



دانشگاه آزاد اسلامی
واحد تهران مرکزی
دانشکده حقوق

پایان نامه برای دریافت درجه کارشناسی ارشد (M.A)
گرایش: حقوق جزا و جرم شناسی

عنوان:

تحصیل و مستندسازی ادله دیجیتال در فضای سایبر

استاد راهنما:

دکتر جعفر کوشا

استاد مشاور:

دکتر جلیل مالکی

نگارش:

شاهپور دولتشاهی

تابستان ۱۳۸۸

چکیده:

فناوري اطلاعات پديده اي نوظهور است و ماهيتي كاملاً متفاوت با پديده هاي سنتي داشته بنابر اين قوانين و دادگاه ها با چالشي بزرگ در رويارويي با مسائل، معضلات و جرائم اين حوزه روبرو هستند.

اصل پذيرفتن دلائل ديجيتالي در دعاوي همواره مورد بحث بوده :

پيش تر از آن پيچيدگي فضاي ساير به عنوان تجلي گاه فناوري اطلاعات و ارتباطات و به تبع آن پيچيدگي جرائم اين حوزه خود به معضلي بزرگ تبديل گشته و كشف جرم، شناسايي ادله ، تحصيل ادله، مستند سازي ادله و نگهداري ادله ديجيتالي، بسترهاي حقوقي و فني خاص خود را مي طلبد.

مشكلات و موانع موجود بر سر راه تحصيل ادله ديجيتالي از يك سو و استناد پذيري ادله ديجيتالي از سوي ديگر دو بال گسترده حقوقي كيفري فناوري اطلاعات و ارتباطات بوده كه سعي بر اين شده تا در مورد نخست تا حد امکان در اين پايان نامه بحث و بررسي صورت پذيرد اما مورد دوم كه عبارت از «استناد پذيري ادله ديجيتال» در دادرسي است، هر چند در خور يك پايان نامه مفصل و مجزاست اما به لحاظ پيوستگي و تكامل بحث در فصل پاياني اشاره اي گذرا بدان شده است.

فهرست مطالب

عنوان	صفحه
چکیده	
مقدمه	۱
ضرورت و اهمیت موضوع.....	۳
روش تحقیق، معضلات و مشکلات.....	۴
فصل اول - مبانی ادله اثبات جرم در فضای سایبر	
بخش اول - داده های دیجیتالی بعنوان سئولهای بنیادین فضای سایبر.....	
مبحث اول- تعریف داده	۶
مبحث دوم- ماهیت داده ها.....	۷
مبحث سوم- داده ها بعنوان ادله دیجیتالی.....	۷
مبحث چهارم- قالبهای ادله دیجیتال.....	۹
مبحث پنجم- کاربردهای ادله دیجیتال.....	۱۰
مبحث ششم- تفاوتها و تشابهات ادله دیجیتالی با ادله سنتی.....	۱۱
مبحث هفتم- معایب و مزایای ادله دیجیتالی نسبت به ادله سنتی در فرآیند دادرسی.....	۱۳
بخش دوم - شناسایی منابع ادله دیجیتال.....	
مبحث اول- آشنائی با فضای سایبر	۱۷
مبحث دوم- تعریف جرم سایبر	۱۸
مبحث سوم- صحنه جرم سایبر	۲۱

- ۲۲ مبحث چهارم- اهمیت صحنه جرم سایبر
- ۲۳ مبحث پنجم- یافتگاه های ادله دیجیتال
- ۲۵ بخش سوم - جایگاه و نقش ادله دیجیتال در فرآیند پی جویی و کشف جرائم سایبر
- ۲۵ مبحث اول- متدولوژی پی جویی و کشف
- ۲۷ مبحث دوم- فرآیند تحصیل ادله
- ۲۷ گفتار اول- شناسائی
- ۲۸ گفتار دوم- جمع آوری و توقیف
- ۲۹ مبحث سوم- نگهداری
- ۳۰ بخش چهارم - استانداردهای نیروی انسانی و تجهیزات فنی در برخورد با ادله دیجیتال
- ۳۰ مبحث اول- اکیپ بررسی جرائم سایبر
- ۳۰ گفتار اول- ساختار تشکیلاتی
- ۳۱ گفتار دوم- تخصصها و مهارتها
- ۳۳ مبحث دوم- ابزار و تجهیزات بررسی جرائم سایبر
- ۳۳ گفتار اول- انواع سخت افزارها و نرم افزارها
- ۳۴ گفتار دوم- استانداردهای تجهیزات

فصل دوم - تفتیش ، توقیف و مستند سازی ادله دیجیتال

- ۳۷ بخش اول - مبانی قانونی تحصیل (جمع آوری و توقیف) ادله الکترونیکی
- ۳۷ مبحث اول- مبانی تحصیل ادله
- ۳۷ مبحث دوم- هدف از تحصیل ادله دیجیتالی

- مبحث سوم – تفتیش و توقیف ادله در قانون جرائم رایانه ای ۳۸
- مبحث چهارم- قوانین بین المللی و فرامرزی ۴۵
- گفتار اول- کنوانسیون جرایم محیط سایبر ۲۰۰۱ ۴۵
- گفتار دوم- ایالات متحده امریکا ۴۶
- بخش دوم – عملیات اجرایی تحصیل ادله دیجیتال و مستند سازی فرآیند تحصیل ۵۷
- مبحث اول- کشف ادله دیجیتال ۵۷
- گفتار اول- شناسائی صحنه جرم سایبر ۵۷
- گفتار دوم- تعیین گستردگی صحنه جرم سایبر ۵۸
- گفتار سوم- حفظ صحنه جرم ۵۹
- گفتار چهارم- مستند سازی صحنه جرم سایبر ۶۱
- گفتار پنجم- شناسائی ادله ۶۳
- گفتار ششم- شناسایی سخت افزار ۶۳
- گفتار هفتم- شناسایی داده ها ۶۴
- گفتار هشتم- شناسائی ادله دیجیتال بر روی اینترنت ۶۴
- گفتار نهم- مستند سازی شناسائی و کشف ادله ۶۵
- مبحث دوم- تفتیش و جمع آوری ادله دیجیتال ۶۶
- گفتار اول- اقدامات پلیسی ۶۶
- گفتار دوم- اقدامات فنی – تخصصی ۶۹
- مبحث سوم- گسترش محدوده تفتیش و توقیف به خارج از حیطه مجوز قانونی ۹۴

- گفتار اول- دسترسی به سیستمهای مجاور یا متصل ، در شبکه های درون مرزی..... ۹۴
- گفتار دوم- دسترسی به سیستمها و شبکه های برون مرزی..... ۹۶
- گفتار سوم- جستجوی بدون مجوز ۱۰۱
- گفتار چهارم- استثناء دسترسی غیر مجاز در قانون جرائم رایانه ای ۱۰۲
- بخش سوم - توقیف ادله دیجیتال و مستند سازی فرآیند توقیف..... ۱۰۴
- مبحث اول- عملیات اجرائی توقیف نرم افزارها و ادله مرتبط با رایانه ها ۱۰۴
- گفتار اول- توقیف نرم افزارها ۱۰۴
- گفتار دوم- بوقیف ادله مرتبط با رایانه ها ۱۰۴
- مبحث دوم- عملیات اجرائی ضبط تجهیزات و ادله سخت افزاری..... ۱۰۵

فصل سوم - اقدامات پس از تفتیش و توقیف ادله

- بخش اول - نگهداری ادله مکشوفه ۱۱۱
- مبحث اول- تجهیزات سخت افزاری و نرم افزاری نگهداری از ادله ۱۱۲
- مبحث دوم- ایجاد زنجیره حفاظتی ۱۱۲
- مبحث سوم- حفاظت از ادله در برابر آسیبهای محتوایی و محیطی ۱۱۳
- مبحث چهارم- لزوم نگهداری اولین نسخه پشتیبان ۱۱۴
- مبحث پنجم- حفظ محرمانگی ادله ۱۱۵
- بخش دوم - مستند سازی فرآیند نگهداری ۱۱۶
- بخش سوم- ارزیابی و تجزیه و تحلیل ادله ۱۱۷
- مبحث اول- آشنائی با مفاهیم ۱۱۷

۱۱۷مبحث دوم- نتیجه گیری و تنظیم گزارش
۱۱۹بخش چهارم - استناد پذیری ادله دیجیتال
۱۱۹مبحث اول- پذیرش ادله دیجیتالی بعنوان مدرک در جریان دادرسی
۱۱۹مبحث دوم- بررسی اصالت ادله ، صحت و تمامیت داده ها
۱۱۹مبحث سوم- قوانین داخلی
۱۲۱مبحث چهارم- قوانین و رویه های فرامرزی
۱۲۳نتیجه گیری
۱۲۳پیشنهادات
۱۲۴منابع و مآخذ

مقدمه

به جرأت میتوان گفت زندگی امروز حتی با زندگی در سالهای آغازین هزاره سوم بسیار متفاوت گشته و فاصله میان امروز و آن سالها خیلی بیشتر از ۱۰ سال به نظر می رسد و واقعاً گویی يك قرن از آن زمان گذشته است .

بي تردید تنها عامل این تغییر و جهش چشمگیر را می توان بلوغ رایانه ها و شبکه های اینترنتی و در نتیجه نفوذ این سیستم ها به جزئی ترین لایه های زندگی روزمره برشمرد .

رایانه ها در سطوح و ابعاد مختلف زندگی رخنه کرده و در بسیاری از جوامع حتی می توان گفت زندگی بدون رایانه ها اگر ناممکن نباشد حداقل با دشواری های عدیده ای روبروست. به عبارتی غول تکنولوژی اطلاعات و ارتباطات تمامی عرصه های زندگی امروز را زیر پا نهاده و تنها راه کامیابی در جهان امروز رام کردن این غول سرکش و به معنی دیگر فراگیری علوم و فنون این تکنولوژی است.

در این مرحله به درستی گفته اند چنانچه در دنیای امروز کسی مسلط به زبان انگلیسی و علوم رایانه نباشد بی سواد است !

اهمیت این تمثیل روز به روز بیشتر رخ می نماید. از جایگیر شدن ارتباطات الکترونیکی در نهادهای دولتی گرفته تا معاملات تجاری و سیستم بانکداری، آموزش و ... تماماً پیشوند E به معنای الکترونیکی به خود گرفته و به عبارتی تمامی سطوح و ابعاد زندگی در حال الکترونیکی شدن می باشد.

آن چه متأسفانه همواره بالای جان جوامع بوده، هست و خواهد بود به خدمت گیری تکنولوژی و نوآوریها در ارتکاب جرائم بوده است. مجرمین عرصه فناوری های نوین را نیز درنور دیده و با بهره مندی از ابزار تکنولوژی بسیار ساده تر و آسوده تر به هدف می رسند. در پرتو استفاده مجرمین از تکنولوژی زمان برای ارتکاب جرائم و نیل به اهداف مجرمانه چند هزار برابر

تقلیل یافته و ترس از شناسایی شدن ناشی از حضور فیزیکی در انجام و ارتکاب فعل مجرمانه و دیگر تبعات آن جای خود را به امنیت نسبی در سایه فضای لایتنهای مبادلات الکترونیکی داده است. آنچه در این میان بگرنج است این که رژیم های حقوقی در سراسر دنیا بر پایه مفاهیم سنتی بنیان نهاده شده و انطباق آن با مفاهیم جدید ارتباطات الکترونیکی و رایانه ای کاری بس دشوار است. چیزی که بیش از هر کس مجرمین این حوزه را خوشحال و آسوده خاطر می سازد این که سیستم های حقوقی و از جمله پلیس گام های زیادی تا انطباق خود با ماهیت فضای جدید به وجود آمده، فاصله دارند لذا تجهیز رژیم های حقوقی و دادگاه ها و نهادهای پلیسی به دانش فناوری های نوین تنها راه حل فائق آمدن بر این معضل و تنها ابزار تامین امنیت و برقراری نظم در بستر مبادلات الکترونیکی خواهد بود.

باشد تا این مجموعه گام کوچکی در این راه پرفراز و نشیب برداشته باشد و از قول سعدي عليه الرحمه :

به راه بادیه رفتن به از نشستن باطل که گر مراد نیابم، به قدر وسع بکوشم

ضرورت و اهمیت موضوع :

عنوان این پایان نامه «تحصیل و مستند سازی ادله دیجیتال» است و آنچه ابتدا و در همان لحظه اول به ذهن خواننده می رسد این سؤال است که با وجود قاعده ای به نام «منع تحصیل دلیل در دادرسی توسط دادرس» اصولاً بنیان این پایان نامه زیر سؤال خواهد رفت .

بنابراین قاعده اصولاً دادگاه ممنوع از تحصیل دلیل است و بر عهده خواهان یا شاکی است که آنچه در چنته دارد به عنوان دلیل مدعی خود ضمیمه دادخواست یا شکوائیه نماید و عنوان تحصیل ادله شامل شناسایی، جمع آوری و توقیف ادله، بدین ترتیب برای این پایان نامه عنوان درستی نمی باشد.

این ایراد بزرگ معمولاً از سوی اساتید و علمای آیین دادرسی مدنی همچون استاد محترم مشاور این پایان نامه عنوان می گردد. چرا که به درستی در دادرسی های حقوقی یا به عبارتی «غیر کیفری» بحث تحصیل دلیل در میان نیست و قاضی ممنوع از تحصیل دلیل می باشد .

پاسخ به این سوال این گونه خواهد بود که اولاً با توجه به گرایش تحصیلی نگارنده که حقوق جزا و جرم شناسی می باشد و ثانیاً تمرکز مباحث پایان نامه بر شیوه های فنی - پلیسی جمع آوری ادله دیجیتال، بستر تحقیق این پایان نامه بر مباحث حقوق کیفری گسترده است و در رسیدگی های کیفری، نهاد تعقیب «دادسرا» چه در صورت وجود و حضور شاکی خصوصی و چه در صورت عمومی بودن جرم با ابزارهای پلیسی و کارشناسی وظیفه تحصیل ادله مجرمانه را به عهده خواهد داشت، ثالثاً این پایان نامه صرفنظر از رسیدگی و بحث در مورد قاعده «منع تحصیل دلیل» که درخور یک پایان نامه مفصل آن هم از سوی دانش پژوهان گرایش آیین دادرسی مدنی خواهد بود، فرضی را در نظر می گیرد که قاضی دادسرا به هر نحو و علت تصمیم بر تحصیل ادله دیجیتالی برای کشف یا پیجویی جرائم سایبر اتخاذ نموده و آنچه منظور این مقاله است، بیان مبانی و شیوه های فنی - حقوقی در صدور دستور قضائی تحصیل

دلیل و سپس نحوه جمع آوری و مستندسازی ادله توسط بازوهای فنی - پلیسی نهاد تعقیب خواهد بود.

روش تحقیق و موانع و مشکلات آن

به لحاظ حضور نگارنده در کمیته مبارزه با جرائم رایانه ای قوه قضائیه بین سالهای ۱۳۸۱ تا ۱۳۸۴ و عضویت در گروه پیش نویس لایحه «جرائم رایانه ای» و آشنایی با مبانی حقوق کیفری فناوری اطلاعات و ارتباطات از یک سو و وکالت در پرونده های جرائم رایانه ای از سال ۱۳۸۲ تا کنون، آشنایی نسبتاً زیادی با جرائم فضای سایبر پیدا نموده و به طور کلی در جریانات علمی و عملی پی‌جویی جرائم سایبر قرار داشته و دارد.

لذا اصل روش تحقیق برای این پایان نامه بر مبنای آموخته های نگارنده در خلال این سالها و برخورد مشکلات و معضلات علمی و کاربردی دادرها و دادگاه ها و نیز نهادهای پلیس در مواجهه و پی‌جویی جرائم سایبر استوار بوده است.

بدین ترتیب بهره مندی از منابع علمی ترجمه شده در کمیته مبارزه با جرائم رایانه ای قوه قضائیه که برای تهیه ی پیش‌نویس لایحه مزبور جمع آوری شده بود از یک سو و حضور در همایش ها و کنفرانسهای تخصصی فناوری اطلاعات و ارتباطات و همچنین بهره مندی از تجارب ارزشمند دبیر محترم کمیته مزبور جناب آقای رضا پرویزی در تمام این سالها از سوی دیگر، تحقیق بر روی موضوع این پایان نامه را جهت بخشید.

عمده موانع و مشکلات این تحقیق را می توان در محدودیت منابع موجود به زبان فارسی برشمرد که علیرغم سایر حوزه های حقوق کیفری سنتی از منابع وسیع و متعدد بی بهره است.

لذا در برخی موارد نگارنده سعی نموده تا با بیان برخی تجربیات عملی خود مسائل و تمثیل ها را روشن سازد .

فصل اول :

مبانی ادله اثبات جرم در فضای سایبر

بخش اول - داده های رایانه ای بعنوان سلولهای بنیادین فضای سایر

مبحث اول- تعریف داده^۱ :

در متون مختلف، تعاریف متعددی از داده ها بعمل آمده است. کمیته اروپایی مشکلات جرائم^۲، ساده ترین تعریف درباره داده ها را «موضوع وظایف یک سیستم کامپیوتری برای پردازش، ذخیره سازی و انتقال» دانسته^۳. این عبارت را میتوان اینگونه تعبیر نمود:

«آنچه در یک سیستم رایانه ای، مورد پردازش، ذخیره سازی و انتقال قرار می گیرد، داده نام

دارد»

حال این داده ها می توانند در قالب های گوناگون که بعداً بدان خواهیم پرداخت ظاهر شوند.

یک تعریف ساده دیگر اینچنین است :

«داده عبارت از هر گونه اطلاعات پردازش شدنی در سیستم های رایانه ایست»^۴. این تعریف، بسیار مجمل به نظر می رسد چرا که مجدداً بایستی تعریفی از اطلاعات ارائه داد و نیز داده ها در یک سیستم رایانه ای فقط مورد پردازش قرار نمی گیرند بلکه مورد ذخیره سازی و انتقال نیز قرار میگیرند. شاید بتوان تعریف جامعی را از داده، تحت عنوان داده پیام، در بند الف از ماده ۲ قانون تجارت الکترونیکی پیدا کرد :

«داده پیام، هر نمادی از واقعه، اطلاعات یا مفهوم است که با وسایل الکترونیکی، نوری و یا

فناوری های جدید اطلاعات تولید، ارسال، دریافت، ذخیره یا پردازش می شود»

¹- Data

² - European Committee on Crime Problems (CDPC)

^۳- پیش نویس گزارش توجیهی توصیه نامه برای مشکلات آئین دادرسی کیفری مربوط به تکنولوژی اطلاعات، کمیته مبارزه با جرائم رایانه ای قوه قضائیه، ۱۳۸۲، ص ۱۵

^۴ - مجموعه مقالات همایش بررسی جنبه های حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضائی قوه قضائیه، ۱۳۸۳، ص ۱۶۷

همانگونه که ملاحظه میشود، تعریف اخیر، يك قسمت مهم از موجودیت داده ها را نیز بیان نموده که در تعاریف قبلي بدان اشاره نشده بود و آن «تولید داده ها» یعنی در حقیقت تولد يك داده است چرا که داده در هنگام تولید، موجودیت و ماهیت می گیرد .

مبحث دوم- ماهیت داده ها :

همانگونه گفتیم ادله الکترونیکی همان داده هایی هستند توسط سیستم ها تولید، پردازش و ذخیره شده اند و در کشف و اثبات جرایم مورد استناد قرار می گیرند. همانند برخی ادله غیر الکترونیکی مانند DNA، ادله الکترونیکی نیز حالتی به ظاهر مخفی دارند^۵ و قابل رؤیت یا لمس یا شناسایی با حواس ذاتی نیستند. بطوریکه ما نمی توانیم ببینیم یا درک کنیم که درون يك حامل داده مثل يك CD یا کارت حافظه «Flash Memory» چه چیزی نهفته است مگر آنکه با استفاده از ابزار مخصوص، آنها را قابل رؤیت و درک و فهم نمائیم. برای اینکار استفاده از نرم افزارهای خاص علاوه بر تجهیزات سخت افزاری لازم است. مثلاً برای رؤیت يك تصویر که با نرم افزار فتوشاپ یا نقشه ای که با نرم افزار اتوگد «Auto Cad» تولید شده، حتماً بایستی آن نرم افزار ها را در اختیار داشته باشیم. بنابراین می توان بطور خلاصه گفت :

«ماهیت ادله دیجیتالی ماهیت پنهان است و بایستی با استفاده از ابزار خاص آن را تبدیل به مفاهیم قابل درک و قابل رؤیت نمود»

مبحث سوم- داده ها بعنوان ادله دیجیتالی :

در فضای سایبر، دلیل اعمال مجرمانه را می توان از بین داده ها و اطلاعاتی بدست آورد که در يك سیستم رایانه ای یا مخابراتی موجود، یا میان آنها در حال تبادل است. بعبارتی :

^۵- پرویزی رضا، پی جوئی جرائم رایانه ای، دانشگاه علوم انتظامی، ۱۳۸۴، ص ۱۰۹

«داده های دیجیتالی در فرایند پی جویی و کشف جرائم سایبر بعنوان دلیل استفاده می شوند» همانطوری که در دعاوی سنتی، ادله قانونی برای اثبات جرم جمع آوری و به دادگاه ارائه می گردند، در جرائم سایبر نیز نیاز به دلیل مجرمانه برای اثبات و انتساب عمل مجرمانه به شخص نیز از جنس همین فضا «سایبر» و دارای ماهیتی غالباً متفاوت با ادله ای است که همگان بعنوان ادله عینی یعنی قابل لمس، درک و فهم از طریق حواس ذاتی با آن آشنایی دارند. بنابراین:

«داده ها یعنی سلولهای بنیادین فضای سایبر در پیجویی جرائم سایبر، حکم دلایل دیجیتالی را ایفا می نمایند»

برخی نیز معتقدند دلایل دیجیتالی گونه ای از دلایل مادی اند^۱. آنها اعتقاد دارند، هر چند این دلایل نسبت به دیگر دلایل مادی مانند اثر انگشت یا سلاحهای سرد و گرم و اسناد و ... کمتر ملموس هستند، در هر حال دلیل مادی انگاشته می شوند چرا که دلایل دیجیتالی در محیط های مغناطیسی و ارتباطات الکترونیکی موجود می آیند که می توان آنها را با استفاده از ابزار و شگردهای خاصی گردآوری و تجزیه و تحلیل کرد .

آنچه اینجا موضوع بحث است، مادی بودن یا نبودن دلایل دیجیتالی نیست. چرا که حتی اگر دلایل دیجیتالی را از زمره دلایل مادی ندانیم، به هر حال در زمان جمع آوری دلایل دیجیتال و پس از مستند سازی، خواه ناخواه این ادله بایستی بصورت مفهوم و قابل درک با حواس ذاتی به دادگاه ارائه گردند. پس در هر صورت يك نما و ظاهر مادی و عینی به خود گرفته و در دعاوی سایبر بعنوان دلایل آن هم از نوع دیجیتالی قابل استناد می باشند. البته سریعاً به این نکته اشاره کنم که ادله دیجیتالی نه فقط در دعاوی سایبر بلکه در کشف، پی جویی و اثبات دعاوی سنتی نیز قابلیت استفاده و استناد دارند که در جای خود بدان خواهیم پرداخت .

^۱ - خطرات متوجه ادله در بازرسیهای پلیسی، کمیته مبارزه با جرائم رایانه ای قوه قضائیه، ۱۳۸۳، ص ۱۹

مبحث چهارم- قالبهای ادله دیجیتال :

در بحث تعریف داده ها به بند الف از ماده ۲ قانون تجارت الکترونیکی اشاره کردیم. برای بیان قالب و اشکال مختلفی که داده ها می توانند داشته باشند، بهتر است مجدداً به متن ارائه شده رجوع کنیم .

این بند اشاره می دارد : «داده پیام، هر نمادی از واقعه، اطلاعات یا مفهوم است که ...» بنابراین داده ها در اشکال نمادین ظاهر می شوند. اینکه از نظر فنی دارای چه ساختاری می باشند تا حد زیادی مربوط به مباحث تخصصی و رشته های علوم رایانه ای است اما اینکه در ظاهر چگونه می توان داده ها را مشاهده نمود، تا حد زیادی به این بحث مربوط می گردد.

۱. داده ها می توانند در قالب تصویر به نمایش درآیند. این تصویر می تواند ثابت باشد مانند یک عکس که توسط دوربین های دیجیتالی گرفته شده یا حتی عکس قدیمی باشد که توسط ابزار دیجیتالی (اسکرها) مجدداً مورد نمونه برداری دیجیتالی قرار گرفته و نهایتاً یک تصویر دیجیتالی خواهد بود. همچنین می تواند یک تصویر پویا یا متحرک مانند فیلم «Movie» باشد. در گذشته نه چندان دور، فیلم ها از نمایش دادن سریع عکس های بهم پیوسته ساخته می شدند اما هم اکنون، فیلم های دیجیتالی، لحظه به لحظه در حال وقوع را تبدیل به داده های الکترونیکی نموده و هر لحظه از تصاویر، به مجموعه ای از داده ها تبدیل و ذخیره می شوند و در هنگام نمایش، در اثر بازخوانی مجموعه داده ها تصویر نمایشی، به نظر مانند همان نمایش منظم و سریع فریم های متصل عکاسی خواهند بود. این فیلم ها میتواند تصاویر واقعی یا نقاشی پویا (انیمیشن) باشند که از نظر ماهیت داده ای، تفاوتی با یکدیگر نخواهند داشت.

۲. داده ها می توانند به شکل صدا به نمایش درآیند. همانگونه که صدای محیط قابل ذخیره سازی در ابزارهایی مانند ضبط صوتهای دیجیتالی «Digital Sound Recorders» بوده و

با استفاده از این قابلیت داده ها، اصوات و موسیقی نیز بر روی حاملهای داده، نظیر CD و DVD ها ذخیره میگردند، نتهای موسیقی نیز حالت دیجیتال بخود گرفته و برنامه های گوناگون برای نوشتن و نواختن موسیقی که پایه و مبنای آن بر داده های دیجیتالی استوار است، تولید و روانه بازار گردیده .

۳. داده ها همچنین می توانند در قالب يك رشته اطلاعات و در حالات مختلف بنمایش درآیند مانند نمایش يك متن «Text» که می تواند به زبان های مختلف نگاشته شده باشد .

نرم افزار «Word» ساخته شرکت مایکروسافت نمونه بارز تولید، پردازش و نمایش چنین قالبی از داده هاست .

۴. همچنین ممکن است داده ها در يك مجموعه ترکیبی از حالات پیشگفته بنمایش درآیند، یعنی يك فیلم حاوی تصاویر واقعی یا انیمیشن که دارای موسیقی متن، صداهای اطراف و اشخاص باشد که بصورت يك فایل متنی بعنوان زیرنویس نمایش داده شود .

مبحث پنجم کاربردهای ادله دیجیتال :

آنچه مسلم است اینکه قواعد و قواعد دادرسی اعم از حقوقی و کیفری در اکثر کشورها خصوصاً کشورهای صاحب تکنولوژی اطلاعات یا حتی کشورهای استفاده کننده از این تکنولوژی ها، بکارگیری ادله دیجیتالی در دعاوی را هر يك با قید و شرط هایی پذیرفته اند^۷. آنچه مورد قبول قریب به اتفاق است، پذیرش کاربردهای ادله دیجیتال در دعاوی اعم از سنتی و سایر بعنوان دلیل اثبات حق یا دعویست. یعنی تقریباً می توان گفت امروزه این یک اصل پذیرفته شده است که :

^۷- پیش نویس گزارش توجیهی توصیه نامه برای مشکلات آئین دادرسی کیفری مربوط به تکنولوژی اطلاعات، ترجمه کمیته مبارزه با جرائم رایانه ای قوه قضائیه، ۱۳۸۲، ص ۶۷

«ادله دیجیتالی همچون سایر ادله سنتی و در ردیف ادله سنتی دارای ارزش حقوقی و اثباتی هستند»

آنچه مورد بحث و اختلاف نظر است، ارزش اسنادی و قابلیت ارائه ادله در دادرسی است که مفصلاً در قسمت استناد پذیری ادله دیجیتال به آن خواهیم پرداخت. کشورهای مختلف قوانین و رویه های گوناگونی در این خصوص دارند که هر یک در جای خود مورد بحث قرار خواهد گرفت.

مبحث ششم- تفاوتها و تشابهات ادله دیجیتالی با ادله سنتی :

تشابهات ادله دیجیتالی با ادله سنتی را می توان در این موارد خلاصه نمود که :

اولاً- برابر رویه های پیش گرفته، اغلب کشورهای^۱ ادله دیجیتالی را هم عرض ادله سنتی و در ردیف آنها بعنوان مستندی در دادرسی پذیرفته اند .

ثانیاً- ادله دیجیتالی نیز بهنگام ارائه در دادرسی معمولاً در قالب های متعارف و معمولی در آمده که ادله سنتی در آن قالب های شناخته شده به دادگاه ارائه می شوند. مثلاً ادله دیجیتالی هر چند ممکن است در لحظه شناسایی و جمع آوری ماهیتی نامفهوم داشته باشند (مثل ادله رمزنگاری شده) اما بهنگام ارائه به دادگاه و در زمانی که بعنوان دلیل در دادرسی مطرح می گردند، حتماً به شکل مفهوم و قابل درک تبدیل شده اند مثلاً داده های رمزنگاری شده، رمزگشایی می شوند و به یکی از اشکال داده ها با قابلیت فهم و درک عمومی در می آیند. برای مثال چنانچه سند واریز پول به یک حساب بانکی در معاملات غیرقانونی، رمزنگاری و ارسال شده باشد، وقتی بعنوان دلیل به دادگاه ارائه می گردد، حتماً قبل از آن رمز گشایی شده و تصویر رسید بانکی که ظاهری مانند سایر ادله کاغذی پیدا نموده، به دادگاه ارائه میگردد .

^۱- در قوانین مربوط به ادله، «Evidence Act» ایالات متحده و کانادا، ادله دیجیتالی بعنوان دلیل در دادرسی پذیرفته شده است.

ثالثاً- ادله دیجیتالی نیز همانند ادله سنتی دارای قابلیت انتساب به متهم را دارا می باشند. همچنانکه اثر انگشت، خون، دستخط و امضاء، قابلیت انتساب به اشخاص را دارند، ادله دیجیتالی نیز بعلت ساختار سیستم های دیجیتالی و فن آوری که در تولید، پردازش، ذخیره سازی و انتقال داده ها از آن بهره برداری میشود، آثار و علائمی به خود میگیرند که قابلیت انتساب ادله دیجیتالی را مانند ادله سنتی بالا میبرد. از جمله گداهای مخصوص و مشخصی که سیستم های رایانه ای به هنگام تولید و یا انتقال داده ها به آنها اختصاص می دهند و با شناسایی و پیگیری آن گداهای می توان به سر منشاء تولید یا انتقال داده دست یافت .

تفاوت ها را نیز می توان به همین نحو برشمرد :

اولاً- ادله دیجیتالی خلاف ادله سنتی ممکن است به همان حالت های اولیه، قابل شناسایی و بازخوانی نباشند. همانگونه که گفته شد، ممکن است ادله در قالب داده هایی باشند که برای تبدیل آنها به حالت های قابل فهم و درک، نیاز به گذراندن ادله از پروسه های فنی باشد، مثلاً يك تصوير هرزه نگاري کودکان که به روش استگنوگرافی (در رمز نگاری توضیح خواهیم داد) در یک طرح دیگری مکتوم گردیده، قابل ارائه به دادگاه نیست چرا که با حواس عادی قابل درک و فهم و شناسایی نخواهد بود و حتماً بایستی از طریقه های فنی و با استفاده از الگوریتم های مخصوص گدگشایی، تصویر اصلی (مکتوم) از تصویر ظاهری جداسازی گردد. آنگاه می توان پس از مستندسازی همین فرآیند (گدگشایی) آن را بعنوان دلیل در دادرسی ارائه نمود .

ثانیاً- در اغلب موارد، معمولاً تصویر داده های غیر قانونی، بعنوان دلیل ضمیمه پرونده می گردد و نه اصل داده ها. هر چند لزوم نگهداری و ارائه اصل داده ها به همراه تصویر آنها، امر بایسته ایست، اما آنچه در دادرسی ارائه و مورد بحث و بررسی قرار می گیرد، غالباً اصل داده ها نیست، بلکه تصویر داده هاست و ارائه کننده اعم از سیستم پلیسی، دادرسی و اشخاص، باید انطباق داده های ارائه شده بعنوان دلیل با نسخه های اصل را در دادرسی به اثبات برسانند .

از دیگر تشابهات و تفاوت ها نیز می توان در قالب مزایا و معایب ادله دیجیتال نسبت به ادله سنتی یاد کرد:

مبحث هفتم- معایب و مزایای ادله دیجیتالی نسبت به ادله سنتی در فرآیند دادرسی :

از مزایای ادله دیجیتال، که ادله سنتی فاقد آن میباشند به اختصار میتوان چنین نام برد:

اول - نسخه های الکترونیکی يك سند می تواند حاوی اطلاعات مضاعف و کاملتری از نسخه پرینت شده همان اسناد یا نمایش آن بر روی مانیتور رایانه باشد که در نسخه های پرینت شده یا حتی بر روی صفحه نمایش هم، این اطلاعات قابل مشاهده نیستند. مثلاً تاریخ های تولید یا نگارش سند، ارسال و دریافت پیامها، لیست دریافت کنندگان پیام ها (مانند لیست گیرندگان پست الکترونیکی) به همراه متن پیامها در نسخه های دیجیتالی اسناد موجود است. اما وقتی شما آن را بر روی مانیتور و یا حتی چاپ شده بر روی کاغذ مشاهده می کنید، فاقد بسیاری از این اطلاعات خواهد بود. حال در مقایسه ادله دیجیتالی با ادله سنتی در خصوص اسناد و مدارك مشابه، این مزیت، صد چندان بچشم می آید. چرا که در نسخه های اسناد عادی که به عنوان ادله سنتی مورد استناد قرار می گیرند، می توان گفت کمترین اطلاعات جانبی را نیز نمی توان در آنها دریافت، مگر اسناد و ادله دیگری که بطور جداگانه، آن اطلاعات جانبی را اثبات نماید. مثلاً اسناد دیگری وجود داشته باشد که لیست گیرندگان سند اصلی در آن نوشته شده و یکایک گیرندگان، جلوی اسم خود را امضاء نمایند. همانند رویه ای که هم اکنون برای ارسال و مراسلات بکارگیری میشود.

دوم- ادله دیجیتالی در صورت پاک شدن یا از بین رفتن، سوختن، تغییر حالت، مخفی کردن و سایر اشکال تبدیل وضعیت، قابل شناسایی و بازیابی و استفاده می باشند حال آنکه چنانچه ادله سنتی دچار تغییرات اساسی مانند تخریب یا امحاء یا پنهان سازی گردند، شناسایی یا استناد به