فصـــــلنامه پژوهـــش های حقوقی قـــانـــون یـــار

License Number: 80025 Article Cod: W54772715 ISSN-E: 6452-2588

اعتبار امضای الکترونیک و چالش‌های اثبات در دعوای خصوصی[1]

(تاریخ دریافت ۱٤۰٤/۱۰/۱۱ تاریخ تصویب ۱٤۰٤/۱۲/۰٦)

فرشید خوشبخت

چکیده

گسترش مبادلات دیجیتال، امضای الکترونیک را از یک ابزار فنی به نهادی حقوقی با آثار گسترده در روابط خصوصی تبدیل کرده است. با وجود پذیرش کلی «کفایت» امضای الکترونیکی در بسیاری از نظام های حقوقی، مسئله اصلی در عمل نه صرفاً پذیرش، بلکه «اعتبارسنجی» و «اثبات انتساب» آن در دعاوی خصوصی است. در اختلافات قراردادی، مطالبه وجه، ادعای فسخ، مسئولیت مدنی ناشی از تراکنش‌های برخط، یا دعوای تردید در اصالت سند، طرفین غالباً با این پرسش روبه‌رو می‌شوند که آیا داده‌پیامِ امضاشده می‌تواند در حکم سند معتبر عمل کند و چگونه می‌توان اصالت، تمامیت، زمان‌مندی و اراده امضاکننده را اثبات یا انکار کرد. چالش های اثباتی در این حوزه به دلیل ماهیت غیرمادی داده، امکان تکثیر و دستکاری، پیچیدگی زنجیره نگهداری ادله دیجیتال، و فاصله معرفتی میان دادگاه و فناوری تشدید می‌شود. پژوهش حاضر با رویکرد تحلیلی توصیفی و با اتکا به مبانی حقوق ادله اثبات دعوا، قواعد پذیرش داده‌پیام، و مقایسه محدود با استانداردهای بین‌المللی، تلاش می‌کند چارچوبی منسجم برای فهم «اعتبار» امضای الکترونیک و صورت‌بندی «چالش‌های اثبات» در دعوای خصوصی ارائه دهد. نتیجه پژوهش نشان می‌دهد که اعتبار حقوقی امضا زمانی به کارکرد واقعی می‌رسد که دادگاه‌ها ابزارهای عملی برای ارزیابی فنی و حقوقی آن داشته باشند؛ از جمله معیارهای حداقلی برای سیستم اطلاعاتی مطمئن، مدیریت گواهی و کلید،

[1] بر اساس نظر هیات داوران همایش های بنیاد علمی قانون یار، این مقاله به عنوان یکی از مقالات برگزیده و منتخب دهمین همایش بنیاد علمی قانون یار قرار گرفت. این رویداد علمی تحت عنوان (دهمین همایش ملی تحقیقات و یافته های نوین علمی در حوزه علوم انسانی و فرهنگی) در تاریخ ۲۷ بهمن ماه ۱۴۰۴ در استان اصفهان (دانشگاه آزاد واحد دهاقان) برگزار گردید. این مقاله علاوه بر پذیرش در این همایش، به صورت رایگان در فصلنامه الکترونیکی پژوهش های حقوقی قانون یار مورد پذیرش و چاپ قرار گرفت.

گزارش‌های ممیزی، زمان سنج معتبر، و قواعد روشن درباره بار اثبات و امارات قضایی. همچنین پیشنهاد می شود سازوکارهای تکمیلی مانند دستورالعمل‌های قضایی، استانداردهای کارشناسی و پروتکل‌های حفظ ادله دیجیتال، نقش تعیین‌کننده‌ای در کاهش تعارضات و افزایش امنیت حقوقی دارند.

واژگان کلیدی: امضای الکترونیک، دعوای خصوصی، ادله اثبات دعوا، داده‌پیام، سند الکترونیکی، انتساب، تمامیت، بار اثبات، کارشناسی فنی

مقدمه

تحول دیجیتال در دهه‌های اخیر، شیوه انعقاد قراردادها، تبادل اراده‌ها و حتی ادراک ما از «سند» را دگرگون کرده است. زمانی، سند غالباً به شیئی مادی بر روی کاغذ، با اثر قلم و امضای دستی گره خورده بود. اکنون داده‌ها در شبکه‌ها جریان دارند، اراده‌ها در قالب کلیک، رمز یک‌بارمصرف، گواهی دیجیتال یا امضای مبتنی بر کلید عمومی بیان می‌شوند و پرونده‌های قضایی ناگزیر باید با واقعیتی مواجه شوند که در آن «اثر حقوقی» بر بستری غیرمادی شکل می‌گیرد. در چنین فضایی، امضای الکترونیک صرفاً جانشین امضای دستی نیست، بلکه نشانگر تغییر بنیادین در سازوکار اعتماد در روابط خصوصی است؛ اعتمادی که پیش‌تر بر حضور فیزیکی، خط‌شناسی و اصالت ظاهری استوار بود و اکنون بر امنیت سامانه، مدیریت هویت دیجیتال، رمزنگاری، ثبت رویدادها و قابلیت ممیزی بنا می‌شود.

با این همه، تبدیل شدن امضای الکترونیک به ابزار اصلی اعتماد، به همان اندازه که ظرفیت تسهیل معاملات را دارد، منبع اختلاف نیز هست. در دعوای خصوصی، طرفی که امضا به او منتسب شده ممکن است ادعا کند امضا جعلی است، کلید خصوصی در اختیار دیگری بوده، یا

تراکنش بدون قصد و رضای واقعی انجام شده است. از سوی دیگر، طرف مقابل ممکن است به گزارش سامانه، گواهی صادره از مرجع معتبر یا سوابق ورود و خروج استناد کند. نقطه برخورد این دو ادعا در دادگاه شکل می‌گیرد؛ جایی که باید هم قواعد کلاسیک ادله اثبات دعوا رعایت شود و هم ظرایف فنی که بدون فهم آن‌ها قضاوت دقیق ممکن نیست.

پژوهش حاضر بر این تمرکز دارد که «اعتبار امضای الکترونیک» در معنای حقوقی و عملی چگونه ساخته می‌شود و چرا «چالش‌های اثبات» در دعوای خصوصی، حتی با وجود پذیرش قانونی امضا، همچنان پررنگ است. پرسش محوری این است که دادگاه در برابر انکار یا تردید نسبت به امضای الکترونیکی، چه معیارهایی برای تشخیص انتساب و صحت باید داشته باشد و چگونه می‌توان تعادلی میان سه ارزش برقرار کرد: امنیت حقوقی، حمایت از اعتماد مشروع طرفین، و جلوگیری از تحمیل فناوری به‌عنوان امری مبهم و غیرقابل راستی‌آزمایی.

- **بیان مسئله**

مسئله اصلی از شکاف میان «پذیرش قانونی» و «امکان اثبات عملی» ناشی می‌شود. بسیاری از مقررات، اصل عدم رد ارزش اثباتی داده‌پیام صرفاً به دلیل شکل الکترونیکی را پذیرفته‌اند. در سطح نظری، این گام مهمی در هم‌ترازی سند الکترونیکی با سند کاغذی است. اما در سطح دعوا، پرسش‌های دشوارتری مطرح می‌شود:

یکی اصالت و انتساب است. امضای الکترونیکی به معنای عام ممکن است طیفی وسیع از روش‌ها را دربرگیرد؛ از تصویر اسکن‌شده امضا تا امضای مبتنی بر گواهی دیجیتال. هرچه روش ساده‌تر باشد، امکان انکار و جعل افزایش می‌یابد. هرچه روش پیچیده‌تر باشد، دادگاه برای فهم و ارزیابی آن به کارشناسی وابسته‌تر می‌شود. بنابراین، حتی وقتی قانون «کفایت» امضا را می‌پذیرد، سطح اطمینان لازم برای اثبات انتساب در پرونده‌های مختلف یکسان نیست.

دوم تمامیت و عدم دستکاری است. داده‌پیام به‌سادگی قابل کپی، انتقال، تغییر یا بازتولید است. در دعاوی خصوصی، طرفین ممکن است نسخه‌های متفاوتی از یک فایل ارائه کنند یا ادعا

شود پس از امضا، محتوای سند تغییر کرده است. اگر سازوکارهای هش، امضای مبتنی بر کلید عمومی یا ثبت زمان معتبر وجود نداشته باشد، حل اختلاف دشوار می‌شود و دادگاه ممکن است به امارات سنتی متوسل شود که برای محیط دیجیتال کفایت ندارد.

سوم زمان‌مندی و توالی رخدادهاست. بسیاری از دعاوی به زمان دقیق انعقاد قرارداد، زمان ارسال قبول، یا تقدم و تأخر اصلاحات مربوط است. در فضای دیجیتال، زمان سیستم‌ها می‌تواند تغییر کند و گزارش‌ها قابلیت دستکاری داشته باشند. نبود معیارهای استاندارد برای «زمان‌سنجی مطمئن» سبب می‌شود اثبات زمان انعقاد یا ارسال، به نزاعی فنی تبدیل شود.

چهارم مسئله اراده و رضایت است. در حقوق خصوصی، قصد و رضا رکن اساسی معاملات است. در امضای الکترونیکی، ممکن است امضا با رمز عبور، توکن یا گوشی همراه انجام شود. اگر این ابزارها در اختیار دیگری قرار گیرد، یا امضاکننده در معرض فریب و مهندسی اجتماعی باشد، نسبت دادن اراده واقعی دشوار می‌شود. دادگاه باید میان «انتساب فنی» و «انتساب حقوقی» تمایز بگذارد.

پنجم دشواری های آیینی و نهادی است. دعوای خصوصی به قواعد دادرسی و ادله اثبات وابسته است. اما بسیاری از نظام‌های قضایی در سطح رویه، دستورالعمل روشن و یکسانی برای حفظ ادله دیجیتال، زنجیره نگهداری، قالب‌های قابل قبول گزارش سامانه‌ها و استاندارد کارشناسی ندارند. نتیجه آن است که پرونده‌های مشابه ممکن است به نتایج متفاوت برسند و امنیت حقوقی کاهش یابد.

بر این اساس، مسئله پژوهش حاضر تبیین رابطه میان اعتبار حقوقی امضای الکترونیک و دشواری‌های اثباتی در دادگاه‌های دعاوی خصوصی است؛ به‌گونه‌ای که بتوان راهکارهایی برای ارتقای قابلیت اتکای سند الکترونیکی و کاهش تعارضات ارائه داد.

- **مرور ادبیات**

ادبیات این حوزه را می‌توان به چند جریان اصلی تقسیم کرد. جریان نخست، نوشته‌هایی است که بر «تعریف و گونه‌شناسی» امضای الکترونیک تمرکز می‌کند و تفاوت امضای ساده، پیشرفته و مبتنی بر گواهی را توضیح می‌دهد. این آثار معمولاً از منظر فنی و حقوقی، عناصر هویت، کنترل انحصاری ابزار امضا و پیوند منطقی امضا با داده‌پیام را برجسته می‌سازند و نشان می‌دهند که چگونه فناوری رمزنگاری کلید عمومی می‌تواند معیارهای سنتی اصالت را بازتولید کند.

جریان دوم، پژوهش‌هایی است که به «اعتبار و آثار حقوقی» پرداخته‌اند و می‌کوشند جایگاه امضای الکترونیک را در نظام ادله اثبات دعوا مشخص کنند. در این دسته، پرسش اصلی این است که سند الکترونیکی در کدام طبقه از ادله می‌گنجد و آیا می‌تواند نقش سند رسمی یا عادی را ایفا کند. برخی نویسندگان بر این باورند که معیار اصلی باید «سطح اطمینان» باشد نه «شکل»؛ به این معنا که هر امضایی که انتساب و تمامیت را با سطح بالایی تضمین کند، باید آثار کامل سند را داشته باشد. برخی دیگر، به دلیل خطرات جعل و دشواری‌های اثبات، خواهان تمایز جدی میان امضای مطمئن و غیرمطمئن شده‌اند و نقش مراکز صدور گواهی را در ایجاد اطمینان حقوقی پررنگ دانسته‌اند.

جریان سوم، ادبیاتی است که «چالش‌های اثبات و دادرسی» را محور قرار می‌دهد. این آثار غالباً به موضوعاتی مانند بار اثبات، امارات قضایی ناشی از گزارش‌های سامانه، اعتبار لاگ‌ها و متادیتا، روش‌های کشف دیجیتال، و نقش کارشناسی فناوری اطلاعات می‌پردازند. در این رویکرد، امضای الکترونیک صرفاً یک علامت نیست، بلکه بخشی از یک اکوسیستم ادله است: سامانه‌ای که ثبت رویداد، مدیریت دسترسی، ذخیره‌سازی مطمئن و گزارش‌دهی را فراهم می‌کند. بنابراین، اثبات در دعوای خصوصی به کیفیت این اکوسیستم وابسته است.

جریان چهارم، مطالعات تطبیقی و بین‌المللی است که با بررسی اسناد نمونه و مقررات منطقه‌ای، اصول مشترک را استخراج می‌کند. در این حوزه، مفهوم «عدم تبعیض نسبت به شکل الکترونیکی» و نیز مفهوم «سطوح امضا» و آثار ویژه امضای واجد شرایط در برخی نظام‌ها مطرح می‌شود. این ادبیات کمک می‌کند تا نشان داده شود چگونه نظام‌های حقوقی برای کاهش اختلاف، از «فرض‌های قانونی» و «امارات اعتبار» استفاده می‌کنند؛ مثلاً در برخی چارچوب‌ها، امضای واجد شرایط اثر معادل امضای دستی دارد و معمولاً با اماره‌ای قوی نسبت به انتساب همراه است.

در مجموع، ادبیات موجود نشان می‌دهد که هرچند از نظر نظری درباره اصل پذیرش امضای الکترونیک توافق قابل توجهی وجود دارد، اما در سطح عملیِ دادرسی، هنوز درباره معیارهای ارزیابی، میزان اتکا به گزارش سامانه ها، حدود نقش کارشناسی، و نحوه توزیع بار اثبات اختلاف نظر باقی است. پژوهش حاضر تلاش می‌کند با تمرکز بر دعوای خصوصی، این شکاف را با یک تحلیل منسجم‌تر از «اعتبار» و «اثبات» کاهش دهد و پیشنهادهای اجرایی ارائه کند.

- **روش شناسی**

روش پژوهش، توصیفی تحلیلی با رویکرد میان‌رشته‌ای محدود است. در گام نخست، مفاهیم کلیدی امضای الکترونیک، داده‌پیام، انتساب و تمامیت در چارچوب حقوق خصوصی و ادله اثبات تبیین می‌شود. در گام دوم، قواعد پذیرش و ارزش اثباتی داده‌پیام و نیز سازوکارهای امضای مطمئن به‌عنوان مبنای تحلیل حقوقی بررسی می‌گردد. در گام سوم، چالش‌های اثباتی در دعاوی خصوصی صورت‌بندی می‌شود و برای هر چالش، پیوند میان عنصر حقوقی و سازوکار فنی توضیح داده می‌شود. در گام چهارم، از مطالعات تطبیقی منتخب و اسناد نمونه بین‌المللی برای استخراج اصول و راهکارهای قابل اقتباس استفاده می‌شود. در این پژوهش از ارجاع درون‌متنی خودداری شده و منابع به‌صورت مستقل در پایان مقاله ارائه شده‌اند. همچنین

تلاش شده نگارش علمی، دقیق و در عین حال روان باشد و هر بخش به‌صورت محتوایی مستقل، اما پیوسته با بخش‌های دیگر تنظیم شود.

بخش اول: مبانی مفهومی و حقوقی امضای الکترونیک

در تحلیل اعتبار امضای الکترونیک، نخست باید روشن شود که «امضا» در حقوق خصوصی چه کارکردهایی دارد. امضای دستی سنتی، دست‌کم سه کارکرد اصلی دارد: شناسایی امضاکننده، اعلام انتساب متن به او، و نشان دادن اراده او به التزام. گاه کارکرد چهارمی نیز مطرح است و آن، نقش امضا در ایجاد «اماره تمامیت» است؛ یعنی این تصور عرفی که پس از امضا، متن نباید تغییر کند و اگر تغییر کرده باشد، قابل کشف است. در فضای الکترونیکی، این کارکردها باید به‌گونه‌ای بازسازی شود که هم با فناوری سازگار باشد و هم نیازهای دادرسی را پاسخ دهد.

امضای الکترونیکی در معنای عام، هر علامت یا فرآیندی است که به داده‌پیام منضم یا به‌طور منطقی به آن متصل می‌شود و برای شناسایی امضاکننده یا اعلام رضایت او به محتوای داده‌پیام به کار می‌رود. این تعریف عام، بسیار فراگیر است و می‌تواند از تایپ کردن نام در انتهای ایمیل تا امضای مبتنی بر گواهی دیجیتال را شامل شود. نتیجه چنین فراگیری آن است که از نظر اثباتی، «امضا» یک مفهوم واحد نیست و باید میان سطوح مختلف آن تمایز گذاشت. در برابر این مفهوم عام، مفهوم «امضای مطمئن» یا «امضای امن» مطرح می‌شود که معمولاً با معیارهایی مانند انحصاری بودن نسبت به امضاکننده، قابلیت شناسایی او، تحت کنترل بودن ابزار امضا، و اتصال به داده‌پیام به‌گونه‌ای که هر تغییر بعدی قابل تشخیص باشد تعریف می‌شود. این معیارها در واقع ترجمه حقوقیِ همان چهار کارکرد کلاسیک امضا هستند، اما با ابزارهای فنی مانند کلید خصوصی، الگوریتم هش، گواهی دیجیتال و زیرساخت کلید عمومی تحقق می‌یابند.

مبنای حقوقی اعتبار امضای الکترونیک معمولاً بر دو اصل استوار است. اصل نخست، اصل «برابری کارکردی» است: هرگاه قانون وجود امضا را لازم بداند، امضای الکترونیکی در صورتی که کارکردهای لازم را تأمین کند، باید کافی تلقی شود. اصل دوم، اصل «عدم تبعیض نسبت به شکل الکترونیکی» است: داده‌پیام و امضای الکترونیک نباید صرفاً به دلیل الکترونیکی بودن از ارزش حقوقی یا پذیرش در دادرسی محروم شوند. این دو اصل اگرچه در سطح نظری روشن‌اند، اما در عمل نیازمند معیارهای سنجش هستند؛ زیرا دادگاه باید تشخیص دهد که آیا در پرونده مشخص، کارکردهای امضا تحقق یافته یا خیر.

اعتبار حقوقی امضای الکترونیک را می توان در سه لایه تحلیل کرد. لایه نخست، اعتبار به‌عنوان «شرط شکلی» است؛ یعنی آیا قانون برای آن عمل حقوقی، امضا یا شکل خاصی را شرط کرده و آیا امضای الکترونیکی می‌تواند جایگزین شود. لایه دوم، اعتبار به‌عنوان «ادله اثبات» است؛ یعنی آیا سند امضاشده قابل استناد است و چه وزن اثباتی دارد. لایه سوم، اعتبار به‌عنوان «اعتماد عملی» است؛ یعنی آیا در اکوسیستم فنی و قراردادی، سازوکارهایی وجود دارد که امکان انکار یا جعل را به حداقل رساند و هزینه اثبات را کاهش دهد. دعوای خصوصی غالباً در تقاطع این سه لایه شکل می‌گیرد.

از منظر حقوق قراردادها، امضای الکترونیکی معمولاً نقش «نشانگر توافق» را بازی می‌کند. اما توافق در حقوق خصوصی صرفاً یک رخداد فنی نیست؛ بیان اراده است. پس اگر امضا به‌صورت فنی قابل انتساب باشد ولی امضاکننده ادعا کند اراده او مخدوش بوده، دادگاه باید از نظریه‌های عیوب اراده، اشتباه، اکراه، یا تدلیس استفاده کند. اینجا اهمیت تفاوت میان «انتساب فنی» و «انتساب حقوقی» روشن می‌شود. انتساب فنی می‌گوید این امضا با کلید یا حساب کاربری مربوط انجام شده است. انتساب حقوقی می‌پرسد آیا این عمل واقعاً بیان اراده معتبر شخص بوده است. هرچه سامانه‌ها دقیق‌تر باشند، انتساب فنی آسان‌تر می‌شود، اما انتساب حقوقی همچنان نیازمند بررسی زمینه‌ها و قرائن است.

بخش دوم: جایگاه امضای الکترونیک در نظام ادله اثبات دعوا

برای فهم چالش‌های اثبات، باید امضای الکترونیک را در چارچوب ادله اثبات دعوا قرار داد. در دعوای خصوصی، سند معمولاً یکی از مهم‌ترین ادله است، زیرا بر خلاف شهادت که تابع ذهن و حافظه است، سند به‌عنوان یک «ثبت پایدار» عمل می‌کند. با ورود داده‌پیام، مفهوم ثبت پایدار به «سابقه الکترونیکی» منتقل شد. اما پایداری در فضای دیجیتال به معنای ماندگاری فیزیکی نیست، بلکه به معنای قابلیت بازیابی، خوانایی، تمامیت و قابلیت انتساب در طول زمان است. ۰در بسیاری از نظام‌ها، پذیرش داده‌پیام به این معناست که دادگاه نمی‌تواند صرفاً به دلیل شکل الکترونیکی، ارزش اثباتی آن را رد کند. این قاعده، نقطه آغاز است نه پایان. زیرا پس از پذیرش، وزن‌دهی و ارزیابی آغاز می‌شود. دادگاه باید بسنجد که داده‌پیام ارائه‌شده، تا چه حد به واقعیت خارجی نزدیک است و آیا خطر جعل یا دستکاری آن قابل اعتناست.

در این مرحله، مفهوم «سیستم اطلاعاتی مطمئن» اهمیت می‌یابد. اگر داده‌پیام در یک سیستم مطمئن ایجاد، ارسال، دریافت و نگهداری شده باشد، احتمال دستکاری کاهش می‌یابد و دادگاه می‌تواند با اطمینان بیشتری به آن استناد کند. اما «مطمئن بودن» یک ادعای ساده نیست؛ نیازمند شاخص هاست: کنترل دسترسی، ثبت رویدادها، امکان ممیزی، مدیریت تغییرات، نسخه‌برداری امن، و نیز سازوکارهای رمزنگاری.

از منظر اثبات، امضای الکترونیکی به‌تنهایی ممکن است کافی نباشد و معمولاً همراه با قرائن دیگر ارزش پیدا می‌کند. برای مثال، در یک قرارداد برخط، مجموعه‌ای از ادله کنار هم قرار می‌گیرد: متن قرارداد، امضای الکترونیک یا کلیک پذیرش، گزارش لاگ ورود و خروج، آی‌پی و شناسه دستگاه، پیامک‌های تأیید، سوابق پرداخت، و مکاتبات بعدی طرفین. دادگاه با کنار هم گذاشتن این عناصر به یک اقناع می‌رسد. بنابراین، مسئله اثبات در فضای دیجیتال غالباً شبکه‌ای است نه تک‌دلیل.

در دعاوی خصوصی، دو وضعیت رایج رخ می‌دهد. وضعیت نخست، زمانی است که طرف مقابل امضا را می‌پذیرد، اما درباره آثار حقوقی اختلاف دارد؛ مثلاً اختلاف در تفسیر شروط یا ادعای فسخ. در این حالت، امضا نقش «پایان دادن به نزاع درباره انتساب» را دارد و دعوا به حوزه ماهوی قرارداد منتقل می‌شود. وضعیت دوم، زمانی است که امضا یا سند مورد انکار یا تردید قرار می‌گیرد. در اینجا امضا به مرکز نزاع تبدیل می‌شود و پرسش اصلی این است که آیا سند واقعاً از طرف خوانده صادر شده است یا خیر. بخش عمده چالش‌های اثباتی مربوط به وضعیت دوم است.

بخش سوم: چالش‌های اثبات انتساب و اصالت در دعوای خصوصی

مهم‌ترین چالش در دعوای خصوصی، اثبات انتساب امضا به شخص معین است. در امضای دستی، دادگاه می‌تواند به خط‌شناسی، تطبیق امضا، و قرائن فیزیکی استناد کند. در امضای الکترونیک، ابزارها متفاوت‌اند و در نتیجه نوع تردید نیز تغییر می‌کند.

نخستین چالش، تنوع روش‌های امضاست. اگر امضا صرفاً تصویر اسکن‌شده باشد، از نظر فنی به‌سادگی قابل کپی است و ارزش اثباتی آن معمولاً پایین‌تر است، مگر اینکه با قرائن دیگر تقویت شود. اگر امضا مبتنی بر حساب کاربری و رمز عبور باشد، مسئله این است که آیا رمز عبور واقعاً در اختیار شخص بوده یا دیگری به آن دسترسی داشته است. اگر امضا مبتنی بر گواهی دیجیتال و کلید خصوصی باشد، پرسش به سمت مدیریت کلید، امنیت توکن، و فرایند صدور و ابطال گواهی می‌رود. بنابراین، دادگاه باید ابتدا «نوع امضا» را تشخیص دهد و سپس معیارهای متناسب را به کار گیرد.

دومین چالش، ادعای سوءاستفاده از ابزار امضاست. در عمل، بسیاری از امضاهای الکترونیکی بر پایه «کنترل انحصاری» معنا می‌یابد: کلید خصوصی یا ابزار امضا باید تحت کنترل امضاکننده باشد. اگر خوانده ادعا کند گوشی یا توکن او سرقت شده، یا رمز عبور افشا شده، بار اثبات چگونه توزیع می‌شود. پاسخ یکسانی وجود ندارد، اما می‌توان گفت هرچه امضا از

نوع مطمئن‌تر باشد و سامانه استانداردهای امنیتی بالاتری داشته باشد، اماره انتساب قوی‌تر خواهد بود و مدعی خلاف باید دلیل قانع‌کننده‌تری ارائه کند.

سومین چالش، مسئله هویت دیجیتال است. در فضای فیزیکی، هویت با حضور و مدارک شناسایی احراز می‌شود. در فضای دیجیتال، هویت ممکن است از طریق ثبت‌نام، تطبیق شماره ملی، احراز بیومتریک، یا گواهی دیجیتال انجام شود. اگر فرایند احراز هویت ضعیف باشد، امضای بعدی نیز از نظر اثباتی آسیب‌پذیر می‌شود. بنابراین، اعتبار امضا به اعتبار فرایند احراز هویت گره خورده است.

چهارمین چالش، کیفیت لاگ‌ها و گزارش‌های سامانه است. بسیاری از دعاوی خصوصی به گزارش‌های یک پلتفرم، بانک، یا سامانه معاملاتی متکی است. اما گزارش زمانی ارزش اثباتی بالایی دارد که قابل ممیزی و غیرقابل دستکاری باشد و زنجیره نگهداری آن رعایت شده باشد. اگر لاگ‌ها قابل ویرایش باشند یا سامانه سیاست مشخصی برای نگهداری نداشته باشد، طرف مقابل می‌تواند به آن‌ها ایراد بگیرد و دادگاه نیز در پذیرش آن‌ها محتاط می‌شود.

پنجمین چالش، نقش کارشناسی و خطر «فنی‌زدگی» دادرسی است. دادگاه برای فهم سازوکار امضا ممکن است به کارشناس فناوری اطلاعات متکی شود. اما اگر پرسش‌های کارشناسی دقیق تنظیم نشود یا معیارهای استاندارد وجود نداشته باشد، نظر کارشناسی ممکن است مبهم یا متعارض باشد. همچنین خطر آن وجود دارد که نتیجه دعوا عملاً به زبان فنی تقلیل یابد و جنبه‌های حقوقی مانند قصد، رضایت، یا شروط قراردادی تحت‌الشعاع قرار گیرد.

در جمع‌بندی این بخش می‌توان گفت چالش اثبات انتساب در دعوای خصوصی، به جای تمرکز صرف بر «وجود امضا»، به ارزیابی یک زنجیره کامل نیاز دارد: از احراز هویت اولیه تا امنیت ابزار امضا، از ثبت زمان تا نگهداری داده‌پیام، و از گزارش ممیزی تا امکان ارائه ادله تکمیلی.

بخش چهارم: چالش‌های اثبات تمامیت، زمان‌مندی و زنجیره نگهداری ادله

حتی اگر انتساب امضا احراز شود، دعوا ممکن است بر سر این باشد که آیا متن امضاشده همان متنی است که دادگاه می‌بیند. در فضای دیجیتال، امکان تغییر فایل یا جایگزینی نسخه وجود دارد. بنابراین «تمامیت» به یکی از محورهای اصلی اثبات تبدیل می‌شود.

در امضای مبتنی بر کلید عمومی، تمامیت از طریق پیوند امضا با هش داده‌پیام تضمین می‌شود: هر تغییر در متن موجب می شود امضا معتبرسنجی نشود. اما اگر پرونده با امضای ساده یا روش‌های غیررمزنگاری مواجه باشد، تمامیت باید از راه‌های دیگری اثبات شود؛ مانند سوابق سیستم، نسخه‌های پشتیبان، یا مکاتباتی که متن را تأیید می‌کنند.

زمان‌مندی نیز چالشی مستقل است. بسیاری از اختلافات خصوصی درباره این است که چه زمانی پیشنهاد داده شد، چه زمانی قبول انجام شد، یا چه زمانی امضا صورت گرفت. اگر زمان در سامانه دقیق ثبت نشده باشد، طرفین به قرائن متعارض متوسل می‌شوند. راه‌حل حقوقی و فنی، استفاده از «ثبت زمان معتبر» و اتکا به نهادهای زمان‌سنجی یا سازوکارهایی است که دستکاری زمان را دشوار کند. در غیر این صورت، حتی یک اختلاف جزئی درباره دقیقه یا ساعت می‌تواند آثار مالی قابل توجه داشته باشد.

زنجیره نگهداری ادله دیجیتال، حلقه‌ای است که اغلب نادیده گرفته می‌شود. سند دیجیتال ممکن است از سامانه استخراج، به صورت فایل منتقل، روی حافظه ذخیره، چاپ، یا به دادگاه ارائه شود. در هر مرحله، امکان آسیب یا تغییر وجود دارد. اگر پروتکل مشخصی برای استخراج و نگهداری وجود نداشته باشد، طرف مقابل می‌تواند ادعا کند فایل دستکاری شده یا از منبع نامعلوم آمده است. در چنین وضعی، حتی امضای معتبر نیز ممکن است در عمل کارایی خود را از دست بدهد، زیرا «مسیر انتقال به دادگاه» مبهم است.

در دعاوی خصوصی، یک راهکار عملی این است که طرفین و به‌ویژه کسب‌وکارها، از ابتدا سیاست‌های نگهداری ادله داشته باشند: تولید گزارش‌های غیرقابل تغییر، نگهداری هش

فایل‌ها، ثبت دقیق رویدادها، و امکان ارائه خروجی قابل اعتبارسنجی. اگر این سیاست‌ها وجود داشته باشد، دادگاه با هزینه کمتر به اقناع می‌رسد و اختلافات کاهش می‌یابد.

بخش پنجم: بار اثبات، امارات قضایی و مدیریت تعارض ادله

یکی از حساس‌ترین مباحث، توزیع بار اثبات است. در دعوای خصوصی، اصل بر این است که مدعی باید ادعای خود را ثابت کند. اما در موضوع امضای الکترونیک، اگر یک طرف سند امضاشده و گزارش سامانه را ارائه کند، آیا کافی است یا باید همچنان اثبات مثبتِ انتساب را انجام دهد. پاسخ به این پرسش، به سیاست حقوقی درباره حمایت از امنیت مبادلات و نیز به کیفیت امضا بستگی دارد.

اگر امضا از نوعی باشد که معیارهای امضای مطمئن را تأمین می‌کند و در سامانه‌ای با استانداردهای قابل قبول ایجاد شده، می‌توان گفت یک اماره قوی نسبت به انتساب شکل می‌گیرد. در این صورت، خوانده‌ای که امضا به او منتسب شده، برای رهایی از اثر سند باید ادله‌ای ارائه کند که احتمال سوءاستفاده یا نقص سامانه را نشان دهد. اما اگر امضا ساده باشد یا سامانه قابل اعتماد نباشد، اماره ضعیف می‌شود و خواهان باید با ادله تکمیلی انتساب را تقویت کند.

در تعارض ادله، دادگاه باید به «انسجام روایت» توجه کند. برای نمونه، اگر خوانده امضا را انکار می‌کند اما پس از امضا اقداماتی انجام داده که اجرای قرارداد را تأیید می‌کند، این رفتار می‌تواند اماره‌ای علیه انکار باشد. یا اگر پرداخت‌ها، مکاتبات و تحویل کالا با سند امضاشده هماهنگ است، وزن سند افزایش می‌یابد. برعکس، اگر لاگ‌ها ناقص است یا گواهی در زمان دعوا ابطال شده و توضیحی وجود ندارد، تردید تقویت می‌شود.

نکته مهم آن است که امارات قضایی در محیط دیجیتال باید بر «قرائن قابل آزمون» بنا شود، نه بر برداشت‌های کلی. برای مثال، دادگاه باید بداند که آی‌پی به تنهایی برای انتساب کافی نیست، زیرا امکان استفاده مشترک یا تغییرپذیری وجود دارد. یا پیامک تأیید اگرچه مهم

است، اما در صورت ادعای تعویض سیم‌کارت یا دسترسی غیرمجاز، باید با قرائن دیگر همراه شود. هدف این رویکرد آن است که دادگاه از یک‌سو ساده‌انگارانه به فناوری اعتماد نکند و از سوی دیگر با بدبینی مطلق، تجارت دیجیتال را فلج نسازد.

بخش ششم: تجربه‌های تطبیقی و استانداردهای بین‌المللی در تقویت قابلیت اثبات

مطالعات تطبیقی نشان می‌دهد که بسیاری از نظام‌های حقوقی برای کاهش اختلافات، دو کار انجام داده‌اند. نخست، اصل عدم رد اثر حقوقی امضای الکترونیک به دلیل شکل الکترونیکی را پذیرفته‌اند. دوم، برای برخی انواع امضا، آثار تقویتی ایجاد کرده‌اند؛ یعنی اگر امضا دارای شرایط ویژه باشد، اثر حقوقی آن هم‌سنگ امضای دستی تلقی می‌شود و در عمل با نوعی فرض یا اماره قوی همراه است. در چارچوب‌های منطقه‌ای، امضای واجد شرایط معمولاً بالاترین سطح اطمینان را دارد و در نتیجه در دادگاه نیز با سهولت بیشتری پذیرفته می‌شود .

در سطح اسناد نمونه بین‌المللی، تأکید بر «بی‌طرفی فناوری» نیز دیده می‌شود؛ یعنی قانون نباید صرفاً یک فناوری خاص را تحمیل کند، بلکه باید معیارهای کارکردی برای اعتبار امضا تعیین کند تا فناوری‌های مختلف بتوانند آن معیارها را برآورده کنند. این رویکرد، هم نوآوری را محدود نمی‌کند و هم به دادگاه معیار می‌دهد تا میان روش‌های قوی و ضعیف تمایز بگذارد .

تجربه تطبیقی همچنین نشان می‌دهد که صرف متن قانون کافی نیست و دستورالعمل‌های اجرایی و استانداردهای فنی، نقش تعیین‌کننده دارند. برای مثال، در بسیاری از کشورها، مقررات مربوط به ارائه خدمات اعتماد، ممیزی دوره‌ای، ثبت رخدادها و مدیریت گواهی به‌گونه‌ای تدوین شده که در زمان دعوا، دادگاه بتواند به گزارش‌های استاندارد اتکا کند. این نکته برای دعاوی خصوصی اهمیت ویژه دارد، زیرا بخش عمده اختلافات در سطح روابط قراردادی میان اشخاص رخ می‌دهد و دادگاه نیازمند رویه‌های روشن برای ارزیابی ادله است.

بخش هفتم: راهکارهای حقوقی و فنی برای کاهش چالش‌های اثبات در دعوای خصوصی

برای کاهش چالش‌های اثبات، راهکارها را می‌توان در سه سطح پیشنهاد کرد: سطح قراردادی و کسب‌وکاری، سطح فنی و زیرساختی، و سطح قضایی و آیینی.

در سطح قراردادی، طرفین می‌توانند با درج شروط روشن، اختلافات آینده را کاهش دهند. برای نمونه، می‌توان توافق کرد که امضای انجام‌شده در یک سامانه مشخص به عنوان روش معتبر اعلام اراده شناخته شود، یا فرآیند احراز هویت و روش نگهداری سوابق تعریف گردد. همچنین می‌توان شرط کرد که طرفین در صورت ادعای سوءاستفاده از حساب کاربری، مکلف به اعلام فوری و ارائه دلایل معقول باشند. این شروط، هم از سوءاستفاده احتمالی جلوگیری می‌کند و هم به دادگاه در تشخیص حسن‌نیت و ارزیابی ادله کمک می‌کند.

در سطح فنی، استفاده از امضای مبتنی بر گواهی و زیرساخت کلید عمومی، ثبت زمان معتبر، گزارش‌های ممیزی غیرقابل تغییر، و نگهداری امن سوابق اهمیت دارد. بسیاری از اختلافات ناشی از آن است که سامانه‌ها برای «اثبات‌پذیری» طراحی نشده‌اند؛ یعنی ممکن است تراکنش را انجام دهند اما خروجی استانداردی برای دادگاه تولید نکنند. اگر از ابتدا طراحی سامانه با نگاه حقوقی انجام شود، هزینه دادرسی کاهش می‌یابد.

در سطح قضایی و آیینی، چند اقدام کلیدی قابل تصور است. یکی تدوین دستورالعمل‌های روشن برای پذیرش و ارزیابی ادله دیجیتال است؛ از جمله قالب‌های قابل قبول برای ارائه لاگ‌ها، معیارهای حداقلی برای اعتبار گزارش سامانه‌ها، و قواعد مربوط به زنجیره نگهداری. دوم، تقویت نظام کارشناسی فناوری اطلاعات با استانداردهای دقیق است تا نظر کارشناسی قابل سنجش، قابل پاسخ و قابل مقایسه باشد. سوم، آموزش‌های تخصصی برای قضات و کارکنان قضایی در حوزه مبانی امضای الکترونیک و ادله دیجیتال است تا تصمیم‌ها از وابستگی کامل به کارشناس رها شود و دادگاه بتواند پرسش‌های درست مطرح کند.

راهکار مکمل، استفاده از «امارات مبتنی بر رفتار پسینی» است؛ یعنی دادگاه می‌تواند رفتار طرفین پس از امضا را به عنوان قرینه‌ای برای پذیرش یا رد ادعای انکار بررسی کند. البته این امارات باید با احتیاط به‌کار رود تا حقوق دفاعی طرفین محدود نشود.

نتیجه گیری

امضای الکترونیک، به عنوان یکی از ستون‌های اعتماد در اقتصاد دیجیتال، از نظر حقوقی در بسیاری از نظام‌ها به رسمیت شناخته شده است. با این حال، در دعوای خصوصی، مسئله اصلی اغلب نه پذیرش انتزاعی امضا، بلکه امکان اثبات عملی انتساب، تمامیت و زمان‌مندی است. پژوهش حاضر نشان داد که اعتبار امضای الکترونیک، مفهومی چندلایه است و برای تحقق واقعی آن، باید میان «اعتبار شکلی»، «اعتبار اثباتی» و «اعتماد عملی» پیوند برقرار شود.

چالش‌های اثباتی عمدتاً از تنوع روش‌های امضا، احتمال سوءاستفاده از ابزارهای دیجیتال، ضعف فرایندهای احراز هویت، نبود استانداردهای نگهداری و ارائه ادله، و وابستگی شدید به کارشناسی ناشی می‌شود. در مواجهه با این چالش‌ها، راهبرد مناسب، ترکیبی است: ارتقای زیرساخت‌های فنی، تنظیم قراردادها با نگاه اثبات‌پذیری، و تدوین رویه‌ها و دستورالعمل‌های قضایی برای ارزیابی ادله دیجیتال .در نهایت، اگر هدف حقوق خصوصی حمایت از امنیت و پیش‌بینی‌پذیری روابط باشد، باید امضای الکترونیک را نه به عنوان یک «فایل» یا «نشانه»، بلکه به عنوان بخشی از یک اکوسیستم ادله دید؛ اکوسیستمی که کیفیت آن تعیین می‌کند آیا دادگاه می‌تواند با اطمینان به حقیقت نزدیک شود یا خیر. تقویت این اکوسیستم، هم اعتماد در معاملات را افزایش می‌دهد و هم از تحمیل هزینه‌های سنگین دادرسی بر اشخاص جلوگیری می‌کند.

منابع و مآخذ

الف) منابع فارسی

- قانون تجارت الکترونیکی، مصوب ۱۳۸۲، مجلس شورای اسلامی .
- غلیزاده، احد. تحلیلی بر اعتبار امضاء در حقوق تجارت الکترونیکی. فصلنامه حقوقی دانشکده حقوق و علوم سیاسی دانشگاه تهران، سال ۱۳۹۱ .
- صفایی، سیدحسین. ادله اثبات دعوا در حقوق مدنی. تهران: نشر میزان.
- کاتوزیان، ناصر. قواعد عمومی قراردادها. تهران: شرکت سهامی انتشار.
- جعفری لنگرودی، محمدجعفر. ترمینولوژی حقوق. تهران: گنج دانش، چاپ‌های مختلف.
- شمس، عبدالله. آیین دادرسی مدنی. تهران: دراک، چاپ‌های مختلف.

ب) منابع انگلیسی

- *European Parliament and Council. Regulation (EU) No ۹۱۰/۲۰۱٤ on electronic identification and trust services for electronic transactions in the internal market (eIDAS), Article ۲٥.*
- *UNCITRAL. Model Law on Electronic Signatures (۲۰۰۱), United Nations Commission on International Trade Law.*
- *Alizadeh, (author name as cited in journal source). Electronic Signatures in Iran. Digital Evidence and Electronic Signature Law Review, Institute of Advanced Legal Studies, University of London.*