مقاله پژوهشی/ دوره ۸۹/ شماره ۱۳۲/ صفحات: ٤٨٦-٤٥٥
تاریخ دریافت: ١٤٠٤/٠٢/٠٤ تاریخ پذیرش: ١٤٠٤/٠٤/١٧

چالش‌های حقوقی قراردادهای الکترونیکی در تجارت بین‌الملل

محمد طاعتی سرشکه[1]

چکیده

قراردادهای الکترونیکـــی به عنوان پدیده‌ای نوین در تجارت بین‌الملل، ضمن ارائه مزایایی از قبیل ســـرعت، دقت فنی و صرفه‌جویی اقتصادی، چالش‌های حقوقی بی‌ســـابقه‌ای در چهار حوزه کلیدی شامل اعتبارسنجی طرفین، تعارض قوانین، حریم خصوصی و اجرای احکام فرامرزی پدیدار ساخته‌اند. پژوهش حاضر با روش توصیفی تحلیلی و بررسی اسناد بین‌المللی، چهار چالش اصلی شامل تعیین قانون حاکم، احراز هویت دیجیتال،تعارض با مقررات حفاظت داده‌ها و دشـــواری اجرای آرای و احکام بین‌المللی را شناسایی نموده است. راهکارهای پیشنهادی در دو سطح بین‌المللی شامل الحاق به کنوانسیون‌های هماهنگ‌ســـاز، توسعه داوری الکترونیکی و استانداردسازی امضاهای دیجیتال؛ و ســـطح ملی شـــامل بازنگری قانون تجارت الکترونیکی مصوب ۱۳۸۲، ایجاد نهاد ناظر مستقل و تقویت زیرساخت‌های امنیتی احراز هویت ارائه شده اســـت. یافته کلی آن اســـت که نظام حقوقی این قراردادها نیازمند تلفیق هوشمندانه اصول سنتی با فناوری‌های نوین است تا تعادلی میان کارایی تجاری و امنیت حقوقی ایجاد شود، امری که مســـتلزم همکاری بین‌المللی، نوسازی چارچوب‌های داخلی و توانمندسازی بازیگران این عرصه می‌باشد.

واژگان کلیدی: قرارداد الکترونیکی، تجارت بین‌الملل، تعارض قوانین، امضای دیجیتال، حریم خصوصی.

---

۱. کارشناس ارشد حقوق خصوصی lawyer.taati@gmail.com

درآمد

در حقوق تجارت بین‌الملل، قراردادهای الکترونیکی تیغی دولبه‌اند: گشـــاینده باب مبادلات جهانی و زاینده چالش‌های حقوقی نوظهور. ماهیت فرامرزی و ســـیال این نهاد، بنیان‌های ســـنتی قراردادی را به چالش می‌کشـــد. انقلاب دیجیتال سرشت معاملات را دگرگون ســـاخته، و ظهور مفاهیمی چون قرارداد هوشـــمند و بلاکچین، پرسش‌هایی بنیادین درباره اراده، رضایت و حاکمیت قانون را برمی‌انگیزد که مستلزم انگاره‌های حقوقی بدیع است.

قرارداد الکترونیکی در ســـاده‌ترین تعریف، توافقی الزام‌آور است که با استفاده از ابزارهای الکترونیکی نظیر ایمیل، وب‌ســـایت یا سامانه‌های تجارت الکترونیکی و در فضای ســـایبرمیان طرفین صورت می‌گیرد. قانون نمونه[1] به‌طور مستقیم تعریفی از قـــرارداد الکترونیکی ارائه نداده، لیکن با مراجعه به متن اصلی قانون نمونه، می‌بینم که در بنـــد الف ماده ۲ به تعریف داده‌پیام پرداخته که این دقیقاً همان مفهومی اســـت که در نقل قول فوق به ابزارهای الکترونیکی اشـــاره دارد و در ماده ۱۱ به صراحت بیان می‌کندکه «در تشـــکیل قرارداد، اســـتفاده از داده‌پیام برای بیان ایجاب و قبول، موجب بی‌اعتباری یا عدم قابلیت اجرای قرارداد نخواهد شد» که مبنای حقوقی الزام‌آور بودن قراردادهای الکترونیکی را تأیید می‌کند. این قرار دادها ممکن است به شکل هوشمند نیز باشند. تفاوت اساسی آن با قراردادهای سنتی، نه در ماهیت حقوقی، بلکه در نحوه شکل‌گیری، اثبات، امضا و اجراست؛ این ذات دیجیتال، منازعات حقوقی و تفسیرهای گوناگون را درپی داشته است.

این پژوهش موانع حقوقی اجرای قراردادهای الکترونیکی و پاســـخ نظام‌های ملـــی و بین‌المللی را با رویکردی متوازن میان ســـنت و نـــوآوری در حقوق دیجیتال بررســـی می‌کند. هرچند قراردادهای الکترونیکی با افزایش دقت و سرعت، اقتصاد را متحـــول کرده‌اند، اما مفاهیم پایه‌ای حقوقی چـــون حاکمیت قانون، رضایت و اهلیت را با چالش‌های بنیادین مواجه ســـاخته‌اند. فرامرزی بودن ذاتی این قراردادها، تطبیق نظام‌های ملی با چارچوب جهانی را به مســـئله‌ای پیچیده تبدیل نموده است. حل این چالش‌ها نیازمند پژوهش حقوقی عمیق و طراحی سازِکارهای هوشمندانه برای ایجاد

1. Model Law on Electronic Commerce (UNCITRAL) 1996

تعادل پویا میان انعطاف‌پذیری دیجیتال و ثبات حقوقی است.

حاکمیت قانون در فضای سایبری مبتنی بر ارتباط ذاتی میان کنش‌های حقوقی و ساختارهای حکمرانی (نه مرزهای جغرافیایی) است. این ارتباط با سه شاخص راهبردی محدوده ارائه خدمات دیجیتال، پیشینه تعهدات حقوقی و ابراز اراده آگاهانه در چارچوب نظم عمومی و اخلاق تعیین می‌شود. هم‌زمان حرکت حقوق معاصر به سمت حکم‌رانی چندسطحی، ایجاد دیالوگ پویا میان نظام‌های داخلی و فراملی را برای طراحی الگوهای چابک فضای مجازی الزامی می‌کند. در این مسیر، عدالت سایبری نیازمند بازتعریف پویای مفاهیم بنیادین از جمله رضایت است که باید از طریق شفافیت گام‌به‌گام، فرصت بازنگری و مکانیسم‌های تضمینی غیرقابل تخطی، اصالت و اختیاری بودن آن را محقق ساخت. در سطح جهانی، هماهنگی حقوقی مبتنی بر اسنادی مانند قواعد لاهه و آنسیترال از تعارضات می‌کاهد، و الگوهایی نظیر «مقررات عمومی حفاظت از داده‌ها[1]» توازنی میان منافع تجارت و مصرف‌کننده ایجاد می‌کنند.

نظام‌های حقوقی با تصویب قوانین اختصاصی مثل قانون نمونه آنسیترال، استانداردسازی فنی «مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد[2]» و همکاری‌های قضایی «کنفرانس لاهه حقوق بین‌الملل خصوصی[3]» به اصلاح ساختاری روی آورده لیکن اثربخشی راهکارها منوط به هماهنگی بین‌المللی و انطباق با چارچوب‌هایی مانند «مقررات عمومی حفاظت از داده‌ها» است. همچنین این نظام‌ها با بهره‌گیری از «تکامل قانونی» و «هم‌گرایی بین‌المللی»، درصدد پاسخ‌گویی به چالش‌های نوظهور هستند. این رویکرد هم بر توسعه قوانین داخلی و هم بر

---

1. General Data Protection Regulation

چارچوب پیشگام حفاظت از داده‌های شخصی در اتحادیه اروپا که در سال ۲۰۱۶ تصویب و از سال ۲۰۱۸ اجرایی شد. این مقررات استانداردهای جهانی حریم خصوصی را ارتقاء بخشید.

2. electronic Identification, Authentication and trust Services (Eidas)

این ابزار حقوقی‌فنی، با ایجاد استانداردهای فرامرزی برای امضای الکترونیکی، مهر دیجیتال و سایر خدمات اعتماد، درصدد تضمین اعتبار و پذیرش متقابل ادله الکترونیکی در روابط قراردادی و دادرسی‌های خصوصی میان کشورهای عضو است.

3. Hague Conference on Private International Law (HCCH)

این سازمان بین‌الدولی نهاد تدوین‌گر کنوانسیون‌های چندگانه‌ای (مانند کنوانسیون ابلاغ و استناد) با هدف ایجاد هماهنگی و همکاری قضایی میان نظام‌های حقوقی ملی است.

همکاری‌های فراملی تأکید دارد.

پژوهش‌های متأخر در حوزه حقوق قراردادهای الکترونیکی، با رویکردی تحلیلی-تطبیقی، مؤید ضرورت تلفیق اصول سنتی حقوقی با الزامات عصر دیجیتال است. مطالعاتی چون تحقیق اکبرینه و محمدزاده در کنگره بین‌المللی حقوق اسلامی و علوم انسانی (تهران، ۱۳۹۵) بر مقایسه نظام‌مند شرایط اعتبار قراردادهای سنتی و دیجیتال تأکید دارد، درحالی که صاحب‌اختیاری در چهاردهمین کنفرانس بین‌المللی پژوهش‌های مدیریت و علوم انسانی ماهیت این قراردادها را در تجارت بین‌الملل، تلفیقی هوشمندانه از سنت و مدرنیته می‌داند. دره‌شامی در پایان‌نامه خویش با عنوان «شرایط اعتبار قرارداد الکترونیکی» نشان می‌دهد که اعتبار قراردادهای الکترونیکی علاوه بر شروط خاص (مثل داده‌پیام معتبر)، وابسته به شرایط عمومی صحت معامله است و نظریه وصول را به عنوان معیار غالب انعقاد قرارداد می‌پذیرد. از سوی دیگر، طغیانی‌پور در پژوهش انعقاد عقد در فضای سایبری (همایش ملی علوم انسانی، آستارا) با استناد به اصل بی‌طرفی فنی، لزوم طراحی سازِکارهای امنیتی ویژه و به‌روزرسانی قوانین ملی برای توازن میان کارایی تجارت الکترونیک و حمایت از حقوق ضعفا را یادآور می‌شود. در حوزه قراردادهای هوشمند، مطالعه دهقانی تفتی و همکاران با عنوان مطالعه تطبیقی قانون حاکم بر قراردادهای هوشمند دیجیتال در حقوق بین‌الملل خصوصی ایران و مقررات رم، بیان می‌گردد که تعیین قانون حاکم، به‌رغم محوریت اراده طرفین، با چالش‌هایی نظیر پراکندگی جغرافیایی و ناشناسی مواجه است و راهکارهایی چون تصریح قانون حاکم در کد قرارداد را پیشنهاد می‌کند.

سیر تحول این پژوهش‌ها حاکی از گذار از مباحث اولیه (اعتبار امضای دیجیتال) به مسائل پیچیده‌تر مانند مسؤولیت پلتفرم‌ها، نقش هوش مصنوعی و حل اختلافات الکترونیکی است که در نهایت، تعامل سازنده بین نوآوری‌های فناورانه و ثبات نظام‌های حقوقی را به‌عنوان کلید پویایی این عرصه معرفی می‌کنند

یافته‌های این پژوهش که با روش توصیفی تحلیلی انجام شده است نشان می‌دهد که ویژگی‌هایی مانند غیر حضوری بودن، ماهیت فناورانه و تعدد نظام‌های حقوقی، منجر به ابهام در اراده طرفین، ناهماهنگی در اعتبارسنجی

اسناد دیجیتال و ناکارآمدی قواعد سنتی حل تعارض شده‌اند. مطالعه تطبیقی حاکی از ناسازگاری مفاهیم حقوقی مکان‌محور (صلاحیت قضایی و قانون حاکم) با فضای سایبر است که اطمینان تجاری را کاهش داده، اجرای قراردادها را تضعیف کرده و هزینه‌های معاملاتی را افزایش داده است. این پژوهش با تأکید بر ضرورت بازنگری مبانی حقوقی، راهکارهای تقنینی متناسب با محیط دیجیتال را پیشنهاد می‌دهد.

ساختار پژوهش حاضر در شش مرحله اصلی تنظیم گردیده و هر مرحله با توجه به پیوند درونی موضوعات و ضرورتِ حرکت از مفاهیم بنیادین به سوی راهکارهای عینی طراحی شده است. پس از درآمدی که به تشریح مسأله، مرور ادبیات نظری و ترسیم چهارچوب مفهومی اختصاص دارد، نخستین گام به ارکانِ تشکیل‌دهنده قراردادهای الکترونیکی معطوف می‌شود و با تأکید بر دو محورِ «اهلیت» و «اعلام اراده»، چالش‌های مقدماتیِ این حوزه را وامی‌کاود. در گام دوم، با اتخاذ رویکردی تطبیقی که در قلمرو حقوق خصوصی از دیرباز روشی کارآمد برای کشف نقاط قوت و ضعف نظام‌های ملی بوده است ساختارهای اعتماد دیجیتال و وضعیتِ عملیِ پذیرشِ امضای الکترونیکی در سه زیست‌بومِ حقوقیِ ایران، ایالات متحده و اتحادیه اروپا مورد سنجش قرار می‌گیرد و خلأهای تقنینی و موانع اجرایی برجسته می‌شود. سومین بخش، کوششی است برای دسته‌بندیِ نظام‌مندِ چالش‌های حقوقی در سه لایه ماهوی، شکلی‌اثباتی و اجرایی؛ در این میان با دقت در مسائلی چون تعیین قانون حاکم بر قراردادهای فرامرزی، مسؤولیت واسطه‌های فنی، حفظ حریم خصوصی داده‌ها و چگونگیِ اجرای احکام خارجی، ماهیت چندبعدیِ موانع پیشِ روی تجارت الکترونیک آشکار می‌شود. در ادامه، بخش چهارم بر راهکارهای تلفیقیِ حقوقی‌فنی متمرکز می‌شود و با محوریتِ هماهنگ‌سازیِ قوانین ملی با اسناد بین‌المللی، بهره‌گیری از فناوری‌های نوظهور (از جمله قراردادهای هوشمند) و تقویت سازکارهای تخصصیِ حل و فصل اختلاف، پیشنهادهایی عملیاتی عرضه می‌کند. بخش پنجم با رویکردی تطبیقی و عمیق‌تر، به مقایسه نظام‌های سه‌گانه (اتحادیه اروپا، ایالات متحده و ایران) می‌پردازد و نقاط قوت و ضعف هر یک را در مواجهه با بازار دیجیتال فراملی برمی‌شمارد. نهایتاً در ششمین بخش، چالش‌های کلیدی و

خلأهای تقنینی ایران به صورت راهبردی احصاء شده و در پرتو یافته‌های تطبیقی، به منظور اصلاح قانون تجارت الکترونیک، تقویت نهادهای ناظر و ارتقاء زیرساخت‌های حقوقی پیشنهادهایی ارائه می‌شود. این ساختار که از توصیف مبانی به تحلیل تطبیقی چالش‌ها و سپس تدوین راهبردهای عملی سیر می‌کند، در تکاپوی ترسیم نقشه‌راهی منسجم برای ایجاد تعادل میان کارایی تجاری و امنیت حقوقی در عرصه قراردادهای الکترونیکی فراملی است.

۱. ارکان تشکیل‌دهنده قرارداد الکترونیکی

بر اساس اصول حقوق قراردادها، ارکان اساسی تشکیل قرارداد الکترونیکی شامل ایجاب، قبول، اهلیت، موضوع معین، و مشروعیت جهت است. در قلمرو الکترونیک، ایجاب و قبول به سادگی یک کلیک یا پیام تحقق می‌یابد، بی‌آن‌که از ارزش حقوقی آن بکاهد. قانون این شیوه نوین را به رسمیت شناخته و بر آن مهر تأیید زده است؛ همان‌طور که در بند اول ماده ۱۱ قانون نمونه آنسیترال ۱۹۹۶ آمده است[1]. آنچه مهم‌تر می‌نماید، تعیین زمان و مکان این گفت‌وگوی دیجیتال است که همچون قطب‌نمایی، مسیر حل اختلاف را روشن می‌سازد. در این عصر، گاه یک کلیک ناچیز، بار سنگین تعهد را بر دوش می‌نهد!

در مورد شرط اهلیت، با این حال، در قراردادهای الکترونیکی، احراز هویت دیجیتال (مانند امضای الکترونیکی یا سیستم‌های شناسایی دو مرحله‌ای) نقش کلیدی دارد که اعتبار آن تابع مقررات ملی است. چالش اصلی در اینجا احراز هویت و سن طرفین در فضای مجازی است.

موضوع قرارداد الکترونیکی نیز باید معین، مشروع و قابل اجرا باشد. چالش‌های این حوزه شامل ارائه خدمات غیرقانونی آنلاین یا معاملات دارایی‌های مجازی فاقد پشتوانه (مانند برخی NFT ها) است که ممکن است به بطلان قرارداد بینجامد. (Murray, 2018, p. 95) در برخی نظام‌ها مانند حقوق ایران، معاملات الکترونیکی

1. UNCITRAL Model Law on Electronic Commerce 1996: In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

مرتبط با کالاهای غیرقانونی (مانند قمار آنلاین) باطل هستند.

همچنین امضای دیجیتال به‌عنوان مکانیسم محوری اعتبارسنجی قراردادهای الکترونیکی، نقش بنیادین در شناسایی اراده دارد. به‌رغم پذیرش گسترده دولتی، تعاریف، اعتبار حقوقی و زیرساخت‌های آن در نظام‌های ملی متفاوت است. قانون نمونه آنسیترال (۲۰۰۱) آن را داده‌ای مرتبط با سند برای شناسایی امضاکننده و تأیید محتوا تعریف می‌کند. مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد اتحادیه اروپا (۲۰۱٤) سطوح ساده[1]، پیشرفته[2] و کیفی[3] را شناسایی نموده که تنها سطح کیفی معادل امضای دست‌نویس است.

در حقوق ایران، قانون تجارت الکترونیکی (۱۳۸۲) امضای الکترونیکی مطمئن را با شروط مشخص معتبر می‌داند، لیکن شکاف اجرایی با استانداردهای جهانی چالش‌زاست. به‌عنوان نمونه، در ایالات متحده کلیک بر دکمه قبول می‌تواند به‌عنوان امضای معتبر شناخته شود، اما در اروپا تنها امضای کیفی با گواهی‌نامه رسمی قابلیت پذیرش بدون اثبات اضافی دارد[4].

۲. تحلیل تطبیقی امضای الکترونیکی در ایران، آمریکا و اتحادیه اروپا

امضای الکترونیکی، به‌عنوان بازتابی از تحول حقوق در مواجهه با فناوری، هم‌زمان هم میراث‌دار اصالت امضای سنتی است و هم پاسخ‌گوی نیازهای نوین تجاری و اداری. در سطح بین‌المللی[5] و اروپایی «مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد»[6]، این نهاد حقوقی با سطوح مختلف اعتبار تنظیم شده، حال آن‌که در حقوق ایران و قانون تجارت الکترونیکی ۱۳۸۲، اگرچه به ظرفیت‌های آن اذعان شده، چالش‌های اجرایی و اعتباری، گذار کامل به این ابزار اعتماد دیجیتال را کند کرده است. این تقابل، فرصتی برای بازاندیشی در تعادل میان امنیت حقوقی و کارآمدی فناورانه است.

1. Simple Electronic Signature (SES)
2. Advanced Electronic Signature (AES)
3. Qualified Electronic Signature (QES)
4. eIDAS, Art. 25(2)
5. UNCITRAL, 2001
6. eIDAS, 2014

۱-۲. ساختارهای اعتماد دیجیتال

در ایران مرکز توسعه تجارت الکترونیکی به عنوان مرجع صدور گواهی ریشه[1] شناخته می‌شود و زیرساخت امضای دیجیتال از طریق مراکز میانی مانند وزارت صنعت فعال است؛ هرچند پذیرش عملی آن با چالش‌هایی روبه‌روست (مرکز توسعه تجارت الکترونیکی، ۱۴۰۲). در مقابل، در آمریکا شرکت‌هایی مانند ادوبی ساین[2] و داکیوساین[3] با رعایت استانداردهای امنیتی، اعتماد نظام قضایی را جلب کرده‌اند (Murray, 2018, p. 102). اروپا نیز با تعیین فهرست نهادهای معتبر (Trusted List) بر اساس «مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد» تنها گواهی‌های صادرشده از این مراکز را در محاکم معتبر می‌داند. در نهایت، اعتماد دیجیتال تنها با زیرساخت‌های شفاف و پذیرش اجتماعی تحقق می‌یابد.

گواهی ریشه به عنوان عالی‌ترین مرجع اعتماد در سلسله‌مراتب زیرساخت کلید عمومی[4]، مبنا و ضامن حقوقی اعتبار تمامی گواهی‌های صادره در زنجیره اعتماد است. این گواهی که توسط مرجع ریشه صادر می‌شود، با نصب پیش‌فرض در سیستم‌عامل‌ها و مرورگرها، از طریق امضای دیجیتال خود، پایه اعتبارسنجی و انکارناپذیری گواهی‌های زیرمجموعه را ایجاد می‌کند. هرگونه اختلال در تمامیت آن، زنجیره اعتماد را به طور کامل مخدوش و ارزش حقوقی امضاهای مرتبط را باطل می‌سازد. مراجع ملی نظیر مرکز توسعه تجارت الکترونیک ایران، نهادهایی چون مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد» در اتحادیه اروپا و مراجعی چون دیجی سرت[5] تضمین اعتماد دیجیتال در گرو هم‌پیوندی

---

1. Root Certificate
2. Adobe Sign (part of Adobe Document Cloud, an electronic signature solution)
«ادوبی ساین»، خدمت امضای الکترونیکی ابری متعلق به شرکت ادوبی
3. Docusign, Inc. (a cloud-based electronic signature and digital transaction management platform)
برگردان فارسی«داکیوساین»، شرکت ارائه‌دهنده خدمات امضای الکترونیکی و مدیریت تراکنش‌های دیجیتال
4. Public Key Infrastructure (PKI)
5. DigiCert, Inc. (A Global Root Certificate Authority and Qualified Trust Service Provider)

الزامات فنی)زیرساخت کلید عمـومی امن)، حقـوقی (چارچوب‌های نظارتی شفاف) و اجتماعی‌قضایی (پذیرش کاربران و مراجع دادرســـی) است؛ لـــذا گواهی ریشه نه صرفاً یک ابزار فنی، بلکه ســـنگ بنای حاکمیت قانون در فضای ســـایبر محسوب می‌شود.

۲-۲. رویه قضایی و پذیرش عملی

در حقوق ایـــران، امضای الکترونیکی هرچند به صورت قانونی به رســـمیت شناخته شده، اما رویه قضایی در پذیرش عملی آن محتاطانه عمل می‌کند؛ حال آن‌که در نظـــام حقوقی آمریکا تأکید بر معیارهای شـــکلی مانند «رضایت» و «رفتار متقابل» مانند کلیک یا امضای دیجیتال حتی بدون الزامات فنی پیچیده، اعتبار حقوقی اســـناد الکترونیکـــی را تضمین می‌کنـــد (Kerr, 2019: 72) در اتحادیـــه اروپا با رویکردی سلســـله‌مراتبی، تنها امضای الکترونیکی پیشرفته واجد شرایط امضای کیفی را دارای اعتبار کامل دانســـته و ســـایر انواع امضا را مشـــروط به ارائه دلایل تکمیلی می‌داند[1] ایـــن تفاوت‌های نظری و عملی، گویای چالش‌هـــای تقنینی و اجرایی در به‌کارگیری فناوری‌های نوین در عرصه حقوق است.

در نظام‌هـــای حقوقی مبتنی بر قانون مدنی مانند ایران، دادرس در ارزیابی ادله الکترونیکی اختیار بیشـــتری دارد، در حالی که در نظام‌هـــای کامن‌لا (مانند آمریکا)، استانداردهای مشخصی مانند قانون یکنواخت معاملات الکترونیکی» مصوب در سطح ایالتی حاکم است.

۳. تحلیل چالش‌های حقوقی در قراردادهای الکترونیکی

نخســـت، چالش‌های ماهوی که ناظر بر اعتبار ذاتی قرارداد اســـت: تردید در جایگاه اسناد دیجیتال در قیاس با اسناد مکتوب و عدم پذیرش اصل برابری عملکردی در برخی نظام‌های ملی؛ تعارض قوانین در تعیین قانون حاکم و دادگاه صالح به‌واسطه ماهیـــت فرامرزی و فقدان مکان فیزیکی؛ و دشـــواری تعیین حدود مســـؤولیت میان طرفیـــن، ارائه‌دهندگان خدمات میزبانی و واســـطه‌های فنی در فرض نقض امنیت یا اختلال سامانه‌ای.

دوم، چالش‌های شـــکلی و اثباتی که به قابلیت اســـتناد مربوط می‌شود: تردید

1. eIDAS, Recital 49

در پذیـــرش ادله الکترونیکی به دلیل نگرانـــی از جعل و فقدان امضای کیفی؛ الزام به انطبـــاق با مقـــررات فراملی حفاظت از داده‌ها همچون مقـــررات عمومی حفاظت از داده‌ها و مخاطره بطلان یا مســـؤولیت مدنی ناشی از تخلف؛ و تهدید امنیت سایبری ناشـــی از جعل هویت و تحریف داده‌ها که مستلزم چارچوب حقوقی حمایتی برای فناوری‌هایی نظیر امضای پیشرفته و بلاک‌چین است.

ســـوم، چالش‌های اجرایی که تحقق عینی تعهدات را هدف می‌گیرد: تشـــدید موانع شناســـایی و اجرای احـــکام خارجی به‌دلیل ماهیت غیرمتمرکز فضای ســـایبر؛ محدودیت‌های پرداخت الکترونیکی ناشـــی از تحریم‌ها، کنترل‌های ارزی الگوریتمی و ناهمگونی زیرســـاخت‌های بانکداری دیجیتال؛ و تبلور پیچیده‌تر موانع کلاســـیک اجرا (همچون اعتبار اســـناد دیجیتال نزد دادگاه خارجی) که مجموعاً ضرورت تحلیل افتراقی این حوزه را اجتناب‌ناپذیر می‌سازد

۱-۳. چالش‌های ماهوی

۱-۱-۳. اعتبار قراردادهای الکترونیکی

تعیین جایگاه اســـناد دیجیتال در مقایسه با اسناد مکتوب، از نخستین مباحثی اســـت که در عرصه حقوق فناوری اطلاعات مطرح می‌شـــود. هرچند اصل «برابری عملکردی» در اســـناد بین‌المللی نظیر قانون نمونه آنسیترال[1] به رسمیت شناخته شده، لکـــن برخی نظام‌های حقوقی با احتیاط و تأنی، شـــمول ادله الکترونیکی را در اثبات قراردادها می‌پذیرند (Reed, 2018: 94).

تعیین جایگاه اسناد دیجیتال در قیاس با اسناد مکتوب، از مباحث پایه‌ای حقوق فناوری اطلاعات محسوب می‌شـــود. به‌رغم پذیرش جهانی اصل برابری عملکردی[2] در اســـناد بین‌المللی (ماده ٦ قانون نمونه آنسیترال تجارت الکترونیک ١٩٩٦)، برخی نظام‌های حقوقی ملی با تفسیر مضیقِ شرط کتبی‌بودن، اعتبار اسناد دیجیتال را تضعیف و موجـــد عدم قطعیت حقوقی در تجارت بین‌الملل شـــده‌اند. برای نمونه، در پاره‌ای کشورها اسناد الکترونیکی فاقد امضای دیجیتال پیشرفته یا همان امضای کیفی ممکن اســـت فاقد قابلیت اســـتناد قضایی تلقی شـــوند (Reed, 2018: 94) راهکار کلیدی،

1. UNCITRAL, 1996, Art. 6
2. Functional Equivalence

تصویب قوانین ملی هم‌سو با مدل آنسیترال ۱۹۹۶ است که به صراحت اعتبار حقوقی داده‌پیام و امضای الکترونیک را به مثابه اسناد مکتوب به رسمیت می‌شناسد. افزون بر این، طرفین قرارداد می‌توانند با اشتراط صریح امضای دیجیتال پیشرفته در متن توافق‌نامه، قابلیت اثبات‌پذیری اسناد را ارتقا دهند.

۲-۱-۳. تعیین قانون حاکم و صلاحیت قضایی

قراردادهای الکترونیکی با ماهیت فرامرزی، به دلیل اختلاف در ملاک‌های صلاحیت مانند محل سرور، اقامتگاه طرفین یا مرکز ثقل تعهدات، همواره با تعارض قوانین مواجه‌اند. هر چند اصل حاکمیت اراده در تعیین قانون حاکم به صورت جهانی پذیرفته شده، اما در صورت سکوت طرفین، تشخیص مرجع و قانون صلاحیت‌دار به چالشی پیچیده تبدیل می‌شود که اختلاف دیدگاه‌های دولت‌ها بر دشواری آن می‌افزاید (Kuner, 2020: 151).

ماهیت فرامرزی قراردادهای الکترونیکی، تعارض قوانین را در تعیین صلاحیت دادگاه و قانون حاکم تشدید می‌کند. معیارهای متعارضی مانند محل سرور، اقامتگاه طرفین، یا مرکز ثقل تعهدات، منجر به عدم پیش‌بینی‌پذیری حقوقی می‌گردد. حتی با پذیرش اصل حاکمیت اراده، در صورت سکوت قرارداد، اختلاف دیدگاه‌های دولت‌ها در تعیین مرجع صالح، چالشی ساختاری ایجاد می‌نماید (Kuner, 2020: 151; Kohl, 2007: 45). راهکار عملی در اینجا گنجاندن شرط انتخاب قانون و شرط صلاحیت انحصاری دادگاه در متن قرارداد است.

۳-۱-۳. مسؤولیت ناشی از نقض قرارداد

قراردادهای الکترونیکی با چالش‌های متعددی از جمله اختلال در عملکرد سامانه‌ها، نقض امنیت داده‌ها و سوءاستفاده‌های الکترونیکی مواجه هستند. تعیین حدود مسؤولیت حقوقی میان اصحاب قرارداد، ارائه دهندگان خدمات میزبانی و سایر واسطه‌های فنی، مستلزم بررسی عمیق مبانی حقوقی از جمله تقصیر قراردادی، معیارهای احتیاط متعارف و مکانیسم‌های توزیع خطر می‌باشد (Rowe, 2022: 57).

چالش ماهویِ تعیین مسؤولیت حقوقی میان اصحاب قرارداد، ارائه‌دهندگان

خدمات میزبانی[1] و تسهیل‌گران فنی[2] در موارد نقض امنیت داده‌ها یا اختلال سامانه‌ها، نیازمند واکاوی مبانی حقوقی معیار مسؤولیت (تقصیر قراردادی در مقابل مسؤولیت مطلق) است. پیچیدگی این امر با فقدان چارچوب‌های بین‌المللیِ توزیع خطر[3] در فضای سایبر تشدید می‌شود (Rowe, 2022: 57).

راهکار کاربردی قابل ارائه، تعیین شفاف حوزه مسؤولیت هر ذی‌نفع در قراردادها، همراه با شروط محدودکننده جبران خسارت[4] و به‌کارگیری بیمه‌های مسؤولیت سایبری[5] به عنوان مکانیسم انتقال خطر، رویکردی کارآمد برای مدیریت این چالش است.

۲-۳. چالش‌های شکلی و اثباتی

۱-۲-۳. ادله الکترونیکی و قابلیت استناد

پذیرش ادله الکترونیکی در نظام‌های حقوقی با چالش‌هایی روبه‌روست؛ در حالی که اسناد دیجیتال در چارچوب اصل بی‌طرفی فناورانه و با احراز اصالت، تمامیت و قابلیت پی‌گیری معتبر شناخته می‌شود[6]، برخی نظام‌ها همچنان به اسناد مکتوب اولویت می‌دهند (Greenleaf & Waters, 2019: 202) یا به دلیل نگرانی از جعل، با احتیاط بیشتری آن‌ها را می‌پذیرند (Reed, 2010: 67).

۲-۲-۳. حریم خصوصی و مقررات بین‌المللی

تطبیق قراردادهای الکترونیکی با استانداردهای نظارتی همچون «مقررات عمومی حفاظت از داده‌ها» در اتحادیه اروپابه‌ویژه در حوزه‌های رضایت آگاهانه، تعیین صریح اهداف پردازش داده‌ها و انتقال فرامرزی آن‌ها، امری ضروری تلقی می‌شود. این مقررات با وضع الزامات سخت‌گیرانه در خصوص جریان داده‌های شخصی به خارج از قلمرو اتحادیه (ماده ٤٤)، چارچوبی انضباطی ایجاد نموده‌اند. تخطی از این موازنه می‌تواند به بطلان قرارداد یا استقرار مسؤولیت مدنی منجر شود (Voigt & Von dem Bussche, 2017: 65–67).

---

1. Hosting Providers
2. Intermediaries
3. Risk Allocation
4. Liability Limitation Clauses
5. Cyber Liability Insurance
6. UNCITRAL, 1996, Art. 9

۳-۲-۳. امنیت سایبری و خطر جعل داده‌ها

جعل هویت در فضای دیجیتال، تحریف داده‌ها و تهاجمات سایبری، تهدیداتی ملموس در مسیر اعتمادسازی نسبت به فرآیند تشکیل قراردادها محسوب می‌گردند. اگرچه فناوری‌های نوینی نظیر امضای الکترونیک پیشرفته و فناوری بلاک‌چین[1] قابلیت کاهش این مخاطرات را دارا می‌باشند، لکن کارایی مطلوب آنها منوط به وجود چارچوب حقوقی حمایتی است (Clack et al., 2016: 28). از جمله راهکارهای نوین جهت تضمین اصالت و تمامیت داده‌ها در قراردادهای الکترونیکی، بهره‌گیری از فناوری بلاک‌چین است که با ویژگی‌های ذاتی مانند تغییرناپذیری[2]، شفافیت کنترل‌شده و رهگیری پذیری[3] می‌تواند سازِکاری امن برای انطباق با استانداردهای حفاظت داده‌ها فراهم نماید. همچنین تلفیق این فناوری با مکانیسم‌های حقوقی مانند موافقت‌نامه‌های محرمانگی[4] و شرایط اختصاصی حفاظت از داده‌ها[5] می‌تواند چارچوبی جامع برای مدیریت امن اطلاعات محرمانه در فرایندهای قراردادی ایجاد کند.

۳-۳. چالش‌های اجرایی

ممکن است این پرسش مطرح شود که چالش‌های اجرایی عام بوده و مختص قراردادهای الکترونیکی نیستند؛ پس پرداختن به آن در این پژوهش ضرورتی ندارد، اما درج بخش «چالش‌های اجرایی» نه تنها ضروری است، بلکه حذف آن به بهانه عمومیتِ برخی موانع، با رویکرد نظام‌مند به حقوق تجارت الکترونیک بین‌الملل مغایرت خواهد داشت. این ضرورت را می‌توان در سه محور کلیدی توجیه کرد.

۱-۳-۳. ذات فرامرزی تجارت الکترونیک و تشدید موانع اجرا

تجارت الکترونیک به دلیل ماهیت غیرمتمرکز و عبور از مرزهای فیزیکی، چالش‌های اجرایی سنتی را در قالبی نو و پیچیده بازتولید می‌کند. به‌رغم کاربرد «کنوانسیون شناسایی و اجرای آرای داوری خارجی» (نیویورک، ۱۹۵۸)[6] در اجرای

1. Blockchain
2. Immutability
3. Traceability
4. Non-Disclosure Agreement (NDA)
5. Data Protection Clauses
6. Convention on the Recognition and Enforcement of Foreign Arbitral Awards

آرای داوری، تعیین «دادگاه صالح» و «قانون حاکم» در فضای سایبری که فاقد مکان انضمامی انعقاد قرارداد است به عاملی تعیین‌کننده در عدم قطعیت اجرای احکام تبدیل شده‌است (Born, 2021: 821). این امر ناشی از تعارض مضاعف میان حاکمیت دولت‌ها در شناسایی احکام خارجی (ماده V کنوانسیون) و عدم انطباق قواعد سنتی صلاحیت با محیط دیجیتال است.

۲-۳-۳. محدودیت‌های پرداخت‌های الکترونیکی

محدودیت‌های پرداخت‌های الکترونیک صرفاً نسخه دیجیتالِ موانع بانکی سنتی نیستند؛ بلکه پویایی نظام‌های مالی دیجیتال، این چالش‌ها را به‌گونه‌ای کیفی متفاوت ساخته است. تحریم‌های اقتصادی (نظیر مسدودسازی پلتفرم‌هایی مانند پی‌پال[1] در برخی حوزه‌های قضایی)، کنترل‌های ارزی مبتنی بر ریسک‌سنجی الگوریتمی، و ناهمگونی زیرساخت‌های بانکداری دیجیتال، جریان ارزش‌گذاری شده در قرارداد الکترونیکی[2] را با مخاطرات بی‌سابقه‌ای مواجه می‌سازد (Zetzsche et al, 2020: 103) و در نتیجه تحقق تعهدات پرداختی به‌عنوان ستون فقرات اجرای قرارداد در گرو غلبه بر موانعی است که ماهیتاً زاده فضای دیجیتال‌اند. البته می‌توان در این راستا از رمزارزها استفاده نمود. رمزارز یک دارایی دیجیتال قابل مبادله یا شکل دیجیتالی پول خصوصی است که بر اساس سفناوری زنجیره بلوکی ساخته شده است و صرفا در محیط اینترنت وجود دارد و کاربر می‌تواند بدون دخالت دولت و یک نهاد متمرکز به صرافی‌ها ارائه نماید (الهیاری‌فرد و پروین، ۱۴۰۳: ۱۴۰).

۳-۳-۳. تبلور چالش‌های کلاسیک در بستر دیجیتال: ضرورت تحلیل افتراقی

اگرچه موانعی چون شناسایی احکام خارجی یا محدودیت‌های ارزی، منحصر به تجارت الکترونیک نیست، اما فقدان مرزهای فیزیکی و سرعت فوق‌العاده تراکنش‌ها در این فضا، به‌گونه‌ای بنیادین بر معادلات اجرایی تأثیر می‌گذارد. به عنوان مثال، مشکل اجرای رأی داوری در کنوانسیون نیویورک در قراردادهای الکترونیکی با

(New York,1985)

1. PayPal
2. Value Transfer

پیچیدگی اثباتیِ مضاعفی همراه است. پرسش‌هایی مانند اعتبار اسناد دیجیتال به‌عنوان مدرک یا قابلیت پذیرش امضاهای رمزنگاری‌شـــده در دادگاه خارجی، چالش اجرا را به مراتب فراتر از موارد سنتی می‌برد (MANN, 2019: 75).

٤-٣-٣. چالش‌های شکلی و اثباتی و راهکارهای آن

پیچیدگی‌های فرامرزی قراردادهای دیجیتال، موجب بروز چالش‌های حقوقی ماهوی و شـــکلی شده که رفع آن‌ها نیازمند چارچوب‌های هماهنگ بین‌المللی (مانند اسناد آنسیترال) و فناوری‌های امنیتی است. طرفین با تعیین دقیق شرایط و قانون حاکم بر اساس اصل حاکمیت اراده، از حقوق تجاری خود حراست می‌کنند.

نخســـت، چالش‌های ماهوی (اعتبار ســـند، تعارض قوانین، مسؤولیت فنی): در ارزیابی قضایی، اعتبار اســـناد الکترونیک و قراردادهای هوشـــمند مستلزم عبور از چارچوب ســـنتی «اصالت سند» است. تعارض قوانین ملی با اقتضائات فناوری (نظیر مسؤولیت مدنی الگوریتم‌ها) حل‌ناشده باقی مانده است. راهکار کارشناسانه، پذیرش اصل برابری کارکردی (مطابق مـــاده ۱۲ قانون تجارت الکترونیک ایران) و گنجاندن شروط حل اختلاف فنی‌حقوقی در قراردادهای پایه است.

دوم، چالش‌های شـــکلی و اثباتـــی (ادله دیجیتال، حریـــم خصوصی، امنیت ســـایبری): مهم‌ترین معضل، اثبات اصالت و تمامیت ادله دیجیتال در دادگاه اســـت؛ چراکـــه زنجیره حفاظـــت داده و احراز عدم دخل و تصرف ثالث به ســـادگی ممکن نیست. همچنین حریم خصوصی اشخاص در فرایند کشف قضایی الکترونیک با اصل لزوم ادله مواجه می‌شود. راهکارهای موثر در این راستا، تنظیم سیاست‌های حفظ داده، اســـتفاده از رمزنگاری سرتاسری و امضای دیجیتال مبتنی بر گواهی‌های معتبر (مطابق قانون امضای الکترونیک و آیین‌نامه‌های مرتبط) است.

ســـوم، چالش‌های اجرایی (اجرای احکام، محدودیت پرداخت): موانع اجرای احکام فراملی (نظیر شناسایی نشدن قراردادهای هوشمند در برخی نظام‌های حقوقی) و محدودیت نقل‌وانتقال پول ملی، از موانع جدی اجراست. راهکار پیشنهادی عبارت اســـت از: ارجاع به داوری بین‌المللی با تعیین قانـــون حاکم و محل داوری بی‌طرف (مثلاً دیوان داوری بین‌المللی) و نیز تســـویه از طریق رمزارزهای پایدار تا جایی که با مقررات پولی و بانکی ملی تعارض نداشته باشد.

٤. راهکارهای حقوقی و فنی برای کاهش چالش‌ها

با عنایت به پیچیدگی‌های روزافزون قراردادهای الکترونیکی در حوزه تجارت فرامرزی، اتخاذ سازکارهای حقوقی و فنیِ جامع‌نگر، به ضرورتی انکارناپذیر بدل گشته است. در این مسیر، چهار رکن بنیادین راکه در ادامه می‌آید می‌توان به منظور کاستن از چالش‌های پیش‌رو برشمرد.

٤-١. توسعه چارچوب‌های حقوقی هماهنگ

از جمله راهکارهای کارآمد، پیوستن دولت‌ها به اسناد بین‌المللیِ استانداردسازی شده، از جمله قانون نمونه آنسیترال در زمینه تجارت الکترونیکی[1] است. این سند با تشریح مبانی حقوقیِ کلیدی مانند داده‌پیام[2] و ایجاب و قبول الکترونیکی[3]، بسترساز هماهنگیِ نظام‌های حقوقی در به رسمیت شناختن اعتبار قراردادهای دیجیتالی محسوبِ می‌شود[4].

الحاق به قانون نمونه آنسیترال در حوزه تجارت الکترونیک، با ایجاد وحدت رویه در تفسیر و اجرای قراردادهای الکترونیکی میان نظام‌های حقوقی متکثر، هم‌گرایی هنجاری را جایگزین تشتت قوانین داخلی ساخته و از رهگذر تأمین امنیت حقوقی فراملی، پیش‌بینی‌پذیری نتایج معاملات برون‌مرزی را ارتقا می‌بخشد و موجبات کاهش دعاوی ناشی از تعارض قوانین را فراهم می‌آورد. در لایه‌ای عمیق‌تر، این الحاق به‌مثابه نشانه‌ای راهبردی از التزام به استانداردهای جهانی، اعتماد نهادی فعالان اقتصادی و دولت‌های خارجی را جلب کرده، جایگاه کشور را در زنجیره تعاملات دیجیتال بین‌المللی تثبیت و زمینه ادغام در اقتصاد دیجیتال قاعده‌مند را مهیا می‌سازد. بدین‌سان، انسجام درونی نظام حقوقی، امنیت حقوقی فرامرزی و کنش‌گری مؤثر بین‌المللی حلقه‌های به‌هم‌پیوسته یک زنجیره واحد را تشکیل می‌دهند.

تشکیل دیوان تخصصی تجاری به جای دادگاه اختصاصی و یا شعب تخصصی تجاری به عنوان راهکار کارآمدتری برای رسیدگی به دعاوی تجاری

---

1. UNCITRAL Model Law on Electronic Commerce
2. Data Message
3. Electronic Will
4. UNCITRAL, 1999: 3–8

پیشـــنهاد می‌شـــود (غلامی ،۱٤۰۰: ۲۸۳) می‌توان بخش خاصی از این دادگاه‌ها را به صورت اختصاصی یا تخصصی به این قرارداها اختصاص داد.

٤-۲. بهره‌گیری از فناوری‌های نوین

تحـــولات فناورانه زمینه‌ســـاز ایجاد رویکردهای نویـــن در کاهش مخاطرات حقوقی گردیده اســـت؛ بـــه گونه‌ای که اســـتفاده از قراردادهای هوشـــمند مبتنی بر فنـــاوری بلاکچین، امکان اجرای خـــودکار تعهدات قـــراردادی را فراهم نموده و با حذف واســـطه‌های انسانی، موجب کاهش محـــسوس خطاها و تخلفات شده است (Werbach & Cornell, 2017: 345). همچنین ســـازکارهای احراز هویت دیجیتال نظیر امضاهای الکترونیک پیشـــرفته، نقش اساســـی در تأمین اعتبار طرفین معامله ایفا می‌نمایند (Clack, Bakshi & Braine, 2016: 5–6).

همچنین در فرایند حل اختلاف می‌توان از هوشمندســـازی فرایندهای قضایی با بهره‌گیری از فناوری‌هایی نظیر هوش مصنوعی، پردازش کلان‌داده، یادگیری ماشین و بلاکچین، اســـتفاده کرد. اجرای این فرایند پیچیده با چالش‌هایی مواجه است که از مهم‌ترین آن‌ها می‌توان به موانع قانونی، ملاحظات اخلاقی، محدودیت‌های زیرساختی، مقاومت ســـازمانی و نگرانی‌های مربوط به امنیت و حریم خصوصی اشاره کرد (مقدم و حسینی، ۱٤۰٤: ۳٦۸-۳٦۹)

٤-۳. تقویت نظام‌های حل‌وفصل اختلافات تخصصی

با توجه به ماهیـــت فراملی و فناورانه قراردادهای الکترونیکی، ســـازکارهای سنتی حلوفصل اختلافات قادر به پاسخ‌گویی به نیازهای عصر دیجیتال نمی‌باشند؛ لذا ایجاد مراجـــع داوری الکترونیکی و تقویت نهادهای تخصصی میانجیگری بین‌المللی از جمله سامانه داوری الکترونیکی[1] و مرکز بین‌المللی حل اختلاف[2]، علاوه بر تسریع فرایندهای رســـیدگی، از انسجام ذاتی با ویژگی‌های دیجیتال اختلافات تجاری نوین برخوردار است (Kessedjian, 2021: 22).

اساساً تعیین قانون حاکم بر داوری در داوری های تجاری بین المللی به علت دخالت یک رکـــن خارجی در اختلاف، اهمیت زیادی دارد. در این شـــرایط قوانین

1. Electronic Business Related Arbitration and Mediation (Ebram)
2. International Centre for Dispute Resolution (ICDR)

متعددی با جنبه‌های مختلف اختلاف ارتباط پیدا می‌کند و به این علت تعیین قانون حاکم بر هر یک از آن‌ها اهمیت زیادی می‌یابد که در موارد ذیل قابل طرح است: قانون حاکم برای تشخیص اهلیت طرفین قرارداد؛ قانون حاکم بر موافقت‌نامه داوری؛ قانون حاکم بر آیین داوری؛ قانون حاکم بر ماهیت اختلاف؛ قانون حاکم بر شناسایی و اجرای رای داوری؛ قابلیت داوری‌پذیری اختلاف (جوهر، ۱۴۰۳: ۶۰).

٤-٤. ارتقای آگاهی حقوقی تجار و فعالان اقتصادی

تعلیم نظام‌مند و ارتقای سواد حقوقی فعالان تجاری در خصوص ظرایف قراردادهای الکترونیکی، به مثابه زیربنایی استوار برای صیانت از مناسبات تجاری و گزینش خردمندانه پلتفرم‌های معاملاتی عمل می‌نماید. در این میان، تألیف منشورهای راهبردی و اجرای دوره‌های تخصصی کاربردی، سهمی انکارناپذیر ایفا می‌نماید.

٥-٤. ماتریس راهکارهای قراردادهای الکترونیکی بین‌المللی

در واکاوی این ساختار شبکه‌ای چندلایه، باید بر ماهیت مکمل و سلسله‌مراتبی راهکارها انگشت نهاد. الحاق به کنوانسیون‌های بین‌المللی به‌ویژه آنسیترال، راهکاری بنیادین و تقنینی است که با هم‌سنگ‌سازی قوانین داخلی و استانداردهای جهانی، تعارض قوانین را زدوده و امنیت حقوقی فرامرزی را قوام می‌بخشد؛ بنا به تصریح آنسیترال، این شالوده اعتماد به تجارت الکترونیکی بین‌المللی است[1]. با این همه، این اقدامِ پایه‌ای جز با لایه‌های فنی و نهادی تکمیل‌گر کافی نمی‌باشد.

لایه دوم، بهره‌گیری از فناوری‌های نامتمرکز از جمله قراردادهای هوشمند و بلاکچین، اقدامی فنی اجرایی است که با خودکارسازی اجرا و شفافیت تراکنشی، دو کاستی دیرپای تقلب و کندی اجرا را آماج می‌گیرد (Zheng et al., 2018: 376). کارآمدی این لایه تماماً مشروط به شناسایی حقوقی آن در لایه نخست، یعنی چارچوب هم‌سو با استانداردهای آنسیترال است.

لایه سوم، با سرشت نهادی بر تأسیس مراجع تخصصی حل اختلاف، مشخصاً داوری الکترونیکی متمرکز است. این مرجع متخصص در دعاوی دیجیتال، هم‌زمان دو سودمندیِ شتاب‌دهی به دادرسی و کاهش هزینه‌ها را تأمین می‌کند

1. UNCITRAL, 2005: 12

و نقش حلقه واسط میان چارچوب حقوقی (لایه اول) و واقعیت فنی (لایه دوم) را ایفا می‌نماید. آموزش حقوقی تجار راهکاری نرم، پیشینی و پیش‌گیرانه است که خلأ آگاهی حقوقی را آماج قرار می‌دهد. مطابق گزارش کنفرانس تجارت و توسعهٔ سازمان ملل متحد، بخش عمده‌ای از اختلافات تجاری بین‌المللی ریشه در ناآگاهی از اعتبار و مخاطرات این دست قراردادها دارد[1] که با اقدامات آگاهی‌بخش می‌توان از پیدایش آن پیش‌گیری کرد. هم‌افزایی چهار لایه تقنین، فناوری، نهادسازی و آموزش نقشه راهی منسجم برای کاستن از چالش‌های قراردادهای الکترونیکی فراملی ترسیم می‌کند.

۵. بررسی تطبیقی رویکردهای مختلف

۱-۵. اتحادیه اروپا: ساختار حقوقی دقیق، مبتنی بر اعتماد دیجیتال

اتحادیه اروپا از دهه ۱۹۹۰، در مسیر یکسان‌سازی حقوقی تجارت الکترونیک و شکل‌دهی به بازار دیجیتال یکپارچه، با محوریت حریم خصوصی (ماده ۵ مقررات عمومی حفاظت از داده‌ها) و امنیت داده‌ها (ماده ٦ همان سند)، به تقنین پرداخته است. (Regulation (EU) No 910/2014, eIDAS: 73-75).

«مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد» ۲۰۱٤ [2] به عنوان نقطه عطفی تاریخی، نخستین چارچوب الزام‌آور فراملی در حوزه شناسه‌های دیجیتال، امضاهای الکترونیکی و خدمات اعتمادی محسوب می‌شود. بر اساس ماده ۲۵ این مقررات، امضاهای الکترونیکی در سه سطح ساده، پیشرفته و معتبر طبقه‌بندی می‌گردند. پیوند این مقررات با مقررات عمومی حفاظت از داده‌ها موجب تقویت اصولی همچون امنیت داده‌های شخصی، رضایت آگاهانه کاربران و شفافیت تراکنش‌ها به‌عنوان ارکان روابط حقوقی دیجیتال شده و نقش کلیدی در تکامل «بازار واحد دیجیتال اروپا» ایفا کرده است.

در تحلیل کلان‌تر، سه روند حقوقی برجسته است؛ نخست،اولویت اصل اعتماد بر رضایت محض در تنظیم روابط حقوقی؛ دوم، ترجیح حمایت از داده‌ها بر آزادی قراردادی به‌عنوان ارزش بنیادین؛ و سوم، چالش مقررات پیچیده برای

1. UNCTAD, 2021: 23
2. eIDAS (2014)

بنگاه‌های کوچک و متوسط[1] که نیازمند بازنگری سیاستی جهت کاهش موانع توسعه کسب وکارهای نوپاست. این رویکرد متوازن، همزمان به امنیت حقوقی و رشد اکوسیستم دیجیتال توجه دارد.

۲-۵. ایالات متحده: حاکمیت اراده طرفین و رویکرد فناورانه

نظام حقوقی آمریکا در حوزه تجارت الکترونیک، بر مبنای اصل آزادی قراردادی و حداقل مداخله تنظیمی استوار گردیده است. دو سند کلیدی شامل قانون امضاهای الکترونیکی در سطح ملی قانون «امضاهای الکترونیکی در تجارت جهانی و ملی[2]» و فدرال قانون یکنواخت معاملات الکترونیکی» (مصوب در سطح ایالتی) قانون یکنواخت معاملات الکترونیکی در سطح ایالتی، با پرهیز از تحمیل چارچوب‌های فنی خاص، رضایت متعاملین و تحقق هدف قراردادی را به عنوان معیار اعتبار حقوقی تعاملات دیجیتال تثبیت نموده‌اند. مستند قانونی این امر بند ۲ ماده ۱۰۱ قانون «امضاهای الکترونیکی در تجارت جهانی و ملی» است. سیاست انعطاف‌پذیر مذکور با پیامدهای حقوقی اقتصادی همراه بوده که از جمله آن‌ها می‌توان به زمینه‌سازی برای رونق بازار خدمات امضای دیجیتال، توسعه فناوری‌های نوین از جمله بلاک‌چین، و همچنین افزایش مقبولیت راهکارهای غیرمتمرکز اشاره نمود.

از جمله ویژگی‌های کلیدی این قوانین می‌توان به وجود اعتبار حقوقی (امضاهای الکترونیکی معادل امضاهای دست‌نویس هستند[3] و همچنین شرایط این اعتبار (رضایت طرفین و قابلیت اثبات صحت معامله[4]) اشاره کرد. چالش‌های کلان نظام حقوقی شامل تناقضات بین‌ایالتی ناشی از عدم پذیرش یکپارچه قانون یکنواخت معاملات الکترونیکی (مصوب در سطح ایالتی) توسط تمامی ایالت‌ها، تعارض استانداردهابه‌ویژه در هم‌سویی با چارچوب‌های بین‌المللی مانند «مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد» اتحادیه اروپا و اسناد آنسیترال، و ابهام هویتی به دلیل فقدان ضوابط صریح در احراز هویت دیجیتال معتبر

1. Small and Medium-sized Enterprises (SMEs)
2. Electronic Signatures in Global and National Commerce Act (2000)
3. UETA Section7
4. Section 101 ESIGN

می‌شود که این موارد به‌طور کلی کارآمدی و انسجام نظام حقوقی را تحت تأثیر قرار می‌دهند.

۳-۵. ایران: خلأهای نهادی و چالش‌های اجرایی

تصویب قانون تجارت الکترونیکی (۱۳۸۲) اگرچه در زمان خود اقدامی پیشگامانه برای ورود ایران به عرصه تنظیم‌گری تجارت الکترونیک بود، لیکن در عمل به دلیل فقدان سازکار پویای تقنینی، عدم ایجاد نهادهای تخصصی ناظر و ناسازگاری با تحولات شتابان فناوری، با چالش‌های بنیادین مواجه شده است. این قانون که عمدتاً متأثر از قانون نمونه آنسیترال ۱۹۹۶ [1] بود، بدون بومی‌سازی کارشناسی و پیش‌بینی الزامات نهادی، به‌مثابه اسکلتی بی‌روح باقی ماند.

۱-۳-۵. نقایص ماهوی در ساحت تقنین

قانون تجارت الکترونیکی مصوب ۱۳۸۲ به‌رغم ترسیم چارچوب اولیه، در گذر زمان با نقایص ماهوی متعددی در ساحت تقنین مواجه شده که کارآمدی آن را در عصر اقتصاد دیجیتال به چالش کشیده است؛ ابهام در مفاهیم کلیدی، خلأ مقرراتی خدمات اعتماد و انفعال در برابر فناوری‌های نوظهور، نمودهای بارز این کاستی‌ها به شمار می‌روند.

۲-۳-۵. ابهام در مفهوم‌سازی امضای الکترونیکی مطمئن

ماده ۱۰ قانون تجارت الکترونیکی امضای الکترونیکی مطمئن را تعریف نموده، لیکن معیارهای «انحصار به امضاکننده» و «قابلیت ردیابی تغییرات» (ماده ۱۰ بندهای ج و د) فاقد ضمانت اجراهای فنی و نهادی لازم است. فقدان راهکارهای استاندارد احراز هویت غیرحضوری مانند نظام [2] سلسله‌مراتب زیرساخت کلید عمومی ملی و عدم انطباق با سطوح اعتبارسنجی «مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد» پیشرفته/معتبر)، عملاً این نهاد حقوقی را به حاشیه رانده است. نظام سلسله‌مراتب زیرساخت کلید عمومی ملی چارچوبی امنیتی مبتنی بر رمزنگاری نامتقارن است که اصالت هویت دیجیتال، احراز مالکیت داده‌ها و تضمین یکپارچگی و محرمانگی اطلاعات را در فضای مجازی فراهم می‌کند. در سطح ملی، این نظام

1. UNCITRA, 1996
2. Public Key Infrastructure

ایجاد یک اکوسیستم متمرکز و استاندارد تحت نظارت دولت برای ارائه خدمات اعتماد دیجیتال به شهروندان، بنگاه‌ها و نهادهای دولتی است که ارکان اصلی آن عبارت است از:

نخست، مراجع صدور گواهی دیجیتال[1]: نهادهای معتمد (عمدتاً دولتی) مسؤول تأیید هویت و صدور گواهی‌های دیجیتال که حاوی اطلاعات هویتی و کلید عمومی دارنده بوده و به عنوان «امضای الکترونیکی مطمئن» مطابق ماده ۱۰ قانون تجارت الکترونیکی عمل می‌کنند.

دوم، مراکز ثبت: انجام فرایند احراز هویت اولیه متقاضیان (حضوری/ غیرحضوری).

سوم، سیستم لغو گواهی: تضمین یکپارچگی چرخه حیات گواهی‌ها از طریق انتشار فهرست‌های پویای گواهی‌های باطل‌شده.

۳-۳-۵. خلأ مقرراتی پیرامون «خدمات اعتماد»[2]

عدم تصویب آیین‌نامه اجرایی ماده ۳۱ قانون تجارت الکترونیکی (۱۳۸۲) طی دو دهه، به شکل‌گیری دو آسیب ساختاری کلیدی منجر شده است: فقدان یک مرجع صدور ریشه‌ای دولتی ((Root CA و تعدد مراجع صدور گواهی فاقد هم‌سویی. فعالیت جزیره‌ای این مراجع، بدون التزام الزام‌آور به استانداردهای بین‌المللی، موجد ناهمگونی فنی در الگوریتم‌ها و پروتکل‌های امنیتی و نیز گسست در زنجیره اعتماد ناشی از عدم استقرار یک مدل نظارتی یکپارچه گردیده است. پیامد این وضعیت، شکل‌گیری اکوسیستم‌های موازی غیرقابل تعامل، تضعیف امنیت تراکنش‌های الکترونیکی، و ناکامی در تحقق فراگیر نهادهای «داده‌پیام مطمئن» و «امضای الکترونیکی مطمئن» (مواد ۱۱ و ۱۲ قانون) است. قانون مذکور به‌رغم اشاره به این مفاهیم، فاقد چارچوبی مشخص برای اعطای مجوز، نظارت مستمر یا تعیین مسؤولیت مدنی ارائه‌دهندگان خدمات اعتماد (نظیر مراجع صدور گواهی) می‌باشد؛ نقصانی که به شکل‌گیری بازاری غیرشفاف و پرریسک در حوزه خدمات اعتماد انجامیده است.

1. Cas: Certification Authorities
2. Trust Services

پراکندگی نهادی نیز چالشـــی عمیق‌تر محسوب می‌شـــود. تداخل وظایف و تعدد سیاســـت‌ها میان نهادهای متولی شامل وزارت صنعت، معدن و تجارت (متولی تجارت الکترونیک)، مرکز توسعه تجارت الکترونیکی، سازمان فناوری اطلاعات ایران (زیرمجموعـــه وزارت ارتباطات)، و مرکز ملی فضای مجازی، کارآمدی نظام نظارتی را به‌شـــدت کاهش داده اســـت. افزون بر این، نظام دادرســـی با نارسایی‌های جدی در رســـیدگی به اختلافات پیچیده تجارت الکترونیک مواجه اســـت. هرچند ماده ۱۵ قانون آیین‌دادرســـی دادگاه‌های عمومی و انقلاب در امور مدنی اصلاحی ۱۳۹٤ ادله الکترونیکی را معتبر شـــناخته، فقدان پروتکل‌های اســـتاندارد برای جمع‌آوری، حفظ تمامیت[1] و ارائه این ادله، اجرای مؤثر این ماده را دشوار ساخته و دادگاه‌ها را با کمبود تخصص لازم روبه‌رو کرده است.

٤-۳-۵. چالش‌های نوپدید در مواجهه با فناوری‌های تحول‌ساز

در مواجهه با فناوری‌هـــای نوظهور نیز چالش‌های حقوقـــی بنیادینی پدیدار گشـــته‌اند. نظام حقوقی ایران فاقد هرگونه تکلیف‌سازی در خصوص «قابلیت استناد حقوقی قراردادهای هوشـــمند خوداجرا» و «تخصیص مســـؤولیت ناشـــی از اجرای الگوریتمیک» به‌ویژه در حوزه‌هایی مانند اینترنت اشـــیاء اســـت. پرسش محوری این اســـت که آیا مفاهیم ســـنتی حقوقی نظیر «قصد و رضا» (مـــاده ۱۹۰ قانون مدنی) با ماهیت خودکار و غیر قابل توقف قراردادهای هوشـــمند مبتنی بر بلاکچین سازگاری دارد. این خلأها توانایی نظام حقوقی در پاسخ‌گویی به تحولات فناورانه را زیر سؤال برده‌است. همچنین ممنوعیت مبادله رمزارزها توسط بانک مرکزی (۱۳۹۸) بدون ارائه جایگزین حقوقی برای «تســـویه بین‌المللی قراردادهای الکترونیکی»، عملاً بخشی از مزایای تجارت الکترونیک جهانی را مســـدود نموده است. این امر با تحولات حقوقی در حوزه‌هایی مانند مقررات بازار دارایی‌های رمزنگاری‌شـــده اتحادیه اروپا (مصوب ۲۰۲۳)[2] در تضاد آشکار قرار دارد.

1. Integrity
2. Markets in Crypto-Assets Regulation 2023 (MiCA)

ب. ارزیابی راهبردی و پیشنهادهای تحول‌آفرین

در ارزیابی راهبردی، ایستایی تقنینی به‌عنوان چالش کلان نخست، ناشی از عدم اصلاح قانون تجارت الکترونیکی مصوب ۱۳۸۲ است که پیامد مستقیم آن عقب‌ماندگی نظام حقوقی ایران از استانداردهای بین‌المللی نظیر مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد و قانون نمونه آنسیترال در زمینه انتقال الکترونیکی اسناد می‌باشد. رهایی از این رکود، جز از طریق تدوین لایحه‌ای جامع با عنوان «تجارت دیجیتال» و هم‌سوسازی کامل با این اسناد مرجع میسر نیست.

چالش دوم، فقدان نهاد تنظیم‌گر تخصصی است که علت ریشه‌ای آن را باید در تعدد مراجع تصمیم‌گیر جست‌وجو کرد؛ وضعیتی که موجد پراکندگی سیاستی و در نهایت کاهش اعتماد عمومی به اکوسیستم دیجیتال شده است. راهکار پیشنهادی یعنی تأسیس «سازمان تنظیم‌گری تجارت الکترونیک» با اختیارات فرابخشی، پاسخی ضروری برای انسجام‌بخشی و بازسازی این اعتماد از دست رفته تلقی می‌گردد.

ناکارآمدی دادرسی سومین ضلع این مثلث چالش‌های ساختاری است که ریشه در کمبود قضات متخصص دارد و اثبات دعاوی الکترونیکی را با معضل طولانی‌شدن فرایند رسیدگی روبه‌رو ساخته است. در این حوزه، ایجاد شعب تخصصی دادگاه‌های تجارت الکترونیک و استفاده نظام‌مند از کارشناسان فنی، نه‌تنها گلوگاه اطاله دادرسی را برطرف می‌سازد، بلکه به ارتقای اتقان آرای قضایی در این دعاوی پیچیده و تخصصی خواهد انجامید.

٦. چالش‌های کلیدی

با توجه به چالش‌های موجود در حوزه امضاهای دیجیتال، می‌توان مهم‌ترین نقاط ضعف را در سه محور اصلی شامل ضعف سیاست‌گذاری فناوری محور ناشی از فقدان چارچوب‌های منسجم برای هماهنگی با تحولات دیجیتال، نبود نهاد ناظر مستقل و تخصصی جهت نظارت بی‌طرفانه بر فرایند امضاهای دیجیتال و ابهام در ادله اثباتی به‌ویژه عدم شفافیت در جایگاه حقوقی امضای دیجیتال در نظام ادله دعاوی و رویه‌های قضایی تبیین نمود. عدم تفکیک حقوقی میان انواع امضای

الکترونیکی و تعیین ضوابط اختصاصی برای هر یک، ابهام در ارزش اثباتی امضاهای دیجیتال در مراجع قضایی و داوری و وابستگی به زیرساخت‌های دولتی نامنعطف و ناکارآمد در ارائه خدمات اعتماد الکترونیک، مهمترین خلاهای تقنینی می‌باشند. عدم بازنگری در قانون تجارت الکترونیکی پس از دو دهه، کارایی آن را محدود کرده و اصلاح ساختار نظارتی و به‌روزرسانی قوانین برای امنیت قراردادهای الکترونیکی ضروری است.

۶-۱. خلاء قانونی

بازنگری قانون تجارت الکترونیکی با هدف هماهنگی با فناوری‌های نوین (قراردادهای هوشمند و رمزارزها)، تعیین مراجع صالح رسیدگی به اختلافات، تقویت ضمانت‌های اجرایی نقض حریم خصوصی داده‌ها، و تأسیس نهاد نظارتی تخصصی خدمات اعتماد دیجیتال[1] با اختیارات صدور مجوز، نظارت هوشمند و اعتبارسنجی کسب وکارهای دیجیتال، جهت ایجاد چارچوبی امن و شفاف در فضای تجارت الکترونیک ضروری است. همچنین راهبردهای کلان بین‌المللی شامل پیوستن به کنوانسیون CUECIC برای هماهنگی استانداردهای امضای دیجیتال در قراردادهای بین‌المللی، کاهش تعارض قوانین در داوری الکترونیکی و تسهیل شناسایی اسناد دیجیتال از طریق توافق‌های دوجانبه با کشورهای پیشرو در تجارت دیجیتال.

۶-۲. سازکارهای شفاف‌سازی و حکمرانی مشارکتی

به منظور ارزیابی اثرات تنظیمی[2] پیش از تصویب هر مقرره و همچنین انتشار عمومی پیش‌نویس‌ها در پلتفرم‌های مشورتی، لازم است شورای سیاست‌گذاری چندذی‌نفعی متشکل از نمایندگان وزارت صنعت، معدن و تجارت، اتاق بازرگانی، انجمن‌های فناوری اطلاعات و اساتید حقوق سایبری تشکیل شود.

۶-۳. پیاده‌سازی نظام انگیزشی برای بازیگران خصوصی

از آنجا که حکمت در مدیریت اقتصادی، ترکیب هوشمندانه مشوق‌ها با مسؤولیت‌پذیری اجتماعی است. اعطای معافیت‌های مالیاتی به کسب‌وکارهایی

1. Trust Service Agency (TSA)
2. Regulatory Impact Assessment (RIA)

که اســـتانداردهای امنیتی نهاد نظارتی تخصصی خدمـــات اعتماد دیجیتال را فراتر از حداقل‌های قانونی رعایت می‌کنند می‌تواند راهکاری حکیمانه در این بخش باشـــد. همچنیـــن تدوین بانک قراردادهای الکترونیکی نمونـــه با همکاری وکلای مجرب و فناوران حقوقی[1] سبب تسهیل قراردادنویسی الکترونیکی می‌شود.

٤-٦. ارتقای زیرساخت‌های فنی حقوقی

توســـعه مرکز ملی ارزیابی انطباق[2] برای آزمایش و صدور گواهی اســـتاندارد ابزارهـــای پرداخت الکترونیک، مطابق با مقررات مبارزه با پول‌شـــویی و تأمین مالی تروریسم[3] و راه‌اندازی سامانه نظارت بلادرنگ جهت رصد تخلفات مصرف‌کنندگان، امنیت و شفافیت تراکنش‌ها را افزایش می‌دهد. این طرح با ترکیب تنظیم‌گری چابک و پاســـخگویی الگوریتمی، هزینه‌های انطباق را کاهش داده و بستری امن برای تولید دیجیتال فراهم می‌کند. موفقیت آن وابســـته به تنظیم‌گری متناسب و همکاری بخش خصوصی و دولتی است.

٥-٦. مقایســـه تطبیقی نظام‌های امضای الکترونیک و حفاظت از داده‌ها در اتحادیه اروپا، ایالات متحده و ایران

در مقایســـه تطبیقی صورت‌گرفته، شـــکاف عمیق میان نظـــام حقوقی ایران با اســـتانداردهای اتحادیه اروپا آشکار اســـت. اتحادیه اروپا با ایجاد سلسله‌مراتب دقیق میان انواع امضا و اعطای اعتبار کامل صرفاً به «امضای واجد شـــرایط» در چارچوب مقررات شناســـایی الکترونیکی، احراز هویت و خدمات اعتماد، توانسته پیوندی وثیق میان هویت دیجیتال و امنیت تراکنش‌ها برقرار سازد؛ حال آن‌که حقوق ایران با فقدان تفکیک دقیق میـــان انواع امضای الکترونیکی، از بازتعریـــف عملیِ «امضای مطمئن» بازمانده است. این کاســـتی با تمرکزگرایی محدود و فاقد اختیاراتِ فرابخشی «مرکز توســـعه تجارت الکترونیکی» در قیاس با نهادهای نظارتی چندلایه اروپایی تشـــدید می‌شود.

در بُعـــد حفاظت از داده‌ها، اتحادیه اروپا با مقررات عمومی حفاظت از داده‌ها به سطحی از نظام‌مندی رســـیده که اعتماد عمومی را به رکن اساسی اقتصاد دیجیتال

1. Legal Tech
2. Conformity Assessment Centre (CAC)
3. Anti-Money Laundering / Countering the Financing of Terrorism (AML/CFT)

بدل ســـاخته، در حالی که قانون ناقص و پراکنده ایران در این حوزه، موقعیت آن را حتـــی پایین‌تر از نظام نام‌متمرکز و فاقد قانون فدرال جامـــع ایالات متحده قرار داده اســـت. این ضعف ساختاری، هم‌راستایی با اســـناد بین‌المللی نظیر آنسیترال را نیز به شدت کاهش داده است.

نکته قابل تأمل آن‌که، رویکرد ایالات متحده با پذیرش اصل «رضایت طرفین» به عنوان مبنـــای اعتبار هر نوع امضا، انعطاف‌پذیری حداکثـــری را بر امنیت حقوقی ترجیح داده و احراز هویت را ســـاده نگاه داشته، مدلی که با واقعیت‌های اقتصادی آن هم‌خوان اســـت اما با منطق قاعده‌گـــذار اروپایی و نیازهای یک نظام حقوقی در حال توسعه مانند ایران تفاوت بنیادین دارد. قانون تجارت الکترونیکی ایران در میانه این دو طیف، دچار وضعیت تعلیق است: انعطاف‌پذیری متوسطی دارد اما ضعف اجرایی، آن را به سوی ناکارآمدی سوق داده و احراز هویت را در مرحله‌ای ناپایدار از توسعه نگاه داشته است. این مقایسه نشان می‌دهد که ایران نه می‌تواند الگوی کاملاً آزاد آمریکا را بدون زیرســـاخت‌های قضایی و قراردادی آن تقلید کند و نه بدون اصلاحات بنیادین، توان دستیابی به استحکام حقوقی مدل اروپایی را دارد.

برآمد

۱- قراردادهای الکترونیکی به دلیل ماهیت فرامرزی و دیجیتال خود با چالش‌های اساسی در زمینه احراز هویت، تعارض قوانین، امنیت داده‌ها و اجرای احکام بین‌المللی مواجه هستند. این مشکلات عمدتاً ناشی از ناهماهنگی بین قواعد سنتی حقوق قراردادها و ویژگی‌های منحصر به فرد فضای دیجیتال است. برای حل این چالش‌ها، نیاز به بازنگری در قوانین داخلی و تقویت همکاری‌های بین‌المللی است. البته در سطح بین‌المللی، اسنادی به دنبال افزایش امنیت حقوقی و پیش‌بینی‌پذیری قراردادهای الکترونیکی بوده‌اند، اما تفاوت‌های نظام‌های حقوقی ملی و مقاومت برخی کشورها در پذیرش استانداردهای جهانی همچنان چالش‌های جدی در مسیر یکپارچگی حقوقی ایجاد می‌کند.

۲- در سطح داخلی، قانون تجارت الکترونیکی ایران گام اولیه در به رسمیت شناختن اعتبار قراردادهای الکترونیکی بوده، اما به دلیل عدم بازنگری و نبود زیرساخت‌های اجرایی کافی، با چالش‌هایی مانند ضعف در پذیرش قضایی، نبود نهاد ناظر مستقل، و عدم انطباق با فناوری‌های نوین مانند بلاکچین و قراردادهای هوشمند مواجه است. برای ارتقای نظام حقوقی قراردادهای الکترونیک، ضروری است قانون تجارت الکترونیکی با تفکیک انواع امضاهای دیجیتال و پیش‌بینی مقررات فناوری‌های نوین بازنگری شود. تأسیس نهاد نظارتی مستقل برای صدور گواهی‌های دیجیتال، توسعه زیرساخت‌های امن احراز هویت و پرداخت الکترونیک و برگزاری دوره‌های آموزشی تخصصی برای ذی‌نفعان از دیگر اقدامات ضروری محسوب می‌شود. این راهکارها در کنار تدوین استانداردهای قراردادنویسی الکترونیکی می‌توانند چالش‌های موجود را مرتفع سازند.

۳- در سطح بین‌المللی، ضروری است با پیوستن به کنوانسیون‌هایی مانند آنسیترال (۲۰۰۵) و لاهه (۲۰۱۹) تعارضات قانونی کاهش یابد، از طریق ایجاد نهادهای تخصصی مانند مرکز بین‌المللی حل اختلاف به اختلافات رسیدگی شود و با الگوبرداری از استانداردهای موفق بین‌المللی مانند «مقررات عمومی حفاظت از داده‌ها» و «مقررات شناسایی الکترونیکی، احراز هویت و خدمات اعتماد»، مقررات یکپارچه‌ای در زمینه امضای دیجیتال و حفاظت از داده‌ها تدوین گردد.

٤- حقـــوق قراردادهـــای الکترونیکـــی در عصر دیجیتال نیازمنـــد ترکیبی از انعطاف‌پذیری و امنیت حقوقی اســـت و لازم است با بهره‌گیری از فناوری‌های نوین، کارآمدی قراردادها را افزایش داد و با حفظ اصول عدالت قراردادی، توازن مناســـبی بیـــن نوآوری و نظم حقوقی ایجاد کرد. همـــکاری بین‌المللی، تقویت چارچوب‌های داخلی و توسعه زیرساخت‌های دیجیتال، سه رکن اساسی برای موفقیت نظام حقوقی قراردادهای الکترونیکی محسوب می‌شود.

فهرست منابع

الف. فارسی

* اکبرینه، پروین و محمدزاده، فریبا (۱۳۹۵)، «**قراردادهای الکترونیکی**»، در: کنگره بین‌المللی حقوق اسلامی، علوم انسانی. تهران: ایران.

* الهیاری‌فـــرد، علی و پروین، خیراله (۱۴۰۳)، «**تنظیم‌گری مالیات بر ارزش افزوده و سوداگری رمزارزها در اتحادیه اروپا**»، مجله حقوقی دادگستری، دوره ۸۸، شماره ۱۲۶.

* جوهر، ســـعید (۱۴۰۳)، «**قانون ماهوی حاکم بر اختلاف در داوری‌های تجاری بین‌المللی در صورت عدم انتخابِ طرفین اختلاف**»، مجله حقوقی دادگستری، دوره ۸۸، شماره ۱۲۷.

* غلامـــی، نگیـــن (۱۴۰۴)، «**موانع کارآمدی شـــعب تخصصی تجاری در حقوق ایران**»، مجله حقوقی دادگستری، دوره ۸۹، شماره ۱۳۱.

* مقدم، محمد جواد و حسینی، ســـید ابراهیم (۱۴۰۴)، «**هوشمندسازی فرآیندهای قضایی و عدالت کیفری**»، مجله حقوقی دادگستری، دوره ۸۹، شماره ۱۳۱.

* دره‌شـــامی، قاسم (۱۳۹۷)، **شرایط اعتبار قرارداد الکترونیکی**، پایان‌نامه کارشناسی ارشد، ماکو: واحد بین‌الملل دانشگاه آزاد اسلامی.

* دهقانـــی تفتی، مجتبی و افضلی‌مهر، مرضیه و اســـکینی، ربیعـــا (۱۴۰۰)، «**مطالعه تطبیقی قانون حاکم بر قراردادهای هوشـــمند دیجیتالی از منظر حقوق بین‌الملل خصوصـــی در نظام حقوقی ایران و مقررات رم**»، حقوق فناوری‌های نوین، ســـال دوم، دوره ۲، شماره ٤.

* صاحب‌اختیاری، غزالـــه (۱۴۰۲)، «**ماهیت قراردادهای الکترونیکی در چارچوب قواعد تجـــارت بین‌الملل**»، در: مجموعه مقالات کنفرانـــس بین‌المللی پژوهش‌های مدیریت و علوم انسانی دانشگاه تهران.

* طغـــیانی‌پور، علی (۱۴۰۳)، «**انعـــقاد عقد در فضای ســـایبری از منظر حقوق بین‌الملل**»، در: مجمـوعه مـقالات اولین همایش ملی علـوم انسانی با رویکرد نوین، گیلان، آستارا

ب. انگلیسی

* Born, Gary B (2014), **International commercial arbitration (Vol.**

1, 2nd ed.), The Hague: Kluwer Law International.

❋ Clack, Christopher D, Bakshi, Vikram A, & Braine, Lee (2016), **Smart contract templates: Foundations**, **design landscape and research directions,** available at: < https://arxiv.org/abs/1608.00771> (last visited on 17/04/ 2025)

❋ Greenleaf, Graham (2018), **Global data privacy laws 2017: 120 national laws, and still counting**, Privacy Laws & Business International Report, 147, 10–13.

❋ Greenleaf, Graham., & Waters, Nigel (2019), **Global data privacy laws 2019**: **132 national laws & many bills**. Privacy Laws & Business International Report, 157, 14–18.

❋ Karim, Mohammad (2020), **Legal validity of electronic contracts in international trade: A comparative study**. Journal of International Commercial Law, 19(2), 145–172.

❋ Kerr, Orin S (2019), **Digital evidence and the new criminal procedure**, Columbia Law Review, 119(1), 52–98.

❋ Kessedjian, Catherine (2021), **Digital dispute resolution and international arbitration**, Journal of International Arbitration, 38(1), 1–26.

❋ Kohl, Uta (2007), **Jurisdiction and the Internet: Regulatory competence over online activity (1st ed.)**, Cambridge: Cambridge University Press.

❋ Kohl, Uta (2018), **The net and the nation state**, Cambridge: Cambridge University Press.

❋ Kuner, Christopher (2020), **Transborder data flows and data privacy law**, Oxford: Oxford University Press.

❋ Mann, Frederick Alexander (2019), **The legal aspect of money (7th ed.)**, Oxford: Oxford University Press.

❋ Martin, Charles H (2014), **Every1's guide to electronic contracts:**

Contract law on how to create electronic signatures and contracts: Every1's Guide Publishing.

❋ Murray, Andrew (2023), **Information technology law: The law and society (5th ed.)**, Oxford: Oxford University Press.

❋ Reed, Chris & Murray, Andrew (2019), **Rethinking the jurisprudence of cyberspace: A comparative analysis**, International Journal of Law and Information Technology, 27(3), 203–229.

❋ Reed, Chris (2010), **Making laws for cyberspace (1st ed.)**, Oxford: Oxford University Press.

❋ Reed, Chris (2018), **Law of electronic commerce**, Oxford: Oxford University Press.

❋ Rowe, Michael (2022), **E-commerce contracts: Allocation of risk and responsibility**, International Journal of Law and Information Technology, 30(1), 45-61 .

❋ Schmidt-Kessel, Martin, (Ed.). (2020). **The future of the CISG: A global assessment**, Munich: Sellier European Law Publishers.

❋ Voigt, Paul., & Von dem Bussche, Axel (2017), **The EU General Data Protection Regulation (GDPR)**, Berlin: Springer.

❋ Werbach, Kevin & Cornell, Nicolas (2017), **Contracts Ex Machina**, Duke Law Journal, 67(2), 313–382.

❋ Zheng, Sophia (2018), **Cybersecurity and cybercrime: A legal guide (3rd ed.)**, London: Routledge.

❋ Zheng, Zibin, Xie, Shaoan, Dai, Hong-Ning, Chen, Xiangping, & Wang, Huaimin (2018), **Blockchain challenges and opportunities: A survey**, International Journal of Web and Grid Services, 14(4), [pp 352-375], available at: < https://doi.org/10.1504/IJWGS.2018.095647> (last visited on 15/04/ 2025).