فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال ششم، شماره‌ی ۲۳ (پاییز ۱۳۹۶): صص ۱۸۶ – ۱۵۷

بررسی مسئولیت مدنی ناشی از نقض امنیت داده در تهدیدات سایبری

نبی‌اله نعمتی[۱]
امیر صادقی نشاط[۲]

تاریخ دریافت: ۱۳۹۶/۱۰/۳۰
تاریخ پذیرش: ۱۳۹۶/۱۲/۱۵

چکیده

تهدیدات سایبری ناقض حریم خصوصی اشخاص حقیقی و حقوقی است و امنیت ملی کشور را تهدید می‌کند. حریم خصوصی فضای سایبر از جنس اطلاعات است و از طرق مختلف از جمله نفوذ به سیستم رایانه‌ای اشخاص، استفاده از روش‌های فریب، وب‌سایت‌ها و شبکه‌های اجتماعی نقض می‌شود. نقض امنیت داده موجب مسئولیت کیفری و مدنی است و واسطه‌های الکترونیک در تحقق این نقض، نقش موثری دارند. موضوع این تحقیق بررسی و تعیین مسئولیت مدنی هریک از واسطه‌های الکترونیک است که فعل یا ترک فعل آنها موجب نقض حریم خصوصی اشخاص و در نتیجه ورود خسارت‌های مادی و معنوی به آنها می‌گردد. این پژوهش متکی به مطالعات کتابخانه‌ای است و هدف آن تبیین مسئولیت مدنی اشخاص حقیقی یا حقوقی درتهدیدات یا حملات سایبری است و حفظ منافع ملی، تأمین امنیت داده‌های ملی و جبران خسارت‌های مادی و معنوی اشخاص در زمرهٔ اصلی‌ترین نتایج این تحقیق به‌شمار می‌رود. براین‌اساس پیشنهاد می‌شود قوانین و مقررات موضوعه این حوزه از جمله قانون مسئولیت مدنی مصوب ۱۳۳۹ متناسب با تهدیدات و حملات سایبری بازنگری و لوایح مرتبط باحقوق سایبری از جمله «لایحه حمایت از اطلاعات و حریم خصوصی افراد در فضای مجازی»و«لایحه مسئولیت ارائه دهندگان خدمات حوزه فناوری اطلاعات » در سیر مراحل تصویب قرارگیرد.

کلید واژگان: *تهدیدات سایبری، امنیت داده، نقض حریم خصوصی، مسئولیت مدنی*

---

[۱] دانشجوی دکتری حقوق دانشگاه جامع امام حسین (ع)
[۲] استادیار دانشکده حقوق دانشگاه تهران

مقدمه

قانونگذاران در ابعاد ملی و سازمانهای بین المللی با تصویب قوانین مورد نیاز و تدوین و امضاء کنوانسیونها تلاش نموده اند خلأهای قانونی و حقوقی دنیای فناوری اطلاعات و فضای مجازی را مرتفع نمایند.

قانون کپی رایت در عرصه دیجیتال ۱۹۹۸آمریکا، قانون مصونیت ارتباطات ۱۹۹۶ امریکا، معاهدات اینترنت ۱۹۹۶ ، مقررات سازمان جهانی مالکیت فکری درخصوص اموال فکری در اینترنت، دستورالعملهای اتحادیه اروپا، معاهدهٔ آنسیترال در استفاده از ارتباطات الکترونیک در قرار دادهای بین المللی و همچنین قوانین ملی از قبیل قانون جرایم رایانه ای و قانون تجارت الکترونیک در ایران از جمله مقرراتی است که در خصوص حمایت از داده و ساماندهی حقوقی فضای سایبر وضع شده است.

حقوق مرتبط با فضای سایبر در یک تقسیم بندی کلی به حقوق کیفری و حقوق خصوصی قابل تفکیک است. با بررسی ابعاد حقوقی حاکم بر فضای سایبر این واقعیّت آشکار می شود که موضوعات قابل طرح در این مقوله ضمن ارتباط با حقوق عمومی، شاخه های حقوق خصوصی را شامل می شود. سایر موضوعات حقوقی قابل بررسی و قابل طرح در حوزه فضای سایبر را می توان به شرح زیر برشمرد :

۱. حقوق تجارت الکترونیک(شامل قراردادها،اسناد و اشخاص تجاری)

۲. جرایم رایانه ای

۳. حقوق حمایت از داده

۴. دولت الکترونیک

۵. حقوق اموال فکری در فضای مجازی

۶. مسئولیّت مدنی در فضای سایبر از جمله مسئولیّت مدنی ناشی از نقض أمنیت داده (نقض حریم خصوصی) در فضای سایبر که الزام اشخاص به جبران خسارات وارده به دیگران را بررسی می کند.

به عبارت دیگر وادار نمون و الزام اشخاص به تدارک و جبران خسارتی که به دیگری تحمیل نموده اند، مسئولیّت مدنی نام دارد أعم از آنکه زیان مذکور بر اثر عمل شخص مسئول یا عمل اشخاص وابسته به او و یا ناشی از اشیاء و اموال تحت مالکیت یا تصرّف او باشد.

مسئولیّت مدنی ناشی از نقض أمنیت داده در فضای سایبر والزام اشخاص به جبران خسارات وارده به دیگران بر خلاف مسئولیّت کیفری بیش از آن‌که جنبه مجازات و کیفر داشته باشد، ترمیم کننده است.

مصادیق مجرمانه مندرج در قوانین جزائی سایبری از قبیل مسئولیت مرتبط با نام های دامنه، هتک حرمت اشخاص، تولید و انتشار ویروسهای رایانه ای، نقض حقوق دارندگان علایم تجاری،نقض حقوق مولف و حقوق دارندگان آن و نقض أمنیت داده علاوه برمسئولیت کیفری پیش بینی شده توسط قانونگذار، می تواند واجد جنبهٔ مسئولیّت مدنی نیز باشد.

اهمیت و ضرورت تحقیق

فضای سایبر یک دنیای واقعی است که به صورت غیر جغرافیایی و در عین حال به صورت واقعی، افراد و کاربران در آن فضا بایکدیگر در حال تولید و تبادل اطلاعات هستند. در نتیجه این فضا دربردارندهٔ کلیه آثار اجتماعی ،فرهنگی و حقوقی است که ارتباطات فیزیکی دارد. از دههٔ ۱۹۹۰ به بعد، انتقال اطلاعات در فضای سایبر بگونه ای رشد و افزایش یافته که موجب پیدایش و وضع مفاهیم جدیدی مانند «جامعه اطلاعاتی»گردیده است. مصونیت چارچوبهای فضای فکری، معنوی و مادی متعلق به اشخاص از حملات سایبری از جمله مهمترین حقوق فطری ،اساسی و شهروندی است که در تعالیم اسلام،اسناد بین المللی و نظامهای حقوقی کشورها مورد حمایت و تاکید قرار گرفته است. منازل و اماکن خصوصی،جسم افراد، اطلاعات شخصی و حوزهٔ ارتباطات افراد، اصلی ترین عرصه های حریم خصوصی را تشکیل می دهند. أمنیت داده در فضای سایبر حق اشخاص در محرمانه ماندن اطلاعات و ارتباطات خصوصی آنها در فضای سایبر و حمایت از داده های شخصی افراد از هرگونه تعرّض و تلاش به منظور دسترسی، جمع آوری ،پردازش و افشاء داده ها، بدون اجازه و بدون مجوز قانونی است.

در دهه‌های اخیر با گسترش فناوری‌های نوین، نقض امنیت داده بیش از پیش خود نمایی می‌کند. نقض حریم خصوصی یکی از مصادیق ورود ضرر و تحقق خسارت در فضای سایبر ناشی از حملات سایبری است. در نظام حقوقی ایران تحلیل و تقنین جرایم رایانه ای از حیث مسئولیت کیفری مورد توجه اساتید حقوق، قوه قضائیه و قوه مقننه قرار گرفته. مع الوصف در موضوع مسئولیت مدنی و خسارات ناشی از حملات سایبری و نقض امنیت داده متناسب با مسئولیت کیفری تحقیقات مقتضی به عمل نیامده است. علاوه بر آن بسیاری از فعالیت‌های زیان‌باری که از طریق اینترنت انجام می‌شود هنوز در قوانین ما عناوین کیفری خاصی نداشته و اصل قانونی بودن جرایم و مجازات‌ها و رعایت تفسیر مضیق در مورد جرایم و مجازات‌ها، مانع از آن هستند که با استناد به احکام کیفری به جبران خسارت و تنبیه مرتکب فعل زیان‌بار اقدام شود.لذا تنها ابزار حقوقی که در اختیار زیان‌دیده-گان از این گونه فعالیت‌ها وجود دارد مسئولیت مدنی است. مطالعه در زمینه ابعاد مسئولیت مدنی ناقضین أمنیت داده در فضای سایبر به رفع این خلا کمک می کند.

پیشینه تحقیق

به تبع نوظهور بودن پدیده و فناوری فضای سایبر، موضوع این پژوهش نیز از قدمت طولانی برخوردار نیست، با توجه به لزوم قاعده‌مند سازی و تعیین چارچوب‌های حقوقی ابعاد موضوع، برخی از نویسندگان و اندیشمندان علم حقوق، با تدوین مقالات و کتب مرتبط تلاش نموده‌اند تا در حد وسع در این خصوص غور نموده و ابعاد حقوقی فضای سایبر را مورد کنکاش قرار دهند. مع‌الوصف موضوع این مقاله به‌صورت مستقل، فاقد پیشینه است.

هدف تحقیق

این پژوهش در پی بررسی و مطالعهٔ مسئولیت مدنی ناشی از نقض حریم خصوصی اشخاص حقیقی و حقوقی(نقض امنیت داده)توسط هریک از واسطه‌های الکترونیکی در حملات سایبری است.

سئوال اصلی تحقیق

سئوال اصلی پژوهش عبارت است: چنانچه حریم خصوصی اشخاص در فضای سایبر توسط واسطه‌های الکترونیکی نقض شود، بر چه مبنایی و چگونه باید به‌جبران خسارت ملزم شوند؟

سئوال فرعی پژوهش

به تبع سئوال اصلی ،این سئوال عنوان می‌شود که: زیان‌دیده‌گان چه نوع خسارت‌هایی را و تا چه اندازه می‌توانند مطالبه کنند؟

فرضیه تحقیق

فرضیهٔ ما در این پژوهش مبین این است که قواعد مسئولیت مدنی به نوع خاصی از خسارت نظر ندارند. هریک از این گروه‌های فعال در اینترنت در صورت انجام حملات سایبری و نقض امنیت داده ، حسب مورد منفرداً یا متضامناً براساس نظریهٔ تقصیر یا خطر یا مختلط، مسئول تلقی می‌شوند و وفق قواعد مسئولیت مدنی زیان‌دیده می‌تواند جبران همه خسارت‌های خود را اعم از مادی و معنوی مطالبه نماید.

روش شناسی تحقیق

این پژوهش متکی به مطالعات کتابخانه‌ای و تحقیقات میدانی است. تلاش شده است ضمن منبع یابی در ابعاد متعددِ محتوایی و عملیاتی،اطلاعات حاصل از منابع، مورد تحلیل و استنتاج حقوقی قرار گیرد.

مبانی نظری تحقیق

۱. مفهوم فضای سایبر

واژه سایبر از لغت یونانی (Kybernetes) به‌معنی سکاندار یا راهنما مشتق شده است. (پاکزاد، بی‌تا: ۲۱۲-۲۴۶).«فضای سایبر»، از حیثِ مفهوم اصطلاحی با عبارات متفاوت و در عین‌حال با مفهوم مشترک

و متناسب با کاربرد این فضا تعریف شده است. درلغتنامهٔ« اتیس تلکام »[1]آمده است: « فضای سایبر، اثرِ فضا و اجتماع شکل گرفته توسط رایانه، شبکه‌های رایانه‌ای و کاربران است. به‌عبارتی‌دیگر یک دنیای مجازی که کاربران اینترنت وقتی برخط هستند، موجودیت پیدا می‌کند» .

در بند«۱» از مادهٔ«۱» سند راهبردی پدافند سایبری کشور مصوب ۱۳۹۴/۰۳/۲۱ کمیتهٔ دائمی پدافند غیر عامل کشور، فضای سایبری به‌شرح زیر تعریف شده است:

« به شبکه‌های وابسته به یکدیگر از زیرساخت‌های فناوری اطلاعات، شبکه‌های ارتباطاتی، سامانه‌های رایانه‌ای،پردازنده‌های تعبیه شده، کنترل کننده‌های صنایع حیاتی، محیط مجازی اطلاعات و اثر متقابل بین این محیط و انسان به‌منظور تولید، پردازش، ذخیره سازی، مبادله، بازیابی و بهره برداری از اطلاعات گفته می‌شودکه ممکن است در ارتباط مستقیم و مداوم با سامانه‌های فناوری اطلاعات و شبکه‌های ارتباطی اعم از شبکه اینترنت باشد و یا تنها قابلیت اتصال به‌محیط پیرامونی در آن تعبیه شده باشد».

هر یک از تعاریف مورد اشاره به‌تنهایی مفهوم فضای سایبر را بیان می‌کند، مع‌الوصف با دقت در مطالب پیش گفته فضای سایبر را می‌توان به‌شرح زیر تعریف کرد :

« فضای سایبر » شامل اثرِ فضا و اجتماع شکل گرفته ناشی از کاربرد رایانه و تعامل کاربران در محیط شبکه‌های رایانه‌ای به‌ویژه شبکه جهانی اینترنت است. اطلاعات راجع به‌روابط افراد، فرهنگ‌ها، ملت‌ها، کشورها و به‌طورکلی جنبه‌های مختلف دنیای واقعی و کلیه آثار اجتماعی، فرهنگی و حقوقیِ ارتباطات فیزیکی، به‌شکل دیجیتالی، مجازی و غیر ملموس در این فضا وجود دارد و از طریق رایانه وشبکه‌های بین‌المللی در دسترس کاربران است».

۲. تهدیدات سایبری

تهدید به هرگونه ظرفیت و امکان بالفعل یا بالقوه بروز یک رویداد مخرب گفته می‌شود. هدف اصلی در حملات سایبری بر هم زدن «موازنه اطلاعات و دانش» است. نقض سیاست امنیتی یک سیستم،

[1] نگاه شود به: http://www.atis.org/glossary/definition.aspx?id=۶۸۶۶

رخنه و نقض امنیت داده‌ها و به‌عبارت‌دیگر هر رویدادی که توانایی دسترسی غیر مجاز به اطلاعات اشخاص و دولت‌ها را در فضای سایبر داشته باشد، در زمره تهدیدات سایبری محسوب می‌گردد.

۳. امنیت داده

از مقولهٔ حریم خصوصی اطلاعات در فضای سایبر و حوزه فناوری اطلاعات و ارتباطات به «امنیت داده » تعبیر می‌شود. اطلاعات افراد با علم و اطلاع یا بدون آگاهی با اهداف متنوّع و مختلف و به‌شیوه‌های گوناگون مورد جمع آوری، ذخیره، پردازش و نگهداری و استفاده قرار می‌گیرد. بنابراین امنیت داده، به فرآیند حفاظت داده‌ها و اطلاعات در برابر انواع کارهای غیرمجاز شامل دسترسی، استفاده، افشا، اختلال، تغییر، مطالعه، بازرسی، ضبط یا تخریب گفته می‌شود. به‌عبارت‌دیگر امنیت داده به‌حفاظت از اطلاعات و به‌حداقل رساندن خطر افشای اطلاعات در بخش‌های غیر مجاز اشاره دارد.

۴. مفهوم، مبانی و منابع مسئولیت مدنی

مسئولیت[1] از مصدر سؤال گرفته شده و سؤال به‌معنی پرسیدن، درخواست کردن و بازخواست کردن است.«مسئولیت در لغت به‌معنی مورد پرسش و سؤال واقع شدن است و غالباً به‌مفهوم تفکیک وظیفه و آنچه که انسان عهده‌دار و مسئول آن باشد» (عمید، بی‌تا: ۱۳۵).

در یک تقسیم‌بندی کلی مسئولیت‌ها به اخلاقی و حقوقی تقسیم می‌شوند. مسئولیت حقوقی مشتمل بر مسئولیت کیفری و مسئولیت مدنی به‌معنای عام است. مسئولیت اخیر نیز به دو دستهٔ قراردادی و غیر قراردادی تقسیم می‌شود که قسم اخیر، مسئولیت مدنی به‌معنای خاص، ضمان قهری و الزامات خارج از قرارداد نیز نامیده می‌شود. (عاشوری، ۱۵:۱۳۸۹). مسئولیّت مدنی از حیث مفهوم کاربردی و اصطلاحی عبارت است از تدارک و جبران ضرر وارده به غیر. مسئولیت مدنی به‌معنی مسئولیت پرداخت خسارت است. بنابراین هرجا که شخص در برابر دیگری مسئول جبران خسارتی باشد، در آن‌جا مسئولیت مدنی وجود دارد.

[1] responsibility

در نظام حقوقی اسلام قواعدی پیش‌بینی شده است که بر تـدارک و جبـران ضـرر و پرداخـت خسارت وارده مادی و معنوی در صورتی‌که رابطه وقوع ضرر و سببِ زیان احراز گـردد، تأکیـد دارد. مهم‌ترین قواعد مورد استناد در این زمینه عبارت‌اند از قاعدهٔ لاضـرر (**لاضَرَرَ وَ لا ضِرارَ فِـی الأسـلام**)، قاعدهٔ اتلاف و تسبیب(**مَن اَتلَفَ مَالَ الغَیر فَهُوَ لَهُ ضَمان**)، قاعده ضمان ید(**عَلَیَ الیَدِ مـا أَخَـذَت حَتَّـی تُؤَدِی**)، قاعده غرور(**المَغرُورُ یَرجُع الی من غرّه**) و برخی قواعد همچون قاعـدهٔ غَـرَر ، قاعـده اقـدام و ضمان تعدی و تفریط. (کاتوزیـان،۴۸:۱۳۷۴، افشـار،۱۳۹۴: ۱۳۲–۷۲ و محمـدی،۱۳۷۳ : ۱۹۳–۱۶۹). مفهـوم و قلمرو شمول این قواعد در این مقال نمی گنجد.

در خصوص مبانی نظری مسئولیت مدنی، نظریهٔ تقصیر، نظریه خطـر، نظریـه تضـمین حـق و نظریه‌های مختلط مطرح است (قاسم زاده ، ۱۳۸۳ :۴۷). مع‌الوصف در هیچ کشوری یک نظریه به‌طـور کامل مورد پذیرش واقع نشده است (صفایی و رحیمی،۱۳۹۱: ۶۷).

منظور از منابع مسئولیت مدنی، منابع قانونی این مسئولیت در نظام حقوقی ایـران اسـت، منـابع مورد اشاره عبارت است از احکام ناظر بر مسئولیت مدنی که در قانون اساسی، قوانین عادی ماهوی و قوانین عادی شکلی و رویه‌های قضایی پیش‌بینی شده است.[1]

[1] مراجعه شود به اصول۲۲(مصون بودن حریم اشخاص از هرگونه تعرض) ،۲۴ (عدم اختلال مطبوعات با مبانی اسلام و حقوق عمومی)،۱۴۰(اضرار به غیر یا تجاوز به‌منافع عمومی) و ۱۷۰(تقصیر یا اشتباه قاضی و جبران خسارت وارده) از منابع مسئولیت مدنی در قانون اساسی، مواد۳۰۱ تا۳۳۷ قانون مدنی در الزامات بدون قرارداد و ضمان قهری و موادی همچون ۱۲۱۵و۱۲۱۶ در خصوص مسئولیت غیر رشید، مواد ۱۳۰تا ۱۳۳ موضوع تعرض به فضای خانهٔ همسایه و تصرف در ملک مستلزم تضرر همسایه، مواد ۱۰۳۵و۱۰۳۷موضوع وعده ازدواج و هدیه ازدواج و مواد ۱۱۷۳و ۱۱۹۱ موضوع حضانت طفل و و وصی منصوب به نگهداری طفل. مواد۴۹۲تا۵۳۷ در خصوص موجبات ضمان در قانون مجازات مصوب ۹۲و مواد ۶۹۰ تا ۶۹۶ قانون مزبور، موضوع هتک حرمت منازل و املاک غیر ، مواد۶۹۷تا۷۰۰، قانون مسئولیت مدنی مصوب ۱۳۳۹و برخی دیگر از قوانین موضوعی و خاص از قبیل مواد ۴ ، ۷و ۱۰۱ قانون آیین دادرسی کیفری۱۳۹۲، قانون احترام به آزادی‌های مشروع و حفظ حقوق شهروندی مصوب ۸۲، مواد ۷ و۲۱ قانون انتشار و دسترسی آزاد به اطلاعات مصوب۱۳۸۷، مادهٔ۲ قانون اهداف و وظایف فرهنگ و ارشاد اسلامی مصوب۶۵، ماده« ۳۱ » قانون مطبوعات مصوب ۶۴و اصلاحی ۷۹، قانون حمایت از حقوق مولفان و مصنفان و هنرمندان مصوب۴۸ و قانون ترجمه و تکثیر کتب و نشریات و آثار صوتی مصوب ۱۳۵۲

۵. مفهوم حریم خصوصی

حریم بر وزن فعیل از ریشهٔ «حرم» به‌معنای منع و تشدید، انشقاق یافته است (احمد بن فارس بن زکریا، ۱۴۰۴ ه ق ، ج۲: ۴۵). مفهوم اصطلاحی حریم خصوصی ارتباط تنگاتنگ با معنای لغوی آن دارد. در بند«۲» ماده «۱»طرح حریم خصوصی، چنین آمده است:

« حریم خصوصی قلمرویی از زندگی هرشخص است که آن شخص عرفاً یا با اعلان قبلی در چارچوب قانون، انتظار دارد تا دیگران بدون رضایت وی به آن وارد نشوند یا بر آن نگاه یا نظارت نکنند و یا به اطلاعات راجع به آن دسترسی نداشته یا در آن قلمرو وی را مورد تعرض قرار ندهند. جسم،البسه و اشیای همراه افراد، اماکن خصوصی و منازل، محل‌های کار، اطلاعات شخصی و ارتباطات خصوصی با دیگران حریم خصوصی محسوب می‌شوند».

مطالعهٔ مسئولیت مدنی ناشی از نقض حریم خصوصی درفضای سایبر مستلزم بررسی حوزه‌ها یا قلمرو حریم خصوصی و مصادیق آن است که عبارت‌اند از حریم اموال و اماکن، حریم جسمانی و معنوی، حریم ارتباطات و حریم اطلاعات یا داده و خمیر مایهٔ نقض حریم خصوصی یا حق خلوت انسانها در همهٔ این حوزه‌ها و قلمروها، اطلاعاتی است که مورد تعرض قرار می‌گیرد.

۶. حریم خصوصی اطلاعات[1]

عبارت است از حق اولیه افراد در محرمانه ماندن و جلوگیری از تحصیل، پردازش و انتشار داده‌های شخصی مربوط به ایشان مگر در موارد مصرّح قانونی. نگرانی‌ها در مورد حریم خصوصی، در هنگام جمع‌آوری و نگهداری به‌صورت دیجیتال یا غیر دیجیتال داده‌ها و اطلاعاتی که فردی را به‌صورت خاص مورد شناسایی قرار دهد، وجود دارد. ریشه و اساس مشکل حریم خصوصی مربوط به افشاگری نامناسب و بدون کنترل داده‌های شخصی است. حریم خصوصی اطلاعاتی دارای مصادیق متعددی ازجمله؛ حریم اطلاعات تجاری و اقتصادی، حریم اطلاعات پزشکی، حریم اطلاعات خانوادگی، حریم اطلاعات مربوط به‌سوابق کیفری و حریم اطلاعات محل کار است.

[1] Information Privacy

از مقولهٔ حریم خصوصی اطلاعات در فضای سایبر و حوزه فناوری اطلاعات و ارتباطات به«امنیت داده »[1] تعبیر می‌شود(رجبی،۱۳۹۱ :۲۹). اطلاعات افراد با علم و اطلاع یا بدون آگاهی با اهداف متنوّع و مختلف و به‌شیوه‌های گوناگون مورد جمع آوری، ذخیره، پردازش و نگهداری و استفاده قرار می‌گیرد.

شیوه های نقض أمنیت داده و تحقق تهدیدات سایبری

بررسی مسئولیت مدنی نقض حریم خصوصی فضای سایبر مستلزم شناخت موضوعی شیوه‌های نقض أمنیت داده در این فضا است.منظور از شیوه‌های نقض حریم خصوصی یا نقض أمنیت داده عبارت است از روش‌هایی که با تمسک به آنها امکان نفوذ و دسترسی به اطلاعات خصوصی اشخاص در فضای سایبر فراهم می‌گردد. بدیهی است با توجه به گسترش دامنهٔ اینترنت و هوشمند سازی اشیاء که از آن تحت عنوان اینترنت اشیاء[2]یاد می‌شود، قلمروِ فضای سایبر و بالتبع نقض حریم خصوصی افراد افزایش می‌یابد.

۱. نفوذ به سیستم رایانه‌ای

نفوذ مستقیم و بدون واسطه به سیستم رایانه‌ای اعم از رایانه، تلفن هوشمند و تبلت که حاوی اطلاعات خصوصی افراد است یا از طریق آن سیستم، اشخاص نسبت به‌ذخیره، پردازش و مبادله داده‌های شخصی، محرمانه و سرّی خود اقدام می‌کنند، ضبط اطلاعات مرورگر و همچنین ایجاد درگاه‌های مشابه درگاه اصلی که از آن به درگاه فریب[3] یاد می‌شود در زمرهٔ شیوه‌های نقض حریم خصوصی قلمداد می‌گردد. ویژگی این روش دسترسی فیزیکی و مستقیم به سیستم رایانه‌ای است.

---

[1] Data protection

[2] Internet of Things (IoT): اینترنتِ اشیاء مفهومی جدید در دنیای فناوری و ارتباطات به‌شمار می‌آید. این اصطلاح برای نخستین بار در سال ۱۹۹۹ توسط کوین اشتون مورد استفاده قرار گرفت و جهانی را توصیف کرد که در آن هر چیزی، از جمله اشیای بی‌جان، برای خود هویت دیجیتال داشته باشند و به کامپیوترها اجازه دهند آن‌ها را سازماندهی و مدیریت کنند. اینترنت در حال حاضر همه مردم را به‌هم متصل می‌کند ولی با اینترنت اشیاء تمام چیزها به‌هم متصل می‌شوند. برای اطلاعات بیشتر مراجعه شود به: https://iot.itrc.ac.ir/content.https://fa.wikipedia.org/wiki

[3] Phishing

در این روش امکان مشاهده فایل‌های شخصی، مشاهده سوابق فعالیت افراد در فضای مجازی، تعبیه نرم افزارهای رصد کننده فعالیت اشخاص در فضای مجازی، فعال سازی دوربین هوشمند سیستم و گزارش‌گیری مستمر، نصب بد افزارها و ...، متصور است.

۲. نفوذ از طریق سیستم‌های تقلّبی

از دیگر شیوه‌های دسترسی سیستمی به اطلاعات کاربران و نقض حریم خصوصی آنها، استفاده از سیستم‌های مشابهِ سیستم اصلی است. با رونق و گسترش بانکداری الکترونیک و پرداخت الکترونیک، جرایم سایبری به‌شکل‌های مختلف در این حوزه نیز همگام با این صنعت گسترش یافته است. کپی کردن غیر قانونی داده‌های نوار مغناطیسی کارت بانکی روی یک کارت دیگر که اصطلاحاً «کپی کارت »[1] نامیده می‌شود و نفوذ از طریق صفحه کلیدهای ثانویه، یعنی صفحه کلیدها روی صفحه کلید اصلی نصب می‌شوند در زمره مصادیق این روش هستند.

۳. نفوذ از طریق اینترنت(فضای سایبر)

عرصهٔ سایبر را بعد از زمین، هوا و فضا و دریا، پنجمین عرصه جنگ جهانی می‌دانند. با نگرش به اینکه در حال حاضر کلیهٔ صنایع از ارتباطات شبکه‌ای برای تبادل اطلاعات استفاده می‌کنند، در صورت بروز جنگها و حملات سایبری، خسارت‌های ناشی از این جنگها بسیارسنگین خواهد بود. مطالعات نشان می‌دهد اهداف حملات سایبری اختلال در زیر ساخت‌های اینترنتی کشورها، وب‌سایت‌های دولتی و سازمانی، وب‌سایت‌های شرکتها، صنایع و وب‌سایت‌های رسانه‌ای است. (خلیل زاده ،۱۳۹۳،:۳۸ و هیتر هریسون دنیس۱۳۹۴،:۲۴- ۱۷) دسترسی به اطلاعات کاربران فضای سایبر و نقض امنیت داده‌های آنها، علاوه بر نفوذ مستقیم به سیستم‌های رایانه‌ای از طریق اینترنت و بر پایهٔ وب نیز میسر است.[2]

---

[1] Card Skimming

[2] برای مطالعه بیشتر راجع به حملات سایبری، مفاهیم، ابعاد حقوقی، خسارات و مسئولیت‌های آن مراجعه شود به:
Carr, Jeffrey.2007, Inside Cyber Warfare Available at:
https://wikileaks.org/sony/docs/05/docs/eBooks/Inside_Cyber_Warfare.pdf

طراحی درگاه‌های فریب برپایهٔ وب، نفوذ به رایانامه، در اختیار گرفتن شناسه کاربری و نفـوذ از طریق شبکه‌های اجتماعی از شیوه‌های نفوذ به اطلاعات کاربران در این مقوله هستند.

تجزیه و تحلیل یافته ها

در مباحث قبلی مبانی نظری تحقیق به عنوان مقدمه ورود به تحلیل محتوایی و آشنایی با کلید واژه های پژوهش به اجمال مرور شد،در این بخش موضوع پژوهش،یعنی مسـئولیت مـدنی نقـض أمنیت داده در حملات سایبری مورد تحلیل قرار می گیرد.

برابر آمار رسمی و اعلامی توسط پلیس فتا، شـاهد افـزایش ۹۰۰ درصـدی جـرایم سـایبری در ایران هستیم، بگونه ای که در سال ۹۶، حدود ۲۹۶ حملـه جـدی بـه سـامانه‌ها و زیرسـاخت‌های حیاتی و حساس کشور صورت گرفته که ۵۰ درصد آنها از سمت آمریکا و چین بوده اسـت . هـدف این حملات را بانک‌ها و مؤسسات پولی و اعتباری، زیرساخت‌های مخابراتی، زیرساخت‌های توزیـع انرژی برق و گاز، صنایع و بخش فراورده‌های نفتی و وزارتخانه‌ها و سازمان‌هاتشکیل می دهند

وفق آمارهای فوق، بالغ بر ۳۰هزار کانال و گـروه مجرمانـه در تلگـرام و حـدود،۵۱ هـزار پـیج اینستاگرامی مجرمانه شناسایی شده اند و در طول ۶ سال گذشته بالغ بر ۱۲۰ هزار فقره پرونـده در زمینه جرایم سایبری تشکیل شده است.[۱]

Singer, P. W and Friedman, Allan, 2013 ybersecurity and Cyberwar, Available at:
https://news.asis.io/sites/default/files/Cybersecurity_and_Cyberwar.pdf
Geers, Kenneth, 2015, cyber war in perspective russian aggression against Ukraine, Available at:
https://ccdcoe.org/sites/default/files/.../pdf/CyberWarinPerspective_full_book.pdf
Martin, C, Libickip 2009 ,Cyberdeterrence and cyberwar, Available at:
www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf
Schmidt, Andreas,2013, The Estonian Cyberattacks, Available at:
netdefences.com/wp.../SchmidtA-2013-Estonian-Cyberattacks.pdf

[۱] مراجعه شود به: ttp://www.farsnews.com/newstext.php?nn=۱۳۹۷۰۲۰۹۰۰۰۵۳۰

با تصویب قانون جرایم رایانه ای ایران مصوب ۱۳۸۸/۰۴/۱۰ و ماده «۲» کنوانسیون جرایم رایانه ای بوداپست ۲۰۰۱ ، عناوین کلی شیوه های نقض حریم خصوصی اطلاعات کاربران از طریق ارتکاب جرائم علیه محرمانگی داده ها و سامانه های رایانه ای و مخابراتی مشتمل بر دسترسی غیرمجاز، شنود غیرمجاز و جاسوسی رایانه ای مورد تقنین قرار گرفته است.حال با علم به اینکه با خلا قانونی در زمینهٔ مسئولیت مدنی ومطالبه خسارات مادی و معنوی ناشی از جرایم و حملات سایبری روبرو هستیم، در ادامه مباحث به عنوان یافته های این پژوهش بررسی خواهد شدکه از منظر حقوقی بر اساس کدام موازین و تا چه حدودی خسارات مادی و معنوی از عوامل وقوع حملات سایبری قابل پیگیری قانونی است. بر این اساس تلاش می شود ضمن شناسایی اشخاص حقیقی و حقوقی که عامل وقوع حملات سایبری شناخته می شوند و در اصطلاح به آنها «واسطه های الکترونیکی» گفته می شود، مسئولیت مدنی این اشخاص در تهدیدات سایبری به صورت جداگانه مورد بررسی وتحلیل قرار گیرد.

– تأمین کنندگان خدمات میزبانی[1] درصورت تعدی و تفریط مسئول جبران خسارت هستند.

خدمات میزبانی، به‌معنای اجاره فضا بر روی شبکه اینترنت، جهت نگهداری فایل‌ها و داده‌های سایت می‌باشد. به شرکت‌های ارایه‌کنندهٔ خدمات میزبانی وب[2]یا شرکت میزبانی [3] نیز می‌گویند.

راه اندازی خدمات میزبانی در ایران بر اساس ضوابط ناظر به میزبانی و تبادل محتوا در شبکه‌های ارتباطی و فناوری اطلاعات موضوع مصوبات جلسه مورخ ۰۷/۱۸/ ۱۳۸۹کمیسیون تنظیم مقررات ارتباطات است.

به لحاظ فنی تأمین کنندگان خدمات میزبانی نقش واسطه در انتقال و ذخیره داده‌های اشخاص را به‌عهده دارند و جز در موارد مصرّح و تکالیف ابلاغی توسط کمیسیون تنظیم مقررات ارتباطات، بر محتوای اطلاعات مورد مبادله نظارتی ندارند.

به‌نظر می‌رسد در صورت رعایت چارچوب‌ها و ضوابط ابلاغی توسط شرکت‌های ارایه‌کنندهٔ خدمات میزبانی وب و از طرفی ماهیت حرفه‌ای و صنفی آنها، اصل بر عدم مسئولیت مدنی ناشی از

[1] Hosting service providers(HSP)
[2] Web Hosting
[3] Hosting Company

نقض حریم خصوصی اشخاص یا کاربرانی است که محتوای آنها در این شرکتها ذخیره شده است. مگر اینکه اثبات شود این مؤسسات وفق مادهٔ «۹۵۳» قانون مدنی نسبت به ایفای وظایف خود دچار تعدی و تفریط شده‌اند. در فرض اخیر در صورت احراز رابطهٔ سببیت بین خسارت وارده به اشخاص ناشی نقض حریم خصوصی آنها و تقصیر ارائه دهندهٔ خدمات میزبانی، مؤسسات مزبور وفق قواعد عمومی مسئولیت مدنی موظف به‌جبران خسارت‌های مادی و معنوی زیان‌دیده‌گان هستند.

– ایجاد کنندگان نقطه تماس بین‌المللی[1] درصورت اثبات تقصیر در وقوع حملات سایبری مسئول قلمداد می شوند

مهم‌ترین نقش و کارکرد ایجاد کنندگان نقطه تماس بین‌المللی فراهم نمودن بستر دسترسی به فضای سایبر برای کاربران است. در ایران وفق « مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای مصوب سال ۱۳۸۰ شورای عالی انقلاب فرهنگی و مستند به بند«۱» از «آیین‌نامه نحوه اخذ و ضوابط فنی نقطه تماس بین‌المللی»، حق ایجاد نقطه تماس بین‌المللی در انحصار دولت است و ارائه مجوز به دستگاه‌های ذی‌ربط توسط شورای عالی‌اطلاع رسانی صورت می‌گیرد.

ایجاد کنندگان نقطهٔ تماس بین‌المللی بستر بهره برداری از دنیای سایبر را فراهم می‌کنند ولی نقشی در تعاملات، اقدامات و فعل و انفعلات کاربران ندارند. این دسته از واسطه‌ها برای شروع و ادامهٔ فعالیت نیاز به اخذ مجوز دارند و موظفند مطابق مقررات مرتبط عمل نمایند. به‌نظر می‌رسد با توجه به مقتضیات کارکردی ایجاد کنندگان نقطهٔ تماس بین‌المللی و نظارت[2] دستگاه‌های حاکمیتی بر عملکرد آنها، این طیف از اشخاص فعّال در فضای سایبر، ماهیت حقوقی امین را داشته و تا زمانی که نسبت به‌وظایف قانونی خود تعدی و تفریط ننمایند، مقصر شناخته نمی‌شوند. براین‌اساس اصل بر عدم مسئولیت مدنی ایجاد کنندگان نقطهٔ تماس بین‌المللی است. بدیهی است در صورت تخطی از وظایف مقرر، قواعد کلی مسئولیت مدنی در قبال خسارت‌های واردهٔ احتمالی بابت نقض حریم خصوصی اشخاص توسط ایجاد کنندگان نقطهٔ تماس بین‌المللی حاکم است و برمبنای نظریه تقصیر مسئول قلمداد و موظف به‌جبران ضرر و خسارت‌های وارده هستند. برابرحکم کلی ماده «۱»

[1] Acess Service providers(ASP)

[2] طبق مادهٔ« ۱۱»آیین‌نامه نحوه اخذ و ضوابط فنی نقطه تماس بین‌المللی، نظارت بر حسن اجرای عملکرد نقاط تماس به عهده وزارت ارتباطات و فنّاوری اطّلاعات می‌باشد

قانون مسئولیت مدنی مصوب ۷ اردیبهشت ۱۳۳۹ «هر کس بدون مجوز قانونی عمداً یـا در نتیجـه بی‌احتیاطی به جان یا سلامتی یا مال یا آزادی یا حیثیت یا شهرت تجارتی یا به هـر حـق دیگرکـه به‌موجب قانون برای افراد ایجاد گردیده لطمه‌ای وارد نماید که موجب ضرر مادی یا معنوی دیگری شود مسئول جبران خسارت ناشی از عمل خود می‌باشد».

احکام مندرج در مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای مصوب ۱۳۸۰شورای عـالی انقلاب فرهنگی، مؤید رویکرد مورد اشاره در خصوص مسئولیت مدنی ایجاد کنندگان نقطهٔ تمـاس بین‌المللی است. در بند«۵» آیین‌نامه نحوه اخذ و ضوابط فنی نقطه تمـاس بین‌المللـی تأکیـد شـده است: « هر دستگاه اجرایی که مجوز برقراری تماس بین‌المللی را اخذ می‌نماید، صرفاً مجاز به ارایه خدمات در محدوده وظایف قانونی و تشکیلات مصوب خود می‌باشد....». مستند بـه بنـدهای «۶» و« ۸» آیین‌نامه مورد اشاره، تکالیف مصرّح ایجاد کنندگان نقطه تماس بین‌المللی در زمینـهٔ امنیـت سیستم‌ها، پشگیری از نفوذ و دسترسی غیر مجاز به اطلاعات کاربران و در نتیجه ممانعت از نقـض حریم خصوصی اشخاص در فضای سایبر عبارت است از :

۱. پیش‌بینی سیستم پالایش مناسب به‌منظور ممانعت از دسترسی به پایگـاه ممنـوع اخلاقـی و سیاسی و حذف ورودی‌های غیر مطلوب

۲. تعبیهٔ دیوارهٔ آتش[1] مناسب به‌منظور صیانت شبکه‌ها از تخریب، فریب و سرقت اطّلاعات

۳. جلوگیری از برقراری ارتباطات غیر متعارف

۴. منحصر نمودن ارایه خدمات در فضای سایبر وفق مجوز صادره

با عنایت به مراتب فوق، رساها[2] در زمینهٔ فعالیت و ارایه خدمات در فضای سایبر هماننـد سـایر مشاغل و اصناف، صنف تخصصی محسوب شده و تابع ضوابط اختصاصی هستند. براین‌اساس اصل

[1] Fire wall

[2] شرکت‌ها یا مؤسسات ارائه کننده خدمات اطلاع رسانی و اینترنتی، رسا یا (Internet (Service Provider ISP) خوانده می‌شوند.

اینترنت از پیوند تعداد بی‌شماری شبکه‌های ارتباطی کامپیوتری کوچک و بزرگ که حاوی اطلاعات متنوع می‌باشد تشکیل می‌شود. یک فرد متصل به‌شبکه اطلاع رسانی و اینترنت تنها مشاهده‌گر و مرورگر اینترنت نمی‌باشد بلکه جزئی از این شبکه بوده و می‌تواند با آن تبادل اطلاعات نماید. یک رسایا ISP اتصال به‌شبکه اطلاع رسانی و اینترنت را فراهم می‌آورد و جزء ضروری دسترسی و اتصال افراد به‌شبکه اینترنت می‌باشد

بر عدم مسئولیت این واسطه‌ها است. معالوصف در صورت نقض حریم خصوصی افراد بر اثر تخلف از وظایف ابلاغی، بر مبنای نظریهٔ تقصیر، واجد مسئولیت مدنی هستند، ضمن آنکه اثبات تقصیر متوجه خواهان دعاوی مسئولیت مدنی است.

بند «۹»آیین‌نامه مورد اشاره در خصوص ضمانت اجرای تکالیف پیش‌بینی شده برای دارندگان مجوز نقطه تماس بین‌المللی مقرر می‌دارد:

«دارندگان مجوز نقطه تماس بین‌المللی موظف به‌رعایت کلیه ضوابط مندرج در این آیین‌نامه و قوانین و مقررات جاری کشور می‌باشند و در صورت تخلف از آن در مرحله اول تذکر و در مرحله دوم قطع موقت (حداکثر یک هفته) صورت می‌گیرد و در صورت تکرار ضمن قطع ارتباط، با تأیید شورای عالی اطلاع‌رسانی و کمیسیون مربوط برای رسیدگی به‌جرایم، به‌مراجع ذی‌ربط معرفی می‌شوند».

نکته آخر اینکه؛ مادهٔ« ۷۸» قانون تجارت الکترونیکی مصوب ۱۳۸۲نیز مبنای مسئولیت مدنی این قبیل واسطه‌ها در فضای سایبر را اثبات تقصیر دانسته و مقرر داشته است: « هرگاه در بستر مبادلات الکترونیکی در اثر نقص یا ضعف سیستم مؤسسات خصوصی و دولتی، ... خسارتی به اشخاص وارد شود، مؤسسات مزبور، مسئول جبران خسارت وارده می‌باشند مگر اینکه خسارت‌های وارده ناشی از فعل شخصی افراد باشد که در این صورت، جبران خسارت بر عهده این اشخاص خواهد بود».

– مسئولیت مدنی رساها در زمینه تحقق نقض امنیت داده بر اساس نظریه تقصیر و نظریه خطر قابل تحلیل است.

بند«ب» مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای مصوب ۱۳۸۰شورای عالی انقلاب فرهنگی، مشتمل بر آیین‌نامه واحدهای ارائه کننده خدمات اطلاع رسانی و اینترنت رسا، است. در این آیین‌نامه، حدود فعالیت رساها به‌شرح ذیل تعریف شده است:

۱. شرکت‌ها یا مؤسسات ارائه کننده خدمات اطلاع رسانی و اینترنت رسا (ISP) تحت ضوابط و قوانین مشخص شده در کشور فعالیت می‌نمایند و می‌توانند هم مستقلاً و هم در ارتباط با شبکه اینترنت به فرآوری اطلاعات پرداخته و به‌کاربران خود عرضه نمایند.

۲. ارائه مجموعه خدمات ارزش افزوده بر خط (on-line) و برون خط (off-line) برای کاربران

۳. فراهم آورنده دسترسی و همچنین تهیه و فرآوری محتوی برای کاربران خود.

۴. انجام انواع فعالیتها برای آشنا نمودن کاربران در استفاده بهینه از شبکه اطلاع رسانی و اینترنت.

۵. فراهم سازی خدمات، تهیه، تولید، توزیع یا ارائه اطلاعات برای کاربران مربوط

شرح وظایف رساها ما را به این نکته رهنمون می‌سازد که برخلاف ایجاد کنندگان نقطه تماس بین‌المللی که صرفاً ارائه دهنده خدمات دسترسی به فضای سایبر هستند، رساها کارکرد دوگانه دارند. به‌عبارت‌دیگر رساها در عین‌حال که فراهم آورنده دسترسی کاربران به فضای سایبر هستند، می‌توانند نسبت به تهیه و فرآوری محتوی برای کاربران خود اقدام کنند.

بر این اساس در تعیین مبانی مسئولیت مدنی رساها در فرض نقض حریم خصوصی اشخاص باید قائل به تفصیل شد. آیین‌نامه واحدهای ارائه کننده خدمات اطلاع رسانی و اینترنت رسا با دقت به ساختار حقوقی مسئولیت مدنی رساها در نقض حریم خصوصی توجه داشته است. بند ۵-۳- ۱۲ آیین‌نامه ناظر به‌نقش و کارکرد رساها در زمینهٔ بستر سازی و فراهم سازی خدمات دسترسی کاربران به اینترنت است و مقرر می‌دارد:

«رسا (ISP) موظف است اطلاعات مربوط به‌نحوه حفاظت از حریم خصوصی اطلاعات و ارتباطات افراد در شبکهٔ خود را در اختیارکاربران قرار دهد».

بند ۵-۳-۱۵ آیین‌نامه موصوف نیز در مقام تبیین مسئولیت رساها در نقش فرآوری محتوا است. برابر این بند؛ «حریم اطلاعات خصوصی کاربران از مصونیت برخوردار بوده و هرگونه دسترسی غیرقانونی توسط رساها و هر مرجع دیگر به فعالیت‌های‌اینترنتی کاربران ممنوع می‌باشد» ضمن آنکه در بند ۶-۱۳، تولید و عرضهٔ برخی از محتواها از جمله افشای روابط خصوصی افراد و تجاوز به‌حریم اطلاعات شخصی آنان، توسط رساها و کاربران ممنوع شده است. باتوجه به‌مقررات مورد اشاره، در جمع‌بندی مبنای مسئولیت مدنی رساها می‌توان گفت:

۱. مسئولیت مدنی رساها تا زمانی که برابر مقررات صنفی و ضوابط ابلاغی[1] صرفاً نقش واسطهٔ خدمات دسترسی به فضای سایبر را دارند، مبتنی بر تقصیر است. بند ۵-۳-۴ آیین‌نامه در تأیید این نظر بیان می‌دارد؛ « مسئولیت رسا (ISP) در مورد دسترسی به اطلاعات عرضه شده توسط دیگران محدود به ایجاد امکان و اعمال برقراری پالایه در شبکه خواهد بود».

۲. مسئولیت مدنی رساها در زمینهٔ نقض حریم خصوصی اشخاص در مواردی که به‌تولید و فرآوری محتوا می پردازند، همانند سایر کاربران مبتنی بر مسئولیت صرف است. براین‌اساس هرگونه نفوذ غیرمجاز به مراکز دارنده اطلاعات خصوصی و محرمانه و تلاش در جهت شکستن قفل رمز سیستم‌ها موضوع بند ۶-۱۷آیین‌نامه و افشای روابط خصوصی افراد و تجاوز به‌حریم اطلاعات شخصی آنان موضوع بند ۶-۱۳ آیین‌نامه ولو بدون تقصیر باشد، واجد مسئولیت مدنی است.

کلام آخر در خصوص مبانی مسئولیت رساها اینکه،بندهای ۹ و ۱۰، آیین‌نامه، سازوکار رسیدگی به‌تخلفات رساها را پیش‌بینی نموده است. بند ۱۰ ناظر به‌مسئولیت کیفری و مجازات رساها است.

وفق این بند: «در صورت تخطی از موارد مندرج در این مصوبه، مجازات‌های اعمال شده شامل تذکر، قطع موقت مجوز، لغو پروانه و طرح در دادگاه‌ها و محاکم قانونی بسته به‌نوع تخلف براساس قوانین و ضوابط ذی‌ربط بر عهده کمیسیون راهبردی می‌باشد که براساس گزارش فناوری اطلاعات و ارتباطات بررسی و اعلام نظر می‌نماید».

به‌نظر می‌رسد مستند به بند ۱۰ آیین‌نامه، مطالبه خسارت‌های و ضرر و زیان مدنی نیز از طریق ارجاع به محاکم امکان‌پذیر است. براساس این بند؛ « نظر کمیسیون راهبردی لازم‌الاجرا و قطعی است، لیکن مانع شکایت و اقامه دعوی افراد ذی‌نفع در محاکم نخواهد بود».

– خسارات مادی و معنوی ناشی از شکل‌گیری تهدیدات سایبری توسط دفاتر خدمات حضوری اینترنت[2] حسب مورد براساس نظریه تقصیر یا خطر قابل مطالبه است.

[1] وفق بند ۷-۴- آیین نامه واحدهای ارائه کننده خدمات اطلاع رسانی و اینترنت رسا (ISP) ؛کلیه دستگاه‌های دولتی و نهادهای عمومی در ارائه خدمات اطلاع رسانی و اینترنتی موظفند در محدوده وظایف و مأموریت سازمانی خود فعالیت نمایند.

[2] Coffeenet

مطابق آیین‌نامه دفاتر خدمات حضوری اینترنت موضوع بند«ج» مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای مصوب ۱۳۸۰ شورای عالی انقلاب فرهنگی؛ دفتر خدمات دسترسی حضوری به شبکه‌های اطلاع رسانی و اینترنت محلی برای دسترسی حضوری مشتریان و کاربران به شبکه اطلاع رسانی (اینترنت و اینترانت) می‌باشد. این دفاتر، ضمن رعایت ضوابط مندرج در این آیین‌نامه، واحد صنفی محسوب می‌شوند و مشمول قانون نظام صنفی بوده و مجوز لازم توسط اتحادیه صنفی صادر می‌شود. دفاتر مورد اشاره در عداد واسطه‌های فنی خدمات دسترسی به اینترنت قرار نمی‌گیرند، بلکه این دفاتر با فراهم ساختن سخت افزار و نرم افزار مورد نیاز در قالب یک اتحادیهٔ صنفی، به‌صورت حضوری امکان دسترسی کاربران را با فضای سایبر فراهم می‌کنند. در نتیجه این دفاتر در وهلهٔ اول مستقیماً و بالذات با فضای سایبر و حریم خصوصی کاربران ارتباط ندارند، مگر اینکه علاوه بر نقش اولیه، راسا نیز به‌تولید و عرضه محتوا اقدام نمایند که در این فرض در قالب شخصیت حقوقی یک تولید کنندهٔ محتوا یا یک کاربر، ایفای نقش می‌کنند.

با توجه به ساختار حقوقی دفاتر مورد اشاره، مبنای مسئولیت مدنی آنها از حیث صنفی و حرفه‌ای همانند سایر صنوف اثبات تقصیر در انجام مطلوب وظایف توسط خواهان است. مطابق بند ۷– ۱۵ آیین‌نامه دفاتر خدمات حضوری اینترنت ، افشای روابط خصوصی افراد و تجاوز به‌حریم اطلاعات شخصی آنان ممنوع است فلذا در صورت توسل به‌شیوه‌های نقض حریم خصوصی اشخاص و تولید و عرضهٔ محتوا در این خصوص، بر مبنای نظریه خطر مسئول جبران و تدارک خسارت‌های وارده از حیث نقض حریم خصوصی اشخاص هستند.

بند «۶» آیین‌نامه مورد اشاره در تأیید این برداشت حقوقی مقرر می‌دارد: « دفاتر و کاربران برای محتوایی که خود تولید و عرضه می‌نمایند مطابق مقررات و ضوابط قانونی موجود کشور از جمله رعایت قوانین و مقررات حق مالکیت معنوی، مسئول و پاسخگو می‌باشند».

بند «۸» آیین‌نامه، ناظر به‌رسیدگی به‌تخلفات و جرایم این دفاتر است و با تأکید بر قواعد عمومی مسئولیت مدنی و مقررات مندرج در بند «۸» آیین‌نامه، طرح دعاوی کیفری و مدنی در صورت نقض حریم خصوصی کاربران از پشتوانهٔ قانونی برخوردار است.

– مسئولیت مدنی مدیران و اداره کنندگان سایت‌ها در وقوع حملات سایبری متناسب با فعالیت حرفه ای آنها قابل تحلیل است.

وب‌سایت‌ها در فضای سایبر دربردارندۀ محتوای مواد دیداری، شنیداری، نوشتاری و یـا ترکیبـی از آنها در هرشکل و قالب هستند. وفق بند «ض»مادۀ«۱» آیین‌نامه ساماندهی و توسعه رسانه‌هـا و فعالیت‌های فرهنگی دیجیتال مصوب ۱۳۸۹ هیأت وزیران، رسـانه دیـجیتال: رسـانه مبتنـی بـر فـناوری نـوین اطلاعـات و ارتباطـات، شـامل گونه‌های زیر است:

۱. بسته نرم افزاری رسانه‌ای

۲. حامل دیجیتال حاوی داده

۳. رسـانه برخط

برابر بندهای«ز»،«ژ»،«س» و«ش»مادۀ«۱» آیین‌نامه مورد اشاره، رسانه‌ها بـه رسـانه بـرخط، رسانه برخط اختصاصی، رسانه پیام‌ده و رسانه کاربر محور تقسیم می‌شود.[۱]

بند «ط»مادۀ «۱»آیین‌نامه موصوف، فعالیت فرهنگی دیجیتال را به‌شرح زیر تعریف نموده است:

فعالیت فرهنگی دیجیـتال: فعالیـت فـرهنگی مبتنی بر فـناوری نـوین اطلاعـات و ارتباطـات، شامل گونه‌های زیر:

[۱] « ز– رسانه برخط: هر سامانه- که امکان قراردادن محتوای دیجیتال در معرض دسترس عمـوم یا بیش از یک‌هزار مخاطب مشخص یا نا مشخص از طریق بستر شبکه نظیر شبکه گسترده جهانی، شبکه‌های محلی، شبکه‌های مبتنی بر فناوری بلوتوث، شبکه‌های تلفن ثابت و همراه را فراهم می‌آورد.

ژ– رسانه برخط اختصاصی: رسانه برخط که فقط شخص حقیقی یا حقوقی متـصدی آن را معرفی و محتوای دیجیتال درقلمرو اطلاعات، اخبار، خدمات، آثـار و محـصولات شـخص یاد شده را در معرض دسترس قرار می دهد.

س– رسانه پیام‌ده: رسانه برخط مبتنی بر سامانه‌ای که امکان ارسال پیام‌های حاوی محتوای دیجیتال از طریق بسترشبکه ارتباطی و مخابراتی برای بیش از یک‌هزار مخاطب مشخص یا نامشخص را فراهم می‌آورد، از قبیل سامانه‌های ارسال انبوه پیامک و سامانه‌های ارسال پیام با فناوری بلوتوث.

ش– رسانه کاربر محور: رسانه برخطی که بـستر قـراردادن محتـوای دیجیتـال در معـرض دسترسـی عمـوم یـا بـیش از یـکهزار مخاطـب مـشخص و همچنـین تعامـل و تـشکیل گروه ها و شبکه‌های مجازی را برای کاربران فراهم آورد».

۱. تصدی رسانه برخط.

۲. پدیدآوردن، تهیه کردن و عرضه بسته نرم افزاری رسانه‌ای و بستهٔ نرم افزاری رسانه‌پرداز.

۳. تکثیر حامل دیجیتال و خدمات مرتبط به قصد انتفاع یا برای عرضه توسط تکثیر کننده.

۴. نشر دیجیتال.

۵. تصدی مرکز بازی و سرگرمی دیجیتال.

۶. تصدی ایجاد، توسعه، پشتیبانی و اداره هرشکل رسانه برخط، سامانه یا مرکز بازی و سرگرمی دیجیتال به‌سفارش متصدیان مربوط.

۷. ارائه هرگونه خدمات ویرایش محتوا با استفاده از ابزارهای مبتنی بر فناوری نوین اطلاعات و ارتباطات

برابر بند«ظ»ماده«۱»آیین‌نامه پیش گفته؛ واحد فرهنگی دیجیتال به‌شرح زیر تعریف شده است:

« هر سامانه، مکان کسب و کار، شخص حقوقی و یا تشکیلات تحت هر شکل و عنوان از قبیل گروه، سازمان، مرکز، شرکت، مؤسسه، فروشگاه، کارگاه، کارخانه، شبکه، وب‌سایت، پایگاه اطلاع رسانی و رسانه برخط که فعالیت فرهنگی دیجیتال انجام داده یا برای فعالیت فرهنگی دیجیتال مورد استفاده قرار می‌گیرد».

مادهٔ«۲»آیین‌نامه مورد اشاره، ایجاد و فعالیت هر واحد فرهنگی دیجیتال و انتشار هر رسانه دیجیتال را منوط به اخذ مجوز از وزارت فرهنگ و ارشاد اسلامی دانسته و تأکید نموده است؛ متخلفان وفق قانون تعطیل مؤسسات و واحدهای آموزشی و تحقیقاتی و فرهنگی که بدون اخذ مجوز قانونی دائر شده و می‌شود– مصوب ۱۳۷۲– و سایر قوانین موضوعه مورد پیگرد قانونی قرارخواهند گرفت.

ستاد ساماندهی پایگاه‌های اینترنتی وابسته به مرکز توسعه فناوری اطلاعات و رسانه‌های دیجیتال وزارت فرهنگ و ارشاد اسلامی مرجع احراز هویت مدیران تمام پایگاه‌های اینترنتی است. تمامی اطلاعات ثبت شده سایت‌ها در این ستاد در کارگروه تعیین محتوای مجرمانه مورد استفاده قرار می‌گیرد. این سامانه تحت عنوان سایت ساماندهی پایگاه‌های اینترنتی در سال ۱۳۸۵ به‌منظور

ثبت اطلاعات مدیران پایگاه‌های اینترنتی ایرانی تشکیل شده است و کلیهٔ سایت‌های فعال ایرانی صرف‌نظر از نوع و موضوع فعالیت اعم از تجاری، شرکتی، شخصی، فرهنگی یا دولتی ملزم به‌ثبت مشخصات خود در این سامانه هستند و از لحاظ نوع و موضوع فعالیت تفاوت خاصی بین آنها وجود ندارد. به استناد تبصرهٔ«۱» ماده «۲۱» قانون جرایم رایانه‌ای مصوب ۱۳۸۸، اگر پایگاهی حاوی محتوای مجرمانه باشد، در صورتی‌که مشخصات مدیر پایگاه در ساماندهی ثبت شده باشد، چنانچه وی در اسرع وقت نسبت به حذف محتوای مجرمانه اعلام شده از پایگاه خود اقدام نماید، پایگاهش فیلتر نخواهد شد. مدیران و اداره کنندگان سایت‌ها، اشخاص حقیقی و حقوقی هستند که وفق ضوابط پیش گفته مجوز فعالیت و اداره گروه، سازمان، مرکز، شرکت، مؤسسه، فروشگاه، کارگاه، کارخانه، شبکه، وب‌سایت، پایگاه اطلاع رسانی و رسانه برخط را در فضای سایبر عهده دار هستند.

برخی از پژوهشگران با تأکید بر اینکه؛ مدیران و اداره کنندگان سایت‌ها غالباً خود نقشی در ارائه اطلاعات و محتوا ندارند و ماهیت فعالیت این گروه از حاضران در فضای سایبر به‌گونه‌ای است که با ایجاد یک سایت یا پایگاه اینترنتی، مکانی را برای اشتراک گذاری اطلاعات متنی یا تصویری و صوتی دیگران فراهم می‌آورند معتقدند مدیران اینگونه سایت‌ها علی‌الاصول از مسئولیت مدنی مبرّا هستند و مسئولیت اصلیِ عمل بر عهده کاربران و کسانی است که اقدام به‌عرضه و بارگذاری اطلاعات و محتوا می‌کنند. (ملکوتی، ۱۳۹۵: ۱۴۲– ۱۲۹). به‌نظر می‌رسد این قبیل از محققان با تعریف اشتباه از ماهیت عمل مدیران سایت، وظایف و قلمرو فعالیت آنها، در تحلیل مسئولیت مدنی این مدیران به خطا رفته‌اند.

مستند به مادهٔ«۲» آیین‌نامه ساماندهی و توسعه رسانه‌ها و فعالیت‌های فرهنگی دیجیتال مصوب ۱۳۸۹ هیأت وزیران، ماده«۱۹» قانون جرائم رایانه‌ای ۱۳۸۸و مادهٔ«۷۸» قانون تجارت الکترونیک ۱۳۸۲، مدیران سایت‌ها وظیفهٔ اداره، هدایت و نظارت بر کارکنان تحت امر و همچنین محتوای ارائه شده در بستر فضای سایبر را عهده دار هستند. تبصرهٔ «۱»مادهٔ«۱۹» قانون جرائم رایانه‌ای ۱۳۸۸ مقرر می‌دارد:« منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم‌گیری یا نظارت بر شخص حقوقی را دارد».ماده«۱۹» قانون فوق در زمینه مسئولیت کیفری مدیر وب‌سایت

مقرر می‌دارد: «در موارد زیر، چنانچه جرائم رایانه‌ای به‌نام شخص حقـوقی و در راسـتای منـافع آن ارتکاب یابد، شخص حقوقی دارای مسئولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به‌وقوع بپیوندد

ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثـر عـدم نظـارت وی مرتکـب جرم رایانه‌ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد».

تبصره«۲»مادهٔ فوق، مسئولیت کیفری شخص حقوقی را مانع مجـازات مرتکـب ندانسـته و در صورت نبود شرایط صدر ماده و عدم انتساب جرم به‌شخص خصوصی فقط شخص حقیقی مسـئول خواهد بود.

ماده «۷۸» قانون تجارت الکترونیک مصوب ۱۳۸۲نیـز مسـئولیت ورود خسـارت به‌اشـخاص توسط سیستم مؤسسات خصوصی و دولتی را در وهلهٔ اول متوجه مدیر مربوط می‌داند مگـر اینکـه خسارت‌های وارده ناشی از فعل شخصی افراد باشد که در این صورت جبران خسارت‌هـای برعهـده این اشخاص خواهد بود.

در تحلیل مبنای مسئولیت مدنی مدیران سایت‌ها در نقض حریم خصوصی اشخاص با نگـرش به مقدمات ذکر شده می‌توان گفت:

۱. در مواری که وب‌سایت براساس مجوزهای قانونی تأسیس شده و مـدیر وب‌سـایت مقـررات مربوط را ملتزم شده است، اصل بر عدم مسئولیت مدیر است و در صورت طرح دعاوی نقض حریم خصوصی ناشی از عدم رعایت مقررات، در صورت اثبـات تقصـیر، وفـق قواعـد عمـومی مسـئولیت مدنی[1] و حکم مادهٔ «۱» قانون مسئولیت مدنی و ماده«۹۵۳» قانون مدنی، مدیر باید خسـارت‌هـای وارده را جبران کند.

[1] وفق ماده ۷۲طرح حمایت از حریم خصوصی؛ چنانچه در نتیجه نقض حریم خصوصی، خسارت‌های مادی یا معنوی به اشخاص وارد شده باشد زیان دیده می‌تواند طبق قواعد مسئولیت مدنی جبران کلیه خسارت‌های خود را مطالبه کند. همچنین مطابق ماده ۲۱ قانون انتشار و دسترسی آزاد به اطلاعات مصوب ۱۳۸۷؛ « هر شخصی اعم از حقیقی یا حقوقی که در نتیجه انتشار اطلاعات غیر واقعی درباره او به‌منافع مادی و معنوی وی صدمه وارد شده است حق

۲. چنانچه سایت،مؤسسه یا شرکت مربوط، ماهیت حقوقی دولتی داشته باشد، هرگاه نقض حریم خصوصی اشخاص و خسارت‌های وارده ناشی از نقص وسایل و سیستم‌ها باشد وفق مادهٔ «۱۱» قانون مسئولیت مدنی مصوب ۱۳۳۹ وماده «۷۸» قانون تجارت مصوب ۱۳۸۲، برمبنای نظریه خطر، جبران خسارت زیان دیده متوجه وی خواهد بود.

۳. در فرضی که فی‌مابین مدیر وب‌سایت و کارکنان آن رابطهٔ کارگر و کارفرمایی حاکم باشد، وفق مادهٔ «۱۲» قانون مسئولیت مدنی مصوب ۱۳۳۹، و بر مبنای نظریهٔ خطر؛ کارفرمایانی که مشمول قانون کار هستند مسئول جبران خسارت‌هایی می‌باشند که از طرف کارکنان اداری و یا کارگران آنان در حین انجام کار یا به‌مناسبت آن وارد شده است مگر این‌که محرز شود تمام احتیاط‌هایی که اوضاع و احوال قضیه ایجاب می‌نموده به‌عمل آورده و یا این‌که اگر احتیاط‌های مزبور را به‌عمل می‌آوردند باز هم جلوگیری از ورود زیان مقدور نمی‌بود. کارفرما می‌تواند به وارد کننده خسارت در صورتی‌که مطابق قانون مسئول شناخته شود مراجعه نماید.

۴. در فرضی که مدیر سایت نه به‌عنوان یک شخص حقوقی، بلکه به‌عنوان یک کاربر و تولید کننده و تبادل کنندهٔ محتوا در فضای سایبر و فارغ از چارچوب ضوابط، مقررات و مجوزهای حاکم بر اداره و مدیریت سایت، با نفوذ و دسترسی غیر مجاز به اطلاعات اشخاص، مرتکب نقض حریم خصوصی اشخاص شود، همانند سایر کاربران تلقی می‌شود و دارای مسئولیت صرف است و نمی‌تواند به عدم تقصیر استناد کند.

– مسئولیت مدنی تولیدکنندگان و ارائه دهندگان محتوا و کاربران درتهدیدات سایبری مسئولیت محض است

منظور از تولید کنندگان محتوا اشخاصی هستند که محتوای مواد دیداری، شنیداری، نوشتاری و یا ترکیبی از آنها را در فضای سایبر تولید یا ارائه می‌کنند. این گروه از بازیگران سایبر می‌توانند در قالب کارمندان یک وب‌سایت یا پایگاه یا شبکهٔ تخصصی به‌تولید محتوا اقدام نمایند یا به‌عنوان دارندهٔ یک وبلاگ، عضو یک گروه یا عضو یک شبکه اجتماعی و ... علاوه بر موارد مورد اشاره این

دارد تا اطلاعات مذکور را تکذیب کند یا توضیحاتی درباره آنها ارائه دهد و مطابق با قواعد عمومی مسئولیت مدنی جبران خسارت‌های وارد شده را مطالبه نماید».

گروه می‌توانند در قالب یک کاربر همانند میلیونها نفر بهره بردار در فضای سایبر حسب مورد به‌تولید و ارائه محتوا بپردازند. منظور از کاربران فضای سایبر کسی است که با هر فناوری ارتباطی به شبکه اینترنت متصل می‌شود و حسب نیاز به بهره برداری از خدمات مختلف فضای سایبر یا تولید محتوا اقدام می‌کند.

در خصوص مبنای مسئولیت مدنی ناشی از نقض حریم خصوصی فضای سایبر توسط تولید کنندگان محتوا باید گفت که نفس دسترسی و نفوذ غیر مجاز به اطلاعات دیگران، خواه این اطلاعات در معرض افشا و بازدید کاربران دیگری قرار بگیرد یا نه، محقق مسئولیت مدنی این گروه خواهد بود و تحقق مسئولیت مدنی ایشان، مقید به‌نمایش یا تخریب اطلاعات نخواهد بود.

ماهیت نقض أمنیت داده در فضای سایبر به‌گونه‌ای است که فی‌نفسه موجب تحقق زیان می‌شود و وصرف دسترسی و نفوذ به اطلاعات دیگران حریم خصوصی اشخاص نقض شده تلقی می‌گردد، ضمن آنکه امکان به اشتراک گذاشتن این اطلاعات برای میلیونها کاربر در سراسر دنیا وجود دارد. عرف حاکم بر فضای فناوری اطلاعات و فضای سایبر نیز صرف دسترسی و نفوذ غیر مجاز به اطلاعات اشخاص را به‌مثابه زیان تلقی می‌کند. با عنایت به‌این تحلیل به‌نظر می‌رسد در خصوص مبنای مسئولیت این گروه، باید قائل به‌مسئولیت محض ارائه کنندگان محتوا در فضای سایبر بود.

در خصوص نقض حریم خصوصی اشخاص توسط کاربران نیز می‌توان استدلال نمود که هر چند هتک حریم خصوصی افراد ذاتاً موجب ضرر است، لکن در مواردی است که صرفاً نقش استفاده کننده نهایی از محتوای پردازش و بارگذاری شده توسط دیگران را دارند چه آن‌که اصل بر عدم مسئولیت مدنی کاربران فضای سایبر است. به‌عنوان‌مثال چنانچه فیلم یا اطلاعاتی از حریم خصوصی اشخاص بدون رضایت یا با مجوز صاحب اطلاعات توسط اشخاص ثالث‌بارگذاری شده و کاربر یا کاربران با مراجعه به آن لینک، موضوع زیان را مشاهده و محتوای آن را در رایانه خود تخلیه می‌کنند، باید گفت صرف‌نظر از مسئولیت مدنی‌محض ارائه کنندگان اولیه، مراجعهٔ‌کاربران به لینک‌های مختلف از اقتضاهای ذاتی فضای سایبر است و نفس حضور در فضای سایبر را نباید موجب مسئولیت مدنی به‌شمار آورد . زیرا در این فرض هیچ‌گونه تلاشی به‌منظور نفوذ و دسترسی

غیر مجاز به اطلاعات اشخاص از سوی کاربر صورت نگرفته است، ضمن آنکه اساساً حضور در فضای سایبر به‌معنی مشاهده محتوای دیگران است و نمی‌توان این دو را از نظر فنی از هم تفکیک کرد. ماده «۷۹»طرح حمایت از حریم خصوصی، عوامل زیر را موجب احراز نقض حریم خصوصی قلمداد نموده است:

۱. خصوصی یا عمومی بودن محلی که نقض حریم خصوصی در آنجا واقع شده است

۲. هدف از نقض حریم خصوصی

۳. استفاده از وسایل متعارف یا غیرمتعارف برای نقض حریم خصوصی

۴. موقعیت شخصی که به حریم خصوصی او تجاوز شده است

۵. انجام رفتار یا اقداماتی که قبل یا بعد از نقض حریم خصوصی از جانب دارنده حریم که دال بر عدول جزیی یا کلی از حریم خصوصی او باشد

۶. وجود یا عدم وجود ارتباط خویشاوندی یا سایر علقه‌هایی که عرفاً بتواند وجود زمینه قابل توجه برای نقض حریم خصوصی یک شخص را نشان دهد

مع‌الوصف در مواردی که کاربران با هر نیتی ضمن توسل به‌شیوه‌های فنی نقض حریم خصوصی و با استفاده از رارهکارهای نفوذ به‌صورت غیر مجاز اطلاعات شخصی افراد را در اختیار بگیرند و حریم آنها را نقض کنند،موجب تحقق ضرر و خسارت شده‌اند و بالتبع همانند مسئولیت تولید کنندگان محتوا مسئولیت آنها محض خواهد بود.

نتیجه‌گیری

۱. رشد چشم‌گیر و پر شتاب فضای سایبر و کاربرد گستردهٔ آن در زندگی بشری، منجر به‌بروز و ظهور اعمال مجرمانه، تخلفات و خطاهای عمدی و غیر عمدی خاص این فضا در قالب تهدیدات سایبری شده است. کاهش تبعات منفی و استفادهٔ حداکثری از تبعات مثبت فضای سایبر، مستلزم پیش‌بینی نظام‌های امنیتی، حقوقی، قضایی و انتظامی مورد نیاز فضای سایبر جهت برقراری امنیت بسترهای سخت افزاری و نرم افزاری و همچنین تأمین امنیت اطلاعات و حقوق افراد از طریق تبیین مسئولیت‌های کیفری و مدنی گروه‌ها، اشخاص و کاربران مرتبط با این فضا است.

۲. نقض امنیت داده ناشی از تهدیدات سایبری از جنس نقض حریم خصوصی اطلاعات است. اطلاعات خصوصی اشخاص در فضای سایبر با تمسک به فناوری‌های نوین، به‌روش‌های متعددی مورد تعرّض قرار می‌گیرد.

۳. نقض امنیت داده‌های اشخاص در فضای سایبر توسط اشخاص حقیقی و حقوقی مرتبط با این فضا صورت می‌پذیرد. هرچند مبانی و منابع تحقق مسئولیت مدنی در دنیای واقعی و سایبر مشترک است، مع‌الوصف نظر به مقتضیات و تفاوت ماهیتی این دو حوزه، نمی‌توان قائل به مبنای واحد و منفرد مسئولیت مدنی در ارتباط با همه واسطه‌ها و گروه‌های فعال در فضای سایبر بود. فلذا با توجه به ماهیت حقوقی این گروه‌ها و حسب شرایط و مقتضیات تحقق وقوع جرم و نقض حریم خصوصی به‌عنوان عمل زیان‌آور، وفق قواعد و اصول کلی مسئولیت مدنی، هریک از این گروه‌ها حسب مورد منفرداً یا متضامناً براساس نظریهٔ تقصیر یا مسئولیت محض(خطر)مسئول تلقی می‌شوند.

منابع و مآخذ

۱. آماده، مهدی، (۱۳۹۲)، حمایت از حریم خصوصی، تهران: نشر دادگستر،چاپ اوّل.

۲. ابو الحسین، احمد بن فارس بن زکریا، (۱۴۰۴ ه ق)، معجم مقائیس اللغۀ، ج۲، قم: انتشارات دفتر تبلیغات اسلامی حوزه علمیه قم، چاپ اول.

۳. احمدلو ، مونا، (۱۳۹۲)، حریم خصوصی در فقه و حقوق ایران، تهران: مجد، چاپ اول.

۴. اصلانی،حمید رضا، (۱۳۸۴)،حقوق فناوری اطلاعات،تهران: نشر میزان، چاپ اول.

۵. افشار،حسن،(۱۳۹۴)،مسئولیت مدنی جبران خسارات معنوی در حقوق ایران.

۶. انصاری، باقر و هیات مولف، (بی‌تا)، مسئولیت مدنی رسانه‌های همگانی– معاونت پژوهش، تدوین و تنقیح قوانین ومقررات،چاپ اول.

۷. پاکزاد، بتول، (بی‌تا) ماهیت تروریسم سایبری، مجلۀ تحقیقات حقوقی، ویژه نامه شماره ۴,

۸. حسن پور, مسلم، (۱۳۹۲)، تحلیل بدافزار، اولین همایش ملی رویکردهای نوین در مهندسی کامپیوتر و بازیابی اطلاعات، رودسر، دانشگاه آزاد اسلامی واحد رودسر و املش، .html۲۵۹_۰۱-BPJ۰۱http://www.civilica.com/Paper-BPJ

۹. حسنی ،علی رضا و سید رضا هاشمی، (۱۳۸۹)، رسانه‌ها و مسئولیت مدنی،: نشریه قضاوت، شماره ,۶۶

۱۰. خلیل زاده، مونا، فضای سایبر و حقوق بشر، مروری بر صورت مسئله: .http://www.ihrc.ir

۱۱. خلیل زاده، مونا، (۱۳۹۳)، مسئولیت بین‌المللی دولت‌ها در قبال حملات سایبری، تهران: انتشارات مجد.

۱۲. رجبی اکرم، (۱۳۹۱)، نقض حریم خصوصی در فضای سایبر، تهران: آرمان رشد،چاپ اول.

۱۳. زرکلام، ستار، (۱۳۸۶)، حریم خصوصی ارتباطات اینترنتی (مطالعه در حقوق ایران و اتحادیه اروپا) پژوهش نامه حقوق اسلامی » بهار و تابستان، شماره ۲۵ (از صفحه ۱۷۳ تا ۱۹۶).

۱۴. صادقی، حسین ، (۱۳۸۸)، مسئولیّت مدنی در ارتباطات الکترونیک، تهران: نشر میزان.

۱۵. صادقی،حسین، (۱۳۸۹) مسئولیت مدنی واسطه ها و تأمین کنندگان خدمات ارتباطات الکترونیک فصلنامه حقوق، مجلهٔ دانشکده علوم سیاسی،دوره ۴۰ ،شمارهٔ۲،:۲۱۸-۱۹۹,

۱۶. صاحب بن عباد، (۱۴۱۴ هـق)، کافی الکفاه، اسماعیل بن عباد، المحیط فی اللغه، عالم الکتاب، بیروت.

۱۷. صفایی، سیدحسین و حبیب‌اله رحیمی، (۱۳۹۱)، مسئولیت مدنی، تهران: نشر سمت.

۱۸. صلاحی سهراب و سیدمهدی کشفی (۱۳۹۵)،جنگ سایبری از منظر حقوق بین‌الملل با نگاه به دستورالعمل تالین–دو فصلنامهٔ علمی –پژوهشی مطالعات قدرت نرم، سال ششم،شماره چهاردهم: ۲۸–۴۸

۱۹. عاشوری، مهدی، (۱۳۸۹)، تعارض قوانین در مسئولیت خارج از قرارداد(مطالعهٔ تطبیقی در حقوق ایران و فرانسه)، تهران: نشر دانشگاه امام صادق(ع).

۲۰. عمید، حسن فرهنگ عمید، (بی‌تا)، چاپ یازدهم، تهران: انتشارات جاویدان.

۲۱. قاسم زاده، سید مرتضی، (۱۳۸۳)، مبانی مسئولیت مدنی، تهران: نشر میزان.

۲۲. کاتوزیان، ناصر، (۱۳۷۴)، حقوق مدنی، الزام‌های خارج از قرارداد(ضمان قهری)، تهران: انتشارات دانشگاه تهران،چاپ اول.

۲۳. محمدی، ابوالحسن، (۱۳۷۳)، قواعد فقه، تهران: نشر یلدا.

۲۴. معین آبادی، رضا، (۱۳۸۳) رسانه ها و حریم خصوصی افراد، شیوه‌های حمایت از حریم خصوصی در حقوق ایران و کشورهای آلمان، اسپانیا، فرانسه، ایتالیا، انگلیس و فرانسه– علوم اجتماعی: پژوهش‌های ارتباطی، شماره های ۳۹ و ۴۰.

۲۵. ملکوتی، رسول و پرویز ساورایی، (۱۳۹۵)،درآمدی بر مسئولیت مدنی در فضای سایبر،نشریهٔ پژوهش حقوق خصوصی ، شماره ۱۵ : ۱۴۲–۱۲۹،قابل دسترسی در:http://www.noormags.ir/view/fa/articlepage.

۲۶. هیتر هریسون، دنیس (۱۳۹۴)، جنگ سایبری و حقوق جنگ، مترجم سازمان پدافند غیر عامل کشور،ناشر موسسه انتشاراتی جهان جام.

قوانین و آیین نامه ها

۱. آیین‌نامه واحدهای ارائه کننده خدمات اطلاع رسانی و اینترنت رسا (ISP) مصوب ۱۳۸۰شورای عالی انقلاب فرهنگی.

۲. آیین‌نامه دفاتر خدمات حضوری اینترنت مصوب ۱۳۸۰شورای عالی انقلاب فرهنگی.

۳. سند راهبردی پدافند سایبری کشور مصوب ۱۳۹۴/۰۳/۲۱ کمیتهٔ دائمی پدافند غیر عامل کشور.

سیاست‌های کلی نظام در بخش شبکه‌های اطلاع رسانی رایانه‌ای ابلاغی۱۳۷۷ مقام معظم رهبری.

۴. قانون آیین دادرسی مدنی مصوب ,۱۳۷۹

۵. قانون آیین دادرسی کیفری مصوب ,۱۳۹۲

۶. قانون اساسی مصوب۱۳۵۸با رعایت اصلاحات سال۱۳۶۸شورای بازنگری قانون اساسی.

۷. قانون تجارت الکترونیکی مصوب ۱۳۸۲,/۱۰/۱۷

۸. قانون جرائم رایانه‌ای مصوب ۱۳۸۸,/۳/۵

۹. قانون مجازات اسلامی مصوب ۱۳۹۲.

۱۰. قانون مدنی مصوب۱۳۱۴/۰۱/۲۰.

۱۱. قانون مسئولیّت مدنی مصوب ۱۳۳۹/۰۳/۲۲.

۱۲. طرح حمایت از حریم خصوصی که در تاریخ ۰۷/ ۱۳۸۵/۰۴ اعلام وصول شده است.