Journal iranian political sociology

Vol. 5, No.8, Aban2022

https://dx.doi.org/۱۰,۳۰۵۱۰/psi.۲۰۲۲,۳۱۶۵۸۵,۲۶۶۹

Civil liability of producers and operators of content transfer in cyberspace

Abstract

The coming years will undoubtedly or will continue to face the widespread evolution of the age of communication and information processing in the lives of human societies. Cyberspace and electronic space, according to the technical conditions, have significant capacities for abuse in order to violate human privacy. However, content-related issues in virtual environments lead to the expression of specific issues that have not had much history in non-virtual environments. On the one hand, the common cases of privacy violations in cyberspace have significant features, and on the other hand, the creation of cyberspace has created new angles and grounds for violating the rules. Creating or producing, presenting, offering, providing comprehensive and non-comprehensive distribution of content and using electronic packages in the new space needs new do's and don'ts, so it is necessary based on the technical and legal characteristics of virtual environments and activities, privacy violation To be analyzed and examined in these areas, then the importance, role, rules and guarantee of content protection performances in the virtual environment should be determined.

In order to effectively protect human privacy in cyberspace and create responsibility for the relevant trustees, it is necessary for the Regulatory and Communication Commission, which according to Article 5 of the Law on Duties and Powers of the Ministry of Communication and Information Technology, Implementation to remove the serious vacuum ahead.

-Keywords

Content, cyberspace, electronic intermediaries, civil liability, carrier

.

ماهنامه علمی (مقاله علمی_پژوهشی) جامعه شناسی سیاسی ایران، سال پنجم،شماره هشتم، آبان۱۴۰۱،صص۱۲۴۳-۱۲۲۶
https://dx.doi.org/۱۰,۳۰۵۱۰/psi.۲۰۲۲,۳۱۶۵۸۵,۲۶۶۹

مسولیت مدنی تولید کنندگان و متصدیان انتقال محتوا در فضای مجازی

همایون علی حسینی[۱]
حمیدرضا علی کرمی[۲]
رسول احمدی فر[۳]

تاریخ دریافت :۱ /۱۴۰۱/۲
تاریخ پذیرش: ۱۴۰۱/۰۶/۰۳

- چکیده

سال های آینده بی تردید تکامل گسترده عصر ارتباطات و پردازش اطلاعات زندگی جوامع انسانی را با گفتمان جدیدی روبرو کرده و یا خواهد کرد یکی از مصادیق رایج و جدید طرح مسأله محتوا نگهداری آن درفضای سایبری می باشد این عرصه بنابه شرایط فنی دارای ظرفیتهای قابل توجهی جهت سوءاستفاده بمنظور نقض حریم انسانها ست. با این حال مباحث مربوط به محتوا در محیط های مجازی موجب بیان مباحث ویژه‌ای می گردد که طرح آن در محیط های غیرمجازی سابقه چندانی نداشته است. از یک سو موارد رایج نقض حریم‌خصوصی در محیط مجازی دارای ویژگیهای قابل توجهی می شود و از سوی دیگر ایجاد محیط مجازی باعث ایجاد زوایا و زمینه های جدیدی از نقض قوانین شده است. ایجاد یا تولید ،ارایه ،عرضه تامین ،پخش فراگیر و غیر فراگیر محتوا و استفاده از بسته های الکترونیکی در فضای جدید باید و نبایدهای نوینی را نیاز دارد لذا لازم است بر اساس ویژگیهای فنی و حقوقی محیط ها و فعالیت های این حوزه جدید و نوین مورد برر سی قرار گیرد پس از آن اهمیت، نقش، احکام و ضمانت اجراهای حمایت از محتوا در محیط مجازی مشخص شود

برای حمایت مؤثر از حریم انسانها در محیط مجازی و ایجاد مسولیت برای متولیان مربوطه لازم است کمیسیون تنظیم مقررات و ارتباطات متولی تدوین مقررات بخش ictکشور است همچنین قوانین مرتبط توسط قوه مقننه وبا همکاری قوه مجریه تصویب تا خلاءجدی پیش رو برداشته شود.

- واژگان کلیدی

محتوا ، فضای مجازی یا سایبر ،واسطه های الکترونیکی ، مسئولیت مدنی ،حمل کننده

[۱]دانشجوی دکتری حقوق خصوصی ،گروه حقوق، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران hr_alikarami@iau-arak.ac.ir

[۲]استادیار ،گروه حقوق، واحد اراک، دانشگاه آزاد اسلامی، اراک، ایران. (نویسنده مسئول) r_ahmadifar@yahoo.com

[۳]استادیار، گروه حقوق، دانشگاه ملایر، ملایر، ایران.

– مقدمه

امروز شـبکه های اجتماعی مختلف ازجمله فیس بوک facebook با حدود ۲/۸۷۰/۰۰۰/۰۰۰کاربر، you tube با ۱/۹۰۰/۰۰۰/۰۰۰ کاربر، whats app با ۲/۲۰۰/۰۰۰/۰۰۰ کاربر wechat با ۹۳۸/۰۰۰/۰۰۰ instagram با ۱/۸۰۰/۰۰۰/۰۰۰کاربر و دهها شبکه اجتماعی فعال دیگر زندگی جوامع انسانی را درگیر مباحث جدیدی نموده است که گویای ضریب نفوذ حیرت انگیز شبکه های اجتماعی فوق الذکر در امور فرهنگی ،اجتماعی ،اقتصادی ،قضایی و...دارد .

اسـتفاده از این شـبکه های اجتماعی به عنوان یک روند آغاز ، طی این سـالها به یک ابزار ضـروری در زندگی روزمره میلیون ها نفر تبدیل شـده و زمینه های آسـان برای برقراری ارتباط ،اشـتراک گذاری و انتشـار دیدگاه ها ،اخبار و اطلاعات را فراهم می کند .امروزه داده ها متنی یا بعبارتی محتوا به سـرعت در حال تبدیل شـدن به شاهرگ حیاتی ارتباط جهانی هستند در عصر داد ه ها و هوش مصنوعی همین متون یا محتوای در حال تبادل به عنوان یک فرصت و هم بعنوان یک تهدیدمطرح است که اگر در جایگاه تهدید قرار گیرد بی شک برای مقصران آنها مسولیت های مدنی در پی داشته باشد

مسـولیت های که با از بین رفتن قوانین حتما عارزه هایی بر جامه انسـانی و اقتصـاد در پی دارد و می تواند به اعتبار یک فرد یا موسسه آسیب جدی برساند

اشخاص حاضر در فضای سایبر شامل :

۱–واسطه های اینترنتی به مفهوم عام

۲–کاربران و بهره برداران نهایی خدمات اینترنتی

واسطه های اینترنتی به مفهوم عام عبارتند از:

الف }ارایه دهندگان خدمات اینترنتی fcp -servco که کاربران از طریق این گروه به فضای اینترنت دسترسی پیدا می کنند

ب }ارایه دهندگان خدمات میزبانی [اجاره فضا بر روی شبکه اینترنت جهت ذخیره اطلاعات بر روی سرور میزبان }

این گروه خود به دو بخش مستقل با مسولیت های مدنی متفاوت ایفای نقش میکنند

گروه اول تولید کنندگان و ارایه کنندگان محتوا در فضای مجازی است

گروه دوم مدیران و ارایه کنندگان سایت ها هستند

حال در این فضـای غیر فیزیکی عقل حکم میکند هر کس به دیگری ضـرری وارد کرد ملزم به جبران آن باشـد مگر در مواردی که ورود ضرر به دیگری بر حکم قانون باشد یا بر اساس عرف ضرری ناروا وارد نشده باشد

مسولیت های و ضررهای که کنشگران فوق در عرصه مجازی وارد میکنند چه ناشی از عمد باشد و یا غیر عمد ،اثار آنرا قانون معین میکند

- اهمیت و ضرورت انجام تحقیق

۱- در اهمیت پژوهش هایی از این دسـت همین بس که با اصـلی ترین پرسـش در حقوق یعنی توجیه به کارگیری قدرت الزامی دولت علیه اشـخاص آزاد و خودمختار و اشـخاص نسـبت به یکدیگر ارتباط دارد؛ پر س شی که نوعی فل سفه سیا سی و اخلاقی نیز ه ست .به ویژه اینکه به رسمیت شناختن قلمرو عمومی و خصوصی و حق ها و آزادی هایی که به شکل گیری آنها کمک می کند گاه با ارزش های دیگری چون امنیت که اقتدار دولتی و به دنبال آن حقوق کیفری دل مشـغول آنها نیز هسـت تزاحم پیدا می کند. این به معنای آن اسـت که اهتمام به مصـالح و منافع مربوط به قلمرو عمومی و خصـوصـی گاه با ارزش های دیگری تزاحم می نماید. حتی گاه میان ارزش ها و منافع مرتبط با هریک از این دوحوزه تزاحم پیدامی شـود. برای نمونه دفاع مطلق از حق بر حریم خصوصی و شخصی ممکن است به بخشی از فرایند گردش آزاد اطلاعات که لازمه وجود قلمرو عمومی جدای از دولت اسـت آسـیب برسـاند و بر عکس دولت به بهانه امنیت به حریم شخصی و گردش آزاد اطلاعات تجاوز و تعدی نماید .

۲- در نظام حقوقی و حاکمیتی ایران هیچ نهاد یا د ستگاه اجرایی م سولیت تدوین باید ها و نباید های ف ضای مجازی را نمی پذیرد لذا کنترل و نظارت بر محتوا بین سازمانها ،نهادها و وزارتخانه ها سرگردان و هیچ پاسخگوی قانونی وجود ندارد.

۳- ابداع دکترین نوینی که تنظیم کننده نظام حقوقی با فضای سایبر باشد چراکه با رشد چشم گیر فناوری اطلاعات شاهد دگرگونی همه فعالیت ها و تعاملات ان سانها در جامعه ه ستیم . خدمات اجتماعی ؛ اقت صادی ، بهدا شتی ، سیا سی با ا ستفاده از تکنولوژی های جدید حقوقی را بر هم ایجاد میکنند لذا لازم اسـت نخبگان حقوقی با نگاه فنی و مهندسـی بایدها و نبایدهای حقوقی جدیدی را تدوین کنند تا امنیت این فضـا را مضـاعف نمایند که اگر چنین نکنیم بی شـک هیچ کس نمیتواند با طیب خاطر به کسب و کار و تحصیل و تحقیق و حتی تفریح بپردازد)

- روش:

این پژوهش به روش آمیخته (ترکیبی) انجام شـده اسـت. در ابتدا با توجه به رویکردهای موجود در حیطه حمل و نقل محتوا و نظارت مطلوب بر آن در سـالیان گذشـته و مشـاوره با مسـئولین حوزه، شناخت و ضعیت کنونی و درک خلاهای موجود، ابعاد و مولفه های پژوهش شنا سایی و مطالعات این حوزه بصـورت فنی اهداف و چشـم انداز مطلوب مورد نیاز ترسـیم گردید که ماحصل آن ارائه راهکار حقوقی جهت کنترل و نظارت بر ایجاد کنندگان و متصدیان حمل و نقل

محتوا در فضای مجازی و تدوین مسولئیت آنها ست که در نهایت به شناخت شاکله ی اصلی مورد نیاز برای این موضوع منجر می شود .

– یافته ها:

فعالیت ایجادکنندگان و متصـــدیان حمل و نقل محتوا در فضـــای مجازی می تواند دربردارنده ضـررها و زیان های قابل توجه نسـبت به دیگران باشـد. ایجادکنندگان و متصـدیان حمل و نقل محتوا در فضـای مجازی تحت عنوان واسـطه های اینترنتی، امروزه از مهم ترین فعالان فضـای مجازی هستند که مسئولیت مدنی ناشی از فعالیت ها و اقدامات آن ها، بیش از پیش مورد توجه واقع شده است. لذا نیاز است شرح مدونی از قوانین این حوزه جهت بهبود عملکرد، شناخت مسئولیت ها و نظارت عالیه وضع گردد.

- **تعاریف ،انواع مسئولیت ها و تهدیدهای آن**

الف) تعریف:

به طور کلی «محتوای مجازی » یک مفهوم متنی اسـت که معانی مختلفی به صـورت صـوت ،تصـویر بسـته نرم افزاری و...را شامل می شودکه که به شکل فرا گیر یا غیر فراگیر تولید ،پخش ،عرضه ،انتشار،مدیریت ویا توزیع می گردد .

ب): انواع مسئولیت در محتوا

۱–مسئولیت ارایه دهندگان خدمات اینترنتی fcp -servco ها.

کاربران از طریق این گروه با استفاده از تجهیزات الکترونیکی به فضای اینترنت ورود پیدا می کنند در این زمینه حدو ۳۴شرکت در کل کشور خدمات مذکور را ارایه می دهند .

۲– مسئولیت **ارایه دهندگان خدمات میزبانی شامل اجاره فضا بر روی شبکه اینترنت جهت ذخیره اطلاعات بر روی سرور میزبان.**

ارایه خدمات پایدار اطلاعاتی ا ست که بر روی سرور میزبان قرار گرفته که برای ا شخاص قابل د سترسی ا ست این گروه از طریق ارایه دهندگان خدمات اینترنتی }رساها {به فضای سایبر دسترسی پیدا می کنند.

۳- مسئولیت تولید کنندگان و ارایه کنندگان محتوا در فضای مجازی

اقدام به تولید محتوا و اطلاعات و ذخیره آن در ف ضای مجازی می نمایند نوع داده شامل نرم افزارهای رایانه ای ،اسناد متنی و...می باشد .

ارایه کننده محتوا می تواند کاربر یا حتی ارایه کنندگان خدمات اینترنتی باشند مثل شرکتها مانند پارس آن لاین.

۴-مسئولیت مدیران و ارایه کنندگان سایت ها

این د سته اقدامی جهت ارایه محتوا در ف ضای مجازی نمیکنند اما با ایجاد سایت امکان بارگذاری و تخلیه محتوا را مدیریت می کنند مانند سایت فارسی آپارات

یاد آوری این نکته لازم ا ست که در تقسیم بندی جدید کمیسیون تنظیم مقررات و ارتباطات کشور فعالیت isp ها توسط fcpها و cerrucoساماندهی می گردد.

ج) تهدید ها :

۱- تهدیدات ناشی از اقتدارگرایی دولت‌ها و تمایل آن‌ها به کنترل ارتباطات شهروندان

یکی از موانع جدی در سلامت محتوای در حال تبادل در فضای سایبر شنود غیر مجاز ،جعل رایانه ای ،سرقت ،کلاهبرداری ،جاسوسی،نقض حریم اطلاعاتی و جرایم علیه عفت عمومی با سیستم های جدید می باشد

دولت ها به منظور و به بهانه امنیت جامعه بزرگترین ناقضان حریم شخصی محسوب می شوند بعد از حملات تروریستی از جمله حمله و حادثه ی یازدهم سپتامبر دولت ها به اینکه حامی حریم شخصی باشند یا امنیت جامعه ،به این نتیجه رسیدند که باید حامی امنیت جامعه باشند و عملا درفضای سایبرمحدودیت هایی را در پنهان آغاز نمودند .محدودیت هایی که با استفاده از تجهیزات و لوازم الکترونیکی کمتر قابل رویت می باشند.

۲-تفتیش و بازرسی محتوا

مجریان قانون به ویژه اپراتورها و بعضا مراجع اداری ،قضایی و انتظامی در مواردی خود ناقض و شکننده حرمت داده های الکترونیکی می گردد. مصداق بارز این نقض حق بازرسی و تفتیش محتوای افراد می باشد.
درعامل واقعی و غیرمجازی تفتیش و تجسس در امور و زندگی انسان ها شده است

اگر چه ضرورت‌های اجتماعی و امنیتی و بهدا شتی ایجاب می‌کند که بر اماکن عمومی‌و حتی گاه خ صو صی مانند مسکن نظارت‌هایی صورت گیرد اما این نظارت‌ها نباید از چهارچوب‌های اخلاقی و انسانی برون رود از این رو در نظام‌های حقوقی اکثر کشورها این حریم و موارد استثنایی آن به طور صریح مدون گشته است.

در به حرمت حقوق اشـخاص پرداخته هم حریم معنوی و هم حریم مادی را مدنظر قرار داده اسـت لذا حریم خصوصی معنوی را می توانیم از حقوق حقه اشخاص تلقی نمودکه تعرض در آن را منع نموده است .

با این وجود برخی موارد وجود دارد که نقض این حریم یا به وا سطه ی قوانین و ضعی که در مرحله عمل با این ا صل و مو ضوع در تعارض می با شند یا به وا سطه اعمال مجریان قانون نظیر نیروهای انتظامی یا وا سطه های الکترونیکی به مفهوم عام این حریم نقض می شود.

مانند : دوربین های مدار بسـته که در اماکن مختلف دولتی و غیر دولتی در همه جوامع نصـب شـده و علی رغم منع قانونی آن رد یابی و تفتیش مردم عملی متداول است.

اینگونه تفتیش و بازرسی در فضای مجازی نیز مصادیقی دارد با توجه به اصل ۲۵ قانون اساسی جای تامل دارد :

آنچه در این میان گم کشته و هیچگاه به تصویب نرسید قانون مندرج در این اصل و رکن نظام جمهوری اسلامی ایران است .

نمونه های از این قبیل در فضای فیزیکی در خ صوص تفتیش و بازر سی از خودروها وجود دا شت که تو سط هیات عمومی دیوان عدالت اداری در تاریخ ۱۳۸۰/۵/۲۸طی دادنامه‌ای به شـماره ۱۷۷ پیرو شـکایتِ شـخص حقیقی، بر غیرقانونی و غیر قابل ترتیب اثربودن بخشنامه نیروی انتظامی صادر نموده است .

۳-تعرض به محتوای اطلاعات

ماده ۷ قانون مرکز آمار ایران (۱۳۵۳) در ارتباط با حریم خ صوص داده ها، حاوی نکات قابل توجهی ا ست. این ماده تاکید دارد که اطلاعات اخذ شده نباید مورد سواستفاده به بهانه امنیت جامعه قرار گیرد

در عین حال آزادی اطلاعات و حق جامعه برای دانستن اخبار و اطلاعات گوناگون که یکی از مصادیق آن اطلاع بر زندگی ا شخاص ا ست میبا شد. لذا گاهی این دو حق با یکدیگر در تزاحم و تعارض قرار میگیرند. از یک سو حق فرد ا ست که ا سرارش مکتوم بماند و دیگران از آن اطلاع نیابند یعنی " ندانند " و از سوی یکدیگر جامعه حق آگاهی دارد یعنی "بدانند". جامعه حق دارد هرگونه مطلبی را خبری را در مورد اشـخاص جامعه چه افراد عادی چه سـیاسـی چه هنری بداند. ولی این حق ممکن اسـت با حق حریم شـخصـی و مصـونیت و آزادی در زندگی

خصوصی در تعارض واقع شود. در بسیاری موارد اطلاعات دیگران از اسرار شخصی فرد موجب سلب آسایش و امنیت میگردد".[۱]

در هر کشوری، حق برخورداری از حریم خصو صی ناگزیر می‌بایست با منافع دولت همخوانی دا شته با شد.به عنوان مثال دسترسی به اطلاعات پزشکی و بهداشتی افراد برای مهندسی خدمات پزشکی و ارتقای کیفیت زندگی

---

[۱] (فقیه،عباس،حریم خصوصی شهروندان،فقه وحقوق ارتباطات،پژوهشکدهباقرالعلوم،سالاول، ۱۳۸۹ص۱۵)

همواره مورد نیاز سیاستگذاران است. در حالی که بسیاری از مردم دنیا می‌دانند دولت اطلاعات شخصی آنان را گردآوری می‌کند، اغلب حق نظارت و سرکشی دولت را به رسمیت می‌شناسند. نکته مهم اینجاست که تحقیقات نشان می‌دهد این قوانین تا چه حد ضعیف و فاقد ضمانت اجرایی است. ضمن آنکه خلأها و نواقص بسیاری دارد و در کنار این همه، دولت را از نظارت و گردآوری اطلاعات افراد منع نکرده است.

۴-تهدیدات ناشی از فناوری های نوین از قبیل وسایل ثبت یا انتقال صوت وتصویر

بطور خلاصه مهم‌ترین عواملی که امروزه محتوا ارتباطات اشخاص بویژه حریم خصوصی اطّلاعاتی ایشان را به چالش طلبیده‌اند عبارتند از:

۱-بدافزارها : نوعی نرم افزاری مخرب است که در آن میتوان از هر فایل یا برنامه برای آسیب زدن استفاده کرد .

۲- باج افزارها نوعی بد افزا است که مانند یک مهاجم فایل های رایانه قربانی را قفل می کند .

۳-پایش توسط ناظران

۴- داده های مکانی

۵- پیشرفت چشمگیر دانش‌های مرتبط با تشخیص هویت و ویژگی‌های شخصیتی (شناسایی مشخصات از روی DNA، شبکه چشم، صدا، یک تار مو، دندان و...،).

موارد نقض یا دستکاری محتوا با فناوری‌های نوین عبارتند از :

۱. سرقت و افشای اطلاعات شخصی از طریق اینترنت

۲. رهگیری و توقیف نامه‌های الکترونیکی و ارتباطات اینترنتی

۴. استفاده از تراشه‌های میکرو الکترونیکی

۵-شنود و رهگیری مکالمات تلفنی

۶-هتک حرمت و حیثیت از طریق انتشارصوت وفیلم و نشراکاذیب ازطریق سیستم‌های رایانه ای.

۷- مشکلات اخلاقی جدیدو منحصر به فردی دراین حوزه ایجاد شده که نیازمند رسیدگی است

۸- مسدود یا مختل کردن محتوا

مهمترین مصادیق نقض محتوا در فضای مجازی عبارتند از:

۱- مزاحمت پیام های تبلیغاتی
۲- وجود کوکی ها (تنظیم گر)
۳- امحا داده شخصی
۴- داده های ترافیکی
۵- داده های مکانی
۶- نگهداری یا عدم نگهداری داده ها
۷- ربودن داده های متعلق به دیگری

در نظام حقوقی ایران مقررات مهم و مرتبطی با مسئولیت مدنی و داده های الکترونیکی {محتوا} به صورت مستقیم یا غیر مستقیم در فضای سایبر که مشتمل بر حمایت مدنی و کیفری نیز می باشد عبارتند از :

- قانون مسئولیت مدنی

- قانون مدنی ایران

- قانون برنامه چهارم، پنجم و ششم توسعه،

-قانون تجارت الکترونیکی ایران،(۱۳۸۴/۱۰/۲۴)،

-قانون جرایم رایانه ای (۱۳۸۸/۳/۵)،

و...

الف -قانون اساسی

۱- اصل بیست و پنجم که بسیار شفاف هرنوع تفحص در دنیای نوین ارتباطی را منع نموده است.
باتوجه به تکنولوژی های جدید شامل اکثر محتواهای مبادله شده در فضای مجازی ، ایمیل ها و ... ارسالی میشود یا نمیشود جای تامل است
مضاف آنکه امروز" مگر به حکم قانون" به شنود مجاز تلقی شده که خود بابی برای نقض حریم انسانها شده است.

۲-اصل بیست و دوم قانون اساسی ، اگرچه در این اصل زندگی خصوصی افراد محفوظ نگه داشته شده است لیکن "در مورد این اصل گفتنی است که: کلمه مال و حقوق ، جای تفسیر و تعریف دارد. داده های الکترونیکی افراد در فضای مجازی را هم می توان یکی اموال و حقوق افراد در نظر گرفت.

۳- اصل بیست و چهارم این اصل نیز حقوق انسان ها را محفوظ دانسته است اما باقید کل تفصیل آن را محدود نموده است
در این اصل بیان شده شریات در بیان مطالب آزادند حال آنچه در فضای مجازی منتشر میشود بی شک از حمایت قانون برخوردارند

۴- سایر اصول ق. مانند اصول ۳۲-۳۴-۳۶-۳۷-۳۸-۳۹نیز به صورت غیر مستقیم بر حفظ حریم اشخاص تاکید دارد .

ب –لوایح یا قوانین و مقررات خاص:

منظور از مقررات در اینجا قوانین و مصوباتی است که در سال‌های اخیر با هدف قانونمند کردن استفاده از فناوری های نوین اطلاعاتی و ارتباطات در کشور تدوین شده است. در نظام حقوقی ایران در چند سال اخیر قوانین مهم و مرتبط با محتوای در حال مبادله در فضای سایبر که مشتمل بر حمایت مدنی و کیفری نیز می باشد عبارتند از :

– مصوبات کمیسیون تنظیم مقررات –مقررات و ضوابط شبکه اطلاع رسانی.– قانون برنامه چهارم ،پنجم و ششم توسعه– قانون تجارت الکترونیکی ایران،(۱۳۸۴/۱۰/۲۴)– قانون جرایم رایانه ای (۱۳۸۸/۳/۵)– مصوبات شورای عالی فضای مجازی –دستور العمل حقوق شهروندی در قانون مجازات اسلامی نیز موادی مرتبط با مباحث مقاله وجود دارد:

لایحه حکمرانی الکترونیکی که توسط پژوهشگاه قوه قضاییه ، دانشگاه علم و فرهنگ و سازمان فن آوری اطلاعات ایران مشتمل بر:امور سیاست گذاری الکترونیکی ، اموراجرایی الکترونیکی ، اموردادرسی الکترونیکی ،تعامل الکترونیکی ، شیوه اطلاع رسانی ، نیازمندی های حکمرانی الکترونیکی ، تصدی حکمرانی الکترونیکی ، حقوق و تعهدات متصدیان ، بهره برداران حکمرانی الکترونیک ، مسئولیت و ضمانت اجراها ، مسئولیت مدنی تهیه و درحال طی مسیر مراحل قانونی است .

لایحه ی حمایت از داده و حریم خصوصی درفضای مجازی که مشتمل بر :

۱- تعاریف داده یشخصی ، پردازش ،ایجاد داده کنترل گر،فضای عمومی مجازی

۲–پردازش مجاز داده های شخصی

۳– ایجاد پردازش و استفاده از داده ای شخصی حساس، تکالیف کنترل گر

۴– نهاد نظارت کننده بر اجرای صحیح مقررات

۵– ضمانت اجرا: که این هم درحال طی مراحل قانونی است

ج)مبانی فقهی :

عدم تعرض به نوشتجات ، مکاتبات ،مراسلات ، صوت و تصویر اشخاص از ابتدایی ترین حقوق همه انسان از جمله دامنه عدم تجاوز و حفظ و حرمت اشخاص که مورد توجه آیات و روایات قرآنی قرار گرفته است :

– سوره نساء تاکید دارد به: ان الله یامرکم اتود و الامانات الی اهلها

همانا خداوند به شما دستور می دهد امانت ها را به اهلش بر گردانید .

این آیه تاکید دارد اگر مالی نزد کسی به امانت سپرده می شود شرعا و عقلا امین باید ضمن رعایت امانت آنرا به صاحبش باز گردان.

نکته قابل تامل اینستکه واسطه های اینترنتی به مفهوم عام خود که شامل ispها و ارایه کنندگان خدمات میزبانی هستند تا چه اندازه امین بودن خود را حافظ هستند و این حکم شرعی و عقلی را چه اندازه جامعه عمل می پوشانند.

همچنین درسوره نور میخوانیم

«یا ایهالذین آمنوا لاتدخلو بیوتاً غیر بیوتکم حتی تستانسوا و تسلموا علی اهلها»

که بیانگر عدم ورود غیرمجاز به منازل یکدیگر است

مبحث اصلی مد نظر اینستکه وقتی شارع مقدس تاکید به اذن ورود به غیر منزل خود را واجب کرده است آیا کاربران و بهره بردارن از فضای مجازی یا مدیران ارایه کنندگان سایت ها بدون اجازه به محتویات در حال مبادله و انتقال سرکشی نمایند.

اگر واسطه های اینترنتی به مفهوم عام در داده های در حال انتقال و مبادله تجسس نمودند مرتکب گناه نشده اند آیه شریفه ۱۹سوره مبارکه نور

"کسانیکه پخش کردن و شهرت دادن کار بد در بین مومنان را دوست دارند در این دنیا و سرای دیگر برای آنها عذاب درد ناک است "

حال اشخاص حاضر در فضای مجازی اعم از واسطه ها اینترنتی ،تولید کنندگان ،ارایه کنندگان یا عرضه کنندگان ،پخش کنندگان ،مدیران سایتها و در نهایت کاربران نهایی واقعا در شهرت دادن کار بد فعال هستند یا خیر .

ارکان و عناصر تشکیل دهنده :

❖ **۱-رکن مادی**

❖ شیوه ها و طرق دسترسی غیرمجاز؛ شیوه های دسترسی غیر مجاز را می توان به شیوه های فنی، (برخی از این شیوه ها عبارتند: از طریق ا سب های تراوا (Trojan)، کرمها و شیوه های غیر فنی (شامل شیوه های مبتنی بر دانش مهندسی اجتماعی، برقراری ارتباط دوستانه با مدیر سیستم جعل عنوان، نشان دادن خود به جای کاربر مجاز و...) تقسیم نمود. در ادامه به شرح این شیوه ها می پردازیم.

ا سب های تراوا برنامه هایی هستند که هیچ آ سیبی به کامپیوتر شما نمی‌ر سانند اما این برنامه های به ظاهر بی خطر با حمل کردن یک برنامه جانبی تمام اطلاعات شما را به راحتی سرقت می کنند. البته این برنامه ها هنگامی که باز نشده اند کاری نمی توانند بکنن ولی چون به همراه یک نامه الکترونیکی ارسال می شوند و پیغام های وسوسه کننده

ای دارند شخص را مجبور به باز کردن نامه می‌کنند. از مهمترین این برنامه‌ها می توان به Sub seven اشاره نمود. مثلا این گونه برنامه ها می توانند در قالب یک بازی مهیج رایانه ای ارائه شوند که بعد اینکه فرد آنها را دریافت نمود و شروع به بازی نمود آنها کار خود را شروع کرده و به اطلاعات او را به سرقت می برند. کرمها نوع دیگری از برنامه های تخریبی هستند یعنی هدف اصلی آنها تخریب اطلاعات شخص دیگر است این برنامه ها بدون آنکه ردپایی از خود باقی بگذارند از کامپیوتری به کامپیوتر دیگر می روند. طرز کار کرمها مانند ویروسها می باشد یعنی هردو آنها از میزبان استفاده می‌کنند و میزبان کرم‌ها معمولا سندهای Word یا Excel می باشند که با جا به جا کردن سندها کرمها نیز جا به جا می شوند.

IP : اگر فایلی به پسوند exe را باز کنید و نمیدانید چیست، IP شما رایانه ی شخصی فرستنده فایل، فرستاده می شود و با این کار شما به هکر کمک زیادی کرده اید. در حقیقت هکر می تواند به راحتی از طریق IP شما به رایانه مورد ا ستفاده شما د ستر سی یابد و اقدام به انجام هر کاری (از قبیل پاک کردن فایل، دزدیدن فایل، فرستادن ویروس و ...) کند.[۲]

عنصر مادی بزه شنود غیر مجاز براساس قانون جرایم رایانه ای متشکل از پنج جزء دانست که برای تحقق بزه،جمع این اجزاء یا شروط لازم و ضروری است.

[۲] روشهای دست یابی به اطلاعات دیگران و نابود کردن آنها، قابل دسترسی به سایت:
http://sakhi54.parsiblog.com/Posts/629

اولا: مو ضوع جرم داده در حال انتقال ا ست و شامل داده های ایستا یا ذخیره شده نمی شود. ذکر «محتوای در حال انتقال» به لحاظ این اســت که محدوده ی جرم شــنود غیر مجاز از ســایر جرایم مشــابه جدا شــود. بنابراین چنانچه شنود به صورت غیرقانونی انجام پذیرد م صداق ماده ۲ قانون مذکور نبوده و م شمول ماده ۱ این قانون است.[۳]

ثانیا: در حال انتقال باید در یک ارتباط محرمانه و غیر عمومی شنوده شود و گرنه اگر ارتباط به صورت عمومی و آزاد باشــد عمل مرتکب مباح خواهد بود. ارتباطات غیرعمومی ارتباطاتی هســتند که همگان مجاز به ورود یا دسترسی به آنها نمیباشند. در حالی که ارتباطات عمومی ارتباطاتی هستند که فلسفه ی وضع آنها اطلاع رسانی به مردم بوده و منعی برای د ستر سی همگان به آنها وجود ندارد. ثالثا: مو ضوع جرم، محتوا ا ست که قانون گذار به جهت درک معنا و مفهوم قابل تشخیص، از این تعبیر به جای داده استفاده کرد.[۴]

رابعا: و سیله جرم در کنار سامانه ها،امواج الکترومغناطیسی نیز هستند که این تاکید به جهت قابلیت حمل محتوا از سوی امواج هستند و غیر این موارد شامل ماده ۲ نخواهد بود. به عنوان مثال، چنانچه شخصی صحبت دو نفر را از کنار آیفون منزل ب شنود و یا به طور عادی صحبت دو نفر را ا ستراق سمع کند، نمیتوان اقدام اورا م شمول ماده ۲ دانست. در واقع این ماده سعی کرده است شنود غیر مجاز ارتباطات الکترونیکی معمول در سطح گسترده یا مهم را در برگیرد.[۵]خامسا: رفتار فیزیکی جرم، شنود است که نه تنها شامل دریافت اطلاعات نیز می گردد بلکه نشان می دهد که شنود همچون دسترسی غیرمجاز جرمی مطلق بوده و نیازی به تحقق نتیجه نیست .[۶]

۲-رکن معنوی

دسترسی غیر مجاز از زمره جرایم عمدی تلقی می شود. انگیزه نیز در دسترسی غیر مجاز، بدون اینکه تأثیری در ماهیت جرم دا شته با شد، مختلف و متنوع می با شد. ق صد مجرمانه: با توجه به اینکه د ستر سی غیر مجاز جرمی مــــــــــــطــــــــــــلــــــــــــق مــــــــــــحســــــــــــوب می شــود و مقید به هیچ نتیجه ای نمی باشــد، هیچ قصــد خاص و ویژه ای نیاز ندارد به همین دلیل برای تحقق عن صر معنوی تنها سوء نیت عام کفایت می کند. مرتکب می بای ست عامدا و عالما مرتکب د ستر سی غیرمجاز شود. انگیزه مجرمانه: این انگیزه ها را می توان شامل انگیزه های شرافتمندانه مانند: بالا بردن امنیت سیستم ها، مراقبت از سیستم ها در برابر آ سیب، کمک به پی شرفت دانش فنی و مهند سی و ... و غیر شرافتمندانه شامل: غرض ورزی و انتقام جویی، کسب شهرت، انگیزه های مالی، حسادت و ... دانست. شایان ذکر ا ست که انگیزه

---

[۳] امانی، حمیدرضا، "بررسی ابعاد کیفری شنود غیر مجاز در عرصه فن آوری اطلاعات و ارتباطات"، صفحه ۱۹، قابل دسترسی در سایت:
http://www.maavanews.ir/tabid/38/ctl/Edit/mid/384/Code/6665/Default.aspx

[۴] (پاکزاد، بتول، "تروریسم سایبری"، رساله دکتری، دانشگاه شهید بهشتی، ۱۳۸۸)

[۶] (پاکزاد، بتول، "تروریسم سایبری"، رساله دکتری، دانشگاه شهید بهشتی، ۱۳۸۸)

های یاد شده هیچ تأثیری در ماهیت جرم ندارد و در نهایت ممکن است به عنوان عاملی تخفیف دهنده محسوب شود.[۷]

دسترسی غیرمجاز طبق مقررات ایران دارای شرایطی است: دسترسی غیرمجاز، جرمی است که عموما توسط افراد برنامه نویس و متخصص در علوم رایانه ای ارتکاب می یابد. جرمی با ماهیت کاملا تکنیکی و فنی است و در میان جرائم رایانه ای از جمله جرائم رایانه ای محض تلقی می شود. زیرا اولا، از جرایم مرتبط با سیستم های رایانه ای ا ست و ثانیا، تنها در محیط سیستم های رایانه ای و سایبر، در تقسیم بندی های سنتی از جرایم می توان آن را از زمره جرایم علیه اموال محسوب داشت. همچنین جرمی است عمدی، آنی، مطلق، غیر مشهود.

جرم شنود مانند هر جرم دیگری نیاز به رکن معنوی دارد که رکن معنوی آن را سوء نیت به معنای عمد تشکیل می دهد. در عبارت ماده ۲جرایم رایانه ای قانون مذکور آمده است:«هر کس به طور مجاز محتوای ... را شنود کند ... .» غیر مجاز فعل «شنود کند» به فردی که به صورت غیر عمدی در جریان خبری قرار می گیرد نسبت داده نمی شود جرم شنود غیر مجاز نیاز به قصد سو دارد به عبارتی شخص باید قصد انجام فعلی را داشته باشد که قانون گذار آن را ممنوع دانسته و این همان سوء نیت

عام است. بنابراین ماده ۲ در صورتی قابلیت اعمال را دارد که شخص از روی علم و عمد مرتکب جرم شده باشد؛ اما سوء نیت خاص در ارتکاب جرم مذکور ضروری نیست. اگر چه دربسیاری موارد ارتکاب جرم با منظور خاصی صورت می گیرد، مانند ضربه زدن به دیگری؛ اما به صرف احراز سوء نیت عام جرم مذکور تحقق یافته تلقی می شود. تشخیص مرز بین خطا و عمد در بحث شنود نیز حایز اهمیت است

مبانی داده ها الکترونیکی در اسناد بین المللی

از جمله اسناد بین المللی مهم پایه گذار حمایت از حریم شخصی عبارت اند از :

۱- مجمع عمومی سازمان ملل با تاکید و تایید حق حریم خصوصی انسان ها که بر اساس آن هیچ شخصی نباید مورد نقض حریم شخ صی قرار گیرد از ۱۸ د سامبر ۲۰۱۳ در قطعنامه ۶۸/۱۶۷حق حریم خ صو صی در ع صر دیجیتال را به ر سمیت شناخت با تاکید براینکه نظارت وا ستراق خود سرانه و غیرقانونی مکاتبات و جمع آوری خود سرانه و غیرقانونی اطلاعات شخ صی به عنوان اقداماتی مداخله جویانه منجر به نقض حریم خ صو صی و آزادی بیان و عقیده شده و با اصول دموکراتیک در تضاد است و برحفظ حریم اشخاص تاکید دارد

۲-قانون حفاظت از داده ها مصوب ماه می ۲۰۱۶اتحادیه اروپا .

این مقررات جدید به انتقال گسترده اطلاعات شخصی در سرتا سر جهان و مخاطرات امنیت داده ها مباحث نوینی را مطرح کرده است از جمله آنکه داده ها بدون رضایت صریح یا مبنای قانونی نباید مورد پردازش توسط حکومت ها قرار گیرند .

۳- دستورالعمل ۹۷/۶۶ پارلمان اروپا:

[۷] (تحری، فرزاد، "دسترسی غیر مجاز جلوه ای از جرم های رایانه ای نوین" ، مجموعه مقالات همایش بررسی جنبه های حقوقی فناوری اطلاعات، معاونت حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضاییه و انتشارات سلسبیل، چاپ نخت،۱۳۸٤، صفحه۱۹۰)

پارلمان اروپا و شورای ۲۴ اکتبر ۱۹۹۵ درمورد حمایت از افراد در رابطه با پردازش اطلاعات شخصی و در مورد جابه جایی آزاد داده ها ، کشـورهای عضـو را مکلف می کند تا حقوق و آزادیهای اشـخاص حقیقی در رابطه با پردازش اطلاعات شـخصـی به ویژه حق آنها برای حفظ حریم خصـوصـی را به منظور اطمینان از جریان آزاد اطلاعات شخصی در جامعه تضمین کنند.

۴- دستورالعمل EC/۴۶/۹۵ پارلمان اروپا:

این د ستورالعمل بر پردازش اطلاعات شخصی و حفاظت از حریم خ صو صی در بخش ارتباطات تاکید دارد و اعلام می نماید شبکه های ارتباط عمومی باید مقررات خاص حقوقی ، فنی نظارتی به منظور رعایت از حقوق و آزادی های اساسی اشخاص حقیقی و منافع شروع آنها تلاش نمایند

۵- دولتهای آلمان ، فرانسه ایرلند ، هلند بعد از اخطار کمیسیون اروپا

بعد از اخطارکمیسیون اروپایی در وهله ی اول متعد به ایجاد شرایطی شدند که در آن بالاترین سطح حمایت از حریم خصـوصـی اشـخاص در ارتباطات الکترونیکی اعمال نمایند و دیگر آنکه از پردازش خودسـرانه داده های درحال انتقال خودداری و برحمایت از آن جدی تر باشند و اگر پردازش برداده ها دارند صرفا بر اساس معیارهای دول عضو عمل کنند.

علیرغم وجود ا سناد متعدد بین المللی در خ صوص حفظ و حمایت از حرمت ا شخاص اکنون این سؤال ممکن ا ست مطرح شود که آیا این حق یا حرمت از جمله حقوقی ا ست که صرفا در معاهدات و ا سناد بین المللی به رسـمیت شـناخته شـده و اعتبار قراردادی دارد و یا اینکه می توان ادعای عرفی شـدن آن را نیز داشـت؟ در این خصوص باید اذعان کرد که اگرچه این حق در اسناد معدودی مورد توجه قرار گرفته است، لیکن اگر آنرا یکی از اصول بشری تصور کنیم و حقوق و اصول بشری را به عنوان یک مقوله بین المللی عرفی که جنبه ی الزامی دارد، نتیجتا حق حریم خصوصی نیز اعتبار عرفی پیدا کرده و در قلمرو حقوق بین الملل جای خود را پیدا کرده است.

۷-مصوبات اتحادیه جهانی مخابرات itu

اتحادیه جهانی مخابرات از مهمترین ارکان تقنینی مباحث ارتباطی در جهان می با شد که علی الا صول مصوبات آن تو سط اع ضاء اجرا میگردد این اتحادیه متولی تدوین مقررات ارتباطی و فناوری اطلاعات می با شد.در حوزه استاندارد سازی اتحادیه جهانی مخابرات و گروه مطالعاتی sg17امور مربوط به امنیت را هماهنک میکند یکی از توصیه نامه های مهم آن ITU-TX.509برای احراز هویت الکترونیکی است

مبانی کلی مسئولیت واسطه های الکترونیکی

تقصیر بر اساس قانون مدنی ما اعم از افراط و تفریط است

تفریط یعنی کاری بیش از حد متعارف انجام شود و افراط یعنی انجام ندادن کاری در حد متعارف .

تقصیر یا بی احتیاطی درماده ۹۵۳ قانون مدنی ایران تعریف شده. «تقصیر اعم است از تفریط تعدی»

ودر ماده ۹۵۱ «تعدی» چنین تعریف کرده است : «تعدی: تجاوز نمودن از حدود اذن یا متعارف است نسبت به مال یا حق دیگری»در ماده ۹۵۲ ق. م «تفریط نیز تعریف شده است.

لذا حاملان پیام درصورتی مسؤول هستند که محقق شود مرتکب کاری شده اند که اگرکسی در آن شرایط قرار می گرفت نمی توانست آنرا انجام دهد .

قانون مسئولیت مدنی بر قبول مسؤولیت ناشی از تقصیر تاکید دارد در نتیجه عنصر لازم برای مسؤولیت واسطه ها تقصیرا ست .درماده ۷۸ قانون تجارت الکترونیکی تاکید دارد چنانچه ارتباط با سیم یا همان فیزیکی اگر قطع بشود و ضرری متوجه کسی شود باید جبران گردد.لذا اگر معین شود ورود خسارت به جهت نقصان در وسایل مخابراتی بوده است به عنوان تقصیر تلقی نموده واسطه الکترونیکی باید امکانات سیستمی مناسبی را برای جلوگیری از ورود خسارت فراهم نماید،

درخصوص مبانی کلی مسئولیت ناشی از عدم حرمت محتویات در فضای مجازی می‌توان گفت امروزه نظریه تقصیر به عنوان اصل پذیرفته شده است. به طوری که امروزه در بحث از مسؤولیت اینگونه اشخاص به عنصر اصلی «تقصیر» یا « بی احتیاطی» توجه می شود. شاید بتوان گفت در دکترین حقوقی موجود و احکام قضایی و نوشتجات حقوقی منتشره در بحث از مسؤولیت مدنی واسطه های الکترونیکی در اکثر کشورها مسؤولیت این اشخاص را تحت عنوان «مسؤولیت ناشی از تقصیر» یا «بی احتیاطی» مطرح می کنند. دلیل اعمال نظریه تقصیر در خصوص مسؤولیت اینگونه اشخاص به نقش و جایگاه واسطه های الکترونیکی بر می گردد. علی الاصول کسانی که نقش واسطه در انجام یک کاری را به عهده دارند فاقد مسؤولیت محض می باشند. در نظام حقوقی ایران اشخاصی همانند مشاورین املاک ، نمایندگان موسسات ، دلالها و همچنین متصدیان حمل و نقل که واسطه انجام کار می باشند، امین شناخته شده و اگر تقصیر داشته باشند مسؤول شناخته می شوند.

در خصوص واسطه های الکترونیکی نیز مسؤولیت مبتنی بر تقصیر به عنوان اساس کار شناخته شده است. زیرا جایگاه قانونی واسطه ها به بروز ضرر برمیگردد. چون که اصولا یک عمل زیانبار ممکن است به صورت مستقیم یا غیر مستقیم باشد.

۱-فعالیت واسطه ها به عنوان حمل کننده عمومی

واسطه های الکترونیکی به معنای عام یعنی ارائه دهندگان خدمات اینترنتی (Isp)ها و تامین کنندگان خدمات میزبانی تنها فعالیت واسطه ای در انتقال و ذخیره داده های اشخاص را بر عهده داشته و بر محتوای اطلاعات مورد مبادله کنترل و نظارتی ندارند. لذا علی الاصول نبایستی مسئولیتی به جهت چاپ و درج مطالب اهانت آمیز یا اطلاعات غلط و مانند آن متوجه ispها باشد. مگر در مواردی که از محتوای غیر قانونی اطلاع داشته یا می بایستی اطلاع می داشته اند و یا در صورتی که در چاپ و درج محتوای اطلاعات مباشرت یا مشارکت داشته باشند. که در حالت اخیر به عنوان «چاپ کننده» ممکن است مسئول باشد

«توزیع کننده در واقع آخرین مرحله از فعالیت اطلاع رسانی و فرایند تولید آثار فناوری اطلاعات و ارتباطات برای مصرف آن توسط کاربران را کامل می کند. چرا که آثار تولیدی سایر اشخاص نظیر مقالات علمی، سیاسی، مذهبی و نیز نرم افزارهای رایانه ای و تصاویر و عکس ها و مانند آنها را به دست کاربران به عنوان مصرف کنندگان اینگونه محصولات می رساند.

ارایه کنندگان خدمات ممکن ا ست به صورت تجاری فعالیت نمایند، به این صورت که مجوز لازم را با طرفیت مشـــخص با توجه به تعداد کاربران احتمالی مورد ســـرویس خود از اپراتورهای مخابراتی اخذ نموده و امکان دسترسی به اینترنت را در قبال اخذ وجه به کاربران خانگی و مشترکان تجاری قرار دهد ".[۸]

۲-- وظیفه واسطه ها در نظارت بر محتوا

آیا موســـســـه حمل کننده عمومی وظیفه کنترل و نظارت بر محتوای داده ها را دارد یا خیر؟ این ســـوال در مورد کنشـگران بخش ict خصـوصـا fcpها و serucoکه متولی انتقال مکالمات و پیام‌های تلفنی مطرح اسـت. آیا وا سطه های الکترونیکی که متولی کلیه امور مربوط به انتقال پیام‌های متنی ، صوتی ،تـصویری یا تلفیقی از آنهادر تلفن همراه هسـتند دارای مسـئولیت می باشـند و دارندگان پروانه فعالیت از سـازمان تنظیم مقررات وارتباطات رادیویی مرســـوم به اپراتور همراه اول و یا کمپانی هایی مانند شـــرکت ایرانســـل و رایتل تکلیف به نظارت بر محتوای پیامهای کوتاه(mmc-SMS) ارسالی مشترکان خود را دارند یا خیر؟

"شـرکتهای ارائه دهنده خدمات نبایسـتی بر محتوای پیامهای ارسـالی آنها نظارت نمایند. در قوانین موضـوعه کشورهای مختلف رهگیری پیام های الکترونیکی ممنوع است. اصل ۲۵ قانون اساسی ایران بازرسی و فاش کردن مکالمات تلفنی و استراق سمع و هر گونه تجسس را جز به حکم قانون ممنوع اعلام داشته است. ماده ۵۲۸ قانون مجازات اسلامی نیز تاکید بر این موضوع دارد .

بنابراین نه تنها وظیفه ای برای دستگاه‌ها و موسسات ذیربط از جمله موسسات حمل کننده عمومی نظیر شرکت مخابرات، شرکت پست و ispها وسایر اپراتورها مبنی بر نظارت بر محتوای مراسلات مکاتبات، مکالمات، پیام های مشتریان پیش بینی نشده بلکه هر گونه تجسس و پایش در این خصوص نیز جرم تلقی شده است و فقط در مواردی که مقام قضایی یا قانون مجوز لازم را صادر نماید مجاز به آن هستند "[۹]

۳- عدم تکلیف بر نظارت بر محتوا

در دنیای واقعی و فیزیکی ناشران به انچه نشر میکنند باید نظارت صد در صدی و کنترل متنی داشته باشند ولی در دنیای مجازی و سـایبر حال و هوای دیگری یا بعبارتی باید و نبایدهای دیگری حاکم اسـت که نقش هر یک نیز با دیگری متفاوت ا ست و در این میان مسئولیت هر یک نیز با دیگری متفاوت ا ست . اگر وا سطه ها ،تامین کنندگان و مدیران سایت ها بتوانند و یا مجاز به بررسی و شنود مکالمات اعم از صوتی و غیر صوتی گردند بی شک به حریم خصوصی اشخاص ورود کرده و این خود بابی خواهد شد بر نقض حریم انسانها .

"واســـطه های الکترونیکی اصـــولاً نقش ناشـــر را در فرایند پردازش داده ها و مبادلات و ارتباطات الکترونیکی نداشـته و در این رهگذر عموماً یا واجد وصـف حمل کننده عمومی هسـتند و آن در مواردی اسـت که گیرنده انتقال اطلاعات شخص معین بوده و یا واجد نقش توزیع کننده اطلاعات به اشخاصی غیر از فرستنده می باشند. در هر دو وصف مزبور نیز ا صولاً در نظام های حقوقی کشورهای مختلف، وظیفه نظارت و کنترل بر محتوی را بر عهده واســـطه الکترونیکی قرار نداده بلکه حتی در بســـیاری موارد همانند قوانین مربوط به حمایت داده یا ارتباطات الکترونیکی بی سیم و با سیم، واحدهای ارائه دهنده خدمات دسترسی و برقرار کننده ارتباط از هر گونه

---

[۸] حسین صادقی

[۹] حسین صادقی

تجسس، پایش و استراق سمع ممنوع شده اند.تاکیدات مبین ممنوعیت هر گونه استراق سمع ، شنود و پایش غیرمجاز از مکالمات تلفنی، مکاتبات و مراسلات است. لذا به عنوان قاعده کلی می توان گفت واسطه های ارتباط پستی و مخابراتی نه تنها مکلف به نظارت بر محتوای مکالمات و نامه ها و مراسلات مشتریان نمی باشند بلکه از انجام این کار ممنوع می باشند. در خصوص ارتباطات اینترنتی قوانین موضوعه حکم صریحی ندارند".[۱۰]

[۱۰] حسین صادقی

نتیجه‌گیری

علی‌رغم آنکه مطالعه تاریخی نشـان می‌دهد که مسـئله حریم خصـوصـی کم و بیش در همه جوامع مطرح بوده ا ست، اما دغدغه حمایت از حریم خ صو صی از دغدغه‌های جدی جوامع امروز و زاییده تحولات مختلف سده اخیر است که در همه جوامع به وقوع پیوسته و درحال توسعه است که از جمله مهمترین این تحولات، توجه به حفظ حریم انسان ها مضاعف شده است تحولات علمی و فناورانه نیز همزمان شده و اهمیت حفظ و صیانت از حریم خصوصی را اهمیتی دو چندان بخشیده است. به طورکلی با تعریف حریم خصوصی و مباحث پیرامون آن، باید اذعان داشت که مشمول حریم و خلوت انسان ها روز به روز مشخص تر می گردد.

انسان‌ها می‌توانند برخی از فعالیت های اجتماعی خود را در زمره حریم شخصی خود قلمداد کنند وآن را حریم خصوصی خود اعلام کنند.

خصوصیات و ویژگی فضای مجازی، مقتضی نظام حقوقی خاصی در ارتباط با مسؤولیت در این حوزه اسـت، اما این بدین معنی نیسـت که نظام مسـؤولیت مدنی در فضـای مجازی به کلی متفاوت از نظام مسؤولیت در جهان واقعی باشد لذا برای تبیین مبانی مسؤولیت در حوزه فضای مجازی و مسـؤولیت واسـطه های اینترنتی، ابتدا باید مبانی سـنتی مسـؤولیت مدنی را مورد شناسایی قرار داد.تا با بهره گیری و انطباق با عالم سایبر نسبت به تعریف و ضوابط جدید و باید و نباید آن مسئولیت مدنی در فضای سایبر گاهی موثر در دنیای مهندسی و حقوقی حادث گردد.

منابع:

۱- قرآن مجید آیه های نور ،نساء و حجرات

۲- قانون مجازات اسلامی

۳- قانون جرایم رایانه ای

۴- فقیه،عباس،حریم خصوصی شهروندان،فقه وحقوق ارتباطات،پژوهشکدهباقرالعلوم،سالاول، ۱۳۸۹ص۱۵

۵- روشهای دست یابی به اطلاعات دیگران و نابود کردن آنها، قابل دسترسی به سایت:
http://sakhi54.parsiblog.com/Posts/629

۶- امانی، حمیدر ضا، "برر سی ابعاد کیفری شنود غیر مجاز در عر صه فن آوری اطلاعات و ارتباطات"، صفحه ۱۹، قابل دسترسی در سایت:
http://www.maavanews.ir/tabid/38/ctl/Edit/mid/384/Code/6665/Default.aspx

۷–صادقی حسین مسولیت مدنی واسطه ها و تامین کنندگان خدمات ارتباطات فصلنامه مطالعات حقوق خصوصی دوره ۴۰شماره۲ ،

۸–تحری، فرزاد، "دسترسی غیر مجاز جلوه ای از جرم های رایانه ای نوین" ، مجموعه مقالات همایش بررسی جنبه های حقوقی فناوری اطلاعات، معاونت حقوقی فناوری اطلاعات، معاونت حقوقی و توسعه قضایی قوه قضاییه و انتشارات سلسبیل، چاپ نخت،۱۳۸۴، صفحه۱۹۰

۹– احمدی، احمد،« سوءاستفادهازحق،نشراطلاعات،چاپ سوم،۱۳۷۷، ص۲۰

۱۰– گزارشات سازمان تنظیم مقررات و ارتباطات رادیویی www.cra.ir