احراز اصالت در اسناد الکترونیکی

مرتضی شهبازی‌نیا[1]*، محبوبه عبدالهی[2]

۱- استادیار گروه حقوق دانشگاه تربیت مدرس، تهران، ایران
۲- کارشناس ارشد حقوق خصوصی دانشگاه تربیت مدرس، تهران، ایران

دریافت: ۸۷/۸/۸ پذیرش: ۸۸/۸/۲۳

چکیده

در نظام ادله اثبات دعوا، اصالت سند، نقش مهمی در اعتبار دلیل دارد و سند اصل، معیار مطمئنی برای تشخیص صحت سند و تمامیت آن است. در ادله الکترونیکی، اصل سند به معنای نسخه‌ای که مستقیماً توسط صادرکنندگان سند به وجود آمده‌باشد وجود ندارد. از طرفی، ادله الکترونیکی، ماهیت مادی و ملموس ندارند و به همین دلیل، تحقق مفهوم «اصل» به معنای سنتی آن در این ادله، امکان‌پذیر نیست؛ اما می‌توان با به‌کارگیری روش‌های فنی، کارکردهای یک سند اصل را در ادله الکترونیکی تأمین کرد. همچنین مفهوم جعل و تغییر و نحوه ارزیابی صحت سند در این دلایل، متناسب با هویت غیرمادی آن‌ها تحول یافته‌است . در مقاله حاضر موضوعات فوق بررسی می شوند..

کلید واژه‌ها: اصل سند، قانون تجارت الکترونیکی، دلیل الکترونیکی، ادله اثبات دعوا.

۱- مقدمه

در نظام ادله اثبات دعوا، عنصر اصالت، نقش مهمی در اعتبار دلیل دارد. ماده ۹۶ قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور مدنی، طرفین دعوا را ملزم به ارائه اصل اسناد در جلسه دادرسی می‌کند. اگر اصل سند عادی که مستند دعوا است در جلسه دادرسی ارائه نشود و طرف دعوا در نخستین جلسه دادرسی نسبت به آن اظهار انکار یا تردید کند، سند از عداد

* نویسندهٔ مسؤول مقاله: Email: shahbazinia@modares.ac.ir

دلایل استنادکننده خارج می‌شود.

اهمیت عنصر اصالت از آن رو است که اصل سند، وسیله مطمئنی برای تشخیص صحت سند است؛ زیرا جعل و تغییر سند، مستلزم تغییر مادی نسخه اصل است، اما دلایل الکترونیکی، غیرملموس و غیرمادی هستند و به همین علت، مصادیق جعل و نیز مفهوم اصل سند در این دلایل، متفاوت از مصادیق سنتی آن است.

در این مقاله، ضمن تعریف اصالت و کارکرد آن، نحوه تأمین این عنصر را در دلایل الکترونیکی بیان کرده، شیوه‌های تکذیب صحت اسناد الکترونیکی را بررسی می‌کنیم.

۲- مفهوم اصالت و کارکرد آن

سند اصل، نسخه‌ای از سند است که امضا یا مهر و اثرانگشت صادرکننده روی آن وجود دارد [۱، ص۹۷]. برخی سندی را اصل می‌دانند که اطلاعات برای اولین بار در آن ذخیره شده‌است [۲، ش٦٢] ویا سندی که به صورت دستی تنظیم شده و اسناد دیگر از روی آن نوشته می‌شوند [۳، ص١٩٤]. اگر هنگام تنظیم سند، چند نسخه نوشته و همگی امضا شوند، همگی اصل محسوب می‌شوند و اگر با ماشین تحریر یا رایانه چند نسخه از متن سند تهیه شود، هر کدام که دارای امضا باشد اصل سند محسوب می‌شود و دیگر نسخ، اگر اختلافی با اصل سند نداشته باشند رونوشت محسوب می‌شوند [۱، ص۹۷]. رونوشت، اصطلاحی است که غالباً در برابر اصل به کار می‌رود و سندی است که از روی سند دیگر نوشته می‌شود [٤، ش٢٧٢١].

هدف از ارائه اصل سند، اثبات تمامیت سند و عدم تغییر آن است. رونوشت سند به‌راحتی و بدون آن‌که جعلی بودن آن قابل تشخیص باشد می‌تواند جعل شود. 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 کارشناس قرار گیرد. کارشناس از طریق دقت در دستخط، کاغذ، جوهر و امضای سند می‌تواند تمامیت سند یا جعلی بودن آن را احراز کند و در صورتی که اختلافی بین اصل و رونوشت سند وجود داشته باشد، اصل سند معتبر خواهد بود. در صورتی که دعوا مستند به یک سند عادی باشد و در نخستین جلسه دادرسی، نسبت به آن، اظهار انکار یا تردید شود و اصل سند به دادگاه ارائه نشود، سند از عداد دلایل استنادکننده خارج می‌شود.

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. ماده ٧٤ قانون ثبت مقرر می‌دارد: «مواردی که مطابقت آن با ثبت دفتر تصدیق شده است به منزله اصل سند خواهد بود، مگر در صورت اثبات عدم مطابقت سواد با ثبت دفتر». بنابراین، ابرازکننده رونوشت سند رسمی که مطابقت آن با اصل سند تأیید شده‌است ملزم به ارائه اصل سند نیست [٥، ص١٦٢].

در اسناد الکترونیکی، تحقق مفهوم رایج سند اصل، یعنی سندی که اطلاعات برای اولین بار در آن ذخیره شده‌اند ممکن نیست [٦، ص١٦٦]؛ زیرا هنگامی که اطلاعات برای نخستین بار وارد یک رایانه می‌شوند نخست در حافظه اصلی سامانه ذخیره و سپس به حافظه کوتاه‌مدت یا دیگر واسطهای مغناطیسی منتقل می‌شوند. آن‌گاه اطلاعات از حافظه رایانه به صفحه نمایش منتقل شده، قابل رؤیت می‌شوند. به‌محض آن‌که سامانه کامپیوتری خاموش می‌شود «اصل» از بین می‌رود و آنچه در حافظه باقی می‌ماند در واقع، تصویری است از آنچه برای نخستین بار فقط در حافظه موقت وجود داشته‌است. نه این نسخه و نه نسخه‌های بعدی هیچ‌کدام اصیل نیستند و از نظر شکلی، همگی تصویر محسوب می‌شوند [٧، ص١١١]. اما می‌توان کارکرد اصل سند، یعنی تمامیت را به شیوه دیگری تأمین کرد؛ زیرا در قلمرو حقوق، شکل و قالب مد نظر نیست، بلکه کارکرد مورد نظر است و اگر در موردی بر رعایت شکل و تشریفات خاص تأکید می‌شود به‌منظور حصول به اهدافی است که از این طریق تأمین می‌شود. به همین دلیل در مواردی که قانونگذار، وجود عنصر خاصی را برای اعتبار دلیل لازم می‌داند، تأمین کارکرد آن، کافی است [٢، ص٣٥].

در مواردی که قانونگذار، وجود امضا را لازم می‌داند، رویه قضایی در پذیرش اثرانگشت به جای امضا، تردید نمی‌کند و گاه حتی نوشته بدون امضا، معتبر محسوب می‌شود.[١] پس در مواردی که ارائه اصل سند لازم است، اثبات تمامیت اطلاعات، شرط لزوم ارائه اصل سند را برآورده می‌کند.

به این ترتیب، «اصل سند» در اسناد الکترونیکی، به معنای نسخه‌ای که مستقیم و بدون

---

١. در رأی تمیزی شماره ٢٧٥٢ مورخ ١٣٨١/١١/١٢ دیوان‌عالی کشور آمده است: «در صورت تحقق صدور نامه، مفاد آن نامه علیه نویسنده سندیت خواهد داشت و لو اینکه مهر یا امضایی از وی در آن نباشد؛ زیرا فرستادن نامه بدون امضا، قرینه‌ای عرفی است مبنی بر این‌که فرستنده ملتزم به مدلول آن است، ولی باید محرز شود که خود او آن را فرستاده است» [به نقل از ٨، ص١٤].

واسطه به وجود آمده، نیست، بلکه در این اسناد،«اصل سند»، به معنای نسخه تغییرنیافته داده‌پیام است.

۳- شرایط احراز اصالت اسناد الکترونیکی

همان‌گونه که بیان کردیم در اسناد الکترونیکی، تحقق مفهوم اصالت ممکن نیست، اما سند الکترونیکی می‌تواند با شرایطی، کارکردهای اصل سند را تأمین کند. قانون تجارت الکترونیک این شرایط را تعیین و سندی را که دارای شرایط تعیین شده باشد «سند اصیل» می‌داند. ماده ۸ این قانون مقرر کرده‌است: «هرگاه قانون لازم بداند که اطلاعات به صورت اصل ارائه یا نگهداری شود، این امر با نگهداری و ارائه اطلاعات به صورت داده‌پیام نیز در صورت وجود شرایط زیر امکان‌پذیر می‌باشد:

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

ب) داده‌پیام به همان قالبی که تولید، ارسال ویا دریافت شده ویا به قالبی که دقیقاً نمایشگر اطلاعاتی باشد که تولید، ارسال ویا دریافت‌شده نگهداری شود.

ج) اطلاعاتی که مشخص‌کننده مبدأ، مقصد، زمان ارسال و دریافت داده‌پیام می‌باشند نیز در صورت وجود نگهداری شوند.

د) شرایط دیگری که هر نهاد، سازمان، دستگاه دولتی ویا وزارتخانه درخصوص نگهداری داده‌پیام مرتبط به حوزه مسؤولیت خود مقرر نموده فراهم شده باشد».

این ماده برای نگهداری و ارائه اصل اطلاعات، ٤ شرط مقرر کرده‌است که به بررسی آن‌ها می‌پردازیم.

۱. قابلیت دسترسی و استفاده در صورت رجوع

منظور از «قابلیت دسترسی» مندرج در بند «الف» آن است که اطلاعات مورد نظر برای انسان‌ها و نیز سامانه‌های رایانه‌ای قابل استفاده مجدد باشند. بنابراین در صورتی که نرم‌افزار مورد نیاز برای بازخوانی سند موجود نباشد و کسانی که به سند نیاز دارند نتوانند آن را به دست آورند یا مطالعه کنند، سند قابل دسترسی و قابل استفاده نیست.

این شرط که داده‌پیام باید در مراجعات بعدی قابل استفاده باشد به معنای لزوم «دوام» یا

«غیرقابل تغییربودن سند» نیست؛ یعنی صرف این‌که سند توسط انسان یا سیستم رایانه‌ای قابل خواندن باشد دردسترس محسوب می‌شود، حتی اگر مطالب مندرج در آن دچار تغییر شده باشد [۸، ش۵۰].

۲. حفظ تمامیت اطلاعاتی که تولید، ارسال یا دریافت شده‌اند

بند «ب» ماده مذکور مقرر می‌دارد: داده‌پیام باید در قالبی باشد که دقیقاً نمایشگر اطلاعاتی باشد که تولید، ارسال یا دریافت شده‌اند؛ یعنی اطلاعات نباید دچار تغییر شوند و تمامیت اطلاعات باید حفظ شود.

در صورتی که اطلاعات ارائه یا نگهداری‌شده به همان قالب اولیه باشند، یعنی از زمان تولید، ارسال یا دریافت، قالب آن‌ها تغییری نکرده باشد تشخیص تمامیت اطلاعات، امر دشواری نیست؛ زیرا اگر سند دارای یک امضای الکترونیکی مطمئن باشد، تمامیت سند تضمین می‌شود و افزودن یا تغییر حتی یک حرف از سند قابل تشخیص است [۹، ص۳۸].

اما گاهی اطلاعات مذکور از قالب اصلی به قالب دیگری تبدیل می‌شوند، یعنی قالب اطلاعاتی که تولید، ارسال یا دریافت شده‌اند تغییر یافته، اطلاعات در قالب جدیدی نگهداری یا ارائه می‌شوند.

اسناد الکترونیکی در هنگام نگهداری، گاه فشرده و گاه برای هماهنگی با تغییرات بازارهای نرم‌افزاری به قالب‌های جدید تبدیل می‌شوند تا قابل خواندن باشند [۲، ص٦٧]. همچنین گاهی یک سند کاغذی به جهتی مثلاً برای بایگانی الکترونیکی، اسکن شده، به یک سند الکترونیکی تبدیل می‌شود [۱۰، ص۱۰۲].

در چنین حالتی، تشخیص تمامیت سند، امری دشوار است. هنگام تغییر قالب سند، شیوه‌های امنیتی، همچون امضای دیجیتالی، قابلیت خود را در حفظ تمامیت سند از دست می‌دهند، زیرا امضای دیجیتالی فقط منضم به سند اولیه است و همراه با سند به قالب جدید منتقل نمی‌شود [۱۰, ص۱۰۳].

برای آن‌که تغییر قالب سند به اطمینان آن لطمه‌ای وارد نکند، فرایند نقل و انتقال باید به قدری ایمن باشد که تغییر یا ازبین رفتن اطلاعات ممکن نباشد. به این منظور بهتر است فرایند تبدیل توسط سامانه‌های خودکار صورت گیرد؛ زیرا رایانه کم‌تر از انسان خطا می‌کند. همچنین

ابزارهایی مثل تصویرگر،[1] چاپگر،[2] و تبدیل‌گر[3] که برای تغییر قالب سند به کار می‌روند باید قابل اطمینان بوده، مطابقت اسناد مبدأ و مقصد را تضمین کنند. در این صورت، فرایند کنترل و تطبیق اسناد به صورت خودکار انجام می‌شود و نیازی به بازبینی تمام اسناد نیست[۱۰، ص۱۰٤-۱۰٥].

همچنین برای اطمینان از عملیات تغییر قالب سند، می‌توان این امر را به مرجع ثالثی واگذار کرد که با استفاده از یک شیوه مطمئن، به تغییر قالب اسناد الکترونیکی و بایگانی آن‌ها بپردازد. این مرجع می‌تواند یک امضای الکترونیکی مطمئن را به شیوه‌ای غیرقابل تفکیک به سند ضمیمه کرده، ایمن بودن عملیات نقل و انتقال سند را تضمین کند[۱۱، ص۱۱].

از طرفی، غالب سامانه‌های الکترونیکی به صورت خودکار، به هنگام انتقال داده‌پیام، اطلاعاتی را به آغاز یا پایان داده‌پیام می‌افزایند، این امور، اصالت سند را مخدوش نمی‌کند و قانونگذار در چنین مواردی در صورتی که قالب سند دقیقاً نشانگر اطلاعات تولید، ارسال، دریافت یا ذخیره شده باشد آن سند را اصیل می‌داند. همچنین در مورد اسنادی که از قالب کاغذی به قالب الکترونیکی تبدیل شده‌اند نیز همین قاعده حکمفرما است، یعنی در صورتی که مندرجات یک سند کاغذی به قالب الکترونیکی تبدیل شود، در صورتی که احراز شود سند الکترونیکی حاوی همان مندرجات است، چنین سندی، اصل محسوب می‌شود [٦، ش١٦٩].

به هر ترتیب در صورت تغییر قالب سند، اثبات تمامیت اطلاعات موجود در سند و این‌که قالب جدید به صورت دقیق و بدون تغییر، نمایشگر اطلاعات قالب سابق سند است با ارائه‌کننده 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.

لازم به ذکر است که غالب سامانه‌های الکترونیکی به صورت خودکار، به هنگام انتقال داده‌پیام، متنی را که توسط کاربر ارسال شده‌است به علاوه اطلاعاتی درباره انتقال و دریافت آن، نام فرستنده و دریافت‌کننده، تاریخ و ساعت پیام‌های ارسال‌شده و دریافت‌شده و تأییدی مبنی بر این‌که نامه دریافت شده‌است به صورت خودکار ذخیره می‌کنند، اما این امور، اصالت سند را مخدوش نمی‌کند [۱۲، ص ١٦-١٧].

1. scanner
2. printer
3. converter

۳. نگهداری اطلاعات شناسایی داده‌پیام

بند «ج» این ماده، نگهداری اطلاعاتی را که مشخص‌کننده مبدأ، مقصد، و زمان ارسال و دریافت داده‌پیام است و برای شناسایی آن ضرورت دارد لازم می‌داند. این الزام، استانداردی را ایجاد می‌کند که حتی بالاتر از اسناد کاغذی اصیل است[۲، ش۷٤]. اطلاعات مذکور می‌تواند برای اثبات زمان و مکان انعقاد قرارداد یا ایقاعات مورد استفاده طرفین دعوا و دادگاه‌ها قرار گیرد [۱۳، ص۱۸٥].

البته ارائه این اطلاعات زمانی ضروری است که موجود باشند و در صورت فقدان چنین اطلاعاتی، نیازی به ارائه آن‌ها نیست و سند ارائه شده، باز هم اصل محسوب می‌شود.

البته گاهی هنگام ارسال داده‌پیام، برخی اطلاعات تکمیلی مثلاً پروتکل ارتباطات نیز ارسال می‌شود که به‌وسیله مخاطب دریافت می‌شود. نگهداری این نوع اطلاعات که صرفاً به دلیل انجام عملیات ارسال توسط سامانه‌های رایانه‌ای به وجود آمده ضروری نیست؛ چون این اطلاعات به منزله یک پاکت‌نامه برای اسناد کاغذی هستند که از طریق پست ارسال می‌شوند[٦، ش۱۷۰].

٤. رعایت شرایط خاص دستگاه‌های اجرایی

بند «د» این ماده مقرر می‌دارد: در مواردی که برخی وزارتخانه‌ها و سازمان‌ها برای نگهداری نسخه اصل، شرایط خاصی را مقرر کرده‌اند، رعایت این شرایط الزامی است، زیرا اطلاعات بایگانی‌شده غالباً در برخی امور اداری، مانند امور مالیاتی یا کنترل‌های گمرکی مورد استفاده قرار می‌گیرند و از آن‌جا که این حوزه‌ها مرتبط با نظم عمومی هستند گاه لازم است شرایط خاصی برای بایگانی اسناد مورد نیاز این ادارات مقرر شود[٦، ش۱۳٥].

البته رعایت شرایط خاص نگهداری اطلاعات به صورت داده‌پیام از وظایف دستگاه اجرایی و سازمان دولتی است که نگهداری داده‌پیام در حوزه مسؤولیتش قرار دارد و عدم رعایت شرایط در مقابل اشخاص ثالث قابل استناد نیست. بنابراین در چنین مواردی اگر اشخاص ثالث، تمامیت اطلاعاتی را که نزد وزارتخانه و سازمان و نهادهای دولتی وجود دارد اثبات کنند، سند مذکور به عنوان اصل سند در دادگاه پذیرفته خواهد شد، حتی اگر شرایط خاص وزارتخانه مذکور رعایت نشده باشد [۱۳، ص۱۸٥-۱۸٦].

نمونه این مقررات، شرایطی است که در ماده ۱۱۳ قانون برنامه چهارم توسعه اقتصادی برای نگهداری اسناد و اوراق قضایی مقرر شده‌است. در این ماده آمده‌است:

«به قوه قضاییه اجازه داده می‌شود:

الف) براساس آیین‌نامه‌ای که توسط وزیر دادگستری با همکاری دادستانی کل کشور و سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران تهیه و به تأیید رئیس قوه قضاییه می‌رسد، 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 واسناد تبدیلی در کلیه مراجع قضایی سندیت داشته و قابل استناد خواهد بود. اصل پرونده‌های مهم و ملی که جنبه سندیت تاریخی دارد توسط سازمان اسناد و کتابخانه ملی جمهوری اسلامی ایران حفظ و نگهداری خواهد شد».

بنابراین، قوه قضاییه برای نگهداری اسناد الکترونیکی، علاوه بر رعایت شرایط ماده ۸ قانون تجارت الکترونیک، باید شرایط خاص مقرر در این ماده، از جمله گذشت مدت سی سال از بایگانی قطعی پرونده و نیز شرایط آیین‌نامه مذکور را رعایت کند.

به موجب آیین‌نامه مذکور، دادگستری‌های سراسر کشور موظفند اوراق مهم پرونده‌هایی را که به شرح مندرج در ماده ۵ آیین‌نامه، نگهداری سوابق آن‌ها ضروری است و ۳۰ سال از زمان مختومه شدن آن‌ها سپری شده‌است و به صورت پرونده راکد درآمده‌اند به اسناد الکترونیکی تبدیل کنند. این اسناد به سازمان اسناد کتابخانه ملی در تهران یا شعب آن در شهرستان تسلیم شده، اسناد کاغذی امحا می‌شوند [۱٤].

این ماده از ماده ۱۰ قانون نمونه آنسیترال[۱] اقتباس شده‌است، با این تفاوت که ماده ۱۰ قانون آنسیترال در مورد «نگهداری داده‌پیام» است و شرایط نگهداری اصل سند در ماده ۸

---

۱. ماده ۱۰ قانون تجارت الکترونیکی آنسیترال: «هنگامی که قانون مقرر می‌دارد که اسناد، رکوردها، یا اطلاعات نگهداری شود این ضرورت با نگهداری داده‌پیام برآورده می‌شود، مشروط بر آن‌که شرایط زیر رعایت شود:

الف) اطلاعات مندرج در آن در دسترس باشد، به نحوی که برای ارجاعات بعدی قابل استفاده باشد.

ب) داده‌پیام در همان قالبی که تولید، ارسال یا دریافت شده ویا قالبی که دقیقاً اطلاعات تولید، ارسال یا دریافت‌شده را نمایش دهد نگهداری شود.

ج) اطلاعات به نحوی نگهداری شود که هویت داده‌پیام، مبدأ و مقصد، تاریخ و زمان ارسال و دریافت داده‌پیام مشخص باشد.

۲. الزام به نگهداری اسناد، سوابق و اطلاعات طبق بند یادشده، اطلاعاتی را که تنها هدف آن‌ها ایجاد امکان ارسال و دریافت داده‌پیام است شامل نمی‌شود.

۳. اشخاص مجازند الزامات مندرج در بند ۱ را با استفاده از خدمات اشخاص ثالث تأمین کنند، مشروط بر آن‌که شرایط مندرج در قسمت‌های «الف»، «ب» و «ج» بند ۱ رعایت شود».

آن قانون ذکر شده‌است. بند ٤ و ٥ ماده ۹ کنوانسیون استفاده از ارتباطات الکترونیکی در قراردادهای بین‌المللی[1] که ایران در سال ۲۰۰۷ به آن ملحق شده‌است نیز با عنوان «قواعد نگهداری به شکل اصل»، عباراتی مشابه با ماده مذکور را مقرر کرده‌است.[2]

ماده ۸ قانون نمونه تجارت الکترونیکی آنسیترال، نسخه اصل را چنین معرفی می‌کند:

«۱. در جایی که اطلاعات باید به صورت اصل ارائه یا نگهداری شود شرایط زیر در مورد داده‌پیام باید رعایت شود:

الف) یک تضمین قابل اتکا نسبت به تمامیت اطلاعات از لحظه‌ای که آن اطلاعات در شکل نهایی آن به عنوان داده‌پیام یا غیر آن، تولید شده‌اند وجود داشته باشد.

ب) در جایی که ارائه اطلاعات لازم است، آن اطلاعات قابلیت عرضه به شخصی را که اطلاعات باید به او ارائه شود دارا باشد.

۲. بند ۱ در مواردی که این نیاز به صورت تعهد و الزام است ویا قانون، آثار عدم نگهداری یا ارائه اصل سند را مقرر کرده‌است نیز اعمال می‌شود.

۳. برای تحقق اهداف قسمت «الف» بند ۱:

الف) ضابطه ارزیابی تمامیت، آن است که اطلاعات کامل و بدون تغییر باقی بماند. بنابراین، اعمالی که برای تصدی سیستم مثلاً ارسال، ذخیره یا نمایش اطلاعات به طور معمول انجام می‌شود و تغییری که در جریان عادی انتقال و ذخیره و نمایش اطلاعات رخ می‌دهد خدشه‌ای

---

1. Convention on The Use of Electronic Communications In International Contract 2007.

۲. ماده ۹ کنوانسیون استفاده از ارتباطات الکترونیکی در قراردادهای بین‌المللی:

بند ٤: در مواردی که قانون مقرر می‌دارد که نسخه اصل ارتباط یا قرارداد باید در دسترس قرار گیرد یا به همان شکل اصلی نگهداری شود یا آثار فقدان نسخه اصل را بیان می‌کند، این شرط به واسطه مبادله از طریق ارتباط الکترونیکی محقق می‌شود اگر:

الف) اطمینان قابل استنادی درخصوص صحت اطلاعات مندرج در ارتباط الکترونیکی مربوط از زمانی که برای نخستین بار و به شکل نهایی خود به صورت ارتباط الکترونیکی یا به صورت دیگر تولید شده موجود باشد و

ب) در صورتی که به موجب قانون اطلاعات مندرج در ارتباط الکترونیکی باید در دسترس باشد در این صورت آن اطلاعات باید برای شخصی که باید اطلاعات در اختیار او قرار گیرد قابل دستیابی باشد.

بند ٥: از نظر بند ٤ «الف»:

الف) معیار اطمینان از تمامیت و انسجام اطلاعات آن است که صرفنظر از اضافه‌شدن و هرگونه تصدیق یا تغییری که در فرایند معمول ارتباط، ذخیره و نمایش آن حادث می‌شود آیا اطلاعات مربوط به صورت کامل و بدون تغییر مانده‌اند یا خیر؛ و

ب) معیار اعتماد مورد نیاز باید در پرتو هدفی که اطلاعات برای آن تولید گردیده و نیز اوضاع و احوال مرتبط با آن ارزیابی شود».

بر تمامیت داده‌پیام وارد نمی‌کند.

ب) استاندارد ایمنی با توجه به اهدافی که اطلاعات برای آن تولید می‌شود و سایر اوضاع و احوال تعیین می‌شود».

با توجه به ماده فوق، معیار تمامیت سند، آن است که «شکل نهایی» سند به صورت کامل و بدون تغییر باقی بماند. منظور از «شکل نهایی» سند، هم آن شکل از سند است که از ابتدا به صورت الکترونیکی به وجود می‌آید وهم سندی است که از شکل کاغذی به شکل الکترونیکی تبدیل یافته‌است [۲، ش٦٦]؛ اما نسخ پیش‌نویس سند، یعنی اسنادی که مفاد آن‌ها هنوز مورد اراده نهایی طرفین قرار نگرفته‌اند، شکل نهایی سند محسوب نمی‌شوند [٦، ش١٦٩].

معیار ارزیابی اصالت، تمامیت سند است. ارزیابی تمامیت سند با توجه به اهدافی که سند برای آن به وجودآمده و سایر اوضاع و احوال، مثل تجهیزات مورد استفاده طرفین، نوع فعالیت تجاری آن‌ها، ارزش موضوع داده‌پیام، هزینه اتخاذ روش‌های ایمنی، انطباق با عرف و رویه تجاری و نیز قراردادهای خصوصی احتمالی لحاظ می‌شود [۲، ش٨٦]. بنابراین، ارزش روش‌های ایمنی مذکور در اثبات اصالت سند با توجه به اوضاع و احوال، متفاوت است. مثلاً در صورتی که ارزش معامله موضوع سند به میزانی است که استفاده از یک روش ایمنی مطمئن برای حفظ تمامیت آن، معقول نیست، استفاده از یک روش ایمنی ساده‌تر، تمامیت آن سند را تأمین می‌کند. همچنین در صورتی که صادرکنندگان سند به روش‌های ایمنی، همچون امضای دیجیتال دسترسی داشته باشند و بتوانند به‌سهولت از آن استفاده کنند استفاده از روش‌هایی که ایمنی کم‌تری دارند، نمی‌تواند تمامیت این اسناد را تأمین کند. همچنین این‌که عرف تجاری برای اسنادی مشابه با سند مورد اختلاف، کدام معیارهای ایمنی را در نظر می‌گیرد نیز باید لحاظ شود. بنابراین، معیار تمامیت در قانون آنسیترال، معیاری بسیار انعطاف‌پذیر است.

از مقایسه قانون تجارت الکترونیک ایران و قانون نمونه آنسیترال درمی‌یابیم که با وجود اختلاف عبارات، حکم هر دو قانون مشابه است و هر دو، شرط اصالت سند را تمامیت آن و قابلیت ارائه آن می‌دانند، اما تفاوت آن دو در این است که قانون آنسیترال برای ارزیابی تمامیت سند، معیار انعطاف‌پذیری مقرر کرده و آن را با توجه به اوضاع و احوال و هدفی که داده‌پیام برایش به وجود آمده‌است قابل ارزیابی می‌داند، اما قانون تجارت الکترونیک ایران، معیار تمامیت را مشخص نکرده‌است.

باید توجه داشت با وجود سکوت این قانون، در حقوق ایران نیز تمامیت سند با توجه به همین معیار ارزیابی می‌شود؛ زیرا بند «ب» ماده ٥ کنوانسیون استفاده از ارتباطات الکترونیکی در قراردادهای بین‌المللی که دولت ایران نیز به آن ملحق شده، با عباراتی مشابه قانون آنسیترال، همین معیار را برای ارزیابی تمامیت سند، مقرر کرده‌است. بنابراین، کنوانسیون مورد اشاره، ایراد مذکور را برطرف می‌سازد. به همین علت در معاملات کم بها استفاده از یک فناوری با سطح ایمنی پایین‌تر برای اثبات تمامیت سند کافی است؛ اما در معاملات پربها باید از فناوری ایمن‌تری برای حفظ تمامیت سند استفاده کرد.

نکته دیگر آن‌که همان‌گونه که بیان کردیم اسنادی که توسط رایانه ایجاد می‌شوند هیچ‌کدام اصل به مفهوم سنتی آن، یعنی سندی که اسناد دیگر از روی آن نوشته می‌شود، نیستند، بلکه همگی رونوشت‌هایی هستند که هیچ تفاوتی با یکدیگر ندارند. این امر موجب بروز مشکلات دیگری در مورد اسناد تجاری می‌شود. در اسناد تجاری، علاوه بر عنصر اصالت، «تک بودن»[1] سند نیز اهمیت دارد. برخی از اسناد تجاری در وجه حامل صادر می‌شوند و دارنده هر سند در وجه حامل، مالک آن محسوب می‌شود و وجود سند در دست شخص، دلالت بر مدیون بودن صادرکننده دارد. به همین علت، المثنی یا تصویر سند نباید وجود داشته باشد وصرفاً در مواردی که سند مفقود می‌شود قانونگذار با شرایطی دشوار، صدور نسخه دیگری از سند را ممکن می‌داند (مواد ۳۲۰ تا ۳۳٤ قانون تجارت مصوب ۱۳۱۱) و با توجه به این‌که در اسناد الکترونیکی، نسخه تولید شده هیچ‌گاه منحصر به فرد نیست قانونگذار باید برای تأمین این هدف تمهیداتی بیندیشد .

۴- شیوه‌های تعرض به اصالت اسناد الکترونیکی

قانونگذار، ارائه اصل سند را در صورتی لازم می‌داند که صحت آن مورد تکذیب قرار بگیرد؛ یعنی سند مورد انکار و تردید قرار گرفته، یا نسبت به آن ادعای جعل شود. در این مبحث به بررسی شیوه‌های تکذیب صحت اسناد می‌پردازیم.

---

1. unique

۴-۱- اظهار انکار و تردید

منظور از انکار، اعلام رد تعلق خط، امضا، مهر ویا اثرانگشت سند غیر رسمی به منتسبٌ‌الیه توسط خود او است [۵، ص۱۸۲]. منظور از تردید، عدم پذیرش انتساب خط، امضا، مهر ویا اثر انگشت سند غیر رسمی به منتسبٌ‌الیه توسط شخص دیگر است [۵، ص۱۸٤] که در دلایل الکترونیکی به صورت رد انتساب امضای الکترونیکی ذیل سند تحقق می‌یابد.

اظهار انکار و تردید فقط نسبت به اسناد عادی الکترونیکی ممکن است و اسناد مطمئن به موجب ماده ۱۵ قانون تجارت الکترونیک، قابل انکار و تردید نیستند. اسناد عادی الکترونیکی نیز در صورتی که از اماره انتساب سند به صادرکننده برخوردار باشند، غیرقابل انکار و تردید هستند. این اماره در مواد ۱۸ و ۱۹ قانون تجارت الکترونیک پیش‌بینی شده‌است. در این مواد، شرایطی مقرر شده‌است که در صورت تحقق آن‌ها، داده‌پیام به اصل‌ساز[۱] منسوب می‌شود.

ماده ۱۸ قانون تجارت الکترونیکی در بیان شرایط انتساب سند به صادرکننده مقرر می‌دارد: «در موارد زیر داده‌پیام منسوب به اصل‌ساز است:

الف) اگر توسط اصل‌ساز ویا به‌وسیله شخصی ارسال شده باشد که از جانب اصل‌ساز مجاز به این کار بوده‌است.

ب) اگر به‌وسیله سیستم اطلاعاتی برنامه‌ریزی شده یا تصدی خودکار از جانب اصل‌ساز ارسال شود».

همچنین ماده ۱۹ شرایطی را پیش‌بینی کرده که در صورت تحقق آن‌ها مخاطب حق دارد فرض کند که سند از جانب اصل‌ساز صادر شده‌است. به موجب ماده مذکور: «داده‌پیامی که براساس یکی از شروط زیر ارسال می‌شود مخاطب حق دارد آن را ارسال شده محسوب کرده و مطابق چنین فرضی (ارسال‌شده) عمل نماید:

الف) قبلاً به‌وسیله اصل‌ساز، روشی معرفی ویا توافق شده باشد که معلوم کند آیا داده‌-پیام همان است که اصل‌ساز ارسال کرده‌است.

ب) داده‌پیام دریافت‌شده توسط مخاطب از اقدامات شخصی ناشی شده که رابطه‌اش با اصل‌ساز یا نمایندگان وی باعث شده تا شخص مذکور به روش مورد استفاده اصل‌ساز

---

۱. اصل‌ساز (originator) منشأ اصلی داده‌پیام است که داده‌پیام به وسیله او یا از طرف او تولید یا ارسال می‌شود، اما شامل شخصی که در ارتباط با داده‌پیام به عنوان واسطه عمل می‌کند نخواهد شد (بند «ب» ماده ۲ قانون تجارت الکترونیک).

دسترسی یافته و داده‌پیام را به مثابه داده‌پیام خود بشناسد».

بند «ب» ماده ۱۹ به اشخاص ثالثی، مثل ارائه‌دهندگان خدمات الکترونیکی اشاره می‌کند که ممکن است به موجب توافق قبلی با اصل‌ساز، پیامی را از جانب وی ارسال دارند [۲، ش٨٦]. بنابراین، در صورتی که سند توسط سیستم اطلاعاتی خودکار تحت کنترل شخص یا توسط نمایندگان او صادر شود یا با روش مورد توافق طرفین یا اعلام‌شده از جانب اصل‌ساز ارسال شود منسوب به او است و اصل‌ساز نمی‌تواند آن را منتسب به خود نداند.

در صورتی که سند مورد انکار و تردید قرار گیرد، اثبات صحت انتساب سند با استنادکننده است. در اسناد کاغذی، اثبات این امر از طریق تطبیق خط، امضا، مهر یا اثرانگشت سند با خط، مهر، امضا یا اثر انگشت اسناد مسلم‌الصدور صورت می‌گیرد [۱۵، ص۳۲٥].

در مورد اسناد الکترونیکی از آن‌جا که امضا و خط سند به‌جز در مورد امضای زیست‌سنجی با ویژگی‌های زیستی و روانی شخص در ارتباط نیست نمی‌توان از این راهکار بهره برد، اما در سایر موارد باید از روش‌های دیگری برای اثبات انتساب سند به صادرکننده استفاده کرد؛ مثلاً اثبات این‌که سند از نشانی پست الکترونیکی صادرکننده، ارسال شده‌است یا این‌که سند دارای امضای دیجیتالی‌ای است که بر اساس فهرست عمومی گواهی‌ها، آن امضا، متعلق به شخص مورد ادعاست، می‌تواند انتساب سند به صادرکننده را اثبات کند؛ زیرا دارنده امضا، ملزم به جلوگیری از افشای کلید خصوصی است.

۴-۲- ادعای جعل

اصطلاح «جعل» در قانون مدنی و آیین دادرسی مدنی ایران تعریف نشده‌است، اما ماده ٥۲۳ قانون مجازات اسلامی این اصطلاح را چنین تعریف کرده‌است: «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 سیاه‌کردن 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».

در محیط الکترونیکی، واژه‌هایی همچون خدشه، تراشیدگی و قلم خوردگی بی‌معنا است و مدعی جعل باید جعل را متناسب با فضای الکترونیک اثبات کند. مثلاً اثبات کند که کلید

خصوصی یا گذرواژه او افشا شده یا کارت هوشمندش که آن را برای امور بانکی مورد استفاده قرار می‌دهد به سرقت رفته‌است. مصادیق جعل در فضای الکترونیک را می‌توان از ماده ٦٨ قانون تجارت الکترونیک استنباط کرد. ماده مذکور، تغییر، محو و متوقف کردن داده‌پیام در بستر مبادلات الکترونیکی، مداخله در پردازش داده‌پیام و سیستم‌های رایانه‌ای، استفاده بدون مجوز از وسایل کاربردی سامانه‌های رمزنگاری، مانند کلید اختصاصی در تولید امضا و نیز تولید امضای فاقد سابقه در فهرست دفاتر الکترونیکی را از مصادیق جعل می‌داند.

ادعای جعل، هم در مورد دلایل الکترونیکی عادی و هم در مورد دلایل الکترونیکی مطمئن می‌تواند مطرح شود. تفاوت ادعای جعل با اظهار انکار و تردید آن است که در ادعای جعل، خوانده می‌پذیرد که امضا و خط سند شبیه و حتی منطبق با خط و امضای او است، اما ادعا می‌کند که شبیه خط و امضای او را ساخته‌اند یا عبارتی از متن را افزوده یا کاسته ویا تغییر داده‌اند [١٥، ص٣٢٥].

از آن‌جا که جعل، نوعی ادعا است باید توسط ادعاکننده اثبات شود [٥، ص١٩٧]. اگرچه تغییر سند الکترونیکی، اثر فیزیکی باقی نمی‌گذارد، اما می‌توان آن را با استفاده از برخی روش‌های فنی اثبات کرد. به عنوان مثال، اگر سندی که دارای امضای دیجیتال است، بعد از امضا، مورد جعل و تغییر قرار گیرد، این تغییر به‌راحتی قابل تشخیص است؛ زیرا امضای دیجیتال از فناوری «خرد کردن»[1] استفاده می‌کند [١٦، ص٤٢-٤٣]. در این فرایند، پیام قبل از ارسال با استفاده از یک الگوریتم ریاضی خرد شده، به یک «خلاصه‌پیام» تبدیل می‌شود. این خلاصه نسبت به متن پیام کاملاً منحصر به فرد است و حکم یک اثر انگشت منحصر به فرد را دارد، به طوری که هیچ‌گاه دو متن نمی‌توانند یک اثر انگشت داشته باشند و در صورتی که حتی یک حرف از پیام تغییر یابد، آن اثر انگشت تغییر می‌کند [١٧، ص٤٢٧ - ٤٢٨] که از این امر می‌توان برای اثبات جعلی بودن پیام استفاده کرد.

همچنین در صورتی که از منوی File گزینه Properties و 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 [١٨، ص٢٣- ٢٤] که اگر تاریخ تغییر، بعد از تاریخ تنظیم سند باشد این امر، مثبت جعلی بودن سند است.

1. Hash Function

به علاوه با توجه به آن‌که ابزارهای الکترونیکی بسیار پویا و دائم در حال تغییرند می-توان از تاریخ ابداع ابزار، به عنوان نشانه‌ای برای اثبات جعلیت استفاده کرد. مثلاً اگر نوع خط و قالب سندی که به دادگاه ارائه شده، بعد از تاریخ تنظیم سند به بازار آمده‌است این امر می-تواند دلیلی بر جعلی بودن سند باشد.

۶- نتیجه‌گیری

اصالت سند، عنصری است که قانونگذار، وجود آن را جهت تشخیص تمامیت سند و عدم جعل و تغییر آن لازم می‌داند. در اسناد الکترونیکی، تحقق مفهوم اصل سند به معنای نسخه‌ای که بی‌واسطه و به طور مستقیم توسط صادرکننده سند به وجود آمده، امکان‌پذیر نیست؛ اما می‌توان با استفاده از شیوه‌های فنی، مانند امضای دیجیتال، تمامیت سند را در دلایل الکترونیکی تأمین کرد و با توجه به آن‌که حقوق، ذاتاً کارکردگرا است، اثبات تمامیت سند، الزام به ارائه اصل سند را برآورده می‌سازد. ماده ۸ قانون تجارت الکترونیک، شرایطی را مقرر کرده‌است که سند الکترونیکی در صورت برخورداری از این شرایط، اصل محسوب می‌شود.

از طرفی، اظهار انکار و تردید و ادعای جعل به عنوان شیوه‌های تکذیب اصالت سند در دلایل الکترونیکی تغییر پیدا کرده و با توجه به ماهیت غیرمادی این ادله، مصادیق ویژه‌ای یافته‌اند. مدعی اصالت سند برای اثبات اطمینان دلیل و صحت آن، باید از شیوه‌های فنی متناسب با این ادله استفاده کند.

۷- منابع

[۱] مدنی، جلال‌الدین، *ادله اثبات دعوا*، چ۵، نشر پایدار،۱۳۷۹.

[2] *UNCITRAL Model Law on Electronic Signature with Guide to Enactment, 2001*,United Nations, New York, 2002, www.uncitral.org/English/texts/electom/ml-elecsig-e.pdf.

[۳] آهنی،بتول، *انعقاد و اثبات قراردادهای الکترونیکی*، پایان‌نامه دوره دکتری حقوق خصوصی، دانشکده حقوق دانشگاه تهران،۱۳۸٤ .

[٤] جعفری لنگرودی، محمدجعفر، *مبسوط در ترمینولوژی حقوق*، تهران، گنج دانش، ١٣٧٨.

[٥] شمس، عبدالله، *آیین دادرسی مدنی*، ج٣، چ٣، تهران، انتشارات دراک، ١٣٨٤.

[6] Convention On The Use Of Electronic Communications In International Contract2007, www.uncitral.org.

[7] Wilding, Edward,*Computer Evidence :A Forensic Investigations Handbook*, London, Sweet & Maxwell, 1997.

[8] UNCITRAL Model Law on Electronic Commerce with Guide to Enactment, 1996, United National.www.Uncitral.org/pdf/English/texts/electoms/ml-e common. html.

[٩] زرکلام، ستار،«امضای الکترونیکی وجایگاه آن در نظام ادله اثبات دعوا»، *مجله مدرس*، دوره هفتم، ش ا، ١٣٨٢.

[١٠] ویلک، دنیل، «اعتبار کپی‌های برابر اصل در اسناد الکترونیکی»، ترجمه غلامعلی بازیاری سروستانی، *ماهنامه کانون سردفتران و دفتریاران*، ش ٦٣، ١٣٨٥.

[11] Irons, Alastair, "Computer Forensics and Records Management-Computer Discipline", PP. 102-112, *Record Management Journal*, vol.16, 2006.

[١٢] سلطانی،محمد، *ادله الکترونیک اثبات دعوا*،پایان نامه کارشناسی ارشد حقوق خصوصی، دانشکده حقوق دانشگاه تهران،١٣٨٤.

[١٣] دوبلفون، زویه لینان، *حقوق تجارت الکترونیک*، ترجمه ستار زرکلام، مؤسسه مطالعات و پژوهش‌های حقوقی شهر دانش، ١٣٨٨.

[١٤] دستورالعمل مواد ٨،١٥ و تبصره ماده ٢ آیین‌نامه اجرایی بند «الف» ماده ١٣١ برنامه چهارم توسعه اجتماعی، اقتصادی و فرهنگی مصوب ١٣٨٦/٦/٢٥، قوه قضاییه.

[١٥] کاتوزیان، ناصر، *اثبات و دلیل اثبات*، ج ١، نشر میزان، ١٣٨٠.

[١٦] عبدالهی، محبوبه، *دلیل الکترونیکی در دعوای حقوقی*، پایان‌نامه کارشناسی ارشد حقوق خصوصی دانشگاه تربیت مدرس، ١٣٨٧.

[17] Susan, Hansche and others, *Official Guide to CISSP Exam*, USA, Press, 2004, pp.427-428.

[18] Rockwood, Rebecca," Shifting Burdens and Concealing Electronic Evidence: Discovery in Digital area", *Journal of Law & Technology*, 2005, vol. xll, no. 4.