارات و قسم تقسیم شده است. از طرفی در ماده ۱۶۰ قانون مجازات اسلامی مصوب ۱۳۹۲ قانونگذار در مقام احصای ادله آن‌ها را «عبارت از اقرار، شهادت، قسامه، سوگند در موارد مقرر قانونی و علم قاضی» دانسته است. برخی را اعتقاد بر این است که چون نظام حقوقی ایران از سیستم ادله تلفیقی برخوردار است (مؤذن زادگان، یوشی، سلیمان دهکردی،۱۳۹۴، ص ۷۷)؛ لذا در این سیستم هر دلیلی صرف نظر از محتوی و شکل آن، درصورتیکه موجب اقناع وجدانی قاضی و علم وی گردد، دارای ارزش اثباتی است؛ بنابراین قالب و شکل ادله الکترونیک به عنوان ادله جدید موضوعیت ندارد (فرهانی، ۱۳۸۶، ص ۸۸)؛ علاوه بر این، برخی نیز معتقدند که چنانچه احصاء دلائل پذیرفته نشود، در آن صورت، داده پیام را می‌توان گونه ای مستقل از دلیل در کنار دیگر ادله به حساب آورد (نوری، نخجوانی، ۱۳۹۰، ص ۲۲۵).

❐ ۲. ماهیت و شکل داده پیام

قانونگذار در ماده ۶ قانون تجارت الکترونیک و همچنین در آخرین اراده خود در ماده ۶۵۵ قانون آئین دادرسی کیفری در باب ارزش اثباتی داده پیام عادی مقرر داشته: «هرگاه وجود یک نوشته از نظر قانون لازم باشد، داده پیام در حکم نوشته[۴] است...». قید در حکم، به سه علت است؛ اولاً باتوجه به تعریف داده پیام، محتوی آن می‌تواند نوشته، صدا، تصویر یا مجموعه ای از آن‌ها و یا هر نماد دیگری از یک واقعیت باشد (زرکلام،۱۳۸۸، ص ۱۷۷). لیکن قانونگذار تمامی این موارد را در حکم نوشته می‌داند.

ثانیاً امری که بعنوان دلیل در دستگاه قضایی ارائه می‌شود، باید در قالب یکی از ادله اثبات دعوا که در قانون آمده است، قرار گیرد (شمس ۱۳۸۸، ص ۹۷)، تا از ارزش اثباتی آن نوع دلیل برخوردار شود.

بدین توضیح که از طرفی داده پیام از نظر قانونی جایگزین نوشته است و از طرف دیگر، قانون هر نوشته ای که برای اثبات دعوا مورد استناد قرار گیرد را سند می‌داند؛ بنابراین به دلیل ویژگی داده پیام (در حکم نوشته) تنها قالبی که ادله الکترونیکی می‌توانند در آن جای گیرند، سند است. ماده ۱۲ این قانون بر اصل لزوم پذیرش اسناد الکترونیکی تصریح و مقرر نموده که «اسناد و ادله اثبات دعوا ممکن است به صورت داده پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان ارزش اثبات داده پیام را صرفاً به خاطر شکل و قالب رد کرد».

بنابراین در نظام سنتی ادله اثبات دعوا هم دلیل الکترونیکی از اعتبار سند برخوردار است

۳- در اسناد بین المللی نظیر قانون نمونه آنسیترال از آن به عنوان دلیل الکترونیک **Electronic evidence** تعبیر شده که اعم از سند و غیر آن است.

۴- نوشته (**Writing**) عبارت است از حروف، کلمات، اعداد، یا معادل آن‌ها که به هر شکلی ذکر شود. ماده ۱۰۰۱ قانون قواعد ادله فدرال (۲۰۱۴) (نشاط، ۱۳۹۳، ص ۹۰).

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

(استنلی، ۱۳۹۱، ص ۴۰). آنچنانکه در ماده ۱۴ قانون تجارت الکترونیک نیز در خصوص ارزش داده پیام مطمئن مقرر شده: «کلیه داده پیام‌هایی که به طریق مطمئن ایجاد و نگهداری شده‌اند، از حیث محتویات و امضای مندرج در آن، تعهدات طرفین یا طرفی که تعهد کرده وکلیه اشخاصی که قائم مقام قانونی آن‌ها محسوب می‌شوند، اجرای مفاد آن و سایر آثار، در حکم اسناد معتبر و قابل استناد در مراجع قضایی و حقوقی است».[۵]

ثالثاً: باید توجه داشت هنگام وارد کردن داده به سامانه رایانه ای، آنچه از حافظه به روی صفحه نمایش یا کاغذ منتقل می‌شود، در ظاهر امر به صورت نوشته است، لیکن ماهیتاً نشانگر محتوای حافظه موقت (رَم) یا دائم رایانه می باشندکه به زبان کامپیوتر (ارقام صفر و یک) است. لذا روشن است مادام که اطلاعات صرفاً به صورت داده‌های الکترونیک باشند، عرفاً نمی‌توانند بعنوان «نوشته» محسوب شوند (صادقی، نشاط،۱۳۹۳، ص ۷۳). بنابراین قانونگذار داده‌های الکترونیک را در حکم نوشته دانسته و مراد از داده الکترونیک نیز بموجب ماده ۵۰ قانون جرائم رایانه ای، موارد مذکور در ماده ۳۲ همان قانون است که عبارت‌اند از داده ترافیک[۶]، اطلاعات کاربر و داده محتوی؛ منتها بموجب همان ماده با احراز دو شرط قابل استنادند. بهر صورت، «چنانچه داده ای 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 نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکار ناپذیری داده‌ها خدشه وارد نشده باشد، ...»؛ بنظر می‌رسد قابلیت ارائه از سوی طرفین دعوا به مراجع قضایی را دارند؛ منتها این «داده پیام» صرفنظر از محتوی، باید به شکلی صحیح و بگونه ای که به اصالت، تمامیت و انکارناپذیری آن‌ها خللی وارد نشود، نگهداری و ارائه شوند.

❐ ۳. انتساب سند الکترونیک

علاوه بر دو قید «مکتوب» و «قابل استناد» بودن دلیل، بموجب ماده ۱۳ قانون تجارت الکترونیک «عوامل مطمئنه» که ویژه اسناد الکترونیکی است، همراه با مصادیقش بیان شده است؛ بنحویکه «ارزش اثباتی داده پیام‌ها با توجه به عوامل مطمئنه از جمله تناسب روش‌های ایمنی به کار گرفته شده با موضوع و منظور مبادله داده پیام، تعیین می‌شود». مفهوم مخالف این ماده ناظر به این است که چنانچه داده پیام فاقد شروط ایمنی یا عوامل مطمئن باشد، از ارزش اثباتی برخوردار نخواهد بود (سوادکوهی فر،۱۳۸۳، ص ۴). بموجب تبصره ذیل ماده ۱۵ آئیننامه استنادپذیری ادله الکترونیک

۵- قانونگذار بعلّت فقدان تشریفات تنظیم سند رسمی در ماده ۱۲۸۷ قانون مدنی؛ دراطلاق سند رسمی بر دلایل الکترونیکی احتیاط کرده است؛ لیکن در مواد ۱۴ و ۱۵ قانون تجارت الکترونیک، ارزش اثباتی داده پیام مطمئن را بیان کرده و آنرا در حکم سند رسمی می‌داند؛ بنابراین اگر دلیل الکترونیکی مطمئن با اسناد سنّتی در تعارض باشد؛ دلیل الکترونیکی که در حکم سند رسمی است، مقدم می‌شود (مؤذن زادگان، ۱۳۸۸، ص ۸۴).

۶- مادۀ ۱ کنوانسیون جرائم سایبر: داده ترافیک، دادۀ رایانه ای است که به ارتباط برقرار شده از طریق سیستم رایانه‌ای مربوط می‌شود. این داده را سیستم رایانه ای ایجاد می‌کند که بخشی از زنجیرۀ ارتباطی را تشکیل داده است و مبدأ، مقصد، مسیر، مدت، تاریخ، اندازه، دوام یا نوع خدمات اصلی ارائه شده را نشان می‌دهد. هر نوع داده ای را که منعکس کنندۀ منظور و مضمون یک ارتباط الکترونیکی باشد، در بر می‌گیرد.

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

مصوب ۱۳۹۳ «روش مطمئن، روشی است که با توجه به نوع داده و طول مدت زمان حفاظت، امکان بهره برداری از داده‌های حفاظت شده را در مراحل بعدی دادرسی ممکن می‌سازد»؛ بعلاوه در بند «ح» ماده ۲ قانون تجارت الکترونیک، خصایصی جهت مطمئن بودن یک سیستم اطلاعاتی برشمرده شده که عبارت‌اند از:

۱ - به نحو معقولی در برابر سوءاستفاده و نفوذ محفوظ باشد؛

۲- سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد؛

۳- به نحوی معقول، متناسب با اهمیت کاری که انجام می‌دهد، پیکربندی و سازماندهی شده باشد؛

۴- موافق با رویه ایمن باشد»

همچنین جهت ایمنی سازی ادله الکترونیک، بند «ط» ماده ۲ قانون تجارت الکترونیک مقرر کرده «رویه ایمن، رویه ای است برای تطبیق صحت ثبت داده پیام منشأ و مقصد آن با تعیین تاریخ و برای یافتن هرگونه خطا یا تغییر در مبادله، محتوا یا ذخیره سازی داده پیام از یک زمان خاص» بنابراین یک رویه ایمن، موجب حفظ صحت و استنادپذیری ادله الکترونیک با استفاده از الگوریتم‌ها یا کدها، کلمات یا ارقام شناسایی، رمزنگاری[۷]، یا طرق ایمنی مشابه شود. در نتیجه، داده پیامی که شروط ایمنی یا عوامل مطمئن در آن رعایت شده، از ارزش اثباتی برخوردار و قابل انتساب است. با این وجود در رویه عملی جهت ایمن سازی اطلاعات تاکنون اقدامی صورت نگرفته است (ساردویی نسب، ۱۳۹۳، ص ۸۳).

با عنایت به اینکه از جمله روش‌های ایمنی در متن ماده ۱۳ قانون تجارت الکترونیک، می‌تواند داده الکترونیکی امضا[۸] بر معیار ماده ۶۵۲ قانون آئین دادرسی کیفری مصوب ۱۳۹۲ باشد، با این وصف، بین امضای الکترونیکی مطمئن و ساده تفاوتی وجود ندارد؛ لیکن اثر حقوقی متفاوتی از لحاظ جعل، انکار و تردید بر اسنادی که با امضای الکترونیکی مطمئن و ساده انتقال می‌یابد، بار می‌شود، بطوریکه امضای الکترونیکی مطمئن داده پیام، آن‌ها را درحکم اسناد رسمی قرار می‌دهد (وصالی ناصح، ص ۶۸). بموجب ماده ۱۰ قانون تجارت الکترونیک شرایط امضای الکترونیکی مطمئن عبارت‌اند از:

الف- نسبت به امضاکننده منحصر به فرد باشد؛

ب- هویت امضاکننده «داده پیام» را معلوم نماید؛

ج - بوسیله امضاکننده یا تحت اراده انحصاری وی صادرشده باشد؛

د- بنحوی به یک «داده پیام» متصل شود که هر تغییری در آن «داده پیام» قابل تشخیص و کشف باشد».

۷- در رمزنگاری، اطلاعات بوسیله تغییر شکل دادن داده پیام، مورد حفاظت قرار می‌گیرند و برای فردی که به این اطلاعات دسترسی ندارد، ناخوانا باقی می‌ماند. به این شیوه، داده‌ها از خطر تغییر و تحریف محفوظ باقی می‌مانند و می‌توانند بگونه ای مطمئن مورد استناد قرار گیرند (وصالی ناصح، ص ۶۰).

۸- منظور از امضای الکترونیکی، داده ای الکترونیکی است که به سایر داده‌های الکترونیکی متصل یا مرتبط بوده و روشی برای احراز اصالت بشمار می‌رود؛ (زرکلام،۱۳۸۲، ص ۳۹).

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

با اینحال، گاه امضا یا مهر، علاوه بر ایفای نقش اثبات انتساب سند به صادرکننده، نقشی ماهوی در به وجود آمدن آن ایفاء می‌نمایند. بطوریکه حتی اگر کاملاً محرز باشد، سند توسط شخصی تنظیم و تسلیم طرف مقابل شده، لیکن به سبب آنکه فاقد امضا یا مهر است، اعتبار و اثر خاص قانونی آن سند را ندارد. اسناد تجاری یا بارنامه اینگونه می‌باشند. امضا یا مهر از شرایط اساسی تنظیم آن‌ها است و بدون امضا، اثبات انتساب آن‌ها به صادرکننده غیر ممکن است. این اسناد، علاو ه بر دلیل اثبات دعوی بودن، صدورشان عمل حقوقی محسوب می‌شود (صادقی، نشاط، ۱۳۹۳، ص ۸۶).

یکی دیگر از راهکارهای ایمن در ماده ۴۹ قانون جرائم رایانه ای مورد اشاره قرار گرفته است. بموجب این حکم قانونی، «بمنظور حفظ صحت و تمامیت، اعتبار انکارناپذیری ادله الکترونیک جمع آوری شده، لازم است مطابق آئیننامه مربوط از آن‌ها نگهداری و مراقبت به عمل آید» بعلاوه به موجب ماده ۴۰ این قانون «در توقیف داده‌ها با رعایت تناسب، نوع، اهمیت و نقش آن‌ها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، کپی برداری یا تصویر برداری از تمام یا بخشی از داده‌ها، غیرقابل دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود» و سرانجام در مواد ۶۵۲ و ۶۵۶ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ (اصلاحی ۱۳۹۴) قوه قضائیه مکلف به استفاده از تدابیر امنیتی مطمئن شده، بنحویکه «بمنظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری اطلاعات مبادله شده میان شهروندان و محاکم قضائی، قوه قضائیه موظف است تدابیر امنیتی مطمئن برای امضای الکترونیکی، احراز هویت و احراز اصالت را فراهم آورد».

بنابراین، وقتی سندی معتبر است که بتواند به صادرکننده‌اش منتسب شود. اثبات این امر محدود به روش خاصی مانند امضا یا غیر آن نیست.[۹] ادله اثبات انتساب می‌تواند هر دلیلی از ادله پنجگانه اثبات دعوی مانند اقرار خود شخص باشد و یا غیر از آن‌ها مانند امضا، مهر، دستخط و هرگونه قرینه‌ای در درون خود سند را در برگیرد. ضمن آنکه هرگاه مدعی نسبت به سند الکترونیکی انکار، تردید یا ادعای جعل نماید، برای اثبات انتساب به صادر کننده، از نظر کارشناسی نیز می‌توان کمک گرفت (صادقی، نشاط، ۱۳۹۴، ص ۸۶). بعنوان مثال، می‌توان تصویر حاصله از چتروم را در جهت تصدیق مکالمه الکترونیکی به صادرکننده‌اش، مورد استفاده قرار داد تا نشان دهد که هیچگونه تغییری در آن ایجاد نشده است (شهبازی نیا، عبداللهی، ۱۳۸۸، ص ۷۸).

❐ ۴. رسیدگی به اصالت اسناد الکترونیکی

دادگاه زمانی رسیدگی به اصالت سند را آغاز می‌نماید که اولاً نسبت به اصالت آن تعرض شده باشد. ثانیاً با توجه به ماده ۱۵ قانون تجارت الکترونیک تعرض نسبت به سند با عنوان متناسب قانونی

۹- قانون متحدالشکل تراکنش‌های اطلاعات رایانه ای آمریکا، به جای تأکید بر امضا، بر یک سامانه مطمئن برای ثبت تراکنش‌ها تأکید کرده است. در معاهده ۲۰۰۵ نیز اثری از لزوم امضا برای اعتبار ارتباط به چشم نمی‌خورد (نشاط، ۱۳۹۴، ص ۸۵).

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

(جعل، انکار و تردید) طرح شود. ثالثاً در زمان مقرر قانونی، بعمل آمده باشد.[۱۰] با رعایت این موارد، دادگاه قراری بعنوان رسیدگی به اصالت سند صادر می‌نماید.

ماده ۲۱ قانون تجارت الکترونیک به نوعی درصدد تفکیک اصل داده پیام از رونوشت (پرینت) آن است و مقرر می‌دارد: «هر «داده پیام» یک «داده پیام» مجزا و مستقل محسوب می‌گردد، مگر آنکه معلوم باشد آن «داده پیام» نسخه مجددی از «داده پیام» اولیه است». بنابراین مقصود از اصالت[۱۱] اسناد الکترونیکی، اصل در برابر کپی است. در واقع احراز اصل سند امر دشواری است که نیازمند دانش متخصصین و امکانات فنی بالایی است. به همین دلیل قانونگذار شرایطی در مواد مختلف از جمله ماده ۸ قانون تجارت الکترونیک پیشبینی کرده تا کپی آن‌ها را همراستا با اصل آن قرار دهد؛ بنابراین آنچه که روی حافظه جانبی اعم از دیسکت سخت، سی دی و سایر وسایل ذخیره، ارسال و یا چاپ و نمایش داده می‌شود، از نظر شکلی، همگی تصویر محسوب می‌شوند (مؤذن زادگان، یوشی، سلیمان دهکردی، ۱۳۹۴، ص ۷۴). از آنجا که در محیط الکترونیکی می‌توان به هر تعداد از یک سند، نسخه‌های متعدد از نسخه اولیه را تکثیر[۱۲] کرد، لذا تشخیص اصل داده الکترونیکی از رونوشت آن از دو نظر واجد اهمیت است.

یکی از حیث ادله اثبات دعوی است. در رسیدگی به دعوی، طرفی که علیه او سندی عادی ابراز شده؛ حق دارد اصل آن را مطالبه کند، وگرنه آن سند از عداد دلایل طرف مقابل خارج می‌شود (ماده ۹۶ قانون آئین دادرسی مدنی). این ماده در فضای الکترونیکی، به این مفهوم است که رونوشت سند تا زمانی اعتبار دارد که طرف دعوا نسبت به آن ایراد نکند، اما در صورت ایراد طرف مقابل، باید اصل سند به دادگاه ارائه شود تا تمامیت آن مورد بررسی قرار گیرد. همچنین چنانچه سند الکترونیکی بر طبق مواد ۱۴ و ۱۵ قانون تجارت الکترونیک رسمی باشد، نسبت به آن ادعای جعل شود، طبق ماده ۲۲۰ ق آ.د. م ادعای جعلیت و دلایل آن به طرف مقابل ابلاغ می‌شود و چنانچه به استفاده از سند باقی باشد، موظف است ظرف ۱۰ روز از تاریخ ابلاغ، اصل سند مورد ادعای جعل را به دفتر دادگاه تسلیم نماید. چنانچه صاحب سند در موعد مقرر از تسلیم اصل سند به دادگاه خودداری کند؛ سند از عداد دلایل او خارج خواهد شد. بنابراین نگهداری و حفظ اطلاعات مطابق شرایط ماده ۸ قانون تجارت الکترونیک درحکم اصل است و در دادگاه پذیرفته می‌شود.

دیگری از حیث اسناد تجاری است که علاوه بر عنصر «تک بودن» (شهبازی نیا، عبداللهی ۱۳۸۸، ص ۱۳۵) صدور این اسناد عمل حقوقی خاص محسوب می‌شود. مدیون سند تجاری که اصل آن مفقود شده یا متصدی حملی که اصل بارنامه[۱۳] دریایی صادره توسط او به وی ارائه نمی‌شود، در برابر کپی اسناد که ممکن است متعدد و در اختیار چندین نفر باشند، پول یا کالا تحویل نمی‌دهند؛ زیرا

---

۱۰ - طبق مفاد مواد ۲۱۷ و ۲۱۹ ق.آ.د.م. تعرض به اسناد حتی الامکان باید تا اولین جلسه دادرسی بعمل آید.

11- Originality

۱۲- رونوشت (**Duplicate**)، به معنای نسخه متناظری است که به طریق ماشینی، عکاسی، شیمیایی، الکترونیک یا هر روش یا تکنیک معادل دیگری بتوان به درستی اصل را تولید مجدد نمود.

۱۳- بارنامه، سند مالکیت کالا است.

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

مادامی که این اسناد در دست طلبکار باشند، مدیون نمی‌تواند ادعای برائت ذمه کند. به لحاظ پر خطر بودن اعتماد به کپی برابر اصل، عملاً تا کنون اینگونه اسناد به صورت الکترونیک رواج نیافته‌اند. البته برخی بی‌نهایت نسخه اصل صادر کردن را از مزایای این اسناد می‌شمارند. به هر حال، علیرغم اهمیت این مطلب، قانونگذار به آن، نپرداخته و ساکت است (نشاط ۱۳۹۳، ص ۸۳).

نکته مهم این است که می‌توان اصل سند، یعنی تمامیت را به شیوه‌های دیگری نیز تأمین کرد؛ زیرا در قلمرو حقوق، شکل و قالب مد نظر نیست، بلکه کارکرد مورد نظر است. با توجه به این کارکرد، در صورتی که تمامیت سند از طریق دیگری - غیر از ارائه اصل سند- احراز شود، آن سند در حکم اصل خواهد بود. برای نمونه ماده ۷۴ قانون ثبت مقرر می‌دارد: «مواردیکه مطابقت آن با ثبت دفتر تصدیق شده است، به منزله اصل سند خواهد بود ...». بنابراین، ابرازکننده رونوشت سند رسمی الکترونیکی که مطابقت آن با مندرجات اصل سند از مرجعی رسمی تأیید شده باشد، ملزم به ارائه اصل سند نیست (شهبازی نیا، عداللهی، ۱۳۸۸، ص ۱۲۸). همچنین تاجری که 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 فقدان نسخه‌های مکرر یکسان از آن نزد سایرین، وجود ندارد.

❐ ۵. شرایط احراز اصالت اسناد الکترونیکی

هدف از ارائه اصل سند، اثبات تمامیت سند و عدم تغییر و انکارناپذیری آن است. در اسناد الکترونیکی، تحقق اصالت به مفهوم واقعی کلمه ممکن نیست، لیکن هرگاه قانون لازم بداند که اطلاعات به صورت اصل ارائه یا نگهداری شود، این امر یا نگهداری و ارائه اطلاعات به صورت داده پیام در صورت وجود شرایط ماده ۸ ق.ت.آ امکان پذیر می‌باشد:[۱۴]

«الف) اطلاعات مورد نظر قابل دسترسی بوده و امکان استفاده درصورت رجوع بعدی فراهم باشد؛

ب) داده پیام به همان قالبی که تولید، ارسال و یا دریافت شده و یا به قالبی که دقیقاً نمایشگر اطلاعاتی باشد که تولید، ارسال و یا دریافت شده نگهداری شود؛

ج) اطلاعاتی که مشخص کننده مبدأ، مقصد، زمان ارسال و دریافت داده پیام می‌باشند نیز در صورت وجود نگهداری شوند؛

د) شرایط دیگری که هر نهاد، سازمان، دستگاه دولتی و یا وزارتخانه درخصوص نگهداری داده پیام مرتبط به حوزه مسوولیت خود مقرر نموده فراهم شده باشد».

۱۴- در نظام‌های حقوقی دیگر نیز اصالت داده پیام منوط به شرایطی است. درحقوق آمریکا اصالت سوابق الکترونیک نیز منوط به وجود شرایط ذیل دانسته شده است: الف- اطمینان بخش و استاندارد بودن تجهیزات رایانه ای. 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 (نشاط،۱۳۹۴، ص ۸۵).

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

۵-۱. قابلیت دسترسی، استفاده مجدد و قابلیت کشف تغییرات

هر دو قید «قابلیت دسترسی» و «استفاده مجدد» به این معنا است که اطلاعات مورد نظر برای انسان‌ها و نیز سامانه‌های رایانه ای غیر قابل استفاده نباشد.[۱۵] این شرط که داده پیام باید در مراجعات بعدی قابل استفاده باشد به معنای لزوم «دوام» یا «غیرقابل تغییربودن سند» نیست (شهبازی نیا، عبداللهی، ۱۳۸۸، ص ۱۳۹). گاهی اسناد به صورت فشرده، بازگردان شده از کدهای اولیه، به صورتی ظاهراً متفاوت با حالت اول ذخیره می‌شوند، ولی همینکه امکان بازیابی اطّلاعات به شکل اولیه وجود داشته باشد، قابل دسترس محسوب می‌شوند (صادقی، نشاط، ۱۳۹۳، ص ۹۰). در نتیجه این شرط، این امکان را فراهم می‌آورد که برای دفعات مکرر به اصل مراجعه و درصورت نیاز، به مراجع دولتی و قضایی ارائه شود.

در انتقال داده پیام، اشخاص و تجهیزاتی دخالت دارند که معمولاً همه آن‌ها تحت مدیریت و نظارت مستقیم صادرکنندگان سند نیستند. قابلیت کشف تغییرات عمدی (مانند جعل) یا ناخواسته و بر اثر اشتباه در داده پیام بدون تمهیدات خاص قابل حصول نیست و امکان تغییرات در مندرجات آن‌ها به دفعات وجود دارد. بدین ترتیب لازم است، به منظور قابلیت دسترسی به اصل اطلاعات و استفاده مجدد پس از تولید و طی زمان ارسال تا وصول و ذخیره، با اعمال روش‌های فنّی اطمینان بخش، به نحو قابل قبولی ایمنی آن‌ها تأمین شود. یکی از روش‌های مطمئن در تأمین شرط عدم تغییر سند الکترونیک، امضای دیجیتال است. تغییر سند الکترونیکی، اثر فیزیکی باقی نمی‌گذارد، تنها می‌توان آنرا با استفاده از روش‌های فنّی اثبات کرد. بعنوان مثال، اگر سندی که دارای امضای دیجیتال[۱۶] است، بعد از امضا، مورد جعل و تغییر قرار گیرد، این تغییر به راحتی قابل تشخیص است؛ حتّی می‌توان از دانش فنّی اندکی برای این منظور سود برد؛ در صورتیکه از منوی File گزینه Properties سپس گزینه Statistic را انتخاب کنیم، رایانه تاریخ ایجاد فایل و نیز تاریخ آخرین تغییر سند و آخرین تاریخ دسترسی به آن را نشان می‌دهد که اگر تاریخ تغییر، بعد از تاریخ تنظیم سند باشد، این امر مثبت جعلی بودن سند و تغییر داده پیام است (شهبازی نیا، عبداللهی، ۱۳۸۸، ص ۱۳۹).

۵-۲. حفظ تمامیت اطلاعات تولید، ارسال یا دریافت شده

حفظ تمامیت اطلاعات برای مصون ماندن «شکل نهایی»[۱۷] سند از جعل و تحریف است (شهبازی‌نیا، عبداللهی، ۱۳۸۸، ص ۱۳۴). همچنین برای کاهش تغییرات غیر مجاز و یا ناخواسته هنگام ارسال پیام بعد از ایجاد و قبل از دریافت، می‌توان از طریق رمزنگاری‌های متفاوت از جمله رمز نگاری کلید عمومی، رمزنگاری سایمتریک، استفاده از سیستم هش فانکشن (آهنی، ۱۳۸۲، ص ۷۸) و رمزنگاری بیومتریک (مؤذن زادگان،یوشی، دهکردی، ص ۷۱، ۱۳۹۴) از ایجاد تغییر اسناد جلوگیری کرد.

---

۱۵ - ادله الکترونیکی غیرقابل استفاده، ادله پاک شده، آسیب دیده، پنهان و یا رمزگذاری شده است (فرهانی، ۱۳۸۶، ص ۱۰۴).

۱۶ - امضای دیجیتال یک فناوری رمز نگاری است که از یک جفت کلید موسوم به کلید اختصاصی و کلید عمومی تشکیل می‌شود که از این امر می‌توان برای اثبات جعلی بودن پیام استفاده کرد. (زرکلام،۱۳۸۲، ص ۳۹).

۱۷ - منظور از «شکل نهایی» سند، آن شکل از سند است که از ابتدا به صورت الکترونیکی به وجود می‌آید.

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

با توجه به موارد فوق، معیار تمامیت سند، آن است که اطلاعات، کامل و بدون تغییر باقی بماند؛ لذا این که حکم اسنادی که قالب آن‌ها در عملیات نقل و انتقال تغییر می‌کند یا از قالب کاغذی به قالب الکترونیکی تبدیل شده‌اند، چیست؟ باید گفت همین قاعده حکمفرما است؛ یعنی در صورتیکه مندرجات یک سند کاغذی به قالب الکترونیکی دیگری تبدیل شود، در صورتی که احراز شود سند الکترونیکی حاوی همان مندرجات است، چنین سندی، اصل محسوب می‌شود.

به هر ترتیب، در صورت تغییر قالب سند، اثبات تمامیت اطلاعات موجود در سند با ارائه کننده اصل سند است که این امر بار اثبات زیادی را به عهده وی قرار می‌دهد. برای تشخیص این امر، دادرس باید با ارجاع امر به کارشناس، تمامیت اطلاعات را ارزیابی کند (شهبازی نیا، عبداللهی ۱۳۸۸، ص ۱۳۴).

۵-۳. نگهداری اطلاعات شناسایی داده پیام

اگرچه قانونگذار در بند «ج» ماده ۸ قانون تجارت الکترونیک بطور کلی به نگهداری اطلاعات نظر داشته است، معهذا این سؤال مطرح است که بطور خاص نگهداری کدام اطلاعات ضروری است و سبب انتساب سند به صادرکننده می‌شود؟ بعلاوه اشخاص تا چه مدتی مکلف به نگهداری اصول الکترونیکی اسناد می‌باشند؟

بنظر می‌رسد منظور، اطلاعات موجود در فصل سوم قانون تجارت الکترونیک (تصدیق دریافت) و فصل چهارم (اطلاعات زمان و مکان ارسال و دریافت «داده پیام») می‌باشد. در ماده ۲۲ این قانون مقرر شده: «هرگاه قبل یا به هنگام ارسال داده پیام، اصل ساز از مخاطب بخواهد یا توافق کنند که دریافت داده پیام تصدیق شود ...». این امر مبیّن نگهداری اطلاعات تصدیق شده و نشانگر اطلاعات تولید، ارسال، دریافت یا ذخیره شده داده پیام می‌باشد، همچنین در خصوص اطلاعات مربوط به سیستم اطلاعاتی موجود، ماده ۲۶ این مقرر داشته: «ارسال داده پیام زمانی تحقق می‌یابد که به یک سیستم اطلاعاتی ... وارد شود». گاهی سامانه‌های الکترونیکی به صورت خودکار، به هنگام انتقال داده پیام، اطلاعاتی را به آغاز یا پایان داده پیام می افزایندکه به آن فراداده می گویند.[۱۸] لازم به ذکر است که در غالب سامانه‌های الکترونیکی به صورت خودکار، به هنگام انتقال داده پیام، برخی اطلاعات تکمیلی مثلاً پروتکل ارتباطات نیز ارسال و بوسیله مخاطب دریافت می‌شود. نگهداری این نوع اطلاعات که صرفاً به دلیل انجام عملیات ارسال توسط سامانه‌های رایانه ای به وجود آمده، ضروری نیست؛ زیرا این اطلاعات به منزله یک پاکتنامه برای اسناد کاغذی هستند که از طریق پست ارسال می‌شوند (شهبازی نیا، عبداللهی ،۱۳۸۸، ص ۱۳۲). در این مورد توصیه شده تنها داده‌های رایانه ای که واقعاً ارزش استناد در دعاوی را دارند از سوی طرفین دعوا نگهداری و ارائه شوند؛ زیرا به راحتی

۱۸- یک سند الکترونیکی فراداده معمولاً حاوی اطلاعاتی درباره سند است. فراداده می‌تواند شامل تاریخ، زمان ایجاد یا تغییر یک فایل واژه پرداز یا شامل نویسنده، تاریخ و زمان ارسال یک پست الکترونیکی باشد (مولودی، ۱۳۹۴، ص ۱۵۷). اطلاعات مذکور می‌تواند برای اثبات زمان و مکان انعقاد قرارداد یا ایقاعات مورد استفاده طرفین دعوا و دادگاه‌ها قرار گیرد.

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

نمی‌توان صحت عملکرد یک سیستم اطلاعاتی رایانه ای را اثبات نمود (مؤذن زادگان، ۱۳۸۸، ص ۸۷).

در بند «ج» ماده ۸ قانون تجارت الکترونیک قید «در صورت وجود» نشان می‌دهد نگهداری این اطلاعات زمانی ضروری است که موجود باشند و در صورت فقدان چنین اطلاعاتی، نیازی به نگهداری و ارائه آن‌ها نیست و اصالت سند ارائه شده تابع قواعد عمومی است. همچنین در ماده ۱۶ در مورد ثبت و نگهداری داده پیام که با رعایت شرایط یک سیستم اطلاعاتی مطمئن باشد، مقرر شده «هر داده پیامی که توسط شخص ثالث مطابق با شرایط ماده ۱۱ این قانون ثبت و نگهداری می‌شود، مقرون به صحت است». بنابراین نه تنها طرفین دعوی، بلکه حفظ ایمنی داده پیام توسط اشخاص ثالث نیز صحیح است.

در مورد مدت نگهداری داده‌ها، قانون تجارت الکترونیکی ساکت است و تنها برای قوه قضاییه مقرر نموده که بعد از مدت ۳۰ سال از بایگانی قطعی، نیازی به نگهداری اسناد و اوراق قضایی نیست. این خلاء، مشکلات جدی را برای اشخاص که مجبورند اسناد الکترونیکی را برای سالیان سال نگهداری کنند، ایجاد می‌کنند؛ امری که باعث می‌شود هزینه و انرژی زیادی مصرف شود (زرکلام، ۱۳۹۱، ص ۱۴۷).

۵-۴. رعایت شرایط خاص دستگاه‌های اجرایی

غالباً رعایت شرایط خاص نگهداری اطلاعات، برای بایگانی اسناد به صورت داده پیام، در حوزه‌های مرتبط با نظم عمومی و امور اداری، مانند امور ثبت اسناد و املاک، امور مالیاتی یا کنتر ل های گمرکی مورد استفاده قرار می‌گیرند. قانونگذار رعایت این شرط برای اصالت سند را تنها از وظایف اشخاص حقوقی دولتی می‌داند که نگهداری داده پیام در حوزه مسوولیتش قرار دارد؛ به این شرط که تمهیدات آن فراهم شده باشد. لیکن چنانچه شرایط خاص دستگاه‌های مذکور در ماده رعایت نشده باشد، عدم رعایت شرایط در مقابل اشخاص ثالث قابل استناد نیست.

نمونه این چنین شرایط ماده ۱۱۳ قانون برنامه چهارم توسعه اقتصادی است که مقرر داشته «به قوه قضاییه اجازه داده می‌شود: الف) ... اسناد و اوراق پرونده‌های قضایی که نگهداری سوابق آن‌ها ضروری می‌باشد را با استفاده از فناوری‌های اطلاعاتی روز به اسناد الکترونیکی تبدیل و سپس نسبت به امحای آن‌ها اقدام نماید، مشروط بر آنکه حداقل سی سال از مدت بایگانی قطعی آن‌ها گذشته باشد. اطلاعات و اسناد تبدیلی در کلیه مراجع قضایی سندیت داشته و قابل استناد خواهد بود...» بنابراین، قوه قضاییه برای نگهداری اسناد الکترونیکی، باید شرایط خاص مقرر در این ماده، از جمله گذشت مدت سی سال از بایگانی قطعی پرونده و نیز شرایط آئیننامه مذکور را رعایت کند (شهبازی‌نیا، عبداللهی، ۱۳۸۸، ص ۱۳۳).

❐ ۶. شیوه‌های تعرض به اصالت اسناد الکترونیکی

مهم‌ترین تفاوت اسناد عادی و رسمی، قواعد حاکم بر تعرض پذیری است. بموجب مواد ۱۴ و ۱۵ قانون تجارت الکترونیک، داده پیام مطمئن (در حکم اسناد معتبر و قابل استناد) قابل انکار و تردید

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

نیستند و تنها می‌توان نسبت به آن‌ها ادعای جعلیت نمود. ماده ۱۲ قانون مذکور اسناد و ادله اثبات دعوی به صورت داده پیام را مورد پذیرش دانسته و تاکید کرده صرفاً به دلیل شکل و قالب، محکوم به رد نیستند. مفهوم ماده این است اسناد الکترونیکی که دارای شرایط مطمئن نیستند، از ارزش اثباتی اسناد عادی برخوردارند؛ تا آنجا که حتی اگر فناوری مورد استفاده در آن‌ها غیر ایمن باشد و تا زمانی که اصالت آن اسناد تکذیب نشده یا طرف دعوا به اصالت آن‌ها اعتراض (اعم از جعل، انکار و تردید) نکرده، حمل بر صحت سند است و دادرس نمی‌تواند بعلّت ایمن نبودن فناوری مورداستفاده و یا نداشتن امضا آنرا معتبر نداند (مؤذن زادگان، یوشی، سلیمان دهکردی، ۱۳۹۴، ص ۷۹).

در فرایند دادرسی پس از ارائه سند و استناد به آن؛ به دو صورت می‌توان سند را مورد تعرض قرار داد:

۱- ماهوی: موضوع محتویات سند، ماهیتاً مورد اختلاف باشد که در اینصورت، شیوه‌های دفاع ماهوی در برابر اسناد بسیار متنوع است؛ ازجمله مهم‌ترین آن‌ها ادعای بطلان سند، ادعای فسخ معامله، انجام تعهد و ... می‌باشد.

۲- شکلی: در این روش، شکل ظاهری سند و اصالت آن مورد خدشه و تعرض واقع می‌شود. در فرایند دادرسی به لحاظ شکلی، اسناد از جهت رسمی یا عادی بودن به سه شکل جعل، انکار و تردید مورد تعرض قرار می‌گیرند. قبل از توضیح، تفاوت آن‌ها در این است که اثبات انکار و تردید از سوی اظهار کننده لازم نیست و وی را باتکلیف مواجه نمی‌سازد؛ اما جعل، ادعاست و باید با دلیل اثبات شود. مثلاً اثبات اینکه سند از نشانی پست الکترونیکی صادرکننده، ارسال نشده است.

۶-۱) اظهار انکار و تردید: مطابق ماده ۲۱۶ ق.آ.د.م «کسی که علیه او سند غیر رسمی ابراز شود، می‌تواند خط یا مهر یا امضا یا اثر انگشت منتسب به خود را انکار نماید و احکام منکر بر او مترتب می‌گردد و اگر سند ابرازی منتسب به شخص او نباشد، می‌تواند تردید کند» که این امر در دلایل الکترونیکی، به صورت رد انتساب امضای الکترونیکی غیر مطمئن ذیل سند، تحقق می‌یابد.

ماده ۱۲۹۱ قانون مدنی مقرر می‌دارد «اسناد عادی در دو مورد اعتبار اسناد رسمی را داشته و درباره طرفین و وراثت و قائم مقام آنان معتبراست». بنابراین چنانچه شرایط این ماده در محکمه ثابت شود، سند عادی اعتبار سند رسمی خواهد داشت. به علاوه اسناد عادی الکترونیکی نیز در صورتیکه از شرایط مقرر شده مواد ۱۸ و ۱۹ قانون تجارت الکترونیک برخوردار باشند (در صورت تحقق آن‌ها، داده پیام به اصل ساز منسوب می‌شود که در واقع اماره انتساب سند است) غیرقابل انکار و تردید می‌باشند (شهبازی نیا، عبداللهی، ۱۳۸۸، ص ۱۳۷).

به دلالت ماده ۱۸ قانون تجارت الکترونیک «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.

ب) اگر بوسیله سیستم اطلاعاتی برنامه ریزی شده یا تصدی خودکار از جانب اصل ساز ارسال شود».

همچنین مطابق ماده ۱۹ این قانون، در صورت تحقق شرایط ذیل، مخاطب حق دارد آنرا ارسال

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

شده محسوب کرده و مطابق چنین فرضی (ارسال شده) عمل نماید:

«الف) قبلاً بوسیله اصل ساز، روشی معرفی و یا 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 رابطه‌اش با اصل ساز یا 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.

۶-۲) ادعای جعل:

وفق ماده ۵۲۳ قانون مجازات اسلامی «جعل، عبارت است از ساختن نوشته یا سند یا ساختن مهر یا امضای اشخاص رسمی یا غیر رسمی، خراشیدن یا تراشیدن یا قلم بردن یا الحاق یا محو یا اثبات یا سیاه کردن یا تقدیم یا تأخیر تاریخ سند نسبت به تاریخ حقیقی یا الصاق نوشتهای به نوشته دیگر یا به کار بردن مهر دیگری بدون اجازه صاحب آن و نظایر این‌ها به قصد تقلب».

مطابق ماده ۲۲۱ قانون آئین دادرسی مدنی، دادگاه مکلف است ضمن صدور حکم راجع به ماهیت دعوی، نسبت به سندی که ادعای جعل شده تعیین و تکلیف نماید. در این موارد چنانچه آنرا اصل تشخیص دهد، معمولاً مبادرت به صدور قرار صحت و اصالت سند کرده و طبق آن حکم مقتضی در ماهیت موضوع صادر می‌نماید و اگر مصادیق جعل کامپیوتری در ماده ۶۸ قانون تجارت الکترونیک[۱۹] را احراز کند و آنرا مجعول بداند، تکلیف آنکه تمام سند از بین برده شود یا قسمت مجعول سند، ابطال گردد یا اینکه کلماتی محو و تغییر داده شود، را تعیین خواهد کرد.

در محیط الکترونیکی، مصادیق جعل فیزیکی همچون خدشه، تراشیدگی و قلم خوردگی بی معنا است و مدعی جعل، باید جعل را متناسب با فضای الکترونیک اثبات کند. مثلاً اثبات کند که کلید خصوصی یا گذرو اژه او افشا شده یا کارت هوشمندش که آنرا برای امور بانکی مورد استفاده قرار می‌دهد، به سرقت رفته است (شهبازی نیا، عبداللهی، ۱۳۸۸، ص ۱۳۹).

برای جلوگیری از جرم جعل می‌توان به مکانیسم‌های ایمنی ازجمله به «رمزنگاری، نقش‌نگاری، انگشت نگاری دیجیتالی و دینامیک‌های کلید فشاری» اشاره نمود. رمزنگاری به منظور از بین بردن خطر رهگیری داده‌ها، استراق سمع، تغییر داده‌ها، جعل داده‌ها و تکذیب منشأ و خاستگاه داده‌ها مورداستفاده قرار می‌گیرد. نقش‌نگاری بمنظور افزودن لایه دیگری از حفاظت در برابر رهگیری، جعل داده‌ها، و مهم‌تر از همه سرقت اطلاعات استفاده می‌شود. انگشت نگاری دیجیتالی جهت جلوگیری از تغییر و جعل داده‌ها مورد استفاده قرار می‌گیرد و در نهایت دینامیک‌های کلید فشاری نیز بمنظور

۱۹- هرکس در بستر مبادلات الکترونیکی، از طریق ورود، تغییر، محو و توقف «داده پیام» و مداخله در پردازش «داده پیام» و سیستم‌های رایانه‌ای، و یا استفاده از وسایل‌کاربردی سیستم‌های رمزنگاری تولید امضاء - مثل کلید اختصاصی - بدون مجوز امضاءکننده و یا تولید امضای فاقد سابقه ثبت در فهرست دفاتر اسناد الکترونیکی و یا عدم‌انطباق آن وسایل با نام دارنده در فهرست مزبور و اخذ گواهی مجعول و نظایر آن اقدام به‌جعل «داده پیام» های دارای ارزش مالی و اثباتی نماید تا با ارائه آن به مراجع اداری، قضایی، مالی و غیره به عنوان «داده پیام» های معتبر استفاده نماید جاعل محسوب و به مجازات حبس از یک تا سه سال و پرداخت جزای نقدی به میزان پنجاه میلیون ریال محکوم می‌شود.

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

جلوگیری از دسترسی غیرمجاز به داده‌ها و سرقت اطلاعات به کار می‌رود (مؤذن زادگان، یوشی، سلیمان دهکردی، ۱۳۹۴، ص ۸۵). بنابراین استفاده از تدابیر امنیتی در انتقال داده پیام، علاوه بر اینکه آن‌ها را از تغییرات عمدی یا ناخواسته دور می‌کند، نوعی قرینه برای انتساب سند به صادر کننده آن در محاکم قضایی است.

❐ نتیجه

آنچه تلاش شد در این نوشتار تبیین گردد، بررسی جایگاه داده پیام در ادله اثبات دعوی در شکل و قالب اسناد الکترونیکی و احراز اصالت اسناد و ادله الکترونیکی در نظام حقوقی ایران بمنظور ارائه آن نزد مراجع قضاوتی و اداری کشور و تبیین مفهوم اصالت اسناد در برابر کپی آنها-که قانون وجود آن را جهت تشخیص تمامیت سند و عدم جعل و تغییر آن لازم می‌داند- می‌باشد. مبرهن است که برای حفظ اصالت و نگهداری سند باید تمهیدات ایمنی با استفاده از شیوه‌های فنّی مانند امضای دیجیتال، تمامیت سند را در دلایل الکترونیکی تأمین کرد. از طرفی اظهار انکار و تردید و ادعای جعل به عنوان شیوه‌های تکذیب اصالت سند در دلایل الکترونیکی، تغییر پیدا کرده و مدعی اصالت سند برای اثبات اطمینان دلیل و صحت آن، باید از شیوه فنّی متناسب با این ادله استفاده کند. به دلیل گسترش این داده‌ها در فضای سایبر، دشواری انتساب داده پیام و احراز اصالت و صحت این داده‌ها در محاکم، سبب شده تا حقوقدانان در پذیرش ادله الکترونیکی بعنوان دلایلی معتبر و قابل استناد تردید نشان دهند؛ لیکن قانونگذار ایران ارزش اثباتی این دلایل را در قوانین مختلف ازجمله قانون جرائم رایانه ای و همچنین قانون تجارت الکترونیکی پذیرفت است. با اینحال در زمینه جمع آوری و استناد پذیری ادله الکترونیکی «داده پیام» و اسناد الکترونیکی، نظام حقوقی ایران با چالش‌هایی روبه رو است که البته در راستای رفع این چالش‌ها ارتقای سطح دانش فنّی در شیوه‌های جمع آوری، مستند سازی و ارائه ادله الکترونیکی به مراجع قضایی، از ضروریات است.

❐ فهرست منابع

۱- آشوری، محمد (۱۳۸۸)، آئین دادرسی کیفری، جلد دوم، چاپ هشتم، تهران، انتشارات سمت.

۲- آهنی، بتول (۱۳۸۲)«برقراری امنیت در قراردادهای الکترونیکی» ندای صداقت، شماره ۳۰ سال هشتم. تابستان.

۳- استنلی، پائول (۱۳۹۱) حفظ حقوق اسرار، مترجم: محمدحسین وکیلی مقدم، چاپ اول، تهران، انتشارات همگان.

۴- جلالی فرهانی امیرحسین (۱۳۸۶) «استنادپذیری ادلۀ الکترونیکی درامور کیفری» فصلنامه فقه و حقوق، شماره ۱۵، سال چهارم، زمستان.

۵- دوبلفون، زویه لینان، (۱۳۸۸) حقوق تجارت الکترونیک، ترجمه ستار زرکلام، موسسه مطالعات چاپ اول، تهران پژوهش‌های حقوقی شهر دانش.

۶- زرکلام، ستار (۱۳۸۲) «امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوا» مدرسه علوم

Downloaded from malieh.dmk.ir at 21:02 +0330 on Tuesday October 16th 2018

انسانی، شماره ۲۸ دوره ۷، بهار.

۷- زرکلام، ستار (۱۳۹۱) «دادرسی‌های الکترونیکی ضرورت‌ها و الزامات و چالش‌ها» مجله آموزه‌های حقوق کیفری، شماره ۳، بهار.

۸- سوادکوهی فر، سام (۱۳۸۳)، «دادرسی دعاوی مدنی و کیفری و اداری مرتبط با بستر مبادلات الکترونیک» ماهنامه کانون، شماره ۴۶، سال ۸.

۹- شمس، عبد الله (۱۳۸۸) آئین دادرسی مدنی، جلد ۳، چاپ چهاردهم، تهران، انتشارات دراک.

۱۰- شهبازی نیا، مرتضی و عبداللهی، محبوبه (۱۳۸۹) «دلیل الکترونیک در نظام ادله اثبات دعوا» فصلنامه حقوق دانشکده حقوق و علوم سیاسی، شماره ۴، دوره ۴۰، زمستان.

۱۱- شهبازی نیا، مرتضی و عبدالهی محبوبه (۱۳۸۸)، «احراز اصالت در اسناد الکترونیکی» فصلنامه پژوهش‌های حقوق تطبیقی، شماره ۴، دوره ۶۳، آذر.

۱۲- فرهانی، رسول و مولودی، محمد (۱۳۹۴) «بررسی تطبیقی افشای اسناد و اطلاعات الکترونیکی در ادله اثبات دعوا در حقوق انگلیس، آمریکا و ایران»، پژوهش‌های حقوق تطبیقی، شماره ۲، دوره ۱۹، شهریور.

۱۳- مؤذن زادگان، حسنعلی و شایگان، محمد رسول (۱۳۸۸) «استناد پذیری و تحصیل ادله الکترونیکی در حقوق کیفری ایران» فصلنامه دیدگاه‌های حقوقی، شماره ۴۸، بهمن.

۱۴- مؤذن زادگان حسنعلی، یوشی، مهشید و سلیمان دهکردی، الهام (۱۳۹۴)، «حفظ صحت و استنادپذیری ادله الکترونیک با استفاده از

۱۵- بیومتریک و رمزنگاری»، پژوهش حقوق کیفری، شماره دوازدهم، سال چهارم، پاییز.

۱۶- صادقی، نشاط، امیر (۱۳۹۳) «اعتبارسنجی اسناد الکترونیک» فصلنامه پژوهش حقوق خصوصی، شماره هشتم، سال سوم، بهمن.

۱۷- نوری، محمد علی و نخجوانی، رضا (۱۳۹۰)، حقوق تجارت الکترونیک، چاپ دوم، تهران، انتشارات گنج دانش.

۱۸- وصالی ناصح، مرتضی (۱۳۸۴)«امضای الکترونیک و جایگاه آن در ادله اثبات دعوی» ماهنامه کانون، شماره ۵۹، سال چهل و هشتم، بهمن.