Received: 10 /10/2024
Review: 04/01/2025
Accepted: 10 /04/2025
DOI: 10.22054/jocl.2025.85062.1268

Journal of Cyber Law
No(1),Vol(2), 34-49.
ISSN: 0972-6934
www.jocl.ir

Examining the Validity and Admissibility of Algorithm-Generated Electronic Evidence in the Judicial System and Cyber Law

Amirhossein SharifzadeKhorram[1]

1- PhD Candidate in Law, Ferdowsi University of Mashhad, Mashhad, Iran

ABSTRACT

With the expansion of digital technologies and the growing role of algorithms in generating and analyzing data, algorithm-based electronic evidence has become a critical component in judicial systems and cyber law. The main question of this study is whether such evidence is legally and judicially admissible, and how its acceptance criteria are defined in courts. The importance of this topic stems from the fact that judicial decisions based on electronic data, if lacking sufficient scientific and legal credibility, may lead to violations of defendants' rights and undermine trust in the judiciary. This article aims to examine the legal, technical, and ethical dimensions of algorithm-generated electronic evidence and determine the criteria for its admissibility in courts. The research method is descriptive-analytical, relying on documentary studies, examination of national and international laws, and analysis of judicial cases. The findings indicate that accepting algorithmic evidence without established scientific and legal standards can increase the risk of errors and misuse, yet with a proper legal framework and reliable technical criteria, these evidences can be legitimately admitted in the judicial process. The innovation of this article lies in presenting an analytical model that integrates legal, technical, and ethical indicators of algorithmic electronic evidence admissibility, providing practical guidance for policymakers and judges.

Keywords:
electronic evidence, admissibility, cyber law, judicial system, legal framework

How to Cite: sharifzadekhorram, A. (2025). Examining the Validity and Admissibility of Algorithm-Generated Electronic Evidence in the Judicial System and Cyber Law. Journal of Cyber Law (JOCL), 2(1), 34-49.
doi: 10.22054/jocl.2025.85062.1268

* Corresponding Author: amirhossein.sharifzadehkhorram@um.ac.ir

نشریه حقوق سایبری
شماره (۱) ۴۹-۳۴
دوره ۱۴۰۴

تاریخ دریافت: ۱۴۰۳/۰۷/۲۰
تاریخ اصلاح: ۱۴۰۳/۱۰/۱۴
تاریخ پذیرش: ۱۴۰۴/۰۱/۲۲

بررسی اعتبار و قابلیت استناد ادله الکترونیک تولیدشده توسط الگوریتم‌ها در نظام دادرسی و حقوق سایبری

امیرحسین شریف زاده خرم

۱- دانشجوی دکترای حقوق، دانشگاه فردوسی مشهد، مشهد، ایران

چکیده

با گسترش فناوری‌های دیجیتال و نفوذ الگوریتم‌ها در تولید و تحلیل داده‌ها، ادله الکترونیک مبتنی بر الگوریتم‌ها به یکی از محورهای مهم در نظام دادرسی و حقوق سایبری تبدیل شده است. پرسش اصلی این تحقیق این است که آیا این نوع ادله از نظر قانونی و قضایی قابلیت استناد دارند و معیارهای پذیرش آن‌ها در دادگاه‌ها چگونه تعریف می‌شود. اهمیت این موضوع از آنجا ناشی می‌شود که تصمیمات قضایی بر پایه داده‌های الکترونیک، اگر بدون اعتبار علمی و حقوقی کافی اتخاذ شوند، می‌توانند به نقض حقوق متهمان و بی‌اعتمادی به نظام قضایی منجر شوند. هدف مقاله حاضر بررسی ابعاد قانونی، فنی و اخلاقی ادله الکترونیک تولیدشده توسط الگوریتم‌ها و تعیین شاخص‌های قابلیت استناد آن‌ها در دادگاه‌ها است. روش پژوهش در این مقاله توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی، بررسی قوانین ملی و بین‌المللی مرتبط و تحلیل نمونه‌های قضایی است. نتایج تحقیق نشان می‌دهد که پذیرش ادله الگوریتمی بدون استانداردهای مشخص علمی و حقوقی می‌تواند ریسک خطا و سوءاستفاده را افزایش دهد، اما با طراحی چارچوب قانونی و معیارهای فنی قابل اعتماد، امکان استناد این ادله در نظام قضایی فراهم می‌شود. نوآوری این مقاله در ارائه مدلی تحلیلی است که شاخص‌های قانونی، فنی و اخلاقی قابلیت استناد ادله الکترونیک الگوریتمی را یکپارچه می‌سازد و راهکاری عملی برای سیاست‌گذاران و قضات ارائه می‌دهد.

کلیدواژه‌ها:

ادله الکترونیک، قابلیت استناد، حقوق سایبری، نظام دادرسی، چارچوب قانونی

نحوه استناد:

شریف زاده خرم, امیرحسین . (۱۴۰۴). بررسی اعتبار و قابلیت استناد ادله الکترونیک تولیدشده توسط الگوریتم‌ها در نظام دادرسی و حقوق سایبری. حقوق سایبری, ۲(۱), ۳۴-۴۹

* ایمیل نویسنده مسئول: amirhossein.sharifzadehkhorram@um.ac.ir

مقدمه

با گسترش سریع فناوری‌های دیجیتال و نفوذ الگوریتم‌ها در زندگی روزمره و فرآیندهای قضایی، ادله الکترونیک به یکی از ارکان اصلی در نظام‌های قضایی و حقوق سایبری تبدیل شده است (حسینی، ۱۳۹۹، ص. ۱۲). این ادله که مبتنی بر داده‌های دیجیتال و پردازش الگوریتمی هستند، امکان جمع‌آوری، ذخیره و تحلیل شواهد را با دقت و سرعت بالا فراهم می‌آورند، اما همزمان با ظهور آنها، چالش‌های قانونی و قضایی جدیدی نیز مطرح شده است. یکی از مسائل اساسی در این حوزه، قابلیت استناد این نوع ادله در دادگاه‌ها و معیارهای پذیرش آنهاست. پذیرش بدون رعایت استانداردهای قانونی و فنی می‌تواند موجب تصمیمات نادرست قضایی، تضییع حقوق متهمان، و کاهش اعتماد عمومی به نظام قضایی شود (عبداللهی، ۱۴۰۰، ص. ۵۷). اهمیت موضوع زمانی پررنگ‌تر می‌شود که توجه داشته باشیم، با افزایش جرایم سایبری و توسعه تجارت الکترونیک و شبکه‌های اجتماعی، حجم و پیچیدگی داده‌های دیجیتال به شدت افزایش یافته و روند تحلیل و تفسیر شواهد سنتی دیگر پاسخگوی نیازهای قضایی نیست (احمدپور، ۱۳۹۹، ص. ۵۳). در نظام حقوقی ایران، ماده ۳۴ قانون آیین دادرسی کیفری و تبصره‌های مرتبط با آن، ضرورت ارائه ادله معتبر و قابل استناد را مورد تأکید قرار داده و مقررات خاصی برای ادله الکترونیک پیش‌بینی کرده است (قانون آیین دادرسی کیفری، ۱۳۹۲، ص. ۲۱). همچنین، اسناد بین‌المللی، از جمله کنوانسیون بوداپست در زمینه جرایم سایبری، اهمیت استفاده از شواهد الکترونیک را در پرونده‌های بین‌المللی مورد تأکید قرار داده‌اند (Smith, 2018, p. 94). این قوانین و اسناد نشان می‌دهند که پذیرش و استفاده از داده‌های دیجیتال نه تنها جنبه قانونی دارد بلکه جنبه اخلاقی و فنی نیز برای تضمین عدالت قضایی بسیار حائز اهمیت است. پژوهش‌های متعدد داخلی و بین‌المللی نشان می‌دهند که موضوع ادله دیجیتال و قابلیت استناد آنها همواره مورد توجه محققان بوده است. احمدی (۱۳۹۸، ص. ۴۵) در پژوهشی جامع به بررسی محدودیت‌های قانونی پذیرش ادله دیجیتال پرداخته و ضرورت تدوین چارچوب قانونی دقیق برای تضمین عدالت قضایی را مورد تأکید قرار داده است. کریمی (۱۳۹۷، ص. ۶۸) با تمرکز بر جنبه‌های فنی و امنیتی ادله الکترونیک، نشان داده است که عدم شفافیت الگوریتم‌ها و فقدان استانداردهای فنی معتبر می‌تواند پذیرش قضایی این نوع شواهد را با مشکل مواجه سازد. در سطح بین‌المللی، (Jones 2019, p. 132) و (Lee,2020, p. 75) به تحلیل استانداردهای دادگاه‌های آمریکا و اروپا در خصوص ادله دیجیتال پرداخته و معیارهای پذیرش، اصالت و صحت این شواهد را مورد بررسی قرار داده‌اند. همچنین (Abdullah,2021, p. 88) با تمرکز بر چارچوب‌های حقوقی بین‌المللی، محدودیت‌ها و فرصت‌های پذیرش شواهد الگوریتمی را بررسی کرده است. رضایی (۱۴۰۰، ص. ۸۱) نیز با مطالعه جنبه‌های اخلاقی و حقوقی استفاده از داده‌های الگوریتمی، خلأهای قانونی و ناهماهنگی‌های موجود در نظام حقوقی داخلی و بین‌المللی را شناسایی کرده است. با این حال، علی‌رغم مطالعات متعدد، هنوز تحلیل جامع و یکپارچه‌ای از ابعاد قانونی، فنی و اخلاقی ادله الکترونیک تولیدشده توسط الگوریتم‌ها صورت نگرفته است. بیشتر پژوهش‌ها یا بر جنبه قانونی متمرکز بوده‌اند یا جنبه فنی و امنیتی را بررسی کرده‌اند و کمتر تحقیقاتی اقدام به تلفیق همه این جنبه‌ها در قالب یک چارچوب تحلیلی کرده‌اند. این خلا پژوهشی، نیاز به یک مطالعه تحلیلی–توصیفی و تطبیقی را آشکار می‌سازد تا شاخص‌های قابلیت استناد این نوع ادله به شکل جامع شناسایی و ارائه شود. پرسش‌های اصلی تحقیق عبارتند از: چه معیارهایی برای اعتبار و قابلیت استناد ادله الکترونیک تولیدشده توسط الگوریتم‌ها

در نظام قضایی ایران و چارچوب حقوق سایبری بین‌المللی وجود دارد و چگونه می‌توان یک مدل تحلیلی برای ارزیابی آن‌ها ارائه داد؟

اهداف این تحقیق شامل بررسی قانونی و حقوقی ادله دیجیتال، تحلیل شاخص‌های فنی و امنیتی و ارائه چارچوب تحلیلی برای استناد قضایی این نوع شواهد است. علاوه بر این، تحقیق تلاش می‌کند تا با شناسایی خلأهای قانونی و ناهماهنگی‌ها در پذیرش ادله الکترونیک، راهکارهایی کاربردی برای سیاست‌گذاران، قضات و قانون‌گذاران ارائه کند تا کیفیت تصمیم‌گیری‌های قضایی ارتقاء یابد و اعتماد عمومی به نظام قضایی حفظ شود. روش پژوهش در این مقاله توصیفی–تحلیلی و مبتنی بر مطالعه اسنادی و تطبیقی است. داده‌ها از طریق مرور کتاب‌ها، مقالات علمی، قوانین و آیین‌نامه‌های داخلی و بین‌المللی جمع‌آوری شده و سپس با رویکرد تحلیلی و تطبیقی، نتایج استخراج و ارائه شده‌اند. این روش امکان می‌دهد تا محدودیت‌های قانونی، خلأهای فنی و ملاحظات اخلاقی به طور همزمان شناسایی شوند و چارچوبی یکپارچه برای ارزیابی قابلیت استناد ادله الگوریتمی تدوین گردد. علاوه بر این، تحلیل تطبیقی قوانین ایران و استانداردهای بین‌المللی به شناسایی نقاط قوت و ضعف نظام حقوقی داخلی کمک می‌کند و امکان ارائه پیشنهادهای عملی برای بهبود پذیرش ادله دیجیتال در دادگاه‌ها را فراهم می‌آورد.

در مجموع، اهمیت بررسی ادله الکترونیک تولیدشده توسط الگوریتم‌ها در نظام قضایی و حقوق سایبری نه تنها به دلیل رشد جرایم سایبری و افزایش پیچیدگی داده‌های دیجیتال است، بلکه به دلیل لزوم تضمین عدالت، شفافیت و امنیت فرآیندهای قضایی نیز بسیار حائز اهمیت می‌باشد. با تدوین چارچوبی تحلیلی و ارائه شاخص‌های قانونی، فنی و اخلاقی، این تحقیق می‌تواند گامی مؤثر در جهت ارتقاء کیفیت تصمیم‌گیری‌های قضایی و ایجاد استانداردهای پذیرش شواهد دیجیتال در ایران و در سطح بین‌المللی باشد. در نهایت، این پژوهش با ارائه مدلی جامع برای سنجش قابلیت استناد ادله الکترونیک تولیدشده توسط الگوریتم‌ها، نوآوری علمی قابل توجهی در حوزه حقوق سایبری و فناوری اطلاعات فراهم می‌آورد و مسیر مطالعات آینده در این زمینه را هموار می‌سازد.

با گسترش فناوری‌های دیجیتال و نفوذ الگوریتم‌ها در زندگی روزمره و فرآیندهای قضایی، ادله الکترونیک به یکی از ارکان اصلی نظام‌های دادرسی و حقوق سایبری تبدیل شده‌اند (حسینی، ۱۳۹۹، ص. ۱۲). این نوع ادله که مبتنی بر داده‌های دیجیتال و پردازش الگوریتمی هستند، امکان جمع‌آوری، ذخیره‌سازی و تحلیل شواهد را با دقت و سرعت بسیار بالا فراهم می‌آورند، اما همزمان با ظهور آن‌ها، چالش‌های حقوقی و قضایی قابل توجهی نیز پدید آمده است. از جمله مسائل مهم، قابلیت استناد این نوع ادله در دادگاه‌ها و معیارهای قانونی پذیرش آن‌هاست. پذیرش ادله بدون رعایت استانداردهای قانونی و فنی، می‌تواند منجر به تصمیمات نادرست قضایی، تضییع حقوق متهمان و کاهش اعتماد عمومی به نظام قضایی شود (عبداللهی، ۱۴۰۰، ص. ۵۷). اهمیت این موضوع با توجه به رشد جرایم سایبری، تجارت الکترونیک و شبکه‌های اجتماعی روزافزون، پررنگ‌تر می‌شود، زیرا حجم و پیچیدگی داده‌های دیجیتال افزایش یافته و روش‌های سنتی بررسی شواهد پاسخگوی نیازهای قضایی نیستند (احمدپور، ۱۳۹۹، ص. ۵۳).

ادله الکترونیک

ادله الکترونیک به مجموعه‌ای از شواهد دیجیتال اطلاق می‌شود که توسط ابزارهای فناوری اطلاعات تولید، ذخیره یا منتقل شده و قابلیت استفاده در فرآیندهای قضایی را دارند. این شواهد شامل داده‌های تراکنشی، لاگ‌های سیستم، ایمیل‌ها،

پیام‌های شبکه‌های اجتماعی، فایل‌های دیجیتال و حتی خروجی‌های الگوریتم‌های تحلیلی می‌شوند و می‌توانند نقش مهمی در اثبات یا رد ادعاهای قانونی ایفا کنند (Smith, 2018, p. 94). انواع ادله الکترونیک:

۱. داده‌های ذخیره‌شده: شامل اسناد دیجیتال، تصاویر، ویدئوها و ایمیل‌هایی است که در حافظه دستگاه‌های رایانه‌ای، تلفن همراه یا سرورها نگهداری می‌شوند.

۲. داده‌های منتقل‌شده: شامل پیام‌های فوری، فعالیت‌های مرورگر وب، تماس‌های صوتی اینترنتی و داده‌های شبکه‌های اجتماعی است که در حین انتقال از یک نقطه به نقطه دیگر ایجاد یا ثبت می‌شوند (Phipps, 2018, p. 2).

ادله الکترونیک ویژگی‌های خاصی دارند که آن‌ها را از سایر انواع شواهد متمایز می‌کند:

فرارپذیری: به دلیل ماهیت دیجیتال، این شواهد ممکن است به راحتی تغییر، حذف یا آسیب ببینند؛ بنابراین، حفظ زنجیره نگهداری معتبر ضروری است (Bonomi et al., 2018, p. 3).

حجم بالا: تولید انبوه داده‌ها باعث می‌شود جمع‌آوری و تحلیل شواهد نیازمند ابزارها و روش‌های پیشرفته باشد (Welty, 2015, p. 4).

تنوع منابع: شواهد دیجیتال از رایانه‌ها، تلفن‌های همراه، سرورها، شبکه‌های اجتماعی و دستگاه‌های اینترنت اشیاء به دست می‌آیند و هر منبع ویژگی‌های خاص خود را دارد (Casino et al., 2022, p. 5).

ادله الکترونیک در پرونده‌های جرایم سایبری، کلاهبرداری مالی، نقض حریم خصوصی و حتی دعاوی خانوادگی کاربرد دارند. برای مثال، سوابق تراکنش‌های دیجیتال می‌توانند در پرونده‌های مالی به عنوان شواهد اصلی یا کمکی استفاده شوند (Stoykova, 2021, p. 6).

قابلیت استناد

به معنای توانایی یک مدرک برای ایجاد اثر حقوقی در فرآیند قضایی و پذیرش آن توسط دادگاه است و تحقق این قابلیت منوط به رعایت معیارهای قانونی، فنی و اصول شفافیت و اصالت است (Jones, 2019, p. 132). یک مدرک زمانی قابلیت استناد دارد که بتواند به طور معتبر در اثبات یا رد ادعاهای طرفین دعوا نقش ایفا کند و از نظر قوانین موضوعه و رویه قضایی قابل قبول باشد. در زمینه ادله الکترونیک، این موضوع اهمیت ویژه‌ای پیدا می‌کند زیرا داده‌های دیجیتال می‌توانند به سرعت دستکاری، تغییر یا حذف شوند و بنابراین رعایت اصول زنجیره نگهداری معتبر، حفظ اصالت و شفافیت فرآیند جمع‌آوری الزامی است (Bonomi et al., 2018, p. 3). علاوه بر این، شواهد دیجیتال باید ارتباط مستقیم با موضوع پرونده داشته باشند و ارزش اثباتی آن‌ها توسط کارشناسان حقوقی و فنی تأیید شود تا دادگاه بتواند به آن‌ها اعتماد کند (Phipps, 2018, p. 2). رعایت معیارهای قانونی شامل پیروی از قوانین ملی مانند ماده ۱۲ قانون تجارت الکترونیکی و ماده ۳۴ قانون آیین دادرسی کیفری ایران است که شرایط پذیرش داده‌های دیجیتال را مشخص می‌کنند و بدون رعایت آن‌ها، امکان استناد مدرک به طور رسمی فراهم نخواهد شد (مدنی، ۱۴۰۰، ص. ۹۵). همچنین، ظهور فناوری‌های نوین مانند هوش مصنوعی و الگوریتم‌های تحلیلی باعث شده است که فرآیند تولید و تحلیل داده‌های دیجیتال به طور کامل قابل شفاف‌سازی و مستندسازی باشد تا هرگونه اثر حقوقی که از آن‌ها ناشی می‌شود، معتبر و قابل قبول باشد (Casimo et al., 2022, p. 5). قابلیت استناد نه تنها به داده‌های خام دیجیتال محدود نمی‌شود بلکه شامل خروجی‌های تحلیلی و نتایج محاسبات الگوریتمی نیز می‌شود که در صورت عدم رعایت استانداردهای فنی و حقوقی، ممکن است از نظر دادگاه فاقد ارزش اثباتی تلقی شوند (Stoykova, 2021, p. 6). علاوه بر این، تفاوت قوانین ملی و بین‌المللی،

پیچیدگی و پراکندگی منابع داده‌ها و حجم بالای اطلاعات، ضرورت تدوین دستورالعمل‌ها و استانداردهای دقیق برای جمع‌آوری، نگهداری و تحلیل ادله الکترونیک را بیش از پیش آشکار می‌سازد، چرا که بدون این چارچوب‌ها حتی شواهد معتبر نیز ممکن است رد شوند یا در فرآیند دادرسی اثر واقعی نداشته باشند (Lee, 2020, p. 88؛ Dawas et al., 2024, p. 21022). بنابراین، قابلیت استناد نه تنها یک معیار فنی یا حقوقی صرف است بلکه ترکیبی از رعایت قوانین، اصالت و صحت مدرک، شفافیت فرآیند جمع‌آوری و ارزش اثباتی مدرک در راستای عدالت قضایی محسوب می‌شود و تضمین می‌کند که شواهد ارائه شده در دادگاه بتوانند به طور مؤثر و قابل اعتماد مورد استفاده قرار گیرند، به طوری که تصمیمات قضایی مبتنی بر آن‌ها از نظر حقوقی و فنی قابل دفاع باشند و حقوق تمامی طرفین دعوا حفظ شود (Welty, 2015, p. 4).

حقوق سایبری

حقوق سایبری حوزه‌ای است که مقررات حاکم بر فضای دیجیتال، داده‌های الکترونیک و امنیت اطلاعات را تعریف و کنترل می‌کند و نقش مهمی در تعیین معیارهای قانونی پذیرش ادله دیجیتال دارد (Lee, 2020, p. 75). این حوزه شامل قوانین مربوط به حفاظت از داده‌ها، جرایم رایانه‌ای، تجارت الکترونیکی و حقوق شهروندی در فضای دیجیتال است و هدف آن تضمین استفاده مشروع از فناوری‌های نوین و ایجاد امنیت قضایی و حقوقی در محیط‌های دیجیتال می‌باشد (مدنی، ۱۴۰۰، ص. ۱۰۲). در حقوق سایبری، توجه به استانداردهای بین‌المللی، مانند کنوانسیون بوداپست و دستورالعمل‌های اتحادیه اروپا، اهمیت دارد زیرا اختلاف قوانین ملی می‌تواند پذیرش شواهد دیجیتال در پرونده‌های بین‌المللی را پیچیده کند (Casimo et al., 2022, p. 5). همچنین، حقوق سایبری با تعریف مفاهیم کلیدی مانند اصالت داده، محرمانگی اطلاعات و مسئولیت ارائه‌کنندگان خدمات اینترنتی، زمینه را برای قضاوت دقیق و پذیرش معتبر ادله دیجیتال فراهم می‌کند (Phipps, 2018, p. 2). پژوهش‌های داخلی نشان می‌دهند که تدوین قوانین شفاف و دقیق در زمینه حقوق سایبری، نه تنها موجب افزایش امنیت اطلاعات و کاهش جرایم سایبری می‌شود، بلکه توانایی دادگاه‌ها در پذیرش و ارزیابی شواهد دیجیتال را نیز بهبود می‌بخشد (رضایی، ۱۴۰۱، ص. ۸۸؛ کریمی، ۱۴۰۰، ص. ۹۷). علاوه بر این، ادله الکترونیک که در چارچوب قوانین حقوق سایبری جمع‌آوری و نگهداری می‌شوند، قابلیت استناد بالاتری دارند و می‌توانند به طور مؤثر در فرآیند قضایی مورد استفاده قرار گیرند (Jones, 2019, p. 134). در نتیجه، حقوق سایبری به‌عنوان بستری قانونی و فنی برای مدیریت داده‌های دیجیتال و شواهد الکترونیک، نقش محوری در ایجاد عدالت، حفظ حقوق شهروندان و افزایش کارایی دادگاه‌ها ایفا می‌کند و بدون آن، استفاده مؤثر از ادله دیجیتال در نظام قضایی غیرممکن خواهد بود (مدنی، ۱۴۰۰، ص. ۱۰۵).

نظام دادرسی

نظام دادرسی به چارچوب‌های حقوقی و سازمانی اطلاق می‌شود که بر نحوه رسیدگی به پرونده‌ها و تصمیم‌گیری قضایی نظارت می‌کند و شامل قوانین داخلی و بین‌المللی، اصول حقوقی و حقوق آمره قانون اساسی است که اعتبار و امنیت شواهد دیجیتال را تضمین می‌کند (محمدی، ۱۴۰۰، ص. ۱۱۲). این چارچوب‌ها تعیین می‌کنند که چگونه مدارک، از جمله ادله الکترونیک، جمع‌آوری، تحلیل و ارائه شوند تا دادگاه‌ها بتوانند تصمیمات خود را بر اساس شواهد معتبر و قابل اعتماد اتخاذ کنند. اهمیت نظام دادرسی در زمینه شواهد دیجیتال از آن جهت است که بدون وجود استانداردهای قانونی و روش‌های مشخص برای ارزیابی داده‌های دیجیتال، شواهد حتی اگر فنی و معتبر باشند، ممکن است از نظر دادگاه فاقد

ارزش اثباتی تلقی شوند (حسینی، ۱۳۹۹، ص. ۸۸). قوانین داخلی مانند ماده ۳۴ قانون آیین دادرسی کیفری و ماده ۱۲ قانون تجارت الکترونیکی چارچوب قانونی روشنی برای پذیرش شواهد دیجیتال فراهم می‌کنند و اصولی مانند اصالت مدرک، شفافیت زنجیره نگهداری و ارزش اثباتی را تعیین می‌نمایند (نجفی، ۱۴۰۱، ص. ۱۰۱). در کنار قوانین داخلی، رعایت استانداردهای بین‌المللی و کنوانسیون‌های مرتبط با جرایم رایانه‌ای و امنیت داده‌ها، به ویژه در پرونده‌های بین‌المللی، ضروری است تا شواهد دیجیتال بتوانند از نظر قانونی در کشورهای مختلف قابل پذیرش باشند (Lee, 2020, p. 75). نظام دادرسی همچنین فرآیندهای سازمانی و رویه‌ای را تعریف می‌کند که دادگاه‌ها، کارشناسان و مقامات قضایی باید در جمع‌آوری، تحلیل و ارائه شواهد دیجیتال رعایت کنند، از جمله تعیین صلاحیت کارشناسان، بررسی صحت داده‌ها و اطمینان از رعایت حقوق متهمان و شهروندان (Jones, 2019, p. 132). پژوهش‌های اخیر نشان می‌دهند که نبود یک چارچوب یکپارچه و هماهنگ می‌تواند منجر به پذیرش متفاوت شواهد دیجیتال در دادگاه‌ها شود و حتی در برخی موارد منجر به تضییع حقوق شهروندان گردد (صادقی، ۱۴۰۱، ص. ۹۵). علاوه بر این، نظام دادرسی با تأکید بر شفافیت و قابلیت ردیابی فرآیند جمع‌آوری شواهد، امنیت و اعتبار آن‌ها را تضمین می‌کند و شرایط لازم برای پذیرش قانونی ادله الکترونیک را فراهم می‌سازد (Phipps, 2018, p. 2). بدین ترتیب، نظام دادرسی نه تنها به عنوان یک چارچوب حقوقی بلکه به عنوان یک سازوکار عملی برای حفاظت از عدالت، ارزیابی صحیح شواهد و افزایش اعتماد عمومی به نظام قضایی عمل می‌کند و تضمین می‌کند که تصمیمات قضایی مبتنی بر مدارک معتبر و مطمئن اتخاذ شوند (Stoykova, 2021, p. 6). در مجموع، بدون وجود نظام دادرسی منسجم و استانداردهای روشن در زمینه شواهد دیجیتال، امکان بهره‌گیری مؤثر از ادله الکترونیک و رعایت حقوق شهروندان در فرآیندهای قضایی به شکل بهینه ممکن نخواهد بود و روند عدالت دچار چالش می‌شود (Bonomi et al., 2018, p. 3).

از منظر فقهی، قواعد اثبات و شهادت در فقه اسلامی معیارهای قابل اعتمادی برای سنجش صحت و اعتبار شواهد ارائه می‌دهند و تطبیق این قواعد با ادله دیجیتال انسجام حقوقی و پذیرش قانونی آن‌ها را تضمین می‌کند. اصولی مانند لزوم اصالت و صحت شواهد در فقه اسلامی مستلزم آن است که شواهد دیجیتال بدون دستکاری ارائه شوند و هرگونه تغییر یا عدم شفافیت در داده‌ها می‌تواند موجب رد آن‌ها در دادگاه گردد (مکارم، ۱۳۹۷، ص. ۴۵). علاوه بر این، فقه اسلامی بر حق دفاع و امکان بررسی شواهد توسط متهم تأکید دارد، بنابراین در زمینه ادله دیجیتال نیز متهم باید قادر باشد صحت داده‌های ارائه شده علیه خود را ارزیابی کرده و در صورت لزوم به آن اعتراض کند (ریاحی، ۱۴۰۰، ص. ۷۸). این سازوکار نه تنها از حقوق متهمان حفاظت می‌کند، بلکه اطمینان از دادرسی عادلانه و شفاف را افزایش می‌دهد و امکان بررسی مستقل شواهد توسط تمامی طرفین را فراهم می‌سازد. از منظر اقتصادی، پذیرش ادله الکترونیک می‌تواند هزینه‌های ناشی از خطاهای قضایی و فرآیندهای طولانی دادرسی را کاهش دهد، زیرا تحلیل دقیق داده‌ها و استفاده از ابزارها و الگوریتم‌های معتبر، احتمال تشخیص نادرست جرم یا تبرئه اشتباه را کاهش می‌دهد. استفاده مؤثر از ادله دیجیتال همچنین آثار اجتماعی مثبت قابل توجهی دارد، زیرا اعتماد عمومی به نظام قضایی افزایش یافته و اطمینان از اجرای عدالت در محیط دیجیتال تقویت می‌شود (نادرزاده، ۱۴۰۰، ص. ۹۰). بنابراین، شواهد دیجیتال نه تنها به عنوان ابزار اثباتی بلکه به عنوان عاملی برای ارتقای اعتماد عمومی و کاهش هزینه‌های اجتماعی و حقوقی عمل می‌کنند.

از نظر حقوقی داخلی، بررسی قابلیت استناد ادله الکترونیک با استناد به قوانین ملی اهمیت ویژه‌ای دارد. ماده ۳۴ قانون آیین دادرسی کیفری و تبصره‌های آن، ارائه ادله معتبر و قابل استناد را الزامی می‌داند و تصریح می‌کند که هر گونه مدرکی

که در دادگاه ارائه می‌شود باید از نظر اصالت و صحت تأیید شده باشد (قانون آیین دادرسی کیفری، ۱۳۹۲، ص. ۲۱). همچنین، ماده ۱۲ قانون جرایم رایانه‌ای و تبصره‌های مرتبط، جمع‌آوری شواهد دیجیتال و نحوه استفاده از آن‌ها را مشخص می‌سازد و چارچوب قانونی لازم برای پذیرش قانونی ادله دیجیتال را ارائه می‌دهد (سعیدی، ۱۴۰۲، ص. ۱۰۵). این قوانین با هدف تضمین عدالت قضایی و جلوگیری از تضییع حقوق متهمان تدوین شده‌اند و مبنای قانونی محکمی برای تحلیل قابلیت استناد شواهد دیجیتال فراهم می‌کنند. علاوه بر قوانین موضوعه، اصول حقوق آمره قانون اساسی ایران نیز اهمیت دارند. حق دفاع و شفافیت در رسیدگی، اصولی هستند که در اصول ۳۵، ۱۷۴ و ۱۵۶ قانون اساسی مورد تأکید قرار گرفته‌اند و نشان می‌دهند که شواهد دیجیتال باید در چارچوبی شفاف و مطابق با اصول قانونی و حقوق اساسی ارائه شوند. این اصول حقوق آمره، همراه با قوانین داخلی و قواعد فقهی، چارچوبی منسجم برای تضمین قابلیت استناد شواهد الکترونیک فراهم می‌آورند (نادرزاده، ۱۴۰۱، ص. ۹۷). به طور کلی، پذیرش شواهد دیجیتال نیازمند تعامل هماهنگ بین اصول فلسفی عدالت، قواعد فقهی، الزامات اقتصادی و چارچوب‌های قانونی داخلی و بین‌المللی است، به طوری که تمامی این مؤلفه‌ها در کنار هم، امکان تصمیم‌گیری عادلانه، شفاف و مبتنی بر داده‌های معتبر را فراهم می‌کنند (Riahi, 2022, p. 56). و همچنین شواهد دیجیتال، با رعایت استانداردهای فنی و حقوقی، می‌توانند جایگاهی محوری در فرآیندهای قضایی داشته باشند و تضمین کنند که تصمیمات دادگاه نه تنها بر اساس داده‌های معتبر و قابل اعتماد اتخاذ می‌شوند بلکه مطابق با اصول عدالت، شفافیت و حق دفاع متهم نیز هستند. این رویکرد جامع، پذیرش شواهد دیجیتال را به یک ضرورت عملی و فلسفی برای ارتقای کارایی و عدالت نظام قضایی تبدیل می‌کند و تضمین می‌کند که تکنولوژی‌های نوین در مسیر تحقق حقوق اساسی و حفظ اعتماد عمومی به نظام قضایی به کار گرفته شوند (Abdullah, 2021, p. 90).

دیدگاه‌های دکترین حقوقی نیز نشان می‌دهند که پذیرش ادله دیجیتال با چالش‌های متعددی مواجه است. کریمی (۱۳۹۷، ص. ۶۸) بر این باور است که فقدان استانداردهای فنی و عدم شفافیت الگوریتم‌ها می‌تواند پذیرش ادله دیجیتال را محدود کند. احمدپور (۱۳۹۹، ص. ۵۳) پیشنهاد می‌دهد که ترکیب معیارهای قانونی و فنی برای تضمین عدالت قضایی ضروری است. در سطح بین‌المللی، دادگاه‌های آمریکا و اروپا معیارهایی برای پذیرش شواهد دیجیتال وضع کرده‌اند (Jones,2019, p. 132) و (Lee 2020, p. 75)) نشان داده‌اند که اصالت، صحت و شفافیت اطلاعات دیجیتال از اصول کلیدی در پذیرش ادله هستند. (Abdullah,2021, p. 88) نیز چارچوب‌های بین‌المللی قانونی برای استفاده از شواهد الگوریتمی را تحلیل کرده و نقاط ضعف موجود در قوانین را شناسایی کرده است. از منظر حقوقی تطبیقی، مقایسه ایران با استانداردهای بین‌المللی نشان می‌دهد که با وجود وجود قوانین داخلی برای ادله دیجیتال، هنوز هماهنگی کامل با معیارهای بین‌المللی وجود ندارد. برای مثال، کنوانسیون بوداپست در زمینه جرایم سایبری، اهمیت حفظ اصالت و صحت شواهد دیجیتال را به‌صورت مفصل مورد تأکید قرار داده و دستورالعمل‌هایی برای جمع‌آوری، نگهداری و ارائه شواهد ارائه کرده است (Smith, 2018, p. 94). این تفاوت‌ها نشان‌دهنده ضرورت تدوین چارچوب قانونی یکپارچه در ایران است تا قابلیت استناد ادله دیجیتال همسو با استانداردهای بین‌المللی تضمین شود. از بعد اقتصادی و اجتماعی نیز قابل توجه هستند. پذیرش ادله دیجیتال می‌تواند هزینه‌های ناشی از خطاهای قضایی را کاهش دهد و با تحلیل دقیق داده‌ها، از صدور حکم نادرست جلوگیری کند. همچنین، استفاده درست از شواهد دیجیتال اعتماد عمومی به نظام قضایی را افزایش می‌دهد و شفافیت در فرآیند رسیدگی را ارتقا می‌بخشد. پژوهش‌ها نشان داده‌اند که ادله الکترونیک، با ارائه اطلاعات دقیق و قابل

اعتبار، امکان تصمیم‌گیری سریع و منصفانه را فراهم می‌آورد و موجب کاهش طول زمان رسیدگی به پرونده‌ها می‌شود (Ahmadi, 2019, p. 45).

در زمینه نظریه‌های حقوقی، دیدگاه‌های متفاوتی ارائه شده است. برخی حقوق‌دانان معتقدند که ادله دیجیتال باید از نظر اصالت، صحت و شفافیت الگوریتمی مورد بررسی قرار گیرد و تنها پس از تأیید این معیارها، قابلیت پذیرش در دادگاه را خواهند داشت (رضایی، ۱۴۰۰، ص. ۸۱). در مقابل، گروهی دیگر بر این باورند که قوانین فعلی کفایت می‌کنند و تنها نیاز به ایجاد دستورالعمل‌های فنی برای استانداردسازی شواهد دیجیتال است (حسینی، ۱۳۹۹، ص. ۲۳). این اختلاف نظرها نشان‌دهنده پیچیدگی و ضرورت تحلیل دقیق هم‌زمان ابعاد قانونی، فنی و اخلاقی است. علاوه بر آن، در سطح بین‌المللی، تحقیقات نشان می‌دهند که دادگاه‌های آمریکا و اروپا معیارهایی مانند صحت دیجیتال، عدم دستکاری، قابلیت بازتولید داده‌ها و شفافیت الگوریتم‌ها را به‌عنوان پیش‌شرط پذیرش ادله دیجیتال در نظر می‌گیرند (Lee, 2020, p. 75 Abdullah,2021, p. 88) نیز با بررسی چارچوب‌های قانونی بین‌المللی، به نقاط ضعف و خلأهای قانونی موجود در پذیرش شواهد الگوریتمی اشاره کرده است. این یافته‌ها می‌توانند به عنوان مرجع برای تقویت قوانین داخلی و ایجاد استانداردهای تطبیقی در ایران مورد استفاده قرار گیرند.

در بخش پیشینه پژوهشی داخلی و خارجی، احمدی (۱۳۹۸، ص. ۴۵) با تحلیل قوانین داخلی و نمونه‌های قضایی محدود، به محدودیت‌های قانونی در پذیرش ادله دیجیتال اشاره کرده و نیاز به چارچوب قانونی دقیق را مورد تأکید قرار داده است. حسینی (۱۳۹۹، ص. ۱۲) در مطالعه‌ای تحلیلی، نقش الگوریتم‌ها در تولید شواهد الکترونیک و تأثیر آن‌ها بر فرآیند قضایی را بررسی کرده است. عبداللهی (۱۴۰۰، ص. ۵۷) به بررسی چالش‌های حقوقی پذیرش ادله دیجیتال و اثرات آن بر تصمیم‌گیری قضایی پرداخته است. در سطح بین‌المللی، (Smith 2018, p. 94) به تحلیل استفاده از شواهد دیجیتال در پرونده‌های بین‌المللی و چالش‌های پذیرش آن‌ها پرداخته است. تحقیقات Lee (2020, p. 75 و (Abdullah,2021, p. 88) نیز به استانداردهای بین‌المللی برای اعتبارسنجی و پذیرش ادله الگوریتمی پرداخته‌اند و خلأهای قانونی و فنی را شناسایی کرده‌اند. با وجود این پیشینه گسترده، هنوز تحلیل جامع و یکپارچه‌ای از ابعاد قانونی، فنی و اخلاقی ادله الکترونیک تولیدشده توسط الگوریتم‌ها ارائه نشده است. بیشتر پژوهش‌ها یا بر جنبه قانونی متمرکز بوده‌اند یا جنبه فنی و امنیتی را بررسی کرده‌اند و کمتر تحقیقاتی اقدام به تلفیق همه این جنبه‌ها در قالب یک چارچوب تحلیلی و تطبیقی کرده‌اند. مقاله حاضر با هدف پر کردن این خلأ، شاخص‌های قابلیت استناد ادله دیجیتال را در ایران و در چارچوب استانداردهای بین‌المللی شناسایی و تحلیل می‌کند.

نتایج پژوهش های پیشین نشان می‌دهد که موضوع ادله الکترونیک و قابلیت استناد آن در نظام‌های قضایی داخلی و بین‌المللی همواره مورد توجه محققان بوده است. پژوهش‌های داخلی به‌ویژه بر جنبه قانونی و فنی تمرکز دارند. احمدی (۱۳۹۸، ص. ۴۵) با بررسی پرونده‌های سایبری در ایران به محدودیت‌های قانونی موجود و ضرورت تدوین دستورالعمل‌های شفاف برای پذیرش ادله دیجیتال اشاره کرده است. حسینی (۱۳۹۹، ص. ۱۲) با تحلیل تحولات فناوری و نقش الگوریتم‌ها در تولید شواهد الکترونیک، بر اهمیت انطباق فرآیندهای قضایی با استانداردهای فنی تأکید کرده است.

عبداللهی (۱۴۰۰، ص. ۵۷) نیز به چالش‌های حقوقی مرتبط با پذیرش ادله دیجیتال و ضرورت شفافیت در ارائه شواهد اشاره دارد.

رضایی (۱۴۰۰، ص. ۸۱) با تمرکز بر جنبه‌های اخلاقی استفاده از داده‌های الگوریتمی در نظام قضایی، نشان داده است که فقدان معیارهای اخلاقی و شفافیت می‌تواند منجر به تضییع حقوق متهمان و کاهش اعتماد عمومی شود. همچنین، احمدپور (۱۳۹۹، ص. ۵۳) تحلیل کرده است که ترکیب معیارهای قانونی و فنی می‌تواند کیفیت تصمیم‌گیری قضایی را بهبود بخشد و خطر اشتباهات قضایی را کاهش دهد. پژوهش‌های داخلی در مجموع به بررسی محدودیت‌های قانونی و فنی پرداخته‌اند، اما کمتر به تلفیق همه ابعاد قانونی، فنی و اخلاقی در یک چارچوب تحلیلی جامع پرداخته‌اند. در سطح بین‌المللی، مطالعات گسترده‌تری انجام شده است. (Smith,2018, p. 94) در تحلیل پرونده‌های بین‌المللی، معیارهایی مانند صحت دیجیتال، اصالت و قابلیت بازتولید داده‌ها را به عنوان اصول کلیدی برای پذیرش شواهد الگوریتمی معرفی کرده است(Jones,2019, p. 132) به بررسی استانداردهای دادگاه‌های آمریکا در خصوص شواهد دیجیتال پرداخته و نشان داده است که عدم رعایت این معیارها می‌تواند منجر به رد شواهد شود. (Lee,2020, p. 75) نیز معیارهای دادگاه‌های اروپا، از جمله شفافیت الگوریتم و قابلیت بازتولید داده‌ها، را برای پذیرش ادله دیجیتال بررسی کرده است. Abdullah,2021, p. 88)) با تحلیل چارچوب‌های قانونی بین‌المللی، به خلأها و نقاط ضعف موجود در پذیرش شواهد الگوریتمی اشاره کرده و ضرورت استانداردسازی و هماهنگی قوانین داخلی با معیارهای بین‌المللی را برجسته کرده است. با توجه به مرور پیشینه پژوهشی داخلی و بین‌المللی، می‌توان گفت که اکثر تحقیقات یا بر جنبه قانونی تمرکز داشته‌اند یا بر جنبه فنی و امنیتی. کمتر پژوهشی اقدام به تلفیق همه ابعاد قانونی، فنی و اخلاقی در قالب یک چارچوب تحلیلی و تطبیقی کرده است. این خلأ پژوهشی نشان‌دهنده نیاز به مطالعه‌ای جامع است که معیارهای پذیرش ادله دیجیتال را همزمان از منظر قانونی، فنی و اخلاقی تحلیل کند و چارچوبی عملی برای استفاده در دادگاه‌ها ارائه دهد. نوآوری مقاله حاضر در همین نقطه مشخص می‌شود. این پژوهش با ترکیب تحلیل قوانین داخلی، استانداردهای بین‌المللی، دیدگاه‌های دکترین حقوقی و مبانی فلسفی و فقهی، مدلی جامع برای ارزیابی قابلیت استناد ادله الکترونیک تولیدشده توسط الگوریتم‌ها ارائه می‌دهد. این مدل امکان سنجش اصالت، صحت، شفافیت و قابلیت پذیرش شواهد دیجیتال را در نظام قضایی ایران فراهم می‌کند و همزمان قابلیت تطبیق با معیارهای بین‌المللی را نیز دارد.

یکی از دستاوردهای مهم این تحقیق، ارائه معیارهای سنجش قابلیت استناد است. این معیارها شامل:

۱. اصالت داده‌ها: شواهد دیجیتال باید بدون تغییر و دستکاری ارائه شوند.

۲. شفافیت الگوریتمی: فرآیند تولید و تحلیل داده‌ها باید قابل بررسی و بازتولید باشد.

۳. قابلیت بازتولید داده‌ها: داده‌ها باید امکان بررسی مجدد توسط کارشناسان مستقل داشته باشند.

۴. انطباق با قوانین داخلی و استانداردهای بین‌المللی: شواهد دیجیتال باید مطابق با ماده ۳۴ قانون آیین دادرسی کیفری، تبصره‌های مرتبط و اصول حقوق آمره قانون اساسی و همچنین معیارهای بین‌المللی ارائه شوند.

این چارچوب تحلیلی، نه تنها نوآوری علمی قابل توجهی دارد، بلکه می‌تواند به عنوان ابزاری عملی برای قضات، وکلا و کارشناسان حوزه فناوری اطلاعات و حقوق سایبری مورد استفاده قرار گیرد. با اجرای چنین چارچوبی، علاوه بر ارتقاء عدالت و شفافیت، امکان هماهنگی قوانین داخلی با استانداردهای بین‌المللی نیز فراهم می‌شود. همچنین، نتایج این پژوهش می‌تواند سیاست‌گذاران و قانون‌گذاران را در اصلاح قوانین و ایجاد دستورالعمل‌های اجرایی برای پذیرش شواهد دیجیتال

راهنمایی کند. تدوین دستورالعمل‌های شفاف و استانداردسازی فرآیند جمع‌آوری، نگهداری و ارائه شواهد دیجیتال می‌تواند از تضییع حقوق متهمان جلوگیری کرده و اعتماد عمومی به نظام قضایی را افزایش دهد.

همچنین این تحقیق نشان می‌دهد که ترکیب تحلیل قانونی، فنی، اخلاقی و بین‌المللی، امکان ارائه یک چارچوب جامع و کاربردی برای سنجش قابلیت استناد ادله الکترونیک تولیدشده توسط الگوریتم‌ها را فراهم می‌آورد. چنین چارچوبی، ضمن پر کردن خلأ پژوهشی موجود، مسیر مطالعات آینده در حوزه حقوق سایبری و فناوری اطلاعات را هموار می‌کند و می‌تواند پایه‌ای برای توسعه تحقیقات و سیاست‌گذاری‌های عملی در ایران و سطح بین‌المللی باشد.

تحلیل و بررسی

در نظام حقوقی ایران، پذیرش و قابلیت استناد ادله الکترونیک به عنوان یکی از شاخص‌های مهم عدالت قضایی، در چارچوب قوانین ملی و آیین دادرسی مورد توجه ویژه قرار گرفته است. ماده ۳۴ قانون آیین دادرسی کیفری مصوب ۱۳۹۲، به صراحت مقرر می‌دارد که «هرگونه ادله ارائه‌شده در دادگاه باید از نظر صحت و اصالت مورد تأیید قرار گیرد» و تبصره‌های آن نحوه بررسی مدارک دیجیتال را مشخص کرده‌اند (قانون آیین دادرسی کیفری، ۱۳۹۲، ص. ۲۱). این ماده، به ویژه در پرونده‌های سایبری، به‌عنوان مبنای قانونی برای تعیین قابلیت استناد شواهد دیجیتال عمل می‌کند و قاضی را ملزم به ارزیابی اصالت داده‌ها و صحت فرآیند جمع‌آوری آن‌ها می‌کند. از منظر دکترین حقوقی، کریمی (۱۳۹۷، ص. ۶۸) معتقد است که رعایت این ماده در کنار استانداردهای فنی، نقش تعیین‌کننده‌ای در کاهش خطاهای قضایی دارد، زیرا بدون احراز اصالت، داده‌های دیجیتال ممکن است مستندات غیرقابل اعتماد محسوب شوند.

ماده ۱۲ قانون جرایم رایانه‌ای نیز به صراحت فرآیند جمع‌آوری، ذخیره و ارائه شواهد دیجیتال را مشخص کرده است. بر اساس این ماده، هر گونه دسترسی غیرمجاز به داده‌های رایانه‌ای جرم محسوب می‌شود و داده‌های به‌دست‌آمده از طریق روش‌های غیرقانونی، قابلیت استناد در دادگاه را ندارند (قانون جرایم رایانه‌ای، ۱۳۸۸، ص. ۱۴). این موضوع اهمیت رعایت اصول قانونی و اخلاقی در جمع‌آوری ادله دیجیتال را برجسته می‌سازد و از هرگونه سوءاستفاده یا تحریف شواهد جلوگیری می‌کند. همچنین، بر اساس تبصره ماده مذکور، ارائه مدارک دیجیتال باید توسط کارشناسان رسمی دادگستری یا افراد دارای صلاحیت فنی معتبر تأیید شود، تا از لحاظ قانونی قابل استناد باشد. اصل ۳۵ قانون اساسی ایران که به حق دفاع متهم اختصاص دارد، نقش مکملی در پذیرش ادله دیجیتال دارد. طبق این اصل، متهم حق دارد شواهد ارائه‌شده علیه خود را مشاهده و بررسی کند و در صورت وجود اشکال یا نقص، اعتراض نماید. این اصل حقوق آمره نشان می‌دهد که دادگاه‌ها نمی‌توانند بدون امکان بررسی و مقابله با شواهد، تصمیم‌گیری کنند، حتی اگر داده‌ها دیجیتال و مبتنی بر الگوریتم باشند (قانون اساسی جمهوری اسلامی ایران، ۱۳۵۸، ص. ۴۳). از دیدگاه دکترین، احمدپور (۱۳۹۹، ص. ۵۳) معتقد است که ترکیب اصل حق دفاع با ارزیابی فنی و قانونی شواهد دیجیتال، چارچوبی مستحکم برای پذیرش ادله الکترونیک ایجاد می‌کند و تضمین می‌کند که عدالت قضایی در دنیای دیجیتال نیز برقرار بماند. تحلیل مواد قانونی نشان می‌دهد که قوانین ایران به طور مستقیم یا غیرمستقیم به چهار معیار اصلی برای سنجش قابلیت استناد ادله دیجیتال اشاره دارند: اصالت داده‌ها، صحت فرآیند جمع‌آوری، شفافیت ارائه شواهد و تطبیق با حقوق متهم. این معیارها، علاوه بر تضمین عدالت قضایی، نقش مهمی در پیشگیری از سوءاستفاده و تضییع حقوق شهروندان ایفا می‌کنند. برای مثال، ماده ۳۴ قانون آیین دادرسی کیفری و ماده ۱۲ قانون جرایم رایانه‌ای، هرگونه دستکاری یا جمع‌آوری غیرمجاز داده‌ها را فاقد اعتبار می‌دانند، در حالی که اصل ۳۵ قانون اساسی، حق مقابله و بررسی داده‌ها را به متهم اعطا می‌کند. این ترکیب قانونی نشان‌دهنده تلاش قانون‌گذار برای

تطبیق فناوری‌های نوین با اصول حقوقی و انسانی موجود است. از سوی دیگر، دیدگاه‌های دکترین حقوقی داخلی نیز بر ضرورت شفافیت الگوریتم‌ها و روش‌های تحلیلی تأکید دارند. کریمی (۱۳۹۷، ص. ۷۵) معتقد است که بدون مشخص شدن فرآیند دقیق تولید شواهد دیجیتال، نمی‌توان به قابلیت استناد آن‌ها اعتماد کرد. حسینی (۱۳۹۹، ص. ۱۲) نیز با بررسی پرونده‌های واقعی سایبری، نشان داده است که داده‌های دیجیتال بدون تأیید کارشناسان رسمی دادگستری، احتمال دارد توسط دادگاه‌ها رد شوند. این دیدگاه‌ها حاکی از آن است که صرفاً ارائه داده‌های دیجیتال کافی نیست و الزام به تحلیل و تأیید فنی و قانونی، جزء لاینفک پذیرش ادله است.

علاوه بر قوانین داخلی، برخی آراء دیوان عالی کشور نیز معیارهایی برای پذیرش شواهد دیجیتال تعیین کرده‌اند. برای مثال، رأی شماره ۹۸/۲۱۳ صادره توسط دیوان عالی کشور به وضوح بیان می‌کند که «شواهد دیجیتال تنها در صورتی قابلیت استناد دارند که فرآیند جمع‌آوری آن مطابق با مقررات قانونی و توسط کارشناسان معتبر صورت گرفته باشد.» این رأی، اهمیت رعایت استانداردهای قانونی و فنی را در پذیرش ادله دیجیتال برجسته می‌کند و برای قضات ایران یک مرجع مهم به حساب می‌آید. همچنین، رأی شماره ۹۷/۴۵۶ دیوان عالی کشور بر لزوم تطابق داده‌های دیجیتال با اصل حق دفاع تأکید کرده و تأکید می‌کند که بدون امکان بررسی توسط متهم، داده‌ها نمی‌توانند مورد استناد قرار گیرند. تحلیل استدلالی نشان می‌دهد که قوانین داخلی ایران و رویه قضایی، چارچوبی نسبی برای پذیرش ادله الکترونیک ارائه کرده‌اند، اما هنوز خلأهایی در استانداردسازی فنی و شفافیت فرآیند وجود دارد. دکترین حقوقی بر ضرورت تدوین دستورالعمل‌های روشن برای نحوه جمع‌آوری، نگهداری و ارائه شواهد دیجیتال تأکید دارد و معتقد است که این دستورالعمل‌ها می‌توانند به کاهش اختلاف نظر بین قضات و کارشناسان فنی کمک کنند و قابلیت استناد شواهد را افزایش دهند (عبداللهی، ۱۴۰۰، ص. ۶۵).

در مجموع، محور نخست تحلیل و بررسی نشان می‌دهد که قوانین داخلی ایران، اصول بنیادین قابلیت استناد ادله دیجیتال را تعیین کرده‌اند، اما برای تضمین پذیرش مؤثر و کاهش خطاهای قضایی، نیاز به استانداردسازی فنی، شفافیت الگوریتم‌ها و دستورالعمل‌های عملیاتی مشخص وجود دارد. این تحلیل استدلالی، پایه‌ای برای محور بعدی است که به بررسی رویه قضایی ایران و نحوه اجرای این قوانین در عمل می‌پردازد و نشان می‌دهد که چگونه دادگاه‌ها با استفاده از مواد قانونی و ارجاع به دکترین، قابلیت استناد شواهد دیجیتال را ارزیابی می‌کنند. تحلیل رویه قضایی ایران نشان می‌دهد که دادگاه‌ها در مواجهه با ادله الکترونیک، علاوه بر رعایت قوانین داخلی، به ارزیابی فنی و اصالت داده‌ها توجه ویژه‌ای دارند. رأی شماره ۹۸/۳۱۲ دیوان عالی کشور تأکید می‌کند که «داده‌های دیجیتال صرفاً در صورتی قابلیت استناد دارند که فرآیند جمع‌آوری آن‌ها مطابق مقررات قانونی و با تأیید کارشناسان رسمی دادگستری انجام شده باشد» (دیوان عالی کشور، ۱۳۹۸، ص. ۲۴). این رأی بیانگر آن است که حتی در صورت دسترسی به داده‌های دیجیتال پیچیده، بدون احراز صحت و اصالت، دادگاه‌ها امکان استفاده از آن‌ها را ندارند. مشابه این دیدگاه در رأی شماره ۹۷/۴۷۵ نیز آمده است که «ارائه شواهد دیجیتال بدون امکان بررسی و مقابله توسط متهم، فاقد ارزش قانونی است» (دیوان عالی کشور، ۱۳۹۷، ص. ۵۸). تحلیل تطبیقی رویه قضایی نشان می‌دهد که قضات در عمل، غالباً ترکیبی از مواد قانونی و ارجاعات دکترین حقوقی داخلی را برای ارزیابی شواهد دیجیتال به کار می‌برند. به عنوان نمونه، در پرونده‌ای که به دستکاری داده‌های تراکنش‌های بانکی مربوط می‌شد، قاضی با استناد به ماده ۳۴ قانون آیین دادرسی کیفری و رأی شماره ۹۸/۲۱۳ دیوان عالی کشور، شواهد دیجیتال را تنها پس از تأیید کارشناسان رسمی معتبر پذیرفت (کریمی، ۱۴۰۰، ص. ۹۲). این مثال نشان می‌دهد که

رویه قضایی ایران سعی دارد تعادل میان دسترسی به داده‌های دیجیتال و حفاظت از حقوق متهمان را حفظ کند. از منظر دکترین حقوقی، نظریه‌پردازانی مانند رضایی (۱۴۰۱، ص. ۷۵) معتقدند که شفافیت الگوریتم‌ها و قابلیت بازتولید داده‌ها یکی از معیارهای اصلی دادگاه‌ها برای پذیرش شواهد دیجیتال است. بر اساس این دیدگاه، دادگاه‌ها نه تنها به داده‌ها، بلکه به فرآیندهای تولید و تحلیل آن‌ها نیز توجه می‌کنند تا از صحت و اصالت شواهد اطمینان حاصل شود. همچنین، احمدپور (۱۴۰۰، ص. ۶۲) تاکید دارد که ارزیابی شواهد دیجیتال باید به صورت هم‌زمان قانونی و فنی انجام گیرد، تا هم عدالت قضایی تضمین شود و هم امکان سوءاستفاده کاهش یابد.

تحلیل آراء و رویه قضایی نشان می‌دهد که هنوز فقدان دستورالعمل‌های یکپارچه برای ارزیابی داده‌های دیجیتال وجود دارد و این امر باعث اختلاف نظر میان قضات می‌شود. در برخی پرونده‌ها، داده‌های دیجیتال بدون تأیید کارشناسان پذیرفته شده‌اند، در حالی که در پرونده‌های دیگر، حتی با تأیید کارشناسان رسمی، دادگاه‌ها خواستار شفافیت کامل الگوریتمی شده‌اند (Mokri, 2020, p. 45). این تفاوت‌ها حاکی از نیاز به تدوین استانداردهای عملی و دستورالعمل‌های قضایی برای ارزیابی شواهد دیجیتال در ایران است.

در سطح بین‌المللی، رویه قضایی کشورهای مختلف نیز معیارهایی مشابه را دنبال می‌کند. به عنوان مثال، در پرونده (United States v. Microsoft Corp,2018, p. 102)، دادگاه بر اصالت داده‌ها و شفافیت فرآیند جمع‌آوری شواهد دیجیتال تأکید کرد و نشان داد که حتی در سیستم‌های پیشرفته، ارزیابی فنی و قانونی هم‌زمان ضروری است. مطالعه (Lee,2020, p. 88) نیز نشان می‌دهد که دادگاه‌های اروپایی از استانداردهای دقیق برای قابلیت بازتولید و اصالت داده‌ها استفاده می‌کنند و بدون رعایت این معیارها، شواهد دیجیتال قابل استناد نیستند. این نمونه‌ها نشان می‌دهد که رویه قضایی بین‌المللی می‌تواند به الگوی تطبیقی برای ایران تبدیل شود و به ایجاد هماهنگی میان قوانین داخلی و استانداردهای جهانی کمک کند. از منظر تحلیلی، ترکیب رویه قضایی و دکترین حقوقی داخلی نشان می‌دهد که دادگاه‌ها به دنبال تضمین عدالت قضایی، حفاظت از حقوق متهم و اعتبار شواهد دیجیتال هستند. تحلیل استدلالی این رویه‌ها نشان می‌دهد که صرفاً پیروی از مواد قانونی کافی نیست و دادگاه‌ها نیازمند معیارهای فنی، شفافیت الگوریتمی و امکان بازتولید داده‌ها هستند تا تصمیم‌گیری‌ها معتبر و منصفانه باشند. به علاوه، این تحلیل نشان می‌دهد که تجربه عملی قضات در ایران می‌تواند مبنای تدوین دستورالعمل‌های جدید برای ارزیابی ادله دیجیتال و استانداردسازی رویه‌ها قرار گیرد. در نتیجه، محور دوم تحلیل نشان می‌دهد که رویه قضایی ایران تلاش دارد میان قوانین داخلی، حق دفاع متهم و الزامات فنی تعادل برقرار کند، اما هنوز خلأهایی در استانداردسازی و شفافیت وجود دارد. این محور، پایه‌ای برای محور بعدی تحلیل است که به مقایسه با حقوق سایر کشورها و اسناد بین‌المللی می‌پردازد و نشان می‌دهد چگونه تجربیات بین‌المللی می‌تواند قابلیت استناد ادله دیجیتال را در ایران بهبود بخشد. در محور سوم و در مقایسه با حقوق سایر کشورها و اسناد بین‌المللی در سطح بین‌المللی، پذیرش و اعتبار ادله دیجیتال در نظام‌های حقوقی مختلف، تحت تأثیر استانداردهای جهانی و رویه قضایی بین‌المللی قرار دارد. بر اساس ماده ۶۹(۴) اساسنامه دیوان کیفری بین‌المللی (ICC)، پذیرش ادله دیجیتال باید در سه مرحله ارزیابی شود: (۱) ارتباط با موضوع، (۲) ارزش اثباتی، و (۳) تأثیر منفی بر دادرسی عادلانه (Smith, 2018, p. 94). این رویکرد بر

اهمیت ارزیابی فنی و حقوقی هم‌زمان تأکید دارد و نشان می‌دهد که صرف ارائه داده‌های دیجیتال بدون رعایت استانداردهای جهانی کافی نیست.

در نظام حقوقی آمریکا، پرونده (Gates Rubber Co. v. Bando Chemical Industries,1996, p. 102) به‌عنوان یک مرجع مهم در زمینه پذیرش ادله دیجیتال شناخته می‌شود. در این پرونده، دادگاه بر لزوم رعایت استانداردهای فنی در جمع‌آوری و تحلیل داده‌های دیجیتال تأکید کرد و مقرر داشت که هر کارشناس دیجیتال باید از روشی استفاده کند که بیشترین و دقیق‌ترین نتایج را ارائه دهد. این حکم، معیارهای پذیرش شواهد دیجیتال در دادگاه‌های آمریکا را مشخص کرد و اهمیت ترکیب ارزیابی فنی و قانونی را نشان داد. در اتحادیه اروپا، پروژه (AEEC,Admissibility of Electronic Evidence in Court) در سال ۲۰۰۵ آغاز شد تا روش‌های پذیرش ادله دیجیتال در دادگاه‌های ۱۶ کشور عضو را بررسی کند (Lee, 2020, p. 88). نتایج این پروژه نشان داد که پذیرش ادله دیجیتال با وجود شباهت‌های قانونی، تفاوت‌های عملی و رویه‌ای قابل توجهی دارد. این تفاوت‌ها، ضرورت تدوین استانداردهای مشترک بین کشورها را نمایان می‌سازد. در مقایسه با نظام‌های بین‌المللی، نظام حقوقی ایران با وجود قانون تجارت الکترونیکی که داده‌پیام‌ها را به‌عنوان مکتوب می‌پذیرد (Madavani, 2014, p. 27)، در عمل با چالش‌هایی مواجه است. فقدان دستورالعمل‌های اجرایی مشخص و استانداردهای فنی، ابهام در پذیرش ادله دیجیتال را ایجاد کرده است. پژوهش‌ها نشان می‌دهند که حتی با وجود تأیید قانونی داده‌ها، در برخی پرونده‌ها، قضات خواستار شفافیت کامل الگوریتمی و امکان بازتولید داده‌ها هستند (Dawas, Jafarzadeh & Nikkhah Saranghi, 2024, p. 21022).

تحلیل تطبیقی نشان می‌دهد که پذیرش و اعتبار ادله دیجیتال در نظام‌های حقوقی مختلف، نیازمند اصالت داده‌ها، شفافیت فرآیند جمع‌آوری، قابلیت بازتولید و انطباق با حقوق متهم است. ترکیب این معیارها با ارزیابی حقوقی و فنی، تضمین می‌کند که شواهد دیجیتال قابلیت استناد داشته باشند و همزمان عدالت قضایی حفظ شود. علاوه بر این، تجربیات بین‌المللی می‌تواند به عنوان الگوی تطبیقی برای ایران مورد استفاده قرار گیرد و به تدوین دستورالعمل‌های عملی کمک کند.

بحث و نتیجه گیری

بحث پیرامون قابلیت استناد ادله الکترونیک تولیدشده توسط الگوریتم‌ها در نظام قضایی ایران و مقایسه با رویه بین‌المللی نشان می‌دهد که این موضوع از اهمیت ویژه‌ای برخوردار است. بررسی قوانین داخلی، شامل ماده ۳۴ قانون آیین دادرسی کیفری، ماده ۱۲ قانون جرایم رایانه‌ای و اصل ۳۵ قانون اساسی، حاکی از آن است که قانون‌گذار تلاش کرده است چارچوبی برای تضمین اصالت، صحت و شفافیت شواهد دیجیتال ایجاد کند. این قوانین، نه تنها نقش محافظتی برای حقوق متهمان ایفا می‌کنند، بلکه فرآیند جمع‌آوری و ارائه شواهد را نیز از نظر فنی و قانونی مشخص می‌سازند. با این حال، فقدان دستورالعمل‌های اجرایی و استانداردهای یکپارچه، محدودیت‌هایی را در پذیرش مؤثر ادله دیجیتال ایجاد کرده است. بررسی رویه قضایی ایران نشان می‌دهد که دادگاه‌ها در عمل، ترکیبی از مواد قانونی و تحلیل کارشناسی را برای ارزیابی شواهد دیجیتال به کار می‌برند. آراء دیوان عالی کشور، مانند رأی شماره ۹۸/۳۱۲ و رأی شماره ۹۷/۴۷۵، بر لزوم تأیید شواهد دیجیتال توسط کارشناسان معتبر و حفظ حق دفاع متهم تأکید دارند. این رویه نشان می‌دهد که دادگاه‌ها تنها به ارائه داده‌های دیجیتال بسنده نمی‌کنند و نیاز به شفافیت فرآیند تولید و امکان بازتولید داده‌ها را جزء الزامات اصلی می‌دانند. دکترین حقوقی داخلی نیز تأکید دارد که بدون شفافیت الگوریتم‌ها و تأیید کارشناسی، شواهد دیجیتال نمی‌توانند اعتبار کافی داشته باشند و ممکن است منجر به تصمیم‌گیری نادرست شوند (رضایی، ۱۴۰۱، ص. ۷۵). تدوین دستورالعمل‌های

دقیق و هماهنگ در ایران را برجسته می‌سازد تا ضمن حفظ اصول قانونی و حقوق شهروندان، پذیرش شواهد دیجیتال قابل اعتماد و استاندارد شود. حقوقی و استانداردهای فنی و شفاف باشد. به عبارت دیگر، اصالت

منابع

۱. منابع فارسی

کتاب‌ها

مکارم، م. (۱۳۹۷). فقه و قواعد اثبات در حقوق اسلامی. تهران: مجله فقه و حقوق اسلامی.

احمدپور، ع. (۱۳۹۹). جنبه‌های اخلاقی استفاده از داده‌های الگوریتمی در نظام قضایی. تهران: مجله حقوق فناوری.

مقالات

احمدی، ه. ر. (۱۴۰۲). بررسی قابلیت استناد ادله الکترونیک در دعاوی اداری و تجاری. مجله حقوق اداری و دعاوی تجاری، ۱۵ (۲)، ۴۵–۶۷.

مدنی، م. س. (۱۳۹۳). استفاده از شواهد الکترونیک در محاکم کیفری ایران. مجله حقوق کیفری ایران، ۹ (۱)، ۲۳–۴۰.

محمدی، س. (۱۳۸۸). بررسی تطبیقی ارائه شواهد الکترونیک در محاکم ایران و بین‌الملل. مجله حقوق تطبیقی، ۵ (۳)، ۱۱۲–۱۳۰.

علیدوستی شاهرکی، ن. (۱۴۰۱). مطالعه مقررات پذیرش شواهد الکترونیک: تمرکز بر نظام‌های حقوقی ایران و آمریکا. مجله فقه و حقوق، ۱۸ (۱)، ۷۷–۹۲.

مولایی، ع. پ. (۱۴۰۳). شرایط پذیرش شواهد دیجیتال در دعاوی مدنی در ایران. مجله مدیریت و علوم مهندسی، ۱۲ (۱)، ۱۱۹–۱۳۵.

مدنی، م. (۱۴۰۰). بررسی شواهد دیجیتال و قابلیت استناد آن‌ها در دادگاه‌های ایران. مجله حقوق ایران، ۱۲ (۳)، ۹۵–۱۰۸.

رضایی، س. (۱۴۰۱). تحلیل حقوق سایبری و کاربرد ادله الکترونیک در نظام قضایی ایران. مجله فقه و حقوق، ۱۸ (۱)، ۸۸–۱۰۲.

کریمی، م. (۱۴۰۰). امنیت داده‌ها و الزامات قانونی پذیرش شواهد دیجیتال. مجله حقوق فناوری اطلاعات، ۱۰ (۲)، ۹۵–۱۰۵.

ریاحی، ع. (۱۴۰۰). تحلیل حقوقی ادله دیجیتال و الزامات پذیرش آن‌ها. مجله حقوق فناوری اطلاعات، ۹ (۲)، ۷۸–۹۵.

سعیدی، ف. (۱۴۰۱). استانداردهای پذیرش شواهد الکترونیک در نظام قضایی ایران. مجله حقوق سایبری، ۶ (۱)، ۱۰۳–۱۱۰.

نادرزاده، ک. (۱۴۰۰). قابلیت استناد شواهد دیجیتال در حقوق داخلی و بین‌الملل. مجله فقه و حقوق فناوری، ۳ (۲)، ۹۰–۱۰۲.

اسناد قانونی و آراء قضایی

دیوان عالی کشور. (۱۳۹۸). رأی شماره ۹۸/۳۱۲. تهران: دیوان عالی کشور.

دیوان عالی کشور. (۱۳۹۷). رأی شماره ۹۷/۴۷۵. تهران: دیوان عالی کشور.

قانون آیین دادرسی کیفری. (۱۳۹۲). تهران: سازمان چاپ و نشر قوانین.

قانون جرایم رایانه‌ای. (۱۳۸۸). تهران: سازمان چاپ و نشر قوانین.

۲. منابع انگلیسی

Books

Rawls, J. (1971). A Theory of Justice. Harvard University Press.

Article

Smith, J. (2018). Computer-Generated Evidence: International Standards. Journal of Cyber Law Studies, 12(1), 94–110.

Lee, A. (2020). Digital Evidence in European Courts. Journal of International Criminal Justice, 18(2), 88–102.

Dawas, R. A., Jafarzadeh, S., & Nikkhah Saranghi, R. (2024). The status of electronic evidence and its role in proving criminal cases. Pakistan Journal of Life and Social Sciences, 22(2), 21018–21030.

Madavani, M. S. (2014). The use of electronic evidence in criminal courts in Iran. Iranian Journal of Criminal Law, 9(1), 23–40.

Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B-CoC: A blockchain-based chain of custody for evidence management in digital forensics. Digital Forensics Journal, 14(3), 201–215.

Farzan, R. (2019). Cyber Evidence and Judicial Evaluation. Journal of Legal and Technological Studies, 7(2), 67–82.

Jackson, J. D. (2011). Two methods of proof in criminal procedure. Modern Law Review, 74(1), 23–40.

Abdullah, R. (2021). Digital Evidence and Judicial Decision-Making. Journal of Cyber Law and Policy, 14(1), 88–90.

Jones, M. (2019). Legal Admissibility and Evidentiary Value of Digital Evidence. Journal of Legal Technology Studies, 14(2), 132–145.

Phipps, S. A. (2018). Admissibility of Electronic Evidence. Anticipation Litigation Advisor Blog, 2.

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the integrity of the legal process. ScienceDirect, 6.

Welty, J. B. (2015). Digital Evidence. In Digital Evidence (pp. 4).

Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border Criminal Investigations and Digital Evidence. arXiv preprint arXiv:2205.12911, 5.