محدودیت‌های دسترسی به اطلاعات در اینترنت

تاریخ دریافت: ۸۹/۵/۹ تاریخ تأیید: ۸۹/۱۱/۲۷

سیداحمد حبیب‌نژاد*
عبدالله عصّاره**

چکیده

عصر انفجار اطلاعات و پیشرفت‌های الکترونیکی مصادیق حق دسترسی به اطلاعات را به عنوان یکی از نتایج حق آزادی بیان، توسعه بخشیده است. آزادی بیان مستلزم آزادی در جستجوی فعال اطلاعات، از منابع آن است و اشخاصی که از حق آزادی بیان برخوردارند؛ باید از حق دسترسی به اطلاعات نیز برخوردار باشند و لذا آزادی اطلاعات را باید مقدمه و لازمه تضمین آزادی بیان دانست. پهنه گسترده اینترنت، محدوده آزادی بیان و اطلاعات را تا حدود زیادی گسترش داده و فضای بی‌انتهایی برای نشر اطلاعات و اخبار فراهم آورده است. یکی از دغدغه‌هایی که همراه با روند همه‌گیری این پدیده در عالم ایجاد شده است، مسئله نظارت‌ناپذیری و تا حدودی عدم کنترل محتوای آن است. چرا که هر شخصی می‌تواند مطالبی را بر صفحه وب قرار دهد که این محتوا مخاطبانی میلیونی بیابد. از سوی دیگر برخی از اندیشمندان غربی با تأکید بر تئوری‌های لیبرالیستی معتقدند که موضوع فیلترینگ اینترنت در تقابل با حق آزادی بیان قرار دارد و البته برخی دیگر نیز، از اندیشه‌ای خلاف این نظریه، جانبداری می‌کنند. موضوعات مختلفی همچون حفظ اخلاق عمومی، امنیت ملّی، حریم خصوصی و ... سبب شده است تا دولت‌ها مجاب شوند که باید به‌طور جدی به مقوله پالایش وب بپردازند.

واژگان کلیدی: *آزادی بیان، حق دسترسی به اطلاعات، فیلترینگ، حریم خصوصی.*

* دانشجوی دکتری حقوق عمومی واحد علوم تحقیقات تهران، دانشگاه آزاد اسلامی (a_habib84@yahoo.com).
** کارشناسی ارشد حقوق عمومی دانشگاه شهید بهشتی (abdollahassareh@gmail.com).

مقدمه

تضمین آزادی بیان و حق دسترسی آزاد به اطلاعات در اسناد بین‌المللی حقـوق بشـری مورد تصریح قرار گرفته است. از آن جمله می‌توان به ماده ۱۹ اعلامیـه جهـانی حقـوق بشر،* ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی** و ماده ۱۰ کنوانسیون اروپایی حقوق بشر*** اشاره نمود.

بهره‌مندی از آزادی بیان و دسترسی آزادانه به اطلاعات در زمـره نسـل اول حقـوق بشر (Rights Human Generation of First) قرار دارند. برخورداری از حقـوق نسـل اول نیز، مستلزم عدم دخالت حکومت در جریان این حقـوق و آزادی‌هـا از یـک‌سـو و تکلیف وی در پاسداشت آنها و برخورد با متجاوزان از سـوی دیگـر اسـت. (هاشـمی، ۱۳۸٤، ص ١٦٤-١٦٥) به عبارت دیگر این حقـوق بیشـتر دارای مفهـوم سـلبی‌انـد تـا ایجابی (لوسین زهادی، ۱۳۸۳، ص ۱۲۱).

در مقام توصیف، این آزادی‌ها، از تعبیر آزادی حـداکثری حتـی‌الامکـان (اسـلامی، ۱۳۸۵، ص۵) استفاده شده است. بدین‌معنا که هرکجا آزادی بیان و دسترسـی شخصـی به اطلاعات، در تعارض با حقوق یا آزادی‌های دیگران باشد؛ همان‌جـا منطقـه ممنوعـه حمایتی محسوب شده و نه‌تنها مورد حفاظت واقع نمی‌شود؛ بلکه مرتکب تجاوز به آن حقوق، متخلف محسوب می‌شود.

لذا آزادی بیان برخلاف آزادی عقیده، حقی مطلق نبوده و مقید است. ایـن نکتـه در

* «هر کس حق آزادی عقیده و بیان دارد و حق مزبور شامل آن است که از داشتن عقاید خود بیم و اضطرابی نداشته باشد و در کسب اطلاعات و افکار و در اخذ و انتشار آن به تمام وسایل ممکن و بدون ملاحظات مرزی آزاد باشد.

** «هر کس حق آزادی بیان دارد و این حق شامل آزادی جست‌وجو و کسب و اشاعه اطلاعات و اندیشه‌ها از هر قبیل بدون توجه به سرحدات، خواه شفاهاً یا به صورت نوشته یا چاپ یا به صورت هنری و یا به هر وسیله دیگر به انتخاب خود می‌باشد».

*** «هرکس حق آزادی بیان دارد. این حق باید متضمن داشتن آزادی در عقیده، کسب و اشاعه اطلاعات و عقاید بدون مداخله اقتدار عمومی و صرف‌نظر ار مرزها باشد».

اسناد بین‌المللی نیز مشهود است. برای نمونه، اعلامیه جهانی حقوق بشر پس از تبیین حقوقِ بنیادین، در ماده ۲۹، آزادی‌های مذکور را چنین محدود ساخته است:

... هر کس در اجرای حقوق و استفاده از آزادی‌های خود فقط تابع محدودیت‌هایی است که به وسیله قانون، منحصراً به منظور تأمین شناسایی و مراعات حقوق و آزادی‌های دیگران و برای رعایت مقتضیات صحیح اخلاقی و نظم عمومی و رفاه همگانی در شرایط یک جامعه دموکراتیک وضع شده است.

عبارات یکی از اندیشمندان حقوق نیز درباب توجیه محدودیت‌های آزادی بیان گویا و رساست:

آزادیِ مطلقِ بیان، می‌تواند یکی از حقوق مسلم دیگر افراد جامعه که همانا حق بر آبرو و حیثیت است را به صورت ناموجهی به خطر اندازد. همچنین اعمال نامحدود این حق ممکن است به امنیت و منافع ملّی یک کشور، آسیب جدی وارد نماید (قاری سیدفاطمی، ۱۳۸٤، ص ۲٦٦).

در این میان ظهور پدیده اینترنت و گسترش آن در دوران کنونی زندگی بشر، انبوهی از مسائل مرتبط با آزادی بیان و اطلاعات؛ خصوصاً بحث‌هایی پیرامون محدودیت‌های این آزادی‌ها را به وجود آورده است. به نظر می‌رسد یکی از مهم‌ترین مسائل در حوزه قوانین و مقررات مرتبط با اینترنت؛ مسئله ایجاد محدودیت در دسترسی به اطلاعات موجود در فضای سایبر توسط دولت‌هاست که دائماً با مخالفت‌ها و موافقت‌هایی همراه است.

شروع، گسترش و همه‌گیریِ استفاده از فن‌آوری جدیدِ ارتباطات شبکه‌ای، آن‌قدر شتاب داشته که به نظر می رسد؛ مصادر و مراجع علمی و قانونی از تحلیل، تجزیه و ارائه راهکارهای درست در جهت استفاده هرچه بهتر از این موقعیت، کمی جامانده اند و به‌روزنبودن قوانین، مقررات و دستورالعمل‌ها در این زمینه به کاربران و منتفعین از این حوزه آسیب زده است.

با این وجود، مسائلی همچون کنترل امنیت ملّی، صیانت از حریم خصوصی، جلوگیری از سوءاستفاده از کودکان و غیره، از مواردی هستند که اکثر دولت‌ها بر آن توافق دارند و تلاش می‌کنند تا فضای اینترنت را از این‌چنین آسیب‌هایی محافظت نمایند. البته دایره این کنترل‌ها در کشورها، متفاوت است. از سویی برخی محدودیت‌های دست‌وپاگیر فراوانی

در برابر جریان آزاد اطلاعات قرار داده‌اند و حتی خود را از شبکه جهانی منفک نموده‌اند و از سوی دیگر برخی مانند ایالات متحده آمریکا به کنترل کاملاً حداقلی اینترنت ـ حداقل در ظاهر ـ اعتقاد دارند (طبرسا، ۱۳۸۰، ص ۲۵٤).

پیش از پرداختن به دلایل ایجاد محدودیت در اینترنت، ذکر این نکته ضروری است که در سطح بین‌المللی، هنوز منبع حقوقی معتبر و شفافی که بتواند به کاربران، معیار و سنجه مشخصی در مورد استفاده از اینترنت و محدودیت‌های آن ارائه کند به‌وجود نیامده است و عموماً ارزش‌گذاریِ ارتباطات اینترنتی از روی اصول مورد توافق جهانی صورت می‌گیرد (بردبار، ۱۳۸۰، ص ۱۰۵).

۱. حدود دسترسی به اطلاعات در فضای سایبر

همان‌طور که در باب محدودیت‌های آزادی بیان اشاره شده؛ اِعمال حق دسترسی به اطلاعات نیز همانند سایر حقوق، مطلق و بی‌قید و شرط نیست و دارای حدود خاصی است (انصاری، ۱۳۸٦، ص ۱۷۱). به تعبیری از محدودیت‌ها یا استثناهای حق دسترسی به اطلاعات می‌توان به سوپاپ اطمینان رعایت این حق تعبیر کرد (انصاری، ۱۳۸۷، ص ۱٤۹). در این خصوص قوانین آزادی اطلاعات در کشورهای مختلف جهان تقریباً استثناهای مشابهی را پیش‌بینی کرده‌اند. امنیت ملّی، اسرار دولتی، حریم خصوصی، مالکیت‌های فکری، ایمنی و سلامتی افراد از مهم‌ترین توجیهات محدودسازی، قلمداد شده‌اند (همان، ص ۱٤۹ – ۱۵۰).

البته حمایت از استثناهای دسترسی به اطلاعات در صورتی می‌تواند قابل توجیه باشد که منفعت بالاتری را تضمین نماید؛ لذا به هر بهانه‌ای نمی‌توان آزادی اطلاعات را محدود کرد (همان، ص ۱۵۰). به همین دلیل بند دوم ماده ۹ کنوانسیون اروپایی حمایت از حقوق بشر اعلام داشته:

> آزادی در آشکارساختن مذهب یا عقاید یک شخص، تنها تابع محدودیت‌هایی خواهد بود که در قانون مقرر شده؛ در یک جامعه دموکراتیک به خاطر سلامت عمومی، حفاظت از نظم عمومی، بهداشت یا اخلاقیات یا حمایت از حقوق و آزادی‌های دیگران ضرورت دارند.

همچنین ماده ۱۱ توصیه‌نامه اصول ژوهانسبورگ* بیان می‌دارد:

هر کس حق کسب اطلاعات از مقامات دولتی را داراست؛ از جمله اطلاعات در ارتباط با امنیت ملّی. هیچ محدودیتی بر این حق را نمی‌توان بر پایه امنیت ملّی تحمیل کرد؛ مگر آنکه حکومت بتواند اثبات کند که محدودیت را قانون تجویز کرده است و [اعمال آن] برای اینکه جامعه دموکراتیک بتواند از مصلحت مشروع امنیت ملّی دفاع کند؛ ضروری است.

در ادامه به مهم‌ترین توجیهات ایجاد محدودیت در دسترسی به اطلاعات اشاره می‌کنیم.

۱ـ۱.تطهیر اینترنت از مطالب مخالف امنیت ملّی

امنیت ملّی به عنوان مفهومی تعمیمی به تمامی وجوه اجتماعی، دارای ابعادی فراتر از جنبه نظامی آن است. تردیدی نیست که قدرت نظامی برای حفظ استقلال ملّی، یکی از مهم‌ترین پایه‌های امنیت ملّی به‌شمار می‌آید؛ اما با عنایت به برخی تعاریف کلی از امنیت ملّی که آن را به منزله «قدرت به حداقل رسانیدن هر نوع تهدید به منافع ملّی، تمامیت ارضی و استقلال کشورها» می‌داند، مؤلفه‌های جدید سیاسی، اجتماعی و فرهنگی در تحقق این مفهوم معنا می‌یابد (مینایی، ۱۳۸۳، ص ۱۳۳).

امنیت به صورت وسیع، در مفهومی به‌کار گرفته شده که به صلح، آزادی، اعتماد، سلامتی و دیگر شرایطی اشاره می‌کند که فرد و یا گروهی از مردم، احساس آزادی از نگرانی، ترس، خطر یا تهدیدات ناشی از داخل یا خارج را داشته باشند (میرعرب، ۱۳۷۹، ص ۱۳۳).

در بیان اهمیت امنیت ملّی، همین بس که به‌زعم برخی، در صورت تعارض با دیگر حقوق و آزادی‌های شهروندی، موجب محدودشدن آنها می‌شود (انصاری، ۱۳۸٦، ص ۱۹۵). امنیت و اهمیت آن، البته ریشه در ذاتیات بشر دارد، چرا که حفاظت و صیانت از نفس، یکی از مصادیق بارز کنش‌های فطری انسان است؛ لذا به همین میزان نیز به مخاطره‌افتادن امنیت عمومی یک جامعه، به منزله تهدید حیات اجتماعی بشر تلقی شده، تا آن‌جا که امنیت و نظم برای ساختن یک مردم‌سالاری پایدار و زنده، لازم و جزء لاینفک

*#The Johannesburg Principles on National Security, Freedom of Expression and Access to Information", Human Rights Quarterly, Vol. 20, No. 1 (Feb, 1998), p. 6.

شمرده شده است (همان، ص ۱۹۵). به همین دلایل نیز، حمایت از امنیت ملّی مهم‌ترین استثنای دسترسی به اطلاعات محسوب می‌شود (همان، ص ۱۵۰). از دیدگاه اسلام، امنیت از مهم‌ترین اصول زندگی در حوزه‌های شخصی و اجتماعی محسوب می‌شود که به واسطه استقرار آن؛ راه حصول به آرمان‌ها و بهره‌مندی از مواهب و گسترش دانش‌اندوزی، هموار می‌شود (خوشروزاده، ۱۳۸۲، ص ۱۹۵).

اگر در صد سال قبل برای فروپاشی امپراطوری‌های عثمانی، اتریش، اسپانیا، پرتغال، فرانسه، انگلیس و آلمان دو جنگ جهانی لازم آمد؛ برای اضمحلال امپراطوری شوروی حضور رسانه‌های جهانی، ویدیو، شبکه‌های رایانه‌ای کافی بود تا سازوکارها و تغییرات اجتماعی از پیش مهیا شده را تشدید نمایند (مینایی، ۱۳۸۳، ص ۱۳۳) و از طریق خدشه بر امنیت ملّی این کشور، ساختار آن‌را دگرگون نمایند. به همین دلیل نیز حملات نرم و سایبری (Cybernetic) را باید یکی از مواجهات جدی اینترنت و امنیت ملّی دانست. در این زمینه مسئله دسترسی به اطلاعات و نشر اخبار و مطالبی که امنیت ملّی را به مخاطره می‌افکند؛ موضوعی است که نیاز به بررسی و تدقیق بیشتری دارد.

سؤال این‌جاست که چگونه تعاملات در فضای اینترنتی برای امنیت ملّی تهدید ایجاد می‌نماید؟ و آیا اصولاً ممکن است که از طریق کابل‌های شبکه اینترنت، پایه‌های یک حکومت، تحت‌تأثیر مخالفت‌ها و اعتراض‌های شدید، به لرزه افتد؟

فرآیند پرشتاب ارتباطات جهانی که حاصل گسترش شبکه‌های اطلاعاتیِ کاملاً دوسویه است، چشم‌اندازِ گسترده‌ای از امنیت ملّی، عوامل بقا و موانع آن ترسیم کرده است. تار و پود این پیشرفت به حدی تنیده شده که به نظر بسیاری از کارشناسان ماهیت جنگ بین دولت‌ها را از حالت صرفاً نظامی خارج نموده است (جاویدان و همکاران، ۱۳۸٤، ص ۳۰). به تعبیری در عصر اطلاعات، جنگ‌ها به سوی نبرد اطلاعاتی سوق یافته‌اند. اگرچه اهمیت اطلاعات در جنگ‌های پیشین نیز شناخته شده بود، اما جنگ‌های این سده، تا اندازه بی‌سابقه‌ای مبتنی بر سامانه‌های اطلاعاتی است. در چنین شرایطی، دیجیتالی‌شدن صحنه نبرد، جلوه‌ای از ظرفیت اینترنت و دیگر فن‌آوری‌های اطلاعاتی برای اکتساب، تبادل و به‌کارگیری به‌موقع اطلاعات در میدان جنگ است؛ به گونه‌ای که فضایی تقریباً شفاف را برای کلیه واحدهای درگیر در جنگ

به‌وجود می‌آورد. این امر در کنار استفاده از جنگ‌افزارهای بسیار دقیق که علیه مراکز حساس و مهم دشمن به‌کار گرفته می‌شود، نقش بسیار مهمی در مدیریت جنگ‌های عصر اطلاعات دارد. نمونه این نوع جنگ‌ها در سال ۱۹۹۱ و ۲۰۰۳ علیه کشور عراق صورت پذیرفت (همان، ص ۳۰).

گذشته از کاربرد این پدیده در زمان جنگ، در شرایط به‌سامان و عادی نیز گونه‌هایی از تهدیدات، علیه امنیت یک کشور به‌وجود آمده است که اهمیتی کمتر از هنگامه نبرد ندارد. امکان به سرقت‌رفتن یا حذف اطلاعات، ورود غیرمجاز به رایانه‌ها و شبکه‌های داخلی، دست‌بردن در اطلاعات رایانه‌ها، جاسوسی اینترنتی و ...، چه با منافع کاملاً فردی و از روی تفنن و چه در قالب سازمان‌دهی وسیع و هوشمند، از نمونه‌های تهدیدات علیه امنیت است.* در عین حال به علت نبود هیچ حد و مرزی در شبکه اینترنت، امکان جرم‌انگاری، تشخیص دادگاه صالح، تعقیب و مجازات این اعمال از پیچیدگی‌های خاصی برخوردار شده است. گونه دیگری از تهدیدات امنیتی اینترنت، تحریک مردم به ایجاد شورش و اغتشاش در کشور و یا انتشار اطلاعاتی است که برای وحدت ملّی و یکپارچگی کشور خطری عمده داشته باشد که از مصادیق بارز تخالف با امنیت ملّی است (انصاری، ۱۳۸٦، ص ۱۹٦). همچنین یکی از نگرانی‌های دیگری که در باب پهنه بی‌انتهای اطلاعات در اینترنت به‌وجود آمده، تسهیل حملات تروریستی است. چرا که اطلاعات، برای یک تروریست بسیار ضروری است و این داده‌ها نیز به صورتی کاملاً آزاد و رها در اینترنت یافت می‌شود. به دلیل اینکه جمع‌آوری اطلاعات اساسی و مهم از اینترنت دارای ریسک پایین و هزینه‌ای اندک است، محتمل است که اینترنت، اولین منبع انتخابی برای طراحی نقشه‌های خراب‌کارانه و تروریستی باشد (landree, 2006, P. 4).

حجم گسترده و غیرقابل احصاء روابط و تعاملات اینترنتی و ظرفیت دست‌برد در اطلاعات و یا افشای بی‌ملاحظه برخی اخبار و اسرار غیر قابل انتشار، باید سامانه قانون‌گذاری و اجرایی هر حکومتی را تحریک کند تا در کنترل و بهره‌مندی معقول و سالم از این رسانه، اقدامات به‌جا و شایسته صورت پذیرد. برای مثال در کشوری

* انتشار ویروس استاکس نت در ایران، توسط دشمنان خارجی که مراکز حساسی همچون نیروگاه هسته‌ای بوشهر را مورد هدف قرار داده بود، یک نمونه از این حملات محسوب می‌شود.

همچون ایالات متحده برای جلوگیری از ورود خسارت‌های هنگفت و غیرقابل جبران، اقداماتی در راستای تقویت بنیان‌های امنیت اطلاعات صورت می‌پذیرد،* هر چند آماری که از دسترسی‌ها و دستبردهای غیرمجاز در مراکز مهم، همچون پنتاگون و ... به گوش می‌رسد که نشان‌دهنده عدم کارایی این اقدامات است.**

۲ـ۱. حفظ اسرار دولتی

اسرار دولتی (State Secrets)، یکی از مهم‌ترین استثناهای دسترسی به اطلاعات محسوب می‌شود. مفهوم دسترسی به اطلاعات دارای گستره وسیعی است و یکی از مهم‌ترین مصادیق آن نیز دسترسی به اطلاعات دولتی است. اطلاعاتی که در این محدوده قرار می‌گیرند؛ به دلیل وجود مصالح امنیتی و یا رعایت نظم عمومی، قابلیت انتشار و افشا ندارند و یا انتشار آنها اقتضای روال خاصی را دارد. با این وجود، نکته مهم این است که از منظر حقوق عمومی، اصل بر آزادی اطلاعات است و عدم انتشار اسرار دولتی استثنایی بر این اصل محسوب می‌شود.

هر کشوری با توجه به شرایط حکومتیِ خاص خود، یک سری اسناد و اطلاعات در اختیار دارد که انتشار علنی آنها ممکن است نظم عمومی را مختل سازد. یکی از ملموس‌ترین نمونه‌ها در کشور ما، انتشار اطلاعات در مورد تأسیسات هسته‌ای است که به طور واضح می‌توان محدودیتی برای آن درنظر گرفت. در کشورهای دیگر نیز این رویه کاملاً جریان دارد؛ در برخی کشورها، کارمندان مراکز امنیتی در صورت افشای اطلاعات سری و مهم به شدت مجازات می‌شوند (brooke, 2005, P. 78).

---

* افزایش جرایم رایانه‌ای در آمریکا از جمله حمله به سایت‌های Amazon و Yahoo، رئیس FBI را واداشت تا در فوریه ۲۰۰۰ از کنگره بخواهد ۳۷ میلیون دلار به بودجه ۱۰۰ میلیون دلاری وزارت دادگستری برای مبارزه با جرایم رایانه‌ای بیفزاید و کلینتون در همان ماه درخواست یک بودجه ۹ میلیون دلاری برای تأسیس مرکز امنیت ملی، مشارکت شرکت‌های اینترنتی و تجارت الکترونیک علیه حمله‌کنندگان به سایت‌های رایانه‌ای را به کنگره ارائه داد.

** برای مطالعه بیشتر رجوع کنید به: www.javanonline.ir/Nsite/FullStory/?Id=348750
و در زمینه امنیت شبکه: http://fa.wikipedia.org/wiki/.

در نظام حقوقی ایران، قانون جامعی درباره اسرار دولتی وجود ندارد. البته در سال ۱۳۸۳ لایحه‌ای با همین عنوان در دولت نهایی شد؛ لکن به مجلس شورای اسلامی ارسال نشد.

در وضع کنونی، نظام‌بندی مقوله‌های مختلف اسرار دولتی، تابع «قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی» مصوب ۱۳۵۳/۱۱/۲۹ و «آیین‌نامه طرز نگاه‌داری اسناد سری و محرمانه دولتی و طبقه‌بندی و نحوه مشخص‌نمودن نوع اسناد و اطلاعات» مصوب ۱۳٥٤/۱۰/۱ هیأت وزیران، قانون مجازات اسلامی و قانون مجازات جرایم نیروهای مسلح مصوب ۱۳۸۲/۱۰/۹ است.

به صورت طبیعی محتمل است که این دو قانون و آیین‌نامه مرتبط‌تر با اسرار دولتی با توجه به قدمتی که دارند؛ نتوانند آرمان‌های آزادی‌گرایانه، درباره اطلاعات و دسترسی به آنها را محقق سازند. چرا که رویکرد حمایت از آزادی اطلاعات، پس از همه‌گیری فن‌آوری‌های نوین ارتباطی، به‌طور بسیار جدی‌تری مطرح شده است؛ لذا هر چند از نظر محتوایی ایراداتی دیگر نیز به قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی وارد شده است (انصاری، ۱۳۸۷، صص ۱۹۰ و ۱۹٦)، اما به‌روزنبودن این قانون یکی از مهم‌ترین، ضعف‌هاست که باید اصلاح شود.

قانون تازه‌تصویب انتشار و دسترسی آزاد به اطلاعات (مصوب ۱۳۸۸) در سرفصلِ استثنائات دسترسی به اطلاعات، یک ماده را به بحث اسرار دولتی اختصاص داده است:

> در صورتی که درخواست متقاضی به اسناد و اطلاعات طبقه‌بندی شده (اسرار دولتی) مربوط باشد؛ مؤسسات عمومی باید از در اختیار قراردادن آنها امتناع کنند. دسترسی به اطلاعات طبقه‌بندی شده تابع قوانین و مقررات خاص خود خواهد بود.

البته ارجاع این قانون به مقررات طبقه‌بندی که در «آیین‌نامه طرز نگاه‌داری اسناد سری و محرمانه دولتی و طبقه‌بندی و نحوه مشخص‌نمودن نوع اسناد و اطلاعات» آمده است که به دلایل ذکر شده، کار را تا حدی دشوار کرده است. با توجه به اصول کلی حقوق، باید اظهار داشت که دسترسی به اطلاعاتی که از طبقه‌بندی خاصی پیروی نمی‌کنند باید به طور کاملاً آزادانه صورت پذیرد. دولت نیز باید در طبقه‌بندی‌کردن اسناد خود به طور مضیق و موافق با نفع عموم و با لحاظ حقوق و آزادی‌های مردم

عمل نماید؛ والا ممکن است با در پیش‌گرفتن این سیاست که کم اهمیت‌ترین مطالب را نیز وارد مقوله طبقه‌بندی نماید، مردم را از دسترسی به منابعی که حقشان است؛ محروم کند. از آن‌سو نیز باید در دسترسی به اطلاعات سری و محرمانه، محدودیت‌های مقتضی را ایجاد کرد.

به موجب ماده ۲ قانونِ «مجازات انتشار و افشای اسناد محرمانه و سری دولتی» هر کدام از کارکنان سازمان‌های مرتبط با طبقه‌بندی سند، که این اسناد را انتشار دهد یا افشا نماید؛ در مورد اسناد سری به حبس از ۲ تا ۱۰ سال و در مورد اسناد محرمانه به حبس از شش ماه تا سه سال محکوم می‌شود. همین مجازات درباره کسانی که این اسناد را با علم و اطلاع، چاپ یا منتشر نمایند نیز، وجود دارد. انتشار این اسناد در محدوده فضای سایبر نیز یک نوع افشا محسوب شده و مجازات‌های ذکر شده را به دنبال دارد. حتی ممکن است، منتشرنمودن این اسناد در اینترنت اثراتی به مراتب زیان‌بارتر از شیوه‌های دیگر داشته باشد، زیرا مطالبی که در اینترنت افشا می‌شود، به سرعت بسیار زیاد و در حجم وسیعی شیوع پیدا می‌کند.

۳ـ۱. حفاظت از عفت عمومی در برابر تهدیدهای اینترنت

حجم بسیار زیاد گردش مالی تجارت سکس، حامل این پیام مهم است که اثرات سوءِ ناشی از سهولت دسترسی به این منابع به بهانه حمایت از آزادی بیان و دریافت آزاد اطلاعات، تمدن بشریت را دچار ضعف و زوال خواهد نمود. برای مثال، یکی از نتایج عدم کنترل اینترنت، سوءاستفاده جنسی از کودکان است که در برخی کشورها به امری طبیعی و عادی مبدل شده است.

به همین دلیل هیک (Hick) و *هالپین* (Halpin) معتقدند باید ملت‌ها، ادارات مجری قانون و سازمان‌های غیردولتی برای کنترل اینترنت و حفاظت از افراد در برابر محتوای غیراخلاقی آن؛ با هم همکاری داشته باشند (Halpin, 2001, P. 60).

همان‌طور که اشاره شد اینترنت و تمام اشکال ارتباطی و اطلاعاتی دیگر بدون شک حقوق کودکان را تحت‌تأثیر خود قرار داده‌اند. بازنگری تأثیر اینترنت بر کودکان، اغلب با نتایج منفی همراه است. اینترنت موقعیت‌های نو و پیچیده‌ای را برای نقض قانون و

ارتکاب جرایم بر ضدّ کودکان از راه‌های غیرمرسوم ایجاد می‌کند. هر چند این فن‌آوری، نقشی اساسی در ارتباط افراد و سازمان‌ها در سرتاسر جهان برای ارتقا و حفاظت حقوق کودکان ایفا می‌کند (Ibid, P. 57)، اما به راحتی نمی‌توان از کنار اثرات زیان‌باری که محتویات اینترنت کودکان را به آن دچار می‌کند، عبور کرد.

۱ـ۳ـ۱. شواهدی از خطرات دسترسی بدون کنترل

مارک لاسر (Lasser.M.R) به پی‌آمدهای منفی هرزه‌نگاری اینترنتی بر بهداشت روانی اشاره کرده و معتقد است؛ استفاده غلط از اینترنت، می‌تواند هم برای کودکان و هم برای بزرگسالان، موجب بروز رفتارهای نامعقول و انحرافی شود و حتی یک نوع اعتیاد به‌وجود آورد (شجاعی، ۱۳۸۷، ص ۱۳۰ – ۱۳۱). بر مبنای تحقیقی در سال ۲۰۰۷، بسیاری از این مشاهدات ناخواسته، به نوجوانان آسیب‌هایی، نظیر افسردگی رسانده و یا در آنها تمایلات جنایت‌آمیز ایجاد نموده است (Cankayaa, 2009, P. 1106).

گذشته از اینکه وب‌گردی در فضای بدون کنترل، کودکان را با تهدید برخورد با صحنه‌های ناهنجار مواجه می‌کند، از خطرناک‌ترین وجوه جرایم رایانه‌ای، شکل‌گیری باندهای تبهکار بین‌المللی، سوءاستفاده جنسی از کودکان، تهیه منابع قابل عرضه بر روی شبکه‌های رایانه‌ای و نقل و انتقال این منابع می‌باشد. علاوه بر این؛ وجود گروه‌های خبری منحرف که به تبادل پیام و منابع غیراخلاقی می‌پردازند؛ نیز اشاعه فحشاء در شبکه جهانی را به شکل قابل توجهی افزایش داده است (جرایم رایانه‌ای و اشاعه مفاسد اخلاقی، ۱۳۸۰، ص ۱۳۹).

از ۱۲۰ مورد متجاوزی که توسط پلیس آمریکا در سال ۲۰۰۰ مورد بازجویی قرار گرفته‌اند، بیش از ۷۰ مورد، خود آدرس و تلفن قربانیانشان را پیدا کرده‌اند و همچنین ۱۰۵ مورد اولین ارتباطشان را از اتاق گفتگوی اینترنت (Chat Room) شروع کرده‌اند و در نهایت از این تعداد ۷۵۰ گیگابایت تصاویر پورنوگرافی کودکان کشف شد (غمامی، ۱۳۸٤، ص ٤٦). تقریباً نیمی از افراد ۹ تا ۱۹ ساله‌ای که دست‌کم، یک‌بار به اینترنت وصل می‌شوند (٤٦ درصد)، می‌گویند؛ اطلاعاتی از قبیل: نام، سن، نشانی پست الکترونیکی، شماره تلفن، سرگرمی‌های مورد علاقه یا نام مدرسه خود را، به کسی داده‌اند که او را در اینترنت ملاقات کرده‌اند (لیوینگستون، ۱۳۸٤، ص ۵۹).

همچنین بر طبق یک تحقیق دیگر با جامعه آماری ۲۳۴۳ نوجوان هلندی در بازه سنیِ ۱۳ تا ۲۰ سال، مشخص شد که بیشتر این افراد در معرض مسائل صریح جنسی در اینترنت بوده‌اند و نیز ۲۲ درصد از کودکان در معرض وب‌سایت‌های محتوی خشونت قرار دارند (Cankayaa, 2009, P. 1106).

این در حالی است که تقریباً یک سوم خانواده‌های آنلاین آمریکایی که دارای کودک هستند، از نرم‌افزارهای فیلترینگ خانگی استفاده می‌نمایند (Rosenberg, 2001, P. 38) و این یعنی نگرانی شهروندان از آسیب‌رساندن اینترنت بدون فیلتر. بدین لحاظ، بسیار به‌جاست که سامانه کنترل این شبکه هم از جنبه پیش‌گیرانه آن و هم از لحاظ حقوق کیفری ارتقا یابد. چرا که به‌نظر می‌رسد، موضوع مهم فیلترینگِ سایت‌های مستهجن و بعضاً منحرف حرفه‌ای، ارتباط کاملاً مستقیمی با اخلاق حسنه و نظم عمومی جوامع پیدا کرده و شاید درخواست پالایش اینترنت به زودی به یک مطالبه همه‌گیر جهانی تبدیل شود.

۲ـ۳ـ۱. مقررات و ابزارهای کنترل دسترسی به اینترنت برای کودکان

اولین قانون برای حمایت آنلاین از کودکان در مقابل هرزه‌نگاری، قانون نزاکت ارتباطاتی آمریکا (CDA: Communications Decency Act) است. این قانون، برخلاف مخالفت‌های شدید سازمان‌های آزادی‌خواه، در سال ۱۹۹۶ به‌وسیله رئیس‌جمهور وقت آمریکا امضاء شد و در آن عنوان شد که نشان‌دادن هرگونه محتوای شرم‌آور بر روی شبکه اینترنت غیرقانونی است. این مصوبه تلاشی بود تا پورنوگرافی را در اینترنت کنترل کند و از کودکان در مقابل هجمه محتویات ناشایست حمایت به عمل آورد (hull, 1999، P. 30-31/Grainger, 2000, P. 6).

با مروری بر این قانون و همچنین مقررات دیگری که برای حمایت‌های موجه از کودکان در مقابل مخاطرات اقیانوس بی‌انتهای اینترنت وضع شده، می‌توان اظهار داشت که به مخالفان کنترل اینترنت چندان هم اقبالی صورت نگرفته است و به نظر نگارنده دلیل عمده آن، ارائه آمار نگران‌کننده از اخبار و نیز تحقیقات صورت‌پذیرفته در این موارد است. پیش‌تر نیز به این موضوع اشاره شد که اخبار جنایت‌های هولناکی که از

سوی متجاوزان اینترنتی صورت مـی‌پـذیرد، در مقابـل تئـوری حمایـت از آزادی‌هـای بنیادین قوت بیشتری داشته است تا جایی که دولت‌مردان را به اجبار به وادی لگـام‌زدن به اینترنت کشانده است.

در سال ۲۰۰۰ نیز قانونی با عنوان حمایـت از کودکـان در اینترنـت (CIPA:Child Internet Protection Act) در ایالات متحده مطرح شد و در سال ۲۰۰۳ میلادی توسط دیوان عالی ایالات متحده امریکا به تصویب رسید. مطابق ایـن قـانون همـه مـدارس و کتابخانه‌های عمومی (که برای اتصال به اینترنت و یا رایانه‌هـای متصـل بـه اینترنـت از کمک‌های دولت استفاده کرده‌اند)، موظف به بستن و یا فیلترکردن سایت‌هـایی هسـتند که در آنها تصاویر وقیح و عکس‌های شهوت‌انگیز مربوط به کودکان و یـا هـر تصـویر جنسی دیگری که برای نوجوانان مضر باشد؛ وجود داشته باشـد (Harinder, 1997, P. 21). البته از منظر حقوق بشر این کار ممکن است، دسترسی به اطلاعات مناسب دیگـر را برای اعضای کتابخانه‌ها و دانش‌آموزان مدارس محدود نماید. چون در این فیلترینگ ممکن است برخی سایت‌ها که اطلاعات مفیدی دارند، نیز مسدود شوند؛ ولی ظاهراً در برگزیدن یکی از این دو مورد، قانون‌گذاران آمریکـایی اولویـت را بـه کنتـرل محتـوای اینترنتی بخشیده‌اند.

مقابله با انحرافات اینترنتی فقـط بـه ایـالات متحـده، محـدود نمـی‌شـود؛ بلکـه در کشورهای اروپایی نیز این مسئله دولت‌ها را به اقدام در این حوزه وادار کرده است. در فرانسه، در میِ ۱۹۹۶، مدیران دو شرکت ارائه‌کننده خدمات اینترنتی به استناد ماده ۲۳-۲۲۷ مجموعه قوانین جزایی فرانسه، به توزیع و پخـش پورنـوگرافی کودکـان بـر روی گروه‌های خبری اینترنتی، متهم شده و در نتیجه به سه سـال زنـدان و ٦٥ هـزار فرانـک جزای نقدی محکوم شدند (هاشمی، ۱۳۸۳، ص ۱۰).

به نظر می رسد، کشورهایی که در این زمینه، خصوصاً درباره محتوای ضدّ اخلاقـی، خلاء قانونی دارند؛ لازم است دراین‌باره به وضـع قـانون مبـادرت ورزنـد تـا مجـرمین اینترنتی با سوءاستفاده از نقص قانون، برائت حاصل ننمایند.

۴ـ۱. اینترنت و حریم خصوصی

به زعم برخی، گوناگونیِ گستره جغرافیایی و فرهنگی جوامع و نسبیت اخلاقی و اجتماعی، راه را برای نیل به تعریف واحد و مورد قبول اکثریت در مورد حریم خصوصی مسدود نموده است. حریم خصوصی را می‌توان یکی از بنیادی‌ترین و اساسی‌ترین حقوق بشری تلقی کرد که با شخصیت انسان ارتباط مستقیم و تنگاتنگی دارد. حق شخص به تنهابودن و با خودبودن، به وسیله دیگران مورد احترام قرارگرفتن، به دور از کنترل دیگران و رها از تجسس و تفتیش دیگران زیستن؛ حقی است که لازمه یک شخصیت مستقل به‌شمار می‌آید (رحمدل، ۱۳۸٤، ص ۱۲۰).

در بیان برخی، به‌جای تعریف مستقیم از حریم خصوصی برای وضوح بیشتر به مصادیق آن اشاره شده است». در تعابیر چهارگانه‌ای که معمولاً در تبیین حریم خصوصی به‌کار می‌رود، دو تعبیر به طور خاص به موضوع اطلاعات شخصی به عنوان مصداق‌های حریم خصوصی، دلالت دارند: نخست، حریم اطلاعات که شامل تصویب قوانینی است که چگونگی دسترسی به اطلاعات شخصی نظیر اطلاعات مالی، پزشکی و دولتی افراد را تعیین می‌کند. دیگری، حریم ارتباطات، که به موضوع امنیتِ پست‌های الکترونی، تلفن‌ها، پست و سایر اشکال ارتباطات توجه دارد (نمکدوست تهرانی، ۱۳۸۵، ص ۱۹۸).

حمایت از حریم خصوصی به‌قدری حائز اهمیت است که در قوانین اساسی اکثر کشورهای دنیا و در اعلامیه‌های بین‌المللی، به طور صریح و یا ضمنی مورد توجه واقع شده است؛ تا جایی که اندیشمندان غربی معتقدند، محدودیت‌هایی که برای کنترل رفتارهای حکومت به منظور حمایت از حریم خصوصی وضع می‌شوند؛ ناشی از دموکراتیک‌بودن آن حکومت است (هیک و همکاران، ۱۳۸۵، ص ۲۸۱).

در این زمینه، اصطلاح حریم الکترونیکی هم به مجموعه شرایطی اطلاق می‌شود که در آن شخص، علاقه‌ای به افشای نام و مشخصات دیگر و ارتباطاتی که از طریق اینترنت برقرار می‌کند، ندارد.

کمیسیون اصلاحات حقوقی هنک‌کنگ در مورد اهمیت حریم خصوصی در شبکه اینترنت می‌گوید:

با توجه به اینکه پست الکترونیک، انتشار و توزیع مجدد و مکرر اطلاعات شخصی را

در میان گروه‌های زیادی از مردم میسر می‌سازد؛ لذا خسارتی که در نتیجه انتشار اطلاعات حساس افراد در اینترنت ممکن است به آنها وارد شود در مقایسه با انتشار آن اطلاعات در یک روزنامه یا نشریه محلی، بسیار زیادتر است. بنابراین توانایی دستیابی تعداد زیادی از مردم به اینترنت، امر حریم خصوصی را در خور اهمیت زیاد ساخته است (انصاری، ۱۳۸۲، ص ٤٠- ٤١).

در وهله اول ممکن است در مقایسه محدوده‌های حق دسترسی به اطلاعات و صیانت از حریم خصوصی این‌گونه به نظر بیاید که این دو با یکدیگر تعارض دارند. در صورتی که خط قرمز دسترسی به اطلاعات، به‌دست‌آوردن، انتشار و انتقال اطلاعات و اسناد شخصی است. در حالی که بر خلاف ظاهر، حق شهروندان در دسترسی آزاد به اطلاعات، با حق حریم خصوصی مخالفتی ندارد، چرا که قلمرو آزادی اطلاعات در معنای امروزین آن، اساساً اطلاعات پیرامون زندگی خصوصی افراد را شامل نمی‌شود و در بردارنده اطلاعاتی است که آگاهی شهروندان از آنها بر تصمیم‌گیری در مورد سرنوشتشان تأثیر دارد (همان، ص ۲۲۷).

همان‌طور که در مسئله امنیت ملّی نیز اشاره نمودیم؛ حریم الکترونیکی از چندسو مورد تهدید واقع می‌شود. یکی از این تهدیدها استفاده از ابزار نظارتی توسط خود دولت‌هاست. اگر در محیطی این حس در مردم ایجاد شود که به دلیل بی‌اعتمادی به آنها، همواره تحت نظارت حکومت قرار دارند، این امر به شدت در نحوه فعالیت آنها تأثیر خواهد گذاشت (جلالی فراهانی، ۱۳۸۲، ص ١٥٤).

در این زمینه مباحث قابل ذکری وجود دارد. مهم‌ترین نکته، بررسی صلاحیت دولت‌ها برای رصد امور کاربران اینترنتی، به هر دلیلی از قبیل حفظ نظم، پیش‌گیری از وقوع جرم و یا حفظ امنیت عمومی است. همان‌طور که قبلاً نیز اشاره شد، برخی از دولت‌ها با توجیه حفظ امنیت عمومی و یا جلوگیری از اعمال تروریستی، خود را محق می‌دانند تا بر فعالیت‌ها و پیام‌ها و ارتباطات کاربران اینترنتی نظارت نموده و موارد مشکوک آن را ثبت نمایند. برای مثال بر خلاف حمایت‌های اولیه‌ای که در آمریکا از حریم خصوصی صورت پذیرفته بود، تقریباً دو ماه پس از واقعه یازدهم سپتامبر در سال ۲۰۰۱ قانون بسیار مفصلی تحت عنوان قانون پاتریوت (Patriot Act) برای مبارزه

با تروریسم و حفظ امنیت ملّی به تصویب رسید. به موجب این قانون، برخی از قوانین گذشته حمایت از حقوق بشر اصلاح شد و به مجریان قانون و نیروهای حافظ امنیت ملّی آمریکا، اجازه داده شد با عنوان کنترل اوضاع و پیش‌گیری از وقوع عملیات‌های تروریستیِ دیگر به حریم اشخاص، به‌ویژه حریم آن‌لاین آنها ورود پیدا نمایند (همان، ص ١٥٦). پس از این اقدام توسط دولت‌مردان آمریکایی، اتحادیه اروپا نیز برای تأمین امنیت عمومی اقدام به تصویب قانونی مشابه نمود.

در ۲۵ ژوئن ۲۰۰۲، شورای اتحادیه اروپا، رهنمود جدید حریم خصوصی و ارتباطات الکترونی را که در پارلمان اروپا به آن رأی داده شده بود، تصویب کرد. بر اساس مصوبه مذکور، دولت‌های عضو اتحادیه اروپا می‌توانستند قوانینی وضع کنند که حفظ داده‌های ترافیکی و محل هر نوع ارتباطاتی را مجاز بدارد که این ارتباطات از طریق تلفن‌های همراه، پیام کوتاه، تلفن‌های ثابت، دورنگار، پست الکترونیکی، اتاق‌های گفتگو، خود اینترنت یا هر وسیله ارتباطی الکترونی دیگرصورت می‌گیرد. همان‌طور که اشاره شد، دلایل توجیهی این برخوردها نیل به مقاصد مختلفی از قبیل امنیت ملّی، پیش‌گیری از جرم، تحقیق و پیگرد اقدامات تبهکارانه بود (نمک‌دوست تهرانی، ۱۳۸۵، ص ۲۱۰).

از سوی دیگر به نظر می‌رسد جهت حمایت هرچه بیشتر از شهروندان وضع قوانین در رابطه با حفظ حریم خصوصیِ افراد و کنترل فضای سایبر نیز جزو وظایف دولت‌ها است. برای مثال انتشار تصاویر و فیلم‌های خانوادگی و خصوصی در اینترنت به‌واسطه اینکه به راحتی در دسترس همگان قرار می‌گیرد؛ نیاز به تأکید و تشدید مجازات دارد.

در ایران لایحه حمایت از حریم خصوصی در آخرین روزهای فعالیت دولت اصلاحات به مجلس شورای اسلامی ارائه شد و با روی‌کارآمدن دولت نهم، نمایندگان دولت ایراداتی به آن وارد نموده و لایحه را از مجلس پس گرفتند. نمایندگان مجلس هفتم نیز این لایحه را با همان محتوا در قالب طرحی به مجلس ارائه کردند که در کمیسیون امنیت ملّی و سیاست خارجی مجلس کلیات آن به تصویب رسید. لکن هنوز به‌طور کامل مورد تصویب قرار نگرفته است.

۲. فیلترینگ در ایران و دیگر کشورها

از جمله مباحث مربوط به محدودیت دسترسی به اینترنت، موضوع فیلترینگ می‌باشد که در ادامه، علل گرایش به فیلترینگ در کشورهای مختلف و کشور ایران را مورد بررسی قرار می‌دهیم.

۱ـ۲. علل گرایش به فیلترینگ در میان دولت‌ها

کشورهای مختلف جهان عموماً به چهار دلیل عمده پالایش اینترنت را پی‌گیری می‌کنند که عبارتند از: مسائل سیاسی، اجتماعی، امنیتی و اخلاقی. البته برخی کشورها، برخی دلایل را برجسته‌تر و مهم‌تر می‌دانند. یکی از دلایل آن نیز ارزش‌های بنیادینِ مورد توجه هر کشور است. در مجموع می‌توان گفت، تعداد کشورهایی که در مقیاس منطقه‌ای و جهانی به نحوی با مسئله فیلترینگ و سانسور در اینترنت مواجه هستند؛ نسبتاً قابل توجه است. چنان‌که قبلاً نیز بیان شد؛ در کشور ایالات متحده به عنوان مبدع این فن‌آوری، قواعد فیلترینگ و کنترل اینترنت جاری است. از آن جمله، قانون حمایت از کودکان در اینترنت که دولت را موظف نموده تا با استفاده از نرم‌افزارهای کنترل محتوا، مطالب خلاف اخلاق را به جهت حمایت از کودکان فیلتر کند. کشورهای دیگر نیز مانند سوئد، فرانسه وآلمان در قاره اروپا و کشورهایی مانند هند، عربستان، کوبا، کره جنوبی، مالزی در آسیا و نیز کانادا، دارای گسترده‌ترین میزان تنوع فیلترینگ می‌باشند. همچنین کشورهای انگلستان، استرالیا و ایتالیا نیز دارای قوانین فیلترینگ مخصوصی می‌باشند.*

با ملاحظه رویکرد کشورهای اروپایی و همچنین ایالات متحده آمریکا و گزارش‌های ارائه‌شده از دیگر کشورهای جهان، می‌توان اظهار داشت که پالایش اینترنت در هیچ نقطه‌ای از جهان به طور مطلق مورد رد و تردید قرار نگرفته است. البته روشن است که مرزهای اعمال این قاعده بر مبنای فرهنگ و سیاست هر جامعه‌ای متغیر است، اما به دلایل متعدد از جمله حمایت از کودکان در مقابل پورنوگرافی و یا حریم خصوصیِ افراد و مانند آنها، فرایند کنترل، عملی خلاف قاعده محسوب نمی‌شود.

* برای مطالعه بیشتر رجوع کنید به: http://peyvandha.ir/0-5.htm.

۲ـ۲. فیلترینگ در ایران

هر چند قانون اساسی جمهوری اسلامی ایران به صراحت از حق دسترسی به اطلاعات و ضمانت اجرای تخلف از آن سخنی به میان نیاورده است، اما از آن‌جا که حق آزادی بیان، متضمن حق دسترسی به اطلاعات است، عبارتی که در اصل سوم قانون اساسی ذکر شده، برای تضمین‌نمودن این حق به‌کار می‌آید. بند ۲ اصل سوم، بالابردن سطح آگاهی‌های عمومی را از وظایف دولت عنوان کرده است. طبیعی است که یکی از راه های سهل و نوپدیدِ ارتقای سطح آگاهی های مردم، توسعه دسترسی به اینترنت و تضمینات حقوقی آن است. همچنین بند ۷ نیز، دولت را موظف نموده تا آزادی‌های سیاسی و اجتماعی را در حدود قانون تأمین نماید. همچنان که ذکر شد؛ حق دسترسی به اطلاعات در محدوده آزادی‌های سیاسی و اجتماعی جای دارد.

به نظر می‌رسد در چند بخش، سامان‌دهی مناسبی در این زمینه مورد نیاز است. سایت‌های خبری و یا به اصطلاح خبرگزاری‌های اینترنتی در این مبحث از اهمیت زیادی برخوردارند. سرعت انتشار و عدم محدودیت‌های دست‌وپاگیر مطبوعات کاغذی و گروه‌های خبری تلویزیونی، اقبال عمومی به کسب خبر و تحلیل از این سایت‌ها را به یک‌باره، جهش قابل ملاحظه‌ای بخشیده است. به همین نسبت نیز کنترل و نظارت بر انتشار این اطلاعات، کاهش یافته است. ملاکی که در ارتباط با مطبوعات و تخلفاتشان استفاده می‌شود؛ تقریباً در این‌جا هم می‌تواند لحاظ شود. مسئولان یک سایت خبری باید به دستگاه‌های نظارتی پاسخ‌گو باشند. چه‌بسا پخش یک خبر کذب و یا توهین و هتک حرمت اشخاص در یک پایگاه خبری اثری به مراتب بیشتر از نشر آن در یک مجله یا روزنامه داشته باشد. بیان یکی از اساتید حقوق مؤید این نظر است: «مطالب تصویری، صوتی یا ترکیبی مندرج در شبکه های رایانه‌ای ملّی یا بین‌المللی، یکی دیگر از مظاهر بیان افکار و اندیشه‌های بشر هستند که همانند سایر مصادیق بیان، اگر چه اصولاً آزادند، ولی باید محدودیت‌های خاص را که به‌ویژه برای حمایت و صیانت از حقوق و آزادی‌های عمومی مقرر شده است؛ رعایت نمایند» (انصاری، ۱۳۸۱، ص ٦٧).

البته این نکته نیز نباید مغفول بماند که فضای عمومی و خبری در اینترنت تفاوت‌هایی جدی با مطبوعات دارد. سرعت انتقال اخبار و محدودیت‌های کمتر آن

نسبت به روزنامه‌ها و مجلات و رسانه‌های دیگر، این مطلب را به ذهن متبادر می‌سازد که برای نظارت بر این‌گونه خبرگزاری‌ها باید قانونی کاملاً در شأن فعالیت‌های رایانه‌ای ایجاد شود، والا ممکن است در بسیاری موارد حکم‌نمودن بر مبنای قانون مطبوعات شخص را از اتهام مبری کند، در حالی که اگر فعل او با قوانین سایبری سنجیده شود، منجر به محکومیت متهم شود یا به عکس.

در سال ۱۳۷۹ رهبری جمهوری اسلامی ایران سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای را به شورای عالی انقلاب فرهنگی ابلاغ فرمودند (مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه‌ای، موجود در پایگاه اطلاع‌رسانی شورای عالی انقلاب فرهنگی). به‌واسطه این ابلاغیه نخستین مصوبه درباره شبکه‌های اطلاع‌رسانی، در پانزدهم آبان ۱۳۸۰ از سوی شورای عالی انقلاب فرهنگی تصویب شد.

در مقدمه این مصوبه برخی از امور اساسی مرتبط با اینترنت عنوان شده‌اند. مسائلی از قبیل به رسمیت شناختن حق دسترسی آزاد مردم به اطلاعات و دانش، تأکید بر مسئولیت مدنی و حقوقی افراد در قبال فعالیت‌های خود، تأکید بر رعایت حقوق اجتماعی و صیانت فرهنگی و فنی کشور در این قلمرو و همچنین درخواست از نهادهای مسئول برای ایجاد حداکثر سهولت در ارائه خدمات اطلاع‌رسانی و اینترنت به عموم مردم.

بند ششم از قسمت «الف» این مصوبه در ارتباط با کنترل محتوای اینترنت مقرر می‌کند که کلیه ایجادکنندگان نقطه تماس بین‌المللی (از جمله شرکت مخابرات ایران) موظفند تا امکانات فنی لازم در حفاظت و کنترل متمرکز از شبکه‌های مزبور را به‌عمل آورند. یکی از این طرق نیز که باید مورد استفاده قرار گیرد سیستم پالایش (Filtering) مناسب به منظور ممانعت از دسترسی به پایگاه‌های ممنوع اخلاقی و سیاسی و حذف ورودی‌های (Port) غیرمطلوب است.

بر مبنای این مصوبه انجام برخی فعالیت‌ها و یا انتشار برخی موارد بر روی سایت‌ها و وبلاگ ها ممنوع بوده و جرم محسوب می‌شود: نشر مطالب الحادی و مخالف موازین اسلامی، اهانت به دین اسلام و مقدسات آن، ضدّیت با قانون اساسی و هرگونه مطلبی که استقلال و تمامیت ارضی کشور را خدشه دار کند، اخلال در وحدت و وفاق ملّی و... از جمله این موارد محسوب می‌گردد .

از سال ۱۳۸۰ تا اردیبهشت ۱۳۸۸ که قانونی با عنوان جرایم رایانه ای در مجلس به تصویب رسید، مرجع رسیدگی و سامان‌دهی به مقوله اینترنت در کشور شورای عالی انقلاب فرهنگی بوده است و بنا به مصوبه این شورا کمیته‌ای سه نفره به عنوان مسئول تعیین مصادیق فیلترینگ اینترنتی مشخص شد. بالاخره پس از مدت‌ها سرگردانیِ لایحه جرایم رایانه‌ای، در سال ۱۳۸۸ این لایحه به تصویب مجلس شورای اسلامی رسید. به موجب آخرین ماده این قانون، قوانین و مقرراتِ مغایر ملغی اعلام شده است و لذا بخش‌هایی از مصوبه شورای عالی انقلاب فرهنگی نیز اعتبار خود را از دست داده است.

بر مبنای ماده ۲۲ قانون جرایم رایانه‌ای (منتشر شده در روزنامه رسمی به شماره ۱۸۷۲ مورخ هفدهم تیرماه هزاروسیصد و هشتاد و هشت)کمیته‌ای با عنوان تعیین مصادیق محتوای مجرمانه، مسئول کنترل محتوای اینترنت و مرجع تصمیم‌گیری در مورد تخلف و یا عدم تخلف از مواضع قانونی است.

نقص عدم صلاحیت قضایی که در مصوبه شورای عالی به چشم می‌آمد، به ابتکار قانون جدید مرتفع شده است. چرا که اصولاً قضاوت در مورد حسن و قبح محتویات یک پایگاه اینترنتی و مسدودنمودن یا تنفیذ فعالیت آن، عملی حقوقی و قضایی محسوب می‌شود و قاعدتاً به غیر از قاضی مستقل، شخص دیگری نمی‌تواند در این زمینه وارد شده و به مجازات و یا تنفیذ بپردازد. این نقص بدین شکل برطرف شده است که قانون فوق، ریاست این کمیته را به دادستان کل کشور سپرده است. همچنین وزیر دادگستری و یک نفر از کمیسیون قضایی مجلس نیز در این کمیته عضویت دارند.

قانون، ارائه‌دهندگان خدمت اینترنتی را موظف نموده است تا از فهرست کمیته تعیین مصادیق، جهت محدودنمودن دسترسی کاربران خود به سایت‌های غیرقانونی، پیروی نمایند. کارگروهی به ریاست دادستان کل کشور پس از طی جلساتی در جهت تعیین این فهرست، مصادیقی مشتمل بر پنج فصل را منتشر کرد.

بر اساس قانون، اعضای این کارگروه ـ که مرکب از وزارت‌خانه‌های ارتباطات و فن‌آوری اطلاعات، اطلاعات، فرهنگ و ارشاد اسلامی، آموزش و پرورش، سازمان تبلیغات، ناجا، صدا و سیما و ... می‌باشند ـ در راستای وظایف و مأموریت‌های خود مکلف شدند تا سامانه رصد فضای مجازی را در دستگاه متبوع خود ایجاد نمایند و

همچنین کلیه ارائه‌دهندگان خدمات دسترسی و میزبانی نیز مکلف شدند؛ چنانچه با یکی از مصادیق مصرحه در این فهرست مواجه شوند، بلافاصله مراتب را به دبیرخانه مستقر در دادستانی کل کشور اطلاع دهند. سرفصل این فهرست‌ها در ذیل آورده شده است.

۱ـ۲ـ۲. انتشار محتوا علیه عفت و اخلاق عمومی

به استناد بند ۲ ماده ٦ قانون مطبوعات، اشاعه فحشا و منکرات از مصادیق فیلترینگ محسوب می‌شود. همچنین ناظر به بند «ب» ماده جرایم رایانه‌ای و ماده ٦٤٩ مجازات اسلامی؛ تحریک، تشویق، ترغیب، تهدید یا دعوت به فساد و فحشا و ارتکاب جرایم منافی عفت نیز در زمره این مصادیق قرار دارند. همچنین استفاده ابزاری از افراد اعم از زن و مرد در تصاویر، تحقیر و توهین به جنس زن، تبلیغ تشریفات و تجملات نامشروع و غیرقانونی نیز می‌تواند منجر به فیلترکردن یک سایت شود.

۲ـ۲ـ۲. انتشار محتوا علیه مقدسات اسلامی

انتشار محتوای الحادی و مخالف موازین اسلامی، اهانت به اسلام و مقدسات آن یا اهانت به انبیاء عظام و ائمه معصومین علیهم‌السلام و حضرت *زهرا* علیهاالسلام، اهانت به حضرت *امام* خمینی رحمه‌الله و رهبر انقلاب و سایر مراجع مسلم تقلید، تبلیغات به نفع فرق منحرف و مخالف اسلام که بر طبق قانون مطبوعات و قانون مجازات اسلامی، فی‌نفسه جرم محسوب می‌شوند، از مصادیق فیلترینگ سایت‌های اینترنتی محسوب می‌شود.

۳ـ۲ـ۲. انتشار محتوا علیه امنیت و آسایش عمومی

همان‌طور که اشاره شد، کنترل اینترنت در برابر محتوای مخالف امنیت ملّی تقریباً یک اصل قابل قبول در هر کشوری می‌باشد. در میان فهرستِ مصادیق محتوای مجرمانه ایران نیز بیشترین محدودیت‌ها در راستای کنترل و حفظ امنیت ملّی وضع شده است. فعالیت‌هایی همچون تشکیل گروه‌های سایبری به قصد برهم‌زدن امنیت، اخلال در وحدت ملّی، تبلیغ علیه نظام، افشای اسناد محرمانه و انتشار محتوایی که به اساس جمهوری اسلامی لطمه بزند و ...، همگی منجر به مسدودنمودن سایت یا وبلاگ می‌شود.

۴ـ۲ـ۲. انتشار محتوا علیه مقامات و نهادهای دولتی و عمومی

اهانت، هجو و افترا به مقامات، نهادها و سازمان‌های حکومتی و عمومی و همچنین نشر اکاذیب و تشویش اذهان عمومی علیه این مقامات به استناد مواد ٦ و ٨ قانون مطبوعات و همچنین مواد ٦٠٩، ٦٩٧، ٦٩٨ و ٧٠٠ قانون مجازات اسلامی، می‌تواند موجب منع دسترسی به محتوای یک سایت یا وبلاگ شود.

۵ـ۲ـ۲. انتشار محتوای مرتبط با جرایم رایانه‌ای

ماده ۲۱ و ماده ۲۵ قانون جرایم رایانه‌ای برخی اعمال را ممنوع و قابل مجازات دانسته و کمیته تعیین مصادیق فیلترینگ نیز ارتکاب این جرایم را موجبی برای مسدودکردن سایتی دانسته که این اعمال در آن ارتکاب یافته است. اعمالی همچون انتشار، توزیع و در دسترس قراردادن یا معامله داده‌ها یا نرم‌افزارهایی که صرفاً برای ارتکاب جرایم رایانه‌ای به‌کار می‌رود؛ همچنین فروش، انتشار یا در دسترس قراردادن غیرمجاز گذرواژه‌ها و داده‌هایی که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی دولتی یا عمومی را فراهم می‌کند و نیز انتشار فیلترشکن‌ها و آموزش روش‌های عبور از سامانه‌های فیلترینگ.

۶ـ۲ـ۲. محتوای مجرمانه مربوط به امور سمعی و بصری و مالکیت معنوی

این امر شامل مواردی همچون: انتشار بازی‌های رایانه‌ای دارای محتوای مجرمانه، معرفی آثار غیرمجاز به جای آثار مجاز، عرضه تجاری آثار سمعی و بصری بدون مجوز وزارت فرهنگ و ارشاد اسلامی و تشویق و ترغیب به نقض حقوق مالکیت فکری می‌شود.

۷ـ۲ـ۲. محتوای تحریک، ترغیب، یا دعوت‌کننده به ارتکاب جرم

محتوایی که تحریک، ترغیب، یا دعوت به ارتکاب جرم می‌کند، می‌توان به مواردی همچون: تحریک به خودکشی یا اعمال خشونت‌آمیز، تبلیغ و ترویج مصرف مواد مخدر و روان‌گردان و سیگار، تشویق، تحریک و تسهیل ارتکاب جرایمی که دارای جنبه عمومی هستند (از قبیل اخلال در نظم، تخریب اموال عمومی، ارتشاء، اختلاس، کلاهبرداری، قاچاق مواد مخدر، قاچاق مشروبات الکلی و غیره)، **همچنین** بازانتشار و

ارتباط (لینک) به محتوای مجرمانه تارنماها و نشانی‌های اینترنتی مسدودشده، نشـریات توقیف‌شده و رسانه‌های وابسته به گروه‌ها و جریانات منحرف و غیرقانونی.

یکی از پیشرفت‌های این قانون روشن‌نمودن مرجع رسیدگی به شکایات است. چرا که ممکن است برخی مدعی باشند که مستحق مسدودنمودن سایتشان نبوده‌اند. تبصـره ۲ ماده ۲۱ کمیته تعیین مصادیق را مسئول رسیدگی به شکایات دانسته است و رأی این کمیته را نیز قطعـی اعـلام نمـوده اسـت. در حـالی کـه شایسـته‌تـر ایـن بـود؛ مرجـع تصمیم‌گیری و قضاوت، خود، مسئول تجدیدنظر نباشد و این بازبینیِ حکم به مرجعـی دیگر سپرده شود. به عنوان مثال این امکان وجود داشت که شعبه‌ای در نظر گرفته شود تا به صورت تخصصی به این اختلافات رسیدگی نماید.

نکته‌ای که ظاهراً در این قانون مغفـول مانـده اسـت، مرجـع پرداخـت خسـارات و غراماتی است که به واسطه فیلترینگ اشتباهی سایتی صورت می‌گیرد. واضح اسـت کـه فیلترینگی که به واسطه حساسیت به یک کلمـه اجـازه بازدیـد از سـایت را نمـی‌دهـد؛ درصد خطای بالایی خواهد داشت و بـدین علـت احتمـال مسدودشـدن سـایت‌هـایی تجاری که اشتباهاً فیلتر می‌شوند؛ وجود دارد. در حـالی‌کـه جبـران خسـارت ناشـی از تعطیلی مدت‌دار یک سایت در این قانون، پیش‌بینی نشده است.

آنچه نگاه اکثریت را در مقوله فیلترینگ در ایران معطوف به خود نموده است؛ ایجاد محدودیت برای سایت‌های سیاسی و خبری است. اصولاً درخواست فضای باز سیاسی در کشور این چالش را با حکومت موجب شده است که انسداد و جلوگیری از انتشـار برخی نظرات و ایده‌ها و احتمالاً اخبار از سـوی دولـت، عملـی خـلاف آزادی بیـان و اندیشه و بالتبع ناقض اصول بنیادین حقوق بشر است.

اشاره گذرا و تقریباً مبهم ماده ۱۷ قانون جرایم رایانه‌ای نیز بـه ایـن چـالش پاسـخ درخور شأنی نداده است:

> هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یـا مقامـات رسـمی بـه‌وسـیله سیستم رایانه یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یـا بـا همان مقاصد اعمالی را برخلاف حقیقت، رأساً یا به عنوان نقل قول، به شخص حقیقی یا حقوقی یا مقام‌های رسمی به طور صریح یا تلویحی نسـبت دهـد، اعـم از اینکـه از

طریق یادشده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج تا چهل میلیون ریال یا هر دو مجازات محکوم خواهد شد.

هرچند با نگاهی به فهرست مصادیق فیلترینگ، محدوده مجاز در جهت انتشار مطالب سیاسی و مرتبط با حکومت روشن می‌شود. برای مثال انتشار محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد کند و یا علیه اصول قانون اساسی باشد، موجبی برای فیلتر محسوب می‌شود. همچنین اهانت، هجو و افترا به مقامات، نهادها و سازمان‌های حکومتی و عمومی و همچنین نشر اکاذیب و تشویش اذهان عمومی علیه این مقامات نیز در این دایره محسوب می‌شود.

نکته دیگری که در این قانون به آن اشاره شده این است که اگر تخلف شخص یا گروهی در اینترنت را نتوان منطبق با قانون جرایم رایانه‌ای (به علت نقص قانون) احراز نمود؛ می‌توان بر مبنای قوانین جزایی عمل نمود.

نتیجه

فضای اینترنت به‌واسطه شرایط حاکم بر آن، رسانه‌ای است کاملاً دوسویه و یا چندسویه و به هیچ وجه با رسانه‌های سنتی‌تر مانند تلویزیون یا مطبوعات قابل مقایسه نیست. در عین‌حال فضایی کاملاً آزاد دارد و هر شخص با هر عقیده و مسلکی می‌تواند یک تریبون جهانی داشته باشد؛ لذا این موضوع تقریباً در تمام جهان مورد اجماع است که دولت باید در این فضا، نظارت‌های کاربردی و مؤثر داشته باشد. هم در آمریکا و هم در کشورهای اروپایی قوانینی با موضوع پالایش و جرم‌انگاریِ انتشار برخی محتواها وجود دارد. از مهم‌ترین دلایل به‌کارگیری ابزارهای محدودکننده می‌توان به حفظ امنیت ملّی، اخلاق عمومی، حریم خصوصی اشخاص و ... اشاره کرد. اصولاً پالایش محیط وب برای دولت یک وظیفه محسوب می‌شود؛ چون هر شخص با هر ایده و اخلاقی، در این محیط می‌تواند مطالبش را در تمام دنیا منعکس کند و بدین واسطه دیگران را متأثر سازد. برای مثال فردی که ویژگی‌های نژادپرستانه دارد و مایل است که مکنونات خود را از طریق اینترنت به دیگران نیز سرایت دهد، خطری برای

یک اجتماع سالم محسوب می‌شود. در عین حال دولت باید آزادی بیان و حق دسترسی افراد به مطالب مفید را در این فضا محترم بشمارد و به طور قانون‌مند بر اینترنت نظارت نماید. همچنین فیلترنمودن سایت‌هایی با رویکرد سیاسی نیز باید کاملاً در چارچوب قانون صورت پذیرد. در ایران نیز از سال ۱۳۸۸ قانون جرایم رایانه‌ای به تصویب مجلس شورای اسلامی رسید. این قانون کمیته‌ای را برای تعیین مصادیق فیلترینگ معین کرده و خدمات‌دهندگان اینترنت را موظف نموده است تا دسترسی به سایت‌هایی را که این کمیته اعلام می‌کند؛ ممنوع نمایند. در آخر لازم به ذکر است که نبود قانون جامعی در حمایت از حریم خصوصی و مبهم‌بودن مفاهیمی همچون امنیت ملّی در قوانین ایران، می‌تواند به قانون‌مداری فعالیت‌های حکومت، آسیب وارد کند.

منابع

۱. اسلامی، رضا؛ «آزادی‌های عمومی»؛ **جزوه درسی کارشناسی ارشد حقوق عمومی**؛ تهران: دانشگاه شهید بهشتی، ۱۳۸۵ .

۲. انصاری، باقر؛ «مقدمه‌ای بر مسئولیت مدنی ناشی از ارتباطات اینترنتی»؛ **مجله دانشکده حقوق و علوم سیاسی**، تهران، ش ٦۲، زمستان ۱۳۸۲.

۳. ــــــــــ؛ **آزادی اطلاعات**؛ تهران: انتشارات دادگستر، ۱۳۸۷.

٤. ــــــــــ؛ **حقوق ارتباط جمعی**؛ تهران: انتشارات سمت، ۱۳۸٦.

۵. ــــــــــ؛ **مسئولیت مدنی رسانه‌های همگانی**؛ تهران: معاونت پژوهش تدوین و تنقیح قوانین و مقررات اداره کل پژوهش و اطلاع‌رسانی، ۱۳۸۱.

٦. بردبار، محمدحسن؛ **درآمدی بر حقوق ارتباط جمعی**؛ تهران: ققنوس، ۱۳۸۰.

۷. جاویدان، رضا، امینی لاری، منصور، جنتی، سعید ؛ «فن‌آوری اطلاعات و ارتباطات، تعادل چالش‌ها و فرصت‌ها»؛ **مجله ره‌آورد نور**؛ ش ۱۳، زمستان ۱۳۸٤.

۸. جلالی فراهانی، امیرحسین؛ «پیش‌گیری وضعی از جرایم سایبر»؛ **فصلنامه فقه و حقوق**، پژوهشگاه فرهنگ و اندیشه اسلامی، ش ٦، پاییز ۱۳۸۲.

۹. خوشروزاده، جعفر؛ «مطبوعات و امنیت ملّی جمهوری اسلامی ایران»؛ **فصلنامه اندیشه انقلاب اسلامی**، ش ٦، تابستان ۱۳۸۲.

۱۰. دربیگی، بابک؛ **چالش‌های حقوقی، اخلاقی و اجتماعی فضای رایانه‌ای**؛ تهران: خانه کتاب، ۱۳۷۹.

۱۱. رحمدل، منصور؛ «حق انسان بر حریم خصوصی»؛ **مجله دانشکده حقوق و علوم سیاسی**؛ ش ۷۰، زمستان ۱۳۸٤.

۱۲. شجاعی، محمدصادق؛ «روان‌شناسی و آسیب‌شناسی اینترنت»؛ **فصلنامه علمی تخصصی روان‌شناسی و دین**؛ ش۱، بهار ۱۳۸۷.
۱۳. طبرسا، نقی؛ «گزارش‌های علمی، بررسی پدیده اینترنت در منطقه خلیج فارس»؛ **فصلنامه علوم سیاسی**؛ ش۱۳، بهار ۱۳۸۰.
۱٤. غمامی، سیدمحمدمهدی؛ «خطر سایبر برای کودکان»؛ **اصلاح و تربیت**؛ ش۳۷، تیر ۱۳۸٤.
۱۵. قاری سیدفاطمی، سیدمحمد؛ «آزادی بیان در آیینه حقوق بشر معاصر»؛ **مجله تحقیقات حقوقی**؛ ش٤۱. بهار و تابستان ۱۳۸٤.
۱٦. لوسین زهادی، رها؛ **مفاهیم کلیدی حقوق بشر بین‌المللی**؛ تدوین مهدی ذاکریان؛ تهران: نشر میزان، ۱۳۸۳.
۱۷. لیوینگستون، سونیا؛ «کودکان انگلیسی به اینترنت وصل می‌شوند»؛ ترجمه داوود حیدری؛ **آموزش علوم اجتماعی** (دوره هشتم)؛ ش ٤، تابستان ۱۳۸٤.
۱۸. معاونت کشف علمی جرم؛ «جرایم رایانه‌ای و اشاعه مفاسد اخلاقی»؛ **دانش انتظامی**، ش۹، تهران، تابستان ۱۳۸۰.
۱۹. میرعرب، مهرداد؛ «نیم‌نگاهی به مفهوم امنیت»؛ ترجمه سیدعبدالقیوم سجادی؛ **مجله علوم سیاسی**؛ ش ۹، تابستان ۱۳۷۹.
۲۰. مینایی، مهدی؛ «نقش اطلاع‌رسانی و رسانه‌های همگانی در ارتقای امنیت ملی»؛ **فصلنامه اندیشه انقلاب اسلامی**؛ ش ۹، بهار ۱۳۸۳.
۲۱. نمک‌دوست تهرانی، حسن؛ «اخلاق حرفه‌ای، حریم خصوصی و حق دسترسی به اطلاعات»؛ **فصلنامه رسانه** (سال هفدهم)؛ ش ۲، تابستان ۱۳۸۵.
۲۲. هاشمی، سیدحسین؛ «سخن سردبیر، تئوریزه‌کردن سانسور یا ترویج ول‌انگاری؟»؛ **رواق اندیشه**؛ ش ۳۲، مرداد ۱۳۸۳.
۲۳. هاشمی، سیدمحمد؛ **حقوق بشر و آزادی‌های اساسی**؛ تهران: نشر میزان، ۱۳۸٤.
۲٤. هیک، استیون، اف‌هلپین، ادوارد، هوسکینز، اریک ؛ **حقوق بشر و اینترنت**؛ ترجمه سیدقاسم زمانی و مهناز بهراملو؛ تهران: خرسندی، ۱۳۸۵.

25. Landree ,Eric, et al**; Freedom and Information**; Santa Monica, RAND Corporation, 2006.
26. . The Johannesburg Principles on National Security; **Freedom of Expression and Access to Information**; Human Rights Quarterly, Vol. 20, No. 1 (Feb., 1998).
27. Brooke, Heather; **Your Right to Know**; London, Pluto Press, 2005.
28. Çankayaa, Serkan and Odabasi, HaticeFerhan;"Parental controls on children's computer and Internetuse"; **World Conference on Educational Sciences,** 2009, available online at: www.sciencedirect.com.
29. E. Hull, Mary; **Censorship in America: a reference handbook**;(Contemporary world issues) California, 1999.
30. Grainger, Gareth; **Freedom of Expression and "Regulation of Information in Cyberspace**; Issues Concerning Potential, International Cooperation Principles for Cyberspace, The International Dimensions of Cyberspace Law, Law and Cyberspace Series, vol. 1, UNESCO Publishing Ashgate Dartmouth, 2000.
31. Hick, Steven and Halpin, Edward; **Children's Rights and the Internet**;Annals of the American Academy of Political and Social Science, Vol. 575, Children's Rights, 2001.
32. Rosenberg, R. S.; **Controlling Access to the Internet: The Role of Filtering, Ethics and Information Technology**; Kluwer Academic Publishers, Vol HYPERLINK "http://www.springerlink.com/content/1388-1957/3/1/".and "http://www.springerlink.com/content/1388-1957/3/1/"3,Number 1 ,2001.

33. Singh Khangura, Harinder; **Free Speech on the Global Internet: The Role of E-Commerce**; A Thesis Submitted in Partial Fulfillmten of The Requirements For The Degree of Master of Science; University of Toronto, 1997.