Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 2, Issue 3, 2022

Legitimacy of Evidence in Cyberspace Crimes in Iranian Criminal Law

Afshar Khosravizad[1], Roohollah Sepehri*[2], Hamideh Babaee[3]

1. Ph.D Student in Criminal Law and Criminology, Department of Law, Naragh Branch, Islamic Azad University, Naragh, Iran.
2. Assistant Professor, Department of Law, Naragh Branch, Islamic Azad University, Naragh, Iran.(Corresponding Author)
3. Assistant Professor, Department of Law, Naragh Branch, Islamic Azad University, Naragh, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: 75-85

Corresponding Author's Info
ORCID: *0000-0001-9777-216X*
TELL: *+989125088701*
Email: *sepehrio@gmail.com*

Article history:
Received: *07 Jul 2022*
Revised: *01 Agu 2022*
Accepted: *14 Agu 2022*
Published online: *23 Sep 2022*

Keywords:
Legitimacy of Evidence, Crimes in Cyberspace, Evidence to Prove a Lawsuit, Electronic Evidence.

ABSTRACT

Due to the expansion of information technology, Traditional law is faced with a new type of evidence in crime detection called digital evidence. Due to problems such as "difficulty of correct attribution, possibility of distortion and destruction", the judicial system faced a new challenge in proving the evidence. It is extremely difficult to guarantee the security, validity and authenticity of data in the virtual space, which is a prerequisite for the credibility of electronic evidence and it can only be achieved to some extent through technical strategies. The legislator of Iran has not neglected to pay attention to these technical strategies and has mentioned this necessity in various regulations. The method of this article is descriptive and analytical. As a conclusion, it should be said that the legislator in Article 40 of the Computer Crimes Law has dealt with security measures metaphorically in the discussion of data seizure. The legislator has deemed it necessary to use reliable security measures to verify identity and authenticity in Article 656 of the Criminal Procedure Law approved in 2013. Attribution of reason in virtual crimes to the accused should be legitimate and convincing and based on criminal grounds.

How to Cite This Article: Khosravizad, A; Sepehri, R & Babaee, H (2022). " Legitimacy of Evidence in Cyberspace Crimes in Iranian Criminal Law" . *Journal of Comparative Criminal Jurisprudence*, 2(3): 75-85.

فصلنامه فقه جزای تطبیقی
www.jccj.ir
انجمن علمی فقه جزای تطبیقی ایران
فصلنامه فقه جزای تطبیقی

دوره دوم، شماره سوم، پاییز ۱۴۰۱

مشروعیت تحصیل دلیل در جرایم فضای مجازی در حقوق جزایی ایران

افشار خسروی‌زاد[۱]، روح الله سپهری*[۲]، حمیده بابایی[۳]

۱. دانشجوی دکتری حقوق جزا و جرم‌شناسی، گروه حقوق، واحد نراق، دانشگاه آزاد اسلامی، نراق، ایران.

۲. استادیار، گروه حقوق جزا و جرم‌شناسی، واحد نراق، دانشگاه آزاد اسلامی، نراق، ایران. (نویسنده مسؤول)

۳. استادیار، گروه حقوق جزا و جرم‌شناسی، واحد نراق، دانشگاه آزاد اسلامی، نراق، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۷۵-۸۵

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۰-۰۰۰۱-۹۷۷۷-۲۱۶X

تلفن: ۰۱ ۹۸۹۱۲۵۰۸۸۷+

ایمیل: sepehrio@gmail.com

سابقه مقاله:

تاریخ دریافت: ۱۴۰۱/۰۵/۰۷

تاریخ ویرایش: ۱۴۰۱/۰۶/۱۶

تاریخ پذیرش: ۱۴۰۱/۰۶/۲۱

تاریخ انتشار: ۱۴۰۱/۰۷/۰۱

واژگان کلیدی:

مشروعیت تحصیل دلیل، جرایم فضای مجازی، ادله اثبات دعوی، ادله الکترونیکی.

چکیده

به دلیل گسترش فن‌آوری اطلاعات، حقوق سنتی با نوع جدیدی از ادله در کشف جرم روبه‌رو شده که این ادله به دلیل مشکلاتی از قبیل «دشوار بودن صحت انتساب، قابلیت تحریف، تخدیش و تخریب» دستگاه قضایی را در تحصیل کشف دلیل و اثبات آن با چالش جدیدی مواجه نمود. تضمین امنیت، اعتبار و اصالت داده‌ها درفضای مجازی، که پیش‌شرط تعیین کننده استنادپذیری ادله الکترونیک محسوب می‌شود، امری به غایت دشوار است و تنها از طریق راهبردهای فنی تا اندازه‌ای محقق می‌شود. قانونگذار ایران نیز از توجه به این راهبردهای فنی غافل نبوده و در مقررات مختلف به این ضرورت اشاره کرده است. روش این مقاله به‌صورت توصیفی و تحلیلی است و چنین نتیجه گرفته شد که قانونگذار در ماده۴۰ قانون جرایم رایانه‌ای در بحث توقیف داده‌ها به تدابیر امنیتی به طور تمثیلی پرداخته و مقنن در ماده۶۵۶ قانون آیین دادرسی کیفری مصوب ۱۳۹۲ استفاده از تمهیدات امنیتی مطمئن برای احراز هویت و احراز اصالت را ضروری تلقی می‌کند. با نظر به اشارات مکرر قانونگذار به استفاده از این تدابیر امنیتی به نظر می‌رسد اساس قابلیت استناد بودن این ادله، اتخاذ این تدابیر است هرچند تاکنون اقدامات چندانی در خصوص فراهم ساختن بسترها جهت استفاده از این راهکارها انجام نشده است.

مقدمه

فـضای مجازی به مجموعه‌ای از ارتباطات درونی انسان‌ها از طریق رایانه و وسـایل مـخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می‌شود. یک سامانه (سیستم) آنلایـن نمونه‌ای از فضای مجازی است. در فضای مجازی نیازی به جابـه‌جـایی نـیست و کلیـه اعـمال فـقط از طریق فشردن کلیدها یا حرکات ماوس صورت می‌گیـرد.

از سوی دیگر موضوع، یعنی در حوزه پیشگیری و مقابله با جرایم، پلیس با توجه به وظایف خود نقش کلیدی در خصوص تحصـیل دلیـل دارد و این امر در حوزه فضای مجازی نیز از اهمیت فراوانی برخوردار اسـت. پلـیس یکی از ارکان مهم برقراری امنیت و آسـایش عمـومی اسـت. حـال چنانچـه پلـیس عملکرد اصولی و منطبق با تفسیر صحیحی از قانون نداشـته باشـد، خـود از عناصـر کاهش ضریب امنیت خواهد بود. ازآنجاکه اقدامات پلیس در یک نظام قانونی اعـم ازاینکه در چارچوب وظایف سازمانی خویش انجام پذیرد یا اینکـه تحـت ارشـادات دستگاه قضایی باشد به منزله پی‌ریزی ساختار اولیه جهت تشکیل پرونده اتهامی علیه اشخاص است. لذا چنانچه دستگاه پلیس کشور در عمل پای‌بند به اصول کشف جرم و تحصیل ادله کیفری باشد، در ترویج فرهنگ قانون‌مداری یا در حاکمیت بخشـیدن به امنیت روحی و روانی و احساس امنیت افراد جامعـه، مهـم‌تـرین عامـل محسـوب می‌شود. دستگاه پلیسی یک کشور که تکلیف کشف و تهیه عناصر تشکیل دهنده یک پرونده کیفری یا موضوع مستلزم تحقیق را برعهده دارد، می‌تواند در پـی‌ریـزی یـک پرونده اتهامی غیرقانونی و غیرمنصفانه نقش اساسی ایفاء کنـد، بـه‌نحـوی‌کـه حتـی دستگاه قضایی به یک روند ناخواسته هدایت شود. ازآنجاکه دلایل ارتکاب جرم در فضای مجازی، عمدتاً ادله الکترونیکی مـی‌باشـند، پلیس به‌منظور بررسی و کشف جرایم سایبری با مسائلی مواجه می‌شود که در سـایرجرایم مـطرح نـیست. دلایل الکـترونیک، ویژگی‌هایی دارنـد کـه آنهـا را از دلایـل سنتی متمایز می‌سازد. اینگونه دلایل نسبت به اسناد و مدارک دیگر، آسیب‌پـذیرتر هستند؛ زیرا به آسانی می‌توان آنها را دستکاری یا جعل یا با استفاده از دانش فنـی مناسب پنهان کرد که در این مقاله به این مسأله استنادپذیری ادله درفضای مجازی خواهیم پرداخت.

۱- مفهوم‌شناسی و مبانی نظری

۱-۱- مفاهیم

برای شناخت کامل و درک بهتر از هر رشته‌ای از علوم به‌ویژه در حوزه علوم انسانی، تعریف مفاهیم و بیان روشن از آن در شناخت مسائل، مشکلات و ارائه پیشنهادها و راهبردها بسیار مهم است. به همین جهت در این قسمت با توجه به گستردگی مفاهیمی که از یک طرف با حقوق و از سمت دیگر با فن‌آوری مرتبط است و نقش عمده‌ای در شناخت و تحلیل بهتر موضوعات دارد به تبیین مفاهیم پرداخته می‌شود.

۱-۱-۱- دلیل الکترونیک

دلیل در لغت به معنی راهنما است. در ماده۱۹۴ قانون آیین دادرسی مدنی اینطور آمده: **«دلیل امری است که اصحاب دعـوا بـرای اثبـات یـا دفـاع از ادعـا بـه آن اسـتناد می‌کننـد»** (کاتوزیان، ۱۳۸۸:۴۲). درحقوق کیفری تعریفی از دلیل ارائـه نشـده اسـت و تنهـا در مـاده۱۶۰قانون مجازات اسلامی مصوب۱۳۹۲قانونگذار به احصای ادله پرداخته است: **«ادله اثبات جرم عبارت از اقرار، شهادت، قسامه و سوگند در موارد مقـرر قـانونی و علـم قاضـی است»**. با تدقیق در این مقرره به نظر می‌رسد قانونگذار به صراحت علم قاضـی را بـه‌عنـوان یکی از ادله برشمرده است و خلاف قانون مجازات اسلامی سابق تفکیکـی میـان اسـتناد بـه علم قاضی در دعاوی حق الناسی و حق اللهی قائل نشده است و اقناع وجدانی قاضی اهمیت دوچندانی یافتـه اسـت؛ بنـابراین قاضـی در دو مرحلـه گـردآوری ادلـه و ارزیـابی آن در چارچوب قانون از آزادی عمل برخوردار است و می‌تواند از ادلـه الکترونیـک نیـز بـرای اثبات و احراز جرم استمداد جوید.

در قانون آیین دادرسـی کیفـری مصـوب۱۳۹۲ (اصلاحی۱۳۹۴) در فصل دادرسی الکترونیک نیز تعریفی از ایـن نـوع از ادلـه ارائـه نشـده است (مؤذن زادگان و همکاران،۱۳۹۴: ۷۲). دلیل الکترونیک در معنی رایج و

مصطلح عبارت است از **«هـر داده پیـامی کـه اصـحاب دعوا برای اثبات یا دفاع از مدعای خود به آن استناد می‌کنند»** (شهبازی نیا،۱۳۸۹: ۲۰۸). در این تعریف، ادله الکترونیک با واژه «داده پیام» تعریف شده است که شرح آن در ماده ۲ قـانون تجـارت الکترونیـک آمـده اسـت. قـانونگـذار بـا الهـام از قـانون نمونـه تجـارت الکترونیک آنسیترال، قانون تجارت الکترونیک و ماده۴۷ آیین نامه استناد پـذیری ادلـه الکترونیک مصوب۱۳۹۳، داده پیام را تنها منحصر به ابزارهای الکترونیـک ننمـوده اسـت و هر ابزاری اعم از تلگرام، تلکس، ابزارهای نوری و سایر ابزارهای ناشی از فناوری اطلاعات همانند پوشه‌های صوتی و تصویری نیز دلیل الکترونیک محسوب می‌شـوند و قالـب ادلـه الکترونیک موضوعیت نداشته و قانونگذار تنهـا بـه محتـوای داده پیـام توجـه نمـوده اسـت (محمدی،۱۳۸۸: ۱۵۳). درصدر ماده ۱۲ قانون تجارت الکترونیک[1]دو واژه «اسناد» با حرف «و» عطف به واژه «ی» ادله شده و این شبهه را ایجاد کرده که ادله الکترونیک تنها در قالب سند قابلیت ظهور و بروز را دارند؛ اما با توجه به عبارت ذیل ماده به نظر می‌رسد ایـن شـبهه قابل حل است و دلیل الکترونیـک در هـر قـالبی صـرفنظـر از محتـوا قابلیـت ظهـور دارد. هرچند مقنن در این قانون تنها به ادله‌ای چون امضـای الکترونیـک، داده پیـام‌هـای عـادی و داده پیام‌های مطمئن اشاره نموده، لیکن این امر نافی سایر ادله‌ی الکترونیـک نیسـت و مواد۱۳۲و۱۴۳قانون تجارت الکترونیک نیز صحت این مدعا را تأییـد مـی‌کنـد؛ ازایـن‌رو تفسـیر صرف ادله الکترونیک به اسناد الکترونیک صحیح نیسـت و سـند الکترونیـک تنهـا یـک بخش از اسناد الکترونیک به حساب می‌آید.

در کنار تحولات گوناگونی که در مفهوم جرم و شیوه ارتکاب آن در فضای سایبر پدیدار شد، حوزه کشف علمی جرایم مـرتبط نیـز دچـار تحـول و دگرگـونی گردیـد؛ به‌گونه‌ای که از آغاز بحث مقابلـه کیفـری بـا جـرایم رایانـه‌ای، مسائل راجع به آیین دادرسی کیفری ازجمله ادلّه ناشی از این سیستم‌ها و مشـکلات پیرامون آن و چگونگی تحصیل ادلّه الکترونیکی و اثبات جرایم سایبری مورد توجه و مطالعه قرار گرفت. برطبق اصول، برای اینکه هرگونـه اطلاعـات در هـر قالـب اعـم از الکترونیکی و غیرالکترونیکی قابلیت ارائه به دادگاه را داشته باشـد و از سـوی مرجـع قضایی نیز مورد استناد قرار گیرد، باید نخست، هویت پدیدآورنده آن معلـوم باشـد و دوم، اطلاعات معتبر و قابل اعتماد باشند (جلالی فراهانی،۱۳۸۹: ۱۲) با توجه به رواج پیام‌های الکترونیکی در حوزه‌های مهمـی مانند تجارت و بازاریابی الکترونیکی، بهره‌گیری از فنـاوری رمزنگـاری در ایـن حـوزه به‌ویژه به صورت امضاهای الکترونیکی به‌منظور شناسایی هویت پدیدآورنده توجه قرارگرفته است. به‌کارگیری امضـاهای دیجیتـال مطمـئن، حـداقل دو نتیجـه ارزشمند را به همراه دار: نخست اینکه تمامیت محتوای موجود در پیام الکترونیکی، تضمین شود؛ زیـرا تنهـاکسانی به آن دسترسی دارند که کلید اختصاصی رمزگشایی آن را در اختیـار داشـته باشند. دوم اینکه اثبات هویت پدیدآورنده پیامی که امضای الکترونیکی مطمـئن بـه آن ضمیمه شده، مقدور می‌شود. (جلالی فراهانی،۱۳۸۵: ۵۰) البته دلیل الکترونیک از مزایا و معایبی برخوردار است. ازجمله این مزایا مـی‌تـوان بـه مـوارد زیر اشاره کرد:

۱-قابلیـت کپـی بـرداری؛ ۲- سـهولت تغییـر و اصـلاح در نسـخه کپـی و نگهـداری نسخه اصل؛ ۳-صعوبت حذف؛ ۴- قابلیت ذخیره‌سـازی در مکـان‌هـای مختلـف سامانه رایانه‌ای بدون آگاهی واردکننده (رضایی،۱۳۸۷: ۶).

از جهات ضعف نیز مـی‌تـوان بـه ایـن موارد اشاره نمود: ۱- دشواری شناخت پدیدآورنده یا صادرکننده؛ ۲- عدم اطلاع از تغییر در داده به دلیل فقدان ابزار خاص و پیشرفته؛ ۳- قابلیت بالای حذف داده بـا نصـب یـک برنامـه نـه چنـدان پیشرفته؛ ۴- تأثیر نقص سیستم بر خروجی داده؛ ۵- تأثیر ابزارهای پردازشـی بـر روی اصـل داده؛ ۶-سهولت دسترسی

[1]- اسناد و ادله اثبات دعوی ممکن است به صورت داده‌پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان بر اساس قواعد ادله موجود، ارزش اثباتی «داده‌پیام» را صرفاً به دلیل شکل و قالب آن رد کرد.

افراد غیرمجازبه داده؛ ۷-کثرت و فراوانی داده بـه دلیـل ذخیـره شدن در برخی بخش‌های کامپیوتر اعم از کـامپیوتر شخصـی، اداری یـا منـزل، سـرور فایل‌های شبکه یا سیستم‌های بزرگ، پسـت الکترونیـک، نسـخه‌هـای پشـتیبان، ماشـین‌هـای فاکس یا سرورهای فاکس و.... ۸- کدگذاری داده جهت تخریـب (جلالـی فراهـانی،۱۳۸۶: ۸۸). واز چالش‌های پی‌جویی فعالیت‌های مجرمانه در حوزه محاسبات، گستره تحصیل کلیه ادله است و فرآیند استگانوگرافی یا اخفـای اطلاعات نیز چالش مشابهی برای ارزیابی به همراه دارد و کشف داده‌های دیجیتالی را دشوار یا غیرممکن می‌سازد. همچنین پویایی ادله یکی از چالش‌های اساسـی اسـت که همه تحلیلگران جنایی با آن مواجه می‌شوند. پویایی ادله هرگونه تـأثیری اسـت صرفنظر از قصد انجام آنکه موجب تغییر جابه‌جایی، ابهام یا نابودی ادله مـی‌شـود. این فرآیند بین زمانی که ادله منتقل می‌شود و زمانی که رسیدگی بـه پرونـده آغـازمی شود انجام می‌گردد (زندی،۱۳۹۳: ۴۷-۴۶).

۱-۱-۲- فضای مجازی

مفهوم فضای مجازی در اصطلاح که در واقع حاصل فن‌آوری غرب است، واژه‌ای است که در خلال دهه ۱۹۹۰ از طریق اینترنت کاربرد عمومی یافت. فضای مجازی یکی از واژه‌هایی است که نخستین بار ویلیام گیبسون نویسنده داستان‌های علمی تخیلی در سال ۱۹۸۴ به‌کار برد. از نظر او فضای مجازی فضایی تخیلی است که از اتصال رایانه‌ها پدید آمده است که تمامی انسان‌ها و منابع اطلاعاتی را به هم متصل کرده است (بریگز و برک،۱۳۸۶: ۱۲۰). به‌طورکلی برای وارد شدن به اینترنت یا فضای شبکه‌های بین‌المللی ابزاری لازم است، ازجمله کامپیوتر، مودم، وصل بودن به شبکه‌های بین‌المللی اینترنت، شبیه‌سازی و مجازی سازی. از مصادیق شبیه‌سازی می‌توان به کسب شخصیت یا موفقیت موهوم و خیالی یا مشابه یک شخصیت مهم توسط کاربر اشاره کرد یا به گفت‌وگو و حتی به توافق و انعقاد عقد دست یافت. «در خدمات (سرویس‌های) گفت‌وگوی صوتی تصویری که ایجاب و قبول عقد نکاح از طریق لفظ صورت می‌گیرد تردیدی در صحت این دسته از عقود وجود ندارد» (محقق داماد و جلالی، ۱۳۹۸: ۱۹۱).

تمام اطلاعاتی که در اینترنت و شبکه‌های بین‌المللی وجود دارد یا خلق می‌شود (اعم از واقعی و غیرواقعی) به صورت فیزیکی و ملموس وجود ندارند و درواقع آنچه در صفحه مانیتور مشاهده می‌شود، موضوعات مجازی می‌باشند که به صورت دیجیتالی وارد شبکه شده‌اند. برای آنکه شخص کاربر وارد فضای سایبر از طریق شبکه اینترنت شود، باید پس از فراهم آوردن تجهیزات اولیه (کامپیوتر، مودم، خطوط مخابراتی) به شبکه وصل شده و پس از آن آدرس و سایت موردنظر خود را انتخاب کرده و با توجه به نوع، موضوع و هدف خود به بررسی یا اقداماتی در آن بپردازد. با توجه به این توضیحات می‌توان گفت که فضای سایبر (محیطی است مجازی و غیرملموس که در فضای شبکه‌های بین‌المللی (که از طریق اینترنت به هم وصل می‌شوند) وجود دارد. در این محیط، تمام اطلاعات مربوط به روابط افراد، ملت، فرهنگ‌ها، کشورها، به صورت ملموس و فیزیکی (به‌صورت نوشته، تصویر، صوت و اسناد) در یک فضای مجازی و به شکل دیجیتالی وجود داشته مقابل استفاده و دسترس استفاده کنندگان و کاربران می‌باشد؛ کاربرانی که از طریق کامپیوتر و شبکه‌های بین‌المللی به هم مرتبط می‌باشند. (باستانی،۱۳۸۶: ۳۶) لازم به ذکر است فناوری اطلاعات و ارتباطات الکترونیک، به دلیل گستردگی در سراسر جهان، جرایم مجازی را از سایر جرایم ممتاز می‌کند و دلیل بر اثبات جرم را نیز به تبع آن متفاوت از فضای واقعی می‌گرداند. (حسین نژاد، ۱۳۹۸: ۶۲).

۱-۲- سهم دلیل و دادرسی الکترونیکی در نظام دادرسی

اگرچه به موجب قانون تجارت الکترونیکی و قوانین و مقرراتی دیگر، داده پیام در حکم نوشته محسوب می‌شود و ارزش اثباتی آن مورد تردید نیست، اما هنوز قضات و داورانی که مسلط به رایانه باشند، کم هستند.

با توجه به این که مقام رسیدگی کننده باید بر موضوع و فرایند دادرسی تسلط داشته باشد، نمی‌توان انتظار داشت که

برای تمامی امور از کارشناس استفاده شود. علاوه‌بر این، ارائه تمامی دلایل و امارات به صورت الکترونیکی، یا غیرممکن و یا بسیار هزینه‌بر است (السان و منوچهری،۱۳۹۷: ۲۷).

در مقابل باید قبول کرد که به دلایل مختلف، قالب الکترونیکی مدارک و سوابق بسیار مفید است. اول این‌که انتقال الکترونیکی اطلاعات (در قالب‌های مختلف)، بسیار سریع‌تر و ارزان‌تر از ارسال پستی یا ابلاغ از طریق مأمور انجام می‌شود. دوم این‌که، جستجوی اطلاعات در رایانه بسیار راحت‌تر از گشتن به دنبال آن‌ها در بایگانی نامنظم دفاتر شعب دادگاه می‌باشد. سوم این‌که، بایگانی انواع اطلاعات و سوابق به صورت الکترونیکی، بسیار ارزان و مدیریت سوابق بایگانی شده بسیار آسان است. البته امکاناتی که ارتباطات الکترونیکی فراهم سازد، نباید ناقص اصل (دسترسی به دادگاه صالح) باشد. به این معنا که تنها در صورتی می‌توان دادرسی الکترونیکی را (در قالب رسیدگی قضایی، داوری و....) مجاز دانست که از دسترسی هر دو طرف دعوا و مرجع رسیدگی به ابزارهای مناسب ارتباط الکترونیکی اطمینان حاصل شود (السان،۱۳۹۶: ۲۸۲). انجام مستمر تجارت الکترونیکی و پذیرش شیوه حل‌وفصل الکترونیکی اختلافات احتمالی، به‌عنوان شرط ضمن عقد، داشتن تارنمای فعال و تأکید بر پذیرش شیوه دادرسی الکترونیکی و یا ارجاع به رسیدگی مرجعی که تنها به صورت الکترونیکی اقدام به دادرسی می‌کند، از جمله اماراتی هستند که نشان می‌دهد شخص یا اشخاص مرتبط با یک اختلاف، امکانات لازم را برای دادرسی الکترونیکی در اختیار دارند و اقدام به دادرسی با استفاده از وسایل ارتباط الکترونیکی، موجب نقض حق دسترسی آن‌ها به فضای شایسته نمی‌شود.

۱-۳- اعتبار داده‌های الکترونیکی

امروزه در مورد اعتبار ادله الکترونیکی و همسانی ارزش اثباتی آن‌ها با ادله سنتی و کاغذی تردیدی وجود ندارد. قوانین و مقررات کشور ایران از حیث قابلیت استناد بین انواع مختلف داده‌های رایانه‌ای و مخابراتی قایل به تفکیک نشده و تمامی آن‌ها را به شرط ایمنی قابل استناد دانسته است (موذن زادگان و همکاران،۱۳۹۴: ۱۰۲) به موجب ماده ۶۵۵ قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی، در هر مورد که به موجب قوانین آیین دادرسی و سایر قوانین و مقررات موضوعه اعم از حقوقی و کیفری، سند، مدرک، نوشته، برگه اجرائیه، اوراق رأی، امضاء، اثر انگشت، ابلاغ اوراق قضائی، نشانی و مانند آن لازم باشد، صورت الکترونیکی یا محتوای الکترونیکی آن حسب مورد با رعایت سازوکارهای امنیتی مذکور در مواد این قانون و تبصره‌های آن کافی و معتبر است.

قابل اعتماد بودن یا معتبر بودن دلیل الکترونیکی، یک مسأله عرفی است که البته برخی نویسندگان حقوق سایبری از واژه (اعتماد) به معتبربودن تعبیر کرده‌اند (جلالی فراهانی،۱۳۸۶: ۹۵) و جز در مواردی که میان اصحاب دعوا یا در کشورهایی که از هیأت منصفه در روند دادرسی استفاده می‌کنند، میان اعضای این هیأت اختلاف پیش نیاید، لازم نیست صرف اثبات اصالت (اعتماد) به کارشناس ارجاع شود.

۱-۴- شروط استنادسازی به ادله درفضای مجازی

در ماده ۵۱ قانون جرایم رایانه‌ای مقررشده: **«کلیه مقررات مندرج در فصل‌های دوم و سوم این بخش علاوه بر جرایم رایانه‌ای شامل سایر جرایمی که ادله الکترونیک در آنها مورد استناد قرار می‌گیرند نیز می‌شود»**. همچنین در تبصره ماده ۵۲ آمده: **«در مواردی که در بخش دوم این قانون برای رسیدگی به جرایم رایانه‌ای مقررات خاصی از جهت آیین دادرسی پیش‌بینی نشده است، طبق مقررات قانون آیین دادرسی کیفری اقدام خواهد شد»** (مؤذن زادگان و همکاران،۱۳۹۴ : ۷۷). با توجه به این دو ماده به نظر می‌رسد کلیه داده‌های مذکور در فوق در دعاوی سنتی نیز به‌کار می‌رود و این ادله تنها منحصر به رسیدگی به دعاوی سایبری نیست. از سوی دیگر دعاوی سایبری برای اثباتشان بی‌نیاز به ادله سنتی نیستند و در بسیاری از موارد در جایی که قانون جرایم رایانه‌ای با خلأ مواجه است باید به قانون آیین دادرسی کیفری مراجعه و استناد نمود.

در بند «ح» ماده۲ قانون تجارت الکترونیک، قانونگذار خصایصی جهت مطمئن بودن یک سامانه اطلاعاتی برشمرده که عبارتند از: **«۱-به نحو معقولی در برابر سوءاستفاده**

و نفوذ محفوظ باشد؛ ۲-سطح معقولی از قابلیت دسترسی و تصدی صحیح را دارا باشد؛ ۳- به نحوی معقول متناسب با اهمیت کاری که انجام می‌دهد پیکربندی و سازماندهی شده باشد؛ ۴- موافق با رویه ایمن باشد». در ماده ۱۰ این قانون نیز قانونگذار در بحث شرایط امضای الکترونیکی مطمئن شرایطی ذکر کرده که عبارتند از: **«الف- نسبت به امضاکننده منحصربه فرد باشد؛ ب- هویت امضاکننده «داده پیام»را معلوم نماید؛ ج- به وسیله امضاکننده یا تحت اراده انحصاری وی صادرشده باشد؛ د- به نحوی به یک «داده پیام» متصل شود که هر تغییری در آن «داده پیام» قابلیت تشخیص و کشف باشد».** در ماده۱۳ این قانون مقرر شده: **«به‌طورکلی ارزش اثباتی داده پیام‌ها با توجه به عوامل مطمئنه ازجمله تناسب روش‌های ایمنی به‌کار گرفته شده با موضوع و منظور مبادله «داده پیام» تعیین می‌شود».** با تدقیق در این سه مقرره به نظر می‌رسد قانونگذار دو شرط اصلی استناد به اسناد را در مورد ادله الکترونیک که عبارتند از قابلیت انتساب و حفظ صحت، تمامیت و انکارناپذیری داده‌ها را مدنظر داشته و در موارد مختلف این قانون به آن اشاره شده است. هرچند در قانون مذکور از ادله‌ای چون امضای الکترونیکی داده پیام‌های مطمئن و داده پیام‌های عادی به صراحت سخن به میان آمده است، این تصریح نافی ارزش اثباتی سایر داده‌ها نیست و قانونگذار در ماده۱۴۱بر این مدعا مهر تأیید گزارده است.

قانونگذار در مواد ۶ و ۷ داده پیام و امضای الکترونیکی را معادل نوشته و امضای سنتی محسوب کرده و ماده۱۲ این قانون بر اصل لزوم پذیرش اسناد الکترونیکی تصریح کرده است: **«اسناد و ادله اثبات دعوا ممکن است به صورت داده پیام بوده و در هیچ محکمه یا اداره دولتی نمی‌توان ارزش اثبات داده پیام را صرفاً به خاطر شکل و قالب رد کرد».** در مواد ۱۴و۱۵ به ارزش اثباتی ادله مطمئن پرداخته شده است (شیرزاد،۱۳۸۸: ۲۵). برای پذیرش این دلایل در دادگاه، نخست باید دلیل ارائه شده در یکی از قالب‌های ادله سنتی مذکور در قانون قرار گیرد تا از ارزش اثباتی آن نوع دلیل برخوردار شود. تنها قالبی که ادله الکترونیکی می‌توانند در آن جای گیرند، نوشته است. این امر ناشی از ویژگی داده پیام است؛ زیرا تمام دلایل الکترونیکی به‌صورت داده پیام هستند. تمام اطلاعات ثبت شده توسط ابزارهای الکترونیکی شفاهی یا کتبی، داده پیام هستند. ازنظر قانونی همانطور که در بالا اشاره نمودیم، داده پیام ازنظر قانونی جایگزین نوشته است و قانون هر نوشته‌ای که برای اثبات دعوا مورد استناد قرار گیرد را سند می‌داند؛ بنابراین در نظام سنتی اثبات دعوا دلیل الکترونیکی از اعتبار سند برخوردار است (استنلی،۱۳۹۱: ۴۰) اسناد الکترونیکی که دارای شرایط مطمئن نیستند از ارزش اثباتی اسناد عادی برخوردارند؛ حتی اگر فن‌آوری مورد استفاده در آنها غیرایمن باشد و تا زمانی که اصالت آن اسناد تکذیب نشده یا طرف دعوا به اصالت آنها اعتراض نکرده حمل بر صحت سند است و دادرس نمی‌تواند به علت ایمن نبودن فن‌آوری مورداستفاده و یا امضا آن را معتبر نداند.

سند الکترونیکی مانند سند عادی قابل انکار و تردید است و کلیه کارکردهای سند عادی را نیز دارد؛ بنابراین از جمع مواد برمی‌آید که دلیل الکترونیکی از ارزش اثباتی همان قالب نظام ادله سنتی برخوردار است و چون معادل قالب نوشته در نظام سنتی است از کارکردهای سند بهره‌مند است (نوری،۱۳۸۲: ۵۴). یعنی از شیوه‌های خاص جمع‌آوری و نگهداری دلایل ارتکاب جرم جهت حفظ ارزش اثباتی آن‌ها و به بیان دیگر، چگونگی جمع‌آوری قانونی دلایل و نگهداری آنها جهت بهره‌برداری قضایی به همان صورت اولیه که کشف شده‌اند، استفاده نمود (زندی،۱۳۸۹: ۴۹).

۲- تحصیل دلیل در فضای مجازی

به موجب ماده ۱۱ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی، (مقام قضایی در جریان تحقیق و فرآیند رسیدگی می‌تواند دستور حفاظت هر نوع داده رایانه‌ای ذخیره شده را از جمله داده‌های رمزنگاری شده، حذف، پنهان، فشرده یا پنهان‌نگاری شده و یا داده‌هایی که نوع و نام آن‌ها موقتاً تغییر یافته و یا داده‌هایی که برای بررسی آنها نیاز به سخت

افزار مخصوصی می‌باشد، صادر نماید). کشف تحصیل دلیل جرم درفضای مجازی، در مقایسه با روند معمول کشف و پیگرد جرایم، نیازمند فنون و توانمندی‌های خاصی است.

۲-۱- اصول پایه حاکم برتحصیل دلیل در فضای مجازی

تحقیقات مربوط به جرایم فضای مجازی، از اصولی تبعیت می‌کند که در تمامی جرایم- صرف‌نظر از ماهیت آنها- باید مورد توجه نهاد پیگرد قرار گیرد. بسیاری از این ضوابط، همان اصولی هستند که دادسرا و نهادهای ذی‌ربط، برای کشف و پیگرد جرایم معمول به‌کار می‌گیرند و در عین حال، باتوجه به اوصاف خاص فضای مجازی، تعدیل شده‌اند.

به عنوان اصل اول، اقدامات تحقیقی نباید باعث تغییر یا تخریب داده‌هایی شود که در سامانه ذخیره شده یا در حال مبادله هستند. همچنین، کشف و پیگرد جرایم نباید موجب اخلال در عملکرد سامانه شود. در همین راستا صدر ماده ۶۷۲ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی مقرر می‌دارد: **«تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آن‌ها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه‌ها انجام می‌شود».**

در ماده ۶۸۲ قانون مذکور تصریح شده: **«متضرر می‌تواند در مورد عملیات و اقدامات مأموران در توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضایی دستور دهنده تسلیم نماید. به درخواست یاد شده خارج از نوبت رسیدگی می‌شود و قرار صادره قابل اعتراض است».**

در ماده ۶۶۱ همین قانون برای متخلفین تعیین کیفر شده و مقرر گردیده: **«چنانچه اشخاصی که مسؤول حفظ امنیت مراکز، سامانه‌های رایانه‌ای و مخابراتی و اطلاعات موضوع این بخش هستند یا داده‌ها یا سامانه‌های (سیستم) مذکور در اختیار آنان قرار گرفته است بر اثر بی‌احتیاطی یا بی‌مبالاتی یا عدم مهارت یا عدم رعایت تدابیر متعارف امنیتی موجبات ارتکاب جرایم رایانه‌ای به وسیله یا علیه داده‌ها و سامانه‌های رایانه‌ای و مخابراتی را فراهم آورند، به حبس از شش ماه تا دو سال یا انفصال از خدمت تا پنج سال یا جزای نقدی از ده تا صدمیلیون ریال محکوم خواهند شد».**

اصل دوم این است که هرجا- به‌طور استثنایی- نیاز به بازرسی سامانه، داده یا ارتباطات وجود داشته باشد، این امر باید توسط شخص خبره انجام شود. همچنین دلایل توجیهی امر، نتایج به دست آمده از بازرسی و میزان ارتباط آنها با احتمال‌های اولیه ضمن یک گزارش مستند، مشخص گردد.

اصل سوم با بایگانی و ثبت سوابق ارتباط می‌یابد. همه داده‌ها و مدارک به دست آمده یا ایجاد شده در فرایند پیگرد کیفری، باید در محلی ایمن نگاهداری شده و دارای برچسب مشخصات- و در صورت لزوم، جزئیات- باشد. در همین مورد ماده ۱۶ آیین‌نامه جمع‌آوری و استنادپذیری ادله الکترونیکی مقرر می‌دارد: **«حفاظت از داده‌ها باید به نحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده‌ها رعایت شود».** همچنین به موجب ماده ۶۷۵ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی؛ **«در توقیف داده‌ها، با رعایت تناسب، نوع، اهمیت و نقش آن‌ها در ارتکاب جرم، به روش‌هایی از قبیل چاپ داده‌ها، تصویربرداری از تمام یا بخشی از داده‌ها، غیرقابل دسترس کردن داده‌ها با روش‌هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حامل‌های داده عمل می‌شود».**

آخرین اصل آن است که شخص یا اشخاص معینی باید مسؤولیت اجرای اصول فوق را بر عهده گیرد و حدود اختیارات و وظایف آن‌ها و ضمانت اجرای تخلف از اختیارات از سوی ایشان مشخص شود. ذیل ماده ۶۶۹ قانون فوق در این مورد مقرر می‌دارد: **«چنانچه هریک از کارکنان دولت یا ضابطان قضایی یا سایر اشخاص از اجرای این دستور خودداری یا داده‌های حفاظت شده را افشاء کنند یا اشخاصی که داده‌های مزبور به آنها مربوط می‌شود را از مفاد دستور صادره آگاه کنند، ضابطان قضایی و کارکنان دولت به مجازات امتناع از دستور مقام قضایی و سایر اشخاص به حبس از نود و یک روز تا شش ماه یا جزای نقدی از پنج تا ده میلیون ریال یا هر دو مجازات محکوم می‌شوند.»**

۲-۲- جمع‌آوری و حفظ ادله

در فضای مجازی، جمع‌آوری و نگاهداری ادله شامل شناسایی، تعیین، توقیف و تأمین ادله دیجیتالی، تهیه گزارش از صحنه جرم و مکان‌ها و سامانه‌هایی که ادله در آن یافت

شده‌اند، می‌شود. به علاوه، در صورت لزوم باید بر روی هرکدام از ادله‌ای که به دست می‌آید، توضیح مربوط به مشخصات آن قید شود و ادله به دست آمده (اعم از سخت افزار و نرم افزار) به مکان امنی انتقال یابد.

شخصی که ادله در اختیار وی قرار دارد، باید اطمینان یابد که جمع‌آوری ادله از سوی شخص مجاز انجام می‌گیرد. صرف داشتن کارت شناسایی پلیس، کفایت نمی‌کند. بلکه مأمور قانون باید اثبات کند که مجوز اقدام خاصی را که درصدد انجام آن است، دارد. همچنین، باید از نیروی ماهر و ابزارهای دقیق استفاده شود تا کشف جرم موجب خسارت به داده‌ها و یا سامانه‌های رایانه‌ای نشود.

موضوع مهم دیگر، ارزش تحقیقاتی ادله است. پلیس باید بداند که دقیقاً دنبال چه چیزی می‌گردد و برای کشف جرم مجازی مشخص باید از چه سخت‌افزارها و نرم‌افزارهایی استفاده کند. برای این منظور، شناخت فنی پلیس مجازی، نسبت به ویژگی‌های فضای مجازی، افزارهای مورد استفاده در آن و کاربرد هرکدام از افزارها ضرورت دارد.

در این خصوص باید تذکر داد که محتوای دستور مقام قضایی نیز باید روشن و شفاف باشد. به موجب ماده ۶۷۳ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی، **«دستور تفتیش و توقیف باید شامل اطلاعاتی از جمله اجرای دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده‌های موردنظر، نوع و تعداد سخت‌افزارها و نرم‌افزارها، نحوه دستیابی به داده‌های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف باشد که به اجرای صحیح آن کمک می‌کند».**

ادله‌ای که کشف می‌شود، شامل سامانه رایانه‌ای، ابزارهای ذخیره داده (اعم از هارد، سی‌دی، دیسکت، فلش و کارت‌های حافظه) می‌شود. همچنین رایانه ممکن است قالب‌های مختلفی از قبیل تلفن همراه، رایانه همراه (لپ تاب) و دستگاه بازی و سرگرمی داشته باشد. ابزارهای قابل اتصال به رایانه مانند دوربین شبکه (وب‌کم)، کارت خوان‌ها، میکروفون، گوشی و... هم می‌تواند برای ارتکاب جرایم مجازی مورد استفاده قرار می‌گیرد. دستگاه‌هایی همچون ماهواره، دوربین دیجیتالی، انواع مختلف چاپگر، لوازم اتاق گفتگوی اینترنتی (چت، اعم از صوتی و یا تصویری) و ابرحافظه‌ها هم ممکن است در جهت ارتکاب جرم به‌کار گرفته شوند.

وجود سخت‌افزارهایی همچون کارت شبکه، مودم (سامانه اتصال به اینترنت از طریق تلفن)، رایانه همراه (که قابلیت اتصال به اینترنت را دارد)، سامانه اینترنت بی‌سیم، سامانه اینترنت ماهواره‌ای و موارد مشابه در صحنه (مشکوک به ارتکاب) جرم، نشان می‌دهد که متهم امکان دسترسی به اینترنت را داشته و قرینه‌ای ابتدایی برای قابلیت انتساب بزهکاری اینترنتی به وی است.

پلیس، برای کشف ادله، جمع‌آوری و حفظ آن‌ها باید ابزارهای لازم را در اختیار داشته باشد. این ابزارها، از جمله شامل رایانه، انواع کارت حافظه و کارت خوان، دوربین دیجیتالی، دستگاه‌های تشخیص وجود شبکه و ردیاب ارتباطات الکترونیکی می‌باشد. از آن جهت که به صرف اتهام نمی‌توان شخص را از حق دسترسی به اموال و اطلاعات خود محروم کرد، پلیس باید تا حد امکان از به هم زدن صحنه خودداری کرده و در صورت لزوم، دستگاه‌ها و سامانه‌ها را در همان محل تحت بازرسی و کنترل قرار دهد. بدیهی است که اگر امکان ورود به رایانه یا سامانه ای، به دلایل مختلف، از جمله رمزگذاری، وجود نداشته باشد، پلیس اختیار توقیف یا مهر و موم آن را خواهد داشت. مشروط بر اینکه توجیه کافی برای این اقدام وجود داشته باشد (السان و منوچهری،۱۳۹۷: ۱۹).

قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی فرض کرده است که در مورد تفتیش داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی اصل بر این است که نمی‌توان در وهله اول خود سامانه را توقیف کرد و باید طبق ماده ۶۷۴ این قانون، تفتیش داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی از طریق **«دسترسی به تمام یا بخشی از سامانه‌های رایانه‌ای و مخابراتی، دسترسی به حامل‌های داده از قبیل دیسکت‌ها یا لوح‌های فشرده یا کارت‌های حافظه و دستیابی به داده‌های حذف یا رمزنگاری شده»** انجام گیرد. مگر این که **«داده‌های ذخیره شده به سهولت در دسترس نباشد یا حجم زیادی داشته باشد یا**

تفتیش و تجزیه و تحلیل داده‌ها بدون سامانه سخت افزاری امکان‌پذیر نباشد یا متصرف قانونی سامانه رضایت داده باشد یا تصویربرداری از داده‌ها به لحاظ فنی امکان‌پذیر نباشد و یا این که تفتیش در محل باعث آسیب داده‌ها شود» که در این صورت خود سامانه رایانه‌ای یا مخابراتی توقیف می‌شود. (ماده ۶۷۶ قانون آیین دادرسی نیروهای مسلح و دادرسی الکترونیکی).

۳- اعتبار داده‌های الکترونیکی

امروزه در مورد اعتبار ادله الکترونیکی و همسانی ارزش اثباتی آن‌ها با ادله سنتی و کاغذی تردیدی وجود ندارد. قوانین و مقررات کشورایران از حیث قابلیت استناد بین انواع مختلف داده‌های رایانه‌ای و مخابراتی قایل به تفکیک نشده و تمامی آن‌ها را به شرط ایمنی قابل استناد دانسته است (موذن زادگان و همکاران،۱۳۹۴: ۱۰۲) به موجب ماده ۶۵۵ قانون آیین دادرسی جرایم نیروهای مسلح و دادرسی الکترونیکی، **«در هر مورد که به موجب قوانین آیین دادرسی و سایر قوانین و مقررات موضوعه اعم از حقوقی و کیفری، سند، مدرک، نوشته، برگه اجرائیه، اوراق رأی، امضاء، اثر انگشت، ابلاغ اوراق قضایی، نشانی و مانند آن لازم باشد صورت الکترونیکی یا محتوای الکترونیکی آن حسب مورد با رعایت سازوکارهای امنیتی مذکور در مواد این قانون و تبصره‌های آن کافی و معتبر است».**

قابل اعتماد بودن یا معتبر بودن دلیل الکترونیکی، یک مسأله عرفی است که البته برخی نویسندگان حقوق سایبری از واژه (اعتماد) به معتبربودن تعبیر کرده‌اند (جلالی فراهانی،۱۳۸۶: ۹۵) و جز در مواردی که میان اصحاب دعوا یا در کشورهایی که از هیأت منصفه در روند دادرسی استفاده می‌کنند، میان اعضای این هیأت اختلاف پیش نیاید، لازم نیست صرف اثبات اصالت (اعتماد) به کارشناس ارجاع شود.

نتیجه‌گیری

در نظام حقوقی ایران ادله باید از طریق قانونی تحصیل شوند وگرنه فاقد اعتبار برای استناد در حکم خواهند بود. پلیس طبق حقوق ایران نمی‌تواند از طرق غیرقانونی اقدام به جمع‌آوری دلایل کند. به عبارت دیگر با توجه بر اصل بی‌گناهی و اصل قانونی بودن، تحصیل ادله کیفری نیز تحت الشعاع قرارگرفته است و با توجه به اینکه در ماده۶۷۰ قانون آیین دادرسی کیفری دسته خاصی از ضابطان برای جمع‌آوری، مداخله، تفتیش، توقیف و حفظ و نگهداری داده‌ها از سامانه‌های رایانه‌ای پیش‌بینی نشده است، بهتر بود که مأموران پلیس فتا به‌عنوان مقام صلاحیت دار احصا می‌شدند. همچنین شایسته بود قانونگذار در ماده۶۸۰ قانون آیین دادرسی کیفری به جای عبارت«ذینفع»، ازعبارات ذینفع، وکیل یا نماینده قانونی او در صدر ماده استفاده می‌کرد.

ملاحظات اخلاقی: در این پژوهش تمامی ملاحظات اخلاقی رعایت گردیده است..

تعارض منافع: نگارش این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: در این پژوهش، نویسنده نخست به‌عنوان نویسنده اصلی متن و نویسنده دوم به‌عنوان همکار علمی و ناظر تحقیق عمل کرده‌اند.

تشکر و قدردانی: از همه بزرگوارانی که در نگارش این مقاله نویسندگان را یاری نموده‌اند، نهایت قدردانی و تشکر را دارد.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین مالی انجام گرفته است.

منابع و مآخذ

- استنلی، پائول (۱۳۹۱). *حقوق حفظ اسرار*. ترجمه محمدحسین وکیلی مقدم، تهران: نشرکتاب همگان.

- السان، مصطفی (۱۳۹۶). *حقوق تجارت الکترونیکی*. چاپ چهارم، تهران: نشر سمت.

- السان، مصطفی و منوچهری، محمدرضا (۱۳۹۷). «آیین کشف و ابراز دلیل درفضای مجازی». *مجله حقوق کیفری دانشگاه گیلان*، ۹ (۲): ۷ – ۳۰.

- باستانی، برومند (۱۳۸۶). *جرایم کامپیوتری و اینترنتی، جلوه‌ای نوین از بزهکاری*. تهران: انتشارات بهنامی، ۱۳۸۶.

- بریگز، ایسا و برک، پیتر (۱۳۸۶). *تاریخ اجتماعی رسانه‌ها ازگوتنبرگ تا اینترنت*. ترجمه حسن نمک دوست تهرانی و علی مرشدی زاد، تهران: نشر طرح نو.

- جلالی فراهانی، امیرحسین (۱۳۸۶). «استنادپذیری ادله الکترونیکی در امور کیفری». *مجله فقه و حقوق*، ۴ (۱۵): ۸۳ – ۱۱۳.

- جلالی فراهانی، امیرحسین (۱۳۸۹). *درآمدی بر آیین دادرسی کیفری جرایم سایبری*. تهران: نشر خرسندی.

- حسین نژاد، مجتبی (۱۳۹۸). «بررسی فقهی بغی در فضای مجازی». *مجله پژوهش‌های فقه و حقوق اسلامی*، ۵۵: ۵۳– ۷۴.

- رضایی، علی (۱۳۸۲). *حقوق تجارت الکترونیک*. تهران: انتشارات گنج دانش.

- زندی، محمدرضا (۱۳۸۹). *تحقیقات مقدماتی در جرایم سایبری*. تهران: نشر جنگل.

- شهبازی نیا، مرتضی و عبداللهی، محبوبه (۱۳۸۹). «دلیل الکترونیک در نظام ادله اثبات دعوا». *مجله حقوق دانشکده حقوق و علوم سیاسی*، ۴۰ (۴): ۱۹۳ – ۲۰۵.

- شیرزاد، کامران (۱۳۸۸). *جرایم رایانه‌ای از دیدگاه حقوق جزای ایران و حقوق بین‌الملل*. تهران: نشر شرکت نشر بهینه فراگیر.

- کاتوزیان، ناصر (۱۳۸۸). *اثبات و دلیل اثبات*. چاپ ششم، تهران: نشر میزان.

- محقق داماد، مریم و جلالی، زهرا (۱۳۸۹). «بررسی تطبیقی نکاح سایبری در فقه امامیه و اهل سنت». *مجله دوفصلنامه حقوق تطبیقی*، ۶ (۲): ۱۶۴ – ۱۹۷.

- محمدی، سام و میری، حمید (۱۳۸۸). «بررسی تطبیقی ارائه ادله الکترونیک در دادگاه؛ اشکال و اعتبار آن». *مجله نامه مفید*، ۹ (۱۷): ۱۵۱– ۱۷۸.

- مؤذن زادگان، حسنعلی؛ سلیمان دهکردی، الهام و یوشی، مهشید (۱۳۹۴). «حفظ صحت و استنادپذیری ادله الکترونیک با استفاده ازبیومتریک و رمزنگاری». *مجله پژوهش حقوق کیفری دانشگاه علامه طباطبایی*، ۴ (۱۲): ۶۹ – ۹۷.

- نوری، محمد علی (۱۳۸۲). *حقوق تجارت الکترونیک*. تهران: نشر گنج دانش.