Comparative Studies in Jurisprudence, Law, and Politics

The Role of Electronic Evidence in the Detection, Proof, and Criminal Prosecution of Digital Violence Against Victims

1. Fariba Fereshteh Matin: Department of Criminal Law and Criminology, CT.C., Islamic Azad University Tehran, Iran
2. Mehdi Esmaeli*: Department of Criminal Law and Criminology, CT.C., Islamic Azad University Tehran, Iran. Email: dresmaeli@yahoo.com (Corresponding Author)
3. Abbas Tadayyon: Department of Criminal Law and Criminology, CT.C., Islamic Azad University Tehran, Iran

ABSTRACT

The extensive development of information and communication technologies has created new opportunities for social interaction while also facilitating emerging forms of criminal behavior and violence. Digital violence, as one of the most significant manifestations of this transformation, includes a wide range of harmful practices such as online harassment, cyberstalking, internet-based threats, digital extortion, identity impersonation, disclosure of private information, and the non-consensual dissemination of personal content. Characteristics such as the relative anonymity of offenders, rapid dissemination of digital content, the possibility of deleting or altering information, and the cross-border nature of digital infrastructures have created substantial challenges for the detection and criminal prosecution of these acts. In this context, electronic evidence has become a fundamental instrument for establishing connections between criminal conduct, offender identification, and criminal responsibility. This study examines the role of electronic evidence in the detection, proof, and criminal prosecution of digital violence against victims. The research adopts a descriptive-analytical methodology based on legal documents, legislation, and scholarly studies concerning digital evidence and cybercrime. The findings indicate that electronic data, including digital messages, images, audio and video files, traffic data, user account information, metadata, and system records, can play a decisive role in identifying criminal conduct, reconstructing the process of offending, establishing offender attribution, and strengthening criminal proof. However, the effective use of such evidence requires compliance with technical and legal requirements, including lawful acquisition, authentication, preservation of data integrity, documentation of the chain of custody, expert evaluation, and protection of procedural rights. Major challenges include difficulties in attributing digital data to a specific individual, manipulation and fabrication of digital content, identity concealment techniques, encrypted information, technical limitations, and obstacles related to cross-border cooperation. Therefore, developing a comprehensive legal framework, standardizing forensic procedures, strengthening judicial specialization, and enhancing victim protection mechanisms are essential steps for improving the effectiveness of electronic evidence in combating digital violence.

Keywords: *Electronic Evidence; Digital Violence; Crime Detection; Criminal Proof; Criminal Prosecution; Victims; Chain of Custody.*

How to cite: Fereshteh Matin, F., Esmaeli, M., & Tadayyon, A. (2027). The Role of Electronic Evidence in the Detection, Proof, and Criminal Prosecution of Digital Violence Against Victims. *Comparative Studies in Jurisprudence, Law, and Politics*, *9*(2), 1-20.

Submit Date: 28 March 2026
Revise Date: 29 July 2026
Accept Date: 06 August 2026
Initial Publish Date: 23 August 2026
Final Publish Date: 22 June 2027

پژوهش‌های تطبیقی فقه،
حقوق و سیاست

نقش ادله الکترونیکی در کشف، اثبات و تعقیب کیفری خشونت دیجیتال علیه قربانیان

۱. فریبا فرشته متین: گروه حقوق کیفری و جرم شناسی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران
۲. مهدی اسماعیلی*: گروه حقوق کیفری و جرم شناسی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران. پست الکترونیک: dresmaeli@yahoo.com (نویسنده مسئول)
۳. عباس تدین: گروه حقوق کیفری و جرم شناسی، واحد تهران مرکزی، دانشگاه آزاد اسلامی، تهران، ایران

چکیده

تحولات گسترده فناوری‌های اطلاعاتی و ارتباطی، علاوه بر ایجاد فرصت‌های جدید برای تعاملات اجتماعی، زمینه شکل‌گیری اشکال نوینی از بزهکاری و خشونت را نیز فراهم کرده است. خشونت دیجیتال به‌عنوان یکی از مهم‌ترین نمودهای این تحول، شامل طیفی از رفتارهای زیان‌بار مانند آزار و اذیت برخط، تعقیب سایبری، تهدید اینترنتی، اخاذی دیجیتال، جعل هویت، افشای اطلاعات خصوصی و انتشار بدون رضایت محتوای شخصی است. ویژگی‌هایی مانند ناشناس‌بودن نسبی مرتکب، سرعت انتشار داده‌ها، امکان حذف یا تغییر محتوا و فرامرزی‌بودن زیرساخت‌های دیجیتال، فرایند کشف و تعقیب کیفری این رفتارها را با چالش‌های جدی مواجه ساخته است. در این میان، ادله الکترونیکی به‌عنوان مهم‌ترین ابزار اتصال میان وقوع رفتار مجرمانه، شناسایی مرتکب و اثبات مسئولیت کیفری، نقش اساسی ایفا می‌کنند. پژوهش حاضر با هدف بررسی نقش ادله الکترونیکی در مراحل کشف، اثبات و تعقیب کیفری خشونت دیجیتال علیه قربانیان انجام شده است. روش پژوهش توصیفی ـ تحلیلی و مبتنی بر مطالعه منابع حقوقی، اسناد، قوانین و پژوهش‌های مرتبط با ادله دیجیتال و جرایم سایبری است. یافته‌های پژوهش نشان می‌دهد که داده‌هایی مانند پیام‌های الکترونیکی، تصاویر، فایل‌های صوتی و تصویری، داده‌های ترافیکی، اطلاعات حساب‌های کاربری، فرادادهها و سوابق سامانه‌ها می‌توانند در شناسایی رفتار مجرمانه، بازسازی فرایند ارتکاب، احراز هویت مرتکب و تقویت ادله اثباتی نقش تعیین‌کننده داشته باشند. بااین‌حال، بهره‌گیری مؤثر از این ظرفیت مستلزم رعایت الزامات فنی و حقوقی همچون جمع‌آوری قانونی، احراز اصالت، حفظ تمامیت داده، ثبت زنجیره نگهداری، امکان ارزیابی کارشناسی و رعایت حقوق طرفین دعواست. مهم‌ترین چالش‌های موجود شامل دشواری انتساب داده به شخص معین، امکان جعل و دستکاری محتوا، استفاده از فناوری‌های پنهان‌ساز هویت، رمزگذاری اطلاعات، محدودیت‌های فنی و مشکلات همکاری فرامرزی است. بر این اساس، توسعه چارچوب حقوقی جامع، استانداردسازی فرایندهای فنی، تخصص‌گرایی قضایی و تقویت حمایت از قربانیان می‌تواند نقش ادله الکترونیکی را در مقابله مؤثر با خشونت دیجیتال ارتقا دهد.

واژگان کلیدی: *مفاد قرارداد، معیار شخصی، معیار عینی، حقوق تطبیقی، حقوق ایران، حقوق عراق.*

نحوه استناددهی: فرشته متین، فریبا.، اسماعیلی، مهدی.، و تدین، عباس. (۱۴۰۶). نقش ادله الکترونیکی در کشف، اثبات و تعقیب کیفری خشونت دیجیتال علیه قربانیان. *پژوهش‌های تطبیقی فقه، حقوق و سیاست*، ۹(۲)، ۲۰-۱.

تاریخ ارسال: ۸ فروردین ۱۴۰۵
تاریخ بازنگری: ۷ مرداد ۱۴۰۵
تاریخ پذیرش: ۱۵ مرداد ۱۴۰۵
تاریخ چاپ اولیه: ۱ شهریور ۱۴۰۵
تاریخ چاپ نهایی: ۱ تیر ۱۴۰۶

مقدمه

گسترش فناوری‌های اطلاعاتی و ارتباطی، ساختار روابط انسانی، شیوه‌های مشارکت اجتماعی و الگوهای تبادل اطلاعات را به‌طور بنیادین دگرگون ساخته است. فضای دیجیتال دیگر صرفاً ابزاری جانبی برای ارتباط نیست، بلکه به بخشی جدایی‌ناپذیر از زندگی شخصی، خانوادگی، حرفه‌ای و اجتماعی افراد تبدیل شده و بسیاری از تعاملاتی که پیش‌تر در محیط فیزیکی تحقق می‌یافتند، اکنون در شبکه‌های اجتماعی، پیام‌رسان‌ها، پلتفرم‌های اشتراک محتوا، بازی‌های برخط، محیط‌های واقعیت مجازی و سامانه‌های ارتباطی انجام می‌شوند. این تحول، در کنار ظرفیت‌های گسترده برای آموزش، اطلاع‌رسانی و توسعه روابط اجتماعی، فرصت‌های جدیدی را نیز برای ارتکاب رفتارهای زیان‌بار فراهم کرده است. خشونت دیجیتال یکی از مهم‌ترین جلوه‌های این دگرگونی محسوب می‌شود و رفتارهایی مانند آزار و اذیت برخط، تعقیب سایبری، تهدید، اخاذی اینترنتی، افشای اطلاعات خصوصی، انتشار بدون رضایت تصاویر شخصی، جعل هویت، هتک حیثیت، قلدری سایبری و حملات هماهنگ علیه اشخاص را در بر می‌گیرد. تحلیل جرم‌شناختی آزار سایبری نشان می‌دهد که سهولت دسترسی به قربانی، فاصله فیزیکی میان مرتکب و بزه‌دیده و تصور ناشناس‌ماندن، می‌تواند موانع روانی ارتکاب خشونت را کاهش دهد (Abbasi, 2025). از سوی دیگر، هم‌گرایی جرایم سایبری با محیط‌های نوظهور دیجیتال، موجب شده است که رفتارهای مجرمانه از قالب‌های سنتی فراتر روند و در بسترهایی تحقق یابند که مرز میان جهان واقعی و مجازی در آن‌ها کم‌رنگ شده است (Zhou et al., 2024).

خشونت دیجیتال، اگرچه از طریق داده، تصویر، صدا، پیام یا حساب کاربری اعمال می‌شود، آثار آن محدود به فضای مجازی باقی نمی‌ماند. انتشار یک تصویر خصوصی می‌تواند حیثیت اجتماعی، موقعیت خانوادگی یا امنیت شغلی قربانی را تحت تأثیر قرار دهد؛ تعقیب مستمر در شبکه‌های اجتماعی ممکن است احساس ناامنی دائمی ایجاد کند؛ جعل حساب کاربری می‌تواند روابط شخصی یا حرفه‌ای فرد را تخریب کند و تهدید به افشای اطلاعات خصوصی ممکن است قربانی را در معرض کنترل، اجبار یا بهره‌کشی مستمر قرار دهد. مطالعات مربوط به تجربه زنان جوان از آزار سایبری نشان می‌دهد که این پدیده اغلب به‌صورت یک فرایند تدریجی و پیوسته ظاهر می‌شود و از یک پیام مزاحم آغاز شده و به تهدید، تحقیر عمومی، افشای داده‌های شخصی یا مداخله در زندگی واقعی قربانی گسترش می‌یابد (Mohammadkhani et al., 2024). در محیط‌های واقعیت مجازی و متاورس نیز تماس، آزار یا رفتار جنسی ناخواسته ممکن است در قالبی تجربه شود که اگرچه بدن فیزیکی قربانی مستقیماً لمس نشده است، آثار روانی و ادراکی شدیدی ایجاد می‌کند (Ball, 2022). بنابراین، تقلیل خشونت دیجیتال به «رفتار مجازی» یا تلقی آن به‌عنوان پدیده‌ای کم‌اهمیت، با واقعیت بزه‌دیدگی در جامعه دیجیتال سازگار نیست.

ویژگی‌های ساختاری خشونت دیجیتال، رسیدگی کیفری به آن را با دشواری‌های ویژه‌ای مواجه می‌سازد. نخست آنکه مرتکب می‌تواند با نام مستعار، حساب جعلی، شماره مجازی، شبکه خصوصی یا ابزارهای پنهان‌ساز هویت فعالیت کند. دوم آنکه داده‌های مرتبط با جرم ممکن است در مدت کوتاهی حذف، ویرایش، بازنشر یا از یک پلتفرم به پلتفرم دیگر منتقل شوند. سوم آنکه محتوای خشونت‌آمیز می‌تواند هم‌زمان در اختیار تعداد بسیار زیادی از کاربران قرار گیرد و حتی پس از حذف منبع اولیه، نسخه‌های متعدد آن در دستگاه‌ها، حافظه‌های ابری یا سامانه‌های دیگر باقی بماند. چهارم آنکه بخشی از داده‌های ضروری برای شناسایی مرتکب نزد شرکت‌های ارائه‌دهنده خدمات یا پلتفرم‌هایی نگهداری می‌شود که ممکن است خارج از قلمرو قضایی کشور قرار داشته باشند. بررسی‌های مربوط به تعقیب سایبری نیز نشان می‌دهد که جابه‌جایی میان چند حساب و چند ابزار ارتباطی، تفکیک یک رفتار منفرد از الگوی مستمر آزار را دشوار می‌کند (Abu-Ulbeh et al., 2021). در

نتیجه، روش‌های سنتی کشف جرم که عمدتاً بر مشاهده محل وقوع، آثار مادی، شهادت مستقیم یا دسترسی سریع به مرتکب استوارند، برای مواجهه با تمامی ابعاد خشونت دیجیتال کافی نیستند.

در چنین بستری، ادله الکترونیکی در مرکز فرایند عدالت کیفری قرار می‌گیرند. پیام‌های متنی، فایل‌های صوتی و تصویری، سوابق ورود به حساب، نشانی‌های اینترنتی، داده‌های مکانی، گزارش‌های سامانه، فراداده فایل‌ها، اطلاعات دستگاه، تاریخچه جست‌وجو، سوابق ارتباطی و داده‌های نگهداری‌شده نزد ارائه‌دهندگان خدمات، ممکن است وقوع خشونت، نحوه ارتکاب، هویت مرتکب، استمرار رفتار و آثار آن را آشکار سازند. ادله الکترونیکی صرفاً شکل جدیدی از سند نیستند، بلکه مجموعه‌ای از داده‌های فنی و محتوایی‌اند که باید در ارتباط با سامانه تولیدکننده، شیوه استخراج، تمامیت اطلاعات و زمینه وقوع رفتار تفسیر شوند (Moazenzadegan, 2022). در تحقیقات رایانه‌ای، حتی داده‌ای که در ظاهر حذف شده است ممکن است با روش‌های فنی بازیابی شود و اطلاعاتی که برای کاربر عادی قابل مشاهده نیست، از طریق بررسی ساختار فایل یا حافظه دستگاه کشف گردد (Aghaeinia, 2019). ازاین‌رو، ادله الکترونیکی می‌توانند فاصله میان ادعای قربانی و واقعیت قابل اثبات قضایی را کاهش دهند، اما این ظرفیت تنها هنگامی تحقق می‌یابد که داده‌ها به‌موقع، قانونی و تخصصی جمع‌آوری شوند.

کارکرد ادله الکترونیکی در پرونده‌های خشونت دیجیتال به مرحله دادرسی محدود نیست. این ادله در مرحله کشف، نشانه‌های اولیه وقوع جرم را فراهم می‌کنند؛ در مرحله تحقیقات مقدماتی، مسیر شناسایی حساب‌ها، دستگاه‌ها و اشخاص مرتبط را نشان می‌دهند؛ در تصمیم مقام تعقیب، مبنایی برای تشخیص کفایت ظن و ضرورت ادامه تحقیقات ایجاد می‌کنند و در مرحله رسیدگی، برای اثبات عناصر مادی و روانی جرم به کار می‌روند. راهنماهای جرم‌یابی رایانه‌ای بر این نکته تأکید دارند که کیفیت نتیجه نهایی، به اقدامات نخستین مأموران و نحوه حفاظت از داده از همان لحظه کشف وابسته است (Nelson et al., 2020). اگر تلفن همراه بدون رعایت اصول فنی بررسی شود، سامانه روشن به‌طور ناگهانی خاموش گردد، حساب کاربری بدون تهیه نسخه معتبر مسدود شود یا داده‌های پلتفرم پیش از صدور دستور حفظ از بین بروند، ممکن است مهم‌ترین منبع اثبات جرم نابود شود. بنابراین، کشف، اثبات و تعقیب کیفری در این حوزه سه مرحله مستقل و منفک نیستند، بلکه حلقه‌های یک زنجیره‌اند که ضعف در هر حلقه می‌تواند کل پرونده را با شکست مواجه سازد.

در عین حال، اتکای نظام عدالت کیفری به داده‌های دیجیتال نباید به پذیرش بی‌قیدوشرط آن‌ها منجر شود. ادله الکترونیکی، برخلاف ظاهر دقیق و فنی خود، ممکن است ناقص، تحریف‌شده، خارج از زمینه یا منتسب به شخص نادرست باشند. تصویر صفحه را می‌توان ویرایش کرد، زمان ایجاد فایل ممکن است بر اثر تنظیمات دستگاه تغییر کند، نشانی اینترنتی ممکن است به چند کاربر تعلق داشته باشد و حساب متعلق به متهم احتمال دارد در زمان وقوع جرم در اختیار شخص دیگری بوده باشد. ظهور فناوری‌های تولید محتوای مصنوعی و دیپ‌فیک نیز تشخیص مرز میان تصویر واقعی و محتوای ساختگی را دشوارتر کرده است (Chesney & Citron, 2021). پژوهش‌های ناظر بر اصالت‌سنجی ادله دیجیتال تأکید می‌کنند که دادگاه نباید صرفاً بر ظاهر داده تکیه کند، بلکه باید منشأ، تمامیت، شیوه استخراج و قابلیت بازتولید نتیجه را ارزیابی نماید (Braga da Silva, 2022). ازاین‌رو، ارزش اثباتی ادله الکترونیکی تابع رعایت مجموعه‌ای از الزامات حقوقی، فنی و شکلی است.

مسئله دیگر، ضرورت ایجاد تعادل میان کشف جرم و حقوق بنیادین اشخاص است. دسترسی به تلفن همراه، رایانه یا حساب ابری می‌تواند حجم گسترده‌ای از اطلاعات خصوصی قربانی، متهم و اشخاص ثالث را آشکار سازد که ارتباطی با موضوع پرونده ندارند. حریم خصوصی در محیط دیجیتال تنها به محرمانه‌بودن یک پیام محدود نیست، بلکه کنترل فرد بر گردآوری، استفاده، ترکیب و انتشار اطلاعات شخصی او را نیز در بر می‌گیرد (Solove, 2021). سوءاستفاده شبکه‌های اجتماعی از داده‌های شخصی و امکان پردازش گسترده اطلاعات کاربران نشان

می‌دهد که داده‌های جمع‌آوری‌شده برای یک هدف ممکن است در زمینه‌ای متفاوت مورد بهره‌برداری قرار گیرند (Saatchi et al., 2024). بنابراین، مقام قضایی باید میان ضرورت دسترسی به داده و اصل تناسب توازن برقرار کند؛ به‌گونه‌ای که تحقیقات کیفری به تفتیش نامحدود زندگی دیجیتال اشخاص تبدیل نشود و قربانی نیز در جریان اثبات جرم با افشای مجدد اطلاعات حساس خود مواجه نگردد.

هدف پژوهش حاضر، تبیین نقش ادله الکترونیکی در کشف خشونت دیجیتال، اثبات عناصر جرم و فراهم‌کردن مبنای لازم برای تعقیب کیفری مرتکبان است. در این چارچوب، پرسش اصلی آن است که ادله الکترونیکی تحت چه شرایطی می‌توانند میان وقوع رفتار زیان‌بار، شناسایی مرتکب و تصمیم قضایی درباره تعقیب و محکومیت ارتباط معتبر ایجاد کنند. فرض اصلی مقاله آن است که کارآمدی این ادله به وجود یک فرایند منسجم شامل حفظ فوری داده، جمع‌آوری قانونی، مستندسازی زنجیره نگهداری، احراز اصالت، اثبات انتساب، تحلیل تخصصی و رعایت حقوق طرفین وابسته است. روش پژوهش، توصیفی ـ تحلیلی و مبتنی بر مطالعه اسناد، منابع حقوق کیفری، آثار مرتبط با ادله دیجیتال و بخش‌های مرتبط پایان‌نامه است. در این مقاله، مباحث عمومی جرم‌شناختی، تاریخچه تفصیلی فضای سایبری و راهکارهای اجتماعی غیرمرتبط کنار گذاشته شده‌اند تا تمرکز اصلی بر پیوند میان دلیل دیجیتال و عملکرد نظام عدالت کیفری باقی بماند.

مبانی مفهومی و حقوقی ادله الکترونیکی در خشونت دیجیتال

خشونت دیجیتال را می‌توان مجموعه‌ای از رفتارهای عمدی، آسیب‌زا، تهدیدکننده، تحقیرآمیز یا کنترل‌گر دانست که به‌وسیله فناوری‌های اطلاعاتی و ارتباطی ارتکاب می‌یابند، تسهیل می‌شوند یا دامنه آثار آن‌ها افزایش پیدا می‌کند. در این تعریف، فناوری صرفاً وسیله‌ای خنثی نیست، زیرا برخی ویژگی‌های محیط دیجیتال، مانند امکان بازنشر نامحدود، ماندگاری داده، دسترسی مستمر به قربانی، گمنامی نسبی و تشکیل اجتماعات هماهنگ، کیفیت و شدت خشونت را دگرگون می‌کنند. خشونت دیجیتال ممکن است به شکل ارسال مکرر پیام‌های توهین‌آمیز، تهدید به قتل یا آسیب، افشای نشانی محل سکونت، انتشار تصویر خصوصی، جعل حساب، اخاذی با اطلاعات شخصی، تعقیب ارتباطات آنلاین، انتشار شایعات زیان‌بار یا تحریک دیگران علیه قربانی ظاهر شود. بررسی حقوقی خشونت دیجیتال در شبکه‌های اجتماعی نشان می‌دهد که آسیب به سلامت روانی و حیثیت فرد می‌تواند حتی در غیاب تماس فیزیکی، ماهیت جدی و مستمر داشته باشد (Sayah Alborzi, 2025). همچنین مطالعات مربوط به بزه‌دیدگی سایبری شهروندان، نقش دسترسی گسترده به فناوری، ضعف مراقبت دیجیتال و الگوهای استفاده از شبکه‌ها را در افزایش احتمال مواجهه با خشونت نشان داده‌اند (Firouzjaeian & Momeni, 2022).

با وجود تنوع مصادیق، ویژگی مشترک بیشتر اشکال خشونت دیجیتال آن است که رفتار مرتکب به نحوی با ایجاد، انتقال، ذخیره یا پردازش داده همراه می‌شود. تهدید اینترنتی ممکن است در قالب پیام متنی یا صوتی ثبت شود؛ تعقیب سایبری ممکن است در سوابق ورود، درخواست‌های مکرر ارتباط، حساب‌های متعدد و داده‌های مکانی بازتاب یابد؛ انتشار تصویر خصوصی می‌تواند آثار فنی خود را در زمان بارگذاری، شناسه حساب، نشانی اینترنتی و فراداده فایل باقی بگذارد و جعل هویت ممکن است از طریق اطلاعات ثبت حساب، ابزار مورد استفاده و ارتباط میان حساب جعلی و دستگاه مرتکب قابل پیگیری باشد. از این منظر، هر داده‌ای که در جریان فعالیت دیجیتال ایجاد می‌شود، الزاماً دلیل نیست، بلکه زمانی به دلیل الکترونیکی تبدیل می‌شود که بتواند در اثبات یا رد یک واقعیت مرتبط با پرونده نقش داشته باشد. تعریف حقوقی ادله الکترونیکی بر ارتباط داده با موضوع اثبات و قابلیت ارائه آن در فرایند قضایی تأکید دارد (Mirzaei, 2022). بنابراین، ارزش یک داده نه صرفاً از ماهیت فنی آن، بلکه از رابطه منطقی، حقوقی و زمانی آن با رفتار مورد تحقیق ناشی می‌شود.

میان «داده الکترونیکی»، «ردپای دیجیتال» و «دلیل الکترونیکی» باید تمایز قائل شد. داده الکترونیکی مفهومی گسترده است و هرگونه اطلاعات قابل پردازش به‌وسیله سامانه‌های رایانه‌ای را شامل می‌شود. ردپای دیجیتال، آثاری است که بر اثر فعالیت کاربر، دستگاه یا نرم‌افزار باقی می‌ماند؛ مانند ثبت زمان ورود، سابقه جست‌وجو، فایل‌های موقت یا اطلاعات مکانی. دلیل الکترونیکی بخشی از این داده‌هاست که پس از شناسایی، تحصیل، حفظ و ارزیابی، برای اثبات موضوعی در پرونده قابل استفاده می‌شود. ممکن است صدها داده در یک تلفن همراه وجود داشته باشد، اما تنها بخشی از آن‌ها با اتهام تهدید یا انتشار تصویر خصوصی مرتبط باشند. تحلیل ادله کیفری اقتضا می‌کند که میان داده مرتبط، اطلاعات جانبی و داده‌های کاملاً خصوصی و بی‌ارتباط تفکیک صورت گیرد (Mir Mohammad Sadeghi, 2020). این تمایز از یک سو مانع گسترش نامتناسب تحقیقات می‌شود و از سوی دیگر، دادگاه را از غرق‌شدن در انبوه اطلاعات فنی غیرضروری حفظ می‌کند.

ادله الکترونیکی مرتبط با خشونت دیجیتال را می‌توان از حیث محتوا و منشأ به چند گروه کلی تقسیم کرد. نخست، محتوای ارتباطات مانند پیام‌های متنی، رایانامه‌ها، فایل‌های صوتی، تصاویر و مکالمات در پیام‌رسان‌هاست که می‌تواند مستقیماً رفتار تهدیدآمیز، توهین‌آمیز یا اخاذی‌گرانه را نشان دهد. دوم، داده‌های ترافیکی و ارتباطی مانند زمان اتصال، نشانی اینترنتی، مبدأ و مقصد ارتباط، شناسه دستگاه و اطلاعات نشست کاربری است که برای بازسازی مسیر ارتباط و شناسایی حساب یا ابزار اهمیت دارد. سوم، داده‌های سیستمی و فراداده‌ها هستند که اطلاعاتی درباره ایجاد، ویرایش، انتقال یا بارگذاری فایل ارائه می‌دهند. چهارم، داده‌های موجود نزد اشخاص ثالث، از جمله پلتفرم‌ها، شرکت‌های مخابراتی و ارائه‌دهندگان خدمات ابری است. پنجم، داده‌هایی است که قربانی شخصاً حفظ می‌کند؛ مانند تصویر صفحه، ضبط صفحه، نشانی محتوا یا نسخه پیام. آثار تخصصی ادله رایانه‌ای تأکید می‌کنند که ارزش هر دسته به شیوه تولید، محل نگهداری و امکان بررسی مستقل آن بستگی دارد (Sadeghi, 2022).

یکی از مهم‌ترین تمایزها، تفاوت میان محتوای قابل مشاهده برای کاربر و اطلاعات فنی پنهان در سامانه است. قربانی ممکن است تنها متن تهدید یا تصویر منتشرشده را مشاهده کند، درحالی‌که داده‌های پشت صحنه شامل زمان دقیق ارسال، نشانی مبدأ، شناسه نشست، نوع دستگاه و سوابق تغییر حساب است. تصویر صفحه می‌تواند برای آغاز شکایت و جلوگیری از فراموش‌شدن محتوا مفید باشد، اما به‌تنهایی همیشه برای احراز اصالت و انتساب کافی نیست، زیرا امکان ویرایش تصویر، حذف بخش‌هایی از گفت‌وگو یا ساخت محیط مشابه وجود دارد. مطالعات مربوط به قابلیت پذیرش ادله الکترونیکی نشان می‌دهند که دادگاه باید میان نمایش بصری محتوا و داده اصلی تفکیک کند و در صورت امکان، فایل اصلی یا اطلاعات پشتیبان را نیز مطالبه نماید (Abbaspour & Bastani, 2025). کارشناسی اطلاعات متن‌باز دیجیتال نیز تنها زمانی ارزش بالایی دارد که شیوه دستیابی، مراحل راستی‌آزمایی و محدودیت‌های منبع برای دادگاه روشن باشد (Gillet & Fan, 2023).

ادله الکترونیکی دارای ویژگی‌هایی‌اند که آن‌ها را از بسیاری از ادله سنتی متمایز می‌سازد. این ادله غیرملموس‌اند، اما در حامل‌های فیزیکی یا سامانه‌های ابری ذخیره می‌شوند؛ به‌سادگی قابل تکثیرند، بی‌آنکه نسخه کپی از حیث ظاهر با اصل تفاوت داشته باشد؛ ممکن است بدون برجای‌گذاشتن آثار آشکار تغییر کنند و گاه به نرم‌افزار یا تجهیزات خاص برای مشاهده نیاز دارند. افزون بر این، برخی داده‌ها ناپایدارند و با خاموش‌شدن دستگاه، پایان نشست یا تغییر سامانه از بین می‌روند. بررسی چالش‌های اثبات دلیل الکترونیکی نشان می‌دهد که همین ویژگی‌ها سبب می‌شود مفاهیمی مانند اصل و کپی، تصرف فیزیکی و مشاهده مستقیم، در محیط دیجیتال نیازمند بازتعریف باشند (Zaman, 2026).

ادله دیجیتال در دادرسی‌های کیفری بین‌المللی نیز به دلیل حجم بالا، تنوع قالب‌ها و وابستگی به واسطه‌های فنی، فرصت‌ها و مخاطرات هم‌زمانی ایجاد کرده‌اند (Hellwig, 2022).

اعتبارپذیری ادله الکترونیکی را نمی‌توان به یک شرط منفرد فروکاست. نخست، دلیل باید با موضوع پرونده مرتبط باشد؛ داده‌ای که هیچ پیوند منطقی با رفتار مورد اتهام ندارد، صرفاً به دلیل دیجیتال‌بودن قابل استناد نیست. دوم، داده باید به شیوه قانونی تحصیل شده باشد و دسترسی به آن ناقض الزامات دادرسی و حریم خصوصی نباشد. سوم، اصالت آن باید احراز شود؛ یعنی دادگاه اطمینان یابد که داده همان چیزی است که ارائه‌کننده ادعا می‌کند. چهارم، تمامیت داده باید از زمان جمع‌آوری تا ارائه حفظ شده باشد. پنجم، انتساب آن به حساب، دستگاه یا شخص معین باید بر پایه مجموعه‌ای از قرائن معتبر انجام شود. ششم، روش استخراج و تحلیل باید قابل توضیح و بازبینی باشد. هفتم، طرفین باید امکان اعتراض به دلیل و گزارش کارشناسی را داشته باشند. بررسی قواعد پذیرش ادله الکترونیکی در نظام‌های حقوقی مختلف نشان می‌دهد که اصالت، قابلیت اعتماد و رعایت تشریفات تحصیل، سه محور اصلی ارزیابی قضایی هستند (Alidousti Shahreki et al., 2022).

در نظام حقوق کیفری ایران، ادله الکترونیکی در پیوند با قواعد عمومی اثبات جرم و مقررات خاص جرایم رایانه‌ای ارزیابی می‌شوند. ادله دیجیتال ممکن است به‌طور مستقل یا در قالب اماره، گزارش ضابط، نظر کارشناس، سند یا قرینه مؤثر در علم قاضی ظاهر شوند. بااین‌حال، قرارگرفتن داده دیجیتال در یکی از قالب‌های سنتی نباید موجب نادیده‌گرفتن ویژگی‌های فنی آن شود. بررسی جایگاه ادله الکترونیکی در دادرسی کیفری ایران نشان می‌دهد که پذیرش اصل قابلیت استناد، بدون تعیین معیارهای دقیق برای جمع‌آوری، نگهداری و انتساب، برای ایجاد رویه منسجم کافی نیست (Hadi Tabar & Yaghoubi Golvardi, 2023). همچنین حدود ارزش اثباتی این ادله به کیفیت تحصیل، امکان راستی‌آزمایی و میزان سازگاری آن با سایر قرائن پرونده وابسته است (Heidari, 2021). در نتیجه، قاضی باید هم قواعد حقوقی اثبات را رعایت کند و هم از ظرفیت کارشناسی برای درک ابعاد فنی بهره گیرد.

از منظر آیین دادرسی کیفری، مشروعیت دلیل به اندازه قدرت فنی آن اهمیت دارد. دستیابی به یک پیام یا فایل ممکن است واقعیت مهمی را آشکار کند، اما چنانچه داده از طریق دسترسی غیرقانونی، تفتیش نامتناسب یا تجاوز غیرضروری به حریم خصوصی تحصیل شده باشد، استفاده از آن می‌تواند با اصول دادرسی منصفانه تعارض پیدا کند. قواعد دادرسی کیفری بر قانونی‌بودن اقدامات ضابط، نظارت مقام قضایی، رعایت حقوق دفاعی و محدودبودن تحقیقات به موضوع اتهام تأکید دارند (Ashouri, 2023). در تحلیل نوین آیین دادرسی نیز دسترسی به سامانه‌های دیجیتال باید از حیث ضرورت، هدف، دامنه و مدت به‌صورت مشخص کنترل شود (Khaleghi, 2024). دغدغه دادرسی منصفانه در زمینه ادله دیجیتال حتی در رسیدگی‌های بین‌المللی مطرح است، زیرا حجم نامتوازن داده و دسترسی نابرابر طرفین به ابزارهای فنی می‌تواند حق دفاع را تضعیف کند (Arcos Tejerizo, 2023).

مبانی حقوقی ادله الکترونیکی باید با رویکرد بزه‌دیده‌محور نیز همراه شود. قربانی خشونت دیجیتال ممکن است برای اثبات ادعای خود ناچار به ارائه تصاویر خصوصی، مکالمات خانوادگی یا اطلاعاتی شود که افشای آن‌ها خود منشأ آسیب تازه است. نظام عدالت کیفری نباید حمایت از قربانی را به تحمیل افشای نامحدود داده‌های شخصی مشروط کند. در پرونده‌هایی که داده حساس برای اثبات ضروری است، باید دسترسی به آن محدود، ثبت و تحت نظارت قرار گیرد و تنها بخش مرتبط در اختیار اشخاص ضروری قرار داده شود. رویکرد حقوقی به خشونت علیه زنان نیز بر ضرورت سازوکارهایی تأکید دارد که علاوه بر تعقیب مرتکب، از بازتولید خشونت در جریان رسیدگی جلوگیری کنند

(Emamizadeh, 2025). بنابراین، اعتبار ادله الکترونیکی تنها محصول صحت فنی نیست؛ مشروعیت آن به رعایت کرامت، محرمانگی و امنیت قربانی نیز وابسته است.

نقش ادله الکترونیکی در کشف خشونت دیجیتال و شناسایی مرتکب

کشف خشونت دیجیتال غالباً با گزارش قربانی آغاز می‌شود، زیرا بسیاری از رفتارهای خشونت‌آمیز در حساب شخصی، پیام‌رسان خصوصی یا فضایی رخ می‌دهند که ضابطان به‌طور مستقیم بر آن نظارت ندارند. قربانی ممکن است پیام تهدیدآمیز، تصویر منتشرشده، درخواست اخاذی یا حساب جعلی را مشاهده و با ارائه تصویر صفحه، پیوند محتوا یا مشخصات حساب، شکایت خود را مطرح کند. این داده‌های اولیه، حتی اگر برای اثبات نهایی کافی نباشند، می‌توانند وجود ظن معقول درباره وقوع جرم را نشان دهند و مبنای آغاز اقدامات حفاظتی قرار گیرند. پژوهش درباره فرایند آزار سایبری زنان جوان نشان می‌دهد که قربانیان گاه پیش از مراجعه رسمی، مدت زیادی داده‌ها را به‌صورت پراکنده نگهداری می‌کنند یا بخشی از پیام‌ها را به دلیل ترس و فشار روانی حذف می‌کنند (Mohammadkhani et al., 2024). ازاین‌رو، نظام عدالت کیفری باید مسیر روشن و قابل دسترسی برای گزارش خشونت و آموزش شیوه حفظ اولیه داده فراهم آورد تا بار فنی کشف جرم به‌طور کامل بر دوش بزه‌دیده قرار نگیرد.

نخستین اقدام پس از دریافت گزارش، باید جلوگیری از نابودی یا تغییر داده‌های مرتبط باشد. در محیط دیجیتال، زمان عنصری تعیین‌کننده است؛ زیرا مرتکب می‌تواند حساب را حذف کند، پیام‌ها را از دسترس خارج سازد، تنظیمات حریم خصوصی را تغییر دهد یا داده‌های دستگاه را پاک کند. پلتفرم‌ها نیز ممکن است اطلاعات ترافیکی را فقط برای مدت محدودی نگهداری کنند. بنابراین، باید میان «حفظ فوری داده» و «ارائه یا افشای آن» تمایز قائل شد. دستور حفظ به معنای الزام دارنده داده به جلوگیری از حذف یا تغییر آن است و لزوماً اجازه مشاهده محتوا را ایجاد نمی‌کند. این تفکیک، امکان صیانت سریع از دلیل را بدون توسعه زودهنگام دسترسی قضایی فراهم می‌سازد. پژوهش‌های مرتبط با چالش‌های اجرایی مقابله با قلدری سایبری نشان داده‌اند که تأخیر در دریافت پاسخ از پلتفرم‌ها و فقدان سازوکار فوری حفظ اطلاعات، موجب از دست رفتن بخشی از ادله می‌شود (Mirasheghi et al., 2025). در نتیجه، سرعت واکنش باید با رعایت تشریفات قانونی همراه باشد.

جمع‌آوری ادله الکترونیکی با شناسایی منابع احتمالی داده آغاز می‌شود. این منابع می‌توانند تلفن همراه قربانی یا متهم، رایانه شخصی، حافظه جانبی، سامانه نظارتی، حساب شبکه اجتماعی، فضای ابری، رایانامه، سوابق مخابراتی یا سرور یک پلتفرم باشند. ضابط باید پیش از هر اقدام مشخص کند که چه نوع داده‌ای برای پرونده ضروری است، احتمال ناپایداری آن چقدر است و دسترسی به آن به چه مجوزی نیاز دارد. استخراج داده از دستگاه روشن با تهیه نسخه از حافظه پایدار تفاوت دارد؛ زیرا برخی اطلاعات مانند فرایندهای فعال، ارتباطات شبکه و داده‌های حافظه موقت با خاموش‌شدن دستگاه از بین می‌روند. الزامات حقوقی استخراج داده الکترونیکی ایجاب می‌کند که انتخاب روش فنی با ماهیت داده و حدود دستور قضایی متناسب باشد (Shafiei, 2021). اقدامات شتاب‌زده، مانند بازکردن برنامه‌ها یا جست‌وجوی دستی در دستگاه، ممکن است زمان‌ها، گزارش‌ها یا فایل‌های موقت را تغییر دهد و اصالت نتیجه را زیر سؤال ببرد.

یکی از روش‌های اصلی حفاظت از داده، تهیه تصویر فنی کامل از حافظه است. در این روش، نسخه‌ای دقیق از داده‌های موجود تهیه می‌شود تا بررسی‌های بعدی بر روی نسخه کاری انجام گیرد و اصل داده تا حد امکان بدون تغییر باقی بماند. تفاوت این نسخه با کپی معمولی در آن است که تصویربرداری تخصصی می‌تواند بخش‌های حذف‌شده، فضای تخصیص‌نیافته، ساختار فایل‌ها و اطلاعات سیستمی را نیز در بر گیرد. راهنماهای جرم‌یابی رایانه‌ای بر استفاده از ابزارهای جلوگیری‌کننده از نوشتن و ثبت مشخصات ابزار و نرم‌افزار تأکید دارند (Nelson et

al., 2020). پس از تهیه نسخه، مقدار هش یا شناسه تمامیت محاسبه می‌شود تا بتوان در مراحل بعدی نشان داد که داده تغییر نکرده است. اگر مقدار هش نسخه بررسی‌شده با مقدار ثبت‌شده در زمان جمع‌آوری مطابقت داشته باشد، قرینه فنی مهمی برای حفظ تمامیت فراهم می‌شود، هرچند این امر به‌تنهایی هویت تولیدکننده محتوا را اثبات نمی‌کند.

زنجیره نگهداری، سابقه مستمر تصرف، انتقال، ذخیره، بررسی و ارائه دلیل را ثبت می‌کند. در این سابقه باید مشخص باشد که داده در چه زمان و مکانی، به‌وسیله چه شخصی، با کدام ابزار و تحت چه مجوزی جمع‌آوری شده، چگونه بسته‌بندی یا ذخیره شده، چه اشخاصی به آن دسترسی داشته‌اند و چه عملیاتی بر روی نسخه کاری انجام گرفته است. نقص در زنجیره نگهداری الزاماً به معنای جعلی‌بودن دلیل نیست، اما می‌تواند اعتماد دادگاه به تمامیت و منشأ آن را کاهش دهد. چالش‌های مطرح‌شده درباره ادله الکترونیکی در نظام عدالت کیفری ایران نشان می‌دهد که نبود مستندسازی یکسان و وابستگی بیش از حد به توضیحات شفاهی کارشناسان، از عوامل تردید قضایی است (Khanki, 2025). تنظیم فرم‌های استاندارد، ثبت خودکار دسترسی‌ها و تفکیک نسخه اصلی از نسخه تحلیل‌شده می‌تواند امکان بازبینی مستقل را تقویت کند.

پس از حفظ داده، مرحله تحلیل برای کشف ارتباط میان محتوا، حساب، دستگاه و شخص آغاز می‌شود. شناسایی یک حساب کاربری تنها نخستین سطح انتساب است. ممکن است حساب با شماره تلفن، رایانامه، نشانی اینترنتی یا دستگاهی معین مرتبط باشد، اما این ارتباط هنوز اثبات نمی‌کند که متهم شخصاً رفتار مجرمانه را انجام داده است. دشواری انتساب جرایم سایبری از آنجا ناشی می‌شود که دستگاه می‌تواند مشترک باشد، گذرواژه ممکن است در اختیار دیگران قرار گرفته باشد، حساب احتمال دارد هک شده باشد و نشانی اینترنتی نیز ممکن است میان چند کاربر تقسیم شود (Razavi, 2021). بنابراین، شناسایی مرتکب باید بر هم‌گرایی قرائن استوار باشد؛ مانند زمان فعالیت، اطلاعات ثبت حساب، شناسه دستگاه، سوابق مکانی، سبک نوشتار، ارتباط با قربانی، داده‌های موجود در ابزار توقیف‌شده و آگاهی از اطلاعاتی که فقط مرتکب واقعی می‌توانسته بداند.

داده‌های ترافیکی در این مرحله نقش ویژه‌ای دارند. این داده‌ها محتوای ارتباط را نشان نمی‌دهند، اما می‌توانند زمان، مسیر، مبدأ، مقصد و مدت ارتباط را آشکار کنند. برای مثال، هم‌زمانی ورود یک حساب تهدیدکننده با اتصال دستگاهی متعلق به متهم، قرینه‌ای مهم است، اما باید احتمال استفاده دیگران یا دستکاری فنی نیز بررسی شود. داده‌های مکانی نیز می‌توانند نشان دهند که دستگاه در زمان خاص در محل معینی قرار داشته است، ولی دقت و شیوه تولید این داده‌ها متفاوت است. بررسی حقوق فناوری اطلاعات تأکید می‌کند که تفسیر داده‌های فنی بدون شناخت محدودیت‌های زیرساخت می‌تواند به نتیجه‌گیری نادرست منجر شود (Rahami, 2022). بنابراین، گزارش کارشناسی باید نه‌تنها نتیجه، بلکه میزان دقت، احتمال خطا و فرض‌های فنی تحلیل را برای مقام قضایی توضیح دهد.

در بسیاری از پرونده‌ها، مرتکب برای پنهان‌کردن هویت از ابزارهای رمزگذاری، شبکه‌های ناشناس، حساب‌های موقت یا خدمات خارجی استفاده می‌کند. رمزگذاری از یک سو برای امنیت ارتباطات مشروع ضروری است و از سوی دیگر، ممکن است دسترسی به داده مرتبط با جرم را دشوار کند. چالش‌های تحلیل داده رمزگذاری‌شده نشان می‌دهد که فقدان کلید، استفاده از رمزگذاری سرتاسری و امکان حذف خودکار پیام‌ها می‌تواند حتی پس از توقیف دستگاه نیز دسترسی به محتوا را ناممکن سازد (Talebi, 2022). پاسخ حقوقی به این مسئله نباید به تضعیف عمومی امنیت کاربران منجر شود، بلکه باید بر روش‌های هدفمند مانند تحلیل دستگاه، داده‌های پیرامونی، نسخه‌های پشتیبان و اطلاعات ترافیکی متمرکز باشد. ایجاد درهای پشتی گسترده می‌تواند امنیت همه کاربران، از جمله قربانیان خشونت دیجیتال، را کاهش دهد.

تحلیل مجموعه داده‌ها گاه ابعاد پنهانی جرم را آشکار می‌سازد که در گزارش اولیه قربانی مشخص نبوده است. ممکن است معلوم شود مرتکب از چند حساب برای آزار استفاده کرده، محتوای خصوصی را در گروه‌های مختلف توزیع کرده، با اشخاص دیگر هماهنگ بوده یا قربانیان متعددی را هدف قرار داده است. خط زمانی پیام‌ها و ورودها می‌تواند استمرار رفتار را نشان دهد و ارتباط میان تهدید دیجیتال و تعقیب فیزیکی را آشکار سازد. مطالعات تعقیب در میان نوجوانان نیز بر اهمیت تشخیص الگوی تکرار، شدت و گسترش رفتار برای ارزیابی خطر تأکید دارند (Lewis & Wheatley, 2023). در نتیجه، ادله الکترونیکی نه‌فقط برای شناسایی یک پیام یا فایل، بلکه برای بازسازی ساختار کلی خشونت اهمیت دارند.

کشف جرم باید هم‌زمان با حمایت فوری از قربانی انجام شود. اگر محتوای خصوصی در حال انتشار است، انتظار برای تکمیل تمامی مراحل کارشناسی می‌تواند آسیب را چند برابر کند. بااین‌حال، حذف فوری محتوا پیش از تهیه نسخه معتبر، ممکن است مهم‌ترین دلیل را از بین ببرد. راه‌حل، ایجاد هماهنگی میان حفظ قضایی و توقف انتشار است؛ به این معنا که نسخه‌ای معتبر از محتوا، نشانی، زمان، مشخصات حساب و داده‌های پشتیبان ثبت شود و سپس دستور محدودسازی دسترسی یا حذف صادر گردد. همچنین اطلاعات حساس قربانی نباید به‌طور غیرضروری میان واحدهای مختلف یا اشخاص متعدد گردش کند. کارآمدی کشف زمانی تحقق می‌یابد که سرعت، دقت فنی، قانونمندی و حمایت از قربانی به‌عنوان اجزای یک فرایند واحد دیده شوند.

نقش ادله الکترونیکی در اثبات و تعقیب کیفری خشونت دیجیتال؛ چالش‌ها و راهکارها

اثبات کیفری خشونت دیجیتال مستلزم نشان‌دادن وقوع رفتار مجرمانه، ارتباط آن با قربانی، انتساب رفتار به متهم و وجود عنصر روانی لازم است. ادله الکترونیکی ممکن است هر یک از این عناصر را به‌صورت مستقیم یا غیرمستقیم اثبات کنند. متن یک پیام می‌تواند ماهیت تهدید را آشکار سازد؛ سوابق بارگذاری ممکن است انتشار تصویر را نشان دهد؛ اطلاعات ورود می‌تواند ارتباط حساب با دستگاه را روشن کند و پیام‌های پیشین ممکن است انگیزه یا علم مرتکب را اثبات نماید. بااین‌حال، هیچ داده‌ای خارج از زمینه خود نباید تفسیر شود. جمله‌ای که در ظاهر تهدیدآمیز است ممکن است بخشی از گفت‌وگویی متفاوت باشد و یک تصویر نیز ممکن است بدون اطلاع صاحب دستگاه ارسال شده باشد. آثار مربوط به اثبات جرم تأکید می‌کنند که ارزش دلیل از هماهنگی آن با مجموعه اوضاع و احوال پرونده ناشی می‌شود (Mir Mohammad Sadeghi, 2020). ازاین‌رو، رویکرد مطلوب، ارزیابی مجموعی داده‌های محتوایی، فنی و رفتاری است.

برای اثبات عنصر مادی، باید نوع رفتار، زمان، ابزار، بستر و دامنه آن روشن شود. در پرونده تهدید، محتوای پیام، مخاطب، زمان ارسال و شرایطی که موجب ایجاد خوف شده است اهمیت دارد. در انتشار غیرمجاز داده خصوصی، باید عمل انتشار، نبود رضایت، ماهیت خصوصی محتوا و ارتباط متهم با بارگذاری مشخص شود. در تعقیب سایبری، یک تماس منفرد ممکن است کافی نباشد و توالی پیام‌ها، ایجاد حساب‌های متعدد، رصد مداوم و استمرار رفتار باید اثبات گردد. در اخاذی دیجیتال نیز ارتباط میان تهدید و مطالبه مال یا امتیاز اهمیت دارد. نقش دلیل دیجیتال در اثبات جرایم رایانه‌ای زمانی کامل می‌شود که داده فنی بتواند عناصر قانونی رفتار را به واقعیت‌های پرونده پیوند دهد (Almasi & Azarbaik, 2025). بنابراین، گزارش کارشناسی نباید صرفاً وجود یک فایل یا حساب را اعلام کند، بلکه باید ارتباط آن را با عنصر مورد اثبات توضیح دهد.

اثبات انتساب پیچیده‌ترین مرحله است. باید میان انتساب محتوا به حساب، حساب به دستگاه و دستگاه به شخص تفکیک شود. اینکه پیام از حساب متعلق به متهم ارسال شده است، ضرورتاً به معنای آن نیست که متهم در زمان ارسال کنترل حساب را در اختیار داشته است. همچنین

مالکیت تلفن همراه یا خط ارتباطی به‌تنهایی استفاده شخصی را ثابت نمی‌کند. مشکلات انتساب در جرایم سایبری ایجاب می‌کند که مقام قضایی احتمال سرقت هویت، نفوذ به حساب، استفاده مشترک و جعل داده را به‌طور جدی بررسی کند (Razavi, 2021). قرائنی مانند تطابق زمان ورود با حضور متهم، بازیابی همان محتوا از دستگاه او، اطلاعات خصوصی موجود در پیام، سبک نگارش، داده‌های مکانی، سوابق پرداخت و رفتارهای بعدی می‌توانند در کنار یکدیگر انتساب را تقویت کنند. هرچه نتیجه بر منابع مستقل بیشتری استوار باشد، احتمال خطای انتساب کاهش می‌یابد.

عنصر روانی معمولاً به‌طور مستقیم در داده ثبت نمی‌شود، اما می‌توان آن را از محتوای ارتباطات و رفتارهای پیرامونی استنباط کرد. تهدید قبلی به انتشار تصویر، ادامه تماس پس از درخواست صریح قربانی برای توقف، استفاده از چند حساب برای دورزدن مسدودسازی، مطالبه وجه در برابر حذف محتوا یا هماهنگی با دیگران می‌تواند قصد آسیب‌رسانی، علم به عدم رضایت و عمد در استمرار رفتار را نشان دهد. حذف حساب یا داده پس از اطلاع از شکایت نیز ممکن است به‌عنوان قرینه آگاهی از رفتار مورد توجه قرار گیرد، هرچند به‌تنهایی برای اثبات سوءنیت کافی نیست. تحلیل حقوقی نقش دلیل دیجیتال در اثبات جرم بر ضرورت تمایز میان داده‌ای که رفتار را نشان می‌دهد و داده‌ای که قصد و علم را استنباط‌پذیر می‌سازد تأکید دارد (Amid, 2025). دادگاه باید از تبدیل هر رفتار احتیاطی یا حذف عادی داده به نشانه قطعی مجرمیت پرهیز کند.

ادله الکترونیکی علاوه بر اصل وقوع جرم، برای اثبات استمرار، شدت و گستره آثار آن نیز اهمیت دارند. شمار پیام‌ها، فاصله زمانی میان تماس‌ها، تعداد حساب‌های به‌کاررفته، میزان بازنشر محتوا و تعداد مخاطبان می‌تواند شدت خشونت را روشن سازد. داده‌های پلتفرم ممکن است نشان دهند که تصویر خصوصی چند بار مشاهده یا به اشتراک گذاشته شده است. سوابق ارتباطی می‌توانند استمرار آزار در دوره‌ای طولانی را اثبات کنند. در پرونده‌های قلدری سایبری، تکرار، عدم توازن قدرت و گسترش عمومی تحقیر، در ارزیابی ماهیت و آثار رفتار مؤثر است (Rahmati & Seifi, 2021). مطالعات فرامرزی بزه‌دیدگی سایبری نیز نشان می‌دهند که زمینه فرهنگی و اجتماعی بر شدت تجربه آسیب اثر می‌گذارد، اما تداوم دسترسی دیجیتال به قربانی در محیط‌های مختلف ویژگی مشترک این پدیده است (Shapka et al., 2019). اثبات پیامدهای خشونت نیز ممکن است نیازمند ترکیب داده‌های دیجیتال با ادله غیرالکترونیکی باشد. پرونده پزشکی، ارزیابی روان‌شناختی، شهادت نزدیکان، مدارک شغلی و سوابق تحصیلی می‌توانند آثار رفتار را تکمیل کنند. داده‌های دیجیتال ممکن است زمان آغاز اضطراب، ترک شبکه اجتماعی، تغییر حساب، درخواست کمک یا تلاش برای حذف محتوا را نشان دهند، اما تشخیص اختلال روانی نیازمند ارزیابی تخصصی است. مطالعات مربوط به مصرف اجباری محتوای جنسی و آشفتگی شناختی ـ عاطفی نشان می‌دهد که مواجهه مستمر با محتوای آسیب‌زا می‌تواند با پیامدهای روان‌شناختی معنادار همراه باشد (Privara & Bob, 2023). بااین‌حال، در هر پرونده باید رابطه میان رفتار مورد اتهام و آسیب ادعایی به‌طور مستقل بررسی شود و نتایج عمومی جایگزین اثبات فردی نگردد.

ارزش اثباتی تصویر صفحه از مسائل پرتکرار در پرونده‌های خشونت دیجیتال است. این تصویر به دلیل سهولت تهیه، ابزار مهمی برای حفظ اولیه محتواست، اما امکان برش، ویرایش یا ساخت آن وجود دارد و بسیاری از اطلاعات فنی را نمایش نمی‌دهد. برای افزایش اعتبار، بهتر است تصویر شامل نام حساب، زمان، نشانی محتوا، توالی کامل گفت‌وگو و اطلاعات محیط برنامه باشد و در صورت امکان، فایل اصلی یا نسخه استخراج‌شده از دستگاه نیز ارائه شود. تحلیل قابلیت پذیرش دلیل الکترونیکی نشان می‌دهد که اصالت باید بر پایه منشأ قابل توضیح،

ثبات محتوا و تأیید با قرائن دیگر ارزیابی شود (Abbasi, 2022). اتکای انحصاری به تصویر صفحه، به‌ویژه در پرونده‌ای که متهم جعل را ادعا می‌کند، می‌تواند تصمیم قضایی را آسیب‌پذیر سازد.

گزارش پلتفرم یا ارائه‌دهنده خدمات معمولاً از حیث زمان ورود، مشخصات حساب، نشانی‌های ارتباطی و سابقه بارگذاری ارزش ویژه دارد. بااین‌حال، این گزارش‌ها نیز باید از حیث منشأ، شیوه تولید و معنای فنی اصطلاحات بررسی شوند. ممکن است زمان ثبت‌شده بر اساس منطقه زمانی دیگری باشد یا سامانه تنها آخرین نشانی اتصال را نگهداری کند. داده‌های خودکار نباید بدون توضیح عملکرد سامانه قطعی تلقی شوند. مطالعات مربوط به ادله متن‌باز دیجیتال بر ضرورت استفاده از کارشناسانی تأکید دارند که بتوانند مسیر راستی‌آزمایی و محدودیت اطلاعات آنلاین را به زبان قابل فهم برای دادگاه بیان کنند (Gillet & Fan, 2023). نظر کارشناس، دلیل را تفسیر می‌کند، اما جایگزین تصمیم قضایی درباره اعتبار و وزن آن نمی‌شود.

ظهور دیپ‌فیک و محتوای تولیدشده با هوش مصنوعی، مسئله اصالت را وارد مرحله جدیدی کرده است. فایل صوتی یا تصویری ممکن است از حیث ظاهر کاملاً واقعی باشد، اما گفتار یا چهره فرد به‌صورت مصنوعی بازسازی شده باشد. در چنین شرایطی، مشاهده ظاهری یا شنیدن صدا برای احراز اصالت کافی نیست و باید منشأ فایل، فراداده، الگوهای فشرده‌سازی، نسخه‌های پیشین و نشانه‌های فنی بررسی شود. فناوری دیپ‌فیک توانایی ایجاد محتوایی را دارد که برای مخاطب عادی قابل تشخیص نیست و می‌تواند در هتک حیثیت، اخاذی و خشونت جنسی مبتنی بر تصویر به کار رود (Chesney & Citron, 2021). اصالت‌سنجی داده‌های دیجیتال در چنین پرونده‌هایی باید بر روش‌های شفاف، ابزارهای معتبر و امکان ارزیابی نتیجه توسط کارشناس مستقل استوار باشد (Braga da Silva, 2022).

ادله الکترونیکی در مرحله تعقیب، کارکردی متفاوت از مرحله محکومیت دارند. برای آغاز تحقیق، لازم نیست تمامی عناصر جرم به‌طور نهایی اثبات شده باشند؛ وجود اطلاعات قابل اعتماد درباره احتمال وقوع جرم و ارتباط احتمالی شخص یا حساب با آن می‌تواند اقدامات مقدماتی را توجیه کند. تصویر صفحه، گزارش قربانی و پیوند محتوای منتشرشده ممکن است برای صدور دستور حفظ داده یا مطالبه اطلاعات حساب کافی باشند، اما همان مجموعه احتمال دارد برای صدور حکم محکومیت کافی نباشد. آیین دادرسی کیفری میان ظن لازم برای آغاز تحقیقات و اطمینان لازم برای تصمیم نهایی تفاوت قائل است (Khaleghi, 2024). بنابراین، مقام تعقیب نباید ضعف اولیه داده را بهانه‌ای برای بایگانی شتاب‌زده شکایت قرار دهد و در مقابل، نباید بر پایه نشانه‌ای ناقص، اتهام قطعی را متوجه شخص سازد.

ادله الکترونیکی می‌توانند قلمرو و جهت تحقیقات مقدماتی را تعیین کنند. نشانی اینترنتی ممکن است مبنای مطالبه اطلاعات از ارائه‌دهنده خدمت باشد؛ زمان ارسال پیام می‌تواند محدوده بررسی دوربین‌ها یا داده‌های مکانی را مشخص کند؛ سوابق حساب ممکن است شناسایی سایر قربانیان را ممکن سازد و بازیابی فایل از دستگاه متهم می‌تواند ضرورت بررسی حساب‌های مرتبط را نشان دهد. ضابطان در این فرایند وظیفه جمع‌آوری و حفاظت را بر عهده دارند، بازپرس بر قانونمندی و تناسب اقدامات نظارت می‌کند، دادستان کفایت ادله برای ادامه تعقیب را می‌سنجد و کارشناس ابعاد فنی را تبیین می‌کند. قواعد آیین دادرسی بر این تفکیک نقش‌ها و نظارت قضایی تأکید دارند (Ashouri, 2023). اگر کارشناس از نقش فنی فراتر رود و درباره مجرمیت اظهارنظر کند یا ضابط بدون مجوز دامنه جست‌وجو را توسعه دهد، اعتبار فرایند مخدوش می‌شود.

یکی از موانع تعقیب مؤثر، پراکندگی و ناهماهنگی رویه‌های قضایی است. ممکن است یک شعبه تصویر صفحه را بدون بررسی تکمیلی کافی بداند و شعبه دیگر حتی داده استخراج‌شده را نیز بدون معیار روشن نپذیرد. چالش‌های اجرایی گزارش‌شده از سوی قضات نشان می‌دهد که

تفاوت سطح دانش فنی، فقدان دستورالعمل واحد و دشواری دسترسی به کارشناسان متخصص، موجب ناهمسانی تصمیم‌ها می‌شود (Mirasheghi et al., 2025). پژوهش‌های ناظر بر چالش‌های ادله الکترونیکی نیز بر ضرورت تعیین معیارهای واحد برای اصالت، تمامیت، انتساب و زنجیره نگهداری تأکید دارند (Khanki, 2025). وحدت رویه در این حوزه به معنای تعیین ارزش ثابت برای همه داده‌ها نیست، بلکه به معنای ایجاد فرایند ارزیابی شفاف و قابل پیش‌بینی است.

تعارض میان حریم خصوصی و کشف جرم از چالش‌های اساسی تعقیب است. تلفن همراه یا حساب ابری، صرفاً ظرف داده مرتبط با جرم نیست، بلکه آرشیوی از زندگی شخصی، ارتباطات خانوادگی، تصاویر، سوابق مالی و اطلاعات سلامت فرد است. دستور کلی برای استخراج تمامی محتوا می‌تواند بسیار فراتر از هدف مشروع تحقیقات باشد. نظریه‌های جدید حریم خصوصی نشان می‌دهند که آسیب اطلاعاتی تنها در افشا خلاصه نمی‌شود و گردآوری، ترکیب و استفاده خارج از زمینه نیز می‌تواند حق فرد را نقض کند (Solove, 2021). ازاین‌رو، دستور قضایی باید نوع داده، بازه زمانی، حساب یا دستگاه مورد نظر و هدف جست‌وجو را تا حد امکان مشخص کند. داده‌های نامرتبط باید تفکیک شوند و دسترسی اشخاص به محتوای حساس ثبت گردد.

این مسئله درباره قربانی اهمیت بیشتری دارد، زیرا اثبات جرم ممکن است مستلزم ارائه محتوایی باشد که انتشار آن منشأ خشونت بوده است. اگر تصویر خصوصی قربانی در پرونده‌های متعدد تکثیر شود، افراد غیرضروری آن را مشاهده کنند یا در گزارش‌های غیرمحرمانه توصیف شود، فرایند عدالت کیفری خود به عامل بزه‌دیدگی ثانویه تبدیل خواهد شد. قواعد حمایت از قربانی باید امکان ثبت محرمانه، محدودسازی دسترسی، حذف مشخصات هویتی از نسخه‌های غیرضروری و استفاده از نسخه فنی محافظت‌شده را فراهم کنند. حمایت حقوقی از قربانی خشونت دیجیتال نباید به صدور حکم نهایی محدود شود، بلکه باید از لحظه گزارش تا پایان نگهداری داده ادامه یابد. این رویکرد می‌تواند ترس از شکایت و نگرانی از افشای مجدد را کاهش دهد.

فرامرزی‌بودن داده‌ها مانع دیگری برای تعقیب کیفری است. ممکن است قربانی و مرتکب در ایران باشند، اما پلتفرم، سرور یا نسخه پشتیبان در کشور دیگری قرار داشته باشد. در این وضعیت، تفاوت قوانین نگهداری داده، الزامات حریم خصوصی، تشریفات درخواست و مدت پاسخ‌گویی می‌تواند سبب از بین رفتن دلیل شود. همکاری بین‌المللی در جرایم سایبری باید امکان حفظ سریع داده را پیش از تکمیل فرایند طولانی معاضدت قضایی فراهم آورد (Kazemi, 2022). بااین‌حال، دسترسی مستقیم و بدون رعایت حاکمیت دولت‌ها یا حقوق کاربران نیز قابل توجیه نیست. ایجاد نقاط تماس تخصصی، قالب‌های استاندارد درخواست و سازوکارهای اضطراری می‌تواند میان سرعت و مشروعیت تعادل برقرار کند.

ضعف تخصص فنی، محدودیت تجهیزات و تمرکز امکانات در مراکز بزرگ، بر کیفیت تحقیقات اثر مستقیم دارد. اگر نخستین مأمور حاضر در پرونده اصول حفاظت از دستگاه را نداند، ممکن است داده پیش از رسیدن به آزمایشگاه تغییر کند. همچنین استفاده از ابزارهای ناشناخته یا نسخه‌های غیرمعتبر نرم‌افزار می‌تواند قابلیت بازبینی نتیجه را کاهش دهد. آموزش نباید تنها به کارشناسان محدود شود؛ قضات و دادستان‌ها نیز باید مفاهیمی مانند هش، فراداده، داده زنده، نشانی اینترنتی و محدودیت تحلیل الگوریتمی را در سطح لازم بشناسند. کتاب‌های تخصصی دادرسی الکترونیکی بر پیوند میان زیرساخت فنی و تضمین‌های آیینی تأکید دارند (Habibzadeh, 2021). تخصص‌گرایی مستمر می‌تواند وابستگی غیرانتقادی مقام قضایی به نتیجه نرم‌افزار یا نظر کارشناس را کاهش دهد.

برای رفع چالش‌ها، نخست باید قواعد ادله الکترونیکی به‌صورت منسجم و روشن تدوین شوند. مفاهیمی مانند داده اصلی، نسخه فنی، اصالت، تمامیت، زنجیره نگهداری، حفظ فوری، ارائه داده و انتساب باید تعریف شوند. شرایط تفتیش سامانه، استخراج داده زنده، دسترسی به فضای ابری و استفاده از اطلاعات اشخاص ثالث نیز باید مشخص باشد. پژوهش‌های مربوط به چالش‌های تقنینی نشان می‌دهند که پراکندگی مقررات و استفاده از مفاهیم سنتی بدون تبیین فنی، موجب ابهام در اجرا می‌شود (Abbasi, 2022). تحلیل حقوقی جرایم سایبری نیز ضرورت انطباق مقررات با تحولات سریع فناوری را برجسته می‌کند (Anzab Dashti, 2025). قانون نباید به ابزار یا پلتفرم خاص محدود شود، بلکه باید اصول فناوری‌خنثی و قابل انطباق با تحولات آینده را مقرر کند.

استانداردسازی زنجیره نگهداری، راهکار بنیادی دیگری است. از لحظه دریافت داده باید زمان، مکان، هویت تحویل‌دهنده، مشخصات ابزار، وضعیت سامانه، روش استخراج و مقدار هش ثبت شود. نسخه اصلی باید در محیط امن نگهداری و هرگونه دسترسی به آن ثبت گردد. بررسی‌ها باید بر نسخه کاری انجام شوند و تمامی ابزارها و مراحل تحلیل در گزارش ذکر شوند. وجود فرم ملی واحد، سامانه ثبت دسترسی و امکان ممیزی مستقل، اختلاف درباره تغییر داده را کاهش می‌دهد. قابلیت پذیرش دلیل الکترونیکی زمانی تقویت می‌شود که دادگاه بتواند مسیر حرکت داده را از منبع تا جلسه رسیدگی بازسازی کند (Hadi Tabar & Yaghoubi Golvardi, 2023). نقص‌های جزئی باید با توجه به اثر واقعی آن‌ها ارزیابی شوند و هر اشتباه اداری نباید به حذف خودکار دلیل منجر شود، اما نقصی که احتمال تغییر یا جایگزینی را ایجاد می‌کند، باید جدی تلقی گردد.

ایجاد آزمایشگاه‌های تخصصی و تجهیزات سیار می‌تواند کیفیت اقدامات اولیه را ارتقا دهد. همه پرونده‌ها نباید برای حفظ یک تلفن همراه یا استخراج ابتدایی داده به مرکز کشور ارسال شوند. واحدهای تخصصی منطقه‌ای می‌توانند تصویربرداری، هش‌گذاری و حفاظت فوری را انجام دهند، درحالی‌که تحلیل‌های پیچیده در آزمایشگاه مرکزی صورت گیرد. ابزارهای مورد استفاده باید اعتبارسنجی شوند و روش‌های فنی قابل بازتولید باشند. همچنین آزمایشگاه تخصصی اصالت‌سنجی تصویر، صوت و محتوای تولیدشده با هوش مصنوعی برای مقابله با دیپ‌فیک ضروری است. نتیجه الگوریتم تشخیص جعل نباید به‌تنهایی دلیل قطعی تلقی شود و باید همراه با توضیح روش، نرخ خطا و قرائن مستقل ارائه گردد.

پلتفرم‌ها و ارائه‌دهندگان خدمات نیز در حفظ دلیل و حمایت از قربانی نقش دارند. لازم است مسیر سریع و قابل پیگیری برای گزارش خشونت، حفظ داده پس از دستور قانونی و ارائه اطلاعات ضروری ایجاد شود. سیاست نگهداری داده باید شفاف باشد تا مقام قضایی بداند چه اطلاعاتی برای چه مدتی در دسترس است. هم‌زمان، پلتفرم نباید بدون مبنای قانونی حجم نامحدودی از داده کاربران را در اختیار مقامات قرار دهد. مسئولیت‌پذیری به معنای همکاری هدفمند، حفظ محرمانگی و پاسخ سریع به وضعیت‌های اضطراری است. در موارد انتشار محتوای خصوصی، پلتفرم باید پس از حفظ نسخه قابل استناد، امکان محدودسازی سریع دسترسی و جلوگیری از بازنشر را فراهم کند.

در نهایت، کارآمدی تعقیب کیفری مستلزم طراحی یک پروتکل ملی برای قربانیان و شهروندان است. این پروتکل باید به زبان ساده توضیح دهد که قربانی چگونه بدون تغییر محتوا، نشانی، زمان، نام حساب، توالی پیام و نسخه اولیه را حفظ کند؛ از چه اقداماتی مانند پاسخ‌دادن تحریک‌آمیز، حذف فوری یا نصب نرم‌افزار ناشناخته بپرهیزد و چگونه گزارش خود را ثبت نماید. هدف از این آموزش، انتقال مسئولیت کشف جرم به قربانی نیست، بلکه جلوگیری از نابودی ناخواسته داده تا زمان مداخله تخصصی است. با پیوند میان قانون روشن، ضابط

آموزش‌دیده، کارشناس مستقل، دادستان متخصص، پلتفرم پاسخ‌گو و سازوکار حمایتی، ادله الکترونیکی می‌توانند از مجموعه‌ای پراکنده از داده‌ها به مبنایی معتبر برای کشف حقیقت و تحقق عدالت کیفری تبدیل شوند.

نتیجه‌گیری

خشونت دیجیتال یکی از اشکال پیچیده بزهکاری معاصر است که در آن، فناوری هم بستر ارتکاب رفتار زیان‌بار و هم منبع اصلی کشف و اثبات آن محسوب می‌شود. پیام‌ها، تصاویر، داده‌های ترافیکی، اطلاعات حساب، سوابق ورود، فراداده‌ها و گزارش‌های سامانه می‌توانند آنچه را در فضای دیجیتال رخ داده است بازسازی کنند؛ اما وجود داده به‌خودی‌خود به معنای وجود دلیل معتبر نیست. داده زمانی به دلیل قضایی قابل اتکا تبدیل می‌شود که ارتباط آن با موضوع پرونده روشن، شیوه تحصیل آن قانونی، اصالت و تمامیت آن قابل ارزیابی و انتساب آن به شخص معین بر پایه قرائن کافی باشد.

در مرحله کشف، ادله الکترونیکی امکان شناسایی رفتار، حفظ آثار ناپایدار، تعیین منابع داده و ترسیم مسیر تحقیقات را فراهم می‌کنند. گزارش قربانی، تصویر صفحه یا پیوند محتوا می‌تواند نقطه آغاز باشد، اما اقدامات اولیه باید به‌سرعت با حفظ تخصصی داده و مطالبه اطلاعات پشتیبان تکمیل شوند. تأخیر در صدور دستور حفظ، بررسی غیرتخصصی دستگاه یا حذف محتوا پیش از مستندسازی می‌تواند مهم‌ترین دلیل پرونده را از میان ببرد. ازاین‌رو، واکنش اولیه ضابط و مقام قضایی نقش تعیین‌کننده‌ای در موفقیت یا شکست تعقیب دارد.

در مرحله شناسایی مرتکب، باید میان حساب، دستگاه و شخص تفکیک شود. تعلق حساب یا خط ارتباطی به متهم به‌تنهایی برای اثبات استفاده شخصی او کافی نیست. انتساب معتبر معمولاً از ترکیب چند منبع مستقل حاصل می‌شود؛ از جمله اطلاعات ثبت حساب، زمان ورود، شناسه دستگاه، داده مکانی، محتوای بازیابی‌شده، ارتباط قبلی با قربانی و الگوی رفتاری. نظام عدالت کیفری باید احتمال هک‌شدن حساب، استفاده مشترک، جعل هویت و پنهان‌سازی فنی را نیز بررسی کند. هرچه تصمیم بر یک داده منفرد استوار باشد، خطر خطای قضایی بیشتر خواهد بود.

در مرحله اثبات، ادله الکترونیکی می‌توانند عنصر مادی، عنصر روانی، استمرار رفتار و گستره آسیب را روشن سازند. متن پیام ممکن است تهدید را نشان دهد، سوابق پلتفرم انتشار را اثبات کند و توالی رفتارها قصد آزار یا علم به عدم رضایت قربانی را آشکار سازد. بااین‌حال، هیچ داده‌ای نباید جدا از زمینه ارتباط، روش تولید و سایر قرائن تفسیر شود. تصویر صفحه، گزارش خودکار سامانه یا نتیجه ابزار تشخیص جعل هر یک دارای محدودیت‌هایی هستند و باید در کنار سایر ادله ارزیابی شوند.

نقش ادله الکترونیکی در تعقیب کیفری نیز باید با توجه به تفاوت میان مراحل دادرسی فهمیده شود. اطلاعاتی که برای آغاز تحقیق یا صدور دستور حفظ کافی است، ممکن است برای محکومیت نهایی کفایت نکند. مقام تعقیب باید از یک سو از بایگانی شتاب‌زده شکایت‌های معتبر به دلیل ناقص‌بودن ادله اولیه خودداری کند و از سوی دیگر، نشانه‌های مقدماتی را معادل اثبات قطعی مجرمیت نداند. تحقیقات مقدماتی باید برای تکمیل زنجیره دلیل، رفع احتمال‌های جایگزین و تأمین حقوق دفاعی به کار رود.

کارآمدی ادله الکترونیکی بدون رعایت حقوق قربانی و متهم قابل تحقق نیست. دسترسی به دستگاه یا حساب باید ضروری، هدفمند و متناسب باشد و اطلاعات نامرتبط نباید در معرض مشاهده یا استفاده قرار گیرد. در پرونده‌هایی که محتوای خصوصی موضوع خشونت است، حفاظت از محرمانگی قربانی اهمیت مضاعف دارد. تکثیر غیرضروری تصویر، گردش نامحدود پرونده یا مشاهده محتوا توسط اشخاص غیرمرتبط

می‌تواند خود به ادامه خشونت منجر شود. بنابراین، حمایت از قربانی باید از نخستین گزارش آغاز شود و تا حذف ایمن داده‌های غیرضروری پس از پایان رسیدگی ادامه یابد.

اصلاح وضعیت موجود مستلزم تدوین قواعد جامع ادله الکترونیکی، تعریف معیارهای اصالت و انتساب، استانداردسازی زنجیره نگهداری، ایجاد دستورهای فوری حفظ داده و تعیین حدود تفتیش سامانه‌های دیجیتال است. ایجاد شعب تخصصی، آموزش مستمر قضات و ضابطان، توسعه آزمایشگاه‌های منطقه‌ای، اعتبارسنجی ابزارهای فنی و تشکیل مرکز تخصصی اصالت‌سنجی صوت و تصویر نیز ضروری است. علاوه بر این، همکاری ساختاریافته با پلتفرم‌ها و مراجع خارجی باید به نحوی تنظیم شود که هم سرعت حفظ داده را افزایش دهد و هم حریم خصوصی و حاکمیت قانونی رعایت شود.

برآیند تحلیل آن است که ادله الکترونیکی می‌توانند حلقه اتصال میان تجربه قربانی، کشف رفتار، شناسایی مرتکب، اثبات جرم و تصمیم به تعقیب کیفری باشند. این نقش زمانی تحقق می‌یابد که کل مسیر دلیل، از نخستین ثبت تا ارائه در دادگاه، به‌صورت هماهنگ، شفاف و قابل بازبینی سازمان‌دهی شود. اتکای صرف به فناوری بدون تضمین حقوقی به همان اندازه ناکارآمد است که اجرای قواعد سنتی بدون توجه به ماهیت داده‌های دیجیتال. الگوی مطلوب، تلفیقی از دانش فنی، قواعد دادرسی منصفانه، تخصص قضایی و حمایت بزه‌دیده‌محور است؛ الگویی که در آن فناوری از ابزار ارتکاب خشونت به وسیله‌ای برای کشف حقیقت، توقف آسیب و تحقق عدالت تبدیل می‌شود.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

حامی مالی

این پژوهش حامی مالی نداشته است.

EXTENDED SUMMARY

The rapid expansion of digital communication technologies has fundamentally transformed patterns of interpersonal interaction, social participation, and access to information, while simultaneously creating new opportunities for technologically mediated abuse. Digital violence encompasses a wide range of harmful practices, including cyber harassment, cyberstalking, online threats, image-based sexual abuse, non-consensual disclosure of private information, identity impersonation, cyber extortion, coordinated humiliation, and persistent intimidation through social media and messaging platforms. Unlike many conventional forms of violence, these acts may be committed across geographical boundaries, repeated at negligible cost, amplified through mass dissemination, and sustained through the permanent or semi-permanent circulation of digital content. Recent criminological analyses indicate that the perceived anonymity of online environments, the reduced immediacy of face-to-face confrontation, and the ease of reaching victims can weaken behavioral restraints and facilitate repeated abuse (Abbasi, 2025). Research on young women's experiences further demonstrates that cyber harassment is frequently not an isolated event but an escalating process that may begin with unwanted contact and develop into threats, reputational attacks, surveillance, coercion, or disclosure of intimate data (Mohammadkhani et al., 2024). These characteristics create severe evidentiary difficulties because digital content can be deleted, altered, transferred between platforms, or stored on servers outside the territorial jurisdiction of the

investigating authority. At the same time, the same technologies used to perpetrate violence also generate electronic traces that may become crucial evidence. Messages, audiovisual files, metadata, login histories, traffic data, device identifiers, geolocation records, platform logs, and cloud-stored information can connect the harmful act to a particular account, device, or person. Electronic evidence therefore occupies a central position in bridging the victim's account of abuse with the legal requirements of detection, attribution, prosecution, and proof.

This study examines the role of electronic evidence in the detection, proof, and criminal prosecution of digital violence against victims, with particular attention to the Iranian criminal justice system. Its principal objective is to determine the conditions under which digitally generated information can be transformed from a technical trace into legally reliable evidence capable of supporting investigative and prosecutorial decisions. The research adopts a descriptive-analytical and documentary method and draws on criminal law, criminal procedure, cybercrime scholarship, digital forensics, and victim-oriented legal analysis. A central conceptual distinction is made between electronic data, digital traces, and electronic evidence. Electronic data include any information created, processed, stored, or transmitted by digital systems, whereas digital traces are the residual records produced by user or system activity. Such materials become electronic evidence only when they are relevant to a disputed fact, lawfully obtained, preserved in a reliable form, and capable of judicial evaluation. Iranian scholarship emphasizes that electronic evidence should not be treated merely as a digital equivalent of a traditional document because its evidentiary significance depends on the technical environment in which it was generated and extracted (Moazenzadegan, 2022). The evidentiary value of such material is therefore contingent on relevance, lawful acquisition, authenticity, integrity, attribution, reliability of the extraction method, and the possibility of adversarial examination. Studies of electronic evidence in Iranian criminal proceedings also reveal that formal recognition of digital evidence is insufficient when legislation does not provide clear and operational standards for collection, preservation, authentication, and judicial assessment (Hadi Tabar & Yaghoubi Golvardi, 2023). Accordingly, the study analyzes electronic evidence as a continuous evidentiary process extending from the first report of violence to final judicial evaluation.

In the detection stage, electronic evidence can reveal both the existence of digital violence and the broader pattern within which the reported act has occurred. Victims often initiate the process by presenting screenshots, saved messages, account details, hyperlinks, recordings, or copies of threatening communications. Although these materials may be insufficient for final conviction, they can establish a reasonable basis for opening an investigation, issuing urgent preservation orders, or requesting further information from service providers. The fragility of digital data makes speed essential because offenders can delete accounts, remove content, alter privacy settings, overwrite files, or exploit disappearing-message functions. Digital forensic literature stresses that the evidentiary quality of the final result is heavily dependent on the earliest actions taken by investigators (Nelson et al., 2020). Improperly opening applications, conducting a manual search on a seized device, or switching off a live system without considering volatile data may alter timestamps, system logs, or temporary memory. Consequently, the detection process should involve identification of relevant data sources, legal authorization, technical isolation of devices, forensic imaging, calculation of integrity values, secure storage of the original copy, and documented examination of a working copy. Legal requirements concerning the extraction of electronic data also demand that the chosen method correspond to the nature of the data and remain within the scope of judicial authorization (Shafiei, 2021). Chain of custody is especially important because it records who collected, transferred, stored, examined, and presented the evidence. Weak documentation may

not automatically prove fabrication, but it creates uncertainty about possible contamination or alteration. Effective detection additionally requires distinguishing between preservation and disclosure: service providers may first be ordered to prevent deletion of data before any separate decision is made regarding access to its content.

The role of electronic evidence in proof is more complex because the prosecution must establish not only that a digital event occurred, but also that it satisfies the legal elements of a criminal offense and is attributable to the accused. Content evidence may demonstrate the material act, such as the transmission of a threat, publication of an intimate image, repeated unwanted contact, or demand for payment in exchange for deletion. Traffic data, platform records, metadata, and device information may identify the route, time, and source of communication. Nevertheless, attribution should be approached through multiple evidentiary layers. Identifying an account does not necessarily identify the individual who controlled it, and connecting an account to a device does not conclusively establish who used the device at the relevant time. Iranian research on the attribution of cybercrimes highlights the possibility of account compromise, shared devices, identity theft, proxy use, and unauthorized access (Razavi, 2021). Reliable attribution therefore depends on converging indicators, including login times, device identifiers, subscriber information, geolocation, recovered content, payment records, linguistic patterns, prior communications, and knowledge of facts uniquely associated with the offender. Authenticity also represents a major challenge because screenshots, audio recordings, images, and videos may be edited or generated artificially. The emergence of deepfake technologies has substantially increased the risk that highly convincing but fabricated audiovisual content will be used for harassment, extortion, or reputational destruction (Chesney & Citron, 2021). Contemporary authentication therefore requires examination of provenance, metadata, file structure, compression patterns, prior versions, and corroborating evidence rather than reliance on visual appearance alone. Research on digital evidence authentication likewise emphasizes that technical conclusions must be transparent, reproducible, and open to independent examination (Braga da Silva, 2022).

Electronic evidence also shapes prosecutorial decision-making because different evidentiary thresholds apply at different stages of criminal proceedings. Information that is sufficient to justify preservation of data, seizure of a device, or continuation of preliminary investigation may not be sufficient for indictment or conviction. A victim's screenshot and narrative may reasonably initiate investigative measures, but stronger evidence will usually be required to establish authenticity, continuity, and attribution beyond the preliminary stage. Criminal procedure scholarship underscores the need to distinguish between the evidentiary basis for initiating an investigation and the degree of certainty required for a final criminal judgment (Khaleghi, 2024). Prosecutors and investigating judges must therefore avoid two opposite errors: dismissing a credible complaint merely because the victim lacks technically complete evidence, and treating a preliminary digital indicator as conclusive proof of guilt. Major obstacles include inconsistent judicial approaches, limited technical expertise, inadequate forensic infrastructure, encrypted communications, cross-border storage, delays in platform cooperation, and tension between investigative access and privacy. Studies of judicial experience with cyberbullying confirm that uneven technical knowledge and the absence of standardized procedures contribute to inconsistent treatment of electronic evidence (Mirasheghi et al., 2025). Encryption creates further difficulties because access to content may remain impossible even after lawful seizure, requiring reliance on device-level analysis, backups, metadata, or surrounding communications (Talebi, 2022). Cross-border evidence additionally depends on international cooperation, expedited preservation mechanisms, and standardized legal requests

(Kazemi, 2022). Necessary reforms include comprehensive legislation on electronic evidence, standardized chain-of-custody protocols, specialized judicial units, validated forensic tools, regional digital laboratories, clear platform obligations, and strict safeguards for the confidentiality of victims' sensitive data.

The study concludes that electronic evidence can function as the decisive link between the lived experience of digital violence and an effective criminal justice response, but only when it is treated as a legally regulated and technically verifiable process rather than as a collection of isolated digital files. Its role begins with the preservation of unstable traces and continues through the identification of accounts, devices, and users, the reconstruction of patterns of abuse, the establishment of material and mental elements of offenses, and the assessment of whether the evidentiary threshold for prosecution has been satisfied. The probative force of electronic evidence depends on lawful acquisition, relevance, authenticity, integrity, reliable attribution, documented chain of custody, and meaningful opportunities for examination and challenge. A screenshot, platform record, IP address, or algorithmic finding should therefore be evaluated within the broader evidentiary context and not treated as automatically conclusive. An effective framework must also protect victims from secondary victimization by limiting unnecessary reproduction of intimate content, restricting access to sensitive material, preserving evidence before removal of harmful content, and ensuring confidentiality throughout proceedings. At the same time, investigative measures must remain necessary, proportionate, and confined to data relevant to the alleged offense. The most appropriate model is an integrated one combining clear legislation, forensic competence, specialized prosecution, judicial oversight, platform cooperation, international coordination, and victim-centered safeguards. Under such a model, technology ceases to operate solely as an instrument through which violence is perpetrated and becomes a means of preserving truth, identifying offenders, preventing the loss of evidence, supporting lawful prosecution, and strengthening access to justice for victims of digital violence.

References

Abbasi, A. (2022). Legislative Challenges of Electronic Evidence in Iranian Law. *Legal Studies Quarterly*(31), 194.

Abbasi, N. (2025). *Criminological Analysis of Cyber Harassment* Sixth National Conference and First International Conference on Strategies for the Development and Promotion of Science Education in Iran, Isfahan.

Abbaspour, A., & Bastani, F. (2025). *Admissibility of Electronic Evidence in Proving Claims* Eleventh National Conference on Modern Studies and Research in the Humanities, Management, and Entrepreneurship in Iran, Tehran.

Abu-Ulbeh, W., Altalhi, M., Abualigah, L., Almazroi, A., Sumari, P., & Gandomi, A. (2021). Cyberstalking Victimization Model Using Criminological Theory: A Systematic Literature Review, Taxonomies, Applications, Tools, and Validations. *Electronics*, *10*(14), 17.

Aghaeinia, H. (2019). *Computer Crime Investigation and Digital Evidence*. Mizan.

Alidousti Shahreki, N., Keshavarz, A., & Sadeghi Asl, A. (2022). Rule Selection for the Admissibility of Electronic Evidence in the Legal Systems of Iran and the United States. *Judiciary Legal Journal*, *86*(119), 11.

Almasi, D., & Azarbaik, M. (2025). *The Role of Electronic Evidence in Proving Cybercrimes* Third International Conference on the Maritime Economy with an Emphasis on Law, Development, and Transportation, Bandar Abbas.

Amid, M. (2025). *The Role of Digital Evidence in Proving Criminal Offenses* Seventh International Conference and Eighth National Conference on Law and Political Science, Tehran.

Anzab Dashti, M. (2025). *Legal Analysis of Cybercrimes in the Iranian Legal System: Challenges and Solutions* First National Conference on Modern Studies in Culture, Art, and the Humanities, Ardabil.

Arcos Tejerizo, M. (2023). Digital Evidence and Fair Trial Rights at the International Criminal Court. *Leiden Journal of International Law*, *36*, 14.

Ashouri, M. (2023). *Criminal Procedure* (23rd ed.). SAMT.

Ball, K. (2022). Sexual Harassment in Virtual Reality Environments and the Emerging Metaverse. *New Media & Society*.

Braga da Silva, R. (2022). Updating the Authentication of Digital Evidence in the International Criminal Court. *international criminal law review*, *22*(5-6), 26.
Chesney, R., & Citron, D. (2021). Deepfakes and the New Disinformation War. *Foreign Affairs*, *98*, 63.
Emamizadeh, Y. (2025). *Strategies for Combating Violence Against Women from the Perspective of International Law with Emphasis on the Istanbul Convention* Ninth International Conference on Social Studies, Law, and Folklore, Tehran.
Firouzjaeian, A. A., & Momeni, F. (2022). Analysis of Factors Affecting Cyber Victimization Among Citizens: A Study of Citizens of Babol. *Social-Cultural Strategy Quarterly*, *11*(3), 9.
Gillet, M., & Fan, W. (2023). Expert Evidence and Digital Open-Source Information: Bringing Online Evidence to the Courtroom. *Journal of International Criminal Justice*, *21*(4), 61.
Habibzadeh, M. J. (2021). *Essentials of Electronic Proceedings*. Mizan.
Hadi Tabar, E., & Yaghoubi Golvardi, M. K. (2023). Electronic Evidence in Criminal Proceedings in the Iranian Legal System. *Comparative Criminal Jurisprudence Quarterly*, *3*(1), 118.
Heidari, M. (2021). *The Scope and Limits of the Evidentiary Value of Electronic Evidence in Criminal Law* Scientific Conference on Legal Studies, Judicial Sciences, and Social Research,
Hellwig, K. (2022). The Potential and the Challenges of Digital Evidence in International Criminal Proceedings. *international criminal law review*, *22*(5-6), 31.
Kazemi, H. (2022). *International Cooperation in Cybercrime*. Mizan.
Khaleghi, A. (2024). *Criminal Procedure* (49th ed.). Shahr-e Danesh.
Khanki, M. (2025). *Challenges of Electronic Evidence in Proving Cybercrimes in the Iranian Criminal Justice System* Third International Conference on Law, Management, Educational Sciences, Psychology, and Educational Planning, Tehran.
Lewis, M., & Wheatley, R. (2023). Classifying Stalking Among Adolescents: Preliminary Considerations for Risk Management. In *Young People, Stalking Awareness and Domestic Abuse* (pp. 26).
Mir Mohammad Sadeghi, H. (2020). *Evidence of Crime in Criminal Law*. Mizan.
Mirasheghi, A., Allahverdi, F., & Hajitabar Firouzjaei, H. (2025). Executive Challenges in Addressing Cyberbullying from the Perspective of Judges. *Journal of Law and Political Studies*, *5*(1), 207.
Mirzaei, A. (2022). *Electronic Evidence and Cybercrimes*. Dadafarin.
Moazenzadegan, H. A. (2022). *Electronic Criminal Evidence*. Khorsandi.
Mohammadkhani, M., Gorousi, S., Amirkafi, M., & Boustani, D. (2024). A Qualitative Exploration of the Cyber Harassment Process Among Young Women. *Strategic Studies of Sport and Youth*, *23*(63), 71.
Nelson, B., Phillips, A., & Steuart, C. (2020). *Guide to Computer Forensics and Investigations*. Cengage Learning.
Privara, M., & Bob, P. (2023). Pornography Consumption and Cognitive-Affective Distress. *Journal of Nervous and Mental Disease*, *211*(8), 652.
Rahami, M. (2022). *Information and Communications Technology Law*. Mizan.
Rahmati, S., & Seifi, R. (2021). Epidemiology and Risk and Protective Factors of Cyberbullying from a Developmental Perspective: A Narrative Review. *Rooyesh-e Ravanshenasi Journal*, *10*(11), 37.
Razavi, M. (2021). Problems in Attributing Cybercrimes to the Accused. *Criminal Law Quarterly*(24), 169.
Saatchi, A., Rezaei, S. A., & Javadi, A. (2024). Misuse of Personal Data by Social Networks and Strategies to Counter It. *Biannual Journal of Media Jurisprudence and Law*, *5*(2), 137.
Sadeghi, A. (2022). *Digital Evidence and Computer Crimes*. Majd.
Sayah Alborzi, M. (2025). *The Legal System for Combating Digital Violence Against Athletes on Social Networks and Its Impact on Athletes' Mental Health* National Conference on University, Public Law, Public Assets, and Social Responsibility,
Shafiei, R. (2021). Legal Requirements for Extracting Electronic Data. *Criminal Research Journal*(7), 157.
Shapka, J. D., Onditi, H. Z., Collie, R. J., & Lapidot-Lefler, N. (2019). Cyberbullying and Cybervictimization Within a Cross-Cultural Context: A Study of Canadian and Tanzanian Adolescents. *Child development*, *89*, 91.
Solove, D. (2021). *Understanding Privacy*. Harvard University Press.
Talebi, M. M. (2022). Technical and Legal Challenges in Analyzing Encrypted Data in the Process of Proving Crimes. *Modern Law Journal*, *15*(4), 113.
Zaman, Z. (2026). Challenges in Proving Electronic Evidence in Criminal Proceedings. *Quarterly Journal of Political Science, Law, and Jurisprudence*, *12*(1), 406.
Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*, *19*, 426.