همایش علمی مطالعات حقوقی، علوم قضایی و پژوهش های اجتماعی

نهاد برگزار کننده همایش: موسسه قانون یار

((با همکاری و حمایت معنوی دانشگاه رهنورد (استان بلخ، کشور افغانستان) – جهاد دانشگاهی استان تهران))

سردبیر علمی و مسئول برگزاری همایش: دکتر بهنام اسدی شماره مجوز: ۷۸۸۶۴-۱۵۲۱/۳۳۰۱

تاریخ برگزاری همایش: ۱۳خرداد۱۴۰۰ شماره مقاله: ۹۵/۱۲۸ رده بندی کنگره: الف ۹۰۳/۷۸۵۵

حدود و ثغور ارزش اثباتی ادله الکترونیکی در حقوق کیفری

مهدی حیدری

وکیل دادگستری و پژوهشگر

چکیده

ادله الکترونیکی هر داده پیامی است که اصحاب دعوی برای اثبات یا دفاع از دعوا به آن استناد می کنند وهر نمادی است از واقعه و یا اطلاعات و مفهوم که با وسایل الکترونیکی ، نوری و فناور های جدید اطلاعات ، تولید وارسال ودریافت و ذخیره می شود به عبارتی به اسناد و مدارک موجود در دنیای مجازی، ادله الکترونیکی گفته می شود البته ادله الکترونیک به رایانه ختم نمی شوند و همهٔ اطلاعات قابل کسب از دستگاه های الکترونیکی از جمله تلفن همراه، دورنگار و غیره را نیز شامل می شود . امروزه به دلیل جمع کثیری از پرونده های جرائم رایانه ای قانون گذار درمقابله با این جرائم سعی در حل مشکلات و معضلات ناشی از فضای سایبر داشته است و با تصویب قانون جرائم رایانه ای و تجارت الکترونیک و حمایت از پدید اورندگان از نرم افزارهای رایانه ای ، در بررسی نحوه جمع آوری ادله الکترونیک پرداخته است . ادله الکترونیک معمولا هیچ گاه از بین نمیروند اگرچه افراد گمان می کنند که اگر آنها را دلیت و یا پاک کنند از بین رفته است اما نسخه حذف شده تقریبا همیشه قابل بازیابی است و قابل ذکر است که داده پیامها به آسانی قابل تکثیر هستند و هنگامی که ایجاد می شوند درمکان های بسیار از جمله پوشه ها ی ثبت وقایع و سربرگ اسناد ، قابل ذخیره شدن می باشند به همین خاطر حذف همه انها دشوار است .

واژگان کلیدی: *جرایم رایانه ای، ادله و دلیل الکترونیکی، استناد پذیری، اصالت سند، اینترنت*

بخش اول: بررسی و شناخت ادله اثبات کیفری و انواع آن

تعاریف مختلفی از دلیل در فرهنگ های لغت و دانشنامه های حقوقی ارائه شده است، اما قانونگذار صرفاً در ماده ۱۹۴ آیین دادرسی مدنی گفته((دلیل عبارت از امری است که اصحاب دعوی برای اثبات یا دفاع از دعوی به آن استناد می نمایند))،اما در عالم حقوق، دلیل در دو مفهوم به کار گرفته می شود : نخست به مفهوم خاص، دلیل به هر وسیله ای گفته می شود که در قانون پیش بینی شده و در مرجع قضاوتی، با نمایاندن امری، سبب اقناع وجدان (ایجاد باور درونی) دادرس به واقعیت ادعا می شود.دوم در مفهومی اعم ((دلیل)) فراهم آوردن وسایلی است که وجدان دادرس را اقناع می نماید، پس اینکه گفته می شود بار دلیل بردوش مدعی است ، به معنای آن است که تدارک، تهیه و ارائه وسایلی که وجدان دادرس را نسبت به واقعیت امر مورد ادعا اقناع می نماید به عهده ی مد عی است ، چه شاکی باشند یا طرف شکایت قرار گرفته باشند.[1]

بند اول: بررسی و شناخت ادله اثبات سنتی

قوانین فعلی ایران از جمله قانون مجازات اسلامی و آیین دادرسی کیفری، تعریفی از دلیل ارائه نداده اند و شاید دلیل آن این بوده که در مباحث کیفری نمی توان به صورت انحصاری به دلایل رسیدگی نمود و از طرفی به اعتقاد برخی از اساتید و نویسندگان در حقوق جزا ، ما دلیل نداریم بلکه آنچه که مطرح است در واقع قرینه می باشد.به همین دلیل باید از مواد مختلف قانون آیین دادرسی کیفری قواعدی را در مورد دلایل در امور کیفری استخراج کرد ، برای مثال ماده ۱۵ قانون مذکور از لزوم ارائه دلایل از طرف شاکی خصوصی، ماده ۲۸ از تکلیف ضابطان دادگستری برای جمع آوری ادله و ماده ۴۴ از حفظ ادله جرم سخن به میان می آورد.بر همین اساس دلیل در آیین دادرسی کیفری ترسیم کننده مسیری است که مراحل مختلف دادرسی کیفری را از لحظه کشف جرم تا صدور حکم به هم پیوند می دهد و در این مسیر ادله برای اثبات جرم یا نفی اتهام مورد استناد قرار می گیرند. دکتر آشوری از اساتید حقوق معتقد است که در امور کیفری از آنجا که ارتکاب جرم موجبات اخلال در نظم جامعه و امنیت عمومی را

۱-عبدالله، شمس، ادله اثبات دعوی(حقوق ماهوی و شکلی)، انتشارات دراک- چاپ شانزدهم- صفحه ۲۸

فراهم می کند و هدف دعوی کیفری کشف حقیقت و دستیابی به منظور اعمال مجازات قانونی است ، علاوه بر دادستان یا شاکی، خود قاضی کیفری نیز در صورت لزوم باید به تکمیل دلایل و حتی تحصیل دلایل کاملاً جدیدی که بتواند در سرنوشت محاکمه موثر باشد، بپردازد.به نظر می رسد تعریف ایشان از دلیل کیفری، از سایر تعاریف دیگر بهتر باشد که بر اساس آن ، در امور کیفری دلیل عبارت از هر گونه وسیله ای است که وجود یا عدم امری و یا صحت و سقم ادعایی را اثبات کندو یا دلیل عبارت از هر وسیله قانونی است که مقامات قضایی را در کشف حقیقت و حصول اقناع وجدانی و اتخاذ تصمیم عادلانه یاری بخشد.[1]

بند دوم: نگاهی به ادله الکترونیکی

ماده ۲ قانون تجارت الکترونیکی تعریفی از داده پیام ارائه نموده و آن را با سند الکترونیکی در مواد بعد مرتبط دانسته و از لحاظ اعتبار در حکم سند رسمی قرار داده که قابلیت انکار و تردید ندارد و فقط می شود در ارتباط با آن ادعای جعل نمود، اما تعریفی که از ادله الکترونیکی ارائه شده ، عبارت است : ((ازهر گونه داده یا نرم افزار یا سخت افزار الکترونیکی که بتواند اطلاعات ارزشمندی را در راستای اثبات ادعا، دفاع، کشف جرم یا استدلال قضایی بدست دهد.))[2]شایان ذکر است که این ادله الکترونیکی محدود به ادله قابل کسب از طریق رایانه نیست بلکه کلیه ادله قابل کسب از دستگاههای الکترونیکی مثل تلفن، تلفن همراه، فاکس، پیجر ، پیام گیر تلفن و ..... را شامل می شود.

بخش دوم: بررسی و شناخت انواع ادله ی الکترونیکی

مقام قضایی رسیدگی کننده به جرایم سایبری، علاوه بر اینکه از ادله منحصر در قانون مجازات یا آیین دادرسی کیفری استفاده می نماید، در صورت وقوع جرایم مذکور می باید با ادله ی الکترونیکی نیز آشنا باشد به دلیل اینکه در مباحث کیفری، سیستم ادله انحصاری وجود نداشته و از هر وسیله ای که قاضی را در کشف جرم کمک نماید، می توان بهره گرفت. آنچه که در حال حاضر در قانون تجارت الکترونیک (ماده ۲) بیان شده، در واقع پایه اصلی این ادله بوده

[1] -دکتر محمد آشوری- آیین دادرسی کیفری- چاپ چهارم – نشر سمت- جلد دوم- ص۲۰۱

[2] - مریم اسماعیلی- مجموعه قوانین و مقررات جرایم رایانه ای- نشر حریر – صفحه۷۲

که می گوید: ((داده پیام، هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی ، نوری و یا فن آوری های جدید اطلاعات ، تولید، ارسال ، دریافت ، ذخیره یا پردازش می شود)) بنابراین محتوای داده پیام می تواند نوشته، صدا، تصویر یا مجموعه ای از آنها و یا هر نماد دیگری از یک واقعیت باشد.اما در یک تقسیم بندی کلی می توان این ادله را به شکل زیر تقسیم بندی نمود:

بند اول: امارات الکترونیکی

در مورد اماره قضایی که بیشتر در حقوق مدنی کاربرد دارد، از آنجا که اموری هستند که به نظر قاضی واگذار شده اند امکان استناد اصحاب دعوی به داده پیامی که متضمن چنین اموری باشد در آیین دادرسی کیفری وجود دارد ،بعنوان مثال چنانچه داده پیام متضمن نوشته ، صدا یا تصویر یا فیلمی باشد که به عنوان سند، اقرار یا شهادت به آن استناد شده باشد، طبق ماده ۱۲ قانون تجارت الکترونیک تشخیص اعتبار آن با دادرس دادگاه می باشد.این وضعیت های رایانه ای که ممکن است به عنوان عناصر دلیل مورد استناد قرار گیرند با توجه به ماهیت در حال تحول فنون رایانه ای جنبه حصری ندارند که برخی از آنها عبارتند از:

- اکران ها – فهرست چاپی – ای میل ها
- فهرست خروجی چاپگرها – میکرو فیلم ها – قالب های نوری
- نوارها و دیسکتهای مغناطیسی – لوح فشرده – فلش حافظه

بند دوم: اسناد الکترونیکی

این اسناد، در واقع مدارکی است که اغلب ویژگیهای اسناد سنتی راحفظ کرده و با عنوانی مشخص و منظم به صورت الکترونیکی تولید، نگهداری، و توزیع می شوند و علاوه بر آن قابلیتهای جستجو، بازیابی، ذخیره سازی اطلاعات، چاپ را به شکلی صحیح و سریع به دست کاربران متعدد می دهند و همواره روز آمد می باشند.[1]این اسناد به سه دسته مطمئن، عادی و

[1]-صادقیان، ناد علی، مقاله اسناد الکترونیکی، شگفت آورترین رسانه ارتباط جمعی، صفحه۶

رسمی تقسیم می شوند که اسناد مطمئن بر اساس ماده ۱۰ قانون تجارت الکترونیکی باید دارای شرایطی از قبیل: منحصر بودن به امضا کننده ، معلوم بودن هویت، صدور آزادانه و ارادی سند،قابلیت تشخیص و کشف را داشته باشد.در نقطه مقابل ، در صورتی که سند به طرق مطمئن مذکور در قانون ایجاد نشده باشد سند الکترونیکی عادی تلقی خواهد شد و چنانچه حاوی شرایط ماده ۱۰ قانون مذکورباشد و توسط مامور رسمی یا با نظارت وی تنظیم شده باشد با سند الکترونیکی رسمی مواجه خواهیم بود.[1]

بند سوم: اقرار الکترونیکی

در قسمت ادله ی الکترونیکی نیز همانندادله ی سنتی به استناد ماده ۱۷۱ قانون مجازات اسلامی، هر گاه متهم اقرار به ارتکاب جرم کند، اقرار وی معتبر است و نوبت به ادله دیگر نمی رسد مگر اینکه با بررسی قاضی رسیدگی کننده قرائن و ا مارات بر خلاف مفاد اقرار باشد که در این صورت دادگاه، تحقیق و بررسی لازم را انجام می دهد و قرائن و امرات مخالف اقرار را در رای ذکر می کند و از طرفی این اقرار هم به صورت لفظ و هم به صورت نوشتن می باشد. بنابراین داده پیامی که به عنوان اقرار مور د استفاده قرار می گیرد اعم از اینکه به صورت نوشته، صدا یا تصویر باشد در صورتی که انتساب آن به مقر احراز شود ، باید مورد پذیرش محاکم قرار گیرد.با این همه اگر داده پیام متضمن اقرار، پیشاپیش توسط یکی از طرفین برای ارائه احتمالی در دادگاه تمهید شده باشد ، چنین اقراری ارزش اقرار خارج از دادگاه را خواهد داشت و در اینجا همانند ماده ۱۶۹ قانون مجازات اسلامی چنانچه قاضی تشخیص دهد که اقرار تحت مواردی مانند اکراه، شکنجه و یا اذیت و آزار روحی باشد، فاقد ارزش و اعتبار بوده و دادگاه مکلف است از متهم تحقیق مجدد نماید.

بند چهارم: شهادت الکترونیکی

در خصوص شهادت قبلاً توضیح داده شد، اما نکته اصلی و مهم این است که ادای شهادت در جرایم سنتی و جرایم الکترونیکی با هم تفاوت دارد، هر چند که برخی اساتید مانند دکتر زرکلام معتقدند که قبول گواهی گواهان به صورت داده پیام با رعایت سایر مقررات راجع به گواهان و

[1] -دوبلفون، زویه لینان ، حقوق تجارت الکترونیک ، ترجمه ی دکتر ستار زرکلام، انتشارات شهر دانش- صفحه۱۹۲

گواهی و نحوه ادای آن وجود دارد، لکن از آنجا که شهادت باید نزد قاضی بوده و در صورت تعذر می توان به صورت تصویری زنده و یا ضبط شده ، آن را با احراز شرایط و صحت انتساب معتبر دانست(مواد ۱۷۴ و ۱۸۶ قانون مجازات اسلامی) در اینگونه جرایم ، از آنجا که شهادت باید معتبر و دارای حجیت باشد، قاضی مکلف است شهادت اشخاصی را بپذیرد که با علوم رایانه ای آشنا داشته باشند ، در غیر این صورت صرف مشاهده یک تصویر دستکاری شده در فضای اینترنت توسط اشخاص عادی قابل شهادت در دادگاه نیست، برای اینکه ممکن است اشخاصی که با این تکنولوژی آشنایی داشته باشند به راحتی متوجه باشند که این تصویر با استفاده از فنون فتوشاپ دستکاری شده و تصویر متعلق به شخص دیگری باشد. قانون آیین دادرسی کیفری سال ۱۳۹۲ در تبصره ۲ ماده ۲۰۴ می گوید: ((در صورتی که دلیل پرونده منحصر به شهادت شهود و مطلعان نباشد، تحقیق از آنان می تواند به صورت الکترونیکی و با رعایت مقررات راجع به دادرسی الکترونیکی باشد))، بنابراین قانونگذار در این ماده با مفهوم مخالف بیان می کند که شهادت الکترونیکی به تنهایی از نظر دادگاه جزایی قابل قبول نیست. اما قانونگذار یک استثنا برای این موضوع قائل شده و در بند پ ماده ۲۱۴ همین قانون گفته که هر گاه بیم خطر جانی یا حیثیتی و یا ضرر مالی برای شاهد یا مطلع ویا خانواده آنان وجود داشته باشد ، استماع اظهارات شاهد یا مطلع خارج از دادسرا با وسایل ارتباط از راه دور با ذکر علت در پرونده اتخاذ می شود. قانونگذار در این ماده به بازپرس اجازه داده که از ابزارهای الکترونیکی برای استماع شهادت استفاده کند و تعریفی نیز از آن ارائه نداده است. البته این کار احتمال بروز خطراتی در خصوص شناسایی شاهد را داشته که بازپرس پرونده می باید به نحو مقتضی اطمینان حاصل کند که تقلبی در کار نبوده و شاهد واقعی می باشد و حتی برای این کار می تواند از کارشناسان فنی کمک بگیرد.

بند پنجم: سوگند الکترونیکی

به دو دلیل استفاده از سوگند در فضای سایبری وجود ندارد، اول اینکه به صراحت ماده ۲۰۸ قانون مجازات اسلامی حدود و تعزیرات با سوگند نفی یا اثبات نمی شود و چون مجازاتهای مربوط به جرایم سایبری ، از نوع تعزیرات حکومتی ومجازاتهای بازدارنده می باشد، لذا،سوگند در این فضا کاربرد ندارد، دوم، اینکه داده پیامی که متضمن سوگند از پیش تمهید شده است در

مقابل قاضی قابلیت استناد ندارد و باید آن را از شمول ماده ۱۲ قانون تجارت الکترونیکی خارج دانست.

بند ششم: امضا الکترونیکی

با توجه به کارکرد متفاوت امضا الکترونیکی در مقایسه با سایر داده پیامهای متضمن دلیل و نیز نحوه ایجاد و مستند سازی آن ، لازم است در این خصوص توضیح بیشتری داده شود. بر اساس ماده ۷ قانون تجارت الکترونیکی ، هر گاه قانون وجود امضا را لازم بداند، امضای الکترونیکی کافی است و از طرفی این امضا عبارت از هر نوع علامت منضم شده یا به نحو منطقی متصل شده به داده پیام است که برای شناسایی امضا کنند ه داده پیام مورد استفاده قرار می گیرد. بر همین اساس چنانچه داده پیام به تنهایی یا به کمک سایر دلایل شناسایی امضا کننده و التزام او به مفاد داده پیام را ثابت کند قاضی آن را به عنوان امضای الکترونیکی معادل با کارکرد امضای دستی بپذیرد. اما در خصوص انواع امضا الکترونیکی، لازم به ذکر است که قانون تجارت الکترونیکی دو سطح مختلف از امضای الکترونیکی را پذیرفته است. اول امضای الکترونیکی که می توان آن را ساده یا عادی نامید که همان امضایی است که به طرق مقرر در قانون ایجاد نشده باشد و دوم ((امضا الکترونیکی مطمئن)) که مطابق ماده ۱۰ قانون تجارت الکترونیک باید شروط مقرر در قانون را داشته باشد.

بخش سوم: شرایط استناد پذیری ادله الکترونیکی

مرجع قضایی مکلف است دلایل و مدارک ارائه شده از جانب طرفین دعوی کیفری یا مجریان قانون ،شهود و کارشناسان را بررسی و نسبت به میزان اعتبار و محکمه پسند بودن آنها تعیین تکلیف نماید. در واقع ((استناد پذیری ادله الکترونیکی در مراجع قضایی مستلزم این است که اطمینان کافی از وجود حداقل شرایط فنی لازم در رابطه با تضمین صحت این اسناد برای این مراجع وجود داشته باشد))[1] به عبارت دیگر باید هویت پدید آورنده این ادله الکترونیکی معلوم بوده ودلایل مذکور از ویژگی اصالت، صحت، تمامیت، محرمانگی ،اعتبار وانکارناپذیری

[1] – کامران شیرازد، جرایم رایانه ای از منظر حقوق جزای ایران و حقوق بین الملل– نشر بهینه فراگیر، چاپ اول. سال ۸۸– ص۱۵۸

برخورداراباشد. درهمین ارتباط فصل سوم جرایم رایانه ای قانون مجازات اسلامی در مواد ۷۷۷ تا ۷۷۹ در ارتباط با استناد پذیری ادله الکترونیکی صحبت به میان آورده است. ماده ۷۷۷ قانون مجازات اسلامی می گوید: ((به منظور حفظ صحت و تمامیت، اعتبار و انکار ناپذیری ادله الکترونیکی جمع آوری شده ، لازم است مطابق آیین نامه مزبور از آنها نگهداری بعمل آید.همچنین آیین نامه جمع آوری و استناد پذیری ادله ی الکترونیکی بعد از پنج سال در تاریخ ۱۳۹۲/۵/۱۲ به تصویب ریاست محترم قوه قضائیه رسیده و از طریق روزنامه رسمی انتشار یافته است.

بند اول: ارکان و شرایط مورد نیاز

به منظور تشریح این موارد، ناگزیر از مراجعه به دکترین قضایی و کتب تهیه شده توسط اساتید فن و یا مراجعه به قانون آیین دادرسی مدنی در بحث استناد پذیری ادله مدنی و کمک گرفتن از آنها خواهد بود که در ادامه مفاهیم مرتبط با آن مورد بررسی قرار خواهد گرفت.

۱. احراز هویت

اولین مرحله در هر اقدام حقوقی چه در روابط قراردادی و غیر آن، احراز هویت طرفین معامله و در موضوعات کیفری منجمله ادله ی الکترونیکی شناخت هویت ارائه کننده سند و یا سازنده سند می باشد که مراجع قضایی می باید به آن اهتمام بورزند.در واقع به لحاظ حقوقی، مهمترین موضوع اثبات رابطه سند یا داده پیام با کسی است که این دلیل به او نسبت داده شده است. در خصوص شناخت هویت پدید آورنده ادله الکترونیکی گفته شده که ویژگیهای منحصر به فرد فناوری اطلاعات و ارتباطات ، ناشناختگی است ، یعنی در محیطی فعالیت های گوناگون انجام می شود که امکان انتساب فعل به پدید آورنده به آسانی میسر نیست.برای مثال هنگامی که متنی در محیط واژه پرداز یک سیستم رایانه ای تایپ می شود ،تنها چیزی که انعکاس می یابد،یک شیوه نگارش تعریف شده مانند zarیا yagut می باشد که مطابق تنظیمات کاربر در سند الکترونیکی درج می شود .اما تنها با مطالعه آن سند نمی توان به پدید آورنده آن پی برد، زیرا هر کاربر با استفاده منطقی و نظام یافته صفحه کلید، می تواند پدید آورنده باشد.البته همه اسناد ایجاد شده در محیط واژه پرداز به نام کسی که به هنگام نصب برنامه نامش درج شده ، ثبت می

شوند.بنابراین با اینکه قرینه خوبی است، اما اطمینان بخش نیست بویژه آنکه سیستم رایانه ای برای افراد زیادی قابل دسترسی می باشد. سوالی که مطرح می شود این است که اگر به جای یک سیستم رایانه ای محدود به زمان ومکان که به هر حال با مراجعه به امارات دیگر، می توان به پدیدآورنده اصلی ظنین شد، گستره ای به اندازه فضای سایبر پیش رو قرار گیرد، چه رخ می دهد؟برای مثال ، در محیط های گفتگو از قبیلchat rooms هر کس می تواند با انواع هویت های مجعول که برای خود انتخاب می کند با دیگر افراد کره زمین ارتباط برقرار کند، کاری که نیاز به مهارت خاص نداشته و با ایجاد یک ایمیل وارد فعالیت های شبکه ای می شود. برای حل این مشکل ، قانونگذار در مواردی مانند امضا الکترونیکی، دفاتر الکترونیکی را ایجاد نموده اند که مثل دفاتر خدمات دولت الکترونیک تمامی مراحل ورود از قبیل احراز هویت امضا کنندگان سند و طی تشریفات قانونی به نوشته سندیت و رسمیت می بخشند و هویت امضا کننده را تضمین می کنند و نتیجتاً به اطلاعات الکترونیکی سندیت می دهند.این مراجع در راستای اجرای ماده ۳۱ قانون تجارت الکترونیکی تشکیل و مطابق این ماده:((دفاتر خدمات صدور گواهی الکترونیکی واحدهایی هستند که برای ارائه خدمات صدور امضای الکترونیکی تاسیس می شوند.این خدمات شمال تولید، صدور، ذخیره، ارسال، تایید، ابطال و به روز نگهداری گواهی های اصالت امضای الکترونیکی می باشد))، در واقع روش کار این دفاتر بدین صورت است که ابتدا تخصیص یک کلید خصوصی به دارنده و ثبت آن به عنوان یک مستند اطلاعاتی نموده و سپس نگهداری کلید مکمل به نام کلید عمومی و در دسترس قراردادن فهرست نامه دارندگان کلید عمومی از طریق سیستم درون خطی و بانکهای اطلاعاتی ویژه[۲]را انجام می دهند.

۲. اعتبار

دومین اصلی که رعایت آن در کنار سایر ادله موجب استناد پذیری آنها می شود، اعتبار است و مقصود از اعتبار ادله الکترونیکی آن است که این ادله تا چه حد ارزش حقوقی و اثباتی دارند و

-جلالی فراهانی- امیر حسین، استناد پذیری ادله الکترونیکی ، مجله فقه و حقوق- صفحه ۹۰-۸۹

-زرکلام، ستار، امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوی، مجله مدرس علوم انسانی، سال ۸۲، دوره هفتم، صص ۴۱و۴۲

آیا می توان آنها راهم سنگ مدارک کاغذی محسوب نمود؟ ماده ۶ قانون تجارت الکترونیک با تایید این کارکرد یکسان، مقرر می دارد که هر گاه وجود نوشته از نظر قانون لازم باشد جزدر موارد استثنایی ، داده پیام در حکم نوشته است. در حقوق ایران ، علاوه بر ماده ۶ و ۸ قانون تجارت الکترونیک، بنابر ماده ۹ ،((جایگزینی اسناد کاغذی به جای داده پیام اثری بر حقوق و تعهدات قبلی طرفین نخواهد داشت)) و سرانجام ماده ۱۲ این قانون به گونه ای تدوین یافته که هر گونه شک و شبهه ای را در باب اعتبار مدارک و اسناد الکترونیکی به صورت شکل و قالب الکترونیکی آنها مرتفع می سازد: ((اسناد و ادله اثبات دعوی ممکن است به صورت داده پیام بوده و در هیچ محکمه یا اداره دولتی نمی توان بر اساس قواعد ادله موجود، ارزش اثباتی داده پیام را صرفاً به دلیل شکل و قالب آن رد کرد)).[1]نتیجه اینکه چنانچه نتوان در فضای مجازی ، اعتبار ادله را به اثبات رساند، با مشکلات جدی قانونی مواجه خواهیم بود وباعث برهم خوردن نظم اجتماعی و تضییع حقوق اشخاص خواهد شد، برای مثال فرض بفرمایید که شخصی با ارسال پیامک های تهدید آمیز یا استفاده از الفاظ رکیک موجبات مزاحمت دیگران را فراهم سازد و در نقطه مقابل مرجع قضایی، پرینت گرفته شده از مخابرات را بعنوان دلیل فاقد اعتبار بداند که با توضیح داده شده، از قابلیت این اسناد کاسته و یا نادیده گرفته خواهد شد.

بند دوم: تمامیت

داده های الکترونیک می باید دست نخورده باقی مانده، به این معنا که شکل نهایی سند کامل و بدون تغییر بماند، هم در اسنادی که ازابتدا به صورت الکترونیکی بوجود آمده اند و هم اسنادی که از شکل کاغذی به شکل الکترونیکی تبدیل شده اند و به عبارتی باید زنجیره حفاظتی در مورد آنها رعایت شود. بند هـ ماده ۲ قانون تجارت الکترونیکی در تعریف تمامیت گفته: ((تمامیت داده پیام(Integrity) عبارت است از موجودیت کامل و بدون تغییر داده پیام .اعمال ناشی از تصدی سیستم از قبیل ارسال، ذخیره یا نمایش اطلاعات که به طور معمول انجام می شود خدشه ای به تمامیت داده پیام وارد نمی کند))، به موجب این ماده ارسال، ذخیره و نمایش داده ها خدشه ای به تمامیت آنها وارد نمی نماید. بند د ماده ۱۰ همین قانون در مورد شرایط امضاء الکترونیکی مطمئن بیان داشته که امضاء الکترونیکی باید به گونه ای به داده پیام متصل

[1]-دکتر السان، مصطفی، حقوق بانکداری اینترنتی، پژوهشکده پولی و بانکی ، چاپ دوم، صفحه ۲۸۰

شود که هر تغییری در داده پیام قابل تشخیص باشد. در نتیجه امضا الکترونیکی در تمامیت داده ها نقش بسزایی دارد.بر همین اساس چون تغییر در داده پیام ها آسان تر از اسناد کاغذی انجام می شود، باید ساز و کاری اتخاذ نمود که تمامیت یک پیام را تضمین نمود که یکی از این موارد استفاده از نرم افزارهای خاص خود و دیگری تبدیل آن به یک چکیده است . این اثر اطلاعات طولی ثابتی است که به کمک یک الگوریتم کوچک کننده(خرد کردن اطلاعات) به دست می آید. مقایسه این ردپا در آغاز و پایان تمامیت پیام را تضمین می کند زیرا کمترین تفاوت به اثرات متفاوت می انجامد و بنابراین ضرورتی ندارد چکیده ها خیلی سنگین باشد.[1]اثبات تمامیت سیستم های اسناد الکترونیکی را بر اساس موارد ذیل می توان ثابت نمود:

الف- با ادله ای که می تواند نشان دهد سیستم رایانه ای یا دیگر دستگاه های مشابه مورد استفاده سیستم اسناد الکترونیکی در زمان های مربوطه صحیح عمل می کرده و در غیر این صورت عدم صحت عملکرد آن تاثیری بر تمامیت اسناد الکترونیکی نداشته و زمینه های منطقی دیگری برای تردید در تمامیت سیستم اسناد الکترونیکی وجود ندارد.

ب- اگر اثبات گردد که سند الکترونیکی بوسیله طرف دعوایی ثبت، ضبط یا ذخیره شده که منافع وی مخالف منافع طرفی است که خواهان ارائه آن می باشد ، یا

ج- اگر اثبات گردد که سند الکترونیکی در روال عادی و معمولی فعالیت شغلی بوسیله فردی ثبت، ضبط یا ذخیره شده باشد که طرف دعوی نبوده و آن را تحت نظارت طرف دعوایی که قصد ارائه آن را دارد، ثبت ، ضبط یا ذخیره نموده است.[2]

بند سوم: قابلیت دست یابی

نگهداری ادله الکترونیکی یک ابزار تحقیقاتی مهم در پی جویی جرایم رایانه ای و کشف حقیقت می باشد و این دلایل زمانی قابلیت استناد را دارد که قابل ارائه باشد و از بین رفتن آنها می تواند مشکلات جدی در خصوص دست یابی به آنها ایجاد نماید، برای همین است که داده

[1] . دکتر زرکلام، ستار، حقوق تجارت الکترونیک ، نشر دانش، صفحه ۱۷۰

[2] -جزوه آموزش ادله، کمیته مبارزه با جرایم رایانه ای قوه قضاییه ، ترجمه: مسیب رمضانی، صفحه ۱۷۴و۱۷۵

پیامهایی مثل مکالمات تلفنی که فاقد قابلیت دست یابی مجدد باشد را نمی توان سند و یا در حکم سند دانست مگر اینکه شرایط ماده ۴۷ آیین نامه را داشته باشد.مواد ۷۶۰ الی ۷۶۳ قانون مجازات اسلامی در همین ارتباط وظایفی در ارتباط با نگهداری و حفاظت از داده های رایانه ای و اطلاعات کاربران برای ارائه کنندگان خدمات میزبانی و دسترسی تعیین کرده است. ((ممکن است ارائه کنندگان خدمات مذکور پس از مدت کمی داده ها را از بین ببرند و یا سامانه به نحوی باشد که پس از ایجاد داده جدید، داده قبلی به طور خودکار از بین برود.اطلاعات کاربران نیز معمولاً پس از خاتمه اشتراک از بین رفته و به طور منظم و در محلهای مناسب نگهداری نمی شوند)) دلیل عمده این امر ، حجم وسیع و گسترده این داده ها واطلاعات می باشد که با توجه به محدودیت رسانه های ذخیر سازی ، نمی توان به نحو صحیح و مطلوبی از چنین داده ها و اطلاعاتی درجهت اثبات جرایم رایانه ای بهره برداری لازم وکافی را نمود، برای همین ارائه دهندگان خدمات دسترسی و خدمات میزبانی داخلی وخارجی و نمایندگان داخلی ارائه دهندگان خدمات میزبانی خارجی بر اساس ماده ۷۶۰ قانون مجازات اسلامی و مواد ۴ و ۵ آیین نامه مذکور موظفند اطلاعات کاربران خود را حداقل شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا ۱۵ روز نگهداری نمایند.

بند چهارم: استثنای پذیرش طرف دعوی

در برخی از نظامهای حقوقی منجمله حقوق عرفی برای اینکه ادله ارائه شده به دادگاه از اعتبار بالایی برخوردار باشد، تنها در صورتی پذیرفته می شود که شخص بر اساس علم یا آگاهی خودش آن را بدست آورده باشد.بنابراین آگاهی ناشی از منابع ثانویه مانند دیگر اشخاص، کتابها یا سوابق در مجموع در قالب ادله ای به نامه ادله سماعی قرار می گیرند که معتبر و استناد پذیر نیستند. با این حال اجرای بی چون و چرای این قاعده بویژه در عصر حاضر و نسبت به جلوه های نوین اطلاعات منطقی به نظر نمی رسد و به همین دلیل با توجه به موارد مذکور، موارد استثنای مهمی براین قاعده وارد شده است. ماده ۷۷۸ قانون مجازات اسلامی در خصوص این استثنا است که می گوید: ((چنانچه داده های رایانه ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی

[1] - زندی، محمد رضا، تحقیقات مقدماتی در جرایم سایبری، انتشارات جنگل، چاپ اول، ۱۳۸۹، صفحه ۱۴۳

نداشته ، ایجادیا پردازش یا ذخیره یا منتقل شده باشد و سامانه رایانه ای یا مخابراتی به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکار ناپذیری داده ها خدشه وارد نشده باشد ، قابل استناد خواهد بود)) در توضیح این ماده باید گفت که این استثنا ریشه در دنیای فیزیکی داشته و با این مبنا مطرح می شود که اگر دلیلی توسط طرف دعوی به وجود آید علیه خودش قابل استناد است، زیرا نوعی اقرار به شمار آمده و معتبر است. قاعدتاً یک انسان عاقل وقایعی را که به وضعیت قانونی اش لطمه بزند یا مسوولیتی را متحمل شود نخواهد پذیرفت مگر اینکه آن وقایع صحیح باشند.همچنین می توان به دلایل ایجاد شده توسط فردی که هیچ نقشی در دعوای مورد نظر ندارد و تحت نظر طرف ذی نفع دعوا ادله را ایجاد نکرده باشد، استناد کرد.[1]

بخش چهارم: نحوه استناد به ادله در فرآیند دادرسی کیفری

همانگونکه گفته شد برای اینکه ادله الکترونیکی قابل استناد باشد، بایستی یکسری تشریفات قانونی و مقدماتی در خصوص آن رعایت شده باشد.به همین منظور در این بخش در نظر است در دو قسمت توضیح داده شود که نحوه عملکرد ضابطان قضایی و بعضی همکاران مرتبط با آنها در جمع آوری ادله و ارائه آن به چه صورت بوده و از طرف دیگر مقامات قضایی در صورت احراز اصالت و اطمینان ادله بر چه اساس اقدام به صدور قرار مجرمیت در دادسرا و نهایتاً رای محکومیت در دادگاه می نمایند .آنچه که وظیفه هر دو اینها را با اهمیت جلوه می نماید ، لزوم احراز اصالت ، اعتبار و..... ادله بوده که آیین نامه راجع به جمع آوری و استناد پذیری ادله الکترونیکی مصوب قوه قضاییه که به تصویب نهایی و ابلاغ رسیده، وظایفی را در مواد مختلف آن برای ظابطان قضایی تعیین نموده و مطالعات انجام شده در آیین نامه نشان می دهد که بعضی از مواد آن به شکل ترجمه از قوانین سایر کشورها و یا روشهای اجرایی آنها بوده که در تمامی سیستمهای قضایی و انتظامی به صورت یکسان اجرا شده مثل اصطلاح معروف ((زنجیره حفاظتی)) که در مقررات بعضی کشورها مشترک بوده و در مباحث بعدی به آن اشاره خواهد شد.

[1] جلالی فراهانی- امیر حسین، استناد پذیری ادله الکترونیکی ، مجله فقه و حقوق- صفحه۹۹

بند اول: مرحله کشف جرم

در قانون جرایم رایانه ای(یا همان مواد قانون مجازات اسلامی) و آیین نامه مربوطه، دسته خاصی از ضابطان برای جمع آوری، مداخله، تفتیش ، توقیف و حفظ و نگهداری داده ها از ساما نه های رایانه ای و مخابراتی به طور خاص پیش بینی نشده و طیف وسیعی از ضابطان را در بر می گیرد، هر چند که در بند ز ماده یک آیین نامه صرفاً به تعریفی از ((مجری حفاظت)) پرداخته که به اشخاصی گفته می شود که به نحوی داده های رایانه ای ذخیره شده را تحت تصرف و کنترل دارد و مطابق ماده ۳۴ قانون و سایر قوانین و مقررات جهت حفاظت آنها تعیین می شود.بهتر بود که ماموران پلیس فضای تولید و تبادل اطلاعات ایران(فتا) به عنوان مقام صلاحیت دار در قانون احصا می شد، چون باید ضابطان دادگستری به نحو دقیق و شایسته ای با شیوه صحیح در اختیار گرفتن داده ها و سامانه های مذکور آشنا باشند ، شاید دلیل دیگر این باشد که ضابطان قضایی بعنوان یکی از کنشگران اصلی فرآیند کیفری که جامعه آنها را به خدمت گرفته باید در اجرای عدالت به نظام قضایی کمک نموده و برای اینکه از چارچوب ضوابط قانونی فراتر نروند و به نحو شایسته عمل کنند در عین حال از یکسری اختیارات قانونی نیز برخوردار باشند. برای همین ضرورت اقتضاء می نماید که برای آنها قواعد خاصی پیش بینی گردد. از جمله مهمترین اقدامات تعریف شده برای ضابطانن، این است که برای اینکه ادله ارائه شده از سوی ضابطان قضایی و مقامات تعقیب استناد پذیر باشد، باید علاوه بر مقررات مندرج در قانون ، زنجیره حفاظتی نیز در مورد آنها رعایت شده باشد. برابر بند هـ ماده یک آیین نامه مذکور: ((زنجیره حفاظتی مجموعه اقداماتی است که ضابط دادگستری و سایر اشخاص ذی صلاح به منظور حفظ صحت ، تمامیت، اعتبار و انکار ناپذیری ادله الکترونیکی با بکارگیری ابزارها و روش های استاندارد در مراحل شناسایی ، کشف، جمع آوری ، مستند سازی، تجزیه و تحلیل و ارائه آنها به مرجع مربوط به اجرا در آورده و ثبت می کنند به نحوی که امکان ردیابی آنها از مبدا تا مقصد وجود داشته باشد.)).به عبارت دیگر در این فرآیند باید چهار مرحله زیر به ترتیب به اجرا در آمده باشند:

۱. شناسایی

حقوق شکلی را باید اصلی ترین قربانی جرایم سایبری(الکترونیکی) تلقی نمود به این دلیل که به واسطه این جرایم به شدت تحت تاثیر قرار گرفته و به بن بست رسیده است.کشف، تحقیق و

تعقیب جرایم در این محیط بسیار دشوار است و بسیاری از جرایم در این فضا عملاً کشف نمی شوند و رقم سیاه جرایم کشف نشده در این حوزه بسیار زیاد است و از سوی دیگر هنوز روش اثبات شده ای برای نظارت موثر براین فضا ایجاد نشده و مواردی نظیر پلیس سایبر یا همان پلیس فتا و حتی روشهای نظارت فنی کافی نیست. همچنین روشهای تکنولوژیک و فناوریهای نوین این امکان را به مجرمین می دهد که آثار جرایم خود را استتار کنند به طوریکه راهکارهای جدیدی برای «نهان سازی جرایم رایانه ای» در این فضا ایجاد شده اند که این امکان را به مجرمین می دهد تا از طریق روش هایی چون رمزنگاری در ظاهری قانونی مرتکب جرم بشوند، از طرفی در بسیاری از موارد حتی پس از کشف جرم، مجرم کیلومترها دور ازدسترس مقامات اجرای قانون و مقامات قضایی بوده و شناسایی او مشکل می باشد.اما در فرآیند شناسایی باید سه موضوع به شرح ذیل مورد توجه قرار گیرد:

الف) شناسایی پدید آورنده سوابق ذخیره شده الکترونیکی

با اینکه ممکن است سوابق دست نویس به گونه ای متمایز ازشیوه های نوشتاری نگارش یابند، اما نمونه های ذخیره شده در رایانه حاوی یک سلسله طولانی صفر و یک هایی است که ضرورتاً نمی توان پدید آورنده آن را شناسایی کرد.این یک معضل ویژه ارتباطات اینترنتی است که به پدید آورندگان تا حد غیر عادی گمنامی اعطا می کند .برای مثال ، فناوریهای اینترنتی به کاربران این امکان را می دهد که به طور کاملاً ناشناخته رایانامه ارسال کنند و کانال های گپ نوبتی اینترنتی نیز به کاربران اجازه می دهند بدون آنکه نام واقعی شان ذخیره شود ، ارتباط برقرار کنند.درجایی که ضابطین قضایی به دنبال تایید اینگونه سوابق ذخیره شده علیه متهم هستند، ممکن است متهم از طریق زیر سوال بردن هویت پدید آورنده سابقه ادعا کند که اعتبار کافی ندارد.برای حل این مشکل ، ضابطین می باید با کمک گرفتن از کارشناسان دادگستری و سایر شرایط و اوضاع و احوال و به عبارتی ادله ضمنی، راهکاری ارایه دهند که نویسنده واقعی و اعتبار سابقه رایا نه ای را ثابت می کند.[۲]

[۱]-مهدی فضلی، مسوولیت کیفری در فضای سایبر، معاونت حقوقی و توسعه قضایی قوه قضاییه ، ص۷۴

[۲]-امیر حسین جلالی فراهانی- تفتیش و توقیف رایانه ها و تحصیل دلایل الکترونیکی در تحقیقات کیفری- معاونت حقوقی قوه قضاییه- ص۲۲۱

ب) شناسایی سخت افزار

در بسیاری از انواع جدید وسایل الکترونیک که در اختیار مصرف کنندگان امروزی قرار می گیرد ، ادله الکترونیک را می شود پیدا نمود ، بعبارتی این ابزار می توانند ادله مزبور را نگهداری نمایند، مثل تلفن های دیجیتال، کامپیوترهای قابل حمل،کامپیوترهای رومیزی، سرورهای بزرگ و ابر کامپیوتر و اشکال متنوع دیگری مثل لوح های فشرده، نوارهای مغناطیسی و وسایل حامل ادله مثل سیم ها ، کابل ها که با ا بزارهای مناسب می توان آنها را جمع آوری و برای بررسی های بعدی ذخیره کرد.

پ) شناسایی ادله دیجیتال

این مرحله اصولاً به نوع جرم ارتکابی بستگی دارد.بدیهی است دلایل بجا مانده از جرمی فیزیکی مانند قتل، کلاهبرداری و تجاوز به عنف در سیستم های رایانه ای با دلایل بجا مانده از جرایمی نظیر دسترسی غیر مجاز یا تعقیب ایذایی سایبری متفاوت هستند.در تمامی آنها لازم است تنها دلایل مرتبط با قضیه جمع آوری شوند والا علاوه بر دردسرهایی که به دلیل آمیختگی ادله مرتبط با غیر مرتبط برای مجریان قانون به وجود خواهد آمد،مشکلات حقوقی نیز گریبانگیرشان خواهد شد.برای همین ضابطین قضایی از ابتدا باید توجه کنند که در خصوص چه جرمی تحقیق می کنند و به دنبال چه چیزی هستند.[1]

۲. حفاظت، جمع آوری و مستند سازی

منظور از محافظت ، این است که از هر گونه تغییری در آنها جلوگیری شود.هم اکنون ابزارهای زیادی وجود دارد که می توان از آنها برای جمع آوری و محافظت مناسب ادله الکترونیک به نحوی که از نظر مراجع قضایی قابل قبول باشند استفاده کرد مانند فرآیند کپی برداری ازدیسک های ارائه شده که می تواند از فضاهای راکد و تخصیص نیافته تصویر برداری انجام دهند که در نتیجه اطمینان حاصل می شود هیچ چیز مغفول نمانده است.مواد ۱۰ تا ۱۶ آیین نامه استناد پذیری ادله الکترونیکی به این موضوع اختصاص داشته و در ماده ۱۶ به صراحت بیان نموده که ((

[1]-امیر حسین جلالی فراهانی- درآمدی بر آیین دادرسی کیفری جرایم سایبری- معاونت حقوقی قوه قضاییه – ص ۲۵۷

حفاظت از داده ها باید به نحوی باشد که محرمانگی، تمامیت، صحت، انکارناپذیری داده ها رعایت شود))، در ادامه ماده ۱۸ آیین نامه نیز می گوید که ارائه داده ها باید بنحوی باشد که محرمانگی، تمامیت، صحت و انکارناپذیری داده ها رعایت شده و حتی الامکان بدون ایجاد مانع برای فعالیت سامانه و با روش متعارف و کم هزینه باشد)) جمع آوری ادله و جستجو از صحنه جرم الکترونیکی به موجب ماده ۱۱ آیین نامه نیاز به مجوز قضایی دارد.ادله ی الکترونیکی همانند دیگر ادله ها باید به دقت و به شکلی جمع آوری شود که ارزش ادله ی آن حفظ و باقی بماند.این عمل نه تنها در ارتباط با جامعیت فیزیکی یک مورد یا وسیله بوده، بلکه با داده الکترونیکی که دارا می باشد مرتبط است.از این جهت انواع خاص ادله الکترونیکی نیاز به جمع آوری، بسته بندی و حمل و نقل ویژه دارند.باید توجه داشت که از داده هایی حفاظت بعمل بیاید که ممکن است در برابر میدان های مغناطیسی ـ الکتریسیته، آسیب یا تغییراتی ببینند، نظیر تغییرات یا آسیب هایی که توسط الکتریسیته ساکن، آهن رباها ،فرستنده های رادیویی یا دیگر وسایل بوجود می آیند.این ادله را باید طبق دستور العملهای مر بوط به پلیس فتا جمع آوری کرد.تصور بر این است که قبل از جمع آوری ادله ، تعیین محل قطعات و مستند سازی آنها انجام گیرد.همچنین باید مشخص شود که انواع ادله دیگری همانند پرینتهای قابل ردیابی، بیولوژیکی یا مخفی ممکن است وجود داشته باشد.ضمناً باید روش های مخرب را (همانند استفاده از مواد شیمیایی در ظهور اثر انگشت) تا قبل از بازیابی ادله الکترونیک را بکار نبرد. مورد بعدی دراین خصوص ، مستند سازی ادله توسط ضابطان قضایی است ،بدین معنی که هدف اصلی از مستند سازی ادله این است که اثبات شود آنها در همان وضعیت اصلی خود قرار دارند و موجب ثبت آن واقعه در تاریخ برای همیشه خواهد بود.ثبت صحیح محل و وضعیت کامپیوترها ، وسایل ذخیره، دیگر وسایل الکترونیکی و ادله ی قراردادی حائز اهمیت می باشد در غیر این صورت بروز کوچکترین اشتباهی ممکن است با استناد ناپذیر بودن دلایل مواجه شوند که به معنی هدر رفتن تمامی زحمات ضابطان خواهد بود.در ماده ۴۳ آیین نامه مورد اشاره آمده که : ((ضابطان قضایی و سایر ماموران در حدود وظایف قانونی در شروع تفتیش و توقیف باید صورت وضعیت اولیه ای از سامانه رایانه ای یا مخابراتی و اجزای آن و کلیه اتصالات کابلی بین اجزای مختلف سخت افزارها و حامل های داده متصل به آن که علامت گذاری وثبت می شوند را تنظیم و به امضای تفتیش کننده یا توقیف کننده و متصرف قانونی که سامانه تحت کنترل اوست یا قائم

مقام قانونی وی برسانند.برای ضبط دقیق مشخصات ابزار و اجزای آن تصویر برداری بلامانع است))در ادامه و در ماده ۴۵همین آیین نامه آمده که دستور العمل حقوقی و فنی جمع آوری ادله و توقیف سامانه های رایانه ای و مخابراتی توسط دادستانی کل کشور با همکاری نیروی انتظامی تهیه و به تصویب دادستان کل کشور می رسد، این دستور العمل باید در بردارنده چگونگی حفظ صحنه جرم و جمع آوری ادله از سامانه در حال اجرا ، خاموش و روشن کردن سامانه، بسته بندی و انتقال اطلاعات و نیز نمونه درخواست های مرتبط با این موارد باشد.)) همچنین ماده ۴۴ آیین دادرسی کیفری سال ۱۳۹۲، ضابطین قضایی را مکلف نموده که در مورد جرائم مشهود تمامی اقدامات لازم را به منظور حفظ آلات، ادوات، آثار، علائم و ادله وقوع جرم و جلوگیری از فرار یا مخفی شدن متهم و یا تبانی به عمل می آورند.و اگر شاهد یا مطلعی در صحنه وقوع جرم حضور داشته باشد، اسم، نشانی، شماره تلفن و سایر مشخصات ایشان را اخذ و در پرونده درج کنند. در ادامه در ماده ۵۷ همان قانون ،آمده است که چنانچه ضابطان دادگستری در هنگام بازرسی محل، ادله ، اسباب و آثار جرم دیگری را که تهدید کننده امنیت و آسایش عمومی جامعه است مشاهده کنند ، ضمن حفظ ادله و تنظیم صورت مجلس بلافاصله مراتب را به مرجع قضائی صالح گزارش و وفق دستور وی عمل می کنند.

۳. طبقه بندی، مقایسه و ماهیت انگاری

طبقه بندی ادله فرآیندی است که بر اساس آن ویژگی هایی کشف می شود و می توان از آنها جهت بیان موضوعات کلی استفاده کرد و آن را از میان نمونه های مشابه تمیز داد. زمانی یک موضوع طبقه بندی شده محسوب می گردد که بتوان آن را در طبقه ای از موضوعات با ویژگی های مشابه قرار دارد.به عنوان مثال سلاح گرم براساس کالیبر و ویژگی های خان آن و بر اساس اندازه و شکل آن طبقه بندی می شود. در حوزه ادله الکترونیک ، به عنوان مثال اکثر افراد با پست الکترونیکی آشنا دارند و می توانند به راحتی آن را شناسایی کنند. اما مجریان قانون باید قدری فراتر روند و بتوانند پس از کسب آموزش های لازم، پست های الکترونیک را بر اساس موضوعات دقیق تری طبقه بندی و حتی مشخص کنند که با کدام برنامه ایجاد شده است.همچنین ، طرح های گرافیکی کامپیوتری از بسیاری زوایا مشابه یکدیگرند.اما آنها را نیز می توان بر

اساس الگوهای متفاوت مانند Gif، JPG بهتر تفکیک کرد.[1] با اینکه فرآیند مذکور، به نوعی طاقت فرسا می باشد، اما در ارزیابی دقیق و مفصل آنها از اهمیت خاصی برخوردار است.چنانچه این اقدامات به شایستگی اجرا شود بسیار احتمال دارد که نشانه هایی هر چند جزئی که از پیوند اساسی با موضوع مورد نظر برخوردارند کشف گردند. همچنین، این فرآیندها می توانند در تبیین هر چه بهتر ادله در محضر دادگاه نقش حساسی ایفا کنند.زیرا از آنجا که این موضوعات جدید محسوب می شوند و در عین حال دادگاه ها با آسیب پذیری های این حوزه بیشتر از مطلوبیت های آن آشنا شده اند، مترصد فرصتی هستند تا ادله الکترونیکی را از عداد دلایل خارج سازند، چنانچه با یک فرآیند اجرایی صحیح و دقیق مواجه گردند، قطعاً به آن ترتیب اثر خواهند داد.

٤. ارائه داده

یکی از وظایف ضابطان قضایی، ارائه داده ها و اطلاعات جمع آوری شده از صحنه جرم به مقام قضایی می باشد که بر اساس ماده ۱۷ آیین نامه ، دستور ارائه توسط مقام قضایی صادر می شود و باید به طور صریح،شفاف و مشتمل بر شخص ارائه دهنده، موضوع و نوع داده ها، زمان تحویل داده ها و مرجع تحویل گیرنده باشد . در ادامه ماده ۱۸آورده که ارائه داده ها باید به نحوی باشد که محرمانه بودن، تمامیت، صحت و انکار ناپذیری داده ها رعایت شده و حتی الامکان بدون ایجاد مانع برای فعالیت سامانه و با روش متعارف و کم هزینه و شیوه های مندرج در آن باشد که قبلاً از آن نام برده شده است. شیوه های ارائه داده طبق این ماده عبارتند از:

الف- تحویل یک نسخه چاپ شده از داده

ب- تحویل یک نسخه رایانه ای از داده

ج- ایجاددسترسی به داده

د- انتقال تجهیزات رایانه ای و مخابراتی

[1]-کیسی، اوئن ،دلایل دیجیتالی و جرم رایانه ای، مترجمان امیر حسین فراهانی و علی شایان، معاونت حقوقی قوه قضاییه، نشر سلسبیل، ص۸۷

آنچه که در بحث ارائه داده در آیین نامه مذکور مورد توجه قرار نگرفته و ضابطان باید به آن توجه کنند در خصوص بازسازی ادله برای ارائه به مرجع قضایی است .بازسازی ادله الکترونیکی ، دو وجه متمایز اما مرتبط با هم دارد:الف- بازسازی ادله غیر قابل استفاده ، ب- بکار گیری ادله در بازسازی جرم(کیسی ، همان ، ص ۱۱۳)، یکی از ویژگیهای ادله الکترونیکی این است که به سختی می توان آنها را از بین برد. امروزه دستگاههای پیشرفته ای در اختیار متخصصین و مجریان قانون فراگرفته است که می توانند ادله غیر قابل استفاده را بازیابی کنند.پیشرفت این حوزه به حدی است که هر چه داد ه ها روی هم نویسی شوند، باز هم با بکارگیری دستگاههای پیشرفته مانند میکروسکوپ های کاوشگر اسکن کننده یا میکروسکوپ های مغناطیسی ، میتوان تکه های دست نخورده داده ها را شناسایی کرد و با کنار هم قرار دادن آنها به محتوی اصلی دست یافت.[1]

بند دوم: مرحله تحقیقات مقدماتی و دادرسی

نکته اصلی و حائز اهمیت در این خصوص، قبول این ادله توسط مراجع قضایی می باشد در غیر این صورت همه زحمات ضابطین از بین رفته و راه فرار متهمین از قانون فراهم می شود، برای همین ابتدا نظام های حقوقی پذیرش ادله رایانه ای بررسی و نهایتاً نظر قانون آیین دادرسی کیفری سال ۱۳۹۲ تبیین و در ادامه سه نمونه از قرارهای صادره توسط دادسرا بررسی می شود.برای بررسی این موضوع، نگارنده مراجعاتی به دادسرای جرایم رایانه ای داشته و از نظریات کارشناسان علوم رایانه ای و به عبارتی حقوق رایانه ای بهره مند شده و نحوه گزارش تهیه شده توسط کارشناسان رسمی دادگستری نیز مورد مذاکره با کارشناسان IT قرار گرفته است تا مشخص شود که صرف نظر از مباحث تئوریک ، رویه فعلی محاکم و دادسراها به چه صورت بوده است.

الف) نظام های حقوقی پذیرش ادله رایانه ای

[1] - جلالی فراهانی، امیر حسین، ترجمه مقاله استناد پذیری ادله الکترونیکی در امور کیفری، زمستان ۱۳۸۶، شماره ۱۵

وضعیت ادله رایانه ای در هر کشور به اصول اساسی ادله در آن کشور بستگی دارد. در نتیجه باید میان دو گروه از کشورها تفکیک قایل شد:

الف- اصل آزادی ارائه و ارزیابی ادله(در کشورهای اروپایی): دادگاههای این کشور ها ا صولاً می توانند هر نوع دلیلی را بکار گیرند و در عین حال باید درجه اعتبار دلیل مربوطه را مشخص کنند.نظامهای حقوقی مبتنی براین اصول، به طور کلی، براحتی سوابق رایانه ای را دلیل تلقی می کنند. تنها هنگامی مشکل بروز می کند که مقررات شکلی تشریفات خاصی را برای اثبات اعمال حقوقی یا اثبات اسناد قانونی لازم بدانند، در این موارد محتوی یک سند را می توان رونوشت تلقی نمود ، نتیجه آنکه دادگاه می تواند داده های مربوطه را مورد بررسی قرار دهد زیرا این داده ها به طور کلی قابل اعتمادتر هستند.در این کشورها در خصوص این مساله که آیا فایل ها و پرینت های رایانه ای ، ادله غیر معتبر و غیر قابل استماع هستند ، بحث و گفتگو شده است.

ب- قوانین کشورهای کامن لا(حقوق عرفی) مثل انگلستان، در بند الف ماده ۶۹ مقرر داشته که اطلاعات موجود در یک سند ایجاد شده بوسیله رایانه در صورتی به عنوان دلیل پذیرفته می شود که علاوه بر شرایط عمومی اعتبار اسناد شرایط ذیل را دارا باشد:

۱- هیچ دلیل منطقی برای اعتقاد به اینکه این اظهارات در اثر استفاده نامطلوب از رایانه، ناصحیح و غیر دقیق هستند وجود نداشته باشد.

۲- در مواقع مهم، رایانه به طور مطلوب عمل کرده و در غیر این صورت درهر مورد که به طور مطلوب عمل نکرده یا خاموش بوده وضعیت مذکور بگونه ای نبوده که بر روند تولید سند یا صحت و دقت و محتویات آن تاثیر بگذارد.

۳- همه شرایط لازم که در بند ۲ در خصوص قواعد مربوط به دادگاهها آمده است رعایت شده باشد

٤- باید همه مسایل آن زمان مورد نظر و این مساله را که آیا شخصی که در موقعیت مقارن زمانی بوده انگیزه ای برای اخفای حقایق یا ارایه اظهارات خلاف واقع داشته است یا نه

ب) رویه قضایی کنونی

نظر غالب حقوقدانان این است که بجز موارد احصا شده در قانون مجازات اسلامی ، در سایر موارد قاضی کیفری از نظام ادله آزاد تبعیت می کند و قاضی آزاد است هر دلیلی را بپذیرد و به آن ترتیب اثر بدهد.ماده ۳۶۲ قانون آیین دادرسی کیفری سال ۱۳۹۲ ، می گوید((دادگاه علاوه بر رسیدگی به ادله ی مندرج در کیفر خواست یا ادله ی مورد استناد طرفین، هر گونه تحقیق یا اقدامی که برای کشف حقیقت لازم است را با قید جهت ضرورت انجام می دهد)). با تحقیق انجام شده ، مشخص گردید که در حال حاضر نیز رویه محاکم بدین شکل بوده که چنانچه متهم در مرحله تحقیقات مقدماتی یا دادسرا به ارتکاب جرایم رایا نه ای اقرار نماید، راه برای سایر دلایل بسته خواهد شدو بر اساس آن قرار صادر می شود ، در غیر این صورت در غالب موارد به دلیل تخصصی بودن موضوع ، پرونده برای اظهار نظر به کارشناس رسمی دادگستری ارجاع می شود و نظریه کارشناس فناوری اطلاعات و ارتباطات برای دادگاه سندیت داشته و دادسرا یا دادگاه براساس آن اقدام به صدور قرار یا حکم می نماید.

نتیجه گیری

همانگونکه توضیح داده شد ، ادله ی الکترونیکی ، داده ها و اطلاعات ارزشمند تحقیقاتی هستند که بر روی یک وسیله الکترونیکی ذخیره یا توسط آنها انتقال داده می شوند، این ادله زمانی قابلیت استناد دارند که اطمینان کافی از وجود شرایط فنی لازم در رابطه با تضمین صحت این اسناد برای مراجع مختلف وجود داشته باشد و به عبارتی باید برای دادگاههای کیفری ابتدا هویت پدید آورنده این ادله الکترونیکی معلوم بوده و دلایل مذکور از ویژگی اصالت(صحت، تمامیت، اعتبار، انکار ناپذیری و.....) برخوردار باشند.همچنین ضابطان قضایی و کارشناسان دادگستری، برای ارائه دلایل مذکور که مورد قبول دادگاه باشد ، زنجیره حفاظتی که بکارگیری ابزارها و روشهای استاندارد در مراحل شناسایی، کشف ، جمع آوری، مستند سازی، تجزیه و

تحلیل، حفظ و مراقبت از ادله دیجیتال و ارائه را رعایت نموده و به اجرا در آورند. همچنین سیستم قضایی ایران و در آیین دادرسی کیفری ایران از سیستم ادله باز تبعیت نموده و در رسیدگی های قضایی آنچه که بیشتر باعث می شود دادگاه بنحو مقتضی از صحت و اصالت آنها اطمینان حاصل کنند، عمدتاً مبتنی بر گزارش های ضابطان قضایی و نظریه کارشناسان رسمی دادگستری می باشد که در پاره ای از مواد از قانون تجارت الکترونیکی، قانون جرایم رایانه ای (یا همان مواد قانون مجازات اسلامی) کمک گرفته شده و مباحثی چون اقرار، اسناد ، امارات قضایی و علم قاضی نیز در آن نقش مهمی ایفا می کند. النهایه اینکه پس از شناخت ادله الکترونیکی و نحوه قابلیت استناد پذیری آنها ، باید به این موضوع تاکید نماییم که قوانین موجود در پاره ای موارد واجداشکال و نقصان بوده و در برخی از موارد نیز ، نیاز به تهیه قوانین و آیین نامه های تکمیلی و در پاره ای از موارد اصلاح مقررات موجود می باشد که شایسته است قانونگذار در تهیه و تصویب آن اقدام نماید.

منابع و مآخذ

۱-آشوری، محمد، آیین دادرسی کیفری، جلد دوم، نشر سمت، چاپ چهارم

۲-اولریش زیبر، کتاب جرایم رایانه ای، ترجمه نخجوانی، نوری، بختیاروند، رحیمی مقدم، انتشارات گنج دانش، چاپ دوم، سال ۱۳۹۰

۳-البوعلی، امیر، صلاحیت محاکم در جرایم سایبری، انتشارات جنگل، چاپ اولریال سال ۱۳۹۲

۴-پور احمدی، مهسا، پایان نامه کارشناسی ارشد دانشگاه آزاد اسلامی، واحد مشهد، جایگاه ادله الکترونیک در اثبات دعوی

۵-تدین، عباس، تحصیل دلیل در آیین دادرسی کیفری، نشرمیزان، چاپ دوم

۶-جاوید نیا، جواد، مطالعات بیشتر در کتاب جرائم تجارت الکترونیکی، چاپ اول، انتشارات خرسندی- سال ۱۳۹۰

۷-جزوه آموزشی ادله الکترونیکی، کمیته مبارزه با جرایم رایانه ای قوه قضائیه ، ترجمه مسیب رمضانی

۸-جلالی فراهانی، امیر حسین، ترجمه مقاله استناد پذیری ادله الکترونیکی، مجله فقه و حقوقی- زمستان ۱۳۸۶-شماره ۱۵

۹-جلالی فراهانی، امیر حسین، تفتیش و توقیف رایانه ها و تحصیل دلایل الکترونیکی در تحقیقات کیفری، معاونت حقوقی و توسعه قضایی قوه قضاییه، چاپ دوم، سال ۱۳۹۰

۱۰-جلالی فراهانی، امیر حسین، درآمدی برآیین دادرسی کیفری جرائم سایبری، معاونت حقوقی و توسعه ی قضایی قوه قضاییه ، انتشارات خرسندی – چاپ دوم- سال ۱۳۹۰

۱۱-دکتر خزانی، جزوه درسی آیین دادرسی کیفری، سال تحصیلی ۷۴-۷۳

۱۲-دوبلفون، زوینه لینان، حقوق تجارت الکترونیک، ترجمه دکتر ستار زرکلام، انتشارات شهر دانش، چاپ دوم، سال ۱۳۹۰

۱۳-زرکلام، ستار، امضای الکترونیکی و جایگاه آن در نظام ادله اثبات دعوی،مجله مدرس علوم انسانی،سال ۱۳۸۲، دوره هفتم

۱۴-زرکلام، ستار، حقوق تجارت الکترونیک، نشر دانش، چاپ دوم، سال ۱۳۹۰

۱۵-زندی، محمد رضا، تحقیقات مقدماتی در جرائم سایبری، انتشارات جنگل، چاپ اول- سال ۱۳۸۹

۱۶-السان، مصطفی، حقوق بانکداری اینترنتی، پژوهشکده پولی و بانکی، چاپ دوم، سال ۱۳۹۲

۱۷-شمس ، عبدالله، ادله اثبات دعوی(حقوق ماهوی وشکلی) ، انتشارات دراک،چاپ شانزدهم ، سال ۱۳۹۲

۱۸-شیرزاد، کامران، جرایم رایانه ای از منظر حقوق جزای ایران و حقوق بین الملل، نشر بهینه فراگیر، چاپ اول، سال ۱۳۸۸

۱۹-صادقیان، ناد علی، مقاله اسناد الکترونیکی، شگفت آورترین رسانه ارتباط جمعی، سایت حقوقدان

۲۰-فضلی، مهدی، مسوولیت کیفری در فضای سایبر، معاونت حقوقی و توسعه ی قضایی قوه قضاییه، انتشارات خرسندی، چاپ دوم، سال ۱۳۹۱

۲۱-کاتوزیان، ناصر، اثبات و دلیل اثبات، نشر میزان، چاپ ششم، سال ۱۳۹۰

۲۲-کیسی اوئن، دلایل دیجیتالی و جرایم رایانه ای ، مترجمان امیر حسین جلالی فراهانی و علی شایان، معاونت حقوقی و توسعه قضایی قوه قضایی،نشر سلسبیل- سال ۱۳۹۰

۲۳-مدنی، سید جلال الدین، آیین دادرسی کیفری یک و دو، نشر پایدار،چاپ اول، سال ۱۳۸۷

موسسه قانون یار

با همکاری مراکز علمی و دانشگاه های داخلی و خارج از کشور همچون
مرکز اطلاعات علمی جهاد دانشگاهی و نمایه مقالات در سایت sid.ir
(دانشگاه بین المللی رهنورد/بلخ/افغانستان)
(موسسه بین المللی ici world of journals/ورشو/لهستان)
(انجمن علمی بین المللی citefactor/فینیکس/آریزونا)
برگزار می کند:

همایش ملی
مطالعات حقوقی، علوم قضایی
پژوهش های اجتماعی

۱۳ خرداد ۱۴۰۰ - تهران

داوری زود هنگام مقالات

استان تهران-موسسه قانون یار

محورهای همایش:

* مقالات در گرایش های حقوق خصوصی، حقوق جزا حقوق عمومی، حقوق بین الملل، حقوق قضایی، فقهی و ....
* مقالات در گرایش های علوم ثبتی و علوم اقتصادی و بانکی
* مقالات در گرایش ها و موضوعات علوم اجتماعی و علوم تربیتی

روش های ارسال مقالات به همایش:

* ارسال فایل Word مقاله (به همراه شماره تماس) به ایمیل Phdsara@yahoo.com
* ارسال فایل Word مقاله به واتس آپ یا تگرام شماره ۰۹۱۰۰۶۳۶۰۰۲



به ده مقاله برتر و برگزیده همایش، ده تندیس به همراه تقدیرنامه مخصوص اعطا می گردد.
به مقالات ارسالی و پذیرفته شده پژوهشگران، گواهی نامه معتبر اعطا می گردد.
تمامی مقالات همایش در پایگاه ها و سایت های ملی و بین المللی نمایه و درج می گردند.
داوری مقالات حداکثر سه روز می باشد و گواهی نامه در کمتر از یک هفته صادر می شود.

جهت تقویت رزومه SID داوطلبان آزمون دکتری اساتید دانشگاه، قضات، وکلا

دبیرخانه: تهران، میدان انقلاب، خیابان اردیبهشت، پلاک ۱۹۲
واحد پذیرش مقالات:
۵۲۶ و ۶۶۹۷۹۵۱۹ - ۰۲۱
واحد صدور گواهی نامه:
۸۴ و ۴۴۴۱۷۶۴ - ۰۲۱
مشاور و راهنمای ارسال مقالات:
۰۹۱۹۶۷۴۸۶۲۵ ۰۹۱۰۰۶۴۶۰۰۲
www.Ghanonyar.ir www.Olomensani.ir