فرهاد شمس
کارشناس ارشد حقوق خصوصی

حقوق فناوری اطلاعات و ارتباطات

● مقدمه

امروزه فناوری اطلاعات و ارتباطات# که موجب کوچک شدن جهان عینی## و بزرگتر شدن جهان ذهنی### می‌گردد در حال تکوین و شکل‌دهی ساختار نوینی از روابط اجتماعی افراد است. ظهور و گسترش اینترنت و شبکه جهانی اطلاع‌رسانی، تغییرات چشمگیری در زندگی انسان امروز، رفتارها و تعاملات وی ایجاد کرده که البته پویایی جامعه را نیز به همراه داشته است. این تغییرات که به سرعت انجام شده و هم‌اکنون با شتاب بیشتری در حال جریان است، علوم اجتماعی را نیز تا حد زیادی متحول ساخته و از همین‌رو بیشتر رشته‌های علوم اجتماعی به فراخور حال خود با فناوری اطلاعات و ارتباطات همگام شده‌اند.[1] بدیهی است که این فناوری نیز مانند هر علم دیگری نظام‌مند و قانونمند بوده و از قوانین خاص خود بهره می‌گیرد اما حقوق علمی نیست که خیلی سریع تحت تأثیر تغییرات ناشی از تکنولوژی قرار گرفته و همگام با آنها متحول شود. زیرا ثبات و دوام از جمله خصوصیات نهادهای حقوقی و قوانین موضوعه است. ولی هنگامی که دولت‌ها به دنبال کنترل و یافتن راه‌حل‌هایی برای مشکلات اجتماعی به وسیله قانون هستند (راه‌حل‌های قانونی)، حقوق هم با تغییرات اجتماعی ارتباط تنگاتنگی پیدا می‌کند و شاید به همین دلیل است که همواره آهنگ تغییر، تحول یا

- Information and Communication Technology (I.C.T)

- Objective world

- Subjective world

اصلاح مفاهیم و موضوعات حقوقی با تأخیر زمانی نسبت به میزان رشد تحولات اجتماعی (مثل گسترش روزافزون فناوری اطلاعات) صورت می‌گیرد. تحولاتی که عمدتاً با ظهور فناوری اطلاعات و ارتباطات مبنا و اساس حقوق را دستخوش تغییر قرار می‌دهند، مواردی هستند که در حال ازبین بردن مرزهای اقلیمی و کاهش دخالت فیزیکی (حضور الزامی فیزیکی) انسان در روابط حقوقی او هستند. از آنجایی که چنین تحولاتی با مبانی اصلی حقوقی در ارتباط هستند لذا حقوق هم ناگزیر از روزآمد شدن و همگام شدن با آهنگ تغییر و تحولات اجتماعی خواهد بود. چرا که توجه به روابط اجتماعی، نتایج بسیار مهمی برای نظام حقوقی هر جامعه‌ای دارد.

فراگیر شدن فناوری اطلاعات و ارتباطات به ظهور یک جامعه الکترونیکی# خواهد انجامید که تمام ارکان آن لزوماً باید در این محیط مجازی حداقل از قابلیت‌های پیشین خود برخوردار باشند.[۲] بالطبع حقوق نیز که نقش تنظیم روابط افراد را برعهده دارد باید بتواند خود را با این محیط جدید وفق دهد و نقش خود را ایفاء کند. بنابراین محیط حقوقی فناوری اطلاعات از جمله مباحث مهمی است که در جامعه الکترونیکی باید مورد توجه قرار گیرد. پیاده کردن و گنجاندن نظام حقوقی کلاسیک در فضای مجازی الکترونیکی موجب پیدایش و شکل‌گیری رشته نوپای حقوق فناوری اطلاعات و ارتباطات## شده که به تدریج در حال تثبیت در نظام‌های حقوقی دنیاست. منظور از حقوق فناوری اطلاعات و ارتباطات، مجموعه قواعد و مقرراتی است که در محیط فناوری اطلاعات و ارتباطات به تنظیم و کنترل روابط اشخاص (حقیقی و حقوقی) می‌پردازد.[۳]

معرفی محیط حقوقی فناوری اطلاعات و تبیین موضوعات و عناوین مطرح در آن، در دو بخش حقوق خصوصی و حقوق عمومی پی‌گرفته می‌شود و حتی‌المقدور سعی خواهد شد فقط به موضوعاتی که به نظر می‌رسد در فضای مجازی دستخوش تغییر و تحول قرار گیرند پرداخته شود. مطالعه دقیق و بررسی جزئی محیط حقوقی فناوری اطلاعات و ارتباطات و شناسایی تمام مؤلفه‌های متأثر از فضای الکترونیکی احتیاج به

- E.Society

- ICT law

زمان و مطالعات مبنایی مفصل‌تری دارد و از حوصله این مقاله خارج است.

● بخش اول ـ حقوق فناوری اطلاعات: حقوق خصوصی

مهمترین موضوعاتی که با اعمال فناوری اطلاعات در عرصه حقوق خصوصی باید مورد توجه و بررسی‌های حقوقی قرار گیرند عبارتند از:

○ گفتار اول: تجارت الکترونیک

منظور از تجارت الکترونیک انجام مبادلات تجارتی اعم از خرید، فروش و ارایه خدمات (منظور خدمات رایگان یا غیررایگانی است که با هدف اقتصادی انجام می‌شود) در اینترنت است.[۴] به عبارت دیگر، تجارت الکترونیک، استفاده از هر نوع شبکه الکترونیکی برای انجام مطالعات و دادوستدهای تجاری و ارایه خدمات می‌باشد. بنابراین مبنای تجارت الکترونیک استفاده از اطلاعاتی است که به صورت داده‌های الکترونیکی مبادله می‌شوند.[۵]

فناوری اطلاعات اگرچه هنوز فرآیند نوپایی است ولی به دلیل ویژگی‌های خاص خود تغییرات و تحولات چشمگیری در امر تجارت ایجاد کرده و شکل تازه‌ای از معاملات تجاری (مبتنی بر داده‌های الکترونیکی) را جایگزین روش‌های سنتی و کلاسیک (مبتنی بر اسناد کاغذی) کرده است. برخی از ویژگی‌های تجارت الکترونیک عبارتند از:[۶]

۱ـ معاملات تجاری می‌توانند به طور کامل و در یک فضای مجازی* یعنی بدون حضور فیزیکی متعاملین انجام شوند.

۲ـ انجام عملیات تجاری از طریق مبادله الکترونیکی داده‌ها با سرعت بیشتر و هزینه کمتری صورت می‌گیرد.

۳ـ اقدامات، فعالیت‌ها و سلایق کاربران به آسانی زیرنظر گرفته و ردیابی می‌شوند.

۴ـ داده‌ها و اطلاعات کاربران به سهولت کپی شده و مورد نقل و انتقال قرار می‌گیرند.

- Cyber Space

۵ـ نام‌های دامنه# در بازاریابی و تبلیغ مارک‌های تجاری نقش بسیار مهمی دارند.

۶ـ فناوری اطلاعات یک بازار جهانی ایجاد کرده است. بنابراین رقابت تجاری در بازارهای الکترونیکی به شکل ملموس‌تری مطرح می‌گردد.

ویژگی‌های فوق چالش‌های زیادی را در بحث سیاست‌گذاری عمومی## ایجاد کرده و موجب طرح مباحث حقوقی در این زمینه شده که در بیشتر قوانین تجارت الکترونیک مورد توجه قرار گرفته‌اند.[۷] در اینجا مباحث مربوطه را به طور اجمالی مورد بررسی قرار می‌دهیم:

○ مبحث اول: انعقاد قراردادهای الکترونیکی الزام آور

اصولاً هر عقدی با ایجاب و قبول طرفین آن منعقد می‌شود، در این میان آنچه که اهمیت دارد این است که متعاملین بتوانند اراده انشایی خود را مبنی بر تشکیل عقد یا انجام معامله به طریقی به یکدیگر منتقل کنند، به گونه‌ای که هر یک از طرفین معامله از اراده جدی طرف دیگر اطمینان حاصل کند. پس همان گونه که قصد طرفین می‌تواند به صورت کتبی، شفاهی، لفظی یا عملی باشد بنابراین می‌توان گفت ایجاب و قبول در یک فضای مجازی و در قالب داده‌های الکترونیک### نیز از نظر حقوقی معتبر و لازم‌الاجرا است. اما در تشکیل قراردادهای الکترونیکی و الزام‌آوار دانستن آنها، باید به برخی تفاوت‌ها و نیز ویژگی‌های خاص اینگونه مبادلات در مقایسه با انواع کلاسیک آنها توجه کرد:

الف) امنیت#### مبادلات الکترونیکی داده‌ها

بدیهی است که گسترش تجارت الکترونیک مستلزم ایجاد اطمینان و اعتماد عمومی نسبت به این نوع از تجارت است و این اطمینان باید از طریق تضمین امنیت تبادل داده‌های الکترونیکی صورت گیرد. امنیت تبادل داده‌های الکترونیکی فرآیندی است که

- Domain Names

- Public Policy

- Electronic Data Format

- Security

باید تمام اجزاء و عناصر یک مبادله تجاری را به طور کامل و مطمئن حفاظت کند به گونه‌ای که دریافت‌کننده پیام داده‌ای مطمئن شود که اطلاعات رسیده توسط ارسال‌کننده موردنظر، فرستاده شده است. علاوه بر این طرفین یک مبادله الکترونیکی باید مطمئن شوند که هیچ گونه دسترسی غیرمجاز و غیرقانونی نسبت به داده‌های الکترونیکی صورت نگرفته است.

یکی از عواملی که باعث اعتبار قرارداد یا هر سند دیگری می‌شود صحت انتساب به آن قرارداد یا سند به صادرکننده است که تاکنون از طریق مهر یا امضاء صورت می‌گرفته و دلیل معتبری برای تحقق صحت انتساب صادرکننده بوده است. در تجارت الکترونیک نیز اسناد، اطلاعات و داده‌های الکترونیکی باید به امضای شخص صادرکننده برسد تا بتوان صحت انتساب آنها را به وی احراز کرد. مسلماً مهر و امضای متداول فعلی که بین عموم و تجار مرسوم است در فضای مجازی کاربردی ندارد. بنابراین متناسب با این محیط الکترونیکی باید یک امضای الکترونیکی* را تعریف و جایگزین امضاهای دست‌نویس کرد.

۱. امضای الکترونیکی

امضای الکترونیکی به هر تأییدی اطلاق می‌شود که به صورت الکترونیکی ایجاد شده باشد و ممکن است یک علامت، رمز، کلمه، عدد، یک اسم تایپ شده، تصویر دیجیتال شده یک امضای دست‌نویس و یا هر نشان الکترونیکی اثبات هویت باشد که توسط صادرکننده یا قائم‌مقام وی اتخاذ و به یک قرارداد و یا هر سند دیگری ملحق شده باشد.[۸]

تاکنون انواع مختلفی از امضای الکترونیکی و با فناوری‌های متفاوت شناخته شده و به محیط تجارت الکترونیک معرفی شده که مهمترین آنها عبارتند از: تصویر اسکن شده یک امضای دست‌نویس،** امضای بیومتریک*** و امضای دیجیتالی**** که

- Electronic signature

- Bitmap Signature

- Biometric Signature

- Digital Signature

پیشرفته‌ترین و پرکاربردترین نوع از امضاهای الکترونیکی است. بنابراین با توجه به اهمیت امضای دیجیتالی و اتخاذ این نوع امضا در بیشتر قوانین مربوطه، نحوه ایجاد آن به طور اجمالی مورد بررسی قرار می‌گیرد.[۹] این نوع امضا مبتنی بر روش‌های رمزنگاری* از طریق کلیدهای عمومی و خصوصی** است. رمزنگاری علم تغییر شکل داده‌ها و اطلاعات است یعنی روشی که شما می‌توانید یک متن را بخوانید و یا از آنچه که موردنظر نگارنده بوده استنباط کنید ولی فرد دیگری قادر به چنین کاری نیست. پس رمزنگاری این اطمینان را برای طرفین ایجاد می‌کند که اطلاعات و داده‌های آنها فقط توسط دریافت‌کننده قابل فهم است. فرآیند رمزنگاری مبادلات الکترونیکی دارای دو مرحله است. مرحلهٔ اول رمزنگاری (یا رمزسازی) یعنی تبدیل یک متن ساده و عادی به یک متن رمز شده است. این متن اگر برای همهٔ افراد هم قابل دسترسی باشد مطمئناً قابل فهم نخواهد بود. مرحلهٔ دوم رمزگشایی یعنی تبدیل متن رمز شده به یک متن ساده و عادی است. به حالت رمز درآوردن و از حالت رمز خارج کردن، از طریق الگوریتم‌های رمزنگاری انجام می‌شود که مستلزم محاسبات و فرمول‌های ریاضی و عددی است. الگوریتم‌های مربوط به رمزنگاری مبتنی بر الگوریتم‌های کلید عمومی است.[۱۰]

امضای دیجیتالی از طریق الگوریتم‌های کلید عمومی صورت می‌گیرد. منظور از کلید بخشی از الگوریتم است که متن را رمزگذاری یا رمزگشایی می‌کند. در روش رمزنگاری الگوریتم کلید عمومی، دو نوع کلید مورد استفاده قرار می‌گیرد. یکی کلید عمومی که پیام را به صورت رمز درمی‌آورد و دیگری کلید خصوصی است که پیام را از حالت رمز خارج می‌کند. کلید عمومی اگر در معرض استفاده و دید عمومی قرار بگیرد هیچ اشکالی ندارد ولی ضروری است که کلید خصوصی (کلید شخصی و منحصر به فرد) پنهان بماند و غیر از خود فرد، کس دیگری به آن دسترسی نداشته باشد.

برای ایجاد یک امضای دیجیتالی، ابتدا امضاءکننده باید از طریق کلید عمومی امضای خود را رمزسازی و سپس ضمیمه پیام داده‌ای کرده و برای گیرنده ارسال کند. گیرنده، امضای دیجیتال را که اکنون به حالت رمز درآورده و قابل فهم نیست از پیام

- Cryptography

- Public and private key

داده‌ای جدا می‌کند و از طریق کلید عمومی ارسال‌کننده (که در فهرست عمومی مرجع گواهی امضا موجود است) پیام را برای وی ارسال می‌کند تا خود ارسال‌کننده با کلید خصوصی‌اش آن را رمزگشایی کند. چنانچه نتایج یکسانی حاصل شد، یعنی همان چیز که امضاءکننده به عنوان امضای دیجیتالی برای خود تعریف کرده بود هویدا شد، معلوم می‌شود که اولاً امضای مذکور به نحو صحیحی از سوی امضاءکننده ارسال شده و ثانیاً وی نمی‌تواند ادعا کند که پیام را امضاء نکرده و یا اینکه پیام تغییر یافته است.[۱۱]

۲. مرجع گواهی* امضای الکترونیکی

همانطور که پیش‌تر بیان شد پذیرش و تصدیق طرفین یک معامله نسبت به محتوا و مندرجات سند توسط امضاء یا مهر صورت می‌گیرد و حاکی از این است که آنها مسؤولیت تعهدات خود را پذیرفته‌اند. ولی به هر حال ممکن است که هر یک از طرفین نسبت به اصالت و صحت انتساب سند تردید کنند. برای رفع این مشکل مراجع ثبت اسناد رسمی وجود دارند که در صورت لزوم صحت انتساب اسناد را به صادرکنندگان آنها تأیید می‌کنند و اطمینان‌خاطر را برای طرفین در خصوص استحکام معاملات به وجود می‌آورند.

در محیط حقوقی فناوری اطلاعات نیز احتمال تردید، انکار یا ادعای جعل نسبت به اسناد الکترونیکی وجود دارد. پس باید در فضای سایبر(مجازی) هم، نهادها و مراجعی را ایجاد کرد که امکان انجام معاملات و ایجاد اعتماد و اطمینان افراد نسبت به تجارت الکترونیکی را تضمین کنند.

حال برای اینکه یک امضای الکترونیکی از نظر قانونی به رسمیت شناخته شود یعنی همانند دیگر امضاهای دست‌نویس نسبت به سند یا پیامی که به آن ضمیمه شده منحصر به فرد باشد و بتواند هویت صاحب امضاء را تأیید کند، لازم است که توسط مرجع تأییدکننده (مرجع گواهی صحت امضاء) مورد گواهی قرار گیرد و به عبارت بهتر امضای الکترونیکی باید از طریق یک گواهینامه رسمی تصدیق و کنترل شود. توضیح اینکه مرجع مزبور باید برای هر امضاء یک گواهی تهیه و تنظیم و ضمیمه آن کند. این گواهینامه

- Certification Authority.(CA)

در واقع هویت امضاءکننده و صحت انتساب سند را به وی تأیید می‌کند.

۳. مزایای استفاده از امضای الکترونیکی

چنانچه فناوری امضای الکترونیکی به صورت استاندارد شده‌ای در سطح جهانی فراگیر شود، آنگاه نه تنها شرکت‌ها و مؤسسات تجاری، بلکه عموم مردم و افراد غیرتاجر هم می‌توانند از منافع و مزایای استفاده از این نوع امضاء به ویژه امضای دیجیتالی در انجام مبادلات الکترونیکی و دادستدهای روزانه بهره ببرند. مزایای استفاده و به کارگیری امضای الکترونیکی نسبت به امضای دست‌نویس عبارتند از:[۱۲]

۳.۱ امنیت: امضای الکترونیکی از امنیت بیشتری برای مصون ماندن از جعل یا دست‌کاری و تقلید توسط دیگران برخوردار است. چون امضای دست‌نویس یا مهر به سهولت قابل تقلید یا جعل بوده در حالی که دسترسی و آگاهی یافتن بر یک امضای الکترونیکی محرمانه، کار بسیار دشواری است.

۳.۲ قابلیت اطمینان و اعتماد عمومی: چنانچه کاربران اینترنتی به امنیت بیشتر امضای الکترونیکی نسبت به امضای دست‌نویس ایمان بیاورند آنگاه این نوع امضاء اعتبار بیشتری پیدا کرده، نتیجتاً اعتماد افراد در بکارگیری امضای الکترونیکی افزایش پیدا خواهد کرد.

۳.۳ شفافیت در انجام معاملات: امضای الکترونیکی می‌تواند به شفافیت و صراحت در انجام معاملات و مبادلات الکترونیکی کمک کند. بدین معنی که مثلاً خطر کلاهبرداری اینترنتی را کاهش می‌دهد و یا مانع از آن می‌شود که امضاءکنندگان پیام داده‌ای با ادعای جعل امضای خود از زیر بار تعهدات و مسؤولیت آن شانه خالی کنند علاوه بر این صادرکننده دیگری نمی‌تواند ادعا کند که محتویات و مندرجات پیام داده‌ای بعد از ارسال تغییر کرده است.

۳.۴ اثبات هویت کاربر: هنگامی که سند یا قراردادی در محیط I.C.T و با امضای الکترونیکی از طرف کاربر صادر می‌شود، گیرنده پیام حقیقتاً مطمئن است که سند یا قرارداد مزبور منتسب به صادرکننده اصل است.

فراگیر شدن استفاده از اسناد و قراردادهای الکترونیکی که مستلزم شناسایی قانونی و اعتماد به مزایای بیشتر امضای الکترونیکی است، موجب می‌شود که سیستم‌های باز

شبکه‌ای بتوانند مبادلات الکترونیکی را با سرعت، سهولت و امنیت بیشتری انجام دهند و مسلماً این امر پویایی و رونق تجارت را افزایش می‌دهد. علاوه بر این چنانچه امضای الکترونیکی به نحو صحیحی در بخش عمومی(یعنی ارتباطات عادی و غیرتجاری افراد) هم به کار گرفته شود می‌تواند کیفیت بالایی از امنیت و شفافیت را در معاملات و روابط حقوقی افراد تضمین کند.

ب) زمان ومکان دریافت داده‌ها

همانطور که قبلاً بیان شد هر عقدی با ایجاب و قبول طرفین آن انعقاد می‌یابد و گفته شد که نحوه ایجاب و قبول از طرف داده‌های الکترونیکی هم امکان‌پذیر و لازم‌الاتباع است. اما آنچه که در این قسمت باید مورد توجه قرار گیرد، زمان و مکان ارسال و وصول داده‌ها (زمان و مکان وقوع عقد) است که از نظر حقوقی ـ مثلاً در تعیین صلاحیت محاکم با اقامتگاه افراد ـ اهمیت فراوانی دارد به عبارت دیگر زمانی که پیام داده‌ای از سیستم اطلاع‌رسانی* (سیستمی برای تولید، ارسال، دریافت، ذخیره و یا پردازش داده‌های الکترونیکی) ارسال‌کننده خارج می‌شود، آیا زمان و مکان ارسال از نظر حقوقی معتبر است یا زمان و مکان وصول؟

لازم به توضیح است که هر یک از طرفین ارتباط یا معامله الکترونیکی ممکن است دارای سیستم اطلاعاتی ویژه‌ای باشند(مثلاً در پست الکترونیکی هر فردی دارای یک صندوق پستی جداگانه‌ای است) که ورود و خروج داده‌ها به همین سیستم اطلاع‌رسانی را ملاک معتبر در تحقق ایجاب و قبول قرار دهند.[۱۳]

ج) تصدیق ارسال و وصول

از دیگر مسایل مهمی که در انتقال داده‌های الکترونیکی مطرح است، تصدیق ارسال و وصول داده‌ها است. به عبارت بهتر از آنجا که امکان نقص یا خطا در ارسال یا وصول داده‌های الکترونیکی وجود دارد، تصدیق و تأیید آنها از سوی مرسل‌الیه میزان استنادپذیری داده‌ها را برای طرفین استوارتر خواهد کرد. بنابراین ممکن است طرفین توافق کرده باشند که وصول داده‌ها از طرف گیرنده آن تأیید شود یعنی شرط وصول و

- Information System

تحقق قبول داده‌ها منوط به تأیید و تصدیق آنها از سوی مرسل‌الیه باشد بنابراین محتویات و مندرجات پیام داده‌ای و نیز وصول آن زمانی اعتبار قانونی لازم را پیدا می‌کند و التزام حقوقی ایجاد خواهند کرد که تأییدیه‌ای از سوی مرسل‌الیه برای ارسال کننده فرستاده شود. روش تصدیق نیز می‌تواند براساس توافق طرفین تعیین شود. مثلاً آنها می‌توانند شکل یا روش خاصی را تعیین کرده و طبق آن عمل کنند. در غیر این صورت هر نوع روشی که برای ارسال کننده پیام داده‌ای، اطمینان کافی ایجاد کند معتبر است.

در هر صورت چنانچه ارسال کننده از مرسل‌الیه درخواست کرده و یا قبلاً توافق کرده باشند که وصول داده‌ها تصدیق شود و ارسال کننده صراحتاً هر نوع اثر حقوقی داده‌ها را منوط به تصدیق وصول آنها کرده باشد، تا زمانی که تصدیق داده‌ها صورت نگرفته و یا تأییدیه مرسل‌الیه به دست ارسال کننده نرسیده، انتقال داده‌ها از نظر حقوقی صورت نگرفته است.

○ مبحث دوم: شیوه پرداخت‌های الکترونیکی

همانطور که قبلاً بیان شد مبادلات الکترونیکی در فضایی کاملاً مجازی صورت می‌گیرند بنابراین پرداخت وجوه نیز که از اجزای یک مبادله است باید لزوماً از طریق یک سیستم الکترونیکی صورت پذیرد.

در پرداخت‌های غیرالکترونیکی پول، چک و کارت‌های اعتباری از ابزارهای پرداخت محسوب می‌شوند ولی در سیستم پرداخت‌های الکترونیکی ابزارهای پرداخت و مهمترین روش‌هایی که تاکنون مورد توجه قرار گرفته عبارتند از:

۱. کارت‌های اعتباری*

در حال حاضر معمول‌ترین روش پرداخت در اینترنت استفاده از کارت‌های اعتباری است. به این کارت‌ها اصطلاحاً کارت‌های هوشمند** هم گفته می‌شود.

- Credit and cards

- Smart cards

۲. پول الکترونیکی*

پول الکترونیکی در واقع جانشین پول جاری (سنتی) است. پول الکترونیکی باید ویژگی‌های زیر را داشته باشد:[۱۴]

- در همه جا رایج باشد.
- اعتبار سراسری داشته باشد.
- قابل جعل نباشد.
- قابل استفاده همگان باشد.

۳. چک الکترونیکی**

چک‌های الکترونیکی هم جایگزین چک‌های کاغذی هستند و می‌توان آنها را یک سند الکترونیکی دانست که شبیه چک‌های مرسوم بوده و باید همان شرایط شکلی را دارا باشند فقط امضای پرداخت‌کننده و دریافت‌کننده چک، الکترونیکی است.

از آنجا که در شیوه پرداخت‌های الکترونیکی در فضای مجازی، علاوه بر فروشنده و خریدار شخص ثالث دیگری نیز مثل واسطه‌های پرداخت، شرکت‌های کارت اعتباری یا دیگر تأمین کنندگان خدمات مالی دخالت دارد، بنابراین بین این افراد یک سری روابط حقوقی وجود خواهد داشت که تقصیر هر یک از آنها ممکن است به نقض قرارداد یا تعهدات بین آنها بیانجامد.[۱۷]

○ مبحث سوم: حمایت‌های قانونی در بستر مبادلات الکترونیکی

پیش از این بیان شد که گسترش مبادلات، دادوستدها و روابط حقوقی افراد در فضای مجازی منوط به ایجاد اطمینان و اعتماد عمومی نسبت به مبادلات الکترونیکی است و یکی از عوامل مهمی که می‌تواند در این خصوص مؤثر واقع شود وجود حمایت‌های قانونی لازم از کاربران اینترنتی است. به عبارت بهتر محیط فناوری اطلاعات باید به گونه‌ای دارای پشتوانه قانونی باشد که افراد اطمینان خاطر داشته باشند که در انجام مبادلات الکترونیکی حقی از آنها ضایع نخواهد شد و یا در صورت نقض برخی از

- E-Cash

- E-Check

حقوق حمایت‌های قانونی لازم برای جبران خسارت‌های مالی یا معنوی وجود خواهد داشت.

مهمترین مسایلی که در بحث حمایت قانونی از کاربران اینترنتی مطرح است عبارتند از:

الف) حمایت از مصرف کننده#

منظور از مصرف کننده در اینجا، مصرف کننده اینترنتی است که اقدام به انجام یک تبادل الکترونیکی کرده و یا اینکه می‌خواهد از خدمات اینترنتی بهره ببرد. بنابراین وی باید در مقابل تأمین کنندگان اینترنتی که شغل و حرفه اصلی آنها در حیطه تجارت الکترونیکی (خرید، فروش و ارایه خدمات) می‌باشد مورد حمایت قرار گیرد. به عنوان مثال برخی از موارد حمایت از مصرف‌کنندگان مورد اشاره قرار می‌گیرد:[۱۶]

۱. هویت و مشخصات کامل تأمین کنندگان باید برای مصرف کننده معلوم باشد.

۲. هر نوع اطلاعاتی که در مورد کالا یا خدمات لازم است باید در اختیار مصرف کننده قرار بگیرد. مثلاً مشخصات کامل کالاها، نوع خدمات، هزینه‌ها و ترتیب پرداخت یا زمان و مکان تحویل کالا یا ارایه خدمات باید برای مصرف کننده معین و معلوم باشد.

۳. پیش بینی «حق انصراف» نیز از موارد حمایت از مصرف کننده است. به این معنا که یک مهلت متعارف برای وی درنظر گرفته شود تا چنانچه در مهلت مذکور از انجام مبادلات الکترونیکی منصرف شود، بتواند بدون هیچ مشکلی از حق انصراف خویش استفاده کند و مثلاً اگر مبلغی پرداخت کرده آن را مسترد کند.

۴. ایجاد و امکان حمایت قضائی از مصرف کنندگان.

ب) حمایت از حریم خصوصی## افراد

فناوری اطلاعات اگرچه سهولت دست‌یابی افراد به اطلاعات را با کمترین هزینه فراهم کرده و این امر از لحاظ اقتصادی قابل توجه است ولی باید گفت که چنین امکانی دارای خطراتی نیز هست که مهمترین آنها نقض «حریم خصوصی» کاربران اینترنتی است. به این معنا که اطلاعات شخصی افراد که به مناسبت‌های مختلف در قالب

- Consumer

- Privacy

داده‌های الکترونیکی ثبت و در شبکه جهانی،پردازش و نگهداری می‌شوند هر لحظه با تهدید استفاده نادرست و غیرمجاز مواجه هستند.[۱۷]

منظور از حریم خصوصی مجموعهٔ اطلاعات شخصی و محرمانه فرد است. این اطلاعات در حیطه عموم ارایه نمی‌شود و خود فرد هم راضی به آگاهی یافتن افراد نسبت به آنها نیست. ممکن است این اطلاعات در مورد خانواده، شغل، اعتقادات مذهبی یا سیاسی، مسایل پزشکی و امثالهم باشد.

داشتن حریم خصوصی حق همهٔ افراد است و این حق باید از تعرض افراد مصون باشد. یعنی هر کس برای مسایل خانوادگی، شغلی، اعتقادات، سلایق و فعالیت‌های خویش حریمی قایل است که باید مورد احترام دیگران قرار گیرد. بنابراین وجود حمایت‌های قانونی برای جلوگیری از نقض حق حریم خصوصی در اینترنت از مهمترین جنبه‌های تعهدات اخلاقی و قانونی در قبال کاربران است.[۱۸]

حق حریم خصوصی که در کنوانسیون اروپایی حقوق بشر# نیز به رسمیت شناخته شده،[۱۹] از حقوق اساسی هر فرد است و در محیط فناوری اطلاعات شکل ملموس‌تری به خود می‌گیرد زیرا امروزه اولاً هر نوع اطلاعاتی می‌تواند به شکل داده‌های الکترونیکی درآید و در روی شبکه‌های باز ثبت و نگهداری شود. ثانیاً هر کس می‌تواند به سادگی از طریق ارتباط با شبکه جهانی اطلاع‌رسانی به داده‌های موجود دسترسی پیدا کند. از همین‌رو وجود حمایت‌های قانونی ضروری است تا چنانچه اطلاعات محرمانه افراد به شکل داده‌های الکترونیکی درآمد و به مناسبتی بر روی شبکه‌های باز اینترنتی پردازش و ذخیره شد، از دسترسی‌های غیرمجاز مصون بماند. به عبارت بهتر، دریافت، ذخیره، پردازش و ارسال داده‌های شخصی افراد باید با رضایت آنها، به اندازه ضروری و برای اهداف معین و قانونی صورت گیرد.[۲۰]

نکته آخر اینکه، اراده افراد تعیین کننده محرمانه بودن اطلاعاتشان است. بنابراین دستیابی به برخی از اطلاعات شخصی افراد که از نظر عرف محرمانه تلقی نمی‌شود ولی خود فرد می‌خواهد که کسی از آنها مطلع نشود، ممنوع است ولی اگر خود فرد بدون

- European Convention On Human Right.

هیچ تدبیری اطلاعات محرمانه‌اش را در معرض دسترسی قرار دهد، کسانی که از آنها اطلاع پیدا می‌کنند دیگر قابل مؤاخذه نیستند.

○ گفتار دوم: حقوق مالکیت معنوی#

از دیگر عرصه‌های حقوقی متأثر از فناوری اطلاعات حقوق مالکیت‌های معنوی است. بدین معنا که آفرینش‌های فکری افراد در قالب داده‌های الکترونیکی نیز از حقوق مالکیت معنوی برخوردار هستند. در فضای دیجیتالی نیز با وجود اینکه نوع کاملاً متفاوتی از متن، فیلم یا موزیک و... در قالب داده‌های الکترونیکی ارایه می‌شود ولی تمام مباحث مربوط به حقوق مالکیت‌های معنوی به شکل ملموس‌تری قابل بحث هستند. زیرا در محیط مجازی الکترونیکی مرزهای مادی و جغرافیایی برداشته شده و افراد قابلیت دسترسی بیشتری به آثار و آفرینش‌های فکری، هنری، ادبی، علمی و... دیگران دارند.

○ مبحث اول: تعریف و قلمرو حقوق مالکیت معنوی

مالکیت‌های معنوی یا فکری، حقوقی هستند که موضوع آنها یک شیء معین و مادی و ملموس نیست ولی دارای ارزش مالی بوده و از نظر اقتصادی قابلیت داد و ستد دارند. پس در واقع مالکیت معنوی شامل آفرینش‌های فکری ذهن و هنر انسان است که می‌توان آنها را روی اشیاء مادی و ملموس جای داد.[۲۱]

حقوق مالکیت معنوی امتیازات و حقوقی را در خصوص تولیدات فکری، هنر یا علم به انسان اعطا می‌کند که ایجاد کننده شکل ویژه و محدودی از مالکیت هستند و قلمرو آنها توسط قانون مشخص می‌شود. به عنوان مثال بعضی از حقوق مثل حق نشر (کپی رایت) فقط برای دوره‌های خاصی از زمان شناخته می‌شوند به طوری که در پایان این دوره زمانی معین حیات این حقوق هم پایان می‌پذیرد.[۲۲] البته برخی دیگر از اشکال حق مالکیت معنوی مثل علایم تجاری این قابلیت را دارند که به طور نامحدودی به حیات

- Intellectual Property

خود ادامه دهند.

○ مبحث دوم: وضعیت حقوق مالکیت‌های معنوی در محیط فناوری اطلاعات

تحول حقوق مالکیت‌های معنوی همواره به خاطر واکنش و مواجهه با چالش‌های مطرح شده به وسیلهٔ فناوری‌های نوین بوده است. در این خصوص اینترنت چالش‌های جدی و پیچیده‌ای را به وجود آورده است. امکان کپی‌برداری و پیاده‌سازی آثار فکری (متن، تصویر، موسیقی، نرم‌افزار و سایر موضوعات غیرملموس) از طریق نرم‌افزارهای جستجوگر# از شبکه، سهل و ساده شده است. کاربران می‌توانند آثار کپی و پیاده‌سازی شده را در اندک زمان ممکن و بدون هزینه تکثیر و توزیع کنند. بنابراین چنین امکانی می‌تواند خطر بالقوه‌ای برای نقض حقوق مؤلفین و پدیدآورندگان آثار فکری محسوب شود.[۲۳]

نوشته‌ها، تصاویر، آثار صوتی و تصویری، پایگاه‌های داده، نرم‌افزارها و صفحات وب در فضای الکترونیکی که همه آن مرکب از بیت## می‌باشد و امکان باز تولیدهای متعدد از آثار را فراهم آورده، باید مورد حمایت‌های قانونی ویژه‌ای قرار گیرد.

○ گفتار سوم: ادله اثبات دعوی (اعتبار اسنادی داده‌های الکترونیکی)

منظور از ادله اثبات دعوی دلایلی است که چنانچه فردی مدعی حقی باشد بتواند با استفاده از آنها حق خود را به هنگام بروز اختلاف و رسیدگی توسط دادرس اثبات کند. به عبارت بهتر مدعی حق باید بتواند دادرس را نسبت به محق بودن خود قانع کند و از نظر حقوقی معتبرترین چیز که باعث اقناع وجدانی دادرس می‌شود اصطلاحاً دلیل نام دارد.[۲۴]

از آنجایی که گسترش روزافزون مبادله داده‌های الکترونیکی شکل روابط و معاملات حقوقی افراد را دستخوش تغییر قرار داده، بنابراین در صورت بروز اختلاف در فضای مجازی ممکن است نحوهٔ رسیدگی و اثبات حق در برخی موارد با شکل سنتی آن

- Browsing Softwares

- Bit

متفاوت باشد. به عبارت بهتر بحث ادله اثبات دعوی در محیط حقوقی فناوری اطلاعات هم مطرح است. بنابراین ماهیت ادله الکترونیکی، قابلیت استناد و نحوهٔ نگهداری آنها باید مورد بررسی‌های حقوقی قرار گرفته و با مقایسه آن در فضای عادی، تفاوت‌های احتمالی شناسایی و در صورت وجود خلاء قانونی زمینه‌های وضع قانون فراهم شود. زیرا اسناد الکترونیکی باانواع کاغذی و سنتی آن ماهیتاً متفاوت هستند.

می‌دانیم که در فضای الکترونیکی تمام مبادلات از طریق انتقال داده‌ها صورت می‌گیرد و افراد از طریق سیستم اطلاع‌رسانی خویش با یکدیگر ارتباط برقرار می‌کنند و ممکن است برخی از روابط حقوقی آنها نیز از همین طریق صورت پذیرد. پس آنچه که بین آنها به عنوان وسیله‌ای برای بیان و اظهار اراده انشایی مورد استفاده قرار می‌گیرد، در قالب داده‌های الکترونیکی است که در صفحه سیستم اطلاع‌رسانی افراد ظاهر می‌شود.

حال چنانچه بین طرفین یک ارتباط حقوقی الکترونیکی اختلافی به وجود آید و چیزی به جز همان داده‌های الکترونیکی بین آنها برای اثبات ادعا وجود نداشته باشد، این سؤال مطرح می‌شود که آیا محتویات و مندرجات روی صفحه سیستم اطلاع‌رسانی می‌تواند به عنوان یک دلیل محکمه‌پسند مورد استفاده قرار گیرد؟ به عبارت ساده‌تر آیا سند الکترونیکی اعتبار حقوقی دارد و می‌توان آن را در زمره اسناد لازم‌الاجراء قرار داد؟ از آنجا که صحت انتساب سند به صاحب آن که موجب اعتبار حقوقی سند است از طریق مهر یا امضاء صورت می‌گیرد، بنابراین برای اینکه یک سند الکترونیکی هم اعتبار حقوقی لازم را داشته باشد باید بتوان آن را به صادرکننده منتسب کرد و این امر هم فقط از طریق امضاء امکان‌پذیر است و سند الکترونیکی نیز طبیعتاً باید دارای امضای الکترونیکی باشد. نتیجه اینکه شناسایی قانونی و قابل پذیرش بودن اسناد الکترونیکی به عنوان دلایل معتبر قانونی مستلزم شناسایی قانونی امضای الکترونیکی است.

لازم به توضیح است که چنانچه پیام داده‌ای فاقد امضاء باشد (مثل نامه الکترونیکی) به خودی خود اعتباری ندارد چون نمی‌تواند بیانگر واقعی اراده انشایی صادرکننده آن نسبت به مندرجات سند یا پیام داده‌ای باشد. بنابراین می‌توان گفت که یک پیام داده‌ای ارزش اسنادی ندارد بلکه فقط ارزش اماره‌ای دارد ولی ممکن است با تصدیق آن توسط منتسب‌الیه یا نظر کارشناسی اعتبار اسنادی کسب کند.

○ گفتار چهارم: مسؤولیت مدنی

در هر موردی که فردی به دیگری صدمه یا زیانی وارد می‌کند و موظف به جبران خسارت می‌گردد، گفته می‌شود که در مقابل وی مسؤولیت مدنی دارد. بنابراین موضوع بحث در مسؤولیت مدنی تعهدات افرادی است که با هم زندگی مشترک اجتماعی دارند. به عبارت بهتر امنیت، سلامت، شخصیت و مالکیت افراد باید مورد احترام و تعهد دیگران باشد تا در صورت نقض تعهدات مذکور، آنها موظف به جبران خسارت باشند. مسؤولیت مدنی به دو شعبه مهم تقسیم می‌شود:[۲۵]

۱ـ مسؤولیت قراردادی

۲ـ مسؤولیت غیرقراردادی

مسؤولیت‌های قراردادی در نتیجه اجرا نکردن تعهداتی به وجود می‌آیند که از یک عقد یا قرارداد ناشی شده‌اند. یعنی مسؤولیت قراردادی عبارت است از تعهدی که در نتیجه تخلف از مفاد قراردادهای خصوصی برای اشخاص ایجاد می‌شود. اما زمانی که بین دو نفر هیچ عقد یا پیمانی وجود ندارد و یکی از آنها به عمد یا به خطا به دیگری زیان می‌رساند در این حالت مسؤولیت را غیرقراردادی یا خارج از قرارداد می‌نامند. به عبارت بهتر در این نوع مسؤولیت هیچ قراردادی بین عامل ورود زیان و زیان‌دیده وجود ندارد و می‌توان گفت که خسارت وارده در اثر مسامحه یا بی‌مبالاتی فرد حاصل شده است.[۲۶]

○ مبحث اول: مسؤولیت مدنی و کاربرد آن در محیط فناوری اطلاعات

در محیط فناوری اطلاعات نیز مباحث مربوط به مسؤولیت مدنی مطرح بوده و شکل تازه‌ای به خود می‌گیرند. زیرا افرادی که در این محیط مجازی در حال تعامل با یکدیگر هستند ممکن است توسط فعل دیگری، خسارتی بر آنها وارد آید. طبق اصول کلی حقوقی هیچ خسارتی نباید جبران نشده باقی بماند و نهاد مسؤولیت مدنی که عهده‌دار جبران خسارت‌های وارده بر افراد است باید بتواند نقش خود را در محیط مجازی الکترونیکی در قبال افراد متضرر ایفا کند.

در مبحث مسؤولیت مدنی در فناوری اطلاعات آنچه که بیشتر مورد توجه قرار

می‌گیرد حمایت از کاربران اینترنتی در مقابل تهیه‌کنندگان خدمات اینترنتی،# اپراتورهای شبکه‌های اینترنتی،## اشخاص ثالث مورد اعتماد### و دیگر کاربران اینترنتی و مسؤولیت‌های قراردادی و غیرقراردادی نرم‌افزارها است.[۲۷] این امکان همواره وجود دارد که کاربران به دلیل تقصیر یکی از اشخاص فوق‌الذکر در انجام وظایف قانونی خویش (قصور در تهیه، ارسال، وصول، پردازش و حفظ و نگهداری داده‌های الکترونیکی) خسارت‌هایی را متحمل شوند یا حقوق مالکیت‌های معنوی آنها نقض شود. به عنوان مثال تأمین‌کنندگان خدمات اینترنتی می‌توانند در جلوگیری یا کاهش نقض حقوق مالکیت‌های فکری نقش مهمی ایفا کنند. بنابراین قواعد و مقررات مسؤولیت مدنی باید با توجه به محیط خاص سایبر از عهده جبران خسارات وارده بر افراد برآیند. از همین‌رو مباحث مربوط به شرایط و مبانی مسؤولیت مدنی در محیط الکترونیکی باید مورد بررسی‌های حقوقی قرار گیرند چرا که ممکن است نوع ضرر، نحوه ایراد و طرق اثبات آن تا حدودی متفاوت باشد.[۲۸]

○ مبحث دوم: شرایط تحقق مسؤولیت مدنی در محیط فناوری اطلاعات

برای تحقق مسؤولیت مدنی وجود ارکان ذیل ضروری است:[۲۹]

۱- وجود ضرر

۲- ارتکاب فعل زیان‌بار

۳- رابطه سببیت بین فعل زیان‌بار و ضرر

الف) وجود ضرر قابل جبران

برای تحقق مسؤولیت مدنی در محیط فناوری اطلاعات هم وجود ارکان فوق ضروری است. ورود ضرر در استفاده از رایانه در فضای مجازی امری اجتناب‌ناپذیر است. یعنی ممکن است موقعیت‌هایی به وجود آید که در به کارگیری رایانه در محیط فناوری اطلاعات خساراتی به افراد وارد آید. بنابراین وجود ضرر به عنوان یکی از ارکان

- Internet Service Providers.

- Network Operators.

- Trusted Third Parties (TTPs).

مسؤولیت مدنی امری بدیهی و قابل تصور است. ضرر را می‌توان به دو نوع متفاوت تقسیم کرد:[۳۰]

۱ـ ضرر مادی مثل ازبین رفتن مال یا کاهش ارزش آن.

۲ـ ضرر معنوی مثل لطمه به حیثیت، شهرت و عواطف افراد یا ایجاد تألم و تأثر روحی.

در محیط فناوری اطلاعات هر دو نوع ضرر ممکن است برای افراد حادث شود. اگرچه استفاده از رایانه در محیط مجازی، بیشتر سبب ورود خسارات مالی به افراد است ولی به هیچ وجه نمی‌توان ضررهای معنوی را نادیده گرفت زیرا در این محیط جدید به سهولت ممکن است افراد مورد هتک حرمت قرار گیرند. حتی می‌توان گفت در محیط مجازی این گونه مسایل از اهمیت بیشتری برخوردار می‌باشد چرا که امکان انتشار داده‌های الکترونیکی در سطح گسترده و قابلیت دسترسی تمام افراد به آنها، مسأله را کمی بغرنج‌تر می‌سازد.

ب) ارتکاب فعل زیان‌بار

از دیگر شرایط تحقق مسؤولیت مدنی، ارتکاب یک فعل زیان‌بار است. منظور از فعل زیان‌بار عملی است که مبتنی بر تقصیر (اعم از تعدی یا تفریط) باشد. یعنی فرد باید به دلیل بی‌احتیاطی، بی‌مبالاتی، سهل‌انگاری، عدم مهارت، تقصیر و یا عدم رعایت تکالیف قانونی، فعلی را انجام دهد تا بتوان او را ملزم به جبران خسارات دانست.

از آنجایی که فناوری اطلاعات و ارتباطات محیط جدیدی را فراهم آورده است، لذا مشکلات مربوط به مسؤولیت مدنی در این زمینه هنوز به طور کامل شناخته نشده است. بنابراین در شناسایی تقصیر می‌توان از کارشناسان مربوطه استفاده کرد تا هیچ خسارتی بدون جبران باقی نماند.

ج) رابطه سببیت

در تحقق مسؤولیت مدنی، ورود ضرر و نیز ارتکاب فعل زیان‌بار (تقصیر) به تنهایی برای مسؤول شناختن فرد کافی نیست بلکه رکن دیگری که همان وجود رابطه سببیت بین زیان وارده و عمل زیان‌بار است نیز ضرورت دارد. اثبات این رابطه سببیت با زیان‌دیده است. یعنی وی باید رابطه علّی و معلولی بین عمل ارتکابی و ضرر وارده را

اثبات کند. احراز و اثبات رابطه سببیت در بیشتر موارد کار بسیار دشواری است به ویژه زمانی که اسباب و علل گوناگونی در تحقق ضرر دخیل باشند و نتوان به طور قطع یک عامل را سبب اصلی ورود ضرر دانست.

برای احراز رابطه سببیت، حقوقدان‌ها نظریات متفاوتی ارایه کرده‌اند که هیچ کدام به طور قطع نمی‌توانند راه‌گشای مسایل پیچیده مسؤولیت مدنی باشند. لذا به نظر می‌رسد که در هر مورد خاص باید با توجه به اوضاع و احوال حاکم، مسأله را بررسی کرده و با در نظر گرفتن معیار عرفی یک انسان متعارف رابطه سببیت بین فعل زیان‌بار و وجود ضرر را احراز کرد.

● بخش دوم: حقوق فناوری اطلاعات: حقوق عمومی

○ گفتار اول: حقوق جزا

طرح بحث: گسترش روزافزون ارتباطات داده‌ای* سبب ایجاد و شکل‌گیری جرایم جدیدی شده که از نظر ماهیت و شیوه ارتکاب با انواع مشابه آن در شکل سنتی و کلاسیک متفاوت هستند و شاید بتوان گفت که آثار سوء و آسیب‌های وارده در اثر ارتکاب این گونه جرایم در بعضی موارد گسترده‌تر است. این دسته از جرایم جدید ابتدا نیازمند شناسایی قانونی از طریق وضع یا اصلاح قوانین کیفری هستند. سپس باید نهادها و تشکیلات جدیدی برای کشف، پیگیری و رسیدگی به جرایم مذکور در اختیار مقامات تحقیق قرار بگیرد. بسیاری از کشورهای پیشرو (استرالیا، کانادا، فیلیپین و...) و نهادهای بین‌المللی (سازمان همکاری و پیشرفت اقتصادی، شورای اروپا و...) همگام با تحولات ایجاد شده در زمینه جرایم مربوط به فناوری اطلاعات برای وضع قوانین کیفری جدید یا اصلاح قوانین سابق خود اقداماتی انجام داده‌اند ولی هنوز مقتضیات قانونی لازم برای مواجهه با جرایم فناوری اطلاعات به طور کامل فراهم نشده است. اگرچه وضع قانون فقط بخشی از مشکلات را حل می‌کند ولی گسترش دامنه قانون به درون فضای شبکه‌های رایانه‌ای و حمایت‌های قانونی لازم اقدام بسیار مهمی در راستای مقابله با

- Data Communications.

مجرمین احتمالی و ایجاد محیطی امن برای انجام مبادلات الکترونیکی است. محیط حقوقی فناوری اطلاعات در بخش حقوق جزا باید از دو جنبه داخلی (ماهوی و شکلی) و بین‌المللی مورد توجه قرار گیرد.

○ مبحث اول: حقوق جزای داخلی

الف. حقوق جزای ماهوی

طبق یکی از اصول پذیرفته شده قانون جزا یعنی اصل قانونی بودن جرایم و مجازات‌ها، فقط فعل یا ترک فعلی را می‌توان به عنوان جرم شناخت که در قانون برای آن مجازاتی تعیین شده باشد. حال با توجه به اینکه در فضای الکترونیکی جرایمی ظهور پیدا کرده‌اند که اگرچه ممکن است ماهیتاً با انواع کلاسیک خود شباهت‌هایی داشته باشند ولی به لحاظ شیوه ارتکاب کاملاً متفاوت هستند و در بستری اتفاق می‌افتند که ممکن است عنصر مادی برخی از آنها (مثل کلاهبرداری یا جعل رایانه‌ای) در مقایسه با انواع عادی این جرایم تفاوت داشته باشند و به عبارت ساده‌تر غیرقانونی بودن آنها کاملاً روشن نیست و این امر دادرس را در امر رسیدگی به جرایم مذکور و تعیین مجازات مرتکبین آنها با مشکل مواجه خواهد کرد. بنابراین باید دید آیا ویژگی‌هایی که قوانین کیفری برای بعضی از جرایم احصاء کرده‌اند را می‌توان برای همان جرم در فضای مجازی (الکترونیکی) هم تصور کرد؟ آیا می‌توان بعضی از جرایم که فقط در محیط فناوری اطلاعات قابل تصور هستند(مثل شنود الکترونیکی داده‌ها، دسترسی‌های غیرمجاز به اطلاعات داده‌ای و...) را تحت شمول قوانین کیفری فعلی درآورد.

در همین راستا و به منظور یکنواخت کردن سیاست جنایی مربوط به تقنین جرم رایانه‌ای تاکنون انواع مختلفی از تقسیم‌بندی جرایم مربوط به فناوری اطلاعات، توسط برخی از کشورها و نهادهای بین‌المللی ارایه شده که به بعضی از انواع مهم آنها اشاره می‌شود.[۳۱]

● **تقسیم‌بندی کمیته تخصصی جرایم رایانه‌ای شورای اروپا از جرایم ماهوی در سال ۱۹۸۹م:**

الف) فهرست حداقل جرایم ضروری:

۱ـ کلاهبرداری رایانه‌ای

۲ـ جعل رایانه‌ای
۳ـ ایراد خسارت به داده‌ها یا برنامه‌های رایانه‌ای
۴ـ خرابکاری رایانه‌ای
۵ـ دستیابی‌های غیرمجاز
۶ـ استراق سمع غیرمجاز
۷ـ تکثیر غیرمجاز برنامه‌های حمایت شده رایانه‌ای
۸ـ تکثیر غیرمجاز یک توپوگرافی

ب) فهرست اختیاری جرایم:

۱ـ تغییر داده‌ها یا برنامه‌های رایانه‌ای
۲ـ جاسوسی رایانه‌ای
۳ـ استفاده غیرمجاز از رایانه
۴ـ استفاده غیرمجاز از برنامه‌های رایانه‌ای حمایت شده
۵ـ تکثیر غیرمجاز برنامه‌های رایانه‌ای مورد حمایت قانون با در نظر گرفتن انواع تقسیم‌بندی‌های پیشنهادی موجود شاید بتوان جرایم فناوری اطلاعات و ارتباطات را به طور کلی در دو دسته جداگانه مورد بررسی قرارداد:[۳۲]

۱. **جرایم رایانه‌ای#**: منظور از جرایم رایانه‌ای جرایمی هستند که از سوی یک رایانه، شبکه و یا هر سیستم اطلاع‌رسانی دیگر صورت گرفته می‌شود و یا علیه آنها صورت می‌گیرد. بنابراین موضوع، ابزار و بستر ارتکاب این گروه از جرایم، رایانه یا شبکه‌های رایانه‌ای است. مثل جرایم مربوط به داده‌ها (سرقت داده و تغییر داده و شنود الکترونیکی داده‌ها) و جرایم مربوط به شبکه (اختلال در شبکه و خرابکاری و صدمه به شبکه) و جرایم مربوط به نفوذیافتگی (دسترسی غیرمجاز به سیستم اطلاع‌رسانی دیگری و دستیابی به اسرار برخلاف قانون).

۲. **جرایم از طریق رایانه##**: این دسته از جرایم به مواردی اطلاق می‌شوند که تحقق آنها مستلزم استفاده از رایانه و یا هر سیستم اطلاع‌رسانی است. به عبارت بهتر رایانه فقط وسیله‌ای برای ارتکاب برخی از جرایمی است که پیش از ظهور فناوری اطلاعات از

- Computer Crimes.

- Computer Related Crimes.

طریق دیگری (روش‌های سنتی) محقق می‌شده ولی اکنون رایانه نحوه ارتکاب آن را تغییر داده است. در واقع جرایم از طریق رایانه، عناوین مجرمانه‌ای هستند که پیش از این در محیط غیرالکترونیکی هم وجود داشته‌اند و قوانین مربوطه برای آنها مجازات‌هایی پیش‌بینی کرده‌اند ولی در حال حاضر این جرایم در محیط مجازی الکترونیکی شکل تازه‌ای به خود گرفته‌اند و در بستری کاملاً متفاوت در حال رخ دادن و گسترش یافتن هستند. مثل جرایم علیه اشخاص (توهین، افتراء و...) جرایم علیه اموال و مالکیت (کلاهبرداری، جعل و...) و یا جرایم علیه امنیت و مصالح عمومی (جاسوسی، تشویش اذهان عمومی و...) انواع این جرایم توسط قوانین کیفری احصاء شده و برای هر یک مجازات‌هایی نیز در نظر گرفته شده است. در بیشتر موارد جرایم مذکور ماهیتاً تفاوت چندانی با انواع مشابه خود در محیط الکترونیکی ندارند. لذا در صورت تشابه در عنصر مادی و معنوی می‌توان برای رسیدگی و تعیین مجازات مرتکبین جرایم مذکور به قوانین کیفری موجود، رجوع کرد (به عنوان مثال تحقق جرم افتراء با استناد به ماده ۶۱۷ق.م.ا از هر طریقی که ارتکاب یابد مشمول مقررات این ماده خواهد بود.) لیکن برخی دیگر از جرایم را می‌توان یافت که برای مجازات مرتکبین آنها در فضای مجازی، به سختی بتوان به قوانین فعلی استناد کرد. مثلاً به دشواری می‌توان پذیرفت که جرایمی همچون جعل یا کلاهبرداری رایانه‌ای ماهیتاً از نظر حقوقی با انواع کلاسیک آن یکسان هستند و مرتکبین آنها را باید با همین قوانین موجود قابل مجازات دانست. حال آنچه که در این بخش اهمیت دارد این است که با درنظر گرفتن ویژگی‌های خاص محیط الکترونیکی، جرایم مذکور بازشناسی شده و عناصر متشکله و شرایط لازم برای تحقق آنها به طور کامل تبیین شود. روزآمد سازی قوانین کیفری و پیش‌بینی مجازات‌های متناسب برای این دسته از جرایم می‌تواند محیط امن مجرمین احتمالی را به مخاطره بیاندازد و تا حد زیادی دفاع جامعه الکترونیکی را در برابر تجاوزهای بیرونی فراهم سازد.

ب. حقوق جزای شکلی (آیین دادرسی کیفری)

منظور از حقوق جزای شکلی یا آیین دادرسی کیفری مجموعه اصول و مقرراتی است که برای کشف و تحقیق جرایم و تعقیب مجرمان و نحوه رسیدگی و صدور رأی و تجدیدنظر و اجرای احکام و تعیین وظایف و اختیارات مقامات قضائی وضع شده است.[۳۳] همانطور که پیداست مراحل آیین دادرسی کیفری از مرحله کشف جرم تا

صدور حکم و تجدیدنظر از آن را دربر می‌گیرد.

محیط حقوقی فناوری اطلاعات هم در این بخش از فرآیند فوق مستثنی نیست و رسیدگی کیفری به یک جرم در فضای مجازی نیز تابع همین مراحل است ولی آنچه که باید مورد توجه قرار گیرد ویژگی‌ها و مقتضیات خاص محیط الکترونیکی است که سازگار شدن قوانین و مقررات آیین دادرسی کیفری را با این محیط جدید می‌طلبد.

برای توضیح بیشتر و ملموس‌تر شدن وضعیت آیین دادرسی کیفری در محیط حقوقی فناوری اطلاعات بحث خود را در دو قسمت مورد بررسی قرار می‌دهیم.

۱.ب. مرحله کشف جرم، تعقیب و انجام تحقیقات مقدماتی

اطلاعات عرضه شده در قالب داده‌های الکترونیکی، شکل تازه‌ای از مراحل آیین دادرسی کیفری و ادله اثبات دعوی را در محیط حقوقی فناوری اطلاعات فراهم می‌آورد که نیازمند قوانین و مقررات جدید و ویژه‌ای در خصوص کشف، تعقیب، تحقیقات مقدماتی و رسیدگی‌های کیفری است. یعنی مقرراتی که در خصوص کشف، جمع‌آوری و نگهداری داده‌های الکترونیکی و استفاده از آنها در تحقیقات جنایی و همچنین ارایه ادله الکترونیکی به هنگام رسیدگی در محاکم پاسخگو باشند. بنابراین مقررات آیین دادرسی کیفری فعلی در زمینه ادله اثبات دعوی کیفری باید به طور مشابهی در یک سیستم مجازی الکترونیکی هم اجرا شده و از همان قابلیت پیشین برخوردار باشد. به عبارت ساده‌تر، ابزارهای قانونی که طبق مقررات آیین دادرسی کیفری به مقامات تحقیق اعطا شده، هم‌اکنون باید با طبع ویژه تحقیقات جنایی در سیستم‌های الکترونیکی سازگار شوند. مثلاً در محیط الکترونیکی نیز مانند وضعیت کلاسیک، باید مقامات تحقیق این اجازه را داشته باشند که تحت همان شرایط مشابه در روش‌های سنتی، شبکه‌ها و سیستم‌های اطلاع‌رسانی را تفتیش و در صورت لزوم داده‌ها با برنامه‌های الکترونیکی را توقیف کنند.

در محیط حقوق فناوری اطلاعات، هدف از تحقیقات جنایی در مورد جرایم مربوطه گردآوری و تحصیل داده‌های معین از شبکه‌ها و سیستم‌های اطلاع‌رسانی است و مسلماً این امر نیاز به دسترسی مقامات تحقیق به تمام اقدامات فنی لازم برای جمع‌آوری و حفظ داده‌هاست.

قوانین فعلی آیین دادرسی کیفری شرایط لازم را برای تحت پوشش قرار دادن

رسیدگی به جرایم حقوق فناوری ندارند و این خلاء به ماهیت ویژه جرایم مذکور باز می‌گردد که در نتیجه مشکلات، موانع و محدودیت‌هایی را در سر راه مقامات تحقیق ایجاد خواهد کرد.

۲ب. تشخیص محل وقوع جرم

منظور از محل وقوع جرم مکانی است که جرم در آنجا اتفاق افتاده است. در مورد جرایمی که در محیط غیرالکترونیکی رخ می‌دهد تعیین محل وقوع جرم کار ساده‌ای است ولی تشخیص این امر در محیط الکترونیکی (فضای مجازی) کمی دشوار به نظر می‌رسد زیرا یکی از ویژگی‌های اصلی محیط فناوری اطلاعات ازبین بردن ظرف مکان و به عبارت بهتر از میان برداشتن مرزهای مادی و جغرافیایی است. از طرفی بحث صلاحیت‌ها کاملاً به موقعیت جغرافیایی وابسته است. بنابراین جمع بین این دو خصیصه متفاوت، برای تشخیص و تعیین صلاحیت رسیدگی به جرایم مربوط به فناوری اطلاعات ضروری است. برای این کار ابتدا لازم است که ماهیت جرایم مزبور مورد شناسایی قرار گیرد.

جرایمی که در فضای مجازی الکترونیکی رخ می‌دهند به گونه‌ای هستندکه محل وقوع عنصر مادی با محل حصول نتیجه آنها متفاوت است. به عبارت بهتر عنصر مادی آن در یک محل واقع می‌شود و در نتیجه یا آثار سوء آن در محل دیگری ظاهر می‌شود. بنابراین احتمال دارد که محل حصول نتیجه در این گونه جرایم، خارج از حوزه قضائی محلی باشد که عنصر مادی جرم در آنجا ارتکاب یافته است. به عنوان مثال ممکن است فردی در محل «الف» یک پایگاه داده‌ای را در محل «ب» برای عملیات مجرمانه‌ای در نظر گرفته که نتیجه آن در محل «ج» ظاهر می‌شود. مشکلات مربوط در این محیط به گونه‌های دیگری نیز قابل تصور است. یعنی از حیث مرتکبین آن، این احتمال می‌رود که فردی در محل «الف» با معاونت و دستیاری فرد یا افراد دیگری در محل «ب» مرتکب جرمی در محل «ج» شوند. این ویژگی خاص محیط فناوری اطلاعات که امکان تعدد مکانی مرتکب، بزه دیده و محل نتیجه جرم را فراهم کرده در مبحث صلاحیت کیفری باید مورد توجه قرار گیرد.

○ مبحث دوم: حقوق جزای بین‌المللی

اصطلاح حقوق جزای بین‌الملل معمولاً در سه معنی به کار می‌رود.[۳۴]

۱ـ جنبه‌های بین‌المللی حقوق جزای داخلی به این معنی که دادگاه‌های یک کشور در دعاوی مشتمل بر یک عنصر خارجی باید چگونه تصمیم‌گیری کند.

۲ـ جنبه‌های جزایی حقوق بین‌المللی به معنی آن دسته از اصول و قواعد حقوق بین‌الملل که برای دول الزاماتی را در مورد محتوای حقوق جزای داخلی آنها ایجاد می‌کند، مثلاً اینکه آنها باید برخی از جرایم برخوردار از خصیصه بین‌المللی را مجازات و یا در قوانین خود رعایت موازین حقوق بشر را لحاظ کنند.

۳ـ حقوق جزای بین‌الملل به معنای خاص و دقیق کلمه به این معنا که یک محکمه کیفری بین‌المللی در هر صورت باید آن را اجرا کند.

یکی از ویژگی‌های خاص محیط حقوق فناوری اطلاعات بی‌اثر ساختن مرزهای فیزیکی و جغرافیایی است بنابراین از حیث تحقق یک جرم در این محیط به سادگی ممکن است که با بیش از یک کشور در ارتباط باشد. نتیجتاً این بحث مطرح می‌شود که هنگامی که چند کشور با یک جرم مرتبط هستند، دادگاه کدامیک از آنها صلاحیت رسیدگی به جرم مزبور را دارند. پس بدون تردید حقوق جزای بین‌الملل در محیط حقوقی الکترونیکی جایگاه مهمی پیدا می‌کند. مشکلات موجود بر سر راه اجرای فناوری اطلاعات در این بخش، چگونگی تعیین صلاحیت کیفری دولت‌ها، نحوه مجازات و استرداد مجرمین و رسیدگی به جرایمی است که جنبهٔ بین‌المللی دارند.

قوانین جزایی برای پاسخگویی به نیازهای تقنینی ناشی از فناوری اطلاعات در زمینه حقوق جزا، برای رویارویی با مجرمین بالقوه، نیازمند اصلاح یا تغییر است به همین دلیل بسیاری از کشورها اقدام به وضع یا اصلاح قوانین جزایی خود کرده‌اند.[۳۵]

○ گفتار دوم: حقوق مالیه (حقوق مالیاتی)#

سیاست مالیاتی مبادلات الکترونیکی از دیگر مباحثی است که در بحث سیاست‌گذاری عمومی در محیط فناوری اطلاعات مورد توجه قرار می‌گیرد. چالشی که

- Taxation Law.

در این خصوص دولت‌ها با آن مواجه هستند وضع قوانین و تنظیم سیاست‌های مالیاتی در محیطی است که مکان در آن معنی ندارد. امروزه ظهور زیر ساختمان‌های اطلاعاتی جهانی توجه دولت‌ها را به مسایل مالیاتی نیز معطوف کرده است. به عبارت بهتر، نبود مرزهای جغرافیایی در مبادلات الکترونیکی و سرعت بالای انجام کار در محیط سایبر، مسؤولان ذیربط را با مشکل کنترل و تعیین میزان مالیات مواجه می‌سازد و می‌توان گفت که اعمال مقررات مالیاتی نسبت به مبادلات الکترونیک کار دشواری است. بحث حقوق مالیاتی در فضای مجازی بیشتر در زمینه تجارت الکترونیک مطرح می‌شود زیرا طبیعت ناملموس و بین‌المللی فعالیت‌ها و مبادلات تجاری الکترونیکی بر پیچیدگی تنظیم سیاست‌های مالیاتی می‌افزاید و این امر موجب تحول در حقوق مالیاتی شده است.[۳۶]

تعیین چارچوب قانونی و وضع قوانین مالیاتی و اعمال آنها در فضای عادی (غیرالکترونیکی) کار ساده‌ای نیست و امروزه اینترنت با ایجاد فضای مجازی بر پیچیدگی‌های آن افزوده است. در ساختار جدید مالیاتی محل تجارت و مبادلات الکترونیکی، محل مشتری (یا کاربر)، محل تأمین‌کننده خدمات اینترنتی مشتری (یا کاربر) و محل سرور* (شرکت فروشنده یا ارایه کننده خدمات) معلوم نیست.[۳۷] مسلماً قوانین مالیاتی فعلی نمی‌توانند در مورد مبادلات الکترونیکی داده‌ها مورد استفاده قرار گیرند. زیرا فاکتورهای موجود در خصوص تعیین میزان مالیات در معاملات عادی، قابلیت انطباق در محیط سایبر را ندارند. نظارت و کنترل بر انجام مبادلات تجاری الکترونیکی به منظور وضع مالیات، گونه کاملاً متفاوتی با وضعیت فعلی آن دارد. بنابراین سیاست مالیاتی مبادلات الکترونیکی از مسایل مهم در بحث سیاست‌گذاری عمومی در عصر فناوری اطلاعات محسوب می‌شود.

○ گفتار سوم: دسترسی آزاد به اطلاعات##**

از ویژگی‌های بارز عصر فناوری اطلاعات و ارتباطات، جریان باز اطلاعات است که در واقع جزء لاینفک جامعه الکترونیکی نیز محسوب می‌شود. به عبارت بهتر در فضای سایبر اطلاعات باید همواره در جریان باشند و هر کس بتواند از طریق شبکه‌های باز

- Server

- Free Access to Information.

اینترنتی به اطلاعات مورد نظر خویش دست یابد. آنچه که بیشتر در دستیابی اطلاعات مطرح می‌شود، لزوم دسترسی شهروندان به اطلاعات و اسناد نهادها و مراجع دولتی است (منظور هر نوع نوشته، تصویر یا اطلاعاتی است که به وسیله مراجع دولتی تنظیم و نگهداری می‌شود و در طبقه‌بندی اسناد محرمانه نیز قرار نمی‌گیرد). اهمیت این امر به اندازه‌ای است که امروزه حق آگاهی یافتن به اطلاعات دولتی از جمله حقوق اساسی بشر در جوامع مدرن تلقی می‌شود. دستیابی عموم جامعه به اطلاعات رسمی و اداری که از طریق افزایش آگاهی‌های سیاسی ـ اجتماعی مردم می‌تواند به تحقق بهتر دموکراسی بیانجامد علام بر منافع سیاسی ـ اجتماعی منافع اقتصادی فراوانی را نیز به دنبال خواهد داشت. چرا که این امر برای تحقق یک اقتصاد آزاد همراه با رقابت نیز ضروری به نظر می‌رسد و به طور کلی می‌توان گفت جریان آزاد اطلاعات یکی از عوامل پیشرفت جوامع باز است.

اما آنچه که دولت‌ها را در بحث سیاست‌گذاری عمومی در مورد جریان باز اطلاعات به چالش فراخوانده، مباحث حقوقی این مقوله است. به عبارت ساده‌تر چارچوب حقوقی جریان باز اطلاعات و اصول و ضوابط دستیابی باید به طور کامل برای شهروندان مشخص و معلوم باشد. اگرچه در عصر فناوری اطلاعات، دسترسی آزاد افراد به اطلاعات از حقوق شهروندی آنها محسوب می‌شود ولی بدیهی است که این حق نمی‌تواند به طور نامحدود و بدون هیچ قید و شرطی اعمال شود. بلکه محدودیت‌ها و موانعی وجود دارد که در برخی موارد حق مذکور را از مطلق بودن خارج می‌سازد. به عنوان مثال در بحث حمایت از داده‌های شخصی و حق حریم خصوصی که قبلاً در خصوص آن صحبت شد، لذا برخی از اطلاعات و داده‌های افراد که در حوزه حریم خصوصی آنها قرار می‌گیرد باید مورد احترام دیگران و حمایت قانون قرار گیرد. یعنی در بحث حریم خصوصی برخلاف حق دسترسی آزاد به اطلاعات، هیچ کس نمی‌تواند به اطلاعات محرمانه و حفاظت شده افراد آگاهی پیدا کند. در اینجاست که پای حقوق به میان کشیده می‌شود تا در یک جامعه اطلاعاتی، بین جریان باز اطلاعات و محرمانگی اطلاعات تعادل و توازن ایجاد کند. از همین‌روست که لزوم قانونمند بودن جریان باز اطلاعات مطرح می‌شود.

آنچه که در محیط حقوقی فناوری اطلاعات در خصوص موضوع مورد بحث باید

مورد توجه قرار گیرد. ابتدا به رسمیت شناختن حق دسترسی عموم به اطلاعات و سپس ضابطه‌مند کردن استفاده از این حقوق است. به عبارت بهتر باید مفهوم و میزان دستیابی به اطلاعات و موارد استثناء آن به خوبی روشن شود.

چنانچه قانون‌مند کردن دسترسی آزاد به اطلاعات به نحو صحیحی صورت پذیرد نه تنها با اصول محرمانگی برخی از اطلاعات (مثل اطلاعات شخصی یا امنیتی و...) تداخل پیدا نمی‌کند بلکه زمینه رشد و توسعه سیاسی ـ اجتماعی جامعه را نیز فراهم می‌سازد، بنابراین ضرورت تدوین قانون آزادی اطلاعات کاملاً محسوس است.[۳۸]

● پی‌نوشت‌ها:

1- William H. Dutto, Information and Communication Technologies, p 20. Oxford University Press,1996.

2- ibid, p 32.

3- Stephen Chen, strategic management of e-Business, p 2,John Wiely & sons Piblishing, London 2001.

4- Michael Chissick, Alistair Kelman, Electronic Commeree: Law and Practice, p 17 Sweet & Maxwell, London. 2002,p.

5- Ian J.Liod, Information Technology law, p 11, Butterworths, London, Edinburgh, Dublin, 1997.

6- Stephen Chen, strategic management of e-Business, p4.

۷ـ در ایران نیز پیش‌نویس قانون تجارت الکترونیک تهیه و به تصویب مجلس رسیده اما هنوز لازم‌الاجرا نشده است.

8- ibid, p 299.

9- Digital Certificate and e-signatures, CSI 28 the Annual Computer Security conference, October 2001, Washington D.C, by Ben Rothke.

10- www.counterpanc. Com, Cryptography, by Bruce Sehneider.

11- www.infomosaic. Com, Digital Signature, by Aki kaniel.

12- Geffrey Ravport, Bernard laworski, e-commerce, p 378 Mc Graw-Hill, International Edition 2001.

۱۳ـ صادقی نشاط، امیر، حقوق تجارت الکترونیک، نشریه کانون وکلای دادگستری، ش ۱۷۰، ص ۷۹.

۱۴ـ نوری، محمدعلی و نخجوانی، رضا، حقوق تجارت الکترونیکی، ص ۱۵۰، انتشارات گنج دانش، چاپ اول، ۱۳۸۲.

15- Jefrry H.Matsuura, Security, Rights and Liabilities in E-commerce, p 172, Artech House Inc., London 2002.

16- Uncitral Model law On Electronic Commerce, 1996.

۱۷- یان لوید، فناوری و نظارت، ترجمه وصالی ناصح، مرتضی، خبرنامه حقوق فناوری، ش۶، ص۲۳.

18- Jooel Reedy, Shauna Schullo, Kenneth Zimmerman, Electronic Marketing, p 387. The Dryden press, Harcourt College publishers, 2000.

۱۹- ماده ۸ کنوانسیون اروپایی حقوق بشر مقرر می‌دارد: «هر کسی حق دارد که برای زندگی خصوصی و خانوادگی، خانه و مکاتباتش احترام قائل شود.» مواردی که کنوانسیون مذکور به عنوان حریم خصوصی شناخته شده‌اند حق آزادی بیان و حق تحصیل اطلاعات را نیز شامل می‌شود.

20- David Bainbridge, Introduction to Computer law, p 405, Long Man ltd, 2000.

۲۱- نوروزی، علی‌رضا، حقوق مالکیت فکری، ص ۱۹، نشر چاپار، ج اول، تهران پاییز ۸۱.

۲۲- طبق ماده ۱۲ قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان مصوب ۱۳۴۸، حقوق مادی پدیدآورنده در طول حیات وی باقی است و بعد از پدیدآورنده نیز بهمدت ۳۰ سال از تاریخ فوت متعلق به وراث یا شخصی است که این حق به موجب وصیت به او منتقل شده است.

23- Timothy D. Casey, ISP Liability, Survival Guide, p99, Wiley Computer Publishing, 2000.

۲۴- صدرزاده اقشار، سیدمحسن، ادله اثبات دعوی در حقوق ایران، ص ۳، مرکز نشر دانشگاهی تهران، ج دوم، ۱۳۷۰.

۲۵- کاتوزیان، ناصر، مسؤولیت مدنی، الزام‌های خارج از قرارداد، ص ۳۸، شرکت سهامی انتشارات بهمن و برنا.

۲۶- همان، ص ۷۲.

27- Ian J.Lioyd, Information Technology law, p 412.

28- Timothy E.Casey, ISP Liability, Survival Guide, p 102.

۲۹- کاتوزیان، ناصر، دوره مقدمایت حقوق مدنی (وقایع حقوقی)، ص ۳۷، شرکت سهامی انتشارات بهمن و برنا.

۳۰- دکتر ساوارایی، حقوق و کامپیوتر، جزوه درسی، دانشگاه شهید بهشتی.

۳۱- به نقل از خبرنامه انفورماتیک، ش ۸۱، ص ۳۸.

32- prof. Dr, Ulrich Sieber, Legal Aspects of Computer-Related Crime in the Information Society, p178 to 198, University of Wurzburg, 1998.

۳۳- ماده یک قانون آیین دادرسی دادگاه‌های عمومی و انقلاب در امور کیفری.

۳۴- میرمحمد صادقی، حسین، حقوق جزای بین‌الملل، ص ۱۹، نشر میزان، چاپ اول، پاییز ۱۳۷۷.

۳۵- در ایران لایحه جرایم رایانه‌ای توسط قوهٔ قضائیه در حال تدوین است.

36- Michael Chissick, Alistair Kelman, Electronic Commerce: Law and Practice, p 259.

37- Geffrey Ravport, Bernard laworski, e-commerce, p 589.

۳۸- طرح اولیه پیش‌نویس قانون آزادی اطلاعات ایران تهیه شده و در حال حاضر بر روی پایگاه اطلاع‌رسانی شورای عالی انفورماتیک موجود و قابل دسترسی است.