

چالش‌های پذیرش ادله دیجیتال در دعاوی مدنی و کیفری (بررسی تطبیقی ایران و نظام‌های حقوقی پیشرفته)

اسرا ولی پور

دانشجوی کارشناسی ارشد، حقوق خصوصی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران

چکیده

در دنیای معاصر، با گسترش فناوری اطلاعات و ارتباطات، استفاده از ادله دیجیتال در دعاوی حقوقی و کیفری به‌عنوان یکی از مهم‌ترین ابزارهای اثباتی مورد توجه قرار گرفته است. با این حال، پذیرش و ارزیابی این نوع ادله در نظام‌های قضایی مختلف با چالش‌های متعددی روبه‌رو است. در حقوق ایران، به‌رغم پیشرفت‌هایی که در زمینه جرم‌انگاری و استناد به داده‌های الکترونیکی صورت گرفته، همچنان ابهامات قانونی، عدم انسجام رویه قضایی، ضعف در احراز اصالت و اعتبار ادله دیجیتال و محدودیت‌های فنی و اجرایی از چالش‌های اصلی محسوب می‌شوند. در مقابل، نظام‌های حقوقی پیشرفته همچون ایالات متحده، اتحادیه اروپا و بریتانیا، با تدوین مقررات مشخص در زمینه جمع‌آوری، تحلیل و استناد به ادله دیجیتال، چارچوب‌های روشنی را برای پذیرش این نوع ادله فراهم کرده‌اند. این پژوهش با روش توصیفی-تحلیلی و تطبیقی، چالش‌های حقوقی، فنی و قضایی پذیرش ادله دیجیتال در نظام حقوقی ایران را بررسی کرده و آن را با استانداردها و رویه‌های نظام‌های حقوقی پیشرفته مقایسه می‌کند. نتایج تحقیق نشان می‌دهد که پذیرش ادله دیجیتال در ایران نیازمند اصلاح قوانین موجود، ایجاد رویه‌های استاندارد برای احراز اصالت و اعتبار ادله، ارتقای دانش فنی قضات و وکلا و همچنین به‌کارگیری فناوری‌های نوین در فرآیند کشف جرم و دادرسی است.

کلیدواژه: ادله دیجیتال، پذیرش ادله، دعاوی مدنی، دعاوی کیفری، حقوق ایران، حقوق تطبیقی، جرم‌شناسی دیجیتال، اصالت و اعتبار ادله، فناوری حقوقی

۱. مقدمه

با گسترش فناوری‌های اطلاعاتی و ارتباطی، نقش ادله دیجیتال در دادرسی‌های مدنی و کیفری به‌طور چشمگیری افزایش یافته است. امروزه، بسیاری از دعاوی حقوقی متکی بر داده‌های الکترونیکی نظیر پیام‌های متنی، ایمیل‌ها، سوابق تراکنش‌های دیجیتال، فیلم‌ها و تصاویر ذخیره‌شده در دستگاه‌های الکترونیکی و شبکه‌های اجتماعی هستند. پذیرش این نوع ادله در محاکم قضایی به‌عنوان یک چالش اساسی مطرح است، زیرا ادله دیجیتال ماهیتی متفاوت از ادله سنتی دارند و مسائلی نظیر اصالت، تمامیت و قابلیت استناد آن‌ها، همواره مورد بحث بوده است [کیسی^۱، ۲۰۱۹].

در نظام حقوقی ایران، قوانین موجود همچون قانون آیین دادرسی کیفری و قانون تجارت الکترونیکی، به نحوی به این موضوع پرداخته‌اند؛ اما همچنان ابهامات و چالش‌هایی در خصوص اعتبار و قابلیت پذیرش ادله دیجیتال در فرآیند دادرسی وجود دارد. این چالش‌ها شامل نبود استانداردهای روشن برای جمع‌آوری، تحلیل و ارائه ادله دیجیتال، عدم سازگاری برخی قوانین با ماهیت این نوع ادله و فقدان آموزش‌های کافی برای قضات و وکلای در این حوزه است [حبیبی و احمدی، ۱۳۹۹].

در بسیاری از نظام‌های حقوقی پیشرفته مانند ایالات متحده آمریکا و کشورهای عضو اتحادیه اروپا، قوانین جامعی برای پذیرش و بررسی ادله دیجیتال تدوین شده است. به‌عنوان مثال، در آمریکا، قانون شواهد فدرال^۲ معیارهایی برای پذیرش ادله دیجیتال مشخص کرده و بر اصالت، قابلیت اعتماد و حفظ حریم خصوصی تأکید دارد (کر^۳، ۲۰۲۱). همچنین، مقررات حفاظت از داده‌های عمومی (GDPR) در اتحادیه اروپا، علاوه بر تأمین امنیت داده‌های دیجیتال، چارچوبی برای استفاده از این داده‌ها در محاکم قضایی فراهم کرده است [وویگت و بوشه^۴، ۲۰۱۷].

در مقایسه با این کشورها، ایران هنوز با چالش‌های متعددی در زمینه شناسایی و اجرای این ادله مواجه است و نیاز به اصلاحات قانونی و فنی در این زمینه احساس می‌شود.

این پژوهش با هدف بررسی چالش‌های پذیرش ادله دیجیتال در دعاوی مدنی و کیفری، نگاهی تطبیقی به نظام حقوقی ایران و برخی کشورهای پیشرفته خواهد داشت. تلاش می‌شود تا از طریق تحلیل قوانین موجود، بررسی نقاط قوت و ضعف رویه‌های قضایی و ارائه پیشنهادهایی برای بهبود فرآیند پذیرش ادله دیجیتال، راهکارهایی مؤثر در جهت ارتقای کارآمدی نظام قضایی ایران ارائه شود.

۱- اهمیت و ضرورت پذیرش ادله دیجیتال در دادرسی‌های مدنی و کیفری

با پیشرفت فناوری و گسترش ارتباطات دیجیتال، استفاده از ادله دیجیتال در دعاوی مدنی و کیفری به یکی از مسائل اساسی در نظام‌های حقوقی مختلف تبدیل شده است. امروزه بسیاری از جرایم و تخلفات در فضای مجازی رخ می‌دهند و شواهد مرتبط با آن‌ها، همچون پیام‌های الکترونیکی، سوابق تراکنش‌های مالی آنلاین، اطلاعات ذخیره‌شده در رایانه‌ها و حتی داده‌های ابری،

Casey^۱Federal Rules of Evidence^۲Kerr^۳Voigt & Bussche^۴

می‌توانند نقش کلیدی در فرآیند دادرسی ایفا کنند [کیسی، ۲۰۱۹]. این امر باعث شده است که نظام‌های قضایی به دنبال تطبیق قوانین خود با این تحولات باشند و چارچوب‌های قانونی مناسبی را برای پذیرش و ارزیابی ادله دیجیتال تدوین کنند.

یکی از مهم‌ترین چالش‌های پذیرش ادله دیجیتال، مسئله‌ی اصالت و اعتبار این نوع از شواهد است. برخلاف اسناد فیزیکی که قابلیت ارزیابی سنتی دارند، ادله دیجیتال ممکن است به راحتی مورد تغییر یا حذف قرار گیرند، که این موضوع، لزوم اتخاذ روش‌های علمی و فنی برای احراز صحت و تمامیت این شواهد را مطرح می‌کند [کر، ۲۰۲۰]. در برخی از نظام‌های حقوقی پیشرفته، مانند ایالات متحده و اتحادیه اروپا، دستورالعمل‌ها و رویه‌های مشخصی برای پذیرش ادله دیجیتال تدوین شده است، به گونه‌ای که قابلیت اطمینان آن‌ها با استفاده از فناوری‌های رمزنگاری و امضای دیجیتال مورد ارزیابی قرار می‌گیرد [وویگت و بوشه، ۲۰۱۷]. در مقابل، در نظام حقوقی ایران، اگرچه گام‌هایی برای پذیرش این نوع ادله برداشته شده است، اما همچنان برخی از قوانین با الزامات جدید فناوری‌های دیجیتال همخوانی ندارند، که این امر موجب بروز مشکلاتی در فرآیند استناد به ادله دیجیتال در محاکم می‌شود [حبیبی و احمدی، ۱۳۹۹].

ضرورت پذیرش ادله دیجیتال در دادرسی‌ها نه تنها به دلیل افزایش جرایم سایبری و پیچیدگی‌های فناوری اطلاعات است، بلکه به دلیل ایجاد عدالت قضایی و جلوگیری از فرار متهمان از مجازات نیز اهمیت دارد. شناسایی و تحلیل دقیق این شواهد، به دستگاه قضایی کمک می‌کند تا درک بهتری از جریان جرایم دیجیتال داشته باشد و تصمیمات عادلانه‌تری اتخاذ کند. از سوی دیگر، عدم پذیرش این ادله می‌تواند به نقض حقوق افراد و عدم تحقق عدالت منجر شود، چرا که بسیاری از جرایم و دعاوی امروزی، بدون استفاده از شواهد دیجیتال، غیرقابل اثبات خواهند بود. بنابراین، برای افزایش کارآمدی نظام دادرسی، لازم است که چارچوب‌های قانونی لازم برای اعتبارسنجی، نگهداری و پذیرش ادله دیجیتال توسعه یافته و رویه‌های اجرایی مناسبی در این زمینه تدوین شود.

۲- مفهوم و ماهیت ادله دیجیتال

ادله دیجیتال به شواهدی اطلاق می‌شود که به صورت الکترونیکی ذخیره و نگهداری می‌شوند و در فرآیندهای قانونی به عنوان مدرک مورد استفاده قرار می‌گیرند [ریلی، ۵، ۲۰۲۰]. این ادله شامل طیف وسیعی از داده‌ها از جمله ایمیل‌ها، پیام‌های متنی، تصاویر، ویدئوها، اسناد الکترونیکی و اطلاعات ذخیره شده بر روی سخت افزارهای کامپیوتری و سرورها می‌شوند. ویژگی کلیدی ادله دیجیتال، قابلیت دسترسی و تجزیه و تحلیل دقیق آن‌ها با استفاده از فناوری‌های دیجیتال است. این قابلیت به شناسایی و شفاف سازی حقایق در پرونده‌های قضایی کمک شایانی می‌کند [اسمیت و جونز، ۶، ۲۰۲۱]. برخلاف ادله سنتی که معمولاً به صورت فیزیکی (مانند اسناد کاغذی) وجود دارند و در معرض گم شدن یا تخریب قرار دارند، ادله دیجیتال به سادگی قابل کپی و ذخیره سازی در محیط‌های مختلف مانند فضای ابری هستند [جانسون، ۷، ۲۰۲۲]. این امر دسترسی به آن‌ها را تسهیل کرده و از بین رفتن آن‌ها را دشوارتر می‌کند.

انواع مختلفی از ادله دیجیتال وجود دارد. به عنوان مثال، می‌توان به ادله مستند که شامل فایل‌های دیجیتالی مرتبط با مستندات قانونی است، اشاره کرد [گارفینکل، ۸، ۲۰۱۵]. همچنین ادله عینی وجود دارد که به اطلاعات ثبت شده در مورد عملکرد سیستم‌ها و رویدادها از جمله لاگ‌های سیستم و رکوردهای فعالیت کاربران مربوط می‌شود. علاوه بر این، شواهد شاهد نیز به عنوان

Reilly^۵

Smith & Jones^۶

Johnson^۷

Garfinkel^۸

قسمتی از ادله دیجیتال قابل ارائه هستند؛ این شواهد از طریق شهادت افراد و به عنوان تأیید و توضیح برای ادله دیجیتال ارائه می‌شود [میسون^۹، ۲۰۱۸]. نوع دیگری از دسته‌بندی ادله دیجیتال، تفکیک به ادله روشن و ادله ضمنی است. ادله روشن به طور مستقیم به یک عمل یا رویداد اشاره دارند، در حالی که ادله ضمنی نیاز به تفسیر و استنباط دارند تا به طور غیر مستقیم به یک عمل یا رویداد مرتبط شوند [اسمیت و جونز، ۲۰۲۱].

یکی از تفاوت‌های اساسی ادله دیجیتال با ادله سنتی در روش جمع‌آوری و مدیریت آن‌هاست. ادله سنتی به روش‌های سنتی جمع‌آوری و نگهداری می‌شوند، در حالی که ادله دیجیتال نیازمند ابزارها و روش‌های تخصصی برای جمع‌آوری، نگهداری، و تجزیه و تحلیل هستند [است^{۱۰}، ۲۰۱۶]. این موضوع بر قابلیت دسترسی و تجزیه و تحلیل شواهد تأثیر بسزایی دارد. به طور کلی می‌توان گفت که ادله دیجیتال، به دلیل قابلیت دسترسی، ظرفیت ذخیره‌سازی بالا، و قابلیت جستجو و تجزیه و تحلیل راحت‌تر، نقش مهمی را در دادرسی‌های مدرن به عهده دارند، اما همزمان چالش‌هایی در زمینه اعتبارسنجی، اثبات اصالت و مدیریت امنیت اطلاعات را به همراه دارد [جوهانسون، ۲۰۲۲].

۳- مبانی حقوقی و قانونی ادله دیجیتال در ایران

در نظام حقوقی ایران، جایگاه ادله دیجیتال هنوز در حال شکل‌گیری و توسعه است. با این حال، قانونگذار به تدریج با تصویب قوانین و مقررات مختلف، زمینه استفاده از این نوع ادله را در دادرسی‌ها فراهم کرده است. قانون تجارت الکترونیکی یکی از قوانین کلیدی در این زمینه است که به پذیرش و استناد به ادله الکترونیکی در دعاوی مدنی و تجاری کمک می‌کند. این قانون، شکل‌گیری هر نوع دلیل را در قالب داده - پیام پذیرفته است و به این ترتیب، اسناد، شهادت‌ها، و سایر ادله‌ای که به صورت الکترونیکی ارائه می‌شوند، در صورت احراز شرایط قانونی، قابلیت استناد در محاکم را دارند.

قانون آیین دادرسی مدنی و قانون آیین دادرسی کیفری نیز به طور غیر مستقیم به ادله دیجیتال اشاره دارند. این قوانین، به طور کلی، به شواهد و مدارک اثباتی می‌پردازند، و در عمل، قضات در مواردی از ادله دیجیتال در فرآیند رسیدگی استفاده کرده‌اند. با این حال، به دلیل نو بودن این نوع ادله، هنوز قوانین و مقررات کاملاً مشخص و جامعی برای نحوه بررسی، اعتبارسنجی و پذیرش ادله دیجیتال در این قوانین وجود ندارد.

قانون جرایم رایانه‌ای مصوب ۱۳۸۸ نیز به ادله دیجیتال مربوط به جرایم رایانه‌ای می‌پردازد. این قانون به تعریف جرایم مرتبط با فناوری اطلاعات و نحوه جمع‌آوری و استفاده از ادله دیجیتال در این زمینه می‌پردازد. همچنین، به مسائلی مانند حفظ حریم خصوصی و امنیت اطلاعات در ارتباط با ادله دیجیتال اشاره می‌کند.

رویه قضایی در ایران در مواجهه با ادله دیجیتال، هنوز یکنواخت و کاملاً منسجم نیست. قضات در موارد مختلف، با توجه به شرایط هر پرونده و با استناد به قوانین موجود، روش‌های مختلفی را برای بررسی و پذیرش این نوع ادله به کار می‌برند. این موضوع نیاز به تدوین دستورالعمل‌های جزئی‌تر و شفاف‌تر در زمینه ارزیابی و اعتبارسنجی ادله دیجیتال را بیشتر مشهود می‌کند. دکتر ناصر کاتوزیان، به عنوان یکی از برجسته‌ترین حقوق‌دانان ایران، در آثار خود به مبانی حقوقی ادله اثبات دعوا پرداخته است. وی در کتاب "اثبات و دلیل اثبات" [کاتوزیان، ۱۳۹۰]، بر اهمیت تطبیق ادله اثباتی با تحولات تکنولوژیک تأکید می‌کند.

^۹Mason

^{۱۰}East

هرچند در زمان نگارش این کتاب، ادله دیجیتال به شکل گسترده مورد بررسی قرار نگرفته بود، اما مبانی کلی ارائه شده توسط وی قابل انطباق با این حوزه است. از دیدگاه کاتوزیان:

- اصل آزادی ادله در دعاوی مدنی به گونه‌ای است که می‌توان ادله دیجیتال را نیز به عنوان یکی از ابزارهای اثبات دعوا پذیرفت، مگر آنکه قانون استثنایی قائل شده باشد.
- در دعاوی کیفری، پذیرش ادله دیجیتال نیازمند رعایت اصل قانونی بودن دلایل است و قانون باید به صراحت اعتبار این نوع ادله را مشخص کند.
- صحت و اصالت اسناد الکترونیکی باید از طریق شیوه‌های فنی و کارشناسی تأیید شود تا امکان استناد قضایی به آن فراهم گردد [کاتوزیان، ۱۳۹۰].

دکتر جعفری لنگرودی، در کتاب "ترمینولوژی حقوق" [جعفری لنگرودی، ۱۳۹۶]، مفهوم "دلیل" را به عنوان یکی از ابزارهای اثبات در دعاوی بررسی کرده و تأکید دارد که دلیل باید مورد پذیرش قانون باشد. همچنین در کتاب "مبانی فقهی و حقوقی اسناد تجاری"، به بررسی اسناد الکترونیکی پرداخته و آن‌ها را به عنوان نوعی از اسناد رسمی و عادی مورد بررسی قرار داده است. از دیدگاه وی:

- اسناد الکترونیکی، چنانچه دارای امضای معتبر و مشخصات قانونی باشند، از نظر حقوقی در حکم اسناد رسمی محسوب می‌شوند.
- هر نوع سند دیجیتال باید از نظر فقهی و حقوقی، قابلیت انتساب به صادرکننده را داشته باشد تا ارزش اثباتی پیدا کند.
- پذیرش ادله دیجیتال نیازمند انطباق با اصول کلی حقوقی، از جمله اصل اصالت دلیل و اصل صحت معاملات است [جعفری لنگرودی، ۱۳۹۰].

در نظام حقوقی ایران، قوانین مختلفی به پذیرش و استفاده از ادله دیجیتال پرداخته‌اند، از جمله:

- قانون تجارت الکترونیکی (۱۳۸۲): این قانون به صراحت اعتبار اسناد و امضای الکترونیکی را تأیید کرده است و ماده ۱۲ آن بیان می‌کند که داده‌پیام‌های دارای امضای الکترونیکی مطمئن، در حکم اسناد کتبی هستند.
- قانون آیین دادرسی کیفری (۱۳۹۲): ماده ۶۵۵ این قانون به صراحت به امکان استناد به ادله دیجیتال در دعاوی کیفری اشاره کرده است.
- قانون جرائم رایانه‌ای (۱۳۸۸): در این قانون به شیوه‌های جمع‌آوری و تحلیل ادله دیجیتال و جرائم مرتبط با آن پرداخته شده است.

در کل، با توجه به اینکه ادله دیجیتال به طور فزاینده‌ای در زندگی روزمره و دادرسی‌ها مورد استفاده قرار می‌گیرند، نیاز به تدوین قوانین جامع‌تر و رویه‌های قضایی منسجم‌تر در زمینه مبانی حقوقی و قانونی آن‌ها در ایران کاملاً محسوس است. این قوانین باید همزمان جنبه‌های فنی و حقوقی را در نظر گرفته و به ایجاد شفافیت و عدالت در فرآیند دادرسی کمک کنند. با تطبیق نظرات حقوق‌دانان برجسته ایران با قوانین موجود، می‌توان نتیجه گرفت که پذیرش ادله دیجیتال در نظام حقوقی ایران به رسمیت شناخته شده است، اما همچنان نیاز به توسعه مقررات تفصیلی‌تر و استانداردهای دقیق‌تر در این زمینه وجود دارد.

۴- چالش‌های پذیرش ادله دیجیتال در نظام قضایی ایران

ادله دیجیتال، به‌عنوان یکی از مهم‌ترین ابزارهای اثبات دعوا در عصر فناوری اطلاعات، جایگاه ویژه‌ای در نظام‌های حقوقی مختلف یافته است. در نظام قضایی ایران نیز این نوع ادله به رسمیت شناخته شده، اما چالش‌های متعددی در زمینه پذیرش، ارزیابی و استناد به آن‌ها وجود دارد. این چالش‌ها را می‌توان در ابعاد قانونی، فنی، اثباتی و رویه‌ای بررسی کرد.

یکی از مهم‌ترین چالش‌ها در پذیرش ادله دیجیتال، ابهام و نقص قوانین موجود در این زمینه است. هرچند قانون تجارت الکترونیکی (۱۳۸۲) اسناد و امضای الکترونیکی را معتبر دانسته و قانون جرائم رایانه‌ای (۱۳۸۸) به روش‌های جمع‌آوری و استفاده از ادله دیجیتال پرداخته است، اما هنوز استانداردهای دقیقی برای ارزیابی صحت و اصالت این ادله وجود ندارد [کاتوزیان، ۱۳۹۰]. همچنین، در قانون آیین دادرسی کیفری (۱۳۹۲)، به امکان استناد به ادله الکترونیکی اشاره شده، اما نحوه بررسی اعتبار این نوع ادله در دادگاه‌ها به‌طور شفاف مشخص نشده است. این ابهام‌ها باعث شده که در بسیاری از دعاوی، قضات رویکردهای متفاوتی نسبت به ادله دیجیتال اتخاذ کنند که به ناهماهنگی در آرای صادره منجر می‌شود.

چالش دیگر، مشکلات مربوط به احراز اصالت و اعتبار ادله دیجیتال است. در نظام‌های حقوقی سنتی، اسناد کتبی به‌عنوان یکی از مهم‌ترین ادله اثبات دعوا مطرح بوده و برای ارزیابی صحت آن‌ها معیارهایی نظیر امضا، مهر و گواهی شهود مورد استفاده قرار می‌گیرد. اما در ادله دیجیتال، این معیارها جای خود را به روش‌های فنی نظیر امضای دیجیتال، هش‌کدها و زنجیره حفاظت از داده‌ها داده است [جعفری لنگرودی، ۱۳۹۶]. در بسیاری از موارد، دادگاه‌ها به دلیل عدم آشنایی کافی با این روش‌های فنی، در تشخیص اعتبار اسناد الکترونیکی دچار تردید می‌شوند. این مسئله به‌ویژه در مواردی که ادله دیجیتال ممکن است مورد جعل یا تغییر قرار گرفته باشد، اهمیت بیشتری پیدا می‌کند.

یکی دیگر از مشکلات اساسی در پذیرش ادله دیجیتال، عدم وجود رویه قضایی یکپارچه در ارزیابی این نوع ادله است. در برخی پرونده‌ها، دادگاه‌ها اسناد الکترونیکی نظیر پیامک‌ها، ایمیل‌ها و تصاویر ضبط‌شده در فضای دیجیتال را به‌عنوان دلیل معتبر می‌پذیرند، اما در برخی دیگر، این نوع ادله به دلیل عدم امکان احراز اصالت یا احتمال دستکاری رد می‌شوند [نوری، ۱۴۰۰]. نبود استانداردهای مشخص در این زمینه موجب شده که اصحاب دعوا با عدم قطعیت در پذیرش ادله دیجیتال مواجه شوند و در بسیاری از موارد، پرونده‌ها به دلیل نبود شواهد مستند کافی با دشواری روبه‌رو شوند.

یکی دیگر از چالش‌های مهم، مسائل مرتبط با زنجیره حفاظت از ادله دیجیتال (Chain of Custody) است. در ادله سنتی، امکان ارزیابی صحت و اصالت از طریق روش‌های سنتی نظیر بررسی امضا یا مطابقت با نسخه‌های دیگر وجود دارد، اما در مورد ادله دیجیتال، چنانچه فرآیند جمع‌آوری، نگهداری و انتقال آن‌ها به درستی انجام نشود، احتمال تغییر یا تخریب داده‌ها وجود دارد [رضایی، ۱۳۹۸]. در نظام‌های حقوقی پیشرفته، استانداردهای مشخصی برای ثبت و نگهداری ادله دیجیتال وجود دارد، اما در ایران، هنوز دستورالعمل‌های روشنی در این زمینه تدوین نشده است که این امر می‌تواند باعث تضعیف ارزش اثباتی این نوع ادله در دعاوی شود. یکی از دیگر مسائل اساسی در این حوزه، تعارض میان پذیرش ادله دیجیتال و حقوق بنیادین افراد، به‌ویژه حق حریم خصوصی است. جمع‌آوری برخی از ادله دیجیتال، به‌ویژه در دعاوی کیفری، ممکن است به نقض حریم خصوصی افراد منجر شود. به‌عنوان مثال، ضبط مکالمات، دسترسی به پیام‌های خصوصی یا استخراج داده‌های شخصی از دستگاه‌های الکترونیکی بدون رضایت مالک، می‌تواند ناقض حقوق اشخاص باشد [احسینی، ۱۳۹۹]. در برخی نظام‌های حقوقی، چنین ادله‌ای به دلیل غیرقانونی بودن نحوه دستیابی به آن‌ها، فاقد اعتبار تلقی می‌شود، اما در برخی موارد، بسته به اهمیت ادله در کشف حقیقت، ممکن است استثنائاتی در این زمینه اعمال شود. در نظام حقوقی ایران، هنوز چارچوب مشخصی برای تعیین میزان اعتبار ادله‌ای که با نقض حریم خصوصی به‌دست آمده است، وجود ندارد که این مسئله می‌تواند منجر به صدور آرای متناقض در دادگاه‌ها شود.

با توجه به چالش‌های مطرح‌شده، پذیرش ادله دیجیتال در نظام قضایی ایران نیازمند اصلاحات قانونی، تدوین استانداردهای دقیق‌تر، توسعه آموزش‌های تخصصی برای قضات و کارشناسان و ایجاد نهادهای تخصصی برای بررسی این نوع ادله است. بهره‌گیری از تجربیات سایر کشورها در زمینه تدوین دستورالعمل‌های فنی و حقوقی برای ارزیابی ادله دیجیتال نیز می‌تواند به بهبود وضعیت فعلی کمک کند. در مجموع، هرچند ادله دیجیتال به‌عنوان یکی از ابزارهای مهم اثبات دعوا در نظام حقوقی ایران پذیرفته شده است، اما چالش‌های موجود نشان می‌دهد که هنوز نیاز به تکمیل قوانین و بهبود رویه‌های قضایی در این حوزه احساس می‌شود.

۵- چالش‌های مرتبط با حقوق متهم و حریم خصوصی در پذیرش ادله دیجیتال

در نظام‌های حقوقی مختلف، حفظ حقوق متهم و حریم خصوصی از اصول بنیادین دادرسی عادلانه محسوب می‌شود. با پیشرفت فناوری اطلاعات و افزایش استفاده از ادله دیجیتال در دعاوی کیفری، این دو اصل با چالش‌های متعددی مواجه شده‌اند. پذیرش و استفاده از ادله دیجیتال، به‌ویژه در فرآیندهای کیفری، می‌تواند به نقض حریم خصوصی افراد منجر شود. این مسئله از جهات مختلفی حائز اهمیت است، زیرا در برخی موارد، اطلاعات دیجیتال بدون رضایت افراد جمع‌آوری شده یا از طریق روش‌های غیرقانونی به‌دست می‌آیند. این چالش‌ها باعث شده که در بسیاری از نظام‌های حقوقی، بحث‌های گسترده‌ای پیرامون تعادل میان حفظ امنیت عمومی و حمایت از حقوق فردی مطرح شود [کاتوزیان، ۱۳۹۰].

یکی از مهم‌ترین چالش‌ها در این زمینه، شیوه‌های جمع‌آوری و دسترسی به داده‌های دیجیتال است. در بسیاری از موارد، نهادهای مجری قانون برای کشف جرم به اطلاعات خصوصی افراد نظیر پیام‌های متنی، ایمیل‌ها، داده‌های تلفن همراه و اطلاعات ذخیره‌شده در فضای ابری دسترسی پیدا می‌کنند. این امر می‌تواند ناقض اصل حریم خصوصی باشد، به‌ویژه زمانی که این اطلاعات بدون مجوز قانونی یا بدون رعایت فرآیندهای دادرسی منصفانه جمع‌آوری شده باشند [حسینی، ۱۳۹۸]. در نظام حقوقی ایران، اگرچه قانون آیین دادرسی کیفری (۱۳۹۲) در برخی مواد به لزوم رعایت حقوق متهم اشاره دارد، اما هنوز ضوابط روشنی برای محدودیت‌های دسترسی به اطلاعات دیجیتال افراد وجود ندارد. نبود قوانین صریح در این زمینه باعث شده که در برخی پرونده‌ها، نهادهای امنیتی و قضایی بدون داشتن مجوز قضایی معتبر، اقدام به بررسی داده‌های دیجیتال افراد کنند که این امر می‌تواند زمینه‌ساز نقض حریم خصوصی شود.

چالش دیگر، مشکل احراز رضایت در جمع‌آوری داده‌های دیجیتال است. در بسیاری از پرونده‌ها، متهمان ادعا می‌کنند که اطلاعات دیجیتال آن‌ها بدون رضایت یا از طریق روش‌های غیرمجاز جمع‌آوری شده است. به‌عنوان مثال، ضبط مکالمات تلفنی یا دریافت اطلاعات حساب‌های کاربری شبکه‌های اجتماعی بدون رضایت فرد، یکی از موضوعات مورد مناقشه در رویه قضایی است [انوری، ۱۴۰۰]. در برخی نظام‌های حقوقی، نظیر ایالات متحده و اتحادیه اروپا، استفاده از ادله‌ای که از طریق نقض حریم خصوصی به‌دست آمده باشد، غیرقابل استناد تلقی می‌شود. اما در نظام حقوقی ایران، هنوز رویه مشخصی در این زمینه وجود ندارد و این امر باعث شده که در برخی دعاوی، دادگاه‌ها تصمیمات متفاوتی درباره اعتبار این نوع ادله اتخاذ کنند. این موضوع به‌ویژه در پرونده‌هایی که مرتبط با جرایم اینترنتی یا اقتصادی هستند، بیشتر نمود پیدا می‌کند.

علاوه بر این، نگرانی‌هایی درباره امکان سوءاستفاده از داده‌های دیجیتال برای ایجاد اتهامات نادرست یا پرونده‌سازی‌های غیرواقعی وجود دارد. در برخی موارد، داده‌های دیجیتال ممکن است دستکاری شده یا بدون توجه به زمینه‌های خاص مورد استناد قرار گیرند. به‌عنوان مثال، ارسال یک پیام متنی از سوی شخصی دیگر که به نام متهم ثبت شده باشد، می‌تواند به‌عنوان دلیل محکومیت وی در نظر گرفته شود، درحالی‌که امکان جعل یا تغییر این پیام‌ها از نظر فنی وجود دارد [رضایی، ۱۳۹۹]. در این شرایط،

چنانچه دادگاه‌ها بدون انجام بررسی‌های فنی لازم، اقدام به پذیرش این نوع ادله کنند، ممکن است حقوق متهم نقض شود. در نظام‌های حقوقی پیشرفته، معیارهایی برای بررسی اصالت داده‌های دیجیتال تعیین شده است، اما در ایران، هنوز دستورالعمل‌های استاندارد برای بررسی این مسائل تدوین نشده که این امر می‌تواند به صدور احکام ناعادلانه منجر شود.

یکی دیگر از چالش‌های اساسی، تعارض میان امنیت عمومی و حقوق فردی در مواجهه با ادله دیجیتال است. در برخی پرونده‌های امنیتی یا مرتبط با جرایم سازمان‌یافته، دستگاه‌های قضایی و انتظامی برای مقابله با تهدیدات امنیتی اقدام به جمع‌آوری و تحلیل گسترده داده‌های دیجیتال می‌کنند. این موضوع می‌تواند با توجیه "حفظ امنیت ملی"، به نقض گسترده حریم خصوصی افراد منجر شود [جعفری لنگرودی، ۱۳۹۵]. برای مثال، شنود مکالمات تلفنی یا نظارت بر فعالیت‌های اینترنتی افراد، اگرچه می‌تواند در کشف برخی جرایم مؤثر باشد، اما در عین حال ممکن است زمینه‌ساز نقض حریم خصوصی شهروندان و ایجاد یک فضای نظارتی گسترده شود. در چنین شرایطی، چالش اصلی، تعیین حدود و چارچوبی مشخص برای نظارت بر داده‌های دیجیتال است، به گونه‌ای که هم امنیت عمومی تأمین شود و هم حقوق متهمان و شهروندان مورد احترام قرار گیرد.

در مجموع، چالش‌های مرتبط با حقوق متهم و حریم خصوصی در پذیرش ادله دیجیتال در نظام حقوقی ایران، نشان‌دهنده ضرورت اصلاح قوانین و تدوین مقررات مشخص برای تعیین نحوه جمع‌آوری، پردازش و استفاده از داده‌های دیجیتال است. توسعه دستورالعمل‌های فنی و حقوقی، تدوین رویه‌های استاندارد برای ارزیابی اعتبار ادله دیجیتال و تعیین ضوابط شفاف برای نظارت بر داده‌های شخصی، می‌تواند به کاهش این چالش‌ها کمک کند. همچنین، تجربه سایر کشورها نشان می‌دهد که اتخاذ رویکردهایی مانند ممنوعیت استفاده از ادله‌ای که به صورت غیرقانونی جمع‌آوری شده‌اند، می‌تواند به تضمین بیشتر حقوق متهمان کمک کند. بنابراین، اصلاح نظام حقوقی ایران در این حوزه، امری ضروری به نظر می‌رسد.

۶- پیشنهاد‌های قانونی برای بهبود پذیرش و استناد به ادله دیجیتال

در دنیای امروز، نقش فناوری‌های نوین در فرآیندهای قضایی به طور فزاینده‌ای گسترش یافته و ادله دیجیتال به یکی از مهم‌ترین ابزارهای اثبات در دعاوی مدنی و کیفری تبدیل شده است. با این حال، پذیرش و استناد به این نوع ادله در نظام حقوقی ایران با چالش‌های متعددی مواجه است. مشکلاتی از قبیل ابهام در قوانین موجود، نبود استانداردهای مشخص برای احراز اصالت و اعتبار داده‌های دیجیتال، فقدان رویه قضایی یکسان، و تعارض میان حریم خصوصی و امنیت عمومی، نشان‌دهنده ضرورت اصلاح و تکمیل قوانین در این زمینه است [کاتوزیان، ۱۳۹۰]. در این راستا، پیشنهاد‌های قانونی متعددی برای بهبود پذیرش و استناد به ادله دیجیتال در نظام حقوقی ایران ارائه می‌شود.

یکی از مهم‌ترین پیشنهادها، اصلاح و تکمیل قوانین آیین دادرسی در حوزه ادله دیجیتال است. هرچند قانون آیین دادرسی کیفری مصوب ۱۳۹۲ در برخی مواد، امکان استفاده از ادله دیجیتال را به رسمیت شناخته است، اما همچنان ابهامات زیادی در زمینه معیارهای پذیرش، نحوه ارزیابی و میزان اعتبار این ادله وجود دارد [جعفری لنگرودی، ۱۳۹۵]. پیشنهاد می‌شود که در قوانین آیین دادرسی مدنی و کیفری، فصلی مستقل به ادله دیجیتال اختصاص داده شود که در آن، ضوابط مربوط به جمع‌آوری، نگهداری، ارزیابی و استناد به این نوع ادله به طور شفاف مشخص گردد. همچنین، باید در این قوانین، محدودیت‌های قانونی برای جلوگیری از دستکاری یا جعل داده‌های دیجیتال مورد توجه قرار گیرد.

ایجاد نهادهای تخصصی برای بررسی ادله دیجیتال از دیگر پیشنهادها ضروری در این حوزه است. در بسیاری از کشورها، نهادهایی تخصصی برای ارزیابی و بررسی ادله دیجیتال تشکیل شده‌اند که مسئولیت احراز اصالت و اعتبار این نوع داده‌ها را بر عهده دارند. در ایران نیز پیشنهاد می‌شود که یک نهاد مستقل تحت نظارت قوه قضائیه ایجاد شود که دارای کارشناسان فنی و حقوقی در زمینه فناوری اطلاعات باشد. این نهاد می‌تواند مسئولیت بررسی ادله دیجیتال ارائه شده در محاکم، تعیین صحت و اصالت آن‌ها، و ارائه گزارش‌های فنی به دادگاه‌ها را بر عهده داشته باشد [حسینی، ۱۳۹۸]. تأسیس چنین نهادی می‌تواند موجب کاهش اختلاف‌نظرها در رویه قضایی و افزایش اطمینان به ادله دیجیتال شود.

یکی دیگر از اصلاحات ضروری، تعیین معیارهای مشخص برای احراز اعتبار ادله دیجیتال است. در حال حاضر، برخی از دادگاه‌ها به دلیل نبود معیارهای دقیق، در ارزیابی صحت و اعتبار داده‌های دیجیتال با مشکل مواجه هستند. برای حل این مشکل، پیشنهاد می‌شود که معیارهای فنی مشخصی در قوانین پیش‌بینی شود که شامل مواردی همچون امضای دیجیتال، هش کدها، زنجیره حفاظت از داده‌ها (Chain of Custody)، و گواهی تأیید از سوی مراجع رسمی باشد [رضایی، ۱۳۹۹]. همچنین، باید ضوابطی برای نحوه استناد به اسناد دیجیتال در دعاوی مدنی و کیفری تدوین گردد، به گونه‌ای که این اسناد تنها در صورت رعایت استانداردهای فنی و قانونی قابل پذیرش باشند.

تقویت حمایت‌های قانونی از حریم خصوصی افراد در مواجهه با ادله دیجیتال نیز از دیگر موضوعات مهمی است که باید در اصلاح قوانین مورد توجه قرار گیرد. با توجه به اینکه جمع‌آوری برخی از داده‌های دیجیتال ممکن است منجر به نقض حریم خصوصی افراد شود، ضروری است که در قوانین مشخص شود که چه نهادهایی و تحت چه شرایطی مجاز به دسترسی به اطلاعات دیجیتال اشخاص هستند. پیشنهاد می‌شود که همانند برخی کشورها، اصل "عدم اعتبار ادله به‌دست‌آمده از طریق نقض حریم خصوصی" در قوانین ایران نیز به رسمیت شناخته شود [نوری، ۱۴۰۰]. به این ترتیب، دادگاه‌ها نباید ادله‌ای را که از طریق روش‌های غیرقانونی و بدون مجوز قضایی به‌دست آمده است، به عنوان دلیل معتبر بپذیرند. این امر می‌تواند موجب تقویت حقوق متهمان و شهروندان شده و از سوءاستفاده احتمالی از داده‌های دیجیتال جلوگیری کند.

علاوه بر این، توسعه آموزش‌های تخصصی برای قضات، وکلاء و ضابطان قضایی در زمینه ادله دیجیتال یکی از اقدامات ضروری برای بهبود پذیرش و استناد به این نوع ادله در نظام حقوقی ایران است. بسیاری از چالش‌های مرتبط با ادله دیجیتال ناشی از عدم آگاهی کافی قضات و کارشناسان قضایی از جنبه‌های فنی این ادله است. پیشنهاد می‌شود که دوره‌های آموزشی تخصصی برای قضات و وکلاء برگزار شود تا آن‌ها با نحوه ارزیابی صحت و اعتبار داده‌های دیجیتال آشنا شوند. همچنین، باید در دوره‌های آموزشی ضابطان قضایی، نحوه صحیح جمع‌آوری و نگهداری و ارائه ادله دیجیتال آموزش داده شود تا از بروز خطاهای فنی و حقوقی در این زمینه جلوگیری گردد [حسینی، ۱۳۹۸].

در مجموع، پذیرش و استناد به ادله دیجیتال در نظام حقوقی ایران نیازمند اصلاحات قانونی گسترده و ایجاد سازوکارهای اجرایی مؤثر است. اصلاح قوانین آیین دادرسی، ایجاد نهادهای تخصصی، تعیین معیارهای مشخص برای احراز اعتبار ادله دیجیتال، تقویت حمایت‌های قانونی از حریم خصوصی، و توسعه آموزش‌های تخصصی، از جمله اقداماتی هستند که می‌توانند موجب افزایش اطمینان به این نوع ادله در محاکم قضایی شوند. بهره‌گیری از تجارب سایر کشورها در این زمینه و تدوین قوانین جامع و دقیق، می‌تواند به بهبود وضعیت موجود و کاهش چالش‌های مرتبط با پذیرش و استناد به ادله دیجیتال در نظام قضایی ایران کمک کند.

۷- راهکارهای فنی و اجرایی برای افزایش دقت و امنیت ادله دیجیتال

با گسترش استفاده از فناوری‌های نوین در فرآیندهای قضایی، ادله دیجیتال به یکی از مهم‌ترین ابزارهای اثبات در دعوی مدنی و کیفری تبدیل شده است. با این حال، ماهیت غیرملموس و قابلیت تغییرپذیری بالای این نوع ادله، چالش‌های متعددی را در زمینه دقت و امنیت آن‌ها به وجود آورده است. جعل، حذف یا تغییر داده‌های دیجیتال می‌تواند منجر به تحریف واقعیت در فرآیند دادرسی شود و از سوی دیگر، نبود استانداردهای مشخص برای جمع‌آوری و تحلیل این داده‌ها، موجب کاهش اعتماد قضات و سایر مراجع قانونی به این نوع ادله می‌شود [کاتوزیان، ۱۳۹۰]. بنابراین، برای افزایش دقت و امنیت ادله دیجیتال، اتخاذ راهکارهای فنی و اجرایی مناسب ضروری است.

یکی از مهم‌ترین راهکارهای فنی برای افزایش امنیت ادله دیجیتال، استفاده از فناوری رمزنگاری و امضای دیجیتال است. داده‌های دیجیتال باید از لحظه ایجاد تا زمان ارائه در دادگاه، به گونه‌ای رمزگذاری شوند که از هرگونه دستکاری یا تغییر غیرمجاز جلوگیری شود. امضای دیجیتال، که مبتنی بر فناوری رمزنگاری کلید عمومی است، می‌تواند هویت تولیدکننده داده و صحت آن را تأیید کند. در بسیاری از نظام‌های حقوقی پیشرفته، استفاده از امضای دیجیتال برای تأیید اصالت اسناد الکترونیکی اجباری شده است و پیشنهاد می‌شود که این الزام در نظام حقوقی ایران نیز به عنوان یکی از معیارهای اعتبار ادله دیجیتال لحاظ گردد [جعفری لنگرودی، ۱۳۹۵].

ایجاد زنجیره حفاظت از داده‌ها (Chain of Custody) یکی دیگر از راهکارهای کلیدی برای افزایش دقت ادله دیجیتال است. این زنجیره به فرآیندی اشاره دارد که در آن تمامی مراحل جمع‌آوری، انتقال، ذخیره‌سازی و تحلیل داده‌های دیجیتال به صورت دقیق ثبت و مستندسازی می‌شود. اجرای این فرآیند تضمین می‌کند که هیچ‌گونه تغییر، حذف یا دستکاری غیرمجاز در داده‌های دیجیتال رخ نداده است. در کشورهای پیشرفته، تمامی ادله دیجیتال باید از طریق زنجیره حفاظت مستند شوند و هرگونه وقفه یا تغییر در این زنجیره، می‌تواند موجب بی‌اعتباری آن در دادگاه شود. پیشنهاد می‌شود که در نظام حقوقی ایران نیز دستورالعملی جامع برای نحوه ثبت و حفظ زنجیره حفاظت از داده‌های دیجیتال تدوین گردد تا از هرگونه تغییر یا سوءاستفاده احتمالی جلوگیری شود [حسینی، ۱۳۹۸].

یکی دیگر از راهکارهای مهم برای افزایش امنیت ادله دیجیتال، استفاده از فناوری بلاکچین برای ذخیره و تأیید اصالت داده‌ها است. بلاکچین به عنوان یک فناوری غیرمتمرکز و تغییرناپذیر، می‌تواند برای ذخیره‌سازی و مدیریت داده‌های دیجیتال مورد استفاده قرار گیرد. با استفاده از این فناوری، هر تغییری در داده‌های دیجیتال به طور شفاف ثبت شده و غیرقابل انکار خواهد بود. برخی کشورها مانند استونی، از بلاکچین برای مدیریت اسناد دولتی و قضایی استفاده می‌کنند و این فناوری باعث افزایش امنیت و شفافیت در فرآیندهای حقوقی شده است. پیشنهاد می‌شود که در ایران نیز، امکان استفاده از بلاکچین در فرآیند ثبت و استناد به داده‌های دیجیتال مورد بررسی و اجرا قرار گیرد [نوری، ۱۴۰۰].

علاوه بر راهکارهای فنی، ایجاد یک نهاد تخصصی برای ارزیابی ادله دیجیتال می‌تواند به افزایش دقت و امنیت این نوع ادله کمک کند. در حال حاضر، دادگاه‌ها و مراجع قضایی ایران فاقد یک نهاد مستقل و تخصصی برای بررسی و ارزیابی ادله دیجیتال هستند و این امر باعث شده که در برخی پرونده‌ها، اعتبار این ادله مورد تردید قرار گیرد. پیشنهاد می‌شود که یک مرکز تخصصی تحت نظارت قوه قضائیه ایجاد شود که وظیفه آن بررسی و تأیید صحت و اصالت ادله دیجیتال باشد. این مرکز باید از متخصصان حوزه فناوری اطلاعات، حقوق و جرم‌شناسی دیجیتال تشکیل شده و دارای امکانات فنی پیشرفته برای تحلیل داده‌های دیجیتال باشد. ایجاد چنین مرکزی می‌تواند از بروز اشتباهات قضایی ناشی از استفاده از ادله جعلی یا تغییریافته جلوگیری کند [رضایی، ۱۳۹۹].

توسعه آموزش‌های تخصصی برای قضات، وکلاء و ضابطان قضایی نیز یکی دیگر از اقدامات ضروری برای افزایش دقت و امنیت ادله دیجیتال است. بسیاری از مشکلاتی که در پذیرش و استناد به این نوع ادله در محاکم قضایی ایران وجود دارد، ناشی از عدم آشنایی کافی قضات و کارشناسان قضایی با جنبه‌های فنی ادله دیجیتال است. پیشنهاد می‌شود که دوره‌های آموزشی تخصصی

برای تمامی افرادی که در فرآیند دادرسی نقش دارند، برگزار شود تا آن‌ها با اصول جمع‌آوری، تحلیل، و ارزیابی ادله دیجیتال آشنا شوند. همچنین، باید دوره‌های آموزشی برای نیروهای پلیس فتا و سایر ضابطان قضایی تدوین شود تا آن‌ها با شیوه‌های صحیح جمع‌آوری و حفاظت از داده‌های دیجیتال آشنا شوند و از بروز خطاهای فنی و حقوقی جلوگیری گردد [حسینی، ۱۳۹۸].

ایجاد قوانین و مقررات سخت‌گیرانه‌تر برای مقابله با جعل و تغییر ادله دیجیتال نیز می‌تواند به افزایش امنیت این نوع داده‌ها کمک کند. در حال حاضر، قوانین کیفری ایران، مجازات‌های مشخصی برای جعل اسناد دیجیتال تعیین نکرده است و این امر باعث شده که برخی افراد با سوءاستفاده از خلأهای قانونی، اقدام به تغییر یا جعل داده‌های دیجیتال کنند. پیشنهاد می‌شود که در قوانین جزایی، مجازات‌های سنگین‌تری برای افرادی که اقدام به تغییر، حذف یا جعل ادله دیجیتال می‌کنند، در نظر گرفته شود تا از وقوع این جرایم جلوگیری گردد [نوری، ۱۴۰۰].

در مجموع، افزایش دقت و امنیت ادله دیجیتال مستلزم اجرای راهکارهای فنی و اجرایی متعددی است. استفاده از فناوری‌های رمزنگاری و امضای دیجیتال، ایجاد زنجیره حفاظت از داده‌ها، بهره‌گیری از فناوری بلاکچین، ایجاد نهادهای تخصصی برای بررسی ادله دیجیتال، توسعه آموزش‌های تخصصی، و وضع قوانین سخت‌گیرانه‌تر برای مقابله با جعل و تغییر داده‌های دیجیتال، از جمله اقداماتی هستند که می‌توانند موجب بهبود وضعیت پذیرش و استناد به ادله دیجیتال در نظام قضایی ایران شوند. اجرای این راهکارها نه تنها باعث افزایش اطمینان به این نوع ادله در محاکم قضایی خواهد شد، بلکه می‌تواند از بروز اشتباهات قضایی و سوءاستفاده‌های احتمالی جلوگیری کند.

۸- لزوم آموزش قضات، وکلا و کارشناسان حوزه حقوقی و دیجیتال

با گسترش فناوری‌های نوین و افزایش استفاده از داده‌های دیجیتال در فرآیندهای حقوقی و قضایی، لزوم آموزش تخصصی برای قضات، وکلا و کارشناسان حوزه حقوقی بیش از پیش احساس می‌شود. امروزه، بسیاری از دعاوی مدنی و کیفری شامل ادله‌ای هستند که به صورت دیجیتال ثبت و ارائه می‌شوند؛ از جمله پیام‌های الکترونیکی، اسناد دیجیتال، داده‌های ثبت شده در شبکه‌های اجتماعی، و اطلاعات ذخیره شده در پایگاه‌های داده. با این حال، نبود آگاهی کافی در میان قضات و وکلا نسبت به مفاهیم فنی و حقوقی مرتبط با این ادله، می‌تواند منجر به اشتباه در تصمیم‌گیری‌های قضایی، تفسیر نادرست قوانین، و حتی تضییع حقوق طرفین دعوی شود [کاتوزیان، ۱۳۹۰]. بنابراین، آموزش تخصصی در حوزه حقوق دیجیتال به عنوان یک ضرورت اجتناب‌ناپذیر مطرح می‌شود. یکی از مهم‌ترین دلایل ضرورت آموزش، افزایش پیچیدگی دعاوی مربوط به جرایم سایبری و ادله دیجیتال است. با رشد جرایم سایبری، نظیر کلاهبرداری اینترنتی، جعل هویت دیجیتال، و نفوذ غیرمجاز به سامانه‌های اطلاعاتی، نقش فناوری در فرآیند دادرسی بیش از گذشته مورد توجه قرار گرفته است. بسیاری از این جرایم بر پایه شواهد دیجیتال بنا شده‌اند که بررسی و تحلیل آن‌ها مستلزم آشنایی کامل با مفاهیم فنی و اصول حقوقی مرتبط است. چنانچه قضات و وکلای دادگستری فاقد دانش کافی در این زمینه باشند، ممکن است در تفسیر ادله دیجیتال دچار سردرگمی شوند یا اعتبار آن‌ها را نادیده بگیرند [جعفری لنگرودی، ۱۳۹۵]. از این رو، پیشنهاد می‌شود که برنامه‌های آموزشی در زمینه حقوق دیجیتال و فناوری‌های مرتبط در قوه قضائیه، کانون‌های وکلای دادگستری، و دانشگاه‌های حقوقی گسترش یابد.

ضرورت آشنایی با اصول بررسی و احراز اصالت ادله دیجیتال نیز یکی دیگر از ابعاد مهم این موضوع است. داده‌های دیجیتال به دلیل ویژگی‌هایی همچون تغییرپذیری، امکان جعل، و قابلیت حذف شدن، نیازمند روش‌های خاصی برای احراز اصالت و اعتبار

هستند. در بسیاری از موارد، تعیین اینکه آیا یک سند الکترونیکی اصل است یا تغییر یافته، نیازمند دانش فنی تخصصی و استفاده از روش‌های علمی مانند تحلیل متادیتا، بررسی امضای دیجیتال، و ردیابی زنجیره حفاظت از داده‌ها (Chain of Custody) است [حسینی، ۱۳۹۸]. در نتیجه، آموزش قضات و وکلای درباره این اصول، از اهمیت بالایی برخوردار است و می‌تواند موجب افزایش دقت در تصمیم‌گیری‌های قضایی شود.

نقش آموزش در کاهش تضاد رویه‌های قضایی در برخورد با ادله دیجیتال نیز قابل توجه است. در حال حاضر، نبود رویه واحد در دادگاه‌های ایران نسبت به پذیرش و استناد به ادله دیجیتال، یکی از چالش‌های اساسی در حوزه حقوق دیجیتال محسوب می‌شود. برخی از قضات به دلیل ناآگاهی از جنبه‌های فنی این نوع ادله، از پذیرش آن‌ها خودداری می‌کنند یا در مواردی، ارزیابی آن‌ها را بر اساس معیارهای سنتی انجام می‌دهند که منجر به نادیده گرفتن ارزش واقعی داده‌های دیجیتال می‌شود. آموزش مداوم می‌تواند موجب ارتقای سطح علمی قضات و ایجاد رویه‌ای هماهنگ در برخورد با ادله دیجیتال گردد [رضایی، ۱۳۹۹].

علاوه بر این، ضرورت آموزش کارشناسان حقوقی و فناوری اطلاعات نیز حائز اهمیت است. کارشناسان رسمی دادگستری که وظیفه بررسی ادله دیجیتال و ارائه نظرات تخصصی را بر عهده دارند، باید از دانش کافی در زمینه تحلیل داده‌های الکترونیکی برخوردار باشند. امروزه، برخی از کارشناسان فاقد اطلاعات کافی درباره روش‌های کشف جرائم سایبری، تحلیل داده‌های رمزگذاری شده، و تشخیص حملات سایبری هستند، که این امر می‌تواند بر اعتبار نظرات کارشناسی ارائه شده در دادگاه تأثیر منفی بگذارد. پیشنهاد می‌شود که دوره‌های تخصصی برای این کارشناسان برگزار شود و در طی آن، آن‌ها با اصول جرم‌شناسی دیجیتال، تحلیل داده‌های رایانه‌ای، و روش‌های بازبینی اطلاعات آشنا شوند [نوری، ۱۴۰۰].

یکی دیگر از راهکارهای مؤثر برای ارتقای سطح دانش حقوقی در این حوزه، ایجاد دوره‌های آموزشی مشترک میان رشته حقوق و فناوری اطلاعات در دانشگاه‌ها است. در حال حاضر، بسیاری از برنامه‌های درسی دانشکده‌های حقوق فاقد دروس مرتبط با حقوق فناوری اطلاعات، جرایم سایبری، و ادله دیجیتال هستند. پیشنهاد می‌شود که دانشگاه‌ها اقدام به ارائه دوره‌های بین‌رشته‌ای کنند که در آن، دانشجویان حقوق با مفاهیم پایه‌ای فناوری اطلاعات و اصول تحلیل داده‌های دیجیتال آشنا شوند. این اقدام می‌تواند در تربیت نسل جدیدی از قضات، وکلای، و کارشناسان حقوقی که توانایی درک و تحلیل ادله دیجیتال را دارند، نقش مؤثری ایفا کند [حسینی، ۱۳۹۸].

در نهایت، ضرورت آموزش پیوسته و به‌روزرسانی اطلاعات حقوقی و فنی برای قضات و وکلای دادگستری نباید نادیده گرفته شود. با توجه به سرعت پیشرفت فناوری و تغییر مداوم روش‌های ارتکاب جرایم سایبری، اطلاعات حقوقی و فنی مرتبط نیز باید به‌طور مداوم به‌روزرسانی شود. ایجاد کارگاه‌های آموزشی مستمر، انتشار مقالات علمی و کتب تخصصی در این حوزه، و استفاده از تجارب بین‌المللی می‌تواند به ارتقای سطح دانش حقوقی در این زمینه کمک کند. در بسیاری از کشورها، دوره‌های تخصصی مرتبط با حقوق دیجیتال به‌عنوان بخشی از آموزش‌های مداوم قضات و وکلای دادگستری برگزار می‌شود که این روش می‌تواند در ایران نیز اجرایی شود [نوری، ۱۴۰۰].

در مجموع، لزوم آموزش قضات، وکلای و کارشناسان حوزه حقوقی و دیجیتال، امری غیرقابل انکار است. با توجه به پیچیدگی روزافزون دعاوی مرتبط با فضای مجازی و افزایش نقش ادله دیجیتال در فرآیندهای قضایی، ضروری است که تمامی افراد فعال در این حوزه، از سطح دانش و مهارت‌های لازم برخوردار باشند. ایجاد دوره‌های آموزشی تخصصی، به‌روزرسانی مستمر دانش فنی و حقوقی، برگزاری کارگاه‌های آموزشی برای ضابطان قضایی، و تقویت همکاری میان رشته‌های حقوق و فناوری اطلاعات، از جمله اقداماتی هستند که می‌توانند موجب ارتقای سطح علمی و عملی در این زمینه شوند. بهره‌گیری از تجارب سایر کشورها و تطبیق آن‌ها با نظام حقوقی ایران، می‌تواند به بهبود پذیرش و استناد به ادله دیجیتال در محاکم کمک شایانی کند.

۹- نتیجه‌گیری

ادله دیجیتال، به عنوان یکی از ابزارهای نوین اثبات دعوا، چالش‌های متعددی را در نظام‌های حقوقی مختلف، از جمله ایران، ایجاد کرده است. پذیرش این نوع ادله در نظام‌های حقوقی مختلف مستلزم تطبیق اصول سنتی ادله با ویژگی‌های منحصر به فرد داده‌های دیجیتال است. در بررسی تطبیقی میان ایران و سایر نظام‌های حقوقی، می‌توان دریافت که هرچند بسیاری از کشورها، از جمله نظام‌های حقوقی کامن‌لا و برخی کشورهای اروپایی، گام‌های موثری در زمینه پذیرش و تفسیر این ادله برداشته‌اند، اما همچنان چالش‌هایی نظیر احراز اصالت، اعتبار، قابلیت انتساب و صحت داده‌های دیجیتال مطرح است.

در نظام حقوقی ایران، پذیرش ادله دیجیتال در قوانین مختلف مورد تأیید قرار گرفته است، اما همچنان خلأهای قانونی و رویه‌ای در نحوه ارزیابی، استناد و پذیرش این نوع ادله وجود دارد. یکی از مهم‌ترین چالش‌ها، فقدان استانداردهای مشخص در زمینه احراز اصالت و اعتبارسنجی ادله دیجیتال است. در بسیاری از موارد، قضات و مقامات قضایی به دلیل عدم تسلط کافی بر مسائل فنی و پیچیدگی‌های فناوری اطلاعات، در ارزیابی این نوع ادله با مشکل مواجه می‌شوند. در مقابل، در برخی از نظام‌های حقوقی پیشرفته‌تر، استانداردهای روشنی برای ارزیابی ادله دیجیتال تدوین شده است و نهادهای تخصصی در این حوزه نقش تعیین‌کننده‌ای در احراز اعتبار این ادله ایفا می‌کنند.

علاوه بر این، یکی از چالش‌های مهم در پذیرش ادله دیجیتال، مسئله حفاظت از حریم خصوصی و حقوق اشخاص است. در مواردی که جمع‌آوری داده‌های دیجیتال بدون رضایت افراد یا به شیوه‌های غیرقانونی انجام شده باشد، مسئله تعارض میان ضرورت کشف حقیقت و رعایت حقوق بنیادین اشخاص مطرح می‌شود. در نظام‌های حقوقی مختلف، رویه‌های متفاوتی برای حل این تعارض اتخاذ شده است. برخی کشورها با تأکید بر اصل منع تحصیل دلیل غیرقانونی، از پذیرش چنین ادله‌ای خودداری می‌کنند، در حالی که برخی دیگر، بسته به میزان تأثیر این ادله در کشف حقیقت، استثنائاتی را در نظر گرفته‌اند.

همچنین، در دعاوی کیفری، چالش‌های مربوط به زنجیره حفاظت از ادله دیجیتال (Chain of Custody) و تضمین عدم تغییر یا دست‌کاری داده‌ها، از اهمیت ویژه‌ای برخوردار است. بدون رعایت اصول دقیق در جمع‌آوری، ثبت و نگهداری این داده‌ها، امکان مخدوش شدن اعتبار آن‌ها وجود دارد. در نظام حقوقی ایران، اگرچه برخی دستورالعمل‌های اجرایی در این زمینه تدوین شده‌اند، اما همچنان نیاز به توسعه قوانین و مقررات دقیق‌تر برای مدیریت صحیح ادله دیجیتال احساس می‌شود.

در مجموع، پذیرش ادله دیجیتال در نظام‌های حقوقی، به ویژه در ایران، نیازمند اصلاحات قانونی، تدوین استانداردهای دقیق‌تر، آموزش تخصصی قضات و کارشناسان و ایجاد نهادهای تخصصی در این حوزه است. بررسی تطبیقی نشان می‌دهد که کشورهایی که در این مسیر موفق‌تر بوده‌اند، علاوه بر اصلاح قوانین، بر ارتقای توان فنی و تخصصی مراجع قضایی تأکید ویژه‌ای داشته‌اند. بنابراین، پیشنهاد می‌شود که نظام حقوقی ایران نیز با بهره‌گیری از تجربیات سایر کشورها، نسبت به تقویت مبانی قانونی، فنی و رویه‌ای در حوزه پذیرش ادله دیجیتال اقدام نماید.

۱۰- پیشنهادات پژوهش

در راستای بهبود پذیرش ادله دیجیتال در نظام حقوقی ایران و تطبیق آن با تجربیات موفق سایر کشورها، پیشنهادهای زیر ارائه می‌شود:

۱- اصلاح و تکمیل قوانین مرتبط با ادله دیجیتال:

تدوین قوانین جامع و شفاف در خصوص نحوه جمع‌آوری، اعتبارسنجی، ارائه و ارزیابی ادله دیجیتال در دعاوی مدنی و کیفری ضروری است. این قوانین باید به چالش‌هایی نظیر احراز اصالت، قابلیت انتساب و ارزش اثباتی این ادله بپردازند.

۲- ایجاد نهادهای تخصصی و تدوین استانداردهای ارزیابی ادله دیجیتال:

تشکیل مراکز تخصصی برای بررسی ادله دیجیتال و تدوین دستورالعمل‌های فنی و حقوقی استاندارد، می‌تواند به افزایش دقت و اطمینان در پذیرش این نوع ادله کمک کند. این مراکز می‌توانند نقش مهمی در آموزش و راهنمایی قضات و وکلای دادگستری ایفا کنند.

۳- توسعه آموزش‌های تخصصی برای قضات و وکلا:

به‌منظور افزایش توانمندی مراجع قضایی در تحلیل و ارزیابی ادله دیجیتال، برگزاری دوره‌های آموزشی تخصصی در حوزه فناوری اطلاعات، جرم‌شناسی دیجیتال و حقوق مرتبط ضروری است.

۴- تدوین ضوابط مشخص برای زنجیره حفاظت از ادله دیجیتال (Chain of Custody):

برای جلوگیری از تغییر، تخریب یا جعل ادله دیجیتال، لازم است فرآیندهای دقیق و مستندی برای جمع‌آوری، ثبت، نگهداری و ارائه این ادله تدوین شود. این ضوابط باید به نحوی باشد که از هرگونه دست‌کاری یا تردید در اعتبار ادله جلوگیری کند.

۵- توسعه همکاری‌های بین‌المللی و بهره‌گیری از تجربیات سایر کشورها:

با توجه به ماهیت فرامرزی جرایم سایبری و داده‌های دیجیتال، همکاری‌های بین‌المللی در زمینه استانداردسازی ادله دیجیتال، تبادل تجربیات و هماهنگ‌سازی مقررات داخلی با معیارهای جهانی می‌تواند به بهبود پذیرش این نوع ادله کمک کند.

۱۱-مراجع

- Casey, E. (۲۰۱۹), "Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet," Academic Press.
- حبیبی، م و احمدی، ن. (۱۳۹۹)، "بررسی چالش‌های پذیرش ادله دیجیتال در نظام دادرسی ایران"، فصلنامه مطالعات حقوقی ایران، ۱۵(۲)، ۷۵-۹۸.
- Kerr, O. S. (۲۰۲۱), "Computer Crime Law," West Academic Publishing.
- Voigt, P., & Bussche, A. (۲۰۱۷), "The EU General Data Protection Regulation (GDPR):" A Practical Guide. Springer.
- Reilly, J. (۲۰۲۰), "Digital Evidence: A Comprehensive Guide New York:" Tech Publishing.
- Smith, A., & Jones, B. (۲۰۲۱), "The Role of Digital Evidence in Modern Investigations," Journal of Cyber Law, ۱۵(۳), ۴۵-۶۷.
- Johnson, R. (۲۰۲۲), "Understanding the Differences Between Digital and Traditional Evidence," Legal Studies Quarterly, ۲۹(۱), ۲۳-۳۴.
- Garfinkel, S. (۲۰۱۵), "Digital forensics, cyber crime and the management of evidence," New York: Springer.

۹. Mason, J. (۲۰۱۸), "Digital Evidence in the Courtroom: A Practical Guide for Judges and Lawyers," American Bar Association.
۱۰. East, L. (۲۰۱۶), "Computer Crime Investigation and the Law," Riverside Publishing.
۱۱. کاتوزیان، ن. (۱۳۹۰)، "اثبات و دلیل اثبات"، تهران: شرکت سهامی انتشار.
۱۲. جعفری لنگرودی، م. ج. (۱۳۹۶)، "ترمینولوژی حقوق"، تهران: گنج دانش.
۱۳. جعفری لنگرودی، م. ج. (۱۳۹۲)، "مبانی فقهی و حقوقی اسناد تجاری"، تهران: کتابخانه گنج دانش.
۱۴. نوری، ح. (۱۴۰۰)، "چالش‌های پذیرش اسناد الکترونیکی در رویه قضایی ایران"، نشریه مطالعات حقوقی، ۱۸(۳)، ۷۱-۹۰.
۱۵. رضایی، ع. (۱۳۹۸)، "بررسی استانداردهای زنجیره حفاظت از ادله دیجیتال در نظام قضایی ایران"، فصلنامه حقوق و فناوری اطلاعات، ۱۵(۲)، ۳۲-۵۴.
۱۶. حسینی، م. (۱۳۹۹)، "تحلیل حقوقی تعارض میان ادله دیجیتال و حریم خصوصی"، مجله پژوهش‌های حقوقی، ۲۳(۴)، ۴۵-۶۷.