News Science
Online ISSN: 2980-9274 Print ISSN: 2382-9788
Homepage: www.mjourcom.ir

The Admissibility of Electronic Messages in Family Law Disputes: Balancing Evidentiary Rules with Privacy Considerations

Zahra Halimi[1] | Nafiseh Sadat Shariati[2]✉

1. Masters, Department of Private Law, Faculty of Law, University of Tarbiat Modares, Tehran, Iran. E-mail: z.halimi@modares.ac.ir
2. Corresponding author, Associate Professor, Department of Private Law, Faculty of Law, University of Tarbiat Modares, Tehran, Iran. E-mail: n.shariati@modares.ac.ir

Article Info

Article type:
Research Article

Article history:
Received: 11 August 2025
Received in revised form: 19 September 2025
Accepted: 22 October 2025
Published online: February 2026

Keywords:
Electronic Messages,
Family Law Disputes,
Privacy,
Social Networks.

ABSTRACT

Objective: Messaging platforms such as WhatsApp, Instagram, and Telegram have increasingly become instrumental in initiating, developing, and substantiating claims in family law disputes. In matters pertaining to divorce, child custody, or spousal and child support, parties frequently rely on messages, images, or voice recordings exchanged through these platforms. Despite this growing reliance, the Iranian legal system lacks a coherent legal framework governing the admissibility and probative value of such electronic evidence. While general statutory provisions address issues such as surveillance, unauthorized access, and data disclosure, the legal status of electronic evidence in the context of family law remains ambiguous—particularly with respect to the legitimacy of its acquisition, attribution to specific individuals, and compatibility with privacy rights. Accordingly, the central research question of this study is: What is the legal status of messages exchanged via messaging platforms in proving claims within Iranian family law?

Methods: This study adopts an analytical and comparative legal methodology to evaluate the evidentiary function of communications on social media platforms in Iranian family law. It also proposes legislative reforms aimed at enhancing legal clarity, consistency, and the protection of individual rights.

Results: Under the Electronic Commerce Act of the Islamic Republic of Iran, courts may not reject electronic documents solely on the basis of their form or format. Messages exchanged via online platforms fall within the definition of "data messages" and may therefore be submitted as evidence in judicial proceedings.

Conclusions: An examination of relevant legal provisions and technical safeguards—such as one-time passwords (OTPs), login notifications, and unique identifiers—demonstrates that such communications satisfy the criteria for reliable data messages. Furthermore, lawful access to these communications does not necessarily violate privacy rights, recognizing that electronic correspondence inherently entails a certain degree of privacy compromise.

Cite this article: Halimi, Z., & Shariati, N. S., (2025). The Admissibility of Electronic Messages in Family Law Disputes: Balancing Evidentiary Rules with Privacy Considerations, News Science, 14 (4), 48-52.

DOI: http//doi.org/10.22034/lrsi.2025.540470.1416

DOI: http//doi.org/10.22034/lrsi.2025.540470.1416

The Journal of *News Science*
Vol. 14, No. 4, Ser.56, Winter 2025, P. 48- 52
Journal homepage: https://www.mjourcom.ir/
DOI : http//doi.org/10.22034/lrsi.2025.540470.1416

Open Access

ORIGINAL ARTICLE

The Admissibility of Electronic Messages in Family Law Disputes: Balancing Evidentiary Rules with Privacy Considerations

Zahra Halimi[1] | Nafiseh Sadat Shariati [2]✉

3. Masters, Department of Private Law, Faculty of Law, University of Tarbiat Modares, Tehran, Iran. E-mail: z.halimi@modares.ac.ir
4. Corresponding author, Associate Professor, Department of Private Law, Faculty of Law, University of Tarbiat Modares, Tehran, Iran. E-mail: n.shariati@modares.ac.ir

Received: August 11, 2025 Accepted: October 22, 2025

EXTENDED ABSTRACT

Interdiction:

In recent years, social networking platforms have profoundly restructured communication patterns across all societies. These platforms offer users a space to share personal interests, thoughts, and activities while simultaneously enabling them to forge new relationships or sustain existing ones. Among the most widely utilized platforms internationally are messaging services such as Telegram, WhatsApp, and Instagram, alongside domestic platforms within Iran including Eitaa and Bale.

Beyond their conventional social and interpersonal applications, these platforms have increasingly assumed a critical function in family law disputes. In cases involving divorce, child custody, spousal and child support, or allegations of infidelity and domestic violence, litigants frequently rely on messages, photographs, audio recordings, and other forms of digital content

exchanged via these platforms to substantiate their legal claims. For instance, in divorce proceedings, a spouse may submit screenshots of WhatsApp conversations wherein the other party explicitly admits to concealing marital assets or refusing to provide child support.
Despite this growing dependence on digital evidence, the Iranian legal system lacks a coherent and comprehensive framework governing the admissibility and evidentiary weight of such materials. Although general statutes—namely the Criminal Procedure Code and the Computer Crimes Act—address issues such as surveillance, unauthorized access, and disclosure of personal information, they remain ambiguous with respect to the specific legal challenges arising in family law contexts. These ambiguities are most salient in three interrelated domains:

Legitimacy of Evidence Collection: The law should explicitly delineate the circumstances under which digital communications may be lawfully obtained and presented as evidence.

Proper Attribution of Messages to Identifiable Individuals: A principal challenge in employing electronic communications as evidence lies in reliably linking digital content to a specific individual. Legislation should therefore establish technical and legal criteria for attribution, potentially encompassing device identifiers, IP addresses, timestamps, and two-factor authentication logs.

Compatibility with Constitutional and Human Rights Principles of Privacy: The legal framework should articulate principles ensuring that the introduction of digital communications as evidence does not result in disproportionate intrusions into private life.

Accordingly, the central research question guiding this study is: What is the legal status of messages exchanged via online messaging platforms in proving family law claims under Iranian law?

Method:

This research employs an analytical and comparative legal methodology. On one hand, it examines Iranian statutory provisions—particularly the Electronic Commerce Act and the Computer Crimes Act—to assess the current legal treatment of electronic evidence. On the other hand, it undertakes a comparative review of foreign legal systems that have developed more explicit standards concerning the admissibility and reliability of electronic communications in family law disputes.
Furthermore, the study evaluates the extent to which the use of electronic communications as evidence aligns with internationally recognized principles, notably the right to privacy. The research also formulates legislative reform proposals aimed at addressing existing legal lacunae while promoting both evidentiary efficiency and the protection of fundamental rights.

Findings:

Pursuant to Article 12 of the Iranian Electronic Commerce Act, documents and evidence supporting a claim may be submitted in the form of data messages, and no court or governmental authority may dismiss their evidentiary value solely by reason of their digital form or format. Moreover, Clause (a) of Article 2 of the same law defines a "data message" as "any symbol of an event, information, or concept that is produced, sent, received, stored, or processed by electronic, optical, or new information technologies." Considering this broad and dynamic definition, it can be inferred that all instruments involved in the process of exchanging, transmitting, or processing information through modern technologies fall within the scope of a

"data message." Consequently, messages exchanged through online platforms qualify as "reliable data messages" and may, in principle, be admitted as evidence in judicial proceedings. Additionally, technical safeguards such as one-time passwords (OTPs), login alerts, IP addresses, and device-specific identifiers enhance the evidentiary value of these messages by supporting authentication and attribution. When accessed through lawful and legitimate means—for example, by one of the participants in the communication—the submission of such evidence does not constitute an unlawful intrusion into privacy. This reflects the inherent reality that electronic communications naturally entail a certain degree of diminished confidentiality.
Nevertheless, the absence of clear procedural and substantive rules in this domain has engendered inconsistent judicial practice, leaving litigants uncertain regarding the admissibility and probative value of their digital evidence. This situation conflicts with the principle of a fair trial, and in the contemporary era—frequently designated as the digital age—it is imperative for the legal system to strive to maintain pace with technological advancements.

Conclusions:

The analysis suggests that electronic messages exchanged through platforms such as WhatsApp, Instagram, and Telegram possess significant potential as admissible evidence in Iranian family law disputes. However, the lack of specific legislation addressing issues of collection, attribution, and privacy creates practical challenges and risks inconsistent application by the courts.
To remedy these deficiencies, the study recommends targeted legislative reform. Clear statutory provisions should establish:

Conditions of legitimacy for collecting and presenting such evidence;

Standards of attribution, including technical and legal criteria for linking messages to specific individuals; and

Privacy safeguards, ensuring that the evidentiary use of digital communications does not result in disproportionate intrusions into private life.

By articulating such rules, the Iranian legal system can strike an appropriate balance between the individual right to prove a claim in family disputes and the fundamental right to privacy. This, in turn, would enhance clarity, consistency, and fairness in judicial practice while ensuring that the law remains responsive to the technological realities of the digital age.

Data Availability Statement
Data available on request from the authors.
Acknowledgements
The authors would like to thank anonymous reviewers.
Ethical considerations
Not applicable.
Funding
Not applicable.
Conflict of interest
The authors declare no conflict of interest.

References

Ansari, B. (2008). *The Law of Mass Communication*. Tehran: SAMT. (In Persian)

Babazadeh Moghaddam, H. & Khedri, N. (2022). *Internet Access as a New Fundamental Right*. *News Science Quarterly (NS)*, 11(1), 73-116. (In Persian)

Canavan, M., & Kolstad, E. (2016). *Does the Use of Social Media Evidence in Family Law Litigation Matter? Whittier Journal of Child and Family Advocacy*. Retrieved from Canavan-article.pdf

Darzyan Rostami, H. and Behzadpour, F. (2019). *The Role of Social Media in Promoting Social Security Using Elite Experts and National Cyberspace Experts. News Science Quarterly* (NS), 8(2), 247-268. (In Persian)

du Belfon, Z. L. (2011). *Electronic Commercial Law* (2nd ed., S. Zarghalam, Trans.). Tehran: Shahre Danesh Institute of Legal Studies and Research. (In Persian)

Elsan, M., & Manouchehri, M. R. (2018). *A Survey on Authenticity and Admissibility of Electronic Evidences. Shiraz University Journal of Legal Studies*, 10(2), 29–52. (In Persian)

ESeye Ltd. (2023). *SMS API Developer Guide* (Last updated March 1, 2023). Retrieved July 23, 2025, from 8297 SMS API Developer Guide

Ghanad, F., & Aligholi, A. (2020). *The Concept and Importance of Personal Data and Privacy and the Types of Protection in Cyberspace. Biannual Journal of Contract Law and New Technologies*, 1(1), 297–322. (In Persian)

Habibzadeh, T. (2017). *Information Technology Law: Electronic Evidence, Electronic Documents, and Electronic Signatures* (1st ed.). Tehran: Mizan Publishing. (In Persian)

Heydarinejad, N. (2017). *Legal Review of Electronic Evidence in the Current System*. *Qanunyar: Scientific–Legal Quarterly*, 3, 125–140. (In Persian)

Mahmodi Parchini, M., Riazi, L., Pour Ebrahimi, A. and Mousavi, S. A. A. (2025). *Comparison of Personal Data Protection Laws: Unique General Regulations under the European Union's General Data Protection Regulation (GDPR) and United States Laws. News Science Quarterly (NS)*, 13(4), 204-224. doi: 10.22034/lrsi.2024.468452.1210 (In Persian)

Markert, P., Lassak, L., Golla, M., & Dürmuth, M. (2024). *Understanding Users' Interaction with Login Notifications.* In CHI Conference on Human Factors in Computing, (853), 1–17.

Mason, S., & Seng, D. (Eds.) (2017). *Electronic Evidence (4th ed.). Institute of Advanced Legal Studies, School of Advanced Study*, University of London.

Mirshkari, A., & Alaei, S. (2020*). The Positive Nature of Data Messages as a Litigation's Evidence. Legal Research Quarterly*, (96), 301–326. (In Persian)

Leach, P., Mealling, M., & Salz, R. (2005). *A Universally Unique Identifier (UUID) URN Namespace* (RFC 4122). Network Working Group.

NIST. (2017). *Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B).* Retrieved July 27, 2025, from NIST Special Publication 800-63B

Omidi, M., & Safaei-Shahrasb, Z. (2022). *The Validity of Electronic Documents in Family Lawsuits. Journal of Jurisprudence and Legal Studies of Media*, Faculty of Refah, 4(2), 111–127. (In Persian)

Rabbani-Mousavian, A., & Naeimi, T. (2019). *Documentation In Accordance with Electronic Classic and Modern Documents and Their Effects in Legal System. Journal of Judgment*, (100), 157–179. (In Persian)

Rahimi, Z., & Taheripour, Z. (2019). *The Validity of Electronic Documents as Evidence in Spousal Disputes. Journal of Jurisprudence and Legal Studies of Media*, Faculty of Refah, 1(1), 51–74. (In Persian)

Sadeghi, H. (2017). *Civil Liability in Electronic Communications* (2nd ed.). Tehran: Mizan Publishing. (In Persian)

Shahbazi-Nia, M., & Abdollahi, M. (2009). *Ascertainment of Genuineness in Electronic Evidence.* Comparative Legal Studies (Modares), 13(4), 125–141. (In Persian)

Telegram. (2013). *Telegram adds Session Control and Two-Step Verification*. Retrieved July 17, 2025, from https://telegram.org/blog/sessions-and-2-step-verification (Accessed: 27 July 2025).

علوم خبری
شاپا چاپی: ۲۳۸۳-۹۷۸۸ شاپا الکترونیکی: ۹۲۷۴-۲۹۸۰

قابلیت استناد پیام‌های الکترونیکی در دعاوی خانواده با تأکید بر ملاحظات حریم خصوصی

زهرا حلیمی[۱] | نفیسه سادات شریعتی[۲]✉

۱. کارشناسی ارشد، گروه حقوق خصوصی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران. ایران. رایانامه: z.halimi@modares.ac.ir
۲. استادیار، گروه حقوق خصوصی، دانشکده حقوق، دانشگاه تربیت مدرس، تهران. ایران، (نویسنده مسئول) رایانامه: n.shariati@modares.ac.ir

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت: ۱۴۰۴/۵/۲۰
تاریخ بازنگری: ۱۴۰۴/۶/۲۸
تاریخ پذیرش: ۱۴۰۴/۷/۳۰
تاریخ انتشار: ۱۴۰۴/۱۱/۲۵

کلیدواژه‌ها:
ادله الکترونیکی،
پیام رسان ها،
حریم خصوصی،
دعاوی خانواده،
شبکه های اجتماعی.

چکیده

هدف: در سال‌های اخیر، پیام‌رسان‌ها و شبکه‌های اجتماعی مانند واتساپ، اینستاگرام و تلگرام به ابزارهایی مؤثر در شکل‌گیری، تشدید و اثبات دعاوی خانوادگی تبدیل شده‌اند. در پرونده‌هایی نظیر طلاق، حضانت یا نفقه، طرفین به پیام‌ها، تصاویر یا مکالمات این فضاها استناد می‌کنند. با وجود این، نظام حقوقی ایران فاقد چارچوبی شفاف درباره ارزش اثباتی این ادله است. هرچند قوانینی همچون آیین دادرسی کیفری و جرایم رایانه‌ای به موضوعاتی چون شنود، دسترسی غیرمجاز و افشای اطلاعات پرداخته‌اند، اما جایگاه این ادله در دعاوی خانوادگی، به‌ویژه از منظر مشروعیت تحصیل، قابلیت انتساب و تعارض با حریم خصوصی، همچنان محل ابهام است. بنابراین پرسش اصلی پژوهش پیش رو آن است که پیام‌های ردوبدل‌شده در پیام‌رسان‌ها چه جایگاهی در اثبات دعاوی خانوادگی دارند؟

روش: این پژوهش با رویکرد توصیفی–تحلیلی و بر پایه مطالعات کتابخانه‌ای و اسنادی، به بررسی نظریات و مقررات موجود می‌پردازد. منابع شامل کتب تخصصی، مقالات علمی، قوانین داخلی و بین‌المللی و دیدگاه‌های حقوقدانان است.

یافته‌ها: یافته های پژوهش نشان می‌دهد که پیام‌های مبادله‌شده در پیام‌رسان‌ها از نوع «داده‌پیام مطمئن» هستند و مطابق قانون تجارت الکترونیک، دادگاه‌ها نمی‌توانند صرفاً به دلیل شکل یا قالب الکترونیکی، آن‌ها را رد کنند.

نتیجه‌گیری: نتایج پژوهش حاکی از ان است که با توجه به معیارهایی همچون رمز یک‌بارمصرف، هشدارهای ورود و شناسه یکتای پیام، این ادله واجد شرایط داده‌پیام مطمئن بوده و باید در دادرسی پذیرفته شوند. اقتضای عدالت در دادرسی نیز ایجاب می‌کند که در عصر دیجیتال، چنین مستنداتی به‌عنوان دلیل معتبر به رسمیت شناخته شوند.

استناد: حلیمی، زهرا و شریعتی، نفیسه سادات (۱۴۰۴). قابلیت استناد پیام‌های الکترونیکی در دعاوی خانواده با تأکید بر ملاحظات حریم خصوصی. *علوم خبری*، ۱۴ (۴)، ۲۵۲-۲۳۲.

DOI: http//doi.org/10.22034/lrsi.2025.540470.1416

مقدمه

در دهه‌های اخیر، تحولات فناوری اطلاعات و گسترش فراگیر اینترنت و تلفن‌های هوشمند، شیوه‌های ارتباطی میان انسان‌ها را دگرگون ساخته‌اند. در این میان، شبکه‌های اجتماعی به‌عنوان بستری نوین برای برقراری ارتباط، نقش چشمگیری در زندگی روزمره ایفا می‌کنند. این شبکه‌ها فضایی را در اختیار کاربران قرار می‌دهند تا علاقه‌مندی‌ها، افکار و فعالیت‌های خود را با دیگران به اشتراک بگذارند و در عین حال، امکان یافتن دوستان جدید یا تداوم ارتباط با دوستان قدیمی را فراهم می‌سازند. از جمله پرکاربردترین شبکه‌های اجتماعی در داخل و خارج از کشور می‌توان به تلگرام، واتساپ، اینستاگرام، ایتا و بله اشاره کرد که میلیون‌ها کاربر در سراسر جهان را به خود جذب کرده‌اند (درزبان رستمی و بهزادی پور، ۱۳۹۸). با این حال، کارکرد شبکه‌های اجتماعی و پیام‌رسان‌ها صرفاً به جنبه‌های ارتباطی و اجتماعی محدود نمی‌شود. پیام‌رسان‌هایی نظیر واتساپ، تلگرام و ایتا، علاوه بر نقش محوری در تعاملات روزمره، به یکی از مهم‌ترین بسترهای بروز اختلافات و ارائه دلایل اثباتی در مراجع قضایی تبدیل شده‌اند. در بسیاری از دعاوی خانوادگی، از جمله پرونده‌های مربوط به طلاق، حضانت فرزند، نفقه یا مهریه، طرفین دعوی با استناد به محتوای پیام‌های رد و بدل‌شده در این فضاها تلاش می‌کنند ادعاهای خود را به اثبات رسانده یا به رد ادله طرف مقابل بپردازند. برای نمونه، پیام‌های تهدیدآمیز در واتساپ می‌توانند به‌عنوان شاهدی بر وقوع خشونت خانگی مورد استناد قرار گیرند.

از سوی دیگر، نظام حقوقی ایران در مواجهه با چنین تحولاتی با چالش‌های متعددی روبه‌روست. از جمله این چالش‌ها می‌توان به نبود مقررات شفاف درباره ارزش اثباتی ادله دیجیتال در دعاوی خانواده، ابهام در سازوکار احراز اصالت و انتساب این نوع محتواها به اشخاص مشخص، و تعارض‌های احتمالی آن‌ها با اصول بنیادینی چون حریم خصوصی اشاره کرد. این وضعیت باعث شده است که وکلا، قضات و اصحاب دعوی در رویه‌های قضایی با نوعی عدم قطعیت و ناهمسانی مواجه باشند. گرچه برخی محاکم در صورت احراز شرایطی نظیر اصالت محتوا، رضایت طرفین و ارتباط مستقیم با موضوع دعوی، این ادله را مورد پذیرش قرار داده‌اند، اما نبود وحدت رویه قضایی و خلأ تقنینی همچنان به‌عنوان مانعی جدی باقی مانده است.

با توجه به گسترش روزافزون کاربرد فضای مجازی در روابط انسانی و حقوقی، نظام‌های حقوقی ناگزیرند در قواعد سنتی بازنگری کنند و آن‌ها را با مقتضیات فضای دیجیتال تطبیق دهند. در این میان، اقتضای عدالت قضایی ایجاب می‌کند که ضمن بهره‌گیری از ظرفیت‌های نوین اثبات، از اصول بنیادین حقوق فردی همچون حریم خصوصی نیز صیانت شود. از این‌رو، بازنگری در قواعد سنتی اثبات دعوا، متناسب با مختصات فضای دیجیتال، امری ضروری و اجتناب‌ناپذیر است.

این مقاله، با تمرکز بر ساختار حقوقی ایران و بهره‌گیری از تحلیل قوانین، بررسی آرای قضایی و مفاهیم فقهی مرتبط، می‌کوشد ضمن تبیین ارزش اثباتی ادله الکترونیکی در دعاوی خانوادگی، چالش‌های فنی و حقوقی پیشِ رو را شناسایی کرده و در نهایت، پیشنهادهایی برای تقنین هوشمندانه‌تر و ارتقاء کارآمدی مراجع قضایی در راستای تأمین بهتر عدالت و حمایت مؤثر از حقوق طرفین ارائه نماید.

ادبیات موضوع و پیشینه پژوهش

در ادبیات حقوقی، به‌ویژه در حوزه حقوق فناوری، ادله الکترونیکی به‌عنوان یکی از شاخه‌های نوظهور ادله اثبات در فرایند دادرسی مطرح شده‌اند؛ شاخه‌ای که با چالش‌هایی اساسی در زمینه ماهیت، مشروعیت، اصالت و قابلیت انتساب مواجه است و بازنگری در قواعد سنتی ادله را ایجاب می‌کند. در سال‌های اخیر، پژوهش‌های متعددی در داخل و خارج از کشور به بررسی ابعاد مختلف این نوع از ادله پرداخته‌اند و تلاش کرده‌اند جایگاه، اعتبار و الزامات حقوقی آن‌ها را در نظام‌های مختلف حقوقی تبیین کنند.

محور اصلی پژوهش‌های داخلی غالباً بر مباحثی چون چیستی و تعریف ادله الکترونیکی، امکان استناد به آن‌ها، چگونگی احراز اصالت و ارزش اثباتی، و در برخی موارد تعارض میان ادله سنتی و دیجیتال متمرکز بوده است که از مهم ترین آن‌ها می توان به پژوهش هایی نظیر «احراز اصالت در اسناد الکترونیکی» نوشته مرتضی شهبازی نیا و محبوبه عبداللهی(۱۳۸۸)، «ارزیابی اصالت ادله الکترونیکی و ارزش اثباتی آن‌ها»نوشته مصطفی السان و محمدرضا منوچهری(۱۳۹۷)، «مستندسازی بر اساس ادله سنتی و

متجدد الکترونیکی و آثار آن در نظام قضایی» نوشته سید علی ربانی موسویان و طاهره سادات نعیمی(۱۳۹۸)، «بررسی حقوقی ادله الکترونیکی در نظام کنونی» از نصرت اله حیدری نژاد(۱۳۹۶) و «اعتبار اسناد الکترونیکی به‌عنوان ادله اثبات دعوا در دعاوی زوجین» نوشته رحیمی و طاهری‌پور (۱۳۹۸) اشاره کرد.

همچنین شماری از پژوهش‌ها به بررسی ابعاد حقوقی حریم خصوصی در مواجهه با ادله الکترونیکی پرداخته‌اند که از آن جمله می‌توان به مقاله ای با عنوان «حمایت از حریم خصوصی در دنیای دیجیتال: تضمین حقوق شخصی در محیط های آنلاین» نوشته عطیه جعفری(۱۴۰۳) و «مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن‌ها در فضای مجازی» از فاطمه قناد و امیره عقیلی(۱۳۹۹) اشاره کرد که به بررسی مفهوم حریم خصوصی و راهکارهای مختلف حفاظت از حریم خصوصی در دنیای دیجیتال می پردازند.

تمایز پژوهش حاضر با آثار پیش‌گفته در آن است که تمرکز آن به‌صورت خاص بر قابلیت استناد پیام‌های رد و بدل شده در شبکه‌های اجتماعی نظیر واتساپ، تلگرام و اینستاگرام در دعاوی خانوادگی است؛ مصادیقی که در عمل کاربرد فراوانی یافته و کمتر به‌طور مستقل در مطالعات حقوقی مورد توجه قرار گرفته‌اند.

از جمله مهم ترین آثاری که توسط پژوهشگران خارجی در این زمینه نگاشته شده اند میتوان به کتابی با عنوان «اسناد الکترونیک» نوشته استیون میسون و دنیل سنگ[1](۲۰۱۷) و مقالاتی نظیر«استفاده از ادله رسانه‌های اجتماعی در دعاوی خانواده» از کاناوان و کولستاد[2](۲۰۱۶) و«ادله ناشی از رسانه های اجتماعی در دعاوی خانوادگی: حدود قابلیت استناد و ارزش اثباتی » نوشته ویکتوریا بلیکلی و همکاران[3](۲۰۱۵) اشاره کرد.

۱. تعریف و ماهیت حقوقی ادله الکترونیک

مطابق ماده ۱۹۴ قانون آیین دادرسی مدنی، دلیل عبارت است از امری که اصحاب دعوا برای اثبات یا دفاع از دعوا به آن استناد می‌کنند. همچنین مطابق با ماده ۱۲۵۸ قانون مدنی، دلایل اثبات دعوا عبارت‌اند از: اقرار، اسناد کتبی، شهادت، امارات و قسم.
با تصویب قانون تجارت الکترونیکی در سال ۱۳۸۲، مفهوم «دلیل الکترونیکی» به‌عنوان قالبی نوین از ادله، وارد نظام حقوقی ایران گردید. هرچند تعریف صریحی از این نوع دلیل در متون قانونی ارائه نشده است، اما با توجه به اینکه وصف «الکترونیکی» ناظر بر قالب و شکل دلیل است، نه ماهیت آن، می‌توان چنین استنباط کرد که دلیل الکترونیکی به هرگونه داده، نرم‌افزار یا سخت‌افزار الکترونیکی اطلاق می‌شود که قابلیت ارائه اطلاعات مؤثر در اثبات دعوا، دفاع، کشف جرم یا استدلال قضایی را دارا باشد (حیدری‌نژاد،۱۳۹۶). بر همین اساس، دلایل مصرح در ماده ۱۲۵۸ قانون مدنی، چنانچه به‌صورت الکترونیکی ارائه شوند، در زمره ادله الکترونیکی قرار می‌گیرند؛ از جمله سند الکترونیکی، امضای الکترونیکی، اقرار الکترونیکی، شهادت و سوگند الکترونیکی (حبیب‌زاده، ۱۳۹۶: ۶۷).
مطابق ماده ۱۲ قانون تجارت الکترونیکی، اسناد و ادله اثبات دعوی می‌توانند به‌صورت داده‌پیام ارائه شوند و هیچ محکمه یا اداره دولتی نمی‌تواند صرفاً به دلیل شکل و قالب دیجیتالی آن‌ها، ارزش اثباتی‌شان را نفی کند. همچنین بند (الف) ماده ۲ همان قانون در تعریف داده‌پیام بیان می‌دارد: «هر نمادی از واقعه، اطلاعات یا مفهوم که با وسایل الکترونیکی، نوری و یا فناوری‌های جدید اطلاعات، تولید، ارسال، دریافت، ذخیره یا پردازش می‌شود.» با توجه به این تعریف وسیع و پویا، می‌توان گفت تمامی ابزارهای موجود که به‌نحوی در فرآیند تبادل، انتقال یا پردازش اطلاعات از طریق فناوری‌های نوین دخیل هستند، مشمول مفهوم «داده‌پیام» قرار می‌گیرند و می‌توانند به‌عنوان ادله اثبات دعوا به دادگاه ارائه شوند. بر این اساس، داده‌پیام صرفاً محدود به پیام‌های متنی ساده

[1] Stephen Mason & Daniel Seng
[2] Canavan Marcia & Eva Kolstad
[3] Victoria Blakeley et al.

(SMS) یا نامه‌های الکترونیکی نیست، بلکه شامل انواع گسترده‌ای از محتواهای دیجیتال از جمله پیام‌های چندرسانه‌ای (MMS)، تصاویر دیجیتال، سیگنال‌های صوتی و تصویری، و حتی تراکنش‌های بانکی آنلاین نیز می‌شود (حبیب‌زاده، ۱۳۹۶، ص ۸۱).

در نظام حقوقی ایران، دلایل اثبات دعوا به هشت نوع تقسیم شده‌اند که برای پذیرش هر دلیلی در دادگاه، لازم است دلیل ارائه‌شده در یکی از این قالب‌های شناخته‌شده قرار گیرد تا از ارزش اثباتی همان نوع برخوردار شود. با این حال، قانون تجارت الکترونیکی، بدون آنکه اصلاحی در قوانین موجود ایجاد کند، داده‌های الکترونیکی را به‌عنوان نوعی جدید از دلیل، هم‌عرض با دلایل سنتی تلقی کرده و اجازه می‌دهد که این دلایل به شکل هر یک از قالب‌های سنتی ظاهر شوند و ارزش اثباتی همان قالب را داشته باشند (ربانی موسویان و نعیمی، ۱۳۹۸).

در نهایت، دلیل الکترونیکی برای تحقق هر نوع کارکرد اثباتی، در قالب سند جای می‌گیرد؛ چرا که داده‌پیام ماهیتی دارد که امکان انطباق آن با قالب نوشته را فراهم می‌سازد. از نظر قانونی، همه دلایل الکترونیکی به‌صورت داده‌پیام هستند و قانون‌گذار نیز داده‌پیام را جایگزین قانونی نوشته دانسته است. از این‌رو ، هر نوشته‌ای که برای اثبات دعوا ارائه می‌شود، سند محسوب می‌شود. بنابراین، دلیل الکترونیکی در چارچوب نظام سنتی ادله اثبات دعوا، از اعتبار سند برخوردار است، مگر آنکه برای بیان شهادت مورد استفاده قرار گیرد؛ در این حالت، مطابق ماده ۱۲۸۵ قانون مدنی، ارزش اثباتی آن در قالب شهادت سنجیده می‌شود و بر اساس ماده ۲۴۱ قانون آیین دادرسی مدنی، تشخیص میزان اعتبار آن بر عهده دادگاه خواهد بود (همان). همچنین، در صورتی که اقرار در قالب داده‌پیام به دادگاه ارائه شود، چون داده‌پیام در حکم نوشته محسوب می‌شود، اقرار الکترونیکی همانند اقرار مکتوب از اعتبار اثباتی برخوردار خواهد بود. ماده ۱۲ قانون تجارت الکترونیکی نیز صراحتاً این موضوع را تأیید کرده است. ذکر عنوان «اسناد و ادله اثبات دعوا» در این ماده بیانگر آن است که قانون‌گذار داده‌پیام را در جایگاه سند قرار داده است (همان).

بنابراین، پیامک‌های ساده و همچنین پیام‌های شبکه‌های اجتماعی مانند واتساپ، اینستاگرام و تلگرام، به نوعی زیرمجموعه‌ای از اسناد الکترونیکی به حساب می‌آیند، به‌ویژه زمانی که پیام‌های متنی یا تصاویر به‌عنوان سند برای اثبات ادعای طرفین مورد استفاده قرار گیرند. با این حال، ویژگی‌های خاص پیام‌های شبکه‌های اجتماعی مانند قابلیت دستکاری و تغییرپذیری، فقدان امضای الکترونیکی مطمئن و دسترسی آسان به آن‌ها، باعث می‌شود که این نوع ادله چالش‌های جدیدی در دادرسی‌ها به وجود آورند که نیاز به مطالعه بیشتر در این زمینه را می‌طلبد.

۲. ارزش اثباتی ادله الکترونیکی

یکی از چالش‌های اساسی در رویه قضایی ایران، فقدان توجه کافی به ادله الکترونیکی در فرآیند رسیدگی به دعاوی است. پرسش مهمی که در این زمینه مطرح می‌شود آن است که چرا در پرونده‌های مطرح در محاکم، نقش ادله الکترونیکی همچنان حاشیه‌ای باقی مانده است. به نظر می‌رسد یکی از پاسخ‌های ابتدایی به این پرسش، نوظهور بودن این نوع از ادله و در نتیجه، نبود درک روشن و یکدست از جایگاه و ارزش اثباتی آن‌ها در میان قضات و مراجع قضایی باشد. این وضعیت در واقع بازتابی از چالشی بزرگ‌تر در عرصه حقوق بشر و حقوق داخلی است: پویایی جامعه و ظهور نیازها و حقوق جدید که نظام‌های حقوقی به‌سختی قادر به همگامی با آن‌ها هستند.

امروزه اینترنت به بخشی جدایی‌ناپذیر از زندگی روزمره افراد تبدیل شده و همین امر تلاش‌ها برای شناسایی و تثبیت «حق دسترسی به اینترنت» در کنار سایر حقوق بنیادین بشر همچون آزادی بیان و حق اشتغال را تقویت کرده است. این تحول نشان می‌دهد که ماهیت پویا و در حال تغییر جامعه‌ی بشری، ضرورت بازنگری و گسترش مستمر دامنه‌ی حقوق بشر را برای پاسخ‌گویی به چالش‌های نوظهور ایجاب می‌کند. بر همین اساس، مفاهیمی چون حق برخورداری از حریم خصوصی ژنتیکی، حق هویت یکتا و حق دسترسی به اینترنت در زمره «حقوق بشر نو» قرار گرفته‌اند (بابازاده مقدم و خدری، ۱۴۰۱).

در همین راستا، ادله الکترونیکی نیز به‌عنوان یکی از مصادیق حقوق نوپدید در عرصه دادرسی مطرح می‌شوند. هرچند قانون جرایم رایانه‌ای مصوب ۱۳۸۸ در بخش دوم تحت عنوان «آیین دادرسی» و به‌ویژه در فصل دوم خود به موضوع «جمع‌آوری ادله الکترونیکی» پرداخته است، اما این قانون چارچوبی برای ارزیابی و سنجش ارزش اثباتی این نوع از ادله ارائه نکرده است. به بیان دیگر، اگرچه بستر قانونی برای شناسایی و جمع‌آوری ادله الکترونیکی فراهم شده، اما مبانی حقوقی لازم برای تعیین اعتبار و نقش آن‌ها در فرآیند استدلال قضایی همچنان مبهم باقی مانده است (دهقانی، فلاح و هاشمی، ۱۴۰۱).

در این راستا، قانون تجارت الکترونیکی مصوب ۱۳۸۲ را می‌توان یکی از نخستین اقدامات تقنینی در جهت شناسایی و پذیرش اعتبار ادله الکترونیکی در نظام حقوقی ایران دانست. این قانون با به رسمیت شناختن داده‌پیام‌ها و اسناد الکترونیکی به‌عنوان ادله‌ای معتبر نزد مراجع رسمی و قضایی، گامی مهم در انطباق نظام حقوقی کشور با تحولات ناشی از فناوری اطلاعات و ارتباطات برداشته است. مطابق مفاد این قانون، ارزش اثباتی ادله الکترونیکی منوط به تشخیص مقام قضایی است. با این حال، یکی از اصول اساسی در حقوق تجارت الکترونیکی آن است که الکترونیکی بودن قالب دلیل نباید موجب سلب اعتبار آن گردد. به بیان دیگر، داده‌پیام‌ها نباید صرفاً به دلیل شکل الکترونیکی‌شان از شمول ادله قابل استناد خارج شوند، مگر آنکه قانون‌گذار به صراحت بی‌اعتباری آن‌ها را اعلام کرده باشد؛ نظیر موارد مقرر در ماده ۶ قانون تجارت الکترونیکی ایران (حبیب‌زاده، ۱۳۹۶: ۶۸).

در یک جمع‌بندی کلی می‌توان گفت که قابلیت استناد ادله الکترونیکی، مستلزم تحقق شرایطی است: نخست، داده‌پیام یا سند الکترونیکی باید به همان شکل اولیه‌ای که تولید شده، همراه با اطلاعات جانبی نظیر زمان و مکان ایجاد، به‌صورت الکترونیکی ذخیره شده باشد. دوم، امکان ارائه آن در مراجع قضایی یا سایر مراجع ذی‌صلاح وجود داشته باشد؛ ارائه‌ای که یا به‌صورت الکترونیکی و از طریق تجهیزات فنی مانند رایانه در دادگاه انجام می‌پذیرد، یا با استفاده از ابزارهای فیزیکی همچون چاپ و ارائه نسخه کاغذی پیامک یا ایمیل ممکن می‌گردد. سوم، آن دلیل باید به‌گونه‌ای ایجاد شده باشد که حداکثر ضریب اطمینان نسبت به عدم تغییر یا دستکاری را دارا باشد؛ موضوعی که استفاده از فناوری‌های امن و قابل اعتماد را ضروری می‌سازد. بدیهی است چنانچه اسناد الکترونیکی از معیارهای لازم برای برخورداری از جایگاه دلیل برخوردار نباشند، همچنان می‌توانند به عنوان اماره قضایی مورد توجه دادگاه قرار گیرند (حبیب‌زاده، ۱۳۹۶: ۶۷).

ادله الکترونیکی از حیث قابلیت استناد، به دو دسته کلی تقسیم می‌شوند: دلایل الکترونیکی عادی (غیرمطمئن) و دلایل الکترونیکی مطمئن.

دلیل الکترونیکی عادی یا غیرمطمئن، داده‌پیامی است که از طریق یک سیستم اطلاعاتی غیرمطمئن تولید، پردازش، ارسال یا ذخیره شده باشد و به وسیله امضای الکترونیکی ساده تصدیق گردد. امضای الکترونیکی ساده می‌تواند به اشکال مختلفی مانند تصویر اسکن‌شده امضای دستی، درج نام شخص، ذکر نشانی رایانامه (ایمیل) یا استفاده از گذرواژه باشد. ویژگی مشترک این روش‌ها آن است که فاقد توانمندی لازم برای احراز هویت امضاکننده، انتساب سند به وی یا تضمین تمامیت محتوای سند هستند؛ چراکه به‌راحتی قابل جعل و دستکاری‌اند. به عنوان نمونه، شخص ثالث می‌تواند با الصاق تصویر امضای دیگری یا با دسترسی به گذرواژه وی، هویت شخص را جعل کند (شهبازی‌نیا و عبداللهی، ۱۳۸۸).

بنابراین، اسناد عادی قابلیت انکار و تردید دارند. مطابق مواد ۱۲۹۱ و ۱۲۹۲ قانون مدنی، هرگاه صدور سند از سوی منتسب‌الیه تصدیق شود و یا در دادگاه ثابت گردد که سند مزبور توسط وی امضا یا مهر شده است، سند عادی اعتبار سند رسمی را خواهد داشت و انکار و تردید نسبت به آن مسموع نیست (دهقانی، فلاح و هاشمی، ۱۴۰۱).

در مقابل، دلیل الکترونیکی مطمئن به داده‌پیامی اطلاق می‌شود که در بستر یک سامانه اطلاعاتی مطمئن تولید، ارسال، پردازش یا نگهداری شده و با استفاده از امضای الکترونیکی مطمئن مورد تأیید قرار گرفته باشد. بر اساس ماده ۱۴ همین قانون، داده‌پیام‌هایی که به نحو مطمئن ایجاد و نگهداری شده‌اند، از نظر محتوا و امضای مندرج در آن‌ها، آثار و تعهداتی نظیر اسناد رسمی خواهند داشت و در مراجع قضایی و حقوقی قابل استناد هستند. همچنین به موجب ماده ۱۵ این قانون، در خصوص داده‌پیام مطمئن، امضای

الکترونیکی مطمئن و سوابق الکترونیکی مطمئن، اصل بر اعتبار آن‌هاست و انکار و تردید نسبت به آن‌ها مسموع نیست؛ تنها ادعای جعل یا اثبات سقوط اعتبار قانونی آن‌ها قابل طرح خواهد بود. در نتیجه، سطح ایمنی و اعتبار حقوقی ادله الکترونیکی مطمئن به نحوی است که انتساب سند به صادرکننده، هویت او یا تمامیت اسناد را تضمین می‌کند و این اسناد غیرقابل انکار، غیرقابل تردید و غیرقابل جعل هستند (شهبازی‌نیا وعبداللهی، ۱۳۸۸). در رابطه با اینکه امضای الکترونیکی مطمئن چیست باید به قوانین مختلف رجوع کنیم.

بند الف ماده ی ۲ قانون راهنمای امضاهای الکترونیکی آنسیترال (۲۰۰۱) امضای الکترونیکی را این چنین تعریف می‌کند: «امضای الکترونیکی عبارت است از داده‌ای دیجیتالی، که به یک پیام داده‌ای پیوست شده، یا به‌گونه‌ای منطقی به آن مرتبط است، و می‌تواند برای شناسایی امضاکننده در ارتباط با آن پیام داده‌ای و برای نشان دادن تأیید او نسبت به اطلاعات موجود در پیام داده‌ای به‌کار رود.»

دستورالعمل امضای الکترونیکی اروپا نیز درتعریف امضای الکترونیکی بیان می‌کند: «داده‌های الکترونیکی که به سایر داده‌پیام‌های الکترونیکی منضم شده یا به نحو منطقی به آنها متصل شده و به عنوان وسیله‌ای برای مستندسازی به کار می‌رود.»

قانون‌گذار ایران نیز دربند ی از ماده ی ۲ قانون تجارت الکترونیک، در تعریف امضای الکترونیکی چنین مقرر می‌دارد: «امضای الکترونیکی عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده‌پیام است که برای شناسایی امضاکننده داده‌پیام مورد استفاده قرار می‌گیرد.» و در ماده ۱۰ قانون تجارت الکترونیکی ویژگی‌های امضای الکترونیکی مطمئن را این‌گونه بیان می‌کند: «امضای الکترونیکی مطمئن باید دارای شرایط زیر باشد:

الف – نسبت به امضاکننده منحصر به فرد باشد.

ب – هویت امضاکننده داده‌پیام را معلوم نماید.

ج – به وسیله امضاکننده و یا تحت اراده انحصاری وی صادر شده باشد.

د – به نحوی به یک داده‌پیام متصل شود که هر تغییری در آن داده‌پیام قابل تشخیص و کشف باشد.»

بنابراین مطابق با این تعاریف، امضای الکترونیکی داده‌ای دیجیتالی است که به یک پیام داده‌ای پیوست می‌شود یا به‌گونه‌ای منطقی با آن مرتبط است و با هدف شناسایی امضاکننده و اعلام رضایت یا تأیید وی نسبت به محتوای پیام داده‌ای مورد استفاده قرار می‌گیرد. این نوع امضا می‌تواند اشکال متنوعی از جمله امضای دیجیتال، کد رمز، کلیک بر دکمه تایید، یا سایر فناوری‌های قابل اطمینان را دربر گیرد و نقش بنیادینی در احراز هویت، اعتبارسنجی و اثبات قصد حقوقی در تعاملات الکترونیکی ایفا می‌کند. بنابراین هرچند قانونگذار روش‌های احراز هویت و سندیت اسناد الکترونیکی را بسیار ساده تبیین کرده است اما درعمل آنچه در دستگاه های اجرایی رخ میدهد خلاف این موضوع است که با دادرسی عادلانه منافات دارد.

۳. ارزش اثباتی پیامک‌ها و پیام‌های شبکه های اجتماعی

پیام‌های متنی که در فرآیند دادرسی به عنوان دلیل ارائه می‌شوند، به‌طور کلی در دو گروه قابل تقسیم‌اند: الف) پیام‌های مخابراتی نظیر پیامک‌هایی که از طریق اپراتورهایی مانند همراه اول، ایرانسل و رایتل ارسال می‌شوند و ب) پیام‌های پلتفرمی که از طریق بستر اینترنت و سکوهایی نظیر تلگرام، واتساپ، ایتا و... مبادله می‌گردند. پیام‌های گروه دوم عموماً از طریق سرورهای اختصاصی این سکوها منتقل و ذخیره می‌شوند و ارتباطی با زیرساخت‌های مخابراتی ندارند.

تفاوت اصلی این دو گروه، در نوع و حجم اطلاعات قابل انتقال است؛ در حالی‌که سرویس پیامک تنها قابلیت ارسال متن ساده را دارد، پیام‌رسان‌های نوین امکان تبادل انواع محتوای چندرسانه‌ای (صوت، تصویر، ویدیو و...) را فراهم می‌آورند (حبیب‌زاده، ۱۳۹۶: ۸۱).

از منظر حقوقی، پیام‌های دیجیتالی جزء «داده‌پیام‌های مطمئن» محسوب می‌شوند و مطابق با اصول مندرج در قانون تجارت الکترونیکی و آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، می‌توان به آن‌ها در دعاوی مدنی و کیفری استناد کرد.

برای تشخیص اصالت و اعتبار فنی این نوع پیام‌ها، می‌توان به شاخص‌های زیر توجه کرد:

۱-۳. هشدارهای امنیتی ورود به حساب کاربری: یکی از شاخص‌های فنی مؤثر در اعتبارسنجی پیام‌های دیجیتال، هشدارهای امنیتی ورود به حساب کاربری است که توسط پیام‌رسان‌هایی مانند واتساپ و تلگرام ارائه می‌شود. این هشدارها زمانی صادر می‌شوند که ورود به حساب از یک دستگاه جدید صورت گیرد و معمولاً شامل اطلاعاتی نظیر نوع دستگاه (مانند اندروید یا ویندوز)، موقعیت جغرافیایی تقریبی (بر مبنای IP)، زمان و تاریخ دقیق ورود هستند (مارکرت و همکاران، ۲۰۲۴). اهمیت این داده‌ها در مستندسازی فعالیت‌های کاربر و تشخیص صحت ادعاهای طرفین دعوا بسیار بالاست. برای نمونه، اگر شخصی ارسال پیام خاصی را انکار کند، ارائه هشدار ورود از دستگاهی که با سوابق قبلی او مطابقت دارد، می‌تواند قرینه‌ای بر دسترسی وی به حساب و صدور پیام باشد. این اطلاعات در محیط پیام‌رسان ذخیره شده و از طریق گزینه‌هایی مانند نشست‌های فعال[1]در تلگرام یا هشدارهای ایمیلی[2] در واتساپ قابل مشاهده هستند.

۲-۳. قابلیت بررسی نشست‌های فعال: از دیگر شاخص‌های فنی مؤثر در احراز اصالت پیام‌ها، قابلیت بررسی نشست‌های فعال در پیام‌رسان‌هایی مانند تلگرام و واتساپ است. این قابلیت به کاربران امکان می‌دهد مشاهده کنند که چه دستگاه‌هایی به حساب کاربری آن‌ها متصل‌اند و در صورت لزوم، دسترسی هر دستگاه را به‌صورت دستی مسدود کنند. برای هر نشست، اطلاعاتی همچون نوع دستگاه، موقعیت جغرافیایی تقریبی، آدرس IP، زمان آخرین فعالیت و نسخه سیستم‌عامل یا اپلیکیشن ارائه می‌شود. این داده‌ها برای اثبات زمان و محل تقریبی دسترسی کاربر به حساب و تفکیک میان استفاده مجاز و غیرمجاز از حساب بسیار حائز اهمیت است (تلگرام، ۲۰۱۵).

در مواردی که یکی از طرفین دعوا منکر ارسال پیام خاصی می‌شود، ارائه فهرست نشست‌ها و مطابقت آن با سابقه استفاده فرد، می‌تواند دلیلی برای انتساب آن پیام باشد. این اطلاعات در دعاوی خانوادگی، به‌ویژه در مواردی مانند تهدید، توهین یا مزاحمت، قابلیت اثباتی ویژه‌ای دارند.

۳-۳. استفاده از رمز یک‌بار مصرف(OTP)[3] : یکی دیگر از شاخص‌های فنی کلیدی در اعتبارسنجی و احراز هویت کاربران در پیام‌رسان‌هایی نظیر واتساپ و تلگرام استفاده از رمز یک‌بار مصرف است. این رمزها معمولاً به هنگام ورود کاربر به حساب کاربری یا تغییر دستگاه، از طریق پیامک، تماس صوتی یا پیام درون‌برنامه‌ای ارسال می‌شوند. رمزهای یک‌بارمصرف، به‌طور تصادفی تولید شده، محدود به زمان مشخصی بوده و فقط برای یک‌بار قابل استفاده‌اند؛ به همین دلیل، امکان جعل یا استفاده مجدد از آن‌ها عملاً وجود ندارد. کارکرد اصلی این رمزها، جلوگیری از دسترسی غیرمجاز حتی در صورت افشای رمز عبور اصلی است(مؤسسه ملی استاندارد و فناوری آمریکا، ۲۰۱۷). از منظر دادرسی، دریافت رمز یک‌بار مصرف ازسوی کاربر در زمان خاص، قرینه‌ای مهم بر قصد ورود و دسترسی مستقیم او به حساب تلقی می‌شود. در مواردی که یکی از طرفین دعوا منکر ورود به حساب و ارسال پیام خاصی است، وجود مستندات مربوط به صدور و ورود با رمز یک‌بار مصرف، می‌تواند نقش اثباتی تعیین‌کننده داشته باشد. نهادهای استانداردگذاری نظیر مؤسسه ملی استاندارد و فناوری آمریکا[4] استفاده از رمزیکبار مصرف را به‌عنوان یک لایه مؤثر

[1] Active Sessions
[2] Email Alerts
[3] One-Time Password
[4] NIST: National Institute of Standards and Technology

در احراز هویت دیجیتال توصیه کرده‌اند. در حقوق ایران نیز این مکانیسم در راستای اصل امنیت داده‌پیام‌ها، می‌تواند مؤید اطمینان از انتساب باشد. از این‌رو، رمزهای رمز یک‌بار مصرف از منظر فنی و حقوقی نقش مهمی در اثبات یا رد ادعاهای طرفین ایفا می‌کنند.

۴-۳. شناسه یکتا *(UUID)*[1]: یکی از مهم‌ترین شاخص‌های فنی در شناسایی و تفکیک داده‌های دیجیتال، وجود شناسه یکتا برای هر پیام یا واحد اطلاعاتی است که مانند شناسنامه برای افراد عمل می‌کند. شناسه یکتا رشته‌ای از کاراکترهاست که به‌صورت تصادفی یا زمان‌محور تولید شده و به‌گونه‌ای طراحی شده است که احتمال تکرار آن در هیچ دو پیام یا شیء دیجیتالی وجود ندارد(لیچ، میلینگ و سالز، ۲۰۰۵). در پیام‌رسان‌ها، هر پیام، حتی اگر حاوی متنی کاملاً مشابه با پیام دیگر باشد (مانند پیام «سلام» به افراد مختلف)، دارای شناسه‌ای کاملاً مجزا است(شرکت بامسئولیت محدود *ESeye*، ۲۰۲۳). این شناسه‌ها در فرایند ذخیره‌سازی، انتقال، و بازیابی داده‌ها نقش تعیین‌کننده‌ای دارند و امکان ردیابی دقیق هر پیام را فراهم می‌کنند. در فرآیند دادرسی، وجود این شناسه‌ها به قاضی یا کارشناس امکان می‌دهد تا صحت، اصالت، و عدم‌دستکاری پیام‌ها را با دقت بررسی کند. همچنین در مواجهه با ادعای جعل، حذف یا دست‌کاری پیام، تطبیق شناسه یکتا با داده‌های ثبت‌شده در سیستم منبع می‌تواند قرینه‌ای قطعی در تأیید یا رد ادعا باشد. استاندارد *UUID* به‌عنوان مبنای جهانی در بسیاری از سامانه‌های دیجیتال پذیرفته شده است. در نتیجه، استفاده از شناسه‌های یکتا در پیام‌رسان‌ها نقش مهمی در افزایش قابلیت استناد و اعتماد به داده‌پیام‌ها دارد و باید در ارزیابی ارزش اثباتی آن‌ها مورد توجه جدی قرار گیرد.

با اتکا به این معیارهای فنی، می‌توان پیام‌های ردوبدل‌شده در پیام‌رسان‌ها را داده‌پیام‌های مطمئن تلقی کرد. در صورت انکار ارسال پیام از سوی شخص منتسب، وی باید خلاف آن را اثبات کند و در این مسیر، خود نیز می‌تواند از شاخص‌های فنی فوق بهره گیرد.

در رویه معمول، پس از ارائه پیام‌ها به عنوان ادله، مقام قضایی مستند به بند (الف) ماده ۱۸ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، دستور ارائه نسخه‌ای چاپی از داده‌پیام را صادر می‌کند که این امر غالباً توسط شاکی یا ضابطان قضایی و از طریق چاپ نماگرفت پیام در محیط پیام‌رسان‌ها انجام می‌گیرد. ماده ۴۷ آیین‌نامه نیز مقرر می‌دارد که: «نسخه‌های تهیه‌شده از داده‌های رایانه‌ای قابل استناد به‌صورت متن، صوت یا تصویر در حکم اصل داده می‌باشند». با این حال، نکته‌ای اساسی که باید مورد توجه قرار گیرد آن است که قاضی پیش از پذیرش داده‌پیام یا سند الکترونیکی به عنوان دلیل، موظف است احراز کند که این مستندات واقعاً به ارسال‌کننده منتسب هستند (دبلفون، ۱۳۸۸: ۱۶۰).

در این راستا، نخستین اقدام مقام قضایی می‌تواند پرسش از فرد منتسب‌الیه باشد تا مشخص شود که آیا ارسال پیام‌های ارائه‌شده را می‌پذیرد یا خیر. در صورت انکار، مطابق ماده ۱۷ «آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی»، قاضی می‌تواند به ارائه‌دهندگان خدمات دستور دهد تا اصل داده‌ها را در اختیار مرجع قضایی قرار دهند. این داده‌ها ممکن است شامل محتوای پیام، زمان ارسال و دریافت، و اطلاعات هویتی فرستنده و گیرنده باشند. در مورد پیام‌های مخابراتی، این اطلاعات معمولاً در سامانه‌های اپراتور ذخیره شده و دسترسی به آن‌ها برای مراجع قضایی امکان‌پذیر است. همچنین در پیام‌رسان‌های داخلی که سرورهای آن‌ها در داخل کشور مستقر است، دسترسی به اطلاعات مرتبط با پیام‌ها از طریق دستور قضایی فراهم است. اما در مورد پیام‌رسان‌های خارجی مانند تلگرام، واتساپ، اینستاگرام و سایر شبکه‌های مشابه که سرورهای آن‌ها در خارج از کشور قرار دارد، دسترسی مستقیم به داده‌ها برای مراجع داخلی دشوار یا عملاً ناممکن است.

با این وجود، چنین محدودیتی نباید به این معنا تلقی شود که پیام‌های مبادله‌شده در این بسترها فاقد امضای الکترونیکی معتبر یا سابقه الکترونیکی مطمئن‌اند. در این موارد، ضروری است از کارشناسان فناوری اطلاعات برای بررسی اصالت داده‌پیام و شناسایی هرگونه جعل یا دست‌کاری احتمالی بهره گرفته شود.

[1] Universally Unique Identifier

در نتیجه، پیام‌های مبادله‌شده در شبکه‌های اجتماعی نیز می‌توانند «داده‌پیام مطمئن» تلقی شده و به عنوان دلیل در فرآیند دادرسی مورد استناد قرار گیرند، چرا که پذیرش آن‌ها لازمه تحقق دادرسی عادلانه در عصر دیجیتال است.

۴. چالش حریم خصوصی در استفاده از پیام‌ها به عنوان ادله

اهمیت و ضرورت حمایت از حریم خصوصی از دیرباز در نظام‌های حقوقی دنیا مورد توجه قرار گرفته است و در مقررات مختلف تعاریف متفاوتی از حریم خصوصی ارائه شده است. حریم خصوصی، قلمرو زندگی هر فرد دانسته شده است که نوعاً یا عرفاً و یا با اعلان قبلی، انتظار دارد دیگران بدون رضایت وی به اطلاعات مربوط به آن قلمرو دسترسی نداشته باشند یا به آن قلمرو وارد نشوند یا به آن قلمرو نگاه یا نظارت نکنند یا به هر صورت دیگری وی را در آن قلمرو مورد تعرض قرار ندهند (انصاری، ۱۳۸۷). این مفهوم ابعاد مختلفی چون حریم جسمانی، مکانی، اطلاعاتی و ارتباطاتی را در بر می‌گیرد. یکی از مهم‌ترین ابعاد مزبور، حریم خصوصی ارتباطاتی است که بر محرمانگی مکاتبات و تعاملات افراد از طریق وسایل ارتباطی تأکید دارد و حق هر شخص بر عدم دسترسی غیرمجاز به این تعاملات را تضمین می‌کند. بر همین مبنا، ارتباطات خصوصی مانند پیامک، ایمیل، تماس تلفنی، و سایر ابزارهای نوین ارتباطی مشمول حمایت‌های ویژه قانونی قرار گرفته‌اند (صادقی، ۱۳۹۶: ۱۱۷).

از آن‌جا که پیام‌های رد و بدل‌شده در پیام‌رسان‌ها معمولاً حاوی اطلاعات خصوصی و شخصی هستند، موجب بروز چالش‌هایی در رابطه با حریم خصوصی و امکان دسترسی به این داده‌ها در چارچوب قانونی شده‌اند. دسترسی به محتوای پیامک‌های کاربران بدون مجوز قضایی، به نوعی ورود در حریم خصوصی آنان محسوب می‌شود. در واقع، کنترل پیامک‌ها همانند شنود، محتاج تجویز قانون است. تبصره ماده ۴۸ قانون جرایم رایانه‌ای ۱۳۸۸ مقرر می‌کند: «شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود. دسترسی به محتوای ارتباطات غیرعمومی ذخیره‌شده، نظیر پست الکترونیکی یا پیامک در حکم شنود و مستلزم رعایت مقررات مربوط است» (حبیب‌زاده، ۱۳۹۶: ۷۷).

مقررات حاکم بر شنود مکالمات تلفنی دو دسته‌اند: یک دسته از مقررات به اصل موضوع پرداخته و اصل را بر عدم امکان شنود مکالمات تلفنی و هر نوع ارتباطات مخابراتی اشخاص می‌گذارند. این مقررات در ارتباط با حریم خصوصی اشخاص است که دارای حرمت و محدودیت برای ورود دیگران است؛ حریم منزل، دفتر کار، نامه‌نگاری‌ها، ایمیل، پیامک و نامه‌های اداری و شخصی و تماس‌های تلفنی، مصداق‌های حریم خصوصی اشخاص می‌باشند. در حقوق ایران، اصل ۲۵ قانون اساسی به لزوم احترام به حریم خصوصی اشخاص در ارتباطات از راه دور اشاره می‌کند و در راستای ایجاد اطمینان در طرفین برای برقراری ارتباط ایمن و خصوصی، هرگونه دسترسی به محتوای ارتباطات را ممنوع اعلام می‌کند. در ماده ۱۰۵ قانون آیین دادرسی کیفری ۱۳۹۲ نیز به این موضوع تصریح شده است.

دسته دوم از مقررات، مجازات شنود غیرمجاز را که در واقع ضمانت اجرای آن است، بیان کرده‌اند. برای مثال، ماده ۷۳۰ قانون مجازات اسلامی (ماده ۲ قانون جرایم رایانه‌ای ۱۳۸۸) مقرر می‌دارد: «هر کس به‌طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ۸۲٬۵۰۰٬۰۰۰ تا ۵۰۰٬۰۰۰٬۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد» (حبیب‌زاده، ۱۳۹۶: ۷۸).

علاوه بر این، قانون‌گذار در ماده ۱ قانون جرایم رایانه‌ای و چند ماده از قانون تجارت الکترونیکی به بحث حمایت از داده‌ها پرداخته است. ماده ۱ قانون جرایم رایانه‌ای در زمینه حمایت از داده‌ها چنین مقرر می‌دارد: «هرکس به‌طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال

یا جزای نقدی از پنج میلیون ریال تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.» این ماده، با هدف حمایت همه‌جانبه از اقدام اشخاص در اتخاذ تدابیر امنیتی برای سیستم یا داده‌های خود، دسترسی غیرمجاز را به‌صورت ساده جرم‌انگاری کرده است. از آن‌جا که هکرها دارای امکانات‌اند و جزای نقدی صرف، قدرت بازدارندگی ندارد، مجازات حبس نیز برای آن‌ها پیش‌بینی شده است.

قانون‌گذار در مواد ۵۸ تا ۶۱ قانون تجارت الکترونیکی مصوب ۱۳۸۲ به حمایت از داده‌پیام‌های شخصی پرداخته است. در ماده ۵۸ این قانون، ذخیره، پردازش و یا توزیع داده‌پیام‌های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و داده‌پیام‌های راجع به وضعیت جسمانی، روانی یا جنسی اشخاص بدون رضایت صریح آن‌ها غیرقانونی دانسته شده است. ماده ۵۹ قانون مورد بحث، ذخیره و پردازش و توزیع داده‌پیام‌های شخصی در بستر مبادلات الکترونیکی را در صورت رضایت اشخاص، به شرط آنکه محتوای داده‌پیام موافق قوانین مصوب مجلس باشد، تابع شرایط زیر قرار داده است:

الف) اهداف آن مشخص باشد و به‌طور واضح شرح داده شده باشند.

ب) داده‌پیام باید فقط به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع داده‌پیام شرح داده شده جمع‌آوری شود و فقط برای اهداف تعیین‌شده به کار رود.

ج) داده‌پیام باید صحیح و روزآمد باشد.

د) شخص موضوع داده‌پیام باید به پرونده‌های رایانه‌ای حاوی داده‌پیام‌های شخصی مربوط به خود دسترسی داشته و بتواند داده‌پیام‌های ناقص یا نادرست را محو یا اصلاح کند.

ه) شخص موضوع داده‌پیام باید بتواند در هر زمان، با رعایت ضوابط مربوطه، محو کامل پرونده رایانه‌ای داده‌پیام شخصی مربوط به خود را درخواست کند.

مواد ۷۱ تا ۷۳ این قانون نیز برای اشخاصی که مواد ۵۸ و ۵۹ را نقض کنند، مجازات تعیین کرده‌اند (قناد و علیقلی، ۱۳۹۹).

بنابراین، می‌توان گفت پیامک‌ها تنها در صورتی می‌توانند مورد استناد قضایی قرار گیرند که به‌صورت قانونی و مشروع تحصیل شده باشند و فرآیند گردآوری آن‌ها، متضمن نقض حریم خصوصی فرد مقابل نباشد. دسترسی غیرمجاز به این نوع داده‌ها نه‌تنها از منظر کیفری قابل پیگرد است، بلکه موجب بی‌اعتباری دلیل در فرآیند دادرسی خواهد شد. افزون بر مشروعیت در تحصیل دلیل، رعایت اصل تناسب و ضرورت نیز در استفاده از محتوای پیام‌ها اهمیت دارد؛ بدین معنا که طرف دعوا نمی‌تواند بی‌ضابطه و گسترده به پیامک‌های طرف مقابل استناد کند، بلکه باید تنها در حدودی که برای اثبات ادعای خود در پرونده لازم است، این اطلاعات را به دادگاه ارائه نماید.

آنچه بدیهی است این است که قوانین موجود در حوزه‌ی حفاظت از داده‌ها در ایران از جامعیت و شفافیت لازم برخوردار نیستند و همین امر موجب بروز ابهام در فرآیند اجرای آن‌ها شده است. برای رفع این مشکل، ضروری است که قوانین فعلی مورد بازنگری قرار گرفته و با دقت و جامعیت بیشتری تدوین شوند. این بازنگری باید به گونه‌ای صورت گیرد که تمامی ابعاد مرتبط با حفاظت از داده‌ها از قبیل شفافیت، رضایت، اطلاع‌رسانی و حفاظت از داده‌ها را پوشش داده و به طور روشن و صریح نحوه‌ی اجرای مقررات را تبیین کند (پرچینی و همکاران، ۱۴۰۳).

در چنین بستری رویکرد قضایی به پیامک‌ها باید بر پایه موازنه میان حقوق طرف دعوا برای ارائه دلیل و حقوق طرف مقابل در حفظ حریم خصوصی استوار باشد. این موازنه مستلزم آن است که مداخله در حریم خصوصی ارتباطاتی تنها با مجوز قانونی، با

رعایت اصل تناسب، و در جهت تحقق دادرسی منصفانه صورت گیرد. این امر، به‌ویژه در دعاوی خانوادگی که معمولاً با روابط عاطفی، مسائل شخصی و اطلاعات حساس همراه‌اند، از اهمیت مضاعفی برخوردار است.

۵. کاربرد پیام‌های شبکه‌های اجتماعی در دعاوی خانوادگی

با توجه به نقش فزاینده شبکه‌های اجتماعی در شکل‌دهی به روابط انسانی، دادگاه‌ها ناگزیر با پیام‌ها و محتوای رد و بدل‌شده در این بسترها به‌عنوان یکی از ادله ممکن در پرونده‌های خانوادگی مواجه شده‌اند. در نظام دادرسی ایران، هرچند قواعد مشخصی در خصوص نحوه استفاده از این‌گونه داده‌ها وجود ندارد، اما در عمل، طرفین دعاوی خانوادگی، به‌ویژه در پرونده‌های مربوط به طلاق، حضانت، نفقه و تمکین به پیام‌های رد و بدل شده بین خود استناد می‌نمایند. این بخش از مقاله با هدف بررسی مصادیق و شیوه‌های کاربرد پیام‌های شبکه‌های اجتماعی در دعاوی خانوادگی، به تحلیل جایگاه این ادله در فرآیند اثبات و ارزیابی قضایی خواهد پرداخت.

یکی از نمونه‌های قابل توجه در تأیید قابلیت استناد به پیام‌ها در دعاوی خانوادگی، رأی صادره از دیوان عالی کشور در پرونده‌ای است که زوجه (پ. ق.) با استناد به پیامک‌های توهین‌آمیز زوج، تعهدات محضری و استشهادیه‌های محلی، تقاضای طلاق به دلیل عسر و حرج نموده بود.[۱] اگرچه دادگاه بدوی و تجدیدنظر در ابتدا دعوی زوجه را رد کردند، اما دیوان عالی کشور با بررسی جامع مدارک از جمله مفاد پیامک‌های ارسالی که حاوی توهین و تحقیر مستمر زوج بود، این دلایل را از مصادیق عسر و حرج دانست.

این رأی علاوه بر آنکه جایگاه ادله الکترونیکی مانند پیامک را در دعاوی خانوادگی تقویت می‌کند، نشان‌دهنده تغییر نگرش قضایی نسبت به داده‌های الکترونیکی می‌باشد. هرچند دادگاه‌های بدوی و تجدیدنظر به مفاد پیام‌های ارائه‌شده توجهی نکرده بودند، اما دیوان عالی کشور در رأی خود به مؤثر بودن استناد به پیام‌ها تأکید کرد.

در پرونده‌ای دیگر با محکوم‌علیه «ع. ع.»، دادگاه به استناد پیامک‌هایی حاوی توهین و تهدید که محکوم علیه در جریان اختلاف خانوادگی برای همسرش ارسال کرده بود، وی را به اتهام توهین، افتراء و تهدید نسبت به پدرِ همسر و باجناق وی محکوم کرد. هر یک از این افراد، به طور جداگانه و در زمان‌های متفاوت، با ارائه پیامک موردنظر شکایت کرده‌اند و برای هر شکایت نیز حکمی جداگانه صادر شده است.[۲] محکوم‌علیه با استناد به قاعده منع محاکمه و مجازات مجدد (اصل اعتبار امر مختوم)، مدعی شد که همه شکایت‌ها ناشی از یک پیام واحد بوده و نباید چندبار بابت آن محکوم شود. بنابراین در دیوان عالی کشور درخواست اعاده دادرسی کرد. اما دیوان عالی کشور در رأی خود تصریح نمود که حتی اگر توهین و تهدید در قالب یک پیام واحد صورت گرفته باشد، هر یک از افراد توهین‌شده دارای شخصیت مستقل حقوقی هستند و حق شکایت جداگانه دارند؛ بنابراین صدور چند حکم محکومیت بابت همان پیام، با اصول دادرسی کیفری مغایرت ندارد .

پیامک ارسال‌شده از سوی زوج (محکوم‌علیه) به همسر، در این پرونده به‌عنوان دلیل کیفری معتبر مورد پذیرش قرار گرفته و بر مبنای آن، شکایات جداگانه مطرح شده است و در هر مورد، دادگاه حکم محکومیت جداگانه صادر کرده است. این نشان می‌دهد که ارائه و پذیرش این پیامک به دادگاه صرفاً وسیله اطلاع‌رسانی نبوده بلکه قابلیت استناد به عنوان دلیل داشته و مبنای صدور حکم قطعی قرار گرفته است .

---

[۱] رأی دیوان عالی کشور، شماره دادنامه 1.4000639000057061E+17مورخ۱۴۰۰.۰۸.۰۹ با عنوان احراز عسروحرج زوجه به دلیل کراهت، منتشر شده در سایت ارای رویه قضایی به نشانی https://ara.jri.ac.ir/Judge/Text/36710

[۲] رأی دیوان عالی کشور، شماره دادنامه 140106390000610191 مورخ۱۴۰۱.۰۸.۲۱ با عنوان توهین از طریق ارسال پیامک، منتشر شده در سایت ارای رویه قضایی به نشانیhttps://ara.jri.ac.ir/Judge/Text/36807

در ادامه می‌توان به پرونده‌ای دیگر استناد کرد که در آن زوج (س.ا.ف.ا.) با استناد به اختلافات شدید و ترک منزل مشترک، درخواست صدور گواهی عدم امکان سازش به طرفیت زوجه (م.ا.ف.ا.) مطرح کرد.[۱] دادگاه بدوی نیز با احراز رابطه زوجیت، عدم توفیق در سازش و با استناد به ماده ۱۱۳۳ قانون مدنی، گواهی عدم امکان سازش صادر نمود. زوجه از طریق وکیل خود نسبت به رأی صادره اعتراض کرد و خواهان دریافت نحله و اعمال شرط تنصیف دارایی شد، اما دادگاه تجدیدنظر با استناد به شهادت شهود و پیامک‌هایی که زوج مبنی بر سوءرفتار زوجه ارائه کرده بود و همچنین نظریه پزشکی قانونی مبنی بر ابتلای زوجه به افسردگی، سوءمعاشرت زوجه را احراز و اعتراض را رد کرد. با این حال، دیوان عالی کشور با پذیرش فرجام‌خواهی زوجه، اعلام داشت که دلایل موجود اعم از شهادت شهود، پیامک‌ها و نظریه پزشکی قانونی برای اثبات سوءرفتار زوجه در حدی که موجب سقوط حقوق مالی وی شود، کافی نبوده و صرف ابتلا به افسردگی خفیف قابل درمان، نمی‌تواند نافی حقوق اکتسابی وی پس از سی سال زندگی مشترک باشد. بر این اساس، دادنامه نقض و پرونده جهت رسیدگی مجدد به شعبه هم‌عرض ارجاع شد .

در این پرونده، یکی از مستندات زوج برای اثبات سوءمعاشرت زوجه که ناظر به سقوط حقوق مالی وی از جمله نحله و شرط تنصیف دارایی بود، پرینت پیامک‌های ارسالی از سوی زوجه به وی بود. این پیام‌ها از سوی دادگاه بدوی و سپس تجدیدنظر، به‌عنوان بخشی از امارات و قرائن مؤید ادعای زوج مورد پذیرش قرار گرفتند. دادگاه تجدیدنظر، با استناد به پیامک‌ها و شهادت شهود، نتیجه گرفت که زوجه سوءرفتار داشته و از این جهت مستحق دریافت حقوق مالی موضوع ماده واحده قانون اصلاح مقررات مربوط به طلاق نیست. با این حال، دیوان عالی کشور در مرحله فرجام‌خواهی، این استناد را مورد خدشه قرار داد و تصریح کرد که پیام‌ها مربوط به پس از طرح دعوای طلاق هستند، بنابراین نمی‌توانند دلیل سوءمعاشرت پیش از دعوا که شرط اسقاط حقوق مالی زوجه است تلقی شوند.

بدین ترتیب، در صورت احراز انتساب، پیامک‌ها می‌توانند به‌عنوان دلیل در دعاوی خانوادگی مورد پذیرش و استناد دادگاه قرار گیرند. با این حال، در خصوص پیام‌های مبادله‌شده از طریق سکوهای اینترنتی، به‌ویژه پیام‌رسان‌های خارجی مانند واتساپ و تلگرام، همچنان تردیدهایی وجود دارد و رویه قضایی در این زمینه یکدست و منسجم نیست. نبود مقررات صریح و روشن، چالش‌های مرتبط با احراز هویت و اصالت داده‌ها، و تفاوت دسترسی به زیرساخت‌های فنی موجب شده است قضات در پذیرش چنین مستنداتی رویکردهای گوناگونی در پیش بگیرند. از این‌رو، تدوین دستورالعمل‌های اجرایی توسط قوه قضاییه یا تصویب مقررات خاص در حوزه ادله دیجیتال، می‌تواند نقش مهمی در یکپارچگی رویه و ارتقای اعتماد قضایی ایفا کند.

۶. جایگاه و چالش‌های پذیرش شواهد الکترونیکی در نظام‌های حقوقی مختلف

اعتبار و پذیرش ادله الکترونیکی در هر نظام حقوقی، تابع اصول بنیادین آن نظام است. در نظام‌های حقوقی رومی–ژرمنی، اصل آزادی در تحصیل و ارزیابی دلایل حاکم است و دادگاه‌ها می‌توانند انواع مختلف ادله، از جمله ادله الکترونیکی را بررسی کرده و درباره ارزش و اعتبار آن‌ها تصمیم‌گیری کنند. در مقابل، در نظام کامن‌لا که بر رسیدگی شفاهی و تقابل طرفین مبتنی است، محدودیت‌های بیشتری در پذیرش اسناد الکترونیکی وجود دارد و چالش‌هایی جدی درباره قابلیت استماع آن‌ها مطرح شده است (دهقانی، فلاح و هاشمی، ۱۴۰۱).

[۱] رأی دیوان عالی کشور، شماره دادنامه 1400639000060905 مورخ۱۴۰۰.۰۸.۲۵ با عنوان تاثیر افسردگی زوجه بر اسقاط حقوق مالی وی، منتشر شده در سایت ارای رویه قضایی به نشانی https://ara.jri.ac.ir/Judge/Text/38614

رویه قضایی انگلستان نشان می‌دهد که دادگاه‌ها در عمل، انواع شواهد الکترونیکی مانند صدا، تصویر و داده‌های الکترونیکی را به‌عنوان دلیل می‌پذیرند. نمونه بارز این رویکرد در پرونده «دولت علیه رابسون، میچل و ریچاردز»[1] دیده می‌شود؛ در این پرونده، پرینت تماس‌های یک تلفن همراه به‌عنوان دلیل ارائه شد. دفاعیه آن را مشمول قاعده «شایعات[2]» دانست، اما قاضی این استدلال را نپذیرفت و اظهار داشت:«هرگاه یک ماشین، واقعیتی را مشاهده و ثبت کند، آن ثبت، خود یک واقعیت است و می‌تواند به‌عنوان مدرک مورد استناد قرار گیرد.»(میسون و سنگ، ۲۰۱۷: ۴۳)

در پرونده «دولت علیه دی (آرتور جان)»[3] نیز، قاضی با تأکید بر تفسیر موسع مفهوم سند بیان داشت: «به نظر من، هر چیز نوشتاری که قابلیت استناد به‌عنوان دلیل داشته باشد، به‌درستی می‌توان سند نامید؛ و اهمیتی ندارد که این نوشته بر روی چه چیزی نگاشته شده باشد. ممکن است به جای کاغذ، بر روی پوست، سنگ، مرمر، گل یا حتی فلز حک شده باشد. بنابراین، با این استدلال که سند تنها در صورتی سند است که روی کاغذ نوشته شده باشد، مخالفم. به اعتقاد من، هر نوشته یا متن چاپی که قابلیت استناد داشته باشد، صرف‌نظر از ماده نگارش، سند محسوب می‌شود.»(میسون و سنگ، ۲۰۱۷: ۴۴)

با این حال، صرف پذیرش ظاهر یک سند الکترونیکی کافی نیست. همانند سایر اسناد، احراز اصالت برای ادله الکترونیکی نیز ضروری است؛ ولی این فرایند به‌مراتب حساس‌تر و پیچیده‌تر است، چراکه داده‌های دیجیتال مستعد بروز خطاهای فنی، تغییرات ناخواسته یا دستکاری عمدی هستند. بنابراین، طرفی که به سند دیجیتال استناد می‌کند، باید اصالت و یکپارچگی آن را اثبات نماید؛ حتی اگر این امر هزینه‌بر یا نیازمند تخصص فنی باشد. این الزام، بنیانی برای تضمین عدالت دادرسی و حفظ اعتبار اسناد الکترونیکی به‌شمار می‌رود (میسون و سنگ، ۲۰۱۷: ۴۸).

در همین راستا، در انگلستان دادگاه‌های حقوقی اختیار گسترده‌ای در مدیریت نحوه ارائه ادله دارند. مطابق با مقررات آیین دادرسی مدنی انگلستان[4]، دادگاه‌های حقوقی می‌توانند مشخص کنند که:

الف) کدام مسائل نیاز به دلیل دارند،

ب) چه نوع دلایلی برای اثبات آن‌ها لازم است،و

ج) این ادله به چه نحوی باید ارائه شوند.

همچنین، حتی اگر دلیل ارائه‌شده در ظاهر قابل پذیرش باشد، این دادگاه‌ها می‌توانند آن را رد کنند؛ البته این اختیار باید با دقت بسیار و صرفاً در جهت تحقق هدف نهایی دادرسی منصفانه اعمال گردد. همان‌گونه که پروفسور تاپر بیان کرده است: «دادگاه‌ها باید به‌جای هراس از پذیرش ادله، آن‌ها را بپذیرند و سپس درباره وزن و ارزش استنادی آن تصمیم‌گیری کنند. (میسون و سنگ، ۲۰۱۷: ۵۸)

در ایالات متحده آمریکا، با توجه به گسترش فناوری اطلاعات و نگرانی‌های جدی نسبت به نقض حریم خصوصی در فضای دیجیتال، پذیرش شواهد الکترونیکی مستلزم احراز سه شرط اصلی است:

الف) نقض حریم خصوصی شخصی صورت نگرفته باشد،

ب) ارتباط معناداری با دعوا داشته باشد،

ج) به‌طور غیرقانونی تحصیل نشده باشد (کاناوان و کولستاد، ۲۰۱۶).

---

[1] R v Robson, Mitchell and Richards
[2] Hearsay
[3] R v Daye (Arthur John)
[4] Civil Procedure Rules

بنابراین، شواهد الکترونیکی و پیام‌های شبکه‌های اجتماعی در ایالات متحده زمانی پذیرفته می‌شوند که این سه شرط رعایت شده باشند. در این راستا، قانون حریم خصوصی ارتباطات الکترونیکی *(ECPA)*[1] که در سال ۱۹۸۶ تصویب شده است، به‌عنوان سند قانونی اصلی در حفاظت از حریم خصوصی شناخته می‌شود و قواعد خاصی برای دسترسی به شواهد الکترونیکی را تعیین کرده است. این قانون، فعالیت‌های نهادها و افراد در زمینه انتقال اطلاعات الکترونیکی را تنظیم کرده و در عین حال به مقامات دولتی تنها در صورت دریافت مجوز قضایی، امکان دسترسی به این اطلاعات را می‌دهد (صادقی، ۱۳۹۶: ۱۲۸).

با وجود وضع قوانین مختلف در راستای حمایت از حریم خصوصی افراد، هنوز هم چالش‌هایی در تشخیص نقض آن در دادگاه‌ها وجود دارد. نمونه‌ای از این چالش‌ها در پرونده‌ای صادره از دیوان عالی کارولینای جنوبی در سال ۲۰۱۲ میان زوجین جنینگز مطرح شد.[2] در این پرونده، زوجه با دسترسی غیرمجاز به ایمیل همسر خود (از طریق پاسخ به سؤالات امنیتی) مکاتبات او با شخص ثالث را به‌دست آورده و در جریان دعوای طلاق به آن‌ها استناد کرده بود. به همین دلیل، شوهر علیه او به دلیل دسترسی غیرمجاز به ایمیل شکایت کرد. در مرحله بدوی، دادگاه حکم به بی‌ارتباط بودن قانون ارتباطات *ذخیره‌شده* (SCA[3]) *با* این موضوع داد و اقدام زوجه را غیرمجاز تشخیص نداد. هرچند دادگاه تجدیدنظر رأی را نقض کرد و زوجه را مشمول احکام قانون مذکور دانست، اما دیوان عالی ایالت کارولینای جنوبی در نهایت اعلام کرد که ایمیل‌هایی که قبلاً باز شده‌اند و تنها نسخه‌ای از آن‌ها در سرور باقی مانده است، مشمول تعریف «ذخیره‌سازی پشتیبان» در قانون ارتباطات ذخیره شده نیستند و بنابراین، دسترسی به آن‌ها نقض این قانون محسوب نمی‌شود. در نتیجه، زوجه از اتهامات تبرئه شد.

در پرونده‌ای دیگر در دادگاه عالی نیوجرسی نیز رایی مشابه با رأی قبلی صادر شد. در این پرونده که بین زوجین وایت جریان داشت، زوج (شاکی) مدعی شد زوجه بدون اجازه به حساب ایمیل او دسترسی پیدا کرده و مکاتبات خصوصی او با یک زن دیگر را به عنوان مدرک در فرایند طلاق مورد استفاده قرار داده است.[4] رایانه‌ای که ایمیل‌ها در آن ذخیره شده بود در «اتاق آفتاب» محل سکونت مشترک طرفین قرار داشت؛ اتاقی که فرزندان و همسر نیز به طور مرتب از آن استفاده می‌کردند و مسیر دسترسی به فضاهای عمومی خانه نیز از آن عبور می‌کرد. دادگاه در رأی خود تصریح کرد که معیار نقض حریم خصوصی نه باور ذهنی افراد، بلکه انتظار عقلانی و معقول از محرمانه بودن فضا یا اطلاعات است. در این مورد، با توجه به اینکه رایانه در محل سکونتی مشترک و قابل دسترس برای تمام اعضای خانواده قرار داشت، انتظار شاکی از محرمانه بودن اطلاعات در آن فضا ناموجه تلقی شد. به بیان دیگر، صرف نگهداری ایمیل‌ها در دستگاهی که در فضای مشترک قرار دارد، حریم خصوصی را تضمین نمی‌کند و دسترسی زوجه به فایل‌ها در رایانه، مشابه جست‌وجو در فایل‌کابینت قفل‌نشده است و نقض قانون استراق سمع یا حقوق عرفی محسوب نمی‌شود.

بنابراین، در نظام‌های حقوقی مختلف تلاش بر این است که ادله الکترونیکی، از جمله پیام‌های شبکه‌های اجتماعی، پس از انجام فرآیند احراز اصالت، به‌عنوان اسناد قابل استناد پذیرفته شوند. در بسیاری از پرونده‌ها، این ادله ممکن است ارزشی برابر با سایر ادله قانونی داشته باشند. با این حال، چالش اصلی در پذیرش این نوع شواهد، مسئله حریم خصوصی است که همچنان موضوع بحث‌های گسترده و پیچیده‌ای می‌باشد. پذیرش این ادله به‌ویژه به ارزیابی قضات و تفسیر آن‌ها از مقوله حریم خصوصی بستگی دارد. در اغلب موارد، در صورتی که روش دسترسی به شواهد به‌صورت غیرمجاز صورت نگرفته باشد، این دسترسی به‌عنوان نقض حریم خصوصی تلقی نمی‌شود و بر اساس آن، حکم قضایی صادر می‌شود.

---

[1] Electronic Communications Privacy Act
[2] Jennings v. Jennings, 697 S.E.2d 671 (S.C. Ct. App. 2010).
[3] Stored Communications Act
[4] White v. White (781 A.2d 85, 344 N.J. Super. 211)

بحث

نتایج این پژوهش نشان می‌دهد که استفاده از پیام‌های موجود در فضای مجازی در دعاوی خانوادگی می‌تواند به‌عنوان دلیل قابل استناد در دادگاه پذیرفته شود. این یافته با نتایج پژوهش‌های رحیمی و طاهری‌پور (۱۳۹۸) هم‌خوان است؛ آن دو نیز بر ارزش اثباتی پیامک‌ها تأکید کرده و شرط پذیرش آن‌ها را اقناع وجدان قاضی دانسته‌اند. با این حال، برخلاف نظر میرشکاری و علائی (۱۳۹۹) که پیام‌های ارسال‌شده در فضای مجازی را فاقد اصالت می‌دانند، در این پژوهش با استفاده از معیارهای احراز اصالت دیجیتال، پیامک‌ها معتبر ارزیابی شدند. این تفاوت احتمالاً ناشی از نوظهور بودن این نوع ادله و عدم شکل‌گیری رویه‌ای منسجم در این زمینه است. با این حال، نظام قضایی باید همگام با تحولات عصر دیجیتال حرکت کند و از مقتضیات آن عقب نماند. در عصری که بخش عمده‌ای از ارتباطات میان افراد از طریق پیام‌رسان‌ها صورت می‌گیرد، آنچه با عدالت قضایی سازگار است، پذیرش این نوع پیام‌ها به‌عنوان دلیل، با در نظر گرفتن معیارهای فنی و حقوقی است. بنابراین، می‌توان گفت که ارزش اثباتی پیامک‌ها در حقوق خانواده ایران، به‌تدریج در حال پذیرش گسترده‌تر و تثبیت‌شده‌تری است.

نتیجه‌گیری

در عصر حاضر، با گسترش روزافزون اینترنت و کاهش هزینه‌های ارتباطی، بخش عمده‌ای از تعاملات میان افراد از طریق سکوهای دیجیتال صورت می‌گیرد. از این‌رو، نمی‌توان نسبت به محتوای پیام‌های رد و بدل‌شده در این فضا بی‌تفاوت بود؛ چراکه نادیده گرفتن آن‌ها در تعارض با ضرورت‌های حفظ حقوق اشخاص قرار دارد. این تحولات، لزوم اصلاح و بازاندیشی در رویه‌های قضایی موجود را اجتناب‌ناپذیر ساخته است تا بدین وسیله، حمایت مؤثری از حقوق افراد در بستر دیجیتال فراهم آید.

گسترش فناوری اطلاعات و نفوذ پیام‌رسان‌های دیجیتال در زندگی روزمره، موجب تحول در مفاهیم سنتی ادله اثبات دعوا شده است. در حال حاضر، دلایلی همچون اقرار، سند یا حتی شهادت، صرفاً در قالب کاغذ یا بیان لفظی مطرح نمی‌شوند، بلکه ممکن است در قالب پیام‌هایی در تلگرام، واتساپ یا دیگر پیام‌رسان‌ها نیز محقق شوند. این امر در دعاوی خانوادگی، که عمدتاً بر پایه تعاملات مستقیم و شواهد ارتباطی میان زوجین استوارند، نمود بیشتری دارد.

در عمل، بسیاری از اختلافات خانوادگی از دل همین ارتباطات دیجیتال شکل می‌گیرند؛ مانند پیام‌هایی حاوی تهدید، اقرار به خشونت خانگی، عدم تمایل به ادامه زندگی مشترک، اذعان به روابط خارج از چارچوب زناشویی، یا توافق ضمنی بر طلاق و حضانت فرزند. در صورتی که چنین پیام‌هایی به لحاظ فنی قابل انتساب به شخص معین باشند و از نظر محتوایی دلالت حقوقی داشته باشند، می‌توانند در کنار ادله سنتی مورد استناد قرار گیرند. به عنوان نمونه، پیامکی که در آن زوج به ترک انفاق یا اعمال خشونت اذعان کرده باشد، می‌تواند به‌مثابه اقرار قلمداد شده و در راستای اثبات عسر و حرج زوجه مؤثر واقع شود.

با این حال، چالش اصلی در این زمینه، فقدان رویه قضایی شفاف و منسجم درباره نحوه استناد به این پیام‌ها در محاکم خانواده است. در شرایط فعلی، ارزیابی و پذیرش چنین دلایلی تا حد زیادی به نظر شخصی قاضی بستگی دارد. در حالی که برخی قضات ممکن است آن‌ها را صرفاً اماراتی ضعیف تلقی کنند، برخی دیگر ارزش اثباتی چندانی برای آن‌ها قائل نیستند؛ به‌ویژه در صورتی که احتمال جعل، دستکاری یا تردید در انتساب پیام وجود داشته باشد.

از منظر فنی، پیام‌های دیجیتال قابلیت‌هایی دارند که در صورت بررسی دقیق می‌توانند به تقویت اعتبار آن‌ها منجر شوند؛ اطلاعاتی مانند شماره تلفن، زمان ارسال، نوع دستگاه، IP، و هشدارهای امنیتی ورود به حساب کاربری. تطبیق این عناصر می‌تواند به احراز هویت فرستنده و انتساب پیام به وی کمک شایانی کند. به‌عنوان مثال، اگر زوجه مدعی دریافت پیام تهدیدآمیز از سوی همسرش باشد و این پیام هم‌زمان با هشدار ورود به حساب کاربری از دستگاه ثبت‌شده زوج در مکان و زمان معین دریافت شده باشد، می‌توان این مجموعه را به‌عنوان زنجیره‌ای از دلایل مؤید به دادگاه ارائه کرد.

با وجود این قابلیت‌ها، دادگاه‌ها در مواردی پیام‌هایی با محتوای اقرار یا توافق را در حد اماره قضایی دانسته‌اند، حال آن‌که از حیث منطقی و محتوایی، چنین پیام‌هایی می‌توانند بسیار فراتر از یک اماره ضعیف تلقی شوند. این رویکرد می‌تواند به تضییع حقوق طرفین، به‌ویژه در شرایطی که دسترسی به دلایل سنتی ممکن نیست، منجر شود. از این‌رو، به نظر می‌رسد بازنگری در رویکرد قضایی، متناسب با تحولات حقوق تطبیقی و قوانین نوینی مانند قانون تجارت الکترونیکی ایران، ضرورتی انکارناپذیر است.

در همین راستا، تدوین آیین‌نامه‌ای مشخص برای تعیین ضوابط پذیرش پیام‌های الکترونیکی در دعاوی خانواده، می‌تواند راهگشا باشد. این آیین‌نامه باید به‌صراحت بیان کند که در چه شرایطی پیام‌ها می‌توانند در جایگاه اقرار، سند عادی یا دلیل مستقل قرار گیرند و همچنین تدابیری برای احراز هویت دیجیتال و همکاری میان محاکم، کارشناسان فناوری اطلاعات و در صورت لزوم، ارائه‌دهندگان خدمات پیام‌رسان پیش‌بینی کند.

با این حال، نباید از اهمیت مشروعیت تحصیل دلیل و موازنه با حریم خصوصی غافل شد. پیامک‌ها تنها در صورتی می‌توانند مورد استناد قرار گیرند که به‌صورت قانونی و مشروع به‌دست آمده باشند و فرایند گردآوری آن‌ها متضمن نقض حریم خصوصی نباشد. دسترسی غیرمجاز به این اطلاعات، نه‌تنها می‌تواند از منظر کیفری پیگرد داشته باشد، بلکه موجب سلب اعتبار دلیل نیز خواهد شد. افزون بر این، رعایت اصل تناسب نیز حائز اهمیت است؛ بدین معنا که طرف دعوا تنها در حد ضرورت و متناسب با موضوع اختلاف، مجاز به ارائه پیام‌های دیجیتال در دادگاه است.

در نتیجه، رویکرد قضایی به استناد به پیامک‌ها باید بر پایه موازنه‌ای دقیق میان حق دسترسی به دلیل و حفظ حریم خصوصی افراد استوار باشد؛ به‌ویژه در دعاوی خانوادگی که اطلاعات مطرح‌شده اغلب جنبه شخصی و حساس دارند. این موازنه باید با رعایت اصول قانونی، تناسب، و ضرورت و در راستای دادرسی منصفانه صورت پذیرد.

در نهایت، پیام‌های دیجیتال در دادرسی‌های خانوادگی نباید صرفاً در حد یک اماره باقی بمانند. اگر این پیام‌ها از نظر محتوایی دارای دلالت حقوقی روشن و از نظر فنی قابل انتساب به شخص مشخصی باشند، باید به‌عنوان ادله مستقل و معتبر مورد پذیرش قرار گیرند. چنین تحولی نه‌تنها با الزامات حقوقی روز هم‌راستا است، بلکه می‌تواند به تحکیم عدالت و حمایت مؤثرتر از آسیب‌دیدگان، به‌ویژه قربانیان خشونت خانگی، بینجامد.

ملاحظات اخلاقی

پیروی از اصول اخلاق پژوهش

نویسندگان اصول اخلاقی را در انجام و انتشار این پژوهش علمی رعایت نموده‌اند و این موضوع مورد تأیید همه آنهاست.

تعارض منافع

بنا بر اظهار نویسندگان این مقاله تعارض منافع ندارد.

سپاسگزاری

از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.

منابع

السان، مصطفی؛ منوچهری، محمدرضا (۱۳۹۷). *ارزیابی اصالت ادله الکترونیکی و ارزش اثباتی آنها. مجله مطالعات حقوقی دانشگاه شیراز*، ۱۰(۲)، ۲۹-۵۱.

امیدی، مهدی؛ صفایی شهراسب، زهرا (۱۴۰۱). *اعتبار اسناد الکترونیک در دعاوی خانواده. نشریه مطالعات فقه و حقوق رسانه دانشکده رفاه*، ۴(۲)، ۱۱۱-۱۲۷.

انصاری، باقر (۱۳۸۷). *حقوق ارتباط جمعی*. تهران: سمت.

بابازاده مقدم، حامد و خدری، نجمه (۱۴۰۱). *دسترسی به اینترنت به عنوان یک حق بنیادین جدید. فصلنامه علوم خبری*، ۱۱(۱) ، ۷۳-۱۱۶.

تلگرام، «*افزودن کنترل نشست‌ها و تأیید هویت دو مرحله‌ای*»، منتشر شده در ۱۹ دسامبر ۲۰۱۳، در دسترس در: *https://telegram.org/blog/sessions-and-2-step-verification*(تاریخ مراجعه: ۲۷ ژوئیه ۲۰۲۵)

حبیب زاده، طاهر (۱۳۹۶). *حقوق فناوری اطلاعات، ادله الکترونیکی، اسناد الکترونیکی و امضای الکترونیکی*. چاپ اول. تهران: نشر میزان.

حیدری نژاد، نصرت‌اله (۱۳۹۶). *بررسی حقوقی ادله الکترونیکی در نظام کنونی*. فصلنامه علمی-حقوقی قانون یار، ۳، ۱۲۵-۱۴۰.

درزبان رستمی، حسن و بهزادی پور، فرزانه (۱۳۹۸). *نقش شبکه‌های اجتماعی در ارتقاء احساس امنیت اجتماعی با استفاده از نظر نخبگان و کارشناسان مرکز ملی فضای مجازی. فصلنامه علوم خبری*، ۸(۲) ، ۲۴۷-۲۶۸

دوبلفون، زویه لیان (۱۳۹۰). *حقوق تجارت الکترونیک*. چاپ دوم. ترجمه ستار زرکلام. تهران: مؤسسه مطالعات و پژوهش‌های حقوقی شهر دانش.

ربانی موسویان، علی؛ نعیمی، طاهره (۱۳۹۸). *مستندسازی بر اساس ادله سنتی و متجدد الکترونیکی و آثار آن در نظام قضایی. فصلنامه قضاوت*، ۱۰۰، ۱۵۷-۱۷۹.

رحیمی، زهرا؛ طاهری پور، زهرا (۱۳۹۸). *اعتبار اسناد الکترونیک به عنوان ادله اثبات دعوا در دعاوی زوجین. دو فصلنامه علمی مطالعات فقه و حقوق رسانه دانشکده رفاه*، ۱(۱)، ۵۱-۷۴.

شرکت بامسئولیت محدود *ESeye* (۲۰۲۳). *راهنمای توسعه‌دهنده رابط برنامه‌نویسی پیامک* (شماره سند ۸۲۹۷، نسخه ۱.۳). بازیابی‌شده در تاریخ ۱۰ مرداد ۱۴۰۴ از: *8297 SMS API Developer Guide*

شهبازی نیا، مرتضی؛ عبدالهی، محبوبه (۱۳۸۸). *احراز اصالت در اسناد الکترونیک. پژوهش‌های حقوق تطبیقی (مدرس)*، ۱۳(۴)، ۱۲۵-۱۴۱.

صادقی، حسین (۱۳۹۶). *مسئولیت مدنی در ارتباطات الکترونیک*. چاپ دوم. تهران: نشر میزان.

قناد، فاطمه؛ علیقلی، امیره (۱۳۹۹). *مفهوم و اهمیت داده‌های شخصی و حریم خصوصی و انواع حمایت از آن در فضای مجازی. دوفصلنامه حقوق قراردادها و فناوری های نوین*،۱(۱)، ۲۹۷-۳۲۲.

کاناوان، مارسیا؛ کولستاد، اوا (۲۰۱۶). *آیا استفاده از ادله رسانه‌های اجتماعی در دعاوی خانواده اهمیت دارد؟ دوماهنامه ویتی‌یر برای حمایت از کودکان و خانواده*. بازیابی‌شده در تاریخ ۱۰ مرداد ۱۴۰۴ از: *Canavan-article.pdf*

گروه کاری شبکه، لیچ، پی؛ میلینگ، ام؛ سالز، آر (۲۰۰۵). *شناسه یکتا در فضای جهانی: نام* URN، RFC 4122. *سازمان* IETF. بازیابی‌شده در تاریخ ۱۰ مرداد ۱۴۰۴ از: *https://tools.ietf.org/html/rfc4122*

مارکرت، فیلیپ؛ لاساک، لیونا؛ گولا، ماکسیمیلیان؛ دورموت، مارکوس (۲۰۲۴). *درک تعامل کاربران با اعلان‌های ورود*. مجموعه مقالات کنفرانس *CHI* درباره عوامل انسانی در سامانه‌های رایانشی، ۱-۱۴.

محمودی پرچینی، مرتضی؛ ریاضی، لادن؛ پور ابراهیمی، علیرضا و امین موسوی، سید عبداله (۱۴۰۳). *مقایسه قوانین حفاظت از داده‌های شخصی: مقررات عمومی منحصر به فرد تحت مقررات حفاظت از داده‌های عمومی اتحادیه اروپا (*GDPR*) و قوانین ایالات متحده. فصلنامه علوم خبری*، ۱۳(۴) ، ۲۰۴-۲۲۴.

میرشکاری، عباس؛ علائی، صابر (۱۳۹۹). *ماهیت اثباتی داده‌پیام‌های الکترونیکی به عنوان ادله اثبات دعوا. فصلنامه تحقیقات حقوقی*، شماره ۹۶، ۳۰۱-۳۲۶.

میسون، استیفن؛ سنگ، دانیل (ویراستاران) (۲۰۱۷). *ادله الکترونیکی* (چاپ چهارم). مؤسسه مطالعات عالی حقوقی، مدرسه مطالعات عالی، دانشگاه لندن.

مؤسسه ملی استاندارد و فناوری آمریکا (۲۰۱۷). *راهنمای هویت دیجیتال: احراز هویت و مدیریت چرخه زندگی* ، بازیابی شده در تاریخ ۱۰ مرداد از: *NIST Special Publication 800-63B*

References

Ansari, B. (2008). *The Law of Mass Communication*. Tehran: SAMT. (In Persian)

Babazadeh Moghaddam, H. & Khedri, N. (2022). *Internet Access as a New Fundamental Right*. *News Science Quarterly (NS)*, 11(1), 73-116. (In Persian)

Canavan, M., & Kolstad, E. (2016). *Does the Use of Social Media Evidence in Family Law Litigation Matter? Whittier Journal of Child and Family Advocacy*. Retrieved from Canavan-article.pdf

Darzyan Rostami, H. and Behzadpour, F. (2019). *The Role of Social Media in Promoting Social Security Using Elite Experts and National Cyberspace Experts. News Science Quarterly* (NS), 8(2), 247-268. (In Persian)

du Belfon, Z. L. (2011). *Electronic Commercial Law* (2nd ed., S. Zarghalam, Trans.). Tehran: Shahre Danesh Institute of Legal Studies and Research. (In Persian)

Elsan, M., & Manouchehri, M. R. (2018). *A Survey on Authenticity and Admissibility of Electronic Evidences. Shiraz University Journal of Legal Studies*, 10(2), 29–52. (In Persian)

ESeye Ltd. (2023). *SMS API Developer Guide* (Last updated March 1, 2023). Retrieved July 23, 2025, from 8297 SMS API Developer Guide

Ghanad, F., & Aligholi, A. (2020). *The Concept and Importance of Personal Data and Privacy and the Types of Protection in Cyberspace. Biannual Journal of Contract Law and New Technologies*, 1(1), 297–322. (In Persian)

Habibzadeh, T. (2017). *Information Technology Law: Electronic Evidence, Electronic Documents, and Electronic Signatures* (1st ed.). Tehran: Mizan Publishing. (In Persian)

Heydarinejad, N. (2017). *Legal Review of Electronic Evidence in the Current System*. *Qanunyar: Scientific–Legal Quarterly*, 3, 125–140. (In Persian)

Mahmodi Parchini, M., Riazi, L., Pour Ebrahimi, A. and Mousavi, S. A. A. (2025). *Comparison of Personal Data Protection Laws: Unique General Regulations under the European Union's General Data Protection Regulation (GDPR) and United States Laws. News Science Quarterly (NS)*, 13(4), 204-224. doi: 10.22034/lrsi.2024.468452.1210 (In Persian)

Markert, P., Lassak, L., Golla, M., & Dürmuth, M. (2024). *Understanding Users' Interaction with Login Notifications.* In CHI Conference on Human Factors in Computing, (853), 1–17.

Mason, S., & Seng, D. (Eds.) (2017). *Electronic Evidence (4th ed.). Institute of Advanced Legal Studies, School of Advanced Study*, University of London.

Mirshkari, A., & Alaei, S. (2020*). The Positive Nature of Data Messages as a Litigation's Evidence. Legal Research Quarterly*, (96), 301–326. (In Persian)

Leach, P., Mealling, M., & Salz, R. (2005). *A Universally Unique Identifier (UUID) URN Namespace* (RFC 4122). Network Working Group.

NIST. (2017). *Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B).* Retrieved July 27, 2025, from NIST Special Publication 800-63B

Omidi, M., & Safaei-Shahrasb, Z. (2022). *The Validity of Electronic Documents in Family Lawsuits. Journal of Jurisprudence and Legal Studies of Media*, Faculty of Refah, 4(2), 111–127. (In Persian)

Rabbani-Mousavian, A., & Naeimi, T. (2019). *Documentation In Accordance with Electronic Classic and Modern Documents and Their Effects in Legal System. Journal of Judgment*, (100), 157–179. (In Persian)

Rahimi, Z., & Taheripour, Z. (2019). *The Validity of Electronic Documents as Evidence in Spousal Disputes. Journal of Jurisprudence and Legal Studies of Media*, Faculty of Refah, 1(1), 51–74. (In Persian)

Sadeghi, H. (2017). *Civil Liability in Electronic Communications* (2nd ed.). Tehran: Mizan Publishing. (In Persian)

Shahbazi-Nia, M., & Abdollahi, M. (2009). *Ascertainment of Genuineness in Electronic Evidence.* Comparative Legal Studies (Modares), 13(4), 125–141. (In Persian)

Telegram. (2013). *Telegram adds Session Control and Two-Step Verification*. Retrieved July 17, 2025, from https://telegram.org/blog/sessions-and-2-step-verification (Accessed: 27 July 2025).