

# **A Legal Analysis of Confidentiality in International Commercial Arbitration: Challenges Arising from the Digitalization of Documents and Electronic Evidence**

1. Gholamhossein Asheghi: Master's Student in Private Law, Department of Jurisprudence and Islamic Law, Urmia University, Iran
2. Salman Alipour\*: Assistant Professor, Department of Jurisprudence and Islamic Law, Urmia University, Iran. Email: s.alipour@urmia.ac.ir (Corresponding Author)

## **ABSTRACT**

Confidentiality is one of the principal reasons commercial actors choose international arbitration, as parties generally expect their contractual, financial, technical, and commercially sensitive information to remain protected from public disclosure. Nevertheless, confidentiality is not regarded in all legal systems as an inherent, absolute, or uniformly enforceable principle and may instead arise from party agreement, the law of the arbitral seat, institutional rules, tribunal orders, or professional obligations. The distinction between privacy and confidentiality is therefore fundamental, since the exclusion of third parties from arbitral hearings does not necessarily prohibit the subsequent disclosure of pleadings, evidence, procedural decisions, or awards. Using a descriptive-analytical method, this study examines the legal foundations, scope, exceptions, and enforcement mechanisms of confidentiality, with particular emphasis on the challenges created by digital documents and electronic evidence. The findings indicate that instant duplication, cross-border transmission, recoverability of deleted data, embedded metadata, cloud storage, virtual hearings, and artificial-intelligence-assisted processing have significantly increased the risks of accidental disclosure, unauthorized access, and secondary use of arbitral information. The development of smart contracts and technology-based dispute-resolution mechanisms has also generated new concerns regarding permanent data storage, user identification, and the responsibility of technology providers. Confidentiality may additionally conflict with statutory disclosure duties, judicial proceedings, award enforcement, the right of defense, public policy, and demands for transparency. The study concludes that digital confidentiality must be understood not merely as a negative duty to refrain from disclosure, but as an active obligation involving access control, cybersecurity, data minimization, secure transmission, incident response, and final deletion. Detailed confidentiality clauses, cybersecurity protocols, encryption, role-based access, controlled electronic disclosure, and clearly allocated institutional and technological responsibilities are therefore essential to ensuring effective protection throughout the arbitral process.

**Keywords:** *International Commercial Arbitration; Confidentiality; Electronic Documents; Electronic Evidence; Cybersecurity; Data Protection; Artificial Intelligence.*

How to cite: Asheghi, G. & Alipour, S. (2024). A Legal Analysis of Confidentiality in International Commercial Arbitration: Challenges Arising from the Digitalization of Documents and Electronic Evidence. *Comparative Studies in Jurisprudence, Law, and Politics*, 6(4), 292-314.

© 2024 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Submit Date: 06 October 2024  
Revise Date: 30 December 2024  
Accept Date: 06 January 2025  
Publish Date: 20 January 2025



## تحلیل حقوقی محرمانگی در داوری تجاری بین‌المللی؛ چالش‌های ناشی از دیجیتالی‌شدن اسناد و ادله الکترونیکی

۱. غلامحسین عاشقی: دانشجوی کارشناسی ارشد حقوق خصوصی، گروه فقه و حقوق اسلامی، دانشگاه ارومیه، ایران
۲. سلمان علیپور\*: استادیار، گروه فقه و حقوق اسلامی، دانشگاه ارومیه، ایران. پست الکترونیک: s.alipour@urmia.ac.ir (نویسنده مسئول)

### چکیده

محرمانگی از مهم‌ترین دلایل گرایش فعالان اقتصادی به داوری تجاری بین‌المللی است؛ زیرا طرفین انتظار دارند اطلاعات قراردادی، مالی، فنی و تجاری آنان خارج از فرایند حل اختلاف افشا نشود. با این حال، محرمانگی در همه نظام‌های حقوقی اصلی ذاتی، مطلق و یکسان به شمار نمی‌آید و ممکن است از توافق طرفین، قانون مقر داوری، قواعد مؤسسات داوری، دستورهای دیوان یا تعهدات حرفه‌ای ناشی شود. تمایز میان خصوصی‌بودن رسیدگی و محرمانگی اطلاعات نیز اهمیت اساسی دارد؛ زیرا غیرعلنی‌بودن جلسات لزوماً ممنوعیت افشای اسناد، لوایح یا رأی را ایجاد نمی‌کند. پژوهش حاضر با روش توصیفی - تحلیلی، مبانی، قلمرو، استثنائات و ضمانت اجرای محرمانگی را با تمرکز بر چالش‌های ناشی از دیجیتالی‌شدن اسناد و ادله الکترونیکی بررسی می‌کند. یافته‌ها نشان می‌دهد ویژگی‌هایی مانند تکثیرپذیری سریع، انتقال فرامرزی، امکان بازیابی داده‌های حذف‌شده، وجود فراداده، ذخیره‌سازی ابری، جلسات مجازی و استفاده از هوش مصنوعی، خطر افشای ناخواسته و دسترسی غیرمجاز را افزایش داده‌اند. توسعه قراردادهای هوشمند و سازوکارهای حل اختلاف فناورانه نیز مسائل جدیدی درباره ماندگاری داده، هویت کاربران و مسئولیت ارائه‌دهندگان خدمات ایجاد کرده است. افزون بر این، محرمانگی ممکن است با الزام‌های قانونی، اجرای رأی، حق دفاع، نظم عمومی و ضرورت شفافیت تعارض پیدا کند. نتیجه پژوهش آن است که محرمانگی در محیط دیجیتال باید از یک تعهد صرفاً منفی به تعهدی فعال برای کنترل دسترسی، حفاظت سایبری، حداقل‌سازی داده‌ها و حذف امن اطلاعات تبدیل شود. تنظیم شروط دقیق محرمانگی، تصویب پروتکل امنیت سایبری، محدودکردن دسترسی، رمزگذاری اطلاعات و تعیین مسئولیت مؤسسات و ارائه‌دهندگان فناوری، از مهم‌ترین راهکارهای حمایت مؤثر از اطلاعات داوری است.

**واژگان کلیدی:** داوری تجاری بین‌المللی؛ محرمانگی؛ اسناد الکترونیکی؛ ادله الکترونیکی؛ امنیت سایبری؛ حفاظت از داده‌ها؛ هوش مصنوعی

**نحوه استناددهی:** عاشقی، غلامحسین، و علیپور، سلمان. (۱۴۰۳). تحلیل حقوقی محرمانگی در داوری تجاری بین‌المللی؛ چالش‌های ناشی از دیجیتالی‌شدن اسناد و ادله الکترونیکی. پژوهش‌های تطبیقی فقه، حقوق و سیاست، ۶(۴)، ۲۹۲-۳۱۴.

© ۱۴۰۳ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

تاریخ ارسال: ۱۵ مهر ۱۴۰۳

تاریخ بازنگری: ۱۰ دی ۱۴۰۳

تاریخ پذیرش: ۱۷ دی ۱۴۰۳

تاریخ چاپ: ۱ بهمن ۱۴۰۳

داوری تجاری بین‌المللی در دهه‌های اخیر به یکی از مهم‌ترین سازوکارهای حل و فصل اختلافات ناشی از روابط تجاری فرامرزی تبدیل شده است. توسعه قراردادهای بین‌المللی، گسترش فعالیت شرکت‌های چندملیتی، افزایش سرمایه‌گذاری‌های خارجی، پیچیده‌تر شدن مبادلات مالی و فنی و نیاز فعالان اقتصادی به رسیدگی تخصصی و انعطاف‌پذیر، موجب شده است که بسیاری از اشخاص خصوصی و بنگاه‌های تجاری، داور را بر رسیدگی قضایی دولتی ترجیح دهند. امکان انتخاب داوران متخصص، تعیین قانون حاکم، انتخاب زبان و محل داور، انعطاف در طراحی شیوه رسیدگی و قابلیت شناسایی و اجرای فرامرزی رأی، از جمله مزایایی است که جایگاه داور را در تجارت بین‌المللی تقویت کرده است. در ادبیات حقوقی معاصر نیز داور تجاری بین‌المللی نه صرفاً به عنوان جایگزینی برای دادرسی دولتی، بلکه به عنوان نظامی مستقل و متناسب با نیازهای تجارت فرامرزی مورد تحلیل قرار گرفته است (Fouchard et al., 2024). انعطاف ساختاری داور به طرفین اجازه می‌دهد قواعد متناسب با ماهیت اختلاف خود را تعیین کنند و از تشریفات سخت‌گیرانه‌ای که معمولاً در دادگاه‌های ملی وجود دارد فاصله بگیرند (Redfern & Hunter, 2023). در حقوق ایران نیز داور تجاری بین‌المللی بر پایه حاکمیت اراده، استقلال شرط داور و امکان تنظیم آیین رسیدگی متناسب با خواست طرفین تحلیل می‌شود (Shirovi, 2024). همین ویژگی‌ها موجب شده است که داور برای اختلافات پیچیده تجاری، قراردادی، مالی، انرژی، حمل و نقل، ساخت و ساز و فناوری جذابیت ویژه‌ای پیدا کند.

یکی از مهم‌ترین انتظارات فعالان تجاری از داور، حفظ محرمانگی اطلاعات مربوط به اختلاف و جلوگیری از انتشار اسناد و اسرار تجاری آنان است. شرکت‌ها معمولاً تمایل ندارند اختلافات قراردادی، مشکلات مالی، ضعف‌های مدیریتی، شیوه قیمت‌گذاری، اطلاعات فنی، مذاکرات تجاری یا روابط آنان با شرکای خارجی در معرض اطلاع عموم، رقبای، رسانه‌ها یا بازارهای مالی قرار گیرد. از این رو، محرمانگی اغلب به عنوان یکی از مزایای بنیادین داور معرفی می‌شود. برخی نویسندگان، اعتماد طرفین به محرمانه ماندن رسیدگی را یکی از عوامل اصلی رجوع آنان به داور دانسته‌اند (Bagner, 2001). در این برداشت، داور فضایی ایجاد می‌کند که در آن طرفین می‌توانند اطلاعات حساس را بدون نگرانی از انتشار عمومی ارائه کنند و اختلاف خود را در محیطی محدود، تخصصی و کنترل‌شده حل و فصل نمایند. با این حال، نسبت میان ماهیت خصوصی داور و وجود تعهد الزام‌آور به محرمانگی همواره روشن و یکسان نیست. خصوصی بودن جلسه به این معناست که اشخاص ثالث بدون رضایت طرفین یا اجازه مرجع داور حق حضور ندارند، اما محرمانگی مفهومی گسترده‌تر است و می‌تواند شامل ممنوعیت افشای وجود اختلاف، محتوای لوایح، اسناد ارائه‌شده، مذاکرات، شهادت‌ها، گزارش‌های کارشناسی، تصمیمات آیینی و رأی نهایی شود. تحلیل تطبیقی نظام‌های حقوقی نشان می‌دهد که نمی‌توان از خصوصی بودن داور در همه موارد، تعهدی عام و مطلق به محرمانگی استنتاج کرد (Noussia, 2010). برخی نظام‌ها چنین تعهدی را به صراحت شناسایی کرده‌اند، برخی آن را از توافق طرفین یا ماهیت رابطه داور استنباط می‌کنند و برخی دیگر بدون وجود شرط قراردادی یا مقرر مشخص، حاضر به پذیرش تعهد گسترده محرمانگی نیستند.

این اختلاف دیدگاه موجب شده است که مفهوم محرمانگی در داور تجاری بین‌المللی از حیث مبنا، قلمرو، اشخاص متعهد، استثنائات و ضمانت اجرا با ابهام‌های قابل توجهی روبه‌رو باشد. در برخی پرونده‌ها، طرفین تصور می‌کنند صرف انتخاب داور به معنای ممنوعیت هرگونه افشاست، در حالی که قانون مقرر داور یا قواعد مؤسسه منتخب ممکن است تنها داوران و کارکنان مؤسسه را به محرمانگی ملزم کند. در برخی موارد نیز یکی از طرفین برای حمایت از حقوق خود، اجرای رأی، انجام تکلیف قانونی یا دفاع در دعوی دیگر ناگزیر از افشای بخشی از اطلاعات داور است. بررسی‌های کلاسیک درباره محرمانگی نشان داده‌اند که این اصل برخلاف تصور رایج، در بسیاری از نظام‌ها واجد

ساختار یکدست و جهان‌شمول نیست (Misra & Jordan, 2006). از سوی دیگر، گسترش مطالبه شفافیت در برخی حوزه‌های داوری، به‌ویژه اختلافات مرتبط با منافع عمومی، سرمایه‌گذاری خارجی، منابع طبیعی، فساد یا عملکرد نهادهای عمومی، دیدگاه سنتی درباره محرمانگی مطلق را با تردید مواجه ساخته است. تعارض میان محرمانگی و شفافیت یکی از تنش‌های پایدار در حقوق داوری بین‌المللی محسوب می‌شود (Buys, 2003). هرچه اختلاف دارای آثار گسترده‌تری بر اشخاص ثالث، بودجه عمومی یا منافع اجتماعی باشد، توجیه محدودکردن دسترسی عمومی به اطلاعات آن دشوارتر می‌شود.

تحولات فناوریانه، مسئله محرمانگی را از سطح یک بحث کلاسیک درباره منع افشا فراتر برده و آن را به موضوعی مرتبط با امنیت داده‌ها، مدیریت اطلاعات، حفاظت سایبری و مسئولیت حرفه‌ای تبدیل کرده است. در داوری‌های سنتی، عمده اسناد به‌صورت کاغذی تهیه و در پوشه‌های فیزیکی نگهداری می‌شدند و دسترسی به آن‌ها معمولاً از طریق کنترل محل نگهداری، مهر و موم پرونده و محدودکردن نسخه‌برداری مدیریت می‌شد. امروزه بخش عمده ارتباطات تجاری و دلایل اثباتی به‌صورت دیجیتال ایجاد می‌شوند. ایمیل‌ها، پیام‌های فوری، قراردادهای الکترونیکی، داده‌های سامانه‌های حسابداری، فایل‌های صوتی و تصویری، اطلاعات ذخیره‌شده در تلفن همراه، سوابق ورود به سامانه‌ها، داده‌های ابری و اطلاعات حاصل از ابزارهای هوشمند، بخش مهمی از ادله مورد استفاده در داوری را تشکیل می‌دهند. لوايح از طریق سامانه‌های الکترونیکی ارسال می‌شوند، جلسات استماع به‌صورت مجازی برگزار می‌گردند، کارشناسان از راه دور به اسناد دسترسی پیدا می‌کنند و فایل‌های حجیم در فضای ابری یا اتاق‌های داده مجازی ذخیره می‌شوند. این وضعیت، هرچند موجب افزایش سرعت و کاهش هزینه‌های فیزیکی شده است، دامنه اشخاص و سامانه‌هایی را که به اطلاعات پرونده دسترسی دارند گسترش داده و امکان کنترل سنتی بر محرمانگی را کاهش داده است.

دیجیتالی‌شدن اسناد ویژگی‌هایی را پدید آورده است که آن‌ها را از اسناد کاغذی متمایز می‌کند. یک فایل دیجیتال می‌تواند در چند ثانیه تکثیر و به نقاط مختلف جهان منتقل شود، بی‌آنکه دارنده اصلی از تعداد نسخه‌ها یا محل ذخیره آن‌ها آگاه باشد. اطلاعات حذف‌شده ممکن است از طریق ابزارهای بازیابی دوباره در دسترس قرار گیرد و فراداده‌های پنهان می‌تواند اطلاعاتی درباره نویسنده، زمان ایجاد، تاریخچه ویرایش، محل جغرافیایی یا دستگاه مورد استفاده آشکار کند. حتی زمانی که متن ظاهری یک سند فاقد اطلاعات حساس است، مشخصات فنی آن ممکن است راهبرد حقوقی، ساختار داخلی شرکت یا هویت اشخاص درگیر در تهیه سند را فاش سازد. علاوه بر این، یک پرونده داوری می‌تواند هم‌زمان در رایانه وکیل، سرور شرکت، سامانه مؤسسه داوری، فضای ابری ارائه‌دهنده خدمات و دستگاه شخصی کارشناس ذخیره شود. هر حلقه از این زنجیره می‌تواند به نقطه ضعف امنیتی تبدیل شود. بنابراین، مفهوم محرمانگی در محیط دیجیتال دیگر صرفاً به خودداری آگاهانه اشخاص از انتشار اطلاعات محدود نیست، بلکه مستلزم اتخاذ اقدامات فعال برای جلوگیری از دسترسی غیرمجاز، نشت داده، حمله سایبری و استفاده ثانویه از اطلاعات است.

ظهور قراردادهای هوشمند و سازوکارهای حل اختلاف مبتنی بر فناوری نیز مرز میان فرایند حقوقی و زیرساخت فنی را کم‌رنگ کرده است. در اختلافات مرتبط با قراردادهای هوشمند، بخشی از داده‌ها ممکن است در زنجیره بلوکی ثبت شده باشد و بخشی دیگر از فرایند حل اختلاف در خارج از زنجیره انجام شود. این ساختار، مسائل پیچیده‌ای درباره دسترسی عمومی به اطلاعات ثبت‌شده، تغییرناپذیری داده‌ها، هویت اشخاص و مسئولیت نهادهای فنی ایجاد می‌کند (Haddadi, 2024). حتی در داوری‌های غیرمرتبط با زنجیره بلوکی نیز استفاده از ابزارهای هوش مصنوعی برای ترجمه، خلاصه‌سازی، جست‌وجوی اسناد یا تنظیم لوايح، خطر انتقال اطلاعات محرمانه به سامانه‌های خارجی

را افزایش داده است. زمانی که وکیل، کارشناس یا داور بخشی از پرونده را در یک سامانه عمومی هوش مصنوعی وارد می‌کند، ممکن است کنترل خود را بر نحوه ذخیره، پردازش یا استفاده بعدی از داده‌ها از دست بدهد. از این رو، تعهد محرمانگی باید استفاده از فناوری‌های نوین را نیز پوشش دهد و صرفاً به منع انتشار مستقیم اسناد محدود نماند.

اهمیت موضوع زمانی بیشتر می‌شود که ماهیت فرامرزی داوری در نظر گرفته شود. اسناد یک پرونده ممکن است در کشوری ایجاد، در کشور دیگری ذخیره، توسط مؤسسه‌ای در حوزه قضایی سوم مدیریت و در جلسه‌ای مجازی با حضور اشخاصی از چندین کشور بررسی شوند. در چنین شرایطی، قواعد مربوط به محرمانگی، حفاظت از داده‌های شخصی، انتقال بین‌المللی اطلاعات، اسرار تجاری، امنیت سایبری و تکالیف حرفه‌ای ممکن است به طور هم‌زمان قابل اعمال باشند. تعیین قانون حاکم بر تعهد محرمانگی نیز همیشه آسان نیست. ممکن است قانون حاکم بر قرارداد اصلی، قانون مقر داوری، قانون محل اقامت طرفین، قانون محل ذخیره داده و قواعد مؤسسه داوری نتایج متفاوتی ارائه کنند. انتخاب قانون حاکم در داوری یکی از عناصر اساسی تنظیم رابطه حقوقی طرفین است (Johar, 2024)، اما در زمینه محرمانگی دیجیتال، این انتخاب باید با قواعد آمره حفاظت از اطلاعات و الزامات کشور محل پردازش داده نیز هماهنگ شود. به همین دلیل، توافق قراردادی طرفین هرچند اهمیت بنیادین دارد، نمی‌تواند همیشه تمام ابعاد موضوع را پوشش دهد یا قواعد الزام‌آور نظام‌های ملی را کنار بگذارد.

نقض محرمانگی در محیط دیجیتال می‌تواند پیامدهایی فراتر از زیان‌های سنتی ناشی از افشای یک سند داشته باشد. انتشار اطلاعات تجاری ممکن است موقعیت رقابتی یک شرکت را تضعیف کند، اعتماد مشتریان و سرمایه‌گذاران را از بین ببرد، ارزش فناوری یا اسرار تولیدی را کاهش دهد و شرکت را در معرض دعاوی متعدد قرار دهد. افشای داده‌های شخصی شهود، کارکنان یا مشتریان نیز می‌تواند مسئولیت‌های مستقلی بر اساس قوانین حفاظت از داده‌ها ایجاد کند. علاوه بر این، حمله سایبری به سامانه داوری می‌تواند تمامیت فرایند را زیر سؤال ببرد، اصالت دلایل را مخدوش سازد یا زمینه مداخله غیرقانونی در تصمیم‌گیری داوران را فراهم کند. در چنین وضعیتی، داوری تنها با مسئله حفاظت از منافع خصوصی طرفین مواجه نیست، بلکه اعتبار نهادی خود را نیز در معرض خطر می‌بیند. اعتماد به داوری زمانی حفظ می‌شود که طرفین اطمینان داشته باشند اطلاعات حساس آنان در تمام مراحل رسیدگی، از زمان ثبت درخواست تا اجرای رأی و حذف نهایی داده‌ها، با استانداردهای معقول حقوقی و فنی محافظت خواهد شد.

هدف این پژوهش، تحلیل حقوقی محرمانگی در داوری تجاری بین‌المللی با تمرکز بر چالش‌های ناشی از دیجیتالی‌شدن اسناد و ادله الکترونیکی است. این پژوهش می‌کوشد روشن سازد که محرمانگی در داوری بر چه مبانی استوار است، چه اشخاص و اطلاعاتی را در بر می‌گیرد، چگونه با الزامات افشا و شفافیت تعارض پیدا می‌کند و در محیط دیجیتال چه تحولاتی در مفهوم و ضمانت اجرای آن رخ داده است. پرسش اصلی آن است که آیا قواعد سنتی محرمانگی برای پاسخ‌گویی به خطرهای ناشی از ذخیره‌سازی ابری، جلسات مجازی، افشای الکترونیکی اسناد، فراداده‌ها، حملات سایبری و استفاده از هوش مصنوعی کافی است یا آنکه داوری تجاری بین‌المللی به چارچوبی تکمیلی از تعهدات قراردادی، دستورهای حفاظتی، استانداردهای امنیتی و قواعد مسئولیت نیاز دارد. فرض اصلی این است که محرمانگی در محیط دیجیتال از یک تعهد منفی به خودداری از افشا، به تعهدی مثبت و چندبعدی برای پیشگیری، مراقبت، کنترل دسترسی و واکنش به رخدادهای امنیتی تبدیل شده است. روش پژوهش توصیفی - تحلیلی و با استفاده از منابع کتابخانه‌ای، آثار حقوقی، مطالعات تطبیقی و تحلیل قواعد عمومی داوری است. رویکرد پژوهش در عین توجه به مبانی نظری، بر ارائه راهکارهای عملی برای قراردادهای داوری، مدیریت پرونده، مسئولیت مؤسسات و استفاده ایمن از فناوری تمرکز دارد.

## مبانی، منابع و قلمرو محرمانگی در داوری تجاری بین‌المللی

محرمانگی در داوری تجاری بین‌المللی مفهومی چندلایه است که نمی‌توان آن را صرفاً با غیرعلنی‌بودن جلسه یا خصوصی‌بودن رابطه داوری یکسان دانست. خصوصی‌بودن به ساختار رسیدگی مربوط می‌شود و بیانگر آن است که داوری برخلاف دادگاه‌های عمومی، اصولاً برای حضور آزادانه مردم یا رسانه‌ها تشکیل نمی‌شود. محرمانگی، در مقابل، به تعهد اشخاص برای جلوگیری از افشا، انتقال یا استفاده خارج از هدف از اطلاعات مرتبط با داوری اشاره دارد. ممکن است جلسه‌ای خصوصی باشد، اما یکی از طرفین پس از جلسه، محتوای آن را در گزارش مالی یا دعوایی دیگر منتشر کند؛ همچنین ممکن است اصل وجود داوری عمومی شود، ولی بخشی از اسناد به موجب دستور حفاظتی محرمانه باقی بماند. تفکیک این دو مفهوم در تحلیل حقوقی ضروری است، زیرا بسیاری از اختلافات از آنجا ناشی می‌شود که طرفین خصوصی‌بودن را معادل محرمانگی کامل تلقی می‌کنند. مطالعات تطبیقی نشان داده‌اند که نظام‌های حقوقی در استنباط تعهد محرمانگی از ماهیت خصوصی داوری رویکردهای متفاوتی دارند (Noussia, 2010). بنابراین، صرف انتخاب داوری لزوماً به معنای آن نیست که تمام اشخاص دخیل، نسبت به همه اطلاعات و برای مدتی نامحدود، به سکوت مطلق متعهد باشند.

یکی از مبانی اصلی محرمانگی، حاکمیت اراده طرفین است. داوری در اصل بر توافق استوار است و بدون رضایت معتبر اشخاص، مرجع داوری صلاحیت رسیدگی پیدا نمی‌کند. همین مبنای قراردادی به طرفین اجازه می‌دهد حدود محرمانگی را تعیین کنند، اشخاص مجاز به دسترسی را مشخص سازند، استثنائات را پیش‌بینی نمایند و برای نقض تعهد ضمانت اجرا قرار دهند. تحلیل‌های کلاسیک داوری تجاری بین‌المللی، توافق طرفین را منبع بنیادین بسیاری از قواعد آیینی می‌دانند (Fouchard et al., 2024). اگر طرفین در قرارداد اصلی یا موافقت‌نامه داوری شرطی روشن درباره محرمانگی درج کنند، تردید درباره وجود اصل تعهد کاهش می‌یابد. باین‌حال، حاکمیت اراده نامحدود نیست. طرفین نمی‌توانند با توافق خصوصی، تکالیف الزام‌آور ناشی از قوانین عمومی، مقررات بازار سرمایه، قواعد مالیاتی، الزامات مبارزه با پول‌شویی، دستورات قضایی یا حقوق اشخاص ثالث را کنار بگذارند. شرط محرمانگی همچنین نمی‌تواند مانع استفاده ضروری از اطلاعات برای اجرای رأی یا دفاع از حق شود. از این‌رو، ارزش توافق طرفین بیشتر در تعیین قاعده عمومی و شیوه مدیریت اطلاعات است، نه ایجاد ممنوعیتی مطلق که بر همه الزامات قانونی برتری داشته باشد.

مبنای دیگر محرمانگی، حمایت از اعتماد مشروع طرفین است. اشخاصی که داوری را به دلیل غیرعلنی‌بودن و محدودبودن دسترسی انتخاب می‌کنند، انتظار دارند اطلاعات حساس آنان در خارج از پرونده مورد استفاده قرار نگیرد. برخی نویسندگان این انتظار را چنان اساسی دانسته‌اند که محرمانگی را از اصول بنیادی داوری معرفی کرده‌اند (Bagner, 2001). استدلال اصلی این است که بدون اطمینان از محرمانگی، طرفین ممکن است از ارائه کامل اسناد، پذیرش اشتباهات، افشای اطلاعات فنی یا بیان صریح مواضع خودداری کنند و کیفیت رسیدگی کاهش یابد. محرمانگی از این منظر، تنها امتیازی برای حمایت از شهرت تجاری نیست، بلکه ابزاری برای کشف حقیقت و اداره مؤثر فرایند نیز محسوب می‌شود. با وجود این، تبدیل انتظار ذهنی به تعهد حقوقی نیازمند مبنای مشخص است. انتظار عرفی طرفین زمانی می‌تواند الزام‌آور باشد که از قانون، رویه، قواعد نهادی یا اوضاع و احوال قرارداد پشتیبانی شود. در غیر این صورت، ادعای وجود تعهد ضمنی ممکن است در برابر اصل آزادی اشخاص و ضرورت‌های قانونی افشا با دشواری مواجه شود.

حمایت از اسرار تجاری و اطلاعات اقتصادی نیز از مبانی مهم محرمانگی است. پرونده‌های داوری غالباً شامل قراردادهای بلندمدت، فناوری‌های اختصاصی، قیمت‌گذاری، فهرست مشتریان، اطلاعات بانکی، برنامه‌های سرمایه‌گذاری، روش‌های تولید، گزارش‌های حسابرسی و راهبردهای

تجاری هستند. افشای این اطلاعات می‌تواند مزیت رقابتی صاحب آن را از بین ببرد، حتی اگر طرف افشاکننده قصد ورود زیان نداشته باشد. بنابراین، محرمانگی با قواعد حمایت از اسرار تجاری پیوند پیدا می‌کند. باین‌حال، قلمرو این دو کاملاً یکسان نیست. هر اطلاعات محرمانه داوری لزوماً سر تجاری نیست و هر سر تجاری نیز فقط به دلیل حضور در داوری حمایت نمی‌شود. اطلاعاتی مانند اظهارات شهود، برنامه جلسات یا هویت کارشناس ممکن است محرمانه تلقی شود، بی‌آنکه ارزش اقتصادی مستقل داشته باشد. در مقابل، یک سر تجاری ممکن است پیش از داوری نیز به موجب قانون یا قرارداد حمایت شود. اهمیت این تمایز در تعیین ضمانت اجرا آشکار می‌شود، زیرا افشای سر تجاری ممکن است علاوه بر نقض تعهد داوری، موجب مسئولیت مستقل مدنی یا کیفری گردد.

در حقوق داوری، قانون مقر داوری یکی از منابع تعیین‌کننده قلمرو تعهد محرمانگی است. مقر داوری صرفاً محل فیزیکی برگزاری جلسه نیست، بلکه پیوند حقوقی داوری با نظام قضایی خاص را مشخص می‌کند. قانون مقر می‌تواند درباره اختیارات داوران، نظارت دادگاه‌ها، ابطال رأی، تدابیر موقت و گاه محرمانگی قواعدی وضع کند. آثار مربوط به آیین داوری تأکید می‌کنند که انتخاب مقر، پیامدهای حقوقی گسترده‌ای برای فرایند دارد (Redfern & Hunter, 2023). برخی قوانین ملی، تعهد محرمانگی را صریحاً بر طرفین و داوران تحمیل می‌کنند؛ برخی فقط جلسات را غیرعلنی می‌دانند و برخی در این زمینه سکوت دارند. در نظام‌های ساکت، دادگاه ممکن است تعهد را از قرارداد یا ماهیت داوری استنباط کند یا برعکس، بدون شرط روشن از تحمیل آن خودداری نماید. این تنوع سبب می‌شود طرفین پیش از انتخاب مقر، تنها به بی‌طرفی قضایی یا سهولت اجرا توجه نکنند، بلکه موضع نظام حقوقی مربوط درباره محرمانگی و حفاظت از داده‌ها را نیز بررسی نمایند.

در حقوق ایران، داوری تجاری بین‌المللی بر مبنای توافق طرفین، استقلال داوری و آزادی نسبی آنان در تعیین قواعد رسیدگی تحلیل می‌شود (Shirovi, 2024). باین‌حال، محرمانگی به‌عنوان اصلی جامع و با تمام جزئیات مربوط به اشخاص، اطلاعات و ضمانت اجرا، نیازمند تصریح قراردادی و تنظیم دقیق است. تحلیل‌های داخلی درباره محرمانگی داوری نیز از دیرباز میان گرایش به حفظ بسته‌بودن فرایند و ضرورت پذیرش موارد افشا تمایز قائل شده‌اند (Enayat, 1999). بنابراین، در قراردادهای بین‌المللی که یکی از طرفین ایرانی است، اتکا به تصور کلی محرمانه‌بودن داوری کافی نیست. شرط داوری باید به‌روشنی تعیین کند که آیا وجود داوری، اسناد، لوایح، جلسات، رأی و مذاکرات سازشی محرمانه‌اند و چه اشخاصی مجاز به دریافت اطلاعات هستند. همچنین باید رابطه این شرط با الزامات قانونی و امکان مراجعه به دادگاه برای ابطال یا اجرای رأی مشخص شود.

قواعد مؤسسات داوری نیز منبع مهم دیگری برای تعهد محرمانگی هستند. هنگامی که طرفین داوری سازمانی را انتخاب می‌کنند، قواعد مؤسسه جزء چارچوب قراردادی رسیدگی می‌شود. برخی مؤسسات برای اعضای دیوان، کارکنان و منشیان تعهد محرمانگی مقرر می‌کنند، اما نسبت به طرفین سکوت دارند. برخی دیگر، اسناد و تصمیمات را نیز مشمول حمایت قرار می‌دهند یا اختیار صدور دستور حفاظتی را به دیوان می‌سپارند. این تفاوت‌ها نشان می‌دهد که انتخاب مؤسسه نباید صرفاً بر اساس شهرت، هزینه یا سرعت انجام شود. طرفین باید سیاست محرمانگی، نحوه ذخیره داده‌ها، قواعد انتشار آرای ناشناس‌شده و استانداردهای فناوری مؤسسه را بررسی کنند. حتی اگر قواعد مؤسسه محرمانگی را پیش‌بینی کرده باشد، ممکن است پوشش آن محدود به دوره داوری یا اشخاص وابسته به مؤسسه باشد. در چنین وضعیتی، کارکنان شرکت‌ها، تأمین‌کنندگان مالی، بیمه‌گران، کارشناسان مستقل یا ارائه‌دهندگان خدمات فناوری ممکن است خارج از دایره مستقیم تعهد باقی بمانند، مگر آنکه قرارداد جداگانه‌ای با آنان منعقد شود.



دستورهای دیوان داوری نیز می‌تواند منبع مستقلی برای مدیریت محرمانگی باشد. دیوان بر اساس اختیار اداره رسیدگی می‌تواند از طرفین بخواهد اطلاعات حساس را طبقه‌بندی کنند، دسترسی به برخی اسناد را محدود سازند، نسخه‌های ویرایش‌شده ارائه دهند یا از انتشار محتوای جلسات خودداری کنند. این دستورها به‌ویژه زمانی اهمیت دارند که طرفین در موافقت‌نامه اولیه، جزئیات کافی پیش‌بینی نکرده باشند. دیوان می‌تواند میان حق دفاع و حفاظت از اطلاعات تعادل برقرار کند و برای اسناد بسیار حساس، شیوه‌های دسترسی محدود مانند بررسی فقط توسط وکلاء یا کارشناسان تعیین نماید. باین‌حال، قدرت دیوان برای تحمیل تعهد بر اشخاص ثالث محدود است. اگر ارائه‌دهنده فضای ابری، مترجم یا کارشناس خارج از رابطه قراردادی داوری باشد، اجرای دستور علیه او ممکن است نیازمند موافقت‌نامه جداگانه باشد. ازاین‌رو، مدیریت محرمانگی باید زنجیره کامل اشخاص دارای دسترسی را پوشش دهد.

تعهدات حرفه‌ای و اخلاقی نیز بخشی از شبکه حمایت از محرمانگی را تشکیل می‌دهد. وکلاء معمولاً بر اساس مقررات حرفه‌ای به حفظ اسرار موکل ملزم‌اند، داوران باید اطلاعاتی را که در مقام رسیدگی دریافت کرده‌اند افشا نکنند و کارشناسان و مترجمان نیز ممکن است بر اساس قرارداد یا قواعد حرفه‌ای متعهد باشند. در حوزه میانجیگری، محرمانگی ارتباطات و رفتار اشخاص به‌عنوان یکی از شرایط اعتماد به فرایند مورد توجه قرار گرفته است (Burnley & Lascelles, 2004). تجربه میانجیگری از این جهت برای داوری مفید است که نشان می‌دهد تعهد محرمانگی باید هم محتوای ارتباطات و هم شیوه استفاده بعدی از اطلاعات را در بر گیرد. در بررسی‌های مربوط به محرمانگی میانجیگری نیز بر نقش آن در ایجاد محیطی امن برای گفت‌وگو تأکید شده است (Gurry, 1995). باین‌حال، قواعد حرفه‌ای ممکن است در کشورهای مختلف متفاوت باشند و ضمانت اجرای آن‌ها نیز یکسان نباشد. ازاین‌رو، اتکا به اخلاق حرفه‌ای بدون شرط قراردادی روشن، به‌ویژه در پرونده‌های چندملیتی، حمایت کافی ایجاد نمی‌کند.

از حیث اشخاص، تعهد محرمانگی باید فراتر از طرفین و داوران بررسی شود. وکلاء، مشاوران داخلی شرکت، مدیران، کارکنان واحد مالی و فنی، شهود، کارشناسان، مترجمان، منشیان، کارکنان مؤسسه، متخصصان فناوری اطلاعات، ارائه‌دهندگان خدمات ابری، شرکت‌های ضبط جلسه، تأمین‌کنندگان مالی ثالث و بیمه‌گران ممکن است به تمام یا بخشی از پرونده دسترسی داشته باشند. هرچه فرایند دیجیتالی‌تر می‌شود، تعداد اشخاصی که در نگهداری یا انتقال داده دخالت دارند افزایش می‌یابد. ممکن است طرف اصلی به‌طور کامل به محرمانگی پایبند باشد، اما یکی از پیمانکاران فنی با تنظیمات نادرست، اطلاعات را در دسترس عموم قرار دهد. بنابراین، لازم است اصل دسترسی بر مبنای نیاز رعایت شود؛ یعنی هر شخص فقط به اندازه وظیفه خود به اطلاعات دسترسی داشته باشد. همچنین باید تمام اشخاص پیش از دریافت اطلاعات، تعهدنامه مناسب امضا کنند و پس از پایان نقش خود، دسترسی آنان لغو شود.

از حیث موضوع، محرمانگی می‌تواند وجود خود داوری، نام طرفین، ادعاها، دفاعیات، قرارداد اصلی، اسناد، شهادت‌ها، گزارش کارشناسی، مکاتبات، دستورهای آیینی، مذاکرات سازشی و رأی را در بر گیرد. قلمرو دقیق باید بر اساس ماهیت اطلاعات و هدف حمایت تعیین شود. برخی اطلاعات پیش از داوری نیز عمومی بوده‌اند و صرف ورود آن‌ها به پرونده نباید وضعیتشان را تغییر دهد. برخی اسناد از منبع ثالث به دست آمده‌اند و ممکن است مشمول حقوق یا محدودیت‌های جداگانه باشند. همچنین باید میان اطلاعاتی که طرف خود ایجاد کرده و اطلاعاتی که در جریان افشای اسناد از طرف مقابل دریافت کرده است تمایز قائل شد. استفاده از اطلاعات دریافتی برای اهداف تجاری خارج از داوری، حتی بدون انتشار عمومی، می‌تواند نقض محرمانگی باشد. برای مثال، اگر شرکتی اسناد قیمت‌گذاری رقیب را در داوری دریافت و سپس در مذاکرات بازار از آن استفاده کند، ممنوعیت افشا به‌تنهایی پاسخ‌گو نیست و باید ممنوعیت استفاده ثانویه نیز پیش‌بینی شود.



رای داوری از حساس‌ترین موضوعات محرمانگی است. طرفین ممکن است خواهان عدم انتشار کامل رای باشند، زیرا رای می‌تواند جزئیات قرارداد، عملکرد مالی یا رفتار مدیریتی آنان را آشکار کند. در مقابل، انتشار رای ناشناس‌شده به توسعه رویه داوری، پیش‌بینی‌پذیری و آموزش حقوقی کمک می‌کند. تنش میان محرمانگی و شفافیت در این زمینه آشکار است (Buys, 2003). راه‌حل متعادل می‌تواند انتشار نسخه‌ای باشد که نام‌ها، مشخصات تجاری و اطلاعات شناسایی‌کننده از آن حذف شده است، مشروط بر اینکه ناشناس‌سازی واقعی باشد. در پرونده‌های فناوری یا صنایع محدود، حذف نام طرفین ممکن است برای جلوگیری از شناسایی کافی نباشد، زیرا نوع پروژه، مبلغ یا منطقه جغرافیایی هویت آنان را آشکار می‌کند. بنابراین، تصمیم درباره انتشار باید با ارزیابی خطر شناسایی غیرمستقیم همراه باشد.

تعهد محرمانگی از حیث زمان نیز نیازمند تعیین دقیق است. این تعهد ممکن است از مرحله مذاکرات پیش از داوری آغاز شود و پس از پایان رسیدگی، اجرای رای یا حتی خاتمه قرارداد اصلی ادامه یابد. اطلاعاتی مانند اسرار فنی ممکن است سال‌ها ارزش اقتصادی داشته باشند، درحالی‌که محرمانگی برخی اطلاعات صرفاً تا اعلام عمومی یک رویداد اهمیت دارد. شرطی که همه اطلاعات را برای همیشه محرمانه اعلام کند، ممکن است بیش از حد گسترده و در برخی نظام‌ها غیرقابل اجرا باشد. بهتر است مدت حمایت با توجه به نوع اطلاعات تعیین شود. داده‌های شخصی نیز نباید بیش از مدت لازم نگهداری شوند. در محیط دیجیتال، پایان داوری به معنای پایان خطر نیست، زیرا نسخه‌های پشتیبان، ایمیل‌ها و فایل‌های ذخیره‌شده ممکن است سال‌ها باقی بمانند. از این رو، محرمانگی باید با سیاست نگهداری و حذف داده‌ها تکمیل شود تا تعهد حقوقی در عمل نیز قابل اجرا باشد.

#### چالش‌های ناشی از دیجیتالی‌شدن اسناد و ادله الکترونیکی

ادله الکترونیکی در داوری تجاری بین‌المللی به مجموعه گسترده‌ای از داده‌ها اطلاق می‌شود که به‌صورت دیجیتال ایجاد، ذخیره، پردازش یا منتقل شده‌اند و می‌توانند برای اثبات یا رد یک ادعا مورد استفاده قرار گیرند. ایمیل‌ها، پیام‌های متنی، مکاتبات در برنامه‌های ارتباطی، قراردادهای الکترونیکی، فایل‌های رایانه‌ای، صفحات گسترده، سوابق سامانه‌های مدیریتی، اطلاعات بانکی، تصاویر، فایل‌های صوتی، ویدئوها، داده‌های تلفن همراه، سوابق ورود به سامانه و اطلاعات ذخیره‌شده در فضای ابری از جمله این ادله‌اند. تحول دیجیتال موجب شده است که بسیاری از روابط تجاری بدون تولید نسخه کاغذی شکل بگیرند. در نتیجه، مرجع داوری برای فهم واقعیت اختلاف ناگزیر است به داده‌هایی توجه کند که ماهیت، محل و ساختار آن‌ها با اسناد سنتی تفاوت دارد. حقوق داوری به دلیل انعطاف خود ظرفیت پذیرش انواع جدید دلیل را دارد (Nikbakht, 2023)، اما پذیرش این ادله بدون طراحی قواعد مناسب برای اصالت، دسترسی و محرمانگی می‌تواند خطرهای جدی ایجاد کند.

نخستین ویژگی ادله الکترونیکی، تکثیرپذیری گسترده و تقریباً بدون هزینه آن‌هاست. یک سند کاغذی معمولاً تعداد محدودی نسخه دارد و انتقال آن نیازمند اقدام فیزیکی است، اما یک فایل می‌تواند در چند ثانیه برای صدها شخص ارسال شود. پس از ارسال، فرستنده کنترل مؤثری بر محل ذخیره، تعداد نسخه‌ها یا اشخاصی که بعداً به آن دسترسی پیدا می‌کنند ندارد. حتی اگر دریافت‌کننده فایل را حذف کند، ممکن است نسخه‌ای در سامانه پشتیبان، ایمیل، حافظه موقت یا سرور باقی بماند. این ویژگی، مفهوم استرداد سند را دگرگون می‌کند. در محیط کاغذی، بازگرداندن اصل و نابودکردن نسخه‌ها ممکن بود تا حد زیادی دسترسی را پایان دهد؛ در محیط دیجیتال، حذف کامل نیازمند شناسایی تمام نسخه‌ها و رعایت روش‌های فنی مناسب است. بنابراین، دستور داوری درباره بازگرداندن اطلاعات باید شامل حذف نسخه‌های محلی، ابری و پشتیبان نیز باشد و طرف متعهد باید درباره انجام آن تأییدیه ارائه دهد.

دومین ویژگی، پراکندگی مکانی داده‌هاست. یک سند ممکن است در رایانه کارمند شرکت ایجاد، از طریق سرور کشوری دیگر ارسال، در فضای ابری منطقه‌ای متفاوت ذخیره و توسط وکیل مستقر در کشور سوم بررسی شود. این پراکندگی باعث می‌شود قوانین چند حوزه قضایی به‌طور هم‌زمان بر داده اعمال شوند. قانون مقر دآوری ممکن است محرمانگی را به رسمیت بشناسد، اما قانون محل سرور به مقامات عمومی اجازه دسترسی دهد. همچنین ممکن است انتقال داده‌های شخصی از یک کشور به کشور دیگر نیازمند شرایط خاص باشد. در نتیجه، طرفین نمی‌توانند صرفاً با انتخاب قانون حاکم بر قرارداد، تمام مسائل مربوط به اطلاعات دیجیتال را حل کنند. تحلیل‌های مربوط به قانون حاکم در دآوری نشان می‌دهد که روابط دآوری می‌تواند تحت تأثیر چند دسته قواعد قرار گیرد (Johar, 2024). این چندلایگی در محیط دیجیتال تشدید می‌شود، زیرا داده برخلاف سند فیزیکی ممکن است هم‌زمان در چند قلمرو وجود داشته باشد.

سومین ویژگی، وجود فراداده‌هاست. فراداده اطلاعاتی است که درباره خود فایل ارائه می‌شود، مانند نام نویسنده، تاریخ ایجاد، زمان ویرایش، تاریخچه تغییرات، نام دستگاه، محل جغرافیایی، مسیر ذخیره و مشخصات نرم‌افزار. فراداده می‌تواند در اثبات اصالت سند یا ترتیب زمانی رویدادها بسیار ارزشمند باشد، اما در عین حال ممکن است اطلاعات محرمانه‌ای را آشکار کند که در متن ظاهری سند دیده نمی‌شود. برای مثال، تاریخچه ویرایش یک پیش‌نویس ممکن است نام مشاور حقوقی، نظرات داخلی یا راهبرد مذاکرات را نشان دهد. حذف فراداده پیش از ارائه سند می‌تواند از افشای ناخواسته جلوگیری کند، اما اگر فراداده برای اثبات اصالت لازم باشد، حذف آن ممکن است ارزش دلیل را کاهش دهد. دیوان دآوری باید میان حفظ تمامیت دلیل و جلوگیری از افشای اطلاعات نامرتبط تعادل برقرار کند. بهترین شیوه آن است که طرفین پیشاپیش درباره نوع فراداده قابل ارائه، روش استخراج و امکان ویرایش اطلاعات ممتاز یا غیرمرتبط توافق کنند.

چالش دیگر، حجم عظیم داده‌ها در افشای الکترونیکی است. در اختلافات پیچیده، یک شرکت ممکن است میلیون‌ها ایمیل، پیام و فایل مرتبط با دوره زمانی مورد اختلاف داشته باشد. بررسی دستی این حجم عملاً ناممکن یا بسیار پرهزینه است. در نتیجه، طرفین از جست‌وجوی کلیدواژه‌ای، فیلترهای زمانی، ابزارهای تحلیل خودکار و فناوری‌های پیش‌بینی ارتباط استفاده می‌کنند. این ابزارها سرعت را افزایش می‌دهند، اما احتمال ارائه اطلاعات نامرتبط یا محرمانه را نیز به همراه دارند. هرچه دامنه درخواست افشا گسترده‌تر باشد، احتمال ورود اسرار تجاری، داده‌های شخصی و ارتباطات ممتاز به پرونده بیشتر می‌شود. قواعد عمومی آیین دآوری بر تناسب، ارتباط و ضرورت درخواست‌های سند تأکید دارند (Redfern & Hunter, 2023). در محیط دیجیتال، اصل تناسب باید با جدیت بیشتری اعمال شود، زیرا هزینه و خطر افشای گسترده داده‌ها می‌تواند از ارزش اثباتی آن‌ها بیشتر باشد.

یکی از مسائل مهم، افشای ناخواسته اسناد ممتاز یا محرمانه است. ممکن است در میان هزاران فایل، ایمیلی میان شرکت و وکیل آن وجود داشته باشد که به دلیل خطای فنی یا انسانی ارائه شود. در چنین وضعیتی، باید مشخص باشد آیا ارائه ناخواسته به معنای اسقاط حمایت است یا طرف دریافت‌کننده موظف به توقف بررسی و بازگرداندن فایل است. پروتکل افشای الکترونیکی باید سازوکاری برای اعلام سریع، جداسازی، حذف و حل اختلاف درباره این اسناد داشته باشد. بدون چنین سازوکاری، یک خطای ساده می‌تواند راهبرد کامل حقوقی طرف را در اختیار رقیب قرار دهد. محرمانگی در اینجا با اصل انصاف آیینی پیوند می‌خورد؛ طرفی که آشکارا متوجه ارائه اشتباه سند ممتاز شده است نباید از خطا سوءاستفاده کند. دیوان نیز می‌تواند استفاده از سند را ممنوع و نسخه‌های آن را حذف کند.

ذخیره‌سازی ابری مزایای قابل توجهی برای دآوری دارد. طرفین و داوران می‌توانند از نقاط مختلف به پرونده دسترسی پیدا کنند، نسخه‌های واحدی از اسناد را مشاهده نمایند و از ارسال فایل‌های حجیم از طریق ایمیل خودداری کنند. با این حال، امنیت فضای ابری به نحوه طراحی و

مدیریت ارائه‌دهنده بستگی دارد. اگر رمزگذاری مناسب نباشد، رمز عبور ضعیف انتخاب شود یا دسترسی کاربر سابق لغو نگردد، اطلاعات در معرض خطر قرار می‌گیرد. همچنین برخی ارائه‌دهندگان ممکن است داده‌ها را در چندین کشور ذخیره کنند یا از پیمانکاران فرعی استفاده نمایند. طرفین باید بدانند اطلاعات دقیقاً در کجا نگهداری می‌شود، چه اشخاصی به آن دسترسی فنی دارند و پس از پایان قرارداد چگونه حذف خواهد شد. استفاده از فضای ابری عمومی بدون بررسی شرایط خدمات، با تعهد حرفه‌ای به محرمانگی سازگار نیست. قرارداد با ارائه‌دهنده باید شامل محدودیت استفاده از داده، تعهد گزارش رخداد امنیتی، الزامات رمزگذاری و ممنوعیت انتقال اطلاعات به اشخاص ثالث بدون اجازه باشد.

حملات سایبری یکی از جدی‌ترین تهدیدها علیه داورهای تجاری بین‌المللی است. پرونده‌های داور می‌تواند شامل اطلاعاتی با ارزش اقتصادی بسیار بالا باشند و برای رقبای دولت‌ها، مجرمان سایبری یا اشخاص ذی‌نفع جذابیت داشته باشند. حملات فیشینگ می‌تواند اطلاعات ورود وکیل یا داور را سرقت کند، بدافزار می‌تواند فایل‌ها را استخراج نماید و حملات باج‌افزاری ممکن است دسترسی به پرونده را مختل سازد. تهدید همیشه خارجی نیست؛ کارمند ناراضی، پیمانکار سابق یا کاربری با دسترسی بیش از نیاز نیز می‌تواند منبع نشت باشد. امنیت سایبری باید به‌عنوان بخشی از مدیریت پرونده تلقی شود، نه موضوعی صرفاً فنی. دیوان داور و مؤسسه باید در آغاز رسیدگی، سطح حساسیت اطلاعات و احتمال تهدید را ارزیابی کنند. پرونده‌ای درباره فناوری نظامی، انرژی، زیرساخت یا اطلاعات شخصی گسترده، به تدابیری متفاوت از اختلافی محدود درباره پرداخت نیاز دارد.

جلسات استماع مجازی نیز شکل جدیدی از خطر را ایجاد کرده‌اند. در جلسه حضوری، کنترل ورود اشخاص و محیط فیزیکی آسان‌تر است، اما در جلسه آنلاین ممکن است فردی خارج از دید دوربین در اتاق حضور داشته باشد یا ارتباط از طریق دستگاهی ناامن برقرار شود. شرکت‌کننده می‌تواند بدون اطلاع دیگران صدا یا تصویر را ضبط کند و فایل ضبط‌شده ممکن است در فضای ابری پلتفرم ذخیره شود. اشتراک‌گذاری صفحه نیز خطر نمایش ناخواسته ایمیل‌ها، اعلان‌ها یا اسناد دیگر را به همراه دارد. برای کاهش این خطرها باید احراز هویت شرکت‌کنندگان، استفاده از اتاق انتظار، محدودیت ورود، رمزگذاری ارتباط، کنترل ضبط و تعیین قواعد روشن برای محل حضور شاهد پیش‌بینی شود. هر شرکت‌کننده باید تأیید کند که شخص غیرمجاز در محیط او حضور ندارد و از ضبط مستقل خودداری می‌کند. اگر ضبط رسمی لازم باشد، محل ذخیره، مدت نگهداری و اشخاص دارای دسترسی باید مشخص شود.

وضعیت شهود در جلسات مجازی چالش ویژه‌ای دارد. در جلسه حضوری، می‌توان تا حد زیادی اطمینان یافت که شاهد از کمک پنهانی استفاده نمی‌کند، اما در محیط مجازی ممکن است پیام‌هایی بر صفحه دیگر دریافت کند یا شخصی خارج از دوربین او را راهنمایی نماید. این موضوع نه تنها بر اعتبار شهادت، بلکه بر محرمانگی نیز اثر دارد، زیرا اشخاص ناشناس ممکن است محتوای جلسه و اسناد را مشاهده کنند. دیوان می‌تواند از شاهد بخواهد دوربین را به‌گونه‌ای تنظیم کند که محیط مشخص باشد، تلفن همراه را کنار بگذارد، صفحه نمایش را به اشتراک بگذارد یا تأیید کند تنهاست. با این حال، این اقدامات باید با حریم خصوصی شاهد متناسب باشند. هدف، ایجاد نظارت نامحدود نیست، بلکه تضمین تمامیت رسیدگی و جلوگیری از دسترسی اشخاص غیرمجاز است.

استفاده از هوش مصنوعی در داور فرصت‌ها و مخاطرات هم‌زمانی ایجاد کرده است. ابزارهای هوشمند می‌توانند اسناد را طبقه‌بندی، زبان‌ها را ترجمه، اطلاعات تکراری را حذف، موضوعات را استخراج و جست‌وجوی حقوقی را تسریع کنند. با این حال، زمانی که اطلاعات پرونده به سامانه‌ای خارجی داده می‌شود، ممکن است نسخه‌ای از آن برای مدت نامعلوم ذخیره شود یا برای بهبود خدمت مورد استفاده قرار گیرد.

کاربران معمولاً شرایط فنی و قراردادی این سامانه‌ها را به‌دقت مطالعه نمی‌کنند. ورود متن لوایح، قراردادها یا گزارش‌های کارشناسی به ابزار عمومی هوش مصنوعی می‌تواند نقض تعهد محرمانگی باشد، حتی اگر خروجی فقط توسط کاربر مشاهده شود. در حوزه قراردادهای هوشمند نیز مسائل مربوط به داده‌های زنجیره‌ای و سازوکارهای حل اختلاف فناوریانه مورد توجه قرار گرفته است (Haddadi, 2024). این تحولات نشان می‌دهد که استفاده از فناوری باید بر اساس رضایت آگاهانه، ارزیابی خطر و محدودیت قراردادی انجام شود. سامانه‌ای که برای داده‌های محرمانه استفاده می‌شود باید تضمین کند اطلاعات برای آموزش عمومی مدل، تبلیغات یا اهداف ثانویه به کار نمی‌رود.

ادله مبتنی بر زنجیره بلوکی چالش متفاوتی دارند. یکی از ویژگی‌های زنجیره بلوکی، ماندگاری و دشواری تغییر داده ثبت‌شده است. این ویژگی می‌تواند برای اثبات زمان یا اصالت تراکنش مفید باشد، اما با حق حذف یا محدودکردن انتشار اطلاعات تعارض پیدا می‌کند. اگر اطلاعات محرمانه مستقیماً در زنجیره عمومی ثبت شده باشد، حذف آن عملاً ممکن نیست. حتی استفاده از نام مستعار همیشه مانع شناسایی نمی‌شود، زیرا الگوی تراکنش‌ها می‌تواند هویت اشخاص را آشکار کند. در قراردادهای هوشمند، بخشی از اجرای تعهد ممکن است خودکار باشد و اختلاف درباره داده‌هایی شکل گیرد که در شبکه‌ای توزیع شده وجود دارند. تحلیل چالش‌های داوری در قراردادهای هوشمند نشان می‌دهد که تفکیک میان حل اختلاف درون زنجیره و بیرون از زنجیره اهمیت دارد (Haddadi, 2024). برای حفظ محرمانگی باید از ثبت مستقیم اطلاعات حساس در شبکه عمومی خودداری و تنها اثر رمزنگاری‌شده یا شناسه لازم ثبت شود.

حفاظت از داده‌های شخصی نیز بخش مهمی از محرمانگی دیجیتال است. پرونده داوری ممکن است شامل نام، نشانی، اطلاعات شغلی، سوابق مالی، داده‌های سلامت، مکاتبات شخصی یا ارزیابی عملکرد کارکنان باشد. این اطلاعات ممکن است به اشخاصی تعلق داشته باشد که طرف داوری نیستند. وجود تعهد محرمانگی میان طرفین، لزوماً تمام الزامات مربوط به پردازش قانونی داده شخصی را تأمین نمی‌کند. باید هدف جمع‌آوری مشخص باشد، داده اضافی حذف شود، دسترسی محدود گردد و مدت نگهداری متناسب باشد. اگر ارائه یک سند مستلزم افشای اطلاعات شخص ثالث است، می‌توان بخش‌های نامرتبط را پوشاند یا از شناسه‌های جایگزین استفاده کرد. در عین حال، ویرایش نباید به‌گونه‌ای باشد که طرف مقابل نتواند اصالت یا زمینه سند را بررسی کند. دیوان باید میان حق دفاع و حداقل‌سازی داده تعادل برقرار سازد.

اصالت و تمامیت ادله الکترونیکی نیز با محرمانگی پیوند مستقیم دارد. هرچه دسترسی به فایل محدودتر شود، ممکن است بررسی اصالت آن دشوارتر گردد. طرفی که به سند استناد می‌کند باید بتواند نشان دهد فایل از منبع معتبر به دست آمده، تغییر نکرده و زنجیره نگهداری آن مشخص است. استفاده از مقادیر هش، امضای دیجیتال، ثبت زمان و گزارش دسترسی می‌تواند به اثبات تمامیت کمک کند. باین‌حال، انتشار گسترده نسخه اصلی برای همه اشخاص ممکن است خطر افشا را افزایش دهد. راه‌حل می‌تواند ایجاد نسخه بررسی‌شده در محیط کنترل‌شده باشد؛ به‌گونه‌ای که طرف مقابل و کارشناس امکان ارزیابی داشته باشند، اما نتوانند فایل را خارج کنند یا تکثیر نمایند. اتاق داده مجازی با ثبت فعالیت کاربران در این زمینه مفید است، مشروط بر اینکه خود سامانه از امنیت کافی برخوردار باشد.

افشای اطلاعات از طریق اشتباه‌های ساده انسانی نیز نباید نادیده گرفته شود. ارسال ایمیل به مخاطب اشتباه، استفاده از رمز عبور تکراری، اتصال به شبکه عمومی، گم‌شدن لپ‌تاپ، باقی‌ماندن فایل روی حافظه قابل حمل یا اشتراک‌گذاری پیوند بدون محدودیت، از رایج‌ترین علل نقض داده‌اند. پیچیده‌ترین سامانه امنیتی نیز بدون آموزش کاربران کارآمد نیست. وکلاء، داوران، کارشناسان و کارکنان باید درباره شناسایی پیام‌های جعلی، مدیریت رمز عبور، ذخیره امن، استفاده از دستگاه شخصی و گزارش فوری رخداد آموزش ببینند. محرمانگی دیجیتال زمانی

تحقق می‌یابد که رفتار انسانی، قرارداد حقوقی و ابزار فنی در یک چارچوب هماهنگ قرار گیرند. صرف درج عبارت «محرمانه» بر روی سند یا استفاده از یک سامانه پیشرفته، بدون فرهنگ امنیتی و مسئولیت‌پذیری کاربران کافی نخواهد بود.

چالش نهایی، تعیین مسئولیت در زنجیره پیچیده پردازش اطلاعات است. اگر داده از طریق سامانه مؤسسه نشت کند، آیا مؤسسه مسئول است یا ارائه‌دهنده فناوری؟ اگر وکیل از ابزار عمومی هوش مصنوعی استفاده کند، مسئولیت متوجه اوست یا شرکت سازنده؟ اگر داور از رایانه شخصی ناامن استفاده کند و پرونده مورد حمله قرار گیرد، مصونیت داور تا چه اندازه قابل استناد است؟ پاسخ به این پرسش‌ها نیازمند بررسی قراردادهای، استاندارد مراقبت، رابطه سببیت و قواعد آمره است. در محیط دیجیتال، مسئولیت نباید تنها بر افشای عمدی متمرکز باشد. بی‌احتیاطی در انتخاب سامانه، عدم به‌روزرسانی نرم‌افزار، نادیده‌گرفتن هشدار امنیتی یا اعطای دسترسی بیش از حد نیز می‌تواند نقض تعهد مراقبت محسوب شود. بنابراین، تحول فناوری مفهوم تقصیر را نیز تغییر داده و استاندارد رفتار متعارف را به سطحی بالاتر منتقل کرده است.

### استثنائات، مسئولیت‌ها و راهکارهای حمایت از محرمانگی دیجیتال

محرمانگی در داور تجاری بین‌المللی اصلی نسبی است و نمی‌تواند بدون توجه به حقوق دفاعی، الزامات قانونی، اجرای رأی و منافع عمومی اعمال شود. پذیرش محرمانگی مطلق ممکن است به پنهان‌ماندن رفتارهای غیرقانونی، جلوگیری از نظارت قضایی یا تضییع حقوق اشخاص ثالث منجر شود. از سوی دیگر، توسعه بی‌ضابطه استثنائات نیز اعتماد فعالان تجاری به داور را تضعیف می‌کند. راه‌حل مناسب، شناسایی اصل محرمانگی همراه با استثنائات محدود، ضروری و متناسب است. هر افشا باید برای هدفی مشروع انجام شود و دامنه آن از حد لازم فراتر نرود. این رویکرد با تنشی که میان محرمانگی و شفافیت در داور وجود دارد سازگار است (Buys, 2003). به‌جای انتخاب یکی از دو ارزش به‌صورت مطلق، باید بر اساس نوع اختلاف، ماهیت اطلاعات، جایگاه اشخاص و هدف افشا تعادل ایجاد شود.

نخستین استثنا، رضایت طرفین است. چون مبنای اصلی داور توافقی است، طرفین می‌توانند درباره انتشار یا استفاده از اطلاعات نیز توافق کنند. این رضایت ممکن است از ابتدا در قرارداد یا پس از بروز اختلاف داده شود. باین‌حال، رضایت باید روشن و محدود به موضوع مشخص باشد. موافقت با انتشار نتیجه داور به معنای رضایت به انتشار تمام اسناد یا مذاکرات نیست. همچنین یک طرف نمی‌تواند به‌تنهایی اطلاعاتی را منتشر کند که شامل اسرار یا داده‌های شخصی طرف دیگر است، مگر آنکه شرط داور چنین اختیاری بدهد یا قانون اجازه دهد. در شرکت‌های گروهی نیز رضایت شرکت مادر لزوماً به معنای رضایت شرکت تابعه نیست. بنابراین، پیش از انتشار باید هویت صاحب اطلاعات و حدود اختیار شخص رضایت‌دهنده بررسی شود.

الزام قانونی یکی دیگر از استثنائات مهم است. شرکت‌های پذیرفته‌شده در بازار سرمایه ممکن است ملزم باشند دعاوی بااهمیت یا آثار مالی رأی را اعلام کنند. مؤسسات مالی و شرکت‌های بیمه ممکن است تکالیف نظارتی داشته باشند و مراجع مالیاتی یا حسابرسی نیز می‌توانند اطلاعات مربوط به اختلاف را مطالبه کنند. در چنین مواردی، شرط محرمانگی نمی‌تواند مانع اجرای قانون شود. باین‌حال، طرف متعهد باید تنها اطلاعات ضروری را افشا کند، در صورت امکان از مرجع دریافت‌کننده درخواست رفتار محرمانه نماید و طرف دیگر را پیشاپیش مطلع سازد. اگر قانون افشای نتیجه مالی را ضروری می‌داند، ممکن است انتشار متن کامل رأی لازم نباشد. اصل حداقل افشا می‌تواند تعارض میان تکلیف قانونی و حمایت از اطلاعات را کاهش دهد.

رسیدگی‌های قضایی مرتبط با داور نیز ممکن است افشا را اجتناب‌ناپذیر سازد. درخواست تعیین داور، صدور دستور موقت، الزام به ارائه سند، ابطال رأی یا شناسایی و اجرای آن معمولاً مستلزم ارائه بخشی از پرونده به دادگاه است. نظام داور هرچند از استقلال نسبی برخوردار

است، برای برخی اقدامات به حمایت دادگاه‌های ملی نیاز دارد. ادبیات داوری بر نقش دادگاه‌ها در پشتیبانی و نظارت محدود بر فرایند تأکید دارد (Fouchard et al., 2024). ارائه رأی به دادگاه ممکن است آن را وارد پرونده عمومی کند. طرفی که خواهان حفظ محرمانگی است باید در صورت امکان از دادگاه درخواست مهر و موم پرونده، جلسه غیرعلنی یا حذف اطلاعات حساس نماید. البته دادگاه بر اساس قانون خود تصمیم می‌گیرد و توافق خصوصی طرفین الزاماً بر اصل علنی بودن دادرسی غلبه نمی‌کند.

اجرای آرای خارجی نیز نمونه‌ای روشن از ضرورت افشاست. طرف برنده برای شناسایی و اجرا باید رأی، موافقت‌نامه داوری و گاه اسناد تکمیلی را ارائه کند. مطالعه نظام‌های مختلف اجرای آرای تجاری نشان می‌دهد که قواعد داخلی می‌توانند بر نحوه برخورد با اسناد داوری اثر بگذارند (Tahir, 2023). در برخی کشورها، پرونده اجرای رأی عمومی است و در برخی دیگر امکان محدود کردن دسترسی وجود دارد. بنابراین، پیش از آغاز دعوای اجرا باید ارزیابی شود که کدام اطلاعات واقعاً لازم است و آیا می‌توان نسخه ویرایش‌شده ارائه کرد. طرفین همچنین می‌توانند در شرط محرمانگی پیش‌بینی کنند که افشای لازم برای اجرا مجاز است، مشروط بر اینکه اقدامات معقول برای محدود کردن دسترسی انجام شود.

حمایت از حق دفاع نیز می‌تواند افشا را توجیه کند. ممکن است یک طرف برای دفاع در دعوایی دیگر، اثبات تقلب، پاسخ به ادعای مسئولیت مدیران یا مطالبه خسارت از بیمه‌گر نیازمند استفاده از اطلاعات داوری باشد. ممنوعیت مطلق استفاده می‌تواند دسترسی به عدالت را مختل کند. با این حال، صرف مفید بودن اطلاعات کافی نیست؛ افشا باید واقعاً ضروری باشد و راه جایگزین کم‌خطر وجود نداشته باشد. مرجع تصمیم‌گیر باید میان ارزش محرمانگی و اهمیت حق مورد دفاع تعادل برقرار کند. استفاده در پرونده‌ای دیگر نیز باید در حد لازم محدود شود و در صورت امکان تحت دستور حفاظتی قرار گیرد. این تحلیل با مفهوم محرمانگی در سایر روش‌های حل اختلاف نیز سازگار است، زیرا در میانجیگری نیز استثنائات مربوط به اجرای توافق یا جلوگیری از بی‌عدالتی مطرح می‌شود (Burnley & Lascelles, 2004).

منافع عمومی و نظم عمومی از پیچیده‌ترین استثنائات‌اند. اگر اختلاف با فساد، پول‌شویی، امنیت ملی، سلامت عمومی، محیط‌زیست یا استفاده از اموال عمومی ارتباط داشته باشد، حفظ کامل محرمانگی ممکن است قابل دفاع نباشد. نقش نظم عمومی و امنیت ملی در محدود کردن آزادی طرفین در داوری مورد توجه قرار گرفته است (Shahheidari, 2024). با این حال، استناد کلی به منافع عمومی نباید بهانه‌ای برای انتشار نامحدود اطلاعات تجاری شود. باید ارتباط واقعی میان اطلاعات و منفعت عمومی وجود داشته باشد. اگر تنها بخش کوچکی از پرونده به موضوع عمومی مربوط است، افشا باید به همان بخش محدود شود. در اختلافات سرمایه‌گذاری نیز گرایش به شفافیت بیشتر شده است و انتظار سرمایه‌گذاران خارجی نسبت به محرمانگی با نیاز به پاسخ‌گویی عمومی مورد بازنگری قرار گرفته است (Khan, 2020). هرچند داوری تجاری خصوصی با داوری سرمایه‌گذاری تفاوت دارد، تجربه اخیر نشان می‌دهد که محرمانگی مطلق در موضوعات دارای آثار عمومی روزبه‌روز دشوارتر توجیه می‌شود.

از حیث مسئولیت، نخستین گروه متعهد خود طرفین هستند. هر طرف باید ساختار داخلی مناسبی برای مدیریت اطلاعات پرونده ایجاد کند. تعیین مدیر پرونده، شناسایی کاربران مجاز، طبقه‌بندی اسناد، آموزش کارکنان و لغو دسترسی پس از پایان نقش از اقدامات ضروری است. شرکت نمی‌تواند با استناد به رفتار مستقل کارمند از مسئولیت رها شود، اگر دسترسی بدون کنترل یا آموزش مناسب اعطا شده باشد. همچنین استفاده از دستگاه شخصی، ایمیل عمومی یا حافظه قابل حمل باید تحت سیاست مشخص قرار گیرد. در شرکت‌های بزرگ، اطلاعات ممکن

است میان واحد حقوقی، مالی، فنی و مدیریتی گردش کند. اصل دسترسی بر اساس نیاز باید مانع آن شود که هر کارمند صرفاً به دلیل عضویت در سازمان به کل پرونده دسترسی داشته باشد.

وکلاء و مشاوران حقوقی نیز مسئولیت ویژه‌ای دارند. آنان علاوه بر تعهد حرفه‌ای، معمولاً مدیریت اصلی اسناد و ارتباط با دیوان را بر عهده دارند. انتخاب سامانه ناامن، ارسال فایل بدون رمزگذاری یا استفاده از ابزار عمومی هوش مصنوعی می‌تواند تخلف از استاندارد مراقبت حرفه‌ای تلقی شود. وکیل باید درباره نحوه ذخیره و انتقال اطلاعات با موکل توافق کند و خطرهای فناوری را برای او توضیح دهد. در پرونده‌هایی که چند دفتر حقوقی همکاری می‌کنند، باید مشخص باشد هر دفتر چه سطحی از دسترسی دارد و مسئول گزارش رخداد کیست. تعهد محرمانگی نباید تنها در قرارداد وکالت کلی باقی بماند، بلکه باید با سیاست‌های اجرایی و فنی همراه شود.

داوران نیز نه فقط به عدم افشای عمدی، بلکه به مدیریت ایمن اطلاعات ملزم‌اند. داوری که اسناد را در رایانه فاقد رمزگذاری نگهداری می‌کند یا از شبکه عمومی برای دسترسی به پرونده استفاده می‌نماید، ممکن است استاندارد مراقبت متعارف را رعایت نکرده باشد. آثار عمومی داوری بر وظیفه دیوان در اداره منصفانه و مؤثر رسیدگی تأکید می‌کنند (Redfern & Hunter, 2023). در عصر دیجیتال، اداره مؤثر شامل انتخاب روش امن ارتباط و کنترل دسترسی نیز می‌شود. مسئله مصونیت داوران می‌تواند مسئولیت مستقیم آنان را محدود کند، اما نباید به معنای فقدان هرگونه پاسخ‌گویی باشد. مؤسسات داوری می‌توانند استانداردهای امنیتی اجباری برای داوران تعیین کنند و نقض جدی را در ارزیابی حرفه‌ای آنان در نظر بگیرند.

مؤسسات داوری نقش مرکزی در حفاظت از داده‌ها دارند، زیرا غالباً سامانه ثبت پرونده، ارتباطات، پرداخت‌ها و آرشیو را مدیریت می‌کنند. مؤسسه باید معماری امنیتی مناسبی داشته باشد، دسترسی کارکنان را محدود کند، پیمانکاران فناوری را ارزیابی نماید و برنامه واکنش به رخداد تدوین کند. اگر سامانه مؤسسه مورد نفوذ قرار گیرد، صرف درج شرط سلب مسئولیت نباید همیشه آن را از پاسخ‌گویی معاف کند. استاندارد مسئولیت باید بر اساس اهمیت اطلاعات، امکان پیش‌بینی خطر، اقدامات متعارف صنعت و رابطه سببیت تعیین شود. مؤسسه همچنین باید سیاست روشنی درباره مدت نگهداری پرونده، انتشار آرای ناشناس شده و انتقال اطلاعات به کشور دیگر داشته باشد. اعتماد به مؤسسه تا حد زیادی به شفافیت آن درباره این سیاست‌ها وابسته است.

ارائه‌دهندگان خدمات فناوری گروه دیگری از مسئولان بالقوه‌اند. شرکت‌های میزبانی ابری، پلتفرم‌های ویدئویی، خدمات ترجمه ماشینی، سامانه‌های مدیریت اسناد و ابزارهای هوش مصنوعی ممکن است به داده‌های بسیار حساس دسترسی داشته باشند. قرارداد با آنان باید تعهد محرمانگی دقیق، ممنوعیت استفاده ثانویه، استاندارد رمزگذاری، محل ذخیره، شرایط استفاده از پیمانکار فرعی، زمان گزارش نقض و شیوه حذف داده را مشخص کند. همچنین باید معلوم باشد در صورت وقوع رخداد، ارائه‌دهنده چه همکاری‌ای برای تحقیق، بازایی و اطلاع‌رسانی انجام خواهد داد. انتخاب ارائه‌دهنده صرفاً بر اساس هزینه یا سهولت استفاده با الزامات داوری‌های حساس سازگار نیست. ارزیابی سابقه امنیتی، گواهی‌های فنی و توان پاسخ‌گویی باید بخشی از تصمیم باشد.

ضمانت اجرای نقض محرمانگی می‌تواند قراردادی، مدنی، آیینی، انتظامی و در برخی موارد کیفری باشد. اگر شرط محرمانگی نقض شود، زیان‌دیده می‌تواند خسارت مطالبه کند، اما اثبات میزان زیان ناشی از افشای اطلاعات دشوار است. از این‌رو، درج وجه التزام متناسب ممکن است مفید باشد، هرچند مبلغ نامعقول ممکن است در برخی نظام‌ها تعدیل شود. دیوان داوری می‌تواند هزینه‌ها را علیه طرف متخلف تخصیص دهد، استفاده از سند تحصیل‌شده به‌طور نامشروع را ممنوع کند یا دستور حذف و استرداد اطلاعات بدهد. در موارد فوری، دستور منع افشا



اهمیت زیادی دارد، زیرا خسارت مالی پس از انتشار ممکن است جبران کامل ایجاد نکند. اگر وکیل یا کارشناس تعهد حرفه‌ای را نقض کرده باشد، مسئولیت انتظامی نیز ممکن است مطرح شود. افشای داده‌های شخصی یا اسرار تجاری نیز می‌تواند ضمانت اجرای مستقل قانونی داشته باشد.

مؤثرترین ابزار پیشگیرانه، تنظیم شرط جامع محرمانگی دیجیتال است. این شرط باید اطلاعات محرمانه را تعریف کند، اما تعریف نباید چنان گسترده باشد که هر داده عمومی یا مستقل را شامل شود. اشخاص مجاز، هدف مجاز استفاده، روش‌های انتقال، سامانه‌های قابل قبول، ممنوعیت استفاده از ابزارهای عمومی، شرایط افشا به بیمه‌گر یا تأمین‌کننده مالی، مدت نگهداری و شیوه حذف باید مشخص گردد. همچنین لازم است استثنائات قانونی، فرایند اطلاع‌رسانی پیش از افشا و مرجع حل اختلاف درباره محرمانگی تعیین شود. در قراردادهای پیچیده، شرط باید شامل تعهد طرفین به تحمیل همان سطح از محرمانگی بر کارکنان، مشاوران و پیمانکاران خود باشد. شرطی که تنها بگوید «داوری محرمانه است» برای محیط دیجیتال کافی نیست، زیرا درباره نحوه رفتار عملی با داده‌ها راهنمایی نمی‌دهد.

پروتکل امنیت سایبری باید در آغاز رسیدگی و متناسب با خطر پرونده تدوین شود. این پروتکل می‌تواند بخشی از نخستین دستور آیینی دیوان باشد. طرفین باید نوع داده‌ها، حجم اسناد، کشورهای محل حضور کاربران، فناوری مورد استفاده و سطح حساسیت اطلاعات را اعلام کنند. بر اساس این ارزیابی، روش احراز هویت، استاندارد رمزگذاری، سامانه تبادل فایل، سیاست رمز عبور، شیوه تهیه نسخه پشتیبان و فرایند گزارش رخداد تعیین می‌شود. استفاده از احراز هویت چندمرحله‌ای، دسترسی مبتنی بر نقش، ثبت رویدادها و محدودیت دانلود از عناصر اساسی است. پروتکل باید مسئول هر اقدام و مهلت گزارش نقض را روشن سازد. گزارش سریع اهمیت دارد، زیرا امکان تغییر رمزها، مسدودکردن حساب و جلوگیری از گسترش خسارت را فراهم می‌کند.

اتاق داده مجازی یکی از ابزارهای عملی برای مدیریت اسناد حساس است. این سامانه می‌تواند امکان مشاهده بدون دانلود، درج علامت شناسایی روی نسخه، ثبت زمان ورود، محدودکردن چاپ و لغو دسترسی را فراهم کند. برای اسناد بسیار محرمانه، دسترسی می‌تواند فقط به وکلاء یا کارشناسان مستقل داده شود. بااین‌حال، استفاده از اتاق داده باید با بررسی امنیت ارائه‌دهنده همراه باشد. اگر کاربران بتوانند با گرفتن تصویر صفحه یا استفاده از دستگاه خارجی نسخه‌برداری کنند، حفاظت کامل ممکن نیست. بنابراین، ابزار فنی باید با تعهد قراردادی و نظارت تکمیل شود. در موارد حساس، می‌توان دسترسی را در محیط فیزیکی کنترل‌شده یا دستگاه اختصاصی فراهم کرد.

ناشناس‌سازی و ویرایش اطلاعات نیز نقش مهمی دارند. اطلاعات شخصی یا تجاری که برای تصمیم‌گیری ضروری نیست باید پیش از ارائه حذف شود. بااین‌حال، ویرایش باید قابل‌بررسی باشد و نباید بخش‌هایی را پنهان کند که برای فهم زمینه لازم‌اند. طرف ارائه‌دهنده می‌تواند فهرستی از دلایل ویرایش تهیه کند و در صورت اختلاف، نسخه کامل را فقط در اختیار دیوان قرار دهد. انتشار آرای داوری نیز باید با ارزیابی خطر شناسایی غیرمستقیم همراه باشد. حذف نام‌ها کافی نیست اگر صنعت، مبلغ، محل پروژه یا ساختار قرارداد هویت طرفین را آشکار کند. تنش میان توسعه رویه و حمایت از اطلاعات باید از طریق ناشناس‌سازی واقعی و اخذ نظر طرفین مدیریت شود.

سیاست نگهداری و حذف داده‌ها بخش پایانی چرخه حفاظت است. بسیاری از نقض‌ها سال‌ها پس از پایان پرونده رخ می‌دهند، زیرا اطلاعات در سامانه‌های قدیمی یا حساب‌های بلااستفاده باقی مانده‌اند. طرفین، وکلاء، داوران و مؤسسه باید تعیین کنند چه اسنادی برای چه مدتی نگهداری می‌شود و پس از آن چگونه حذف خواهد شد. برخی اطلاعات ممکن است برای دفاع در دعوای آتی یا اجرای رأی لازم باشند، اما

نگهداری نامحدود همه داده‌ها توجیه ندارد. نسخه‌های پشتیبان نیز باید در سیاست حذف لحاظ شوند. در پایان داور، هر شخص باید دسترسی کاربران غیرضروری را لغو و تجهیزات قرضی را پاک‌سازی کند. تأیید کتبی حذف می‌تواند بخشی از تعهد قراردادی باشد. از منظر تقنینی و نهادی، لازم است قوانین و قواعد داور به‌صراحت رابطه میان محرمانگی و امنیت دیجیتال را شناسایی کنند. بیان کلی محرمانه‌بودن کافی نیست و باید حداقل وظایف مربوط به مراقبت، گزارش رخداد، استفاده از ارائه‌دهندگان ثالث و مسئولیت ناشی از بی‌احتیاطی مشخص شود. نظام‌های حقوقی مختلف در توسعه داور تجاری و اجرای آرای خارجی رویکردهای متفاوتی دارند (Fallah, 2024) و همین تنوع ضرورت تنظیم قراردادی دقیق را افزایش می‌دهد. توسعه فرهنگ داور و اعتماد تجاری نیز بدون تضمین امنیت اطلاعات کامل نخواهد بود (Haqmal, 2024). آموزش داوران و وکلاء، انتشار الگوهای پروتکل امنیتی، ارزیابی دوره‌ای سامانه‌های مؤسسات و هماهنگی با قواعد حفاظت از داده‌ها می‌تواند چارچوبی مؤثرتر ایجاد کند. محرمانگی دیجیتال باید به‌عنوان بخشی از کیفیت نهادی داور ارزیابی شود، نه امتیازی فرعی که تنها در صورت اعتراض طرفین مورد توجه قرار گیرد.

### نتیجه‌گیری

محرمانگی یکی از مهم‌ترین عناصر جذابیت داور تجاری بین‌المللی برای فعالان اقتصادی است، اما بررسی مبانی و ساختار حقوقی آن نشان می‌دهد که این اصل در همه نظام‌های حقوقی دارای مفهوم، قلمرو و ضمانت اجرای یکسان نیست. تصور عمومی مبنی بر اینکه صرف انتخاب داور، تمام اطلاعات مرتبط با اختلاف را به‌طور خودکار و مطلق محرمانه می‌سازد، با واقعیت حقوقی سازگار نیست. خصوصی‌بودن جلسه تنها به محدودیت حضور اشخاص ثالث مربوط می‌شود، درحالی‌که محرمانگی تعهدی گسترده‌تر درباره عدم افشا، عدم انتقال و عدم استفاده خارج از هدف از اطلاعات است. این تعهد ممکن است از توافق طرفین، قانون مقر، قواعد مؤسسه داور، دستور دیوان یا الزامات حرفه‌ای ناشی شود. از این‌رو، وجود و حدود آن باید در هر پرونده به‌صورت مستقل بررسی گردد.

حاکمیت اراده طرفین مهم‌ترین مبنای تنظیم محرمانگی است، اما این آزادی نمی‌تواند الزامات آمره قانونی، حقوق اشخاص ثالث یا ضرورت‌های مربوط به اجرای رأی و حمایت از حق دفاع را کنار بگذارد. بهترین رویکرد آن است که طرفین در قرارداد اصلی یا موافقت‌نامه داور، شرطی روشن و تفصیلی درباره محرمانگی درج کنند. شرط کلی و مبهم نه‌تنها از اختلاف جلوگیری نمی‌کند، بلکه ممکن است خود به منشأ تعارض تبدیل شود. لازم است موضوعات محرمانه، اشخاص مجاز، اهداف استفاده، مدت تعهد، استثنائات و ضمانت اجرا به‌طور مشخص تعیین شوند. همچنین تعهد باید بر کارکنان، وکلاء، کارشناسان، مترجمان، تأمین‌کنندگان مالی و ارائه‌دهندگان خدمات فناوری نیز تسری یابد، زیرا نقض محرمانگی ممکن است از سوی هر یک از این اشخاص رخ دهد.

دیجیتالی‌شدن اسناد و ادله، ماهیت خطرهای وارد بر محرمانگی را دگرگون کرده است. در محیط کاغذی، حفاظت عمدتاً بر کنترل فیزیکی سند استوار بود، اما داده دیجیتال به‌سرعت تکثیر می‌شود، در چندین محل ذخیره می‌گردد و ممکن است پس از حذف ظاهری نیز بازایی شود. فراداده‌ها اطلاعاتی را آشکار می‌کنند که در متن سند دیده نمی‌شود و پراکندگی جغرافیایی داده‌ها موجب اعمال هم‌زمان قوانین چند کشور می‌شود. بنابراین، محرمانگی دیجیتال صرفاً تعهد به سکوت نیست، بلکه تعهدی فعال برای پیشگیری از دسترسی غیرمجاز، کنترل گردش اطلاعات، حفظ تمامیت داده و واکنش سریع به رخدادهای امنیتی است.

افشای الکترونیکی اسناد، حجم گسترده‌ای از داده‌ها را وارد فرایند داور می‌کند و خطر ارائه اطلاعات نامرتبط، ممتاز یا شخصی را افزایش می‌دهد. اصل تناسب باید در تعیین دامنه درخواست‌های سند جایگاه محوری داشته باشد. طرفین و دیوان نباید صرف امکان فنی دسترسی به

داده‌های فراوان را مجوز جمع‌آوری نامحدود بدانند. درخواست باید به دوره زمانی، اشخاص، موضوع و منابع مشخص محدود شود. سازوکار بازگرداندن اسناد ناخواسته، نحوه بررسی فراداده‌ها و روش حفاظت از اطلاعات ممتاز نیز باید پیشاپیش تعیین گردد.

فضای ابری و اتاق‌های داده مجازی می‌توانند مدیریت پرونده را تسهیل کنند، اما امنیت آن‌ها به انتخاب ارائه‌دهنده، تنظیمات دسترسی و رفتار کاربران وابسته است. محل سرورها، استفاده از پیمانکاران فرعی، شیوه رمزگذاری، مدت نگهداری و امکان حذف کامل باید پیش از استفاده بررسی شود. یک سامانه مشهور لزوماً برای هر نوع پرونده مناسب نیست. سطح حفاظت باید با ارزش اختلاف، ماهیت اطلاعات و احتمال تهدید متناسب باشد. پرونده‌های مرتبط با فناوری حساس، زیرساخت، داده‌های شخصی گسترده یا اسرار تولیدی نیازمند تدابیر شدیدتری هستند.

جلسات مجازی نیز باید بر اساس پروتکل روشن برگزار شوند. احراز هویت، کنترل ورود، ممنوعیت ضبط غیرمجاز، تعیین محل حضور شاهد، حفاظت از پیوند جلسه و مدیریت اشتراک‌گذاری صفحه از عناصر ضروری‌اند. صرف استفاده از یک پلتفرم متداول، امنیت و محرمانگی را تضمین نمی‌کند. شرکت‌کنندگان باید بدانند فایل‌های ضبط‌شده کجا ذخیره می‌شوند و چه اشخاصی به آن‌ها دسترسی دارند. در مورد شهود نیز باید میان جلوگیری از کمک پنهانی و احترام به حریم خصوصی تعادل برقرار شود.

استفاده از هوش مصنوعی یکی از مهم‌ترین چالش‌های جدید است. ورود اطلاعات پرونده به سامانه‌های عمومی می‌تواند کنترل طرف یا وکیل را بر داده از بین ببرد. لازم است استفاده از این ابزارها تنها پس از بررسی شرایط ذخیره، پردازش، استفاده ثانویه و حذف اطلاعات صورت گیرد. داده‌های محرمانه نباید در سامانه‌ای وارد شوند که برای آموزش عمومی یا بهبود نامحدود خدمات از ورودی کاربران استفاده می‌کند. مؤسسات داور و کانون‌های حرفه‌ای باید راهنماهای روشن درباره استفاده مسئولانه از هوش مصنوعی تدوین کنند و وکلاء نیز پیش از استفاده، رضایت آگاهانه موکل و سازگاری ابزار با تعهدات حرفه‌ای را بررسی نمایند.

محرمانگی مطلق نه ممکن است و نه مطلوب. رضایت طرفین، الزام قانونی، اجرای رأی، دفاع از حق، رسیدگی قضایی و منافع عمومی می‌توانند افشا را توجیه کنند. باین‌حال، هر استثنا باید محدود و متناسب باشد. طرفی که ناگزیر به افشاست باید تنها اطلاعات ضروری را ارائه دهد، در صورت امکان از نسخه ویرایش‌شده استفاده کند و طرف دیگر را پیشاپیش مطلع سازد. در موارد مرتبط با منافع عمومی نیز نباید تمام اطلاعات تجاری به بهانه شفافیت منتشر شود. تعادل باید بر اساس ماهیت اختلاف و ارتباط واقعی اطلاعات با منفعت عمومی برقرار گردد.

مسئولیت حفاظت از اطلاعات میان چند بازیگر توزیع می‌شود. طرفین باید ساختار داخلی مناسب ایجاد کنند، وکلاء باید استاندارد مراقبت حرفه‌ای را رعایت نمایند، داوران باید مدیریت امن پرونده را بخشی از وظیفه خود بدانند و مؤسسات باید سامانه‌های فنی و قراردادهای ارائه خدمات را به‌طور مستمر ارزیابی کنند. ارائه‌دهندگان فناوری نیز نباید صرفاً به‌عنوان پیمانکاران فنی بی‌طرف تلقی شوند، زیرا ممکن است نقش تعیین‌کننده‌ای در نگهداری، پردازش و انتقال اطلاعات داشته باشند. قرارداد با آنان باید مسئولیت، گزارش رخداد، همکاری در تحقیق و جبران خسارت را مشخص سازد.

ضمانت اجرای نقض محرمانگی باید هم جنبه جبرانی و هم بازدارنده داشته باشد. خسارت مالی همیشه برای جبران افشای سر تجاری یا آسیب اعتباری کافی نیست. دستور منع افشا، حذف اطلاعات، محدودکردن استفاده، تخصیص هزینه‌ها و اقدامات انتظامی می‌توانند اهمیت بیشتری داشته باشند. در عین حال، اثبات نقض و رابطه سببیت در محیط دیجیتال دشوار است. ثبت فعالیت کاربران، گزارش ورود، سابقه

دانلود و مستندسازی زنجیره نگهداری می‌تواند در تعیین مسئولیت مؤثر باشد. از این رو، ابزارهای فنی نه تنها برای پیشگیری، بلکه برای اثبات تخلف نیز اهمیت دارند.

پروتکل امنیت سایبری باید به بخش عادی نخستین دستور آیینی در داوری‌های بین‌المللی تبدیل شود. این پروتکل باید بر پایه ارزیابی خطر طراحی شود و روش انتقال فایل، احراز هویت، رمزگذاری، طبقه‌بندی اطلاعات، استفاده از دستگاه شخصی، گزارش رخداد و حذف داده را پوشش دهد. رویکرد یکسان برای همه پرونده‌ها مناسب نیست. تدابیر باید به اندازه‌ای قوی باشند که از اطلاعات حمایت کنند، بدون آنکه هزینه و پیچیدگی نامتناسبی بر طرفین تحمیل شود. تناسب، ضرورت و قابلیت اجرا باید معیارهای اصلی طراحی پروتکل باشند.

چرخه حفاظت از اطلاعات با پایان جلسه یا صدور رأی خاتمه نمی‌یابد. نسخه‌های اسناد ممکن است در رایانه‌ها، ایمیل‌ها، سامانه‌های پشتیبان و حساب‌های کاربری باقی بمانند. بنابراین، سیاست نگهداری و حذف باید از ابتدای پرونده مشخص باشد. هر شخص باید پس از پایان نقش خود دسترسی را از دست بدهد و اطلاعاتی که نگهداری آن‌ها ضرورت ندارد به صورت امن حذف شوند. اسنادی که برای اجرای رأی یا دفاع آتی لازم‌اند باید در محیطی محدود و برای مدت معین حفظ شوند. نگهداری نامحدود، خطر نقض آینده را افزایش می‌دهد و با اصل حداقل سازی اطلاعات سازگار نیست.

در نهایت، آینده داوری تجاری بین‌المللی به میزان توانایی آن در سازگاری با محیط دیجیتال وابسته است. داوری زمانی می‌تواند اعتماد فعالان اقتصادی را حفظ کند که محرمانگی را نه به عنوان ادعایی تبلیغاتی، بلکه به عنوان مجموعه‌ای از تعهدات حقوقی، سازمانی و فنی اجرا کند. حمایت مؤثر نیازمند قراردادهای دقیق، قواعد نهادی روشن، آموزش حرفه‌ای، زیرساخت امن، مدیریت چرخه حیات داده و مسئولیت‌پذیری همه اشخاص دخیل است. محرمانگی در عصر دیجیتال دیگر صرفاً خودداری از سخن گفتن درباره پرونده نیست، بلکه توانایی کنترل مستمر بر ایجاد، دسترسی، پردازش، انتقال، ذخیره و حذف اطلاعات است. هرچه داوری این واقعیت را جدی‌تر بپذیرد، اعتبار و کارآمدی آن در تجارت بین‌المللی پایدارتر خواهد بود.

### تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافع وجود ندارد.

### مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

### حامی مالی

این پژوهش حامی مالی نداشته است.

## EXTENDED SUMMARY

International commercial arbitration has become one of the principal mechanisms for resolving transnational commercial disputes because it enables parties to select specialized decision-makers, determine the applicable procedural framework, choose the language and seat of arbitration, and avoid many of the rigidities associated with national court proceedings. Its contractual foundation and procedural flexibility allow commercial actors to tailor the dispute-resolution process to the technical, financial, and legal characteristics of their transactions (Fouchard et al., 2024). In addition to neutrality, enforceability, and procedural autonomy, confidentiality is frequently presented as one of arbitration's most significant advantages. Commercial parties often prefer arbitration because they seek to prevent the disclosure of contractual disputes, financial difficulties, pricing structures,

internal communications, technical information, customer data, and business strategies. This expectation has led some scholars to regard confidentiality as a fundamental characteristic of international commercial arbitration (Bagner, 2001). Nevertheless, the legal status of confidentiality is neither uniform nor absolute. Comparative legal analysis demonstrates that national systems differ considerably in determining whether confidentiality arises automatically from the private nature of arbitration, must be expressly agreed upon, or depends on institutional rules and professional duties (Noussia, 2010). The distinction between privacy and confidentiality is therefore essential. Privacy concerns the exclusion of unauthorized third parties from hearings and procedural activities, whereas confidentiality concerns the prohibition of disclosure or unauthorized use of information obtained during the arbitral process. A hearing may be private while documents, awards, or information relating to the dispute remain legally disclosable in judicial, regulatory, or corporate contexts. Consequently, the assumption that all arbitration-related information is automatically protected merely because the parties selected arbitration may generate serious legal uncertainty.

The digital transformation of commercial transactions and arbitral procedure has substantially intensified this uncertainty. Contemporary arbitration is increasingly conducted through electronic correspondence, cloud-based case-management platforms, virtual hearings, digital document production, online data rooms, automated translation systems, and artificial-intelligence-assisted document review. Commercial evidence itself is now predominantly electronic and may include emails, instant messages, spreadsheets, accounting databases, mobile-phone data, audio and video files, server logs, smart-contract records, and information stored on distributed networks. Electronic evidence differs from paper evidence because it can be copied instantaneously, distributed across several jurisdictions, altered without obvious physical traces, recovered after apparent deletion, and accompanied by metadata containing information not visible in the text of the document. These characteristics transform confidentiality from a passive obligation not to disclose information into an active obligation to protect information against unauthorized access, accidental transmission, cybersecurity attacks, inappropriate secondary use, and uncontrolled technological processing. Traditional confidentiality rules were primarily developed for proceedings in which access to information could be controlled through physical possession of paper files and closed hearings. Such rules may be inadequate when the same document is simultaneously stored on a party's server, a lawyer's laptop, an institutional case-management platform, a cloud provider's infrastructure, and an expert's personal device. The increasing use of smart contracts and technology-based dispute-resolution mechanisms further complicates the legal position because information may be recorded on-chain while the substantive dispute is resolved through off-chain procedures (Haddadi, 2024). Data entered into public or semi-public digital systems may be difficult or impossible to remove, while pseudonymization may not prevent parties from being identified through transactional patterns. The digital environment thus expands both the range of information requiring protection and the number of actors capable of accessing or processing that information.

The present study aims to examine the legal foundations, scope, limitations, and enforcement mechanisms of confidentiality in international commercial arbitration, with particular emphasis on challenges arising from the digitalization of documents and electronic evidence. It adopts a descriptive-analytical and comparative legal method based on the examination of arbitration scholarship, national approaches, institutional practices, general principles of arbitral procedure, and emerging technological risks. The study distinguishes among contractual confidentiality, statutory confidentiality, institutional confidentiality, professional secrecy, and confidentiality

arising from procedural orders issued by arbitral tribunals. Party autonomy remains the most important basis for establishing confidentiality because arbitration derives its authority from agreement, and parties may define protected information, authorized recipients, permitted uses, temporal duration, exceptions, and remedies for breach. General arbitration theory recognizes party autonomy as a central organizing principle of international arbitral procedure (Redfern & Hunter, 2023). However, contractual autonomy cannot exclude mandatory disclosure obligations, judicial supervision, public-order considerations, or the rights of third parties. The law of the arbitral seat may also influence the existence and extent of the obligation, as some jurisdictions expressly recognize confidentiality, others infer it from the nature of arbitration, and others require an explicit contractual or statutory basis. The procedural significance of the seat and the applicable national arbitration law therefore extends to the protection of information and the availability of judicial remedies. Iranian legal scholarship similarly emphasizes the role of agreement, procedural autonomy, and the legal framework governing international commercial arbitration (Shirovi, 2024). Nevertheless, reliance on general assumptions is insufficient, particularly where digital data are processed across several jurisdictions. The applicable law may involve not only the law governing the arbitration agreement and the law of the seat but also data-protection legislation, rules concerning trade secrets, professional regulations, and mandatory requirements applicable in the country where data are stored or transferred.

The study finds that the personal and material scope of confidentiality must be defined more precisely in digitally administered arbitration. The obligation should not be limited to the parties and arbitrators but should extend, where appropriate, to lawyers, in-house counsel, corporate employees, witnesses, experts, translators, tribunal secretaries, institutional personnel, litigation funders, insurers, cloud-service providers, videoconferencing companies, document-review vendors, and artificial-intelligence service providers. Each participant should receive access only to the information necessary for the performance of a defined role. The protected subject matter may include the existence of the arbitration, the identity of the participants, pleadings, documentary exhibits, witness statements, expert reports, procedural correspondence, hearing recordings, interim decisions, settlement communications, and the final award. The relationship between confidentiality and transparency must nevertheless be managed carefully. International arbitration has long faced tension between the commercial value of secrecy and demands for openness, consistency, and public accountability (Buys, 2003). This tension is especially evident in disputes affecting public funds, national security, corruption, environmental interests, or other matters extending beyond the immediate parties. Public-order and national-security considerations may limit the parties' ability to preserve complete secrecy (Shahheidari, 2024). Similarly, the growth of transparency in investor-state arbitration illustrates that legitimate public interests can require reconsideration of broad confidentiality expectations (Khan, 2020). Although commercial arbitration differs from investment arbitration, the underlying lesson is that confidentiality should be treated as a qualified principle rather than an absolute prohibition. Disclosure may be justified by party consent, statutory duties, regulatory reporting, court proceedings, recognition and enforcement of an award, protection of legal rights, or overriding public interests. Any such disclosure should remain necessary, proportionate, and limited to the information required for the legitimate purpose.

Electronic document production creates particularly serious risks because large volumes of data may contain privileged communications, personal information, commercially sensitive material, and metadata unrelated to the dispute. Requests for electronic documents must therefore be governed by relevance, materiality, and proportionality rather than technical availability. The mere existence

of searchable digital data should not justify unlimited disclosure. Protocols should define custodians, date ranges, search terms, file types, metadata fields, review methods, and procedures for the return or deletion of inadvertently disclosed privileged documents. International arbitral procedure generally supports efficient and proportionate document production rather than extensive litigation-style discovery (Nikbakht, 2023). Cloud storage and virtual data rooms can facilitate secure collaboration, but only when providers are carefully assessed and contractual safeguards are adopted. Relevant agreements should specify server location, encryption standards, access controls, subcontracting arrangements, data-retention periods, incident-reporting duties, and secure deletion procedures. Virtual hearings likewise require identity verification, controlled admission, encrypted communication, restrictions on unauthorized recording, secure screen sharing, and confirmation that witnesses are not receiving undisclosed assistance. Artificial-intelligence tools present an additional layer of risk because confidential materials entered into public platforms may be retained, analyzed, reused, or incorporated into broader training processes. Parties, counsel, arbitrators, and experts should therefore avoid entering protected information into systems whose data-governance practices are unclear. The use of technological tools should be subject to prior risk assessment, informed authorization, and contractual restrictions on secondary processing. Responsibility for breach may arise not only from intentional disclosure but also from negligence, such as using weak passwords, failing to update software, transmitting files through insecure channels, or granting unnecessary access. Effective remedies may include damages, contractual penalties, injunctions, orders for deletion or return, limitations on the use of improperly obtained evidence, adverse cost decisions, professional sanctions, and liability under data-protection or trade-secret laws.

In conclusion, confidentiality in international commercial arbitration must be reconceptualized for the digital environment. It can no longer be treated merely as an implied promise that participants will refrain from publicly discussing the proceedings. It is now a comprehensive duty involving prevention, access management, secure processing, controlled transmission, incident response, data minimization, and final deletion. A reliable system requires an integrated combination of contractual, procedural, institutional, organizational, and technical safeguards. Parties should adopt detailed digital-confidentiality clauses rather than relying on general statements that the arbitration is confidential. Arbitral tribunals should address cybersecurity, electronic disclosure, virtual hearings, artificial-intelligence use, and data retention in an early procedural order. Institutions should maintain secure platforms, establish transparent data-governance policies, assess technology vendors, and define their responsibilities in the event of a breach. Access should be role-based, authentication should be strengthened, sensitive information should be encrypted, and highly confidential documents should be reviewed in controlled environments. Disclosure exceptions should be narrowly interpreted and guided by necessity and proportionality. The lifecycle of information must also be managed beyond the issuance of the award, because electronic copies may remain on personal devices, servers, backup systems, and inactive user accounts. Ultimately, the legitimacy and commercial attractiveness of international arbitration depend on its ability to protect digital information in a manner that is legally predictable, technologically competent, and operationally enforceable. Confidentiality will remain a meaningful advantage of arbitration only when it is supported by active security obligations and shared responsibility throughout the entire arbitral process.

## References

Bagner, H. (2001). Confidentiality - a fundamental principle in international commercial arbitration? *Journal of International*, 18(2), 243-267. <https://doi.org/10.54648/338334>





- Burnley, R., & Lascelles, G. (2004). Mediation confidentiality, conduct and communications. *Arbitration: The Journal of Chartered Institute of Arbitrators*, 70(1), 22-38.
- Buys, C. G. (2003). The tensions between confidentiality and transparency in international arbitration. *The American Review of International Arbitration*, 14.
- Enayat, S. H. (1999). Confidentiality or openness of commercial arbitration. *Legal Research Journal, Faculty of Law, Shahid Beheshti University*(27-28).
- Fallah, E. M. (2024). Jurisdictions of International Commercial Arbitration in Afghanistan and UNCITRAL Laws. *International Journal Of Humanities Education And Social Sciences (IJHES)*, 3(4). <https://doi.org/10.55227/ijhess.v3i4.868>
- Fouchard, P., Gaillard, E., & Goldman, B. (2024). *On international commercial arbitration* (Revised edition ed.). Wolters Kluwer.
- Gurry, F. (1995). Confidentiality in Mediation. WIPO Conference on Mediation, Geneva.
- Haddadi, S. (2024). Arbitration in Smart Contracts: Legal Challenges of On-Chain and Off-Chain Dispute Resolution. *Economic and Commercial Legal Research*, 2(2).
- Haqmal, M. A. (2024). The Need, Development, and Benefits of Commercial Arbitration in Afghanistan. *American Journal of Business and Strategic Management*, 3(1), 1-9. <https://doi.org/10.58425/ajbsm.v3i1.244>
- Johar, S. (2024). Substantive Law Governing Disputes in International Commercial Arbitration in the Absence of the Parties' Choice. *Judicial Law Journal*, 88(127), 59-92.
- Khan, R. E. (2020). Foreign Investors and Greater Transparency in Investor-State Dispute Settlement: Reevaluating Confidentiality Expectations in International Investment Arbitration. In (pp. 187-204). [https://doi.org/10.1007/978-3-030-41920-2\\_11](https://doi.org/10.1007/978-3-030-41920-2_11)
- Misra, J., & Jordan, R. (2006). Confidentiality in International Arbitration. *Journal of International Arbitration*, 23(2), 34-40.
- Nikbakht, H. (2023). *International Commercial Arbitration: Arbitral Procedure* (4th ed.). Commercial Printing and Publishing Company.
- Noussia, K. (2010). *Confidentiality in International Commercial Arbitration; A Comparative Analysis of the Position Under English, US, German and French Law*. Springer.
- Redfern, A., & Hunter, M. (2023). *Law and Practice of International Commercial Arbitration* (7th ed.). Sweet & Maxwell.
- Shahheidari, F. (2024). The Role of Public Order and National Security in International Commercial Arbitration. *Iranian Research Journal on International Relations*, 1(3).
- Shirovi, A. (2024). *International Commercial Arbitration* (16th ed.). SAMT.
- Tahir, M. I. (2023). Arbitration System in Commercial Disputes in Pakistan and Enforcement of Foreign Awards. *Al-Nasr*, 73-92. <https://doi.org/10.53762/alnasr.02.03.e06>