فصلنامه علمی پژوهشی مطالعات بین‌رشته‌ای دانش راهبردی
سال هفتم، شماره ۲۷، ۱۳۹۶، صفحه ۱۹۸-۱۶۷

تبیین مسئولیت‌های ارائه‌دهندگان خدمات اینترنتی از منظر حقوقی

محمدرضا حسینی[۱]، رحیم یزدانی[۲]

تاریخ دریافت: ۹۵/۰۵/۲۵ تاریخ پذیرش: ۹۵/۰۸/۲۵

چکیده

امروزه افراد برای انجام کارهای مختلف نیاز به اتصال خط اینترنت دارند. لکن برخی افراد از اینترنت به عنوان راهی برای انجام فعالیت‌های غیرقانونی استفاده می‌کنند. از آنجا که ارائه‌دهندگان خدمات اینترنتی (ISP) بایستی بخشی از زنجیره مسئولیت‌پذیری هستند پرسش اصلی این تحقیق آن است که آیا ارائه‌دهندگان خدمات اینترنتی در قبال عملکرد مشتریان خود مسئولیت دارند، و اگر دارند مسئولیت آن‌ها چه دامنه‌ای دارد؟

در این پژوهش ابتدا مسئولیت‌های مورد انتظار در ابعاد مختلف بررسی‌شده و در ادامه نظریه‌های متناظر با اعمال مسئولیت و درنهایت رویکردها مورد بحث قرار می‌گیرند. به‌منظور تعیین شاخص‌های مسئولیت، با ابزار پرسشنامه‌ای و با استفاده از نرم‌افزارهای Smart PLS و SPSS، برازش مدل تحقیق و رتبه‌بندی ابعاد انجام گرفت. نتیجه به‌دست‌آمده نشان داد که ارائه‌دهندگان خدمات اینترنتی در زمینه‌ی اطلاع‌رسانی و آموزش صرفا مسئولیت نیابتی، اما در زمینه حفظ حریم خصوصی و نظارت، مسئولیت نیابتی و مشارکتی دارند درحالی‌که در زمینه خدمات‌رسانی و موضوعات فنی، مسئولیت کارفرمائی دارند؛ همچنین نتیجه این پژوهش نشان داد که در خدمات‌رسانی، موضوعات فنی، نظارت و حفظ حریم خصوصی، بایستی ارائه‌دهندگان خدمات اینترنتی بایستی رویکرد فعال پیشگیرانه را تعقیب نمایند.

کلیدواژه‌ها: ارائه‌دهندگان خدمات اینترنتی، مسئولیت.

۱ استادیار و عضو هیئت‌علمی دانشگاه عالی دفاع ملی، نویسنده مسئول: rezahsn88@gmail.ir
۲ دانشجوی دکتری، دانشگاه عالی دفاع ملی

مقدمه

ارائه‌دهندگان خدمات اینترنتی (ISP) طراح، برنامه‌ریز منابع، اتصال‌دهنده قابل‌اعتماد و هدایت‌کننده ترافیک و خدمات هستند (هس وی وسواج،۲۰۱۲: ۳). آن‌ها وقتی در نقش تأمین ترافیک هستند بایستی خدمات و پشتیبانی ۲۴ ساعته داشته باشند تا رضایت مشتری جلب شود. برخی از ارائه‌دهندگان خدمات اینترنتی، سرورهای نام دامنه[1] را به‌صورت محلی در اختیاردارند که برای ارائه اینترنتی صوتی[2] یک عملکرد کلیدی است. وقتی یک کاربر می‌خواهد از طریق این خدمت، تماس صوتی برقرار نماید ، ماشین کاربر با سرور نام دامنه تماس می‌گیرد تا آدرس پروتکل اینترنتی طرف مقابل گرفته شود. لذا اگر حافظه سرور تسخیرشده باشد تماس تلفنی به شخص دیگری هدایت شود و اطلاعات شخصی و محرمانه کاربر مورد سوءاستفاده قرار گیرد. موارد متعددی از بهره‌گیری این آسیب‌پذیری‌ها گزارش‌شده است (هس وی وسواج،۲۰۱۲ :۹). بایستی ارائه‌دهنده این خدمت با امن سازی فنی، مانع تسخیر حافظه سرور شود تا تماس تلفنی به‌جای دیگری هدایت نشود. همچنین حفظ حقوق مؤلفین و حمایت از داده کاربران و حریم خصوصی توسط ارائه‌دهندگان خدمات اینترنتی موضوع قابل‌توجهی است. فرضیه تحقیق چنین است «با توجه به این‌که ارائه‌دهندگان خدمات اینترنتی در موقعیت مناسبی برای انجام کارهای نظارتی در اینترنت هستند و از فن‌آوری‌ها پیشرفته برای شناسایی فعالیت‌های غیرقانونی می‌توانند استفاده کنند لذا مسئولیت‌هایی در ابعاد نظارتی و آموزش دارند». مسئولیت‌پذیری منجر به استانداردهایی جهت ارتقای خدمات‌رسانی، حفاظت از داده‌های باارزش، کاهش جرائم اینترنتی، کاهش فعالیت‌های مجرمانه، افزایش آرامش اجتماعی، رعایت هنجارها، رعایت حقوق مؤلفین، رعایت حریم خصوصی، ارتقای دانش کاربران جهت مقابله با تهدیدات، پایدارسازی زیرساخت ارتباطی و... خواهد شد.

لذا این تحقیق به‌منظور «تعیین دامنه مسئولیت ارائه‌کنندگان خدمات اینترنتی در ابعاد مختلف و رویکردهای حقوقی که می‌توانند داشته باشند وبر نظریه‌ها و مسئولیت‌ها تأثیر داشته باشند»، انجام می‌گیرد. بر این اساس مهم‌ترین هدف این مطالعه تبیین مسئولیت‌های ارائه‌کنندگان خدمات اینترنتی بوده و برای رسیدن به هدف اصلی، بایستی ابتدا به اهداف فرعی زیر رسید:

– تعیین تکالیف ارائه‌کنندگان خدمات اینترنتی در زمینه‌ی نظارتی، خدماتی، فنی، آموزشی و حریم خصوصی

1- Domain Name Server
2- Voice Over Internet Protocol

- تعیین تناظر نظریه‌های مسئولیت‌پذیری با اعمال مسئولیت‌ها

- تعیین رویکردهای اتخاذی لازم در اعمال مسئولیت‌ها

حال سؤالاتی که در این راستا مطرح می‌شوند عبارت‌اند از: آیا ارائه‌دهندگان خدمات اینترنتی در قبال اعمال خود مسئول پذیر هستند؟ آیا مسئولیت ارائه‌دهندگان خدمات اینترنتی نظارتی است؟ آیا مسئولیت ارائه‌دهندگان خدمات اینترنتی خدماتی است؟ آیا مسئولیت ارائه‌دهندگان خدمات اینترنتی فنی است؟ آیا مسئولیت ارائه‌دهندگان خدمات اینترنتی حفظ حریم خصوصی و داده‌های شخصی و حقوق مؤلفین است؟ آیا مسئولیت ارائه‌دهندگان خدمات اینترنتی اطلاع‌رسانی و آگاهی دهی است؟ نظریه‌های متناظر با اعمال مسئولیت‌ها کدام‌اند؟ ارائه‌دهندگان خدمات اینترنتی چه رویکردهایی می‌توانند در پیش بگیرند؟

مبانی نظری

مباحث مسئولیت مدنی مرتبط با ارتباطات اینترنتی ازجمله نقض حریم خصوصی، نقض حقوق مؤلفین، تولید و انتشار ویروس‌های رایانه‌ای ، هتک حرمت اشخاص از مهم‌ترین مباحث حقوق فناوری اطلاعات و ارتباطات بوده و موجب مسئولیت مدنی می‌باشد(جنتی و رستمی، ۱۳۹۱: ۱). منظور از مسئولیت مدنی، آن است که چنانچه در نتیجه فعل هریک از اشخاص مختلفی که با مقاصد متفاوت با خدمات اینترنتی سروکار دارند به حقوق یا منافع دیگری خسارت وارد شود، چه اشخاصی و با چه مبنایی و چگونه باید به جبران خسارت ملزم شوند(انصاری، ۱۳۸۲: ۱۱). مسئولیت مدنی، رابطه مستقیمی با جایگاه و نقش واسطه و ارائه‌دهنده خدمات دارد(خوشدل، ۱۳۹۴: ۱).علاوه بر هکرها، ارائه‌دهندگان خدمات اینترنتی و سازندگان وب سایت‌ها بیش از سایرین مرتکب نقض حقوق مؤلف در اینترنت می‌شوند که از آن جمله می‌توان به حق ممانعت دیگران از تولید مجدد یا کپی کردن یک اثر، نمایش یک اثر به عموم یا توزیع و تکثیر آثار اشاره کرد اشاره کرد(بولین، ۲۰۱۵: ۱). نتیجه تحقیق نشان می‌دهد برای اثبات مسئولیت غیر قراردادی ارائه‌دهندگان خدمات اینترنتی درجایی که خود به انجام اعمال زیان‌بار مبادرت می‌ورزند باید تقصیر آن‌ها را لحاظ کرد(ابهری و میری،۱۳۹۰ :۱۹). با این‌حال به خاطر باور به عدم توانایی ارائه‌دهندگان خدمات اینترنتی برای پایش هر آنچه در اینترنت رخ می‌دهد، به‌منظور یافتن اعمال زیان‌بار و غیرقانونی و توقع ناروا از آن‌ها در این باره، قوانین برخی از کشورها نظام عدم مسئولیت را نوآوری کرده‌اند این نظام‌ها این امکان را برای

آن‌ها فراهم کرده‌اند که با پیروی از شرایط مقرر، از مسئولیت در برابر زیان‌های حاصل توسط کاربران بگریزند. در نظام حقوقی ایران با توجه به‌قاعده کلی مندرج در قانون مسئولیت مدنی باید تقصیر مبنای مسئولیت باشد. همچنین در تحقیقی دیگر آمده است رویکرد کلی در دکترین حقوقی و رویه قضایی در بیشتر نظام‌های حقوقی درباره خسارات ناشی از افعال کاربران مبتنی بر تقصیر است و در مواردی که صرفاً نقش تأمین‌کننده دسترسی یا خدمات میزبانی و یا حمل‌کننده و مجرای انتقال داده را عهده‌دار هستند، وظیفه کنترل و نظارت بر افعال کاربران و مشترکان را نداشته و مسئولیتی از جهت افعال زیان‌بار کاربران نظیر نقض حقوق مؤلف و هتک حرمت دیگران متوجه آنان نیست مگر درصورتی‌که واجد علم واقعی بوده و حسب مورد به‌محض حصول اطلاع، اقدام به حذف محتوای غیرقانونی یا مسدود نمودن دسترسی به آن ننماید(صادقی،۱۳۸۹ :۲۱۷). در قوانین آمریکا و آلمان و استرالیا مقررات اصلی درباره موارد و شرایط عدم مسئولیت واسطه‌ها و وظیفه آن‌ها در مورد حذف محتوای غیرقانونی و شرایط شکلی و ماهوی و ضمانت اجرای این وظیفه پیش‌بینی‌شده است (صادقی،۱۳۸۹: ۲۱۶). در نظام حقوقی ما مصونیت‌های قانونی برای واسطه به نحو صریح پیش‌بینی‌نشده است و صرفا در قانون تجارت الکترونیک یک استثنای عام و مجمل در مورد مسئولیت مدنی ناشی از نقض حقوق مؤلف پیش‌بینی‌شده است، لذا ضرورت دارد موارد عدم مسئولیت واسطه‌ها و شرایط و نحوه حذف یا مسدود نمودن دسترسی به محتوای غیرقانونی را در قوانین پیش‌بینی کرد.

هم چنان‌که ملاحظه شد، در پژوهش‌های انجام‌گرفته، بیشتر به موضوعات نقض حریم خصوصی، نقض حقوق مؤلفین، محتوای غیرقانونی، محتوای مخرب، خسارات ناشی از افعال کاربران پرداخته شده است لکن به مسئولیت‌های فناورانه، آموزشی، گزارش دهی، همکاری با مراجع دیگر در صورت کشف خطر، پرداخته نشده است. همین موضوعات وجه افتراق این پژوهش با پیشینه است.

تعریف مسئولیت ارائه‌دهندگان خدمات اینترنتی

به‌منظور انتساب مسئولیت بایستی سه شرط زیر برقرار باشد:

– **ارتکاب فعل زیان‌بار** (فعل زیان‌بار فعلی است مغایر قانون و قابل انتساب به مرتکب که موجب خدشه حیثیت، اعتبار، شهرت حرفه‌ای و خسارت مادی و معنوی گردد که می‌تواند عامدا یا در اثر بی‌احتیاطی در اثر ذخیره، پردازش و توزیع داده باشد)

- **وجود ضرر** (شامل زیان مادی (از بین رفتن اعیان – کاهش ارزش اموال – از بین رفتن منفعت و حق مشروع – صدمه جسمانی) و زیان معنوی (صدمه به حیثیت، اعتبار و شهرت))

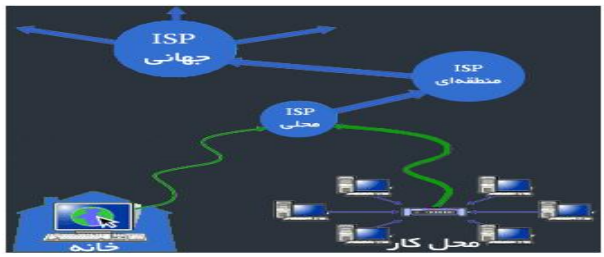
-رابطه سببیت بین فعل و ضرر واردشده(کاتوزیان،۱۳۷۸ :۲۷)

ممکن است ارائه‌دهندگان خدمات اینترنتی، خود سبب ورود زیان به دیگری شوند؛ مانند ایجاد و ارائه محتوایی که باعث تخلف و ضرر گردد همچنان که هر شخص مسئول اعمال خویش است، ارائه‌دهندگان خدمات اینترنتی نیز پاسخگوی خساراتی خواهند بود که خود آن را ایجاد کرده‌اند. و یا ممکن است تخلف و ضرر از طریق ارائه‌دهندگان خدمات اینترنتی باشد؛ که در این حالت بررسی مسئولیت از اهمیت زیادی برخوردار هست. گونه دیگری از مسئولیت، مسئولیت ناشی از مفاد قرارداد ارائه خدمات بین ارائه‌دهندگان خدمات اینترنتی و مشترک است. اثبات وجود قرارداد جهت احراز ارکان مسئولیت قراردادی در فضای اینترنت در همه حال آسان نخواهد بود.

مسئولیت ارائه‌دهندگان خدمات اینترنتی شامل دو گونه «مسئولیت قراردادی» و »مسئولیت بیرون از قرارداد» است(ابهری و میری، ۱۳۹۱: ۷). همچنان که هر شخص مسئول اعمال خویش است، ارائه‌کننده خدمات اینترنتی نیز پاسخگوی خساراتی خواهد بود که خود آن را از طریق ارائه یا ایجاد محتوا، سبب شده است.علاوه بر این، در ارتباط اینترنتی، غیر از آغازگر ارتباط و دریافت-کننده، شخص سومی به نام ارائه‌دهنده خدمات اینترنتی برای قراری ارتباط نقش ایفا می‌کند و در بیشتر خساراتی که در اینترنت رخ می‌دهد، نقش گذرگاهی برای اطلاعات کاربران دارند و لذا در قبال کار زیان‌بار دیگری مسئولیت دارد. این قسم از مسئولیت‌ها، متناظر با مسئولیت بیرون از قرارداد است. اما نوع دیگری از مسئولیت، مسئولیت قراردادی ارائه‌دهندگان خدمات اینترنتی است که متناظر با نقض مفاد قرارداد بین مشترک و ارائه‌دهنده خدمات هم جهت اتصال به اینترنت و هم خدمات پس از اتصال است، که از آن جمله می‌توان به خودداری از خدمات، ارائه خدمات همراه با نقص، حذف یا غیرقابل‌دسترس کردن اطلاعات مشترک، ارائه پهنای باند کمتر و... اشاره کرد.پیدایش این‌گونه مسئولیت در دو حالت رخ می‌دهد: در حالتی که ارائه‌دهنده خدمات از ارائه خدمات خودداری کندو یا در خدمات او نقصی موجود باشد.

مفهوم ارائه‌دهندگان خدمات اینترنتی[1]

اینترنت از پیوند تعداد بی‌شماری شبکه‌های ارتباطی کامپیوتری کوچک و بزرگ که حاوی اطلاعات متنوع هست تشکیل می‌شود (وب‌سایت سازمان فناوری اطلاعات ایران،۱۳۹۴). یک فرد متصل به اینترنت تنها مشاهده‌گر و مرورگر اینترنت نیست بلکه جزئی از این شبکه بوده و می‌تواند با آن تبادل اطلاعات نماید. مراکز ارائه‌دهندگان خدمات اینترنتی اتصال به شبکه اطلاع‌رسانی و اینترنت را فراهم می‌آورد و جزء ضروری دسترسی و اتصال افراد به شبکه اینترنت هست. این مراکز با ارائه نرم‌افزارهای لازم (در صورت ضرورت)، یک رمز عبور حفاظت‌شده و یک شماره تلفن برای تماس با شبکه، امکان استفاده از اینترنت و مبادله نامه‌های الکترونیکی را در اختیار متقاضیان قرار می‌دهند. با توجه به رشد چشمگیر اینترنت در جامعه امروز، این مراکز خود را مسئول می‌دانند که در مقابل تقاضای بی‌شمار کاربران، بتوانند بهترین خدمات را داشته باشند. شاخص‌های انتخاب یک مرکز امنیت، سرویس‌ها، قیمت، اعتماد، سرعت اتصال، پشتیبانی کاربران، کیفیت ارائه خدمات، امکانات و تجهیزات فنی هستند. ارائه‌دهندگان خدمات اینترنتی از طریق نقاط دسترس شبکه به هم وصل می‌شوند که در ستون فقرات اینترنت وجود دارد. این مراکز را می‌توان به سه نوع محلی، منطقه‌ای وجهانی تقسیم کرد. سلسله‌مراتب دسترسی به اینترنت در شکل ۱ زیر آمده است.



شکل ۱. اتصال سلسله‌مراتبی به اینترنت

به طور کلی ارائه‌دهندگان خدمات اینترنتی، نهادهای خصوصی یا دولتی هستند که با استفاده از امکانات سیمی کم‌سرعت، پرسرعت هم‌زمان داده و صوت از طریق اتصال بی‌سیم، ماهواره و...، خدمات متعددی نظیر دسترسی به اینترنت، ثبت دامنه، میزبانی وبلاگ، موتورهای جستجو،

1 Internet Service Provider(ISP)

واسطه‌های تجارت الکترونیک، زمینه‌ساز شبکه مشارکتی، پست الکترونیکی، تلفن‌های اینترنتی و پشتیبان گیری را در اختیار متقاضیان قرار می‌دهند.

گونه‌ها و اقسام مسئولیت‌ها

مسئولیت تأمین ترافیک و خدمات قابل‌اعتماد

شبکه جهانی اینترنت ابزار ارتباطی ضروری و پایه اصلی برای دسترسی عموم است. در رهنمودهای سازمان همکاری و توسعه اقتصادی (OECD) و آژانس دیجیتال اروپا و اتحادیه بین‌المللی مخابرات (ITU) این امر تصریح شده است که اینترنت معتبر و در دسترس عموم بایستی ارائه شود (هس وی وسواج،۲۰۱۲ : ۵). در کشورهای مختلف برنامه‌ریزی برای دسترسی افراد به پهنای قابل‌توجهی از اینترنت صورت می‌گیرد. در فنلاند قانونی تصویب‌شده که هر شخص حق دسترسی۱ مگابیت بر ثانیه‌ای به اتصال پهن باند دارد. در انگلیس به ۲ مگابیت بر ثانیه تأکید شده است (هس وی وسواج،۲۰۱۲ : ۵). در ۱۹۹۷ سازمان تجارت جهانی موافقت‌نامه ارتباط راه دور را تدوین کرد تا موانع خدمات بین‌المللی سهل‌الوصول را برطرف کند و اجازه داد نهادهای خارجی مالکیت امکانات ارائه‌دهنده خدمات صوت و داده را عهده‌دار شوند؛ که شامل تلفن صوتی، انتقال داده، تلکس، تلگراف، فاکس، خدمات اجاره‌ای اختصاصی، خدمات ثابت و سیار سامانه‌های ماهواره‌ای، خدمات تلفن سیار، خدمات داده موبایل، پیج و سامانه‌های ارتباطی شخصی هست. در اکثر کشورها زیرساخت‌های حیاتی و بسیاری از امورات روزمره، مبتنی بر اینترنت است لذا نیاز ضروری است به دسترسی همیشگی و با پهنای مناسب به اینترنت که بایستی ارائه‌دهندگان خدمات اینترنتی ارائه کنند (هس وی وسواج،۲۰۱۲ : ۶).

مسئولیت رعایت حق مؤلف

برخی از محتویات اینترنت توسط حق مؤلف حمایت می‌شوند که هدف، جلوگیری از تکثیر نسخه اصلی فیلم‌ها، تصاویر، گرافیک وب‌سایت‌ها، موزیک و متن است. البته ممکن است محتوا برای اهداف تحقیقی، نقد، خبررسانی، طنز، مشاوره‌های حرفه‌ای مورداستفاده قرار گیرد ولی بایستی عدالت را در نظر بگیرد به‌عنوان‌مثال در قوانین استرالیا نباید از ۱۰ درصد کل محتوا تجاوز کند. یکی از مهم‌ترین موضوعات حق مؤلف در فضای سایبر، به اشتراک‌گذاری موزیک و فیلم و بازی‌ها در بین کاربران شبکه‌هاست. قسمت‌هایی از فایل‌ها موضوع کپی‌رایت‌اند و تفکیک آن‌ها

توسط نرم‌افزار سخت است که در این ارتباط رعایت قوانین و مقررات موضوعه می‌تواند راهگشا باشد.

مسئولیت کنترل محتوا و حفظ حریم خصوصی

کنترل محتوا، نظارت عملی برای کنترل یا سانسور اطلاعات است. طبق قانون، ارائه‌دهندگان خدمات اینترنتی، بایستی از تولید، ارائه، تأمین، توزیع، تهیه یا مالکیت موضوعاتی مانند هرزه‌نگاری، نژادپرستی و... توسط ممانعت کنند. در قوانین کشورمان بر این موضوع تأکید شده است. همچنین در مقررات ارائه‌دهندگان خدمات اینترنتی و فصل سوم قانون تجارت الکترونیکی ایران، داده‌های شخصی حمایت‌شده است (ذخیره، پردازش و توزیع داده‌های شخصی که مبین ریشه‌های قومی، دیدگاه‌های عقیدتی، خصوصیات اخلاقی، وضعیت جسمانی و... باشد غیرقانونی است). دربند ۵-۳-۱۰ قانون رسا[1]، آمده است که ارائه‌دهندگان خدمات اینترنتی باید تمهیدات فنی لازم برای حفظ حقوق و حمایت از داده کاربران را فراهم آورد و هرگونه دسترسی غیرقانونی رسا به حریم اطلاعات خصوصی ممنوع است؛ و همچنین دربند ۶-۱۹ قانون موصوف آمده است که نفوذ غیرمجاز به مراکز دارنده اطلاعات خصوصی و محرمانه و تلاش برای شکستن قفل رمز سیستم‌ها و شنود بسته‌های در حال گذر در شبکه ممنوع است (نوری و نخجوانی،۱۳۸۳ :۱۶).

مسئولیت مربوط به سایت‌های شبکه‌های اجتماعی

در شبکه‌های ارتباطی و اجتماعی، افراد عضو می‌توانند گروه‌های خاصی ایجاد کنند. در این شبکه‌ها که آمارشان فزاینده است، داده‌های شخصی افراد به‌منظور تولید پروفایل، درخواست می‌شود. این شبکه‌های اجتماعی می‌توانند، فهرستی از تماس‌های هر کاربر و تراکنش‌های انجام‌گرفته با دیگر کاربران را در دسترس داشته باشند. ارائه‌کنندگان خدمات اینترنتی که میزبان سایت‌های شبکه‌های اجتماعی هستند، بایستی امنیت را در سطح بالا تأمین کنند و مانع افشای داده‌های افراد به اشخاص ثالث شوند (هات تاپیک، ۲۰۰۹ :۱۱).

[1] – قانون ارائه‌کنندگان خدمات اینترنتی (رسا)

مسئولیت گزارش‌دهی آمارهای حوادث و آموزش‌دهی تهدیدات

ارائه‌دهندگان خدمات اینترنتی وظیفه‌دارند گزارش‌های مربوط به تکرار، شدت، منابع، اهداف حملات و ارائه راه‌حل‌های اصلاحی را به کاربران گزارش دهند. در سال ۲۰۰۶ دو مقاله منتشر شد که پایه‌ای برای نشان دادن چگونگی پاسخ‌دهی دقیق به پرس‌وجوهای پایگاه داده آماری همراه با حداقل سازی احتمال افشای اطلاعات شخصی می‌باشند برای این کار، مفهوم جدید حریم خصوصی تفاضلی[1] با پرس‌وجوهای استفاده‌کننده از اعداد تصادفی مطرح‌شده است (اسمیث،۲۰۰۶ :۲۸۲). اگر ارائه‌دهندگان خدمات اینترنتی وظیفه گزارش دهی از وقایع نامتعارف امنیتی را به عموم مشتریان انجام دهند این امر به تدریج منجر به ظهور یک استانداردهای جهانی می‌شود. برای مثال؛ ارائه‌دهندگان خدمات اینترنتی در استرالیا پذیرفته‌اند که ۴ خدمت زیر را انجام دهند :

الف)نصب سیستم مدیریت و اخطار – ب)تخصیص منابع اطلاعاتی استاندارد برای کاربران – ج)دسترسی ارائه‌دهندگان خدمات اینترنتی‌ها به آخرین اطلاعات تهدیدات – د)گزارش دهی به مرکز واکنش سریع حوادث رایانه‌ای[2] جهت بررسی وضعیت تهدیدات این مدل استرالیا را خیلی از کشورها پذیرفته و اجرا می‌کنند.

وظیفه آگاه‌سازی و همکاری ارائه‌دهندگان اینترنتی در صورت وجود خطر

در آمریکا در صورت درخواست دولت برای شناسایی و متوقف ساختن برخی حملات سایبری مانند انکار خدمات، ارائه‌دهندگان خدمات اینترنتی بایستی ضمن انعکاس حملات به دولت، با یکدیگر همکاری کنند. همچنین در آلمان مرکز مبارزه با نرم‌افزارهای مخرب، توسط گروهی از ارائه‌دهندگان خدمات اینترنتی پشتیبانی می‌شود تا مشتریان آسیب‌دیده را مطلع کرده و با کمک همدیگر، اثرات آسیب را کاهش دهند. طبق قوانین اروپا، عدم همکاری ارائه‌دهندگان خدمات اینترنتی و عدم ارائه سرویس به مراکزی مانند مرکز عملیات شبکه‌ای[3] و گروه‌های واکنش حوادث

1- Differential Privacy
2- Computer Emergency Response Team
3- Network Operation Center

امنیتی[1] و اپراتورهای مبادلات اینترنتی، کارکنان امنیت سایبر، مرکز واکنش سریع و حکومت، جرم شناخته می‌شود. (بناک،۱۹۹۷ :۱)

مسئولیت تأمین مسیر و تحلیل نام معتبر

مسیریابی بین دو مرکز ارائه‌دهندگان خدمات اینترنتی، ابتدا از طریق استاندارد پروتکل دروازه مرزی[2] صورت می‌گیرد. مطابق با این استاندارد، هر مرکز مقاصد ممکنه بسته و مسیرهایی که بسته به آن مقاصد خواهد رفت را اعلام می‌کند. این اعلام به مراکز همسایه و نهایتا به همه مسیریاب‌های اینترنت پخش می‌شود (باتلر و همکاران،۲۰۱۰ :۱۱۹). شنود ترافیک در محل مسیریاب به دلیل ضعف پروتکل فوق امکان‌پذیر است. موارد متعددی از بهره‌گیری این آسیب‌پذیری‌ها گزارش‌شده است (مک کولاق،۲۰۰۸ :۱).

تنها راه برای حل این مشکل، توسعه و مدیریت سامانه‌ای است که اجازه می‌دهد در هر گام از فرایند، امضا و گواهی صورت گیرد. مسیریاب‌ها بایستی قادر به تصدیق با بالاترین اطمینان باشند به‌طوری‌که اعلام‌های مسیریابی در حین گذر قابل اصلاح نباشد و همچنین بایستی فرستنده برای چنین اعلامی، مجاز باشد. با این‌که در برخی کارهای تحقیقی، پروتکل دروازه مرزی امن[3] با امنیت بالا پیشنهاد شده، ولی به خاطر تلقی از زمان‌بر بودن محاسبات این روش، به میزان کمی، گسترش و امکان‌پذیر شده است و همچنین نیاز به زیرساخت کلید عمومی[4] دارد. ثابت شده است که مراکز خدمات رسان اینترنتی بزرگ با استفاده از پروتکل مذکور و داشتن امکان تصدیق امضا سوددهی دارند (چپیرا و همکاران،۲۰۱۱ :۱۸). لذا این چارچوب اگر توسط مراکز بزرگ خدمات رسان اینترنتی پذیرش شود برای مدت طولانی خدمات اینترنتی امن و قابل‌اعتماد خواهیم داشت. رگلاتورها در سراسر دنیا بحث پذیرش پروسه‌های مسیریابی امن را با صنایع شروع کرده‌اند.

علاوه بر تأمین پروسه مسیریابی امن، تحلیل نام دامنه معتبر نیز مقوله مهمی است. در اینترنت سرور نام دامنه، شبیه دفترچه راهنمای تلفن برای اینترنت است. برخی از ارائه‌دهندگان خدمات اینترنتی، سرورهای نام دامنه را به‌صورت محلی در اختیار دارند. اگر کاربری درخواست ترجمه

1- Security Incident Response Team
2- Boarder Gate Protocol
3- Secure Boarder Gate Protocol
4- Public Key Infrastucture

آدرس داشت و در سرور محلی نبود، آن را از سرورهای ریشه[1] از طریق درخواست و جواب‌هایی که امکان جعل (شانس حمله)دارند، پیداکرده و گزارش می‌دهد. سرور نام دامنه برای خدمت اینترنتی صوتی، یک عملکرد کلیدی دارد. وقتی یک کاربری می‌خواهد از طریق این خدمت، تماس صوتی انجام دهد، ماشین کاربر با سرور نام دامنه تماس می‌گیرد تا آدرس پروتکل اینترنتی طرف مقابل گرفته شود. لذا اگر حافظه سرور تسخیرشده باشد تماس تلفنی به شخص دیگری هدایت شده و اطلاعات شخصی و محرمانه کاربر مورد سوءاستفاده قرار می‌گیرد. موارد متعددی از بهره‌گیری این آسیب‌پذیری‌ها گزارش‌شده است (هس وی وسواج،۲۰۱۲ :۹).

وظیفه امن‌سازی

کارشناسان امنیتی معتقدند که مراکز ارائه‌دهنده خدمات اینترنتی، در موقعیت مناسبی برای حفاظت از اینترنت هستند و آن‌ها دروازه‌ای هستند که از طریق آن‌ها نقض امنیت اینترنت مشتریان رخ می‌دهد. آن‌ها بر این باورند که ارائه‌دهندگان خدمات می‌توانند برای شناسایی فعالیت‌های غیرقانونی از فناوری‌های پیشرفته استفاده کنند.علاوه بر این، ارائه‌دهندگان خدمات دانش وسیعی از تهدیدات اثرگذار بر کسب‌وکار و اینترنت کاربران را دارند، لذا باید ارائه‌دهندگان خدمات بخشی از تامین امنیت شبکه مشتریان باشند (عثمان، ۲۰۱۳ : ۷۰). در صورت داشتن رویکرد امنیتی ISP محور، عمده حملات مخرب قابل کاهش هستند(همان).

می‌توان به‌منظور امن‌سازی، فعالیت‌هایی مانند تشکیل تیم پاسخگو به مشکلات امنیتی، نگهداری داده در انباره‌های ذخیره جهانی با ملاحظات امنیتی، کنترل ترافیک‌هایی را که از یک مشتری با آدرس‌های غیراختصاصی می‌آید (تا جلوی حملات مبتنی بر جعل آدرس منبع گرفته شود)، جلوگیری از بارگذاری بیش‌ازحد در بخش‌هایی از شبکه، نگهداری خدمات متعدد (ایمیل، اخبار و میزبانی سایت)بر روی سامانه‌های جداگانه، محدودیت دسترسی، اعمال احراز هویت قوی در چارچوب رمزنگاری، استفاده از سیستم تشخیص نفوذ، جلوگیری از اسکن درگاه‌ها و استفاده از لایه SSL و دیواره آتش بین سرورها، استفاده از لاگ کاربران جهت یافتن روندها (کدام کاربر در چه زمانی و از کدام IP وصل شده است؟) را انجام داد (شایبو،۱،۲۰۱۲).

1- Root Servers

دسته‌بندی مسئولیت‌ها

با توجه به مسئولیت‌های مذکور در بخش قبلی، می‌توان مسئولیت‌ها را بر اساس موضوع در ۵ محور مهم دسته‌بندی کرد:

۱) نظارتی: کنترل محتوا، جلوگیری از نشر اکاذیب، جلوگیری از فعالیت مجرمانه

۲)خصوصی: کپی‌رایت، حریم خصوصی، ممانعت از اسپم، شبکه‌های اجتماعی

۳) فنی: مسیریابی معتبر، حفاظت از سرور نام دامنه، امن سازی شبکه

۴) خدماتی: تأمین ترافیک و پشتیانی خدمات

۵) اطلاع‌رسانی و آموزش: آموزش تهدیدات، گزارش دهی از حوادث اینترنتی، اطلاع‌رسانی درزمینه ایرادهای زیرساختی، آگاه‌سازی و همکاری با دیگر ارائه‌دهندگان در صورت کشف خطر

با توجه به مسئولیت‌های مقرر در قوانین ارائه‌دهندگان خدمات اینترنتی(رسا) در ج.ا.ا که در اینجا به برخی از بندهای این قانون اشاره می‌شود، ضعف‌هایی در مسئولیت‌های فنی و اطلاع‌رسانی دیده می‌شود درحالی‌که به مسئولیت‌های نظارتی و خدماتی توجه خوبی شده است:

شرکت‌های رسا و کاربران برای محتوایی که بر روی شبکه عرضه می‌نمایند پاسخگو می‌باشند.

مسؤولیت رعایت قوانین مالکیت معنوی و حق تألیف به عهده ارائه‌کننده اطلاعات در شبکه هست.

– امکان و اعمال برقراری پالایه باید فراهم باشد.

– هر رسا موظف است اطلاعات کلی کاربران و**IP**های مربوط را ثبت و یک نسخه از آن نیز به وزارت پست و تلگراف و تلفن اعلام نماید.

– رسا موظف است خدمات مورد درخواست کاربر را باکیفیت مطلوب وبر اساس یک موافقت‌نامه به کاربر ارائه نماید.

– رسا موظف است تمهیدات فنی لازم برای حفظ حقوق کاربران و جلوگیری از حمله به کامپیوترها را فراهم آورد.

– رسا موظف است مواردی که مربوط به حقوق کاربران هست را به اطلاع آن‌ها برساند.

– رسا موظف است اطلاعات مربوط به نحوه حفاظت از حریم خصوصی اطلاعات و ارتباطات افراد در شبکه خود را در اختیار کاربران قرار دهد.

– حریم اطلاعات خصوصی کاربران از مصونیت برخوردار بوده و هرگونه دسترسی غیرقانونی توسط رساها و هر مرجع دیگر به فعالیت‌های اینترنتی کاربران ممنوع هست.

نظریه‌های تعمیم مسئولیت مدنی به ارائه‌دهندگان خدمات اینترنتی

در زمینه تسری و نعمیم مسئولیت مدنی به ارائه‌دهندگان خدمات اینترنتی، چهار نظریه مطرح است که عبارت‌اند از:: مسئولیت مستقیم، مسئولیت کارفرمایی، مسئولیت مشارکتی، مسئولیت نیابتی(وین سیناس،۲۰۱۲ :۵۸)

نظریه مسئولیت مستقیم

معمولاً مسئولیت قانونی بر پایه مقصر دانستن است یعنی نسبت دادن مسئولیت اخلاقی به عواقب عمل افراد که آزادانه انجام می‌دهند (پارادایم اراده آزادانه). لذا مسئولیت به کسی اطلاق می‌گردد که قادر به تصمیم آزادانه برای عملی باشد و بداند که چه عملی و چه وقت انجام دهد. درحالی‌که این پارادایم مسئولیت را به انتخاب برای انجام وابسته می‌کنداین نظریه، مسئولیت را به شخص و چگونگی موضوع وابسته می‌کند. لذا باملاحظه این جملات می‌توان فهمید که مسئولیت اساسی تابعی از نقش اجتماعی در ارتباط با عمل انجام‌گرفته یا رفتار صورت گرفته است. لذا می‌توان ارائه‌دهندگان خدمات اینترنتی را در قبال عملکرد مشتریانشان وقتی مرتکب نقض قوانین می‌شوند مسئول دانست و این امر معقول است زیرا به‌طور خودکار، موضوعات مورد حمایت‌شده (کپی‌رایت شده)طبق درخواست مشتریان، بازتولید و توزیع می‌شود.

این نظریه در آمریکا در مورد سوژه‌های تخلفاتی اینترنتی حق مؤلف استفاده‌شده است. چنین رویکرد کوته‌نظرانه مانع بزرگی بر سر راه نظریه ترکیبی است زیرا در نظر نگرفتن نیت یا آگاهی

به معنی این است که هر ارائه‌دهنده خدمات که بازتولید و توزیع یک مقوله‌ای را انجام دهد مرتکب تخلف کپی‌رایت شده است. در این صورت عملا یک فضای نامحدودی از مسئولیت قابل‌تصور است. لذا این نظریه جامعیت امروزی ندارد و تنها به عنوان ابزار تکمیلی برای اعمال مسئولیت قابل‌استفاده است.

نظریه مسئولیت کارفرمائی

معمولاً این دکترین برای اعمال مسئولیت شدید به یک کارفرما اطلاق می‌شود و لازم است رفتار هدایت‌گرانه خود را در قلمرو فعالیت خود اعمال نماید. در صورتی‌که ارائه‌دهندگان خدمات اینترنتی به لحاظ طراحی فنی برخی خدمات ارائه‌شده، به‌عنوان صدمه زننده مستقیم به افراد تلقی شود؛ و همچنین اگر محصول یا خدمت ارائه‌شده، معیوب تلقی شود، ارائه‌دهنده در قبال استفاده از آن مسئولیت خواهد داشت.

نظریه مسئولیت مشارکتی

در اینجا کسی که با علم به تخلف بودن عملی، کسی را وادار کند یا باعث عملی شود یا تشویق نماید یا مشارکت در هدایت متخلف داشته باشد مسئولیت مشارکتی خواهد داشت. قلمرو اصلی این نظریه یافتن مشارکت عالمانه برای موفقیت تخلف است. با توجه به اینکه امروزه از همه خدمات می‌توان دانش کافی به غیرقانونی بودن کاربری آن داشت لذا درصورتی‌که خدمات خاص ارائه‌دهنده خدمات اینترنتی یا هدایت آن‌ها مقدمه بوده باشد برای عالم بودن از فعالیت تخلف کاربرش کافی است. همچنین در صورت عدم استفاده از ابزارهای فیلترینگ جهت ممانعت از فعالیت غیرقانونی و داشتن منفعت مالی ارائه‌دهندگان خدمات اینترنتی دلیلی بر اعمال این مسئولیت است.

نظریه مسئولیت نیابتی

این مسئولیت از آنجا ناشی می‌شود که مدعی علیه حق و توانایی کنترل فعالیت‌های متخلفانه طرف ثالث را دارد و می‌تواند سود مالی را از تخلف خود کسب می‌کند. امروزه ارائه‌دهندگان خدمات اینترنتی، با فن‌آوری‌های جدید توانایی پیشگیری خیلی از تخلفات زیادی را دارند. طبق این

نظریه در صورتی که ارائه‌دهندگان خدمات اینترنتی، توانایی کنترل فعالیت‌های متخلفانه را داشته باشند. ولی به لحاظ منفعت مالی انجام ندهند قطعا مسئولیت خواهند داشت.

رویکردهای اعمال مسئولیت به ارائه‌دهندگان خدمات اینترنتی

رویکردها به مقوله مسئولیت ارائه‌دهندگان خدمات اینترنتی، بر مبانی و استدلال‌های قضایی تأثیر می‌گذارد. انواع رویکردها عبارت‌اند از : فعال پیشگیرانه/غیرفعال واکنشی، خارجی/داخلی، استثناء/غیر استثناء(وین سیناس،۲۰۱۲ :۹۵).

رویکرد فعال پیشگیرانه و غیرفعال واکنشی

در رویکرد غیرفعال واکنشی، ارائه‌دهندگان خدمات اینترنتی، مادامی که دانش متقنی از اینکه شخصی از خدمت یا محصولشان در جهت نقض قوانین استفاده می‌کند نداشته باشند، برای ارائه هر خدمتی یا محصولی آزاد هستند. ولی در صورت علم به وجود نقض قوانین، بایستی واکنش همه‌جانبه نشان دهند. با تغییر شرایط و فشار فزاینده مؤسسات نظارتی و قوه مقننه و صنایع، در برخی کشورها، نقش ارائه‌دهندگان خدمات اینترنتی(به‌خصوص در ارتباطات نقطه‌به‌نقطه و کپی‌رایت) از غیرفعال بودن به فعال پیشگیری‌کننده از تخلفات تبدیل‌شده است. نتیجه این دو رویکرد، تغییر نگرش در ابعاد کنترلی شبکه، فیلترینگ محتوا، شکل‌دهی به ترافیک و همکاری با مجریان قوانین فضای سایبر است.

رویکرد خارجی و داخلی

در رویکرد خارجی، اینترنت به‌عنوان شبکه جهانی با کاربران و برنامه نویسان خارج شبکه‌ای که با رایانه خود به آن وصل می‌شوند تلقی می‌شود. در این رویکرد ارائه‌دهندگان خدمات به‌صورت فنی بایستی امکان ممانعت از نقض قوانین را داشته باشند و در صورت سهل‌انگاری مسئولیت دارند. درحالی‌که در نگرش داخلی به همه‌چیز با توجه به تعریف‌های فن‌آوری از داخل نگاه می‌شود. در این رویکرد، عملکردهای فنی یا ساختار اینترنت از اهمیت کمتری برخوردار است. مسئولیت ارائه‌دهندگان خدمات اینترنتی‌ها در قبال اطلاعات ارسال‌شده محدود است. اگر کنترلی بر محتوا نداشته باشند مسئولیتی ندارند زیرا کاربران هستند که عملکردهای غیرقانونی انجام می‌دهند و

مسئولیت دارند. به احتمال زیاد در آینده نزدیک به خاطر گسترش وسیع اینترنت، رویکرد داخلی غالب شود.

رویکرد استثناء و غیر استثناء

در رویکرد استثناء فضای سایبر به‌عنوان مکان جدیدی که بایستی به‌وسیله نرم‌های توسعه‌یافته توسط کمیته‌های کاربران نقش‌بندی شود در نظر گرفته می‌شود، اما رویکرد غیر استثنایی تأکید می‌کند که سایبر مکان جدایی نیست بلکه شبکه‌ای است که افراد را دریک مکانی با افراد در قلمرو دیگری مرتبط می‌سازد؛ و قوانین متناظر با فضای فیزیکی در آن حاکم است. در صورت غالب شدن رویکرد استثناء، قوانین یا نظارت‌ها محدود نبوده و فعالیت‌های نظارتی زیادی به ارائه‌دهندگان خدمات اینترنتی و دیگر بازیگران حوزه فضای سایبر اعمال خواهد شد.

چارچوب مفهومی تحقیق

با توجه به مجموع مباحث فوق می‌توان دسته‌بندی زیر را در قالب چارچوب مفهومی ارائه داد:

شکل۲. مدل مفهومی تحقیق

روش تحقیق

پژوهش حاضر ازنظر نوع تحقیق، کاربردی و ازنظر رویکرد کیفی بوده و روش تحقیق توصیفی تحلیلی و ازنظر طرح تحقیق گذشته‌نگر نتیجه گراست. ابزار جمع‌آوری اطلاعات پرسشنامه محقق ساخته است که با استفاده از مطالعه مبانی نظری، مصاحبه با خبرگان، قوانین جاری کشور و تجربیات موفق دیگر کشورها در راستای اهداف تحقیق تشکیل می‌دهد. روایی و پایایی داده‌ها به‌طور مفصل در قسمت تحلیل داده‌ها بحث شده‌اند. برای تجزیه‌وتحلیل داده‌ها و آزمون کردن ارتباط ابعاد، از نرم‌افزار SPSS و برای برازش مدل از نرم‌افزار Smart PLS استفاده‌شده است.

جامعه آماری و حجم نمونه

جامعه آماری در این تحقیق خبرگان دانشگاهی و اجرایی در مجتمع شهید اشرفی اصفهانی هستند که آشنایی کامل با ۵ حوزه موردمطالعه ارائه‌دهندگان خدمات اینترنتی (خدماتی، نظارتی، فنی، حریم خصوصی، آموزشی) دارند و تعدادشان به ۶۵ نفر می‌رسد. لذا بر اساس خروجی جدول مورگان حجم نمونه ۵۶ می‌باشد.

جمع‌آوری و تحلیل داده‌ها

پرسشنامه‌ای پنج گزینه‌ای لیکرت که حاوی سؤالات ابعاد مسئولیت‌های ارائه‌دهندگان خدمات اینترنتی و نظریه‌های حاکم بر این مسئولیت‌ها و رویکرد لازم برای اتخاذ مسئولیت‌های آتی بود بین همه خبرگان توزیع و۵۶ نفر به آن‌ها پاسخ دادند. میزان ارتباط هر بعد با استفاده از نرم‌افزار SPSS، آزمون گردید که در جدول ۵ اهمیت هر بعد بر اساس دیدگاه‌های صاحب‌نظران ارائه گردیده است.

به‌منظور برازش مدل از نرم‌افزار Smart PLS استفاده‌شده است. در صورت مواجه بودن با نمونه‌های کوچک، داده‌های غیر نرمال و نیاز به مدل‌سازی معادلات ساختاری و برازش مدل و همچنین مواقعی که در مدل سازه‌ای با یک (شاخص) سؤال مواجه هستیم، می‌توان از این روش استفاده کرد. یکی از قواعد شناخته‌شده برای تعیین حداقل نمونه لازم درروش PLS، توسط بارکلای و همکاران (۱۹۹۵) ارائه‌شده است.

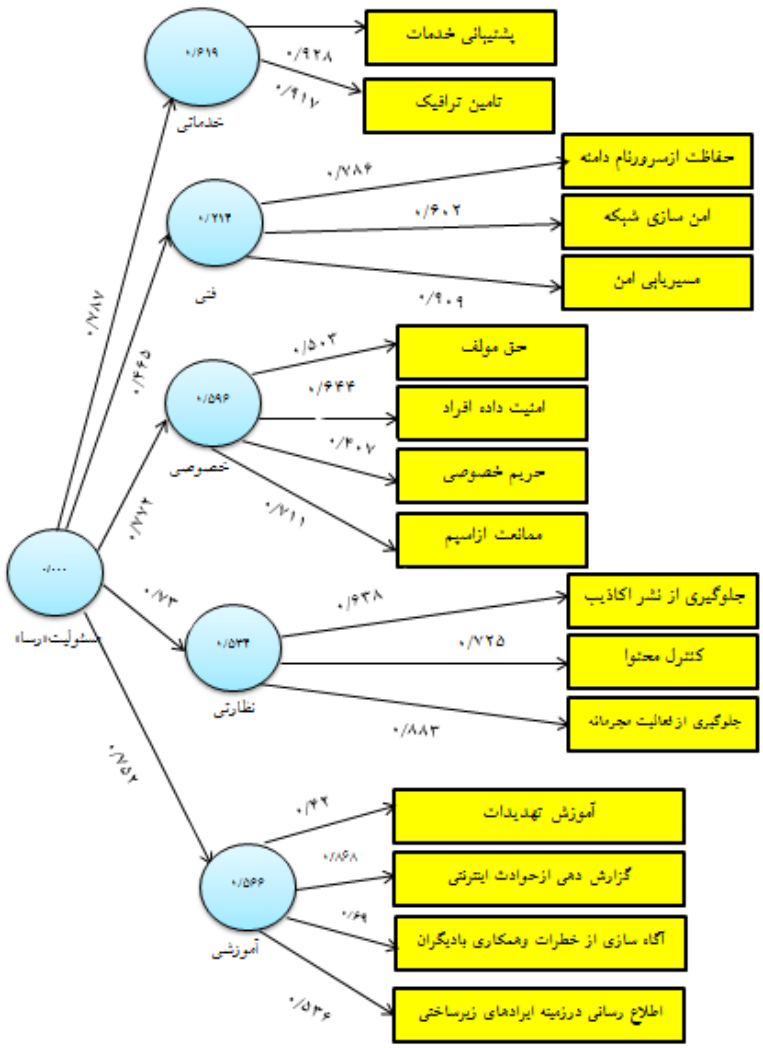
در این روش به‌منظور حصول اطمینان از دقت و صحت نتایج به‌دست‌آمده از تحقیق، باید از ارزیابی ویژگی‌های فنی پرسشنامه استفاده کرد؛ که شامل روایی، پایایی است. بنابراین برای ارزیابی مدل ابتدا باید تشخیص دهیم که مدل پیشنهادی تحقیق از نوع شاخص‌های انعکاس است یا از نوع شاخص‌های سازنده است. به این منظور هم از آزمون رگرسیون در SPSS می‌توان استفاده کرد وهم به یکی از سه طریق زیر می‌توان نوع مدل را تشخیص داد (داوری، رضازاده، ۱۳۹۲: ۵۵):

۱- درصورتی‌که تغییرات در سازه (مؤلفه‌ها)، باعث تغییرات در شاخص‌ها شود نوع مدل انعکاسی و در صورتی که تغییرات در شاخص‌ها باعث تغییر در سازه شود مدل سازنده است؛

۲- در مدل سازنده، شاخص‌ها هرکدام نماینده یک مفهوم جداگانه بوده و لزوما همپوشانی ندارند؛

۳- همبستگی متقابل شاخص‌ها از قبل پیش‌بینی‌نشده است ولی در انعکاسی از قبل مشخص است که شاخص‌ها همبستگی متقابل زیادی دارند.

در مدل تحلیل‌شده، شاخص‌ها هرکدام نماینده یک مفهوم جداگانه بوده و همبستگی متقابل از قبل پیش‌بینی‌نشده است. حال مسئولیت‌های استخراجی از مبانی نظری را که در مدل پیشنهادی آمده است در نرم‌افزار PLS ترسیم می‌کنیم.



شکل۳. مدل تحقیق

لازم به ذکر است که بارهای عاملی از طریق محاسبه مقدار همبستگی شاخص‌های یک سازه با آن سازه محاسبه می‌شود و اگر این مقدار برابر و یا بیشتر از ۰/۴ شود مؤید این مطلب است که واریانس بین سازه و شاخص‌های آن از واریانس خطای اندازه‌گیری آن سازه بیشتر است و پایایی در مورد آن مدل اندازه‌گیری قابل‌قبول است(داوری و رضازاده، ۱۳۹۳: ۸۰).

برازش مدل در بخش‌های برازش اندازه‌گیری‌ها و برازش ساختاری

برازش مدل‌های اندازه‌گیری

برازش مدل‌های اندازه‌گیری مربوط به بخشی از مدل کلی است که دربرگیرنده یک مؤلفه با سؤالات مربوطه است لذا ۵ مدل اندازه‌گیری خدماتی، فنی، حریم خصوصی، نظارتی و آموزشی خواهیم داشت. برای برازش مدل‌های اندازه‌گیری دو معیار پایایی، روایی استفاده می‌شود.

پایایی

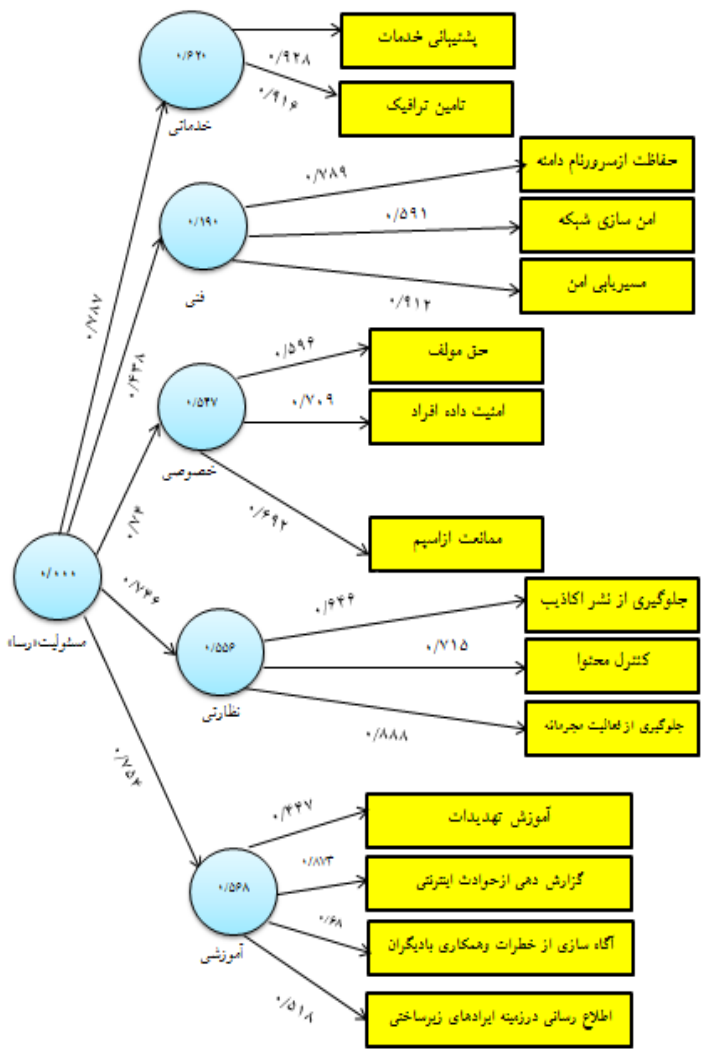
از طریق ضرایب بارهای عاملی یا ضرایب آلفای کرون باخ یا پایایی ترکیبی یا پایایی اشتراکی بررسی می‌شود.

برای بررسی ضرایب بار عاملی مؤلفه‌ها، از طریق منوی calculate/PLS Algorithm و مشخص کردن مقادیر گم‌شده (سؤالاتی که پاسخ‌دهنده به دلیل نپذیرفتن سؤال، جواب نداده است امتیازی به آن سؤال داده نشده است)اقدام می‌شود. بارهای عاملی که همگی بیشتر از۰/۴ است نشانگر مناسب بودن پایایی است.

جدول۱. پایایی ترکیبی قبل از حذف privacy

	AVE	Composite Reliability	R Square
مسئولیت آموزشی	۰/۴۲۳	۰/۷۳۲	۰/۵۶۵
مسئولیت فنی	۰/۶۰۱	۰/۸۱۵	۰/۲۱۴
مسئولیت خصوصی	۰/۳۳۵	۰/۶۵۸	۰/۵۹۶
مسئولیت خدماتی	۰/۸۵۰	۰/۹۱۹	۰/۶۱۹
مسئولیت نظارتی	۰/۵۷۱	۰/۷۹۷	۰/۵۳۳

جدول ۱، پایایی ترکیبی (Composite Reliability) مؤلفه‌ها را نشان می‌دهد. در بررسی قابل قبول بودن پارامترهای این جدول، معیار قبولی برای AVE، ۰/۴ (داوری و رضازاده، ۱۳۹۳: ۱۳۷)و برای R Square، ۰/۱۹ می‌باشد(داوری و رضازاده، ۱۳۹۳: ۱۴۶). در تغییر مکنون «خصوصی»، مقدار کمتر از ۰/۴ است لذا لازم است شاخصی از این تغییر را که کمترین بار عاملی را دارد حذف کرد. بعد از حذف این شاخص، بارهای عاملی بیشتر از ۰/۴ و پایایی ترکیبی بیشتر و یا نزدیک ۰/۷ خواهند شد.



شکل۴. مدل تحقیق بعد از حذف شاخص «حریم خصوصی»

جدول۲. پایایی ترکیبی بعد از حذف «حریم خصوصی»

	AVE	Composite Reliability	R Square
مسئولیت آموزشی	۰/۴۲۳	۰/۷۳۳	۰/۵۶۸
مسئولیت فنی	۰/۶۰۱	۰/۸۱۴	۰/۱۹
مسئولیت خصوصی	۰/۴۳۵	۰/۶۹۶	۰/۵۴۶
مسئولیت خدماتی	۰/۸۵۰	۰/۹۱۹	۰/۶۱۹
مسئولیت نظارتی	۰/۵۷۲	۰/۷۹۷	۰/۵۵۶

دیده می‌شود که همه اعداد AVE و R Square از معیارهای ۰/۴ و ۰/۱۹ برابر یا بالاترند.

روایی

روایی واگرایی روشی برای برازش مدل‌های اندازه‌گیری است که دو موضوع را پوشش می‌دهد (داوری و رضازاده، ۱۳۹۳: ۱۳۹):

الف)مقایسه میزان همبستگی بین شاخص‌های یک سازه با آن سازه در مقابل همبستگی آن شاخص با سازه‌های دیگر (که برای این موضوع بایستی از گزارش cross loading نرم‌افزار smart PLS استفاده کرد).

هم چنان‌که در جدول ۳ دیده می‌شود، تمامی سؤالات مربوط به هر سازه همبستگی بیشتری نسبت به سازه‌های دیگر دارد. لذا این امر روایی واگرایی مناسب مدل را با معیار الف نشان می‌دهد.

جدول۳. بارهای عاملی شاخص‌های سازه‌های پژوهش برای بررسی روایی واگرایی

	آموزشی	فنی	خصوصی	خدماتی	نظارتی
تأمین ترافیک	۰/۳	۰/۱۳	۰/۶۲	۰/۹۱	۰/۳۶
پشتیبانی خدمات	۰/۵۳	۰/۱۸	۰/۴۴	۰/۹۲	۰/۴۱
حفاظت از سرور نام دامنه	۰/۰۸	۰/۷۸	۰/۲۳	۰/۰۷	۰/۱۳
امن سازی شبکه	۰/۰۳	۰/۵۹	۰۱,۰	۰/۲۷	-۰/۰۰۰۸
مسیریابی امن	۰/۳۶	۰/۹۱	۰/۱۶	۰/۱۱	۰/۲۵
ممانعت از اسپم	۰/۲۷	۰/۱۳	۰/۶۹	۰/۳۹	۰/۳
امنیت داده افراد	۰/۱۹	-۰/۰۶	۰/۷	۰/۵۱	۰/۱۹
حق مؤلف	۰/۲۹	۰/۲۹	۰/۵۷	۰/۲۴	۰/۳۶
کنترل محتوا	۰/۴۱	۰/۲۵	۰/۲۱	۰/۲۲	۰/۷۱
جلوگیری از نشر اکاذیب	۰/۳۶	۰/۰۶	۰/۰۹	۰/۲۵	۰/۶۵
جلوگیری از فعالیت مجرمانه	۰/۳	۰/۱۴	۰/۵۸	۰/۴۵	۰/۸۹
گزارش دهی از حوادث اینترنتی	۰/۸۷	۰/۰۸	۰/۱۸	۰/۳۹	۰/۴۶
آموزش تهدیدات	۰/۴۵	۰/۰۵	۰/۳۱	۰/۲۸	۰/۱۱
آگاه‌سازی از خطر و همکاری با دیگران	۰/۶۸	۰/۴۵	۰/۲۴	۰/۳۲	۰/۲۳
اطلاع‌رسانی در زمینه‌ی ایرادهای زیرساختی	۰/۵۲	۰/۰۲	۰/۳۵	۰/۱۷	۰/۳۱

ب)مقایسه میزان همبستگی یک سازه با شاخص‌هایش در مقابل همبستگی آن سازه با سایر سازه‌ها به روش فورنل و لارکر(که برای این موضوع بایستی از گزارش Latent Variable Correlation نرم‌افزار Smart PLS استفاده کرد).

همان‌گونه که از جدول ۴ برگرفته از روش فورنل و لارکر مشخص است مقدار جذر AVE متغیرهای مکنون در پژوهش حاضر که در خانه‌های قطر اصلی ماتریس قرار دارند از مقدار همبستگی میان آن‌ها که در خانه‌های زیرین و چپ قطر اصلی ترتیب داده‌شده‌اند بیشتر است لذا روایی واگرایی در حد قابل‌قبول است.

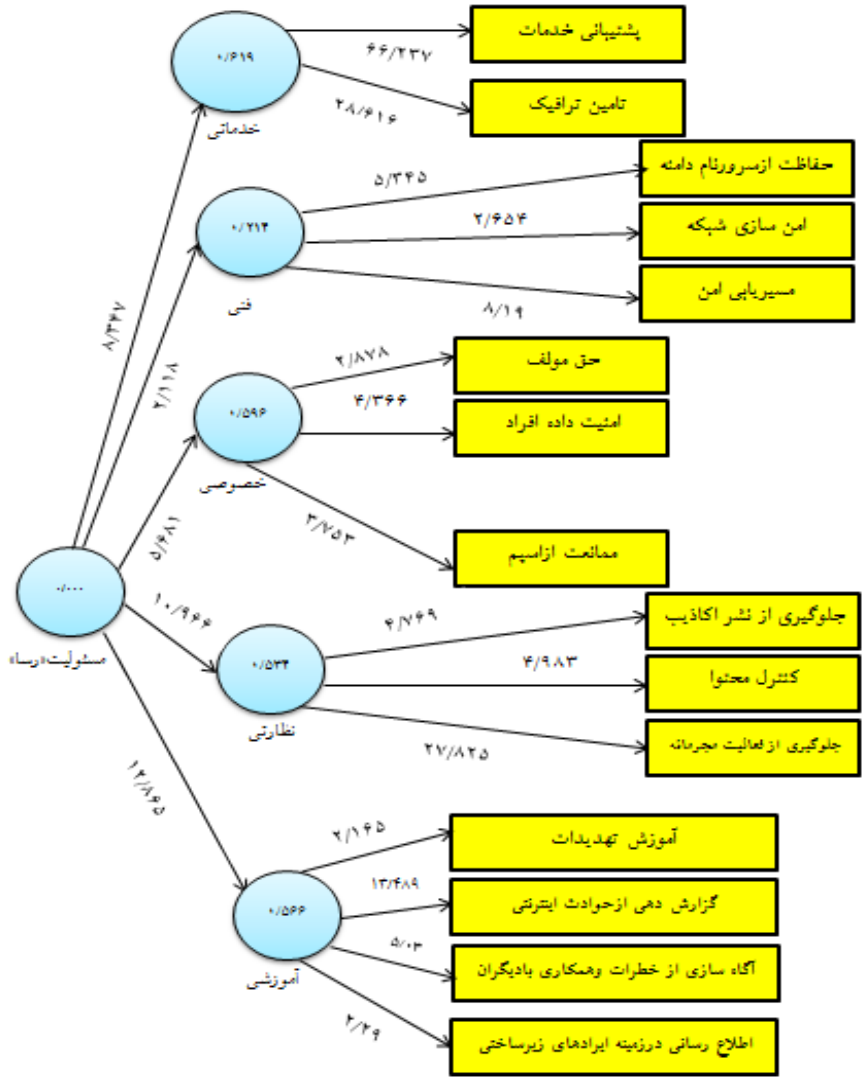
جدول۴. نتایج روایی واگرایی

سازه	آموزشی	فنی	خصوصی	خدماتی	نظارتی
آموزشی	۰/۶۵	–	–	–	–
فنی	۰/۲۵	۰/۷۷	–	–	–
خصوصی	۰/۳۹	۰/۱۸	۰/۶۵	–	–
خدماتی	۰/۴۵	۰/۱۷	۰/۵۷	۰/۹۲	–
نظارتی	۰/۴۵	۰/۲	۰/۴۳	۰/۴۲	۰/۷۵

برازش مدل ساختاری

برازش مدل ساختاری به سؤالات (متغیرهای آشکار)کاری ندارد و تنها متغیرهای پنهان با روابط میان آن‌ها بررسی می‌گردد.

. برای این منظور از ضرایب معناداری Z یا همان t-values بافرمان Bootstrapping استفاده می‌شود. با توجه به اعداد ۸/۳۲۷ و۲/۱۱۸، ۵/۶۸۱ و۱۰/۹۶۶ و۱۳/۸۵۶ که همگی بیشتر از۱/۹۶ می‌باشند لذا برازش مدل با سطح اطمینان ۹۵ درصد معنادار بودن تائید می‌شود. در ضمن معناداری روابط سؤالات و متغیرهای مربوطه نیز (بالاتر بودن ضرایب از ۱/۹۶)مشاهده می‌گردد.



شکل۵. مدل همراه با ضرایب معناداری Z

همچنین به‌منظور رتبه‌بندی ابعاد از آزمون فریدمن نرم‌افزار SPSS استفاده‌شده است که نتایج آزمون در جدول ۵ مشاهده می‌شود.

جدول۵. نتایج آزمون فریدمن

ابعاد	ضریب
حفاظت از سرور نام دامنه	۱۱/۷۳
مسیریابی امن	۱۱/۷۲
امن سازی شبکه	۱۰/۹۱
پشتیانی خدمات	۱۰/۸۶
تأمین ترافیک	۱۰/۰۹
آگاه‌سازی و همکاری با دیگر ارائه‌دهندگان در صورت خطر	۹/۷۷
حق مؤلف	۹/۵۹
شبکه‌های اجتماعی و حفاظت از داده افراد	۹/۰۰
اطلاع‌رسانی در زمینه‌ی ایرادهای زیرساختی	۸/۳۲
گزارش دهی از حوادث اینترنتی	۸/۱۸
جلوگیری از فعالیت مجرمانه	۷/۴۱
ممانعت از اسپم	۶/۸۲
کنترل محتوا	۶/۶۸
آموزش تهدیدات	۴/۹۱
جلوگیری از نشر اکاذیب	۴/۶۸

آماره‌ها

مجذورکای	۸۸/۶۵
درجه آزادی	۱۴
سطح معنی‌داری	۰/۰۰۰

بر اساس نتایج آزمون فریدمن شاخص‌ها به ترتیب از بالاترین اهمیت به کمترین اهمیت عبارت‌اند از :

حفاظت از سرور نام دامنه، مسیریابی امن، امن سازی شبکه، پشتیانی خدمات، تأمین ترافیک، آگاه‌سازی و همکاری با دیگر ارائه‌دهندگان در صورت خطر، حق مؤلف، شبکه‌های اجتماعی و حفاظت از داده افراد، اطلاع‌رسانی در زمینه ایرادهای زیرساختی، گزارش دهی از حوادث اینترنتی، جلوگیری از فعالیت مجرمانه، ممانعت از اسپم، کنترل محتوا، آموزش تهدیدات، جلوگیری از نشر اکاذیب

در آزمون فریدمن فرض صفر مبتنی بر یکسان بودن میانگین رتبه‌ها در بین گروه‌هاست. سطح معنی‌داری آزمون را با مقدار صفر می‌توان مشاهده کرد که نشان از رد شدن فرض صفر دارد و این به این معنی است که در بین گروه‌ها حداقل دو گروه با هم اختلاف معناداری دارند.

به دلیل این‌که در پرسشنامه صاحب‌نظران می‌توانستند شاخص‌های دیگری را پیشنهاد نمایند، شاخص‌های پایداری و پوشش همه مطالبات کاربران در بعد خدماتی و همچنین شاخص‌های همکاری با نهادهای پلیسی و همکاری با شورای فیلترینگ و مسدودسازی محتوای مجرمانه و احراز هویت وبلاگ گیری در بعد نظارتی ونیز شاخص توصیه به نصب انواع ضدویروس‌ها در بعد آموزش و اطلاع‌رسانی توسط صاحب‌نظران پیشنهاد شد که در اولویت‌های بعدی قرار داشتند.

تناظر نظریه‌ها با ابعاد و رویکرد مورد انتظار برای ابعاد

پاسخ‌دهندگان تناظر نظریه کارفرما را با ابعاد فنی و خدماتی، با ۹۶/۴۲ درصد و تناظر نظریه مشارکتی را با ابعاد نظارتی و حریم خصوصی، با ۸۹/۲۸ درصد و تناظر نظریه نیابتی را با بعد

آموزشی، با ۸۵/۷۱ درصد و همچنین تناظر نظریه‌های کارفرما و مشارکتی را با رویکرد فعال پیشگیرانه با ۹۲/۸۵ درصد موردپذیرش قراردادند.

نتیجه‌گیری و پیشنهادها

مسئولیت ارائه‌دهندگان خدمات اینترنتی ازجمله مفاهیمی است که در جوامع پیشرفته مورداستفاده قرار می‌گیرد. مسئولیت‌پذیری منجر به استانداردهایی جهت ارتقای خدمات‌رسانی، حفاظت از داده‌های باارزش، کاهش جرائم اینترنتی، کاهش فعالیت‌های مجرمانه، افزایش آرامش اجتماعی، رعایت هنجارها، رعایت حقوق مؤلفین، رعایت حریم خصوصی، ارتقای دانش کاربران جهت مقابله با تهدیدات و... خواهد شد. در این تحقیق ابعاد مختلف مسئولیت ارائه‌دهندگان خدمات اینترنتی موردبررسی قرار گرفت در پاسخ به سؤالات تحقیق، نتیجه به‌دست‌آمده نشان داد که ارائه‌دهندگان خدمات اینترنتی در زمینه‌ی اطلاع‌رسانی و آموزش مسئولیت نیابتی، در زمینه‌ی حفظ حریم خصوصی و نظارت، مسئولیت نیابتی و مشارکتی دارند درحالی‌که در زمینه‌ی خدمات‌رسانی و موضوعات فنی، مسئولیت کارفرمائی دارند. همچنین در خصوص بکارگیری انواع رویکردها، نتیجه نشان داد که در خدمات‌رسانی، موضوعات فنی، نظارت و حفظ حریم خصوصی، بایستی ارائه‌دهندگان خدمات اینترنتی رویکرد فعال پیشگیرانه مورد استفاده قرار گیرد.

نوآوری تحقیق: هم چنان‌که قبلاً نیز اشاره شد در قوانین ج.ا.ا، به برخی از مسئولیت‌های ارائه‌دهندگان خدمات اینترنتی که موردبحث قرار گرفت به‌وضوح اشاره نشده است به‌عنوان‌مثال مسیریابی معتبر، حفاظت از سرور نام دامنه، آموزش تهدیدات، گزارش دهی از حوادث اینترنتی و ایرادات زیرساختی، همکاری با دیگر مراکز ارائه‌دهنده خدمات اینترنتی در صورت کشف خطر و..... ما در این پژوهش مؤلفه‌های مختلف مسئولیت‌ها را از منظر خبرگان این موضوع مورد بررسی قرار گرفت. لذا می‌توان با در نظر گرفتن مباحث نظری، تجربیات موفق و قوانین دیگر کشورها، قوانین کشورمان را توسعه و تکمیل کرد.

پیشنهادها:

۱- در بسیاری از کشورها، متولیان نظارتی به سمت اعمال فشار به ISPها برای قرار گرفتن بیشتر در زنجیره مسئولیت‌پذیری حرکت کرده‌اند. از طرفی هم، طبیعت اینترنت طوری است که سیستم کاربر، نمی‌تواند به اندازه کافی امن باشد مگر اینکه تمام سامانه‌های متصل، امن باشند. در این

راستا، ISPها در موقعیت بهتری برای تأمین امنیت شبکه کاربران هستند، لذا پیشنهاد می‌گردد کشورمان نیز با داشتن رویکرد امنیت ISP محور، دفاع لایه‌ای کاربران در جهت کاهش حملات سایبری را در دستور کار خود قرار دهد.

۲- با توجه به رشد سریع بات‌نت‌های مخرب در تجهیزات کاربران پیشنهاد می‌شود همانند کشورهایی مانند ژاپن و آلمان، یک برنامه جامع اطلاع‌رسانی که شامل اطلاع‌رسانی حول بات‌نت-ها، گزارش‌دهی از حوادث اسپم، اقدامات مقابله با بات‌نت‌های مخرب، انتقال تجربیات موفق، بهبود فناوری‌های تشخیص‌دهنده بات‌نت‌های کنترل و فرماندهی و بات‌نت‌های سوءاستفاده‌کننده از ترافیک باشد.

۳-با توجه به تأثیر فزاینده فضای سایبر بر زندگی روزمره و فرامرزی بودن این فضا و ظهور ابعاد مختلف حقوقی در این فضا بخصوص در اینترنت که یکی از مؤلفه‌های اصلی سایبر است پیشنهاد می‌شود آینده‌پژوهی حقوقی در اینترنت آینده (که اینترنت پهن باند فراگیر خواهد بود و علاوه بر انسان‌ها، اشیاء نیز در آن نقش خواهند داشت) صورت گیرد و قوانین پیشدستانه تدوین شود.

منابع

الف– فارسی

- کاتوزیان، ناصر (۱۳۷۸)، **ضمان قهری**، ***دانشگاه تهران***، جلد۱، شماره ۱۹۷.
- نوری، محمد؛ نخجوانی، رضا (۱۳۸۳)، حقوق حمایت داده‌ها، ***گنج دانش***
- داوری، علی ؛ رضازاده، آرش (۱۳۹۳)، ***مدل‌سازی معادلات ساختاری با نرم‌افزار PLS***، **جهاد دانشگاهی**، چاپ دوم
- جنتی، سعید ؛ رستمی، عبدالله (۱۳۹۱)، ***مسئولیت مدنی ناشی از ارتباطات اینترنتی***، **پایان‌نامه کارشناسی ارشد**، دانشگاه گیلان
- خوشدل، علی (۱۳۹۴)، ***مسئولیت مدنی ناشی از ارتباطات الکترونیک***، پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکزی
- ابهری، حمید؛ میری، حمید (۱۳۹۰)، مطالعه تطبیقی مبانی مسئولیت مدنی ارائه‌دهندگان خدمات اینترنتی، ***نشریه پژوهش‌های حقوق تطبیقی***، شماره ۳، صص ۲۰-۱.
- انصاری، باقر، (۱۳۸۲) ، مقدمه‌ای بر مسئولیت مدنی ناشی از ارتباطات اینترنتی، ***مجله دانشکده حقوق و علوم سیاسی***، شماره ۶۲، صص ۱۱-۵۳
- صادقی، حسین (۱۳۸۹)، مسؤولیت مدنی واسطه‌ها و تأمین‌کنندگان خدمات ارتباطات الکترونیک، ***فصلنامه حقوق***، دوره چهلم، شماره ۲، صص ۲۱۸ – ۱۹۹
- مهرگان، محمدرضا ؛ قاسم‌زاده، فریدون؛ صفری، حسین (۱۳۸۱)، به‌کارگیری تکنیک دلتا با رویکرد فازی جهت شناسایی موقعیت راهبردی بنگاه‌ها **:**مطالعه موردی شرکت‌های ارائه‌دهنده خدمات اینترنتی، ***فصلنامه دانش مدیریت***، شماره ۵۸
- وب‌سایت سازمان فناوری اطلاعات ایران، مقررات و ضوابط شبکه‌های اطلاع‌رسانی رایانه‌ای، (۱۳۹۴/۱۱/۸) (http://itc.ir/Default.aspx?tabid=288)

ب– انگلیسی

- Price, P. D. (2002). ***Toward an Internet Service Provider*** (ISP)Centric Security Approach,Thesis completed in cooperation with the Institute for Information Superiority and Innovation. Naval Postgraduate School Monterey
- Purcell T. (2002),***User Security and The Internet Service Provider***, SANS Institute.
- Hathaway M. ; Savage J. (2012).***Stewardship of Cyberspace: Duties for Internet Service Providers***, Canada Centre for global security Studies. University of Toronto Publication.
- Karolis Vinciūnas(2012). Civil Liability Of ISP For Transmitted Information: Problems And Perspectives Of Legal Regulation. ***Teisės Apzvalga Law Review***, Number 8, PP 57-99
- Butler K. ; Farley T. (2010). A Survey of BGP Security Issues and Solutions. ***Proceedings of the IEEE***, Volume 98, Number 1 PP100-122.
- "Chinese ISP Hijacks the Internet," BGP.mon blog, 8 April 2010, http://bgpmon.net/blog/?p=282.
- Declan McCullagh(2008).How Pakistan Knocked YouTube Offline. ***CNET News.*** http://news.cnet.com/8301-10784_3-9878655-7.html.
- Gill. P.; Schapira. M. and Goldberg S. (2011).Let the Market Drive Deployment: A Strategy for Transitioning to BGP Security, ***Proceedings of SIGCOMM.*** **PP**15-19
- Shaibo Y. (2012). Operation Ghost Click: International Cyber Ring That Infected Millions of Computers Dismantled. ***FBI website,*** 9 November 2011, accessed 5 February 2012
- www.legalanswers.sl.nsw.gov.au/hot_topics/pdf
- Hot Topics: legal issues in plain language. (2009).published by ***the Legal Information Access Centre(LIAC)***.PP 1-30
- Adam Smith(2006).Calibrating Noise to Sensitivity in Private Data Analysis. in ***Proceedings of the 3rd Theory of Cryptography Conference***.PP265-284.
- Nancy Benac. (1997).Good Samaritan Laws Common in Europe but Rare in America. ***Wisconsin State Journal***. ISSN 0749405X
- Usman, SH. H. (2013).A Review Of Responsibilites Of ISP Toward Their Customers' Netwok Security. ***Journal of Theoretical and Applied Information Technology.*** Vol. 49, No. 1

- Lichtman, D. (2004). Holding Internet Service Providers Accountable. ***Telecommunications and Technology.*** PP54-59
- Tian, Y. (2009). ***Law Models of ISP Liability and Their Implementation***. In Re-thinking intellectual property: the political economy of copyright protection in the digital era. New York, United States of America: Routledge-Cavendish
- Bolin B. (2015). ***ISP Liability;Copyright Liability Concerns for Internet Service Providers***. www.Bit law.htm.