Conference on World New Scientific Researches in Management, Accounting, Law and Social Sciences
23 Nov 2017
venue: Conference Center of Shiraz University International Division
96170-82805

بررسی مسئولیت مدنی ناشی از ارتباطات الکترونیکی

حامد احمد زاده
دانشجوی کارشناسی ارشد حقوق خصوصی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات، تهران
hamed.ahmadzade64@gmail.com
علی خوشدل واجاری
کارشناسی ارشد حقوق خصوصی، دانشگاه آزاد اسلامی واحد تهران مرکز
Ali.khoshdelvajari@gmail.com

چکیده

مسئولیت مدنی یکی از مهم‌ترین و حساس‌ترین بحث‌های حقوقی است که دقت خاصی را می‌طلبد. بحث مسئولیت مدنی ناشی از ارتباطات الکترونیکی از جمله مهمترین مباحث حقوقی فناوری اطلاعات و ارتباطات می باشد. به‌طور کلی افعال زیانبار در ارتباطات الکترونیک را می‌توان تحت‌عنوان نفوذ غیرمجاز، سرقت مطالب و هویت، انتقال و افشای غیرمجاز در زمینه‌های نقض حقوق مؤلف، حریم خصوصی، لینک‌های غیرمجاز، توزیع و انتشار ویروس‌های رایانه‌ای، نقض علائم تجاری مورد بررسی قرار داد. همچنین در عرصه ارتباطات الکترونیک همانند دنیای فیزیکی افرادی در روابط با یکدیگر ممکن است موجبات مسئولیت را فراهم آورده که با توجه به مجازی بودن این محیط شناسایی افراد در آن جهت اعمال مسئولیت بسیار حائز اهمیت است. افراد مسئول را می‌توان تحت نام‌های تولیدکنندگان محتوا، واسطه‌های الکترونیک و کاربران مورد بررسی قرار داد. لذا مقاله حاضر با بهره‌گیری از روش تحلیل و استنتاجی به بررسی مسئولیت مدنی در ارتباطات الکترونیکی، قواعد مختص آن و تطابق قواعد سنتی مسئولیت در آن عرصه می‌پردازد. یکی از عناصر مهم و به بیانی مهمترین آن در ارتباطات الکترونیک وجود واسطه ها و تأمین کننده خدمات ارتباطات الکترونیکی نظیر تأمین کنندگان خدمات اینترنتی (ISP)، تأمین کنندگان خدمات دسترسی و خدمات میزبانی می باشد که شناخت نقش و جایگاه آنها در تحلیل مسئولیت مدنی آنان بسیار حائز اهمیت است. همچنین با وجود مصادیق زیانبار ذکر شده و افراد دخیل در این زمینه خسارات وارده در این فضا را می توان به خسارت مادی و معنوی تقسیم نمود که با توجه به اصل جبران خسارات باید براساس طرق جبران خسارات موجود در حیطه مسئولیت مدنی و راهکارهای جدید بدلیل نوظهور بودن فضای موجود، اقدام به جبران خسارات وارده نمود.

واژگان کلیدی: مسئولیت مدنی، ارتباطات الکترونیکی، نفوذ غیرمجاز، حریم خصوصی، جبران خسارت

مقدمه

مسئولیت مدنی عبارت است از ملزم بودن شخص به جبران خسارتی که به دیگری وارد کرده است. مسئولیت مدنی زمانی به وجود می آید که کسی بدون مجوز قانونی به حق دیگری لطمه بزند و در اثر آن زیانی به او وارد آورد، فرق نمی‌کند عملی که موجب زیان شده است جرم باشد یا شبه جرم، در هر موردی که شخص موظف به جبران خسارت دیگری است گفته می شود که این فرد مسئولیت مدنی دارد و ضامن است و این می‌تواند در ارتباطات الکترونیک(فضای سایبر) و واقعی مصداق داشته باشد. مسئولیت مدنی به‌عنوان ضمانت اجرای حقوق مدنی نقش حساس و مهمی را در مطالبه و استیفای حقوق افراد ودر نتیجه تنظیم روابط اجتماعی وحقوقی باز می کند،بدون تصور وجود مسئولیت مدنی حق مفهوم واقعی و عینی خودرا از دست داده وجنبه فکری و ذهنی به خود میگیرد در ضمن چیزی که به واقع حق را از حالت بالقوه به صورت بالفعل در آورده وآنرا به طورملموس در اختیار صاحبان حق قرار میدهد قواعد و مقررات موجود در نظام حقوقی کشورها واز جمله کشور مامی باشد که در چهارچوب و قوانین مختلف گنجانده شده است. از سویی دیگر با ظهور فضای سایبر و ارتباطات الکترونیک مفاهیم حقوقی نیز با فضای نوینی روبرو گردیده‌اند که بحث مسئولیت مدنی نیز از این قضیه مستثنی نمی‌باشد.

در عرصه ارتباطات الکترونیکی همچون دنیای فیزیکی بسیاری از افعال کاربران و واسطه‌های الکترونیکی ممکن است از موجبات مسئولیت مدنی فاعل آن باشد. با توجه به ویژگی‌های خاص فضای ارتباطات الکترونیک شناسایی مسایل حقوقی مسئولیت در آن با دشواری‌هایی مواجه می شود، چراکه در نظام حقوقی ایران تاکنون دکترین حقوقی خاصی در خصوص موضوع مسئولیت مدنی در ارتباطات الکترونیکی ارائه نشده است و موضوع رویه قضایی نیز بسیار ضعیف و منفعل بوده است. با توجه به رویکرد جدید ارتباطات در جوامع امروزی مسایلی همچون شناسایی افراد مسئول در ارتباطات الکترونیک و مصادیق مسئولیت یا شناسایی افعال زیان‌بار در این فضا نیاز به بررسی‌های دقیق و فنی دارد. بر این اساس باید مشخص گردد که مسئولیت مدنی ناشی از ارتباطات الکترونیک شامل کدام قواعد حقوقی است و چگونه تعیین می شود؟ این موضوع کمتر مورد توجه محققان گرفته است و همانطور که اشاره شد، با توجه به فراگیر شدن فناوری ارتباطات پرداختن به این موضوعات از جنبه حقوقی ضرورت و اهمیت دارد.

مفهوم شناسی

در این مبحث دامنه مفهومی مسئولیت مدنی مشخص شده و سپس مفهوم ارتباطات الکترونیکی مورد بررسی قرار می گیرد.

۱. مفهوم مسئولیت مدنی

مسئولیت در لغت، به معنی پرسش، مورد سؤال واقع شدن و به مفهوم تفکیک وظیفه آمده است و در اصطلاح؛ عبارت است از تعهد قانونی شخص به دفع ضرر دیگری که وی به وجود آورده است خواه ناشی از تقصیر خود وی باشد یا از فعالیت او ایجاد شده باشد. مسئولیت در معنای لاتین مترادف عبارت responsibility قرار می گیرد که از معنای پاسخگو بودن (response) مشتق می شود. در معنای حقوقی و مدنی مسئولیت عبارتست از تکلیف قانونی شخص در عدم وارد نمودن ضرر به دیگری بصورت مستقیم یا غیر مستقیم. در واقع در حقوق مسئولیت به تعهد قانونی شخص بر رفع ضرری که به دیگری وارد کرده است گفته می‌شود (دهخدا، ۱۳۷۷)، خواه این ضرر ناشی از تقصیر ایجاد کننده ضرر باشد، یا اینکه ضرر در اثر فعالیت او حاصل شده باشد. اصطلاحاً ارکان مسئولیت به سه رکن اساسی گفته می‌شود که برای تحقق مسئولیت‌مدنی، ضروری است‌که در صورت فقدان یکی از این سه رکن، مسئولیت منتفی می‌شود. ارکان مسئولیت مدنی عبارتند از: ضرر، فعل زیانبار، رابطهٔ سببیت (بین عمل زیانبار و ضرر.) این سه‌شرط‌را می‌توان شروط ثابت مسئولیت‌نامید، زیرا وجود آنها در هر حال برای تحقق مسئولیت ضرورت دارد (باریکلو، ۱۳۸۵). مسئولیت رکن متغیری نیز دارد که تقصیر است. در بیشتر نظام های حقوقی مسئولیت اصولاً بر پایهٔ تقصیر استوار است. ولی هر گاه مصالح جامعه اقتضا کند، قانونگذار می‌تواند برای جبران ضرر نامشروع یا خطری که برای دیگران ایجاد شده است مسئولیت بدون‌تقصیر ایجاد کند؛ لیکن چون اصل با مسئولیت مبتنی بر تقصیر است هر جا که در نوع مسئولیت تردید شود می‌توان به مسئولیت مبتنی بر تقصیر استناد کرد و برای تحقق مسئولیت، وجود و اثبات تقصیر فاعل زیان را ضروری دانست.

بحث تقصیر، در بین اصول‌کلی مسئولیت‌مدنی اهمیت دو چندان دارد، زیرا هم مبنای مسئولیت است و هم در اثبات رابطهٔ سببیت نقش اساسی دارد (قاسم زاده، ۱۳۸۷).

۲. مفهوم ارتباطات الکترونیکی

واژه ارتباط از ریشه ی لاتین communis به‌معنای اشتراک گرفته شده است. این واژه در زبان فارسی به صورت مصدر عربی باب افتعال به کار می رود که در لغت به معنای پیوند دادن و ربط دادن و به صورت اسم مصدر به معنای بستگی، پیوند، پیوستگی و رابطه کاربرد دارد. فناوری اطلاعات و ارتباطات، به اختصار (ICT) عبارتی کلی در برگیرنده تمام فناوری‌های پیشرفته نحوه ارتباط و انتقال داده‌ها در سامانه های ارتباطی است. این سامانه می‌تواند یک شبکه مخابراتی، چندین کامپیوتر مرتبط با هم و متصل به شبکه مخابراتی، اینترنت و همچنین برنامه‌های استفاده شده در آنها باشد. حال با درنظر داشتن این مسئله پیدایش و استفاده از سیستمهای تلویزیونی دیجیتال یکی از فرایندهایی است که ارتباطات را در این عرصه مطرح نموده و از آن به ارتباطات الکترونیکی تعبیر می‌گردد. ارتباطات الکترونیکی زیرمجموعه ای از فناوری نوین اطعات و ارتباطات است. فناوری اطلاعات، همان طور که به‌وسیله انجمن فناوری اطلاعات آمریکا تعریف شده‌است، «به مطالعه، طراحی، توسعه، پیاده‌سازی، پشتیبانی یا مدیریت سیستم‌های اطلاعاتی مبتنی بر رایانه، خصوصا برنامه‌های نرم‌افزاری و سخت‌افزار رایانه می پردازد». به طور کوتاه، فناوری اطلاعات با مسائلی مانند استفاده از رایانه‌های الکترونیکی و نرم‌افزار سروکار دارد تا تبدیل، ذخیره، حفاظت، پردازش، انتقال و بازیابی اطلاعات به شکلی مطمئن و امن انجام پذیرد. اخیرا تغییر اندکی در این عبارت داده می‌شود تا این اصطلاح به طور روشن دایره ارتباطات مخابراتی را نیز شامل گردد.

نقض حقوق در ارتباطات الکترونیکی

نقض حقوق در ارتباطات الکترونیکی ممکن است در اثر دلایل مختلف و به اشکال متفاوت رخ دهد. در ادامه به طرق نقض حقوق در ارتباطات الکترونیکی اشاره می شود.

۱. نقض کپی رایت از طریق رساها

نقض کپی رایت در اینترنت زمانی رخ می‌دهد که یکی از حقوق انحصاری (مادی یا معنوی) پدیدآورنده در جریان ارتباطات اینترنتی مورد تجاوز قرار گیرد. از میان این حقوق می توان به حق ممانعت دیگران از تولید مجدد یا کپی کردن یک اثر، نمایش یک اثر به عموم یا توزیع و تکثیر آثار اشاره کرد. اکنون اضافه می‌کنیم که عمده ترین موارد نقض کپی رایت از سوی ارائه‌دهندگان خدمات اینترنتی یا رساها رخ می‌دهد.رساها خدمات دسترسی به اینترنت را در ازای دریافت وجه برای مشتریان انجام می‌دهند. آنها همچنین داده‌های مختلفی را برای استفاده مشتریان خود ذخیره می کنند که می‌توان به داده‌های ذخیره شده بر سرور گروه خبری یا سرور جهانی اشاره کرد (صادقی، ۱۳۸۸). مسئولیت رسانه‌ها در قبال فعالیت‌هایی که در برابر مشتریانشان انجام می‌دهند عموماً بر آگاهی آنها از فعالیت‌های مشتری مبتنی است. ارائه دهندگان خدمات برخط در صورتی مسئول نقض کپی‌رایت خواهند بود که به‌طور مستقیم در کپی کردن یک اثر حمایت شده دخالت داشته باشند. علاوه بر این ارائه‌دهندگان خدمات اینترنتی حتی به‌طور مستقیم در کپی کردن آثار مورد حمایت دخالت نداشته باشند ممکن است به خاطر نقض کپی رایت مسئول شناخته شوند.

۲. نقض کپی رایت از سوی سازندگان وبسایت‌ها

استفاده از گرافیک برای انتقال اطلاعات به کاربرها یکی از مصادیق نقض کپی رایت در ارتباطات اینترنتی است. گرافیک‌ها وتصاویری که در ارتباطات اینترنتی از آنها استفاده می‌شود؛ به طرق مختلف ایجاد می‌شوند.گاهی رساها یا سایر اشخاصی که می‌خواهند از گرافیک و تصاویر استفاده کنند؛ خود به طراحی و خلق آنها اقدام می‌کنند و گاهی از تصاویر متعلق به اشخاص ثالث استفاده می‌برند.در فرض نخست هرچند ممکن است تصویری که خلق می‌شود مشابه تصاویر اشخاص دیگر باشد؛ لیکن اگر پای تقلید و کپی کردن از آثار دیگران در میان نباشد و شباهت اتفاق وصرفاً از باب توارد باشد، مسئولیتی ایجاد نمی شود.اما اگر در مرحله خلق و ایجاد تصاویر یا گرافیک جدید، از آثار دیگران

استفاده شده باشد ممکن است اثری که خلق می شود یک اثر اشتقاقی باشد و نقض کپی رایت به شمار آید. منظور از اثر اشتقاقی،اثری است که یک شخص با تلفیق کل یا بخشی از آثار دیگران در طرح یا اثر خود ایجاد می‌کند. در فرضی که از تصاویر و گرافیک اشخاص ثالث استفاده می شود، قاعده حاکم در قلمرو ارتباطات اینترنتی آن است که «تصاویر متعلق به دیگران را ندزدید» (صادقی، ۱۳۸۸).

متن پردازی برای یک صفحه اینترنتی تابع همان اصول تصویر پردازی است. متنی که کاملاً ابتکاری بوده و پدیدآورنده و بسایت آن را پردازش کرده باشد بدون توجه به مسائل کپی همانند تصاویر، قابل استفاده است. تصاحب متن اشخاص ثالث بدون اجازه آنها غیرقانونی است، البته این امر دارای استثنائاتی از قبیل، استفاده منصفانه، استفاده آموزشی و علمی و استفاده شخصی و خصوصی می‌باشد که در ادامه مورد بررسی قرار می‌گیرد.

الف) استفاده منصفانه

در قوانین بسیاری از کشورها و اسناد بین‌المللی، یکی از موارد مهم استثنای بر حقوق انحصاری کپی رایت، استفاده منصفانه می‌باشد. استفاده منصفانه به استفاده از حق انحصاری دارنده اثر مشمول حمایت در جهت یک هدف متعارف بدون اجازه از دارنده اثر اطلاق می‌شود (صادقی، ۱۳۸۸). چهار معیار برای احراز استفاده منصفانه از آثار دیگران وجود دارد که درصورت وجود این چهار معیار مسئولیتی برای استفاده‌کننده وجود نخواهد داشت. وگرانه استفاده او، نقض کپی رایت تلقی خواهد شد:

۱- هدف و وصف استفاده، ازجمله این‌که آیا استفاده، ماهیت تجاری داشته یا برای مقاصد آموزش غیرانتفاعی صورت گرفته است؟

۲- ماهیت و طبیعت اثری که از آن کپی‌برداری شده است.

۳- میزان و اهمیت ماهوی بخشی که از کل اثر کپی‌برداری شده مورد استفاده قرار گرفته است.

۴- تأثیر استفاده بر بازار احتمالی یا ارزش اثری که از آن کپی‌برداری شده است.

با یک مثال استفاده منصفانه را توضیح می‌دهیم:

در نظر بگیرید، متن کوتاه از یک داستان دراز در یک بررسی روزنامه‌ای از ان داستان استفاده منصفانه تلقی می‌شود. اما اعمال چهار ضابطه و معیار فوق ممکن است نتایج متداخلی را ایجاد کند. با اعمال ضابطه اول که هدف و وصف استفاده را مورد توجه قرار می‌دهد، چون ذکر بخشی از یک داستان انتفاعی صورت گرفته است، ما را بدان رهنمون می‌کند که استفاده منصفانه در کار نبوده است. اما این حقیقت که هدف استفاده بررسی کردن و نقد آن اثر بوده است استفاده منصفانه را به اذهان تداعی می‌کند. و احتمالاً این معیار قوتر از معیار اول می‌باشد. با اعمال ضابطه دوم در این مثال، در نظر بگیرید که داستان مذکور منتشر نشده باشد که در آینده تحت حمایت قانون قرار خواهد گرفت، لذا باید نتیجه گرفت که استفاده منصفانه وجود ندارد. لذا به دشواری می‌توان استفاده از یک اثر منتشر نشده را استفاده منصفانه دانست. با اعمال ضابطه سوم، نیز چون تنها یک بخش کوتاه از داستان در بررسی انتقادی از آن مورد استفاده واقع شده باید قائل به استفاده منصفانه شد. اما باید کمیت و کیفیت بخش مورد استفاده را در نظر گرفت. چه‌بسا، ممکن است این بخش مهم‌ترین بخش داستان بوده باشد. نهایتاً آنکه دادگاه عامل و ضابطه چهارم را مهم‌ترین ضابطه می‌داند (انصاری، ۱۳۸۲).

ب) استفاده آموزشی و علمی

ضرورت توجه بیشتر به علم فن‌آوری و توسعه هرچه بیشتر آن ایجاب می‌نماید که محققین و مدرسین دامنه علم و تحقیق در دستیابی به منابع علمی آزاد باشند. هرچند حقوق مادی و معنوی منابع مزبور به‌عنوان آثار مشمول حقوق مؤلف متعلق به اشخاص دیگری است. بر این اساس در قوانین بسیاری در کشورها به مسأله استفاده‌های آموزشی و علمی از آثار مشمول حمایت توجه شده است. در مواد ۷، ۸، ۹، ۱۰ قانون حمایت مؤلفان و مصنفان و هنرمندان و ماده ۵ قانون ترجمه و تکثیر کتب و نشر آثار صوتی، استثنائاتی برحقوق مؤلف پیش‌بینی شده است که مبنای آنها جنبه‌ی آموزشی و علمی استفاده از آثار مورد حمایت است. در قانون حمایت از قانون پدیدآورندگان نرم‌افزارهای رایانه‌ای استثنایی مربوط به استفاده با اهداف آموزشی و علمی پیش‌بینی نشده است.

در زمینه آثار الکترونیکی با توجه به این‌که براساس ماده ۶۲ قانون تجارت الکترونیک، چنین آثاری مشمول احکام مقرر در قوانین صدرالذکر می‌شوند، لذا استثنائات مربوط به استفاده با هدف آموزشی و علمی درخصوص آثار ادبی و هنری قابل اعمال است. اما به‌جهت سکوت قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای اعمال این استثناء در مورد نرم‌افزارهای رایانه‌ای قابل اجرا در محیط‌های اینترنتی محل تردید است. چراکه در قانون تجارت الکترونیکی احکام جدید و مستقلی در مورد حقوق مالکیت فکری آثار در فضای مجازی و محیط الکترونیکی پیش‌بینی نشده و صرفاً احکام قوانین موجود به این‌گونه آثار تسری داده شده‌اند. لذا چون در قانون حمایت از حقوق پدیدآورندگان

نرم‌افزارهای رایانه‌ای، استثنایی مربوط به استفاده با اهداف آموزشی و علمی ذکر نشده است، اعمال این استثناء و معافیت در مورد استفاده‌های آموزشی و علمی از نرم‌افزارهای رایانه‌ای در فضای مجازی و اینترنت قابل تردید است (صادقی، ۱۳۸۸).

ج) استفاده شخصی و خصوصی

ماده ۱۱ قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان یک استثنای دیگر را در مورد تحقیق مؤلف پیش‌بینی نموده است و آن عبارت است از استفاده از اثری برای مصارف شخصی و غیرانتفاعی. لذا براساس ماده مذبور نسخه‌برداری از اثر برای استفاده شخصی و غیرانتفاعی مجاز می‌باشد. مع‌هذا این استثنا شامل کلیه آثار مشمول حمایت قانون یاد شده نبوده و صرفاً ناظر بر دو مورد ذیل می‌باشد.

کتاب، جزوه و نمایش‌نامه و هر نوشته‌ی دیگر علمی و فنی و ادبی و هنری (موضوع بند یک ماده ۲ قانون) ضبط برنامه‌های رادیویی و تلویزیونی در تبصره ذیل ماده ۵ قانون تکثیر کتب و نشریات و آثار صوتی نیز نسخه‌پردازی از کتب و نشریات و آثار صوتی موضوع مواد ۲ و ۳ قانون مزبور را درصورتی که برای استفاده شخصی و خصوصی باشد مجاز پیش‌بینی شده و استثنایی بر حقوق انحصاری دارنده حق پدیدآورنده اثر است.

ماده ۷ قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای نیز استثنای مربوط به استفاده شخصی را اینگونه پیش‌بینی نموده است: «تهیه نسخه‌های پشتیبان و هم‌چنین تکثیر نرم‌افزارهایی که به‌طریق مجاز برای استفاده شخصی تهیه شده است، چنانچه به‌طور همزمان مورد استفاده قرار نگیرد، بلامانع است» در خصوص آثار ادبی و هنری الکتریکی و نیز تکثیر، اجرا در توزیع آثار مشمول قوانین صدرالذکر در محیط‌های ازجمله اینترنت نیز با توجه به حکم ماده ۶۲ قانون تجارت الکترونیک حسب مورد استثنائات مصرحه در قوانین صدرالذکر حاکم خواهد بود. از این‌رو تکثیر یک نرم‌افزار رایانه‌ای در فضای مجازی درصورتی‌که در چارچوب ماده ۷ قانون حمایت از پدیدآورندگان نرم‌افزارها صورت می‌گیرد مجاز تلقی می‌شود و یا درخصوص آثار ادبی و هنری که در مبادلات اینترنتی ممکن است قابل استفاده قرار گیرد. چنانچه اثر مشمول بند یک ماده ۲ قانون حمایت از حقوق مؤلفان و مصنفان و هنرمندان بوده یا یک برنامه رادیو و تلویزیونی باشد مشمول استثنائی مقرر در ماده ۱۱ قانون اخیر، در مورد استفاده‌های شخصی و غیرانتفاعی خواهد شد. لذا چنانچه یک مقاله علمی متعلق به یک نویسنده ایرانی که مشمول حکایت قانون مزبور می‌باشد، به‌صورت فرمت Word و pdf یا هر فرمت الکترونیکی دیگری تبدیل شده و توسط یا با اجازه مؤلف یا دارنده حقوق مألف در یکی از سایت‌های اینترنتی قرار گیرد، استفاده کاربران اینترنتی از چنین مقاله‌ای حتی بدون اجازه نویسنده آن مقاله مجاز می‌باشد و کاربر می‌تواند جهت استفاده شخصی و به‌صورت غیرانتفاعی باشد، ثانیاً استفاده کاربر از اثر مستلزم غلبه غیرمجاز بر تدابیر فنی حمایتی و حفاظتی اثر باشد (صادقی، ۱۳۸۸).

مسئولیت مدنی در ارتباطات الکترونیکی بر اساس نظریه تقصیر

در این تئوری ارتکاب تقصیر شرط مسئولیت مدنی نیست بلکه هر کسی‌که بر اثر فعالیت خود خطرهائی ایجاد می‌کند و موجب زیان دیگری می‌شود مسئول و ملزم به جبران خسارت وارد شده است. بنابراین شخصی که اتومبیلی را به حرکت درمی‌آورد و یا کارخانه‌ای را به‌کار می اندازد ایجاد خطر می‌کند و چون از منافع این فعالیت بهره‌مند می‌شود ناچار باید ضرری را که از این راه متوجه دیگری می‌شود تقبل و جبران کند. علت پیدایش این نظریه جدید آن بود که حوادث وسایل نقلیه موتوری و رخدادهای زیانبار کارخانه‌ها روز به روز توسعه می‌یافت و خسارت‌های زیادی بر دوش زیاندیدگان می‌گذاشت و اغلب، حق آنها ضایع می‌شد. زیرا عامل زیان از شرایط و موقعیت اقتصادی بهتری برخوردار بود و با استفاده از قانون و امکان‌های خود از مسئولیت معاف می‌شد. به‌علاوه ضوابط تقصیر نیز اغلب غیرمشخص و در مورد هر حادثه‌ای علل مختلفی داشت. خلاصه آنکه وضع حقوقی و موقعیت زیاندیدگان بسیار بد و آسیب‌پذیر بود و یک سلسله مشکل‌ها و نابه‌سامانی های اجتماعی ایجاد می‌کرد. به همین جهت حقوقدانان به فکر بهبود و اصلاح وضع زیاندیدگان افتادند و به این نتیجه رسیدند که باید تسهیلاتی در امر اثبات قائل شد. در راه اجراء این نیت، قائل به فرض مسئولیت بدون تقصیر شدند و دارنده شیءِ خطرناک را مسئول جبران زیان وارد به دیگری دانستند. این نظریه موضوع رأی معروف دیوان‌عالی کشور فرانسه در سال ۱۹۳۰ و از ماده۱۳۸۴ قانون مدنی فرانسه استنباط شده است.

مطابق نظریه خطر، مسئولیت مدنی ما به‌ازاء نفع و فایده و لذتی است که شخص از شیءِ متعلق به خود یا از فعالیت خود می‌برد . در واقع حقوقدانان و دادرسان بدون آنکه مفهوم تقصیر را نادیده بگیرند به جست‌وجوی قاعده جدیدی پرداختند که مبنای جبران زیان قرار گیرد و

این قاعده را چنین بیان داشتند که خسارت باید به کسی نسبت داده شود که سبب وقوع آن شده است. بر پایه این نظریه چنانچه بر اثر عمل شخص یا اشخاص وابسته به او یا اشیاء تحت تصرف او خسارتی به دیگری وارد شود، عامل زیان مسئول به‌شمار می‌رود و باید از عهده جبران زیان وارد شده برآید مگر آنکه بتواند خلاف آن را ثابت کند. بنابراین، اصل بر مسئول بودن عامل زیان جاری است و اثبات خلاف آن بر عهده او است. در این‌صورت بار اثبات از دوش زیاندیده برداشته می‌شود و کافی است زیاندیده ثابت کند که خسارتی به او وارد شده و این خسارت ناشی از فعل عامل زیان است (اثبات رابطه علیت). این نظریه بعدها توسعه یافت و به‌دنبال آن نظریه مطلق خطر پیدا شد. مطابق نظریه اخیر هر کس موجب زیان دیگری شود مسئول جبران آن است و اثبات خلاف آن جز در مورد فورس ماژور جایز نیست. علت پیدایش نظریه اخیر توسعه ماشینیسم و پیچیدگی زندگی صنعتی کنونی و ضرورت حمایت کامل زیاندیدگان است. بنابراین مطابق نظریه خطر، دارندگان وسایل نقلیه موتوری و صاحبان کارخانه‌ها و کارگاه‌ها مسئول جبران زیان‌هائی هستند که بر اثر فعالیت آنها به اشخاص دیگری وارد می‌شود. ایرادی که به این نظریه گرفته‌اند آن است که قبول مطلق این نظریه ابتکار و آزادی عمل صاحبان فعالیت‌های اقتصادی را محدود می‌کند و هزینه‌های سنگینی برای جبران خسارت‌ها به‌عهده آنها می‌گذارد (کاتوزیان، ۱۳۸۶). در فضای ارتباطات و حوزه بحث ما نیز این تئوری در زمان به‌کارگیری داده‌ها بیشتر کاربرد دارد که اصول حاکم بر آن در ادامه خواهد آمد.

۱. اصل پردازش مرتبط

اولین اصل از اصول مربوط به کارگیری داده‌ها، اصل پردازش مرتبط می باشد. این اصل بیانگر این است که در مرحله پردازش اطلاعات، باید موسسه یا شخص تحصیل کننده اطلاعات آنها را به نوعی پردازش کند که مطلوب نظر سوژه باشد. در واقع باید از پردازش آنها برای اهداف غیرمرتبط و ثانوی خود داری کند لذا: اوّلاً چنین شخصی باید از پردازش داده ها در مواردی غیر از دو فرض فوق، خودداری نماید. ثانیاً در صورت تردید در روابودن یا نبودن پردازش اصل مجاز نبودن آن است، مگر اینکه صریحاً مجوزی برای آن وجود داشته باشد (اصلانی، ۱۳۸۴). عدم رعایت هریک از موارد فوق می‌تواند برای پردازش‌گر مسئولیت به‌بار آورد. با این‌همه در مواردی که هدف ثانونی از لوازم و فروع منطقی و غیرقابل اجتناب هدف اولیه باشد یا انکه سوژه منطقاً انتشار چنین پردازشی را داشته باشد، به‌جز درخصوص داده‌های شخص حساس، چنین پردازش مجاز است (انصاری، ۱۳۹۱).

۲. اصل ممنوعیّت افشاء

این اصل مربوط به این می‌شود که جمع آوری کننده‌ی اطلاعات، نمی‌تواند آن را از خارج از چهارچوب اذن شخصی که صاحب اطلاعات است (سوژه) افشا نماید. زیرا که افشا اطلاعات به شخص ثالث امری است که در محور اجازه‌ی اولیه از سوی شخص نمی‌گنجد، و به همین خاطر ممنوع است.

گردآوری پردازش محدود به هدفی است که تفسیر موسع آن در هرحال ممنوع بوده و تسری دادن آن به موارد مشابه تجاوز به حریم خصوصی اطلاعاتی محسوب می‌شود. خواه سوژه خود داده‌های شخص را در اختیار پردازش‌گر قرار داده باشد یا انکه پردازش‌گر از سایر طریق قانونی و به طریق۵ اولی غیرقانونی آنها را به‌دست آورده باشد.

برای مثال یک شرکت مخابراتی ممکن است داده‌های مشترکان خود را مستقیم یا غیرمستقیم در اختیار شرکت‌های تجاری قرار دهد تا برای اهداف تبلیغاتی از آنها استفاده کند. همین وضع در مورد ارائه‌دهندگان خدمات اینترنتی نیز وجود دارد (انصاری، ۱۳۹۱).

مسئولیت در ارتباطات الکترونیکی بر اساس فعل زیانبار

گاهی رویکرد حقوقدان یا پژوهشگر به احکام مسؤولیت مدنی بدان جهت است که می‌خواهد قواعد عمومی مسؤولیت مدنی را بر مصداق‌های خاصی از افعال یا فعالیت‌های زیانبار اعمال کند. برای مثال، درصدد آن است که بداند قواعد عمومی مسؤولیت مدنی در مورد خطاهای پزشکی، معماری، وکالت، قضاوت، روزنامه‌نگاری و سایر فعالیت‌های انسانی چه تغییر و تحولاتی پیدا می‌کند. اگر در قواعد عمومی مسؤولیت مدنی چند نظریه مهم درباره مبنای مسؤولیت مدنی وجود دارد، کدام مبنا با مقتضیات حرفه پزشکی یا معماری یا وکالت یا قضاوت و یا روزنامه‌نگاری سازگار است. در این رویکرد، به جای عنوان قواعد عمومی، عناوین «حقوق اعمال نامشروع زیان‌بار»، «مسؤولیت مدنی ناشی از خطای حرفه‌ای» یا «مسؤولیت‌های مدنی» استعمال می‌شود تا نشان دهد که منظور قواعد خاص حاکم بر هر یک از فعالیت‌های حرفه‌ای زیانبار است.

«مسؤولیت مدنی ناشی از ارتباطات اینترنتی» موضوعی است که با توجه به همین رویکرد در حقوق ما مورد بررسی قرار می‌گیرد. منظور از مسؤولیت مدنی ناشی از ارتباطات اینترنتی آن است که چنان‌چه در نتیجه فعل هر یک از اشخاص مختلفی که با مقاصد و عناوین متفاوتی با اینترنت سر و کار دارند به حقوق یا منافع اشخاص دیگری خسارت وارد آید، چه شخص یا اشخاصی، بر چه مبنایی و چگونه باید به جبران خسارت ملزم شوند. علاوه بر آن‌چه گفته شد، در تبیین احکام مسؤولیت مدنی ناشی از ارتباطات اینترنتی باید در نظر داشت که اینترنت جز در برخی عرصه‌های شخصی نظیر پست الکترونیک، یک عضو از خانواده رسانه‌های همگانی به شمار می‌رود. از همین رو، از حقوق، آزادی‌ها، امتیازات و مسؤولیت‌های این خانواده نیز متأثر است.اگر رسانه‌های همگانی حق «آزادی بیان» و «آزادی اطلاع‌رسانی» دارند یا اگر از«حق پاسخگویی» و «تفسیر منصفانه» برخوردارند یا از «امیتازهای مطلق و محدود» استفاده می‌کنند، در حل مسایل مربوط به مسؤولیت مدنی ناشی از ارتباطات اینترنتی نیز باید آن‌ها را لحاظ کرد (حسین پور و صابر نژاد، ۱۳۹۴).

بدین ترتیب، تبیین مسؤولیت مدنی ناشی از ارتباطات اینترنتی نه تنها مستلزم توجه به قواعد عمومی مسؤولیت مدنی و استخراج قواعد خاص حاکم بر جبران خسارت‌های ناشی از ارتباطات اینترنتی است، بلکه معطوف به قواعد عمومی حاکم بر فعالیت رسانه‌های همگانی و ارتباطات جمعی و استنباط قواعد خاص حاکم بر ارتباطات از طریق اینترنت نیز می‌باشد. زیرا، ارتباطات اینترنتی ویژگی‌هایی دارد که آن را از سایر رسانه‌های همگانی متمایز می‌کند و به همین دلیل، باید متناسب با ویژگی‌ها و مقتضیات آن، احکام خاصی را برای تنظیم ارتباطات از طریق این رسانه در نظر گرفت. در این راستا مسئله که بیشتر مورد توجه است و مورد بررسی قرار می‌گیرد مسئولیت ناشی از نگهداری و بخش ویروس است که با توجه به ذات خطر آفرین آن امکان استفاده از نظریه های سختگیرانه مسئولیت مدنی از جمله نظریه مطلق و محض را امکان پذیر می سازد در بحث ویروس هر شخص ممکن است به طور ناخواسته عاملی برای بخش ویروس در اینترنت باشد به نحوی که صدها نفر را در سراسر جهان قربانی ندانم کاری خود کند. از آنجا که ویروس می‌تواند باعث خسارت‌های مالی شود مسئولیت مدنی پدید آورنده و یا عامل انتشار ویروس نیاز به بررسی دارد. صرف‌نظر از مجرمانه بودن فعل شخص پدیدآورنده یا پخش کننده ویروس که نیاز به علم و عمد دارد برای صدق عنوان مسئولیت مدنی درباره چنین اشخاصی نمی‌توان دقیقاً همان ارکانی را لازم دانست که برای مسئولیت کیفری ضرورت دارد درواقع هر نوع بی‌احتیاطاتی و بی‌مبالاتی در تولید، عرضه، ارسال یا پردازش برنامه‌های مخرب یا مشکوک که موجب زیان به سامانه‌های یارانه‌ای یا هر سامانه‌ای ارتباطی دیگری شود می‌تواند ارکان و لوازم مسئولیت مدنی عامل یا عاملان را فراهم کند (السان، ۱۳۹۱).

یکی از موارد مسئولیت ناشی از ویروس حالتی است که شخص مبادرت به نگهداری ویروس در محل خاصی می‌نماید به عنوان مثال یک سازنده نرم‌افزارهای ضدویروس یا یک موسسه آموزشی و پژوهشی در زمینه یارانه از قبیل دانشکده کامپیوتر ممکن است برای انجام آزمایشات خود ویروس‌هایی از انواع مختلف نگهداری نماید. قطعاً از آنجا که ویروس یک شی ذاتاً خطرناک است بایستی در مراقبت از آنها اهتمام کامل صورت پذیرفته تا به جاهای دیگر نفوذ ننموده و موجب بروز خسارت به دیگران نشود. در نظام حقوقی ایران نیز باتوجه به احکام مصرح در ماده ۱ ق مسئولیت مدنی و وحدت ملاک حکم مواد و ماده قانون مجازات اسلامی مصوب ۱۳۹۲ و ماده ۳۳۴ قانون مدنی مسئولیت نگهدارنده ویروس قابل احراز است (صادقی، ۱۳۸۸). فعل زیانبار در فضای سایبر را می‌توان به گونه‌های مختلف تقسیم‌بندی نمود که در ادامه تحلیل آن خواهد آمد.

۱. نفوذ به داده ها

این واژه که در ترجمه‌ی انگلیسی آن واژه‌ی هک آورده شده است، رایج‌ترین نوع فعل زیانبار در فضای سایبر است و می‌توان گفت که در اندیشه‌ی مردم ما بیشتر مورد توجه قرار گرفته است. این واژه نزد اهل فن کامپیوتری و سایبر در یک مفهوم عام شامل هرگونه ورود غیر مجاز، از کار انداختن سیستم و همچنین تخریب و تغییر داده‌ها می‌شود. ولی آنچه که در اینجا از واژه فوق مدنظر است، صرف نفوذ به یک سیستم اطلاعاتی می‌باشد هرچند منجر به پردازش، اصلاح، انتقال و یا تخریب داده‌ها نشود. مراد از واژه‌ی نفوذگر نیز شخصی است که سعی در ورود غیرمجاز به یک سیستم کامپیوتری را دارد (اصلانی، ۱۳۸۴).

البته باید ذکر گردد که، این مسئله مطابق با اصل امنیت یک عمل تخلف آمیز به شمار خواهد آمد چرا که مطابق اصل امنیت باید کسی که داده‌ها را به دست آورده و یا دارنده داده باید تدابیر ضروری برای جلوگیری از نفوذ به این داده‌ها را به کار برد. البته دارند داده‌ها (سوژه) در صورتی که بتواند ثابت کند که نقض امنیت سیستم به لحاظ ضعف تدابیر امنیتی ناشی از ضعف سطح دانش موجود بوده و قابل انتساب به او نمی‌باشد؛ می‌تواند از مسئولیت ناشی از عدم رعایت تدابیر مناسب امنیتی رهایی یابد. البته باید بیفزاییم که عمل تخلف آمیز نفوذ خود منشأ سایر جرایم و اعمال تخلف آمیز دیگری نیز خواهد بود و یکی از این اعمال تخلف آمیز که البته یکی از اموری است که همزمان با نفوذ انجام می‌گیرد، مسئله‌ی زیر نظر گرفتن می‌باشد. مبرهن است، اطلاعات زیادی در محیط سایبری وجود دارد که انگیزه‌ی کافی را برای زیر

نظر گرفتن دیگری به وجود می‌آورد. وسیله‌ای که زیر نظر گرفتن فعالیت‌ها را ممکن می‌سازد، کوکی نام دارد. خدمات دهندگان اینترنتی، بازاریاب‌ها و دیگر شرکت‌ها، با قرار دادن فایل کوچکی به نام کوکی در حافظه رایانه‌ی شما، یک فناوری برای زیر نظر گرفتن فعالیت‌هایتان در اختیار دارند. کوکی‌ها ماهیتاً بد یا متجاوز به حریم خصوصی افراد نیستند ولی مسیر سوءاستفاده گسترده را باز می‌کنند. در افراطی‌ترین و جامع‌ترین موارد یک شرکت اینترنتی می‌تواند پرونده‌ای شامل اطلاعات خرید، سلیقه موسیقیایی، اطلاعات سرمایه‌گذاری مورد علاقه، مهمترین موضوع‌های بهداشتی و سلامتی برای کاربرد و مخاطب خبری مورد علاقه‌ی وی شکل دهد (پاتر، ۱۳۹۱). که صد البته چنین امری نیز مصداق بارزی از نقض حریم خصوصی به عنوان یکی از افعال زیانبار و مقدمه ضرر سایبری می‌باشد.

الف) جمع آوری غیرمجاز

به دست آوردن و تحصیل داده‌ها باید با روش قانونی و مشروع صورت گیرد. البته باید بیان گردد که همانگونه که ذکر رفت علاوه بر اصل مذکور اصول تحصیل مضیق و مرتبط و اصل انتخاب و اطلاع نیز مبین تخلف بودن چنین فعلی می‌باشند، و عطف توجه به تخلف آمیز بودن جمع آوری غیر مجاز داده‌های شخصی با تأسی از بیانات نویسنده‌ی ایرانی هم عصرمان می‌توان افعال زیر را مصداق بارز عمل تخلف آمیز در این ورطه به شمار آورد:

۱- جمع آوری داده‌های شخصی از طریق روش‌های غیر قانونی یا به‌صورت سری (نصب دوربین یا میکروفن‌های مخفی).

۲- جمع آوری داده‌ها بدون جلب رضایت سوژه یا اجازه صریح قانونگذار، ولو آنکه ابزار یا روش جمع آوری غیر قانونی نباشد.

۳- جمع آوری داده‌های اضافی و غیر مرتبط با هدفی که برای آن شخص سوژه موافقت خود را اعلام نموده یا قانونگذار اجازه داده است.

۴- جمع آوری داده‌ها برای هدف غیر قانونی یا نامشروع ولو آنکه روش گردآوری داده‌ها قانونی باشد.

۵- خودداری از مهیا نمودن امکان انتخاب برای سوژه دایر بر اعلام موافقت یا مخالفت با جمع آوری داده‌ها آن هم به نحو مطلوب و مفید.

۶- خودداری از اعلام عواقب اعلام موافقت یا مخالفت سوژه به وی.

۷- مقصود در اعلام اطلاعات کافی در باب گردآوری داده‌های شخصی، هدف چنین کاری و همچنین رویه مورد عمل در صیانت از داده‌ها.

۸- اعلام حقوق سوژه در بهره‌مندی از روش‌های تعقیب و جبران به او (اصلانی، ۱۳۸۴).

درباره‌ی حمایت‌های به وجود آمده در زمینه‌ی این نوع نقض حریم خصوصی می‌توان از دستورالعمل 95/46/EC اتحادیه‌ی اروپا نام برد، که از منظر این دستورالعمل گردآوری داده‌ها به جز در موارد مصرح مجاز در سایر موارد آن تخلف محسوب می‌گردد و ضمانت اجراهای قانونی نیز بر آن مترتب است.

ب) تغییر غیرمجاز

زمانی که نفوذگر غیر مجاز وارد حریم خصوصی شخصی دیگر در سیستم‌های کامپیوتری و محیط دیتا می‌شود؛ بسته به هدف او می‌توان آثاری را مشاهده کرد، که یک نمونه از آن تغییر غیر مجاز داده‌ها می‌باشد. البته به جاست که در همین جای بحث بیفزاییم، چنین اقدامی ممکن است به صورت‌های مختلف رخ دهد. یکی از روش‌ها وقتی است که فردی رایانه‌ی شخصی را به کنترل خود درآورد و در فعالیتی شبکه‌ای با دیگران مرتبط سازد. از این رو، بازاریاب‌ها از این شبکه به عنوان منبعی برای ارسال میلیون‌ها پیام به نام نشانی آی. پی شما استفاده می‌کنند. در بیشتر اوقات، صاحبان رایانه‌های شخصی که به کنترل دیگران در آمده‌اند، از این اتفاق آگاه نیستند. یکی دیگر از روش‌ها را آگهی دهندگان اعمال می‌کنند. آگهی دهندگان با استفاده از یک مرورگر کنترل صفحه‌ی شخصی شما را در اختیار می‌گیرند، یا موتور جستجوگری را در رایانه‌ی شخصی شما جای دهند. ممکن است چنین کاری بی ضرر به نظر برسد ولی این مرورگر یا موتور جستجوگر به گونه‌ای طراحی شده است که شما را فقط به سایت‌های خاصی رهنمون می‌سازد (پاتر، ۱۳۹۱).

به هر حال می‌توان تغییر داده‌ها را در ۴ فاز مجاز (با توجه به نیت نفوذگر) مورد بررسی قرار داد.

۱. شخصی قصد خاصی ندارد.

۲. شخصی قصد تخریب رایانه‌ای دارد.

۳. شخصی قصد جعل سایبری دارد.

۴. شخص قصد نشان دادن اطلاعات کذبی را دارد (اصلانی، ۱۳۸۴).

که اگر بتوانیم به موضوع کمی جزایی‌تر نگاه کنیم مورد اول و دوم را می‌توان تخریب رایانه‌ای نامید؛ و مورد سوم نیز همان جعل خواهد بود منتهی در فضای سایبری، و مورد آخر نیز افترای عملی می‌باشد.

در حقوق بین‌الملل در کنوانسیون بوداپست سال ۲۰۰۱ میلادی مصوبات کنوانسیون توصیه‌هایی به اعضا می‌کند که نشانگر توجه خاص به تخلف‌آمیز بودن این افعال می‌باشد. در بند ۱ ماده ۴ در باب ایجاد اختلال در داده‌ها مقرر می‌دارد که: «بند۱: هر یک از اعضا باید به گونه‌ای اقدام به وضع قوانین و مقررات نماید که در صورت لزوم بر اساس حقوق داخلی خود، هر نوع صدمه زدن، پاک کردن، خراب کردن، دستکاری یا قطع داده‌های رایانه‌ای را که به طور عمدی و غیر قانونی صورت گیرد جرم انگاری نماید».

و همچنین در مورد جعل نیز مقرر می‌دارد: «ماده ۷- جعل مرتبط با رایانه: هر یک از اعضا باید به گونه‌ای اقدام به وضع قانون و مقررات نماید که در صورت لزوم بر اساس حقوق داخلی خود، هر نوع وارد کردن، تغییر، حذف یا قطع عمدی و غیر قانونی داده‌های رایانه‌ای را که منجر به ایجاد داده‌های غیر معتبر می‌شود؛ با همان قصدی که از آن انتظار می‌رفت یا در راستای اهداف غیرقانونی به عنوان داده‌هایی که از اعتبار کافی برخوردارند، به کار گرفته می‌شوند، چه این داده‌ها به طور مستقیم قابل خواندن باشد چه نباشد جرم انگاری نماید. عضو مورد نظر مقرر می‌دارد که وجود قصد فریب یا دیگر مقاصد ناروا، پیش از اتصاف مسئولیت کیفری لازم و ضروری است». البته باید بیان داشت که قانونگذار کشورها نیز چنین اعمالی را تخلف می‌دانند.

علی رغم تفاوت‌های زیادی که این اقدامات با همدیگر دارند ولی در همه‌ی آنها فصل مشترکی وجود داد که آنها را زیرمجموعه‌ی عنوانی به نام تغییر غیر مجاز داده‌ها قرار می‌دهد؛ و آن عبارتست از اینکه همه‌ی این تخلفات در یک نکته خلاصه می‌شود که شخص نفوذگر، اقدام به تغییر دادن و دستکاری داده‌ها نموده و از این طریق به هدف خود نایل می‌شود. یکی دیگر از راه‌های تغییر غیرمجاز داده‌ها نیز حملات ویروسی می‌باشد. وقتی داده‌ای مورد حمله ویروسی قرار بگیرد رایج‌ترین ضرباتی که به رایانه وارد می‌شود این است که فایل‌های اطلاعاتی خراب شده یا از بین بروند (اصلانی، ۱۳۸۴).

۲. سرقت هویت

با ظهور اینترنت خطر سرقت هویت نیز دو چندان شد. این جرم از ناتوانی مصرف کنندگان (و کاربران) در نظارت بر گستره‌ی دسترسی به اطلاعات حساس (چه کسانی می‌توانند به این اطلاعات دسترسی داشته باشند) و شیوه‌ی حفاظت از آنها ناشی می‌شود.

در فضای مجازی به‌عنوان قلمرویی که در آن ارتباطات و تعامل بین دو فرد رایانه از طریق تبادل اطلاعات دیجیتال برقرار می‌شود. عنصر هویتی که در گونه ارتباط و تعامل ضروری است اهمیت بسیار زیادی دارد. هویت دیجیتال در اصل تلاش برای ایجاد سازماندهی خودکار و یکپارچه ساختن همه‌ی جوانب جهان واقعی در جهان الکترونیکی آنلاین و ارتباط آنها با هویت‌های آفلاین است (شکرخواه، ۱۳۹۰).

باید بیان کرد که دستیابی به این اطلاعات به شیوه‌های متعددی امکان پذیر است، مانند سرقت کد کاربرها و شماره دسترسی، استراق سمع الکترونیکی، شانه سواری (دید زدن از روی شانه‌ی کاربر) و اتفاقی. امروزه نوعی نحوه‌ی به دست آوردن اطلاعات شخصی پدید آمده که اصطلاحاً به آن فیشینگ می‌گویند؛ که به معنای کپی همانند سازی شده از یک صفحه‌ی اینترنتی آشناست که کاربر را گمراه کرده و در واقع وسیله‌ای برای به دست آوردن اطلاعات شخصی وی به شمار می‌آید. این حملات شکل‌هایی نظیر درخواست اطلاعات از سوی بانک قلابی، اعلام برنده شدن شما در قرعه‌کشی و یا پیغامی از طرف شبکه‌های اجتماعی به خود بگیرد (پورقهرمانی، ۱۳۹۰).

در حقوق بین‌الملل در کنوانسیون جرایم سایبری به اعمال موخر سرقت هویت در ماده ۶ اشاره گردیده است، ولی نه در این کنوانسیون و نه در اسناد شورا و اتحادیه اروپا هیچ اشاره‌ی صریحی به سرقت هویت نشده است. ولی در این میان، انجمن بین‌المللی حقوق جزا با پذیرش خطوط راهنمایی پیشنهادی به قانونگذاران ملی در توصیه نامه شورای اروپا علاوه بر فهرست جرایم شورای اروپا، قاچاق کلمات رمز را بدون اینکه تعریف کرده باشد، در لیست جرایم آتی و به عنوان جرم مستقل به رسمیت شناخته است؛ و به نظر می‌رسد منظور انجمن بین‌المللی حقوق جزا همان سرقت هویت بوده است (پورقهرمانی، ۱۳۹۰).

۳. انتقال غیر مجاز

عطف توجه به اصل عدم انتقال بعدی داده‌ها، انتقال غیرمجاز داده‌ها به وجود آورنده‌ی ضرر در محیط سایبری است. زیرا این اصل از این جهت قابل توجیه می‌باشد که آنچه دارنده یا پردازش‌گر داده را مجاز به در اختیار داشتن داده‌ها می‌کند (حکم قانون یا رضایت شخص سوژه)، لزوماً نسبت به شخص ثالث قابل تسری نمی‌باشد (اصلانی، ۱۳۸۴).

از طرفی برخی از شرکت‌ها با استفاده از کوکی‌ها جای داده شده در رایانه‌های مشتریان خود، اطلاعات را جمع‌آوری می‌کنند و با تشکیل داده بنیادها آنها را به یکدیگر می‌فروشند. که صد البته در این مورد خاص حتی تحصیل اطلاعات هم غیرمجاز می‌باشد، ولی این موضوع حتی در جایی که تحصیل اطلاعات مجاز نیز بوده باشد به چشم می‌خورد زیرا برخی از شرکت‌هایی که اطلاعات مشتریان خود را جمع‌آوری می‌کنند؛ متعهد شده‌اند تا این اطلاعات را به فروش نرسانند. ولی سرانجام مجبور به چنین کاری می‌شوند (پاتر، ۱۳۹۱).

در حقوق بین‌المللی درباره‌ی حمایت از اینکه انتقال غیرمجاز داده‌ها ممنوع بوده باشد، می‌توان به مواد ۲۵ و ۲۶ دستورالعمل شماره 95/46/EC اتحادیه اروپا اشاره کرد که علاوه بر بیان ممنوعیت استثناهای آن را نیز بر می‌شمارد که بر پایه‌ی چهار محور رضایت شخص و تأمین منافع حیاتی او، منافع ملی و امنیت عمومی، انتقال قراردادی و امر آمر قانونی می‌باشد.

۴. افشای غیرمجاز

اصل ممنوع بودن افشای داده‌ها که خود یکی از زیرمجموعه‌های اصل پردازش مرتبط است. بالمال مقتضای آن را دارد که افشای داده‌ها به اشخاص ثالث تخلف محسوب می‌شود. در واقع در مرحله‌ی به دست آوردن اطلاعات زمانی که اطلاعات یک شخص در اختیار دیگری قرار می‌گیرد، فقط آن شخص مجاز به استفاده بوده و در انتقال و افشای آن داده‌ها مجوزی ندارد. مگر آنچه که خلاف آن ثابت گردد و همانطور که در بند ب ماده ۲ دستورالعمل شماره 95/46/EC اتحادیه اروپا که افشای داده‌ها از مصادیق پردازش می‌باشد و به موجب ماده ۷ همان سند نیز پردازش به جز موارد مصرحه در قانون غیر مجاز می‌باشد یعنی اصل بر عدم پردازش است.

اشخاص مسئول و چگونگی تعیین مسئولیت با دخالت عوامل متعدد در ارتباطات الکترونیک

در دنیای مجازی و ارتباطات الکترونیک تعامل بین اشخاص حقیقی و حقوقی به صورت غیرحضوری و غیرفیزیکی است. لذا سیستم ارتباطات از راه دور اصلی‌ترین و مهمترین مبنای روابط اشخاص در این‌گونه محیط است. بدون وجود فناوری اطلاعات و ارتباطات ایجاد و تداوم چنین دنیایی امکان‌پذیر نمی‌باشد. چنانچه داده‌ها به صورت الکترونیکی جهت انتقال و ارسال برای گیرنده پیام پردازش نشوند و چنانچه سیم انتقال داده عملیات جابجایی و حمل این‌گونه داده‌ها را به نحو صحیح و موثر انجام ندهند قطعاً مفهوم دنیای مجازی فاقد مصداق عینی بوده و ارتباطات الکترونیکی اشخاص میسر نمی‌گردد. لذا عواملی که در این حوزه دخیل هستند باید مورد بررسی قرار گیرد، که این عوامل عبارتند از تامین کنندگان محتوا، واسطه‌های الکترونیک و کاربران. که در ادامه به صورت مبسوط توضیح داده خواهد شد.

۱. تأمین کنندگان محتوا

تامین کننده محتوا درواقع شخصی است که مبادرت به ایجاد یا قرار دادن اطلاعاتی خواه به صورت متن، تصویری یا صوتی یا مانند آن در فضای شبکه اینترنت می‌نماید لذا طیف گسترده مفهوم تامین کننده محتوا شامل کلیه اشخاصی است که به نوعی با اینترنت سروکار دارند که از جمله این اشخاص شامل کاربران و مدیر شبکه می‌شود.

محتوا ممکن است به صور مختلفی ارائه شود، گاهی به صورت قابل تخلیه، گاهی به صورت فایل جاری قابل رویت می‌باشد (صادقی، ۱۳۸۸).

قانونگذار ما نیز در ماده ۲ قانون تجارت الکترونیک مصوب ۱۳۸۲، اصل ساز را که مترادف تولیدکننده محتواست بدین گونه تعریف نموده است «منشا اصلی داده پیام است که داده پیام به وسیله او یا از طرف او تولید یا ارسال می‌شود اما شامل شخصی که درخصوص داده پیام به عنوان واسطه عمل می‌کند نخواهد شد».

همچنین کمیسیون تنظیم مقررات ارتباطات جلسه شماره ۹۶ مورخ ۱۳۸۹/۷/۱۸ در ماده ۵ وظایف و مسئولیت‌های فراهم کننده محتوا را به شرح زیر توضیح داده است:

فراهم کننده محتوا موظف است در ارتباط با مسئولیت‌های مشترک مقررات مربوط و تخلفات و عواقب قانونی آن اطلاع‌رسانی کافی به عمل آورد. فراهم کننده محتوا موظف است قبل از ارائه خدمات درباره مفاد و نحوه اطلاع‌رسانی با سازمان هماهنگی لازم را به عمل آورده و از سازمان تادیه دریافت کند.

۲. واسطه های الکترونیک

در بیان اهمیت جایگاه واسطه‌های ارتباطات الکترونیکی همین بس که بدون وجود چنین واسطه‌های برقراری هرگونه ارتباط از راه دور خبر از طریق شیوه سنتی پست یا حمل ونقل فیزیکی امکان‌پذیر نخواهد بود.

بر این اساس شناخت انواع واسطه‌های الکترونیکی و آگاهی از نوع و نحوه فعالیت آنها و نقش و جایگاه آنها در برقراری صحیح ارتباطات الکترونیک حائز اهمیت می‌باشد. واسطه‌های الکترونیک تحت دو عنوان تامین کنندگان خدمات دسترسی یا ارائه دهندگان خدمات اینترنتی و ارائه دهندگان خدمات میزبانی قابل تقسیم و تبیین است که در ادامه مورد بررسی قرار می‌گیرد.

الف) ایجادکنندگان نقطه تماس بین‌المللی (تامین کنندگان خدمات دسترسی) و ارائه دهندگان خدمات اینترنتی)

این دسته اصلی واسطه‌ها در ارتباطات اینترنتی هستند چرا که هرگونه ارتباط بین سیستم‌های شخصی اشخاص حقیقی و حقوقی با شبکه جهان گستر اینترنت صرفاً از طریق این واسطه‌ها برقرار می‌شود. این دسته از ارائه دهندگان خدمات دسترسی به صورت تجاری فعالیت می‌نمایند تحت عنوان ارائه دهندگان خدمات اینترنتی (رساها) مشغول هستند. در کشور ما براساس بند ۱ آئین‌نامه نحوه اخذ و ضوابط فنی نقطه تماس بین‌المللی (موضوع قسمت الف از مقررات و ضوابط شبکه‌های اطلاع‌رسانی مصوب شورای عالی انقلاب فرهنگی در سال ۱۳۸۰): «ایجاد نقطه تماس بین‌المللی در انحصار دولت می‌باشد و ارائه مجوز به دستگاه‌های ذیربط توسط شورای عالی اطلاع‌رسانی صورت می‌گیرد» (صادقی، ۱۳۸۸).

بنابراین در حال حاضر برقراری ارتباط بین‌المللی از طریق اینترنت در انحصار دولت معهذا به موجب قسمت ب مقررات و ضوابط مزبور که تحت عنوان (آئین‌نامه واحدهای ارائه کننده خدمات اطلاع‌رسانی و اینترنت isp) می‌باشد.

موسساتی تحت عنوان رساها می‌توانند فعالیت‌هایی را در زمینه اطلاع‌رسانی و اینترنت از جمله فراهم آورن امکان دسترسی کاربران به اینترنت با رعایت آئین‌نامه یاد شد انجام دهند. پس در کشور ما با توجه به مصوبه شورای عالی انقلاب فرهنگی رساها به کلیه خدمات اینترنتی، بر خطوط برون خط می‌پردازد. بر این اساس خدمات دسترسی به اینترنت، میزبانی، سرور پراکسی، ارائه محتوا و پردازش داده‌ها و خدمات بر خط را انجام می‌دهند. و عنوان رسا به کلیه واحدهایی اطلاق می‌شود که به ارائه کل یا بخشی از این خدمات می‌پردازند (صادقی، ۱۳۸۸).

باتوجه به آنچه گفته شد می‌توان گفت که مسئولیت مدنی رساها منوط به شرایط خاصی است: اول اینکه اگر رسا در فرایند ذخیره محتوا مباشرت داشته باشد یا به حکم قانون یا قرارداد ملزم به بررسی محتوایی باشد در قبال نقض کلیه اقسام معوق مالکیت فکری مسئولیت مدنی خواهد داشت حتی اگر این نقض از طریق کاربران (مشتریان) آن انجام گرفته باشد. دوم اینکه هرگاه رسا تنها واسطه ارتباطی باشد و به حکم قانون یا قرارداد وظیفه‌ای در بررسی محتوی نداشته و از نظر عرف هم اطلاعی از محتوی که از طریق سامانه آن مبادله می‌شود نداشته باشد در قبال آن مسئولیتی نخواهد داشت (السان، ۱۳۹۱).

ب) ارائه دهندگان خدمات میزبانی

هر اتفاقی در مکان حادث می‌گردد و این یک اصل عقلی و منطقی است. در فضای سایبر هر چند که در تعریف آن به مجازی بودن این فضا اشاره کردیم، ولی این نکته را نباید از خاطر برد که فعالیت‌هایی که در این فضا اتفاق می‌افتد در یک محیط رویایی و خیالی نیست بلکه میحطی است که به این فصل اختصاص یافته است. هر چند که این محیط یک فضای مجازی باشد و با پذیرش چنین سخنی باید این حرف را نیز حصه گذاریم که موسساتی نیز این فضا را در اختیار می‌گذارند که از آنها به نام ارائه دهندگان خدمات میزبانی نام برده می‌شود.

سیستم میزبان یک محل ذخیره دیجیتال است که از طریق اینترنت قابل دستیابی می‌باشد. نوع داده‌هایی که در سیستم میزان ذخیره می‌شود متنوع بوده و شامل نرم‌افزارهای رایانه و آثار متنی و گرافیکی و هر نوع داده دیگری می‌شود. دارنده سیستم میزبان دارای یک طیف گسترده‌ای از روابط احتمالی با داده ذخیره شده در سیستم میزبان است. لذا می‌تواند مالک همه داده‌ها باشد یا به نحو فعالی بر همه آنها کنترل داشته باشد. تحلیل مسئولیت مدنی تامین کننده خدمات میزبانی منوط به شناخت نقش و ماهیت دقیق فعالیت میزبانی است و بایستی نقشی که دارنده سیستم میزبان در ورود ضرر داشته است تحلیل شود. لذا مسئولیت ناشی از هتک حرمت و مسئولیت ناشی از نقض حقوق مالکیت فکری و علائم تجاری در مورد این دسته از اشخاص هر یک قواعد خاصی را اقتضا می‌کند. یکی از مصادیق سرورهای میزبان سرور میزبان «یوزنت» است. یوزنت یک سیستم متشکل از هزاران گروه‌های خبری و بحث و گفتگو است که در خصوص حجم زیادی از موضوعات متنوع بحث می‌کند. به طور کلی هر شخص می‌تواند پیام را برای آن ارسال نماید سرور میزبان یوزنت به نحو خودکار مطالب را از سایر سرورهای میزبان یوزنت به صورت بروز دریافت می‌کند. داده‌های ارسالی را مستقیماً از مشتریان خود دریافت و به صورت بروز شده برای سایر سرورهای میزبان یوزنت ارسال می‌کند. لذا یک سرور میزبان سیستم‌های فنی و اطلاعاتی ویژه صفحه خود را اداره نموده و به طور کلی مدیریت سایت‌ها را به عهده دارد. بنابراین سرور میزبان یک رئیس شبکه نیز محسوب می‌شود (صادقی، ۱۳۸۸).

۳. کاربران

در قانون تجارت الکترونیک تعریفی از کاربر ارائه نشده اما واژه‌هایی مثل مخاطب، شخص و مصرف کننده در ماده این قانون تعریف شده است. براساس تعریف جدید اتحادیه جهانی ارتباطات کاربر اینترنت کسی است که در طول سه ماه گذشته با هر فناوری ارتباطی به شبکه اینترنت متصل بوده است. در تعاریف قبلی کاربر اینترنت کسی بود که در طول دوازده ماه گذشته با هر فناوری ارتباطی به شبکه اینترنت متصل شده بود.

به نظر می‌رسد باید بپذیریم مادامی که یک بدنه حرفه‌ای مسئول وجود دارد و نتوان برای استفاده سیستم اطلاعاتی بدان متوسل شد یک حرفه‌ای دیگر برای عدم موفقیت به انجام آن مسئول نخواهد بود. شرط این مساله آن است که سرعت توسعه به قدری باشد و تفوق فن جدید آنقدر مضمحل کننده باشد که بگوییم هیچ حرفه‌ای مسئولی از بابت آن مقصر نیست. این دیدگاه در ارتباط با استفاده از سیستم‌های خودکار بازاریابی، اطلاعات به وسیله حقوقدانان مادامی که استفاده از سیستم‌ها به عنوان ابزار حیاتی یک دفتر حقوقی مدرن و کارآمد محسوب می‌شود نیز مراعات است. به ندرت اتفاق می‌افتد که کاربری به خاطر نقایص موجود در سیستم اطلاعاتی که وی بدان اعتماد کرده است و درنتیجه این اعتماد به یک طرف ثالث زیان وارد کرده مسئول شناخته شود. نکته اساسی از چنین اقدامی فقط این است که او تشخیص داده دانشش ناقص است و نیاز به اطلاعت سیستماتیک برای تکمیل آن دارد. بنابراین نمی‌توان کاربر را مسئول شناخت مگر در مواردی که کاربر در انتخاب سیستمی که می‌خواهد بر تکیه کند بی‌مبالات باشد یا برای استفاده از سیستم از تخصص و آگاهی کافی برخوردار نباشد (قاجار قیونلو، ۱۳۸۴) و یا با اقدام به مصادیق فعل‌های زیانبار موجود در عرصه ارتباطات الکترونیک در ورود خسارت به اشخاص تهیه گردد به عنوان مثال فرض کنیم کاربری با دستیابی غیرمجاز به داده‌های مربوط به بیماری مسری شخصی این اطلاعات را منتشر نموده و از این طریق ضمن ایجاد سرافکندی و مشکلات اجتماعی برای شخص موجب می‌گردد که مشتریان موسسه تحت مدیریت او از بیم ابتلا به بیماری مسری از مراجعه به موسسه یا معامله با آن خودداری نموده و از این رهگذر شخص دچار خسارات مادی نیز گردد در چنین فرضی شخص اخیرالذکر از رهگذر تخلف کاربرد مزبور متحمل زیان مادی و معنوی شده ست که جبران این خسارات تنها از طریق بکارگیری قواعد مسئولیت مدنی میسر است (اصلانی، ۱۳۸۴).

بحث و نتیجه‌گیری

با توجه به آنچه که در این مقاله بیان شد باید گفت اگرچه فضای مجازی و ارتباطات الکترونیک متفاوت از دنیای افراد به صورت حقیقی می‌باشد اما امکان ورود ضرر در این عرصه نیز باتوجه به ارتباطات واسطه‌ها و کاربران و رد و بدل شدن داده‌های دارای مالیت به عنوان موضوع فعل زیانبار در این فضا متصور می‌باشد. برای تعیین مبنای مسئولیت مدنی در ارتباطات الکترونیک نمی‌توان نظریه واحدی را از جمله تقصیر با خطر ملاک عمل قرار داد بلکه باید باتوجه به مقتضیات هر مورد خاص به انتخاب نظریه‌ای ایده‌آل برای تعیین مبنای مسئولیت در آن مورد اقدام نمود. برای نمونه در بحث واسطه‌های الکترونیکی نظریه غالب اعمال نظریه تقصیر در مبنای مسئولیت می‌باشد اما در جایی که واسطه بدون اطلاع از محتوا صرفاً نقش یک ارائه دهنده خدمات میزبانی را اجرا می‌کند و تولیدکننده محتوا فردی جداگانه از ارائه دهنده آن است و صحت مطالب در ظاهر غلبه دارد به نظر می‌رسد پایبند بودن به تفصیر صرف ما را به نتیجه مطلوب نرساند و نظریات مسئولیت صریح و خطر با ماهیت موضوع سازگارتر باشد.

با عنایت به ماده ۴۶ قانون تجارت الکترونیک مصوب ۱۳۸۲ که ناظر به فضای سایبر در ارتباطات الکترونیکی است و با وحدت ملاک از مبنای ماده مذکور می‌توان این نتیجه را حاصل دانست که اعمال شروط غیرمنصفانه به ضرر کاربران یا دیگر اشخاص دخیل در این ارتباطات قابل پذیرش نمی‌باشد. چرا که اکثریت کاربران فضای مجازی از افراد غیرمتخصص در این زمینه بوده و تحمیل شروط معافیت از مسئولیت مسئولین قابل تصور در فضای مجازی بر این افراد، غیرمنصفانه به نظر می‌رسد. مطابق بررسی‌های صورت گرفته در این مقاله افراد موجود در ارتباطات الکترونیک را می‌توان تحت عنوان تولیدکنندگان محتوا، واسطه‌های الکترونیک و کاربران دسته‌بندی نمود که صور مسئولیت میان این افراد ممکن است منفرداً یا مجتمعاً قابل تصور باشد. همچنین باید گفت ضرر در فضای سایبر به صورت مادی و معنوی قابل تصور می‌باشد و جبران ضرر با قاعده‌های عام مسئولیت از جمله پرداخت غرامت امکان‌پذیر است. از آنجایی که خسارت‌های حاصله از ارتباطات الکترونیک ممکن است از لحاظ جنبه معنوی از اهمیت بیشتری برخوردار باشد، این قبیل ضررها به طریق اعاده وضع به حال سابق و توقف و عدم تکرار عمل زیانبار نیز قابل جبران می‌باشند.

باتوجه به تحولات روزافزون فضای مجازی و گسترش ارتباطات افراد در این عرصه، نیاز به یک قانونگذاری اختصاصی در این مقوله که قابلیت انطباق با پویایی فضای مجازی را دار باشد احساس می‌شود. در کنار مقوله تدوین قوانین نیاز به یک مرجع تخصصی برای رسیدگی به اختلافات حاصل از این حوزه کم اهمیت‌تر از تدوین قوانین نمی‌باشد. برای جلوگیری از ورود خسارات در فضای ارتباطات الکترونیک علاوه بر بالا بردن سطح آگاهی افراد حاضر در این عرصه و تدوین سازوکارهای مناسب جهت ثبت اطلاعات و نظارت بر انجام انتقالات داده در این فضا ضروری به نظر می‌رسد.

بنابراین حائز اهمیت است که قانونگذار با ورود در این زمینه به تدوین قوانین مناسب جهت تعریف دقیق فضای مجازی و ارتباطات الکترونیک و جمع‌بندی تمام مسائل موجود در این عرصه اقدام نموده و با مشخص کردن نهادهای خاص، از طرفی جهت پیشگیری از وقوع جرم و ورود خسارات و نظارت مستمر بر فضای سایبر گام بردارد و از طرف دیگر مراجع اختصاصی رسیدگی به اختلافات به وجود آمده در این فضا را تشکیل دهد که در نتیجه تحقق اقدامات فوق سطح امنیت در ارتباطات الکترونیک را ارتقاء دهد.

منابع

اصلانی، حمیدرضا. (۱۳۸۴). حقوق فناوری اطلاعات، تهران: میزان.

انصاری، باقر. (۱۳۹۱). حقوق حریم خصوصی، تهران: انتشارات سمت.

انصاری، باقر. (۱۳۸۲). مقدمه‌ای برمسئولیت مدنی ناشی از ارتباطات اینترنتی، مجله دانشکده حقوق و علوم سیاسی دانشگاه، ۶۲(۵۱۲)، ۹-۵۲.

باریکلو، علی رضا. (۱۳۸۵). مسئولیت مدنی، تهران: میزان.

پاتر، جیمز دبلیو. (۱۳۹۱). باز شناسی رسانه‌های جمعی با رویکرد سواد رسانه‌ای، ترجمه امیر یزدیان، آزادی، پیام و ناد علی منا، تهران: مرکز پژوهش‌های صدا و سیما.

پور قهرمانی، بابک. (۱۳۹۰). سرقت هویت(جعل هویت) به‌عنوان جرم ناشناخته رایانه‌ای، همایش منطقه‌ای چالش جرایم رایانه‌ای در عصر امروز، مراغه: دانشگاه آزاد اسلامی مراغه.

پورقهرمانی، بابک و صابرنژاد، علی. (۱۳۹۴). حریم خصوصی در فضای سایبر از منظر حقوق بین‌الملل، تهران: مجد.

دهخدا، علی اکبر. (۱۳۷۷). لغت‌نامه دهخدا، تهران: مؤسسهٔ انتشارات و چاپ دانشگاه تهران.

السان، مصطفی. (۱۳۹۱). حقوق تجارت الکترونیکی، تهران: انتشارات سمت.

شکر خواه، یونس. (۱۳۹۰). فضای مجازی، تهران: دانشگاه تهران.

صادقی، حسین. (۱۳۸۸). مسئولیت مدنی در ارتباطات الکترونیکی، تهران: نشر میزان.

قاجار قیونلو، سیامک. (۱۳۸۴). خدمات برای بانک‌های داده آنلان، تهران: انتشارات سازمان مدیریت و برنامه‌ریزی کشور.

قاسم زاده، سیدمرتضی. (۱۳۸۷). الزام‌ها و مسئولیت مدنی بدون قرداد، تهران: میزان.

کاتوزیان، ناصر. (۱۳۸۶). الزام های خارج از قرارداد (ضمان قهری)، تهران: انتشارات دانشگاه تهران.