

به نام خدا

تحلیل فقهی - حقوقی فیلترینگ

مؤلف:

مهدی احمدی دستجردی «جرقویه ای»

انتشارات ارسطو
(چاپ و نشر ایران)
۱۳۹۹

فهرست مطالب

درآمد / صفحه ۸

فصل اول : مفهوم شناسی و مبانی حاکم بر فیلترینگ

/ صفحه ۱۹

۱-۱- فیلترینگ اینترنت؛ انواع و روش‌ها / صفحه ۲۳

۱-۲- فیلترینگ از طریق DNS / صفحه ۲۴

۱-۳- فیلترینگ به وسیله پروکسی / صفحه ۲۵

۱-۴- فیلترینگ به کمک سانسور افزارها / صفحه ۲۵

۱-۵- فیلترینگ به کمک مسدود کردن پورت‌ها /

صفحه ۲۶

۱-۶- لیست سیاه و لیست سفید / صفحه ۲۷

۱-۷- فیلترینگ معکوس / صفحه ۲۷

۱-۸- فیلترینگ هوشمند / صفحه ۲۸

۹-۱- مبانی قانونی فیلترینگ / صفحه ۳۲

۱-۹-۱- مروری بر مبانی آزادی اطلاعات / صفحه ۵۴

۲-۹-۱- مبانی فلسفی و ارکان حقوقی آزادی

مطبوعات و اطلاعات / صفحه ۵۶

۱۰-۱- مبانی آزادی اطلاعات / صفحه ۵۹

۱-۱۰-۱- حق مشارکت و تعیین سرنوشت / صفحه

۶۲

۲-۱۰-۱- شفافیت / صفحه ۶۸

۱۱-۱- مبانی حقوقی / صفحه ۷۳

۱-۱۱-۱- تعلق اطلاعات به مردم / صفحه ۷۳

۲-۱۱-۱- پاسخگو سازی حکومت / صفحه ۷۴

۳-۱۱-۱- خلاف قاعده بودن عدم ارائه اطلاعات /

صفحه ۷۶

۴-۱۱-۱- مبارزه با فساد اداری / صفحه ۷۸

فصل دوم: قواعد فقهی ناظر بر پالایش محتوی

مجرمانه / صفحه ۸۲

- ۲-۱- قاعده فقهی «لا ضرر و لا ضرار» / صفحه ۹۱
- ۲-۲- قاعده فقهی «حرمة الاعانة على الإثم» / صفحه ۱۰۲
- ۲-۳- قاعده حرمت همیاری در گناه در قلمرو خویش،
بسان دیگر قواعد فقه اسلام، / صفحه ۱۰۳
- ۲-۴- قاعده فقهی «حفظ نظام» / صفحه ۱۱۰
- ۲-۵- قاعده فقهی «لزوم دفع ضرر محتمل» / صفحه ۱۱۴
- ۲-۶- قاعده فقهی «نفی سبیل» / صفحه ۱۱۶
- ۲-۷- قاعده فقهی «وفای به عقود» / صفحه ۱۲۴

فصل سوم: رویکرد مداخله کیفری در قلمرو آزادی

اطلاعات / صفحه ۱۳۰

- ۳-۱- فیلتر اصول / صفحه ۱۳۹
- ۳-۲- فیلتر پیش فرض ها / صفحه ۱۴۸
- ۳-۳- فیلتر کارکردها / صفحه ۱۵۲
- ۳-۴- حمایت ایجابی (جرم انگاری به منظور تضمین
دسترسی قانونی به اطلاعات) / صفحه ۱۶۰
- ۳-۴-۱- جرم ممانعت از دسترسی به اطلاعات /

- ۳-۵- خصوصیت بزه دیده / صفحه ۱۷۰
- ۳-۶- موضوع بزه / صفحه ۱۷۱
- ۳-۷- نتیجه مجرمانه / صفحه ۱۷۳
- ۳-۸- رکن روانی / صفحه ۱۷۵
- ۳-۸-۱- علم / صفحه ۱۷۷
- ۳-۸-۲- عمد و اراده / صفحه ۱۷۸
- ۳-۸-۳- انگیزه. / صفحه ۱۷۹
- ۳-۹- جرم ممانعت در ایفای وظیفه کمیسیون انتشار و دسترسی آزاد به اطلاعات / صفحه ۱۸۴
- ۳-۹-۱- رکن قانونی / صفحه ۱۸۴
- ۳-۹-۲- رکن مادی / صفحه ۱۸۵
- ۳-۹-۳- نتیجه مجرمانه / صفحه ۱۹۱
- ۳-۹-۴- رکن روانی / صفحه ۱۹۲
- ۳-۱۰- جرم امحاء اطلاعات / صفحه ۱۹۳
- ۳-۱۰-۱- رکن قانونی / صفحه ۱۹۴

۳-۱۰-۲- رکن مادی / صفحه ۱۹۴

۳-۱۰-۳- شرایط و اوضاع و احوال لازم برای

تحقق بزه. / صفحه ۱۹۶

۳-۱۰-۴- رکن روانی / صفحه ۲۰۱

۳-۱۱- حمایت سلبی (جرم انگاری به منظور جلوگیری

از دسترسی غیر قانونی به اطلاعات) / صفحه ۲۰۳

نتیجه گیری / صفحه ۲۱۸

پیشنهادات / صفحه ۲۲۶

فهرست منابع / صفحه ۲۲۸

مقدس ترین واژه‌ها در لغت نامه دلم،
مادر مهربانم که زندگیم را مدیون مهر و
عطوفت آن می دانم.

مرحوم پدرم که سراسر مهربان، بردبار و
حامی بود

برادر و خواهرم که نشانه لطف الهی در
زندگی من هستند .

و یادگاران تمام عمر استاید گرانقدرم.

درآمد

«دانستن حق مردم است» حالا دیگر سال‌ها است در دنیا از یک شعار فراتر رفته و در قامت قانون دسترسی آزاد به اطلاعات خودنمایی می‌کند. قانونی که از سال‌های دور دغدغه بسیاری از کشورهای جهان بوده و به طور جدی از سال ۲۰۰۰ کشورهای مختلف، خود را مقید به اجرای آن می‌دانند و در ایران هم فرایند ۷ ساله را از زمان طرح تا تصویب و در نهایت رسیدن به مرحله اجرایی طی کرده است، اگرچه هنوز نتیجه ملموسی از اجرای آن به چشم نمی‌خورد. قانون انتشار و دسترسی آزاد به اطلاعات که در آخرین روزهای سال ۸۷ به عنوان لایحه به مجلس رفت و در بهمن ماه سال ۸۸ به تصویب رسید، حالا وارد فاز اجرایی شده است و قرار است

یک انقلاب در روابط ۱۵۰ ساله حاکمیت با مردم ایجاد کند. براساس این قانون، مؤسسات عمومی و خصوصی مکلف هستند اطلاعات خود را در اختیار عموم قرار دهند و مردم می‌توانند با مراجعه به این مؤسسات، اطلاعات مورد نیاز خود را درخواست و دریافت کنند. هدف اصلی این قانون جلوگیری از سودجویی از راه رانت یا ویژه‌خواری اطلاعاتی، شفاف‌سازی فعالیت‌های دولتی و عمومی، ایجاد بستر نظارت عمومی و کشف و مقابله با فساد است.

جریان آزاد اطلاعات دارای آثار مثبت و منفی است. از آنجایی که حفظ و دوام هر جامعه‌ای منوط به نظم موجود در آن است، لذا می‌توان گفت که نظارت در هر جامعه‌ای جهت جلوگیری از تعدی به حقوق مردم و نقض حریم شهروندان ضروری است. این مهم را می‌توان به عنوان نظریه ضرورت نظارت بر دسترسی آزاد به اطلاعات نیز معرفی کرد. جریان آزاد اطلاعات می‌تواند به رشد و بالندگی،

توسعه جامعه و تکامل انسان منجر شود، همچنین می‌تواند برای بسیاری از گروه‌های حاشیه‌ای فرصتی منحصر به فرد به وجود آورد تا صدای قبلاً ناشنیده خود را از طریق مجراهای ارتباطی همچون اینترنت، به گوش دیگران برسانند. لذا کارشناسان حوزه فناوری اطلاعات و ارتباطات تمایل دارند، تا مردم با استفاده از ابزارها و روش‌های مختلف، ضمن حفظ دستاوردهای این پدیده نوین و استفاده صحیح از آن، برای مقابله با چالش‌های در حال ظهور عصر اطلاعات و نیروهای رقیب آن در سطح ملی و بین‌المللی، آماده‌تر شوند و برای تحقق چنین درخواستی باید تعاملی مثبت بین جامعه و دولت وجود داشته باشد. فلذا این قانون برای تبدیل شدن به یک فرصت ویژه و کمک به بهبود روابط استراتژیک دولت-ملت نیاز به یک کار جدی و عمیق دارد، این کار فقط بر عهده دولت نیست، سایر دستگاه‌های اجرایی و نظارتی، رسانه‌ها و دانشگاه‌ها نیز باید همکاری داشته باشند.

در قرارداد نوشته و نانوشته حاکمیت و مردم، یکی از مبانی دموکراسی: آزادی بیان، دسترسی آزاد به اطلاعات، انتشار اطلاعات و دریافت داده‌های مربوط به امور سیاسی، اداری، قضایی و... توسط مردم است. ساختار قدرت در جامعه‌ای مبتنی بر احترام به حقوق شهروندی، در بخش انتشار اطلاعات نیز همین حقوق را برای شهروندان قائل است. در ایران موضوع انتشار و دسترسی آزاد به اطلاعات به دلیل وجود تفاسیر متعدد و برداشت‌های مختلف در شیوه اجرای این ضابطه، تا مدت‌ها محل بحث و اختلاف بود تا اینکه تصویب قانون مربوط به آن در سال به این اختلافات و ابهامات، هر چند دیر هنگام پایان داد (نمک دوست تهرانی، ۱۳۸۴)

با این حال نمی‌توان اهمیت حیاتی این قانون را نادیده گرفت و یادآور نشد که این قانون گذر از مرحله تردید و ابهام و ورود به گستره جدیدی از پذیرش حقانیت مردم و مطالبات آنان در خصوص

اخبار و اطلاعاتی است که در زندگی نوین امروز بدون آن امکان مشارکت در اداره مملکت ممکن نیست و خسران این عمل نه تنها متوجه مردم و موجب تحکیم ناآگاهی آنان، بلکه اعمال ضرر به حاکمیت، نظام و نهادهای عمومی خواهد بود. زیرا هر چه آگاهی مردم بالا رود، امکان مشارکت مسئولانه و اقدامات بخردانه آنان در امور جاری کشور و نقد نشات گرفته از اطلاعات جدید و ارائه پیشنهادات نوین برای حل مشکلات، می تواند در توسعه کشور موثر و مفید باشد. بنابراین وجود این قانون ما را وارد فضای جدیدی در دهه ۴۰ بعد از انقلاب کرده و نهادهای عمومی را به سمت ارائه اطلاعات، انتشار اخبار و اطلاع رسانی به مردم هدایت می کند و از طرفی با تأمین حقوق مردم در خصوص دسترسی آزاد به اطلاعات آنان را در جریان مسائل ریز رویدادها که می تواند بنیادی نیز باشد قرار می دهد (ویژه و طاهری، ۱۳۹۰: ۲۳۸)

چنین قوانینی می‌تواند در اجرای حقوق مردم، منبعث از اصول ۱۹ تا ۴۲ قانون اساسی موجب احساس امنیت در آحاد مردم شود، زیرا دسترسی آزاد به اطلاعات، موجب آمادگی مردم در برخورد با معضلات و همراهی با دولت در اجرای برنامه‌ها و احتراز از شایعه‌سازی و شایعه‌پراکنی در سطح کشور و جذب اخبار از مجاری غیرقابل اطمینان شود. متأسفانه این مهم در سال‌های گذشته مغفول مانده بود و بازار شایعه و مراجعه به منابع خارجی به حدی داغ شده بود که مردم بسیاری از اخبار و اطلاعات را از فضاهاى دیگر تحصیل نموده و در نتیجه، تعارض موجود بین اطلاعات دریافتی از منابع خارجی و اطلاعات منتشره در داخل کشور، سبب نوعی بدگمانی و دوری از رسانه‌های داخلی به ویژه رسانه ملی شد، به گونه‌ای که بخش مهمی از مخاطبین خود را از دست داد. این درحالی است که به نظر کارشناسان اگر چنین قانونی همان یک دهه پیش به اجرا درآمده بود، احتمال بروز

حوادث سیاسی ناگواری که به ویژه در اواخر دهه هشتاد شاهد آن بودیم، بسیار کاهش یافته یا حداقل تا این پایه آسیب رسان نمی‌بود. بر این اساس و با توجه به حجم‌های سیاسی دروغین و بی پایه غرب و معاندین نظام مبنی بر عدم وجود ساختاری دموکرات و مردمی در کشورمان، به نظر می‌رسد نقش چنین قوانینی نسبت به این ادعاهای بی اساس، نقشی اساسی است و بی شک ارزش هزینه‌هایی که به همراه می‌آورد را دارد. اما آنچه مهم تلقی می‌شود، تنها تأکید بر آزادی و تأمین حقوق مردم در تحصیل و دسترسی آزاد به اطلاعات نیست، مهمتر از آن، تعیین تکلیف و اجبار نهادهای عمومی به ارائه اطلاعاتی است که دانستن آنها حق مردم است. چرا که مردم، صاحبان حق بوده و حاکمیت و قوای سه گانه، مجری خواسته‌های مردم و مکلف به تأمین نیازهای مردم هستند. بر اساس این قانون ضمن تأمین این حقوق باید زمینه‌های سانسور و فیلترینگ اطلاعات به

حداقل رسانده شود. البته در مواقعی که اطلاعات مربوط به امور خلاف اخلاق و ارزش‌های حیاتی یک کشور باشد، کماکان معیارهای خاص قانونی حاکم است و وظیفه حاکمیت این است که مردم را از مسیر این اطلاعات خسران ساز در حاشیه امنیت قرار داده و حراست نماید. اما نهادها و ارگان‌ها نباید به بهانه جلوگیری از اطلاعات نادرست، به صورت سلیقه‌ای ارائه و انتشار اطلاعات را ممنوع نمایند.

ایجاد ساختارهای لازم و بسترهای مناسب جهت اجرایی شدن این قانون پیش‌نیاز التزام عملی به شعار «دانستن حق مردم است» می‌باشد. اولین گام در هموار کردن مسیر اجرای این قانون «فرهنگ‌سازی و نهادینه کردن» آن است. باید مدیران ما این قانون را باور داشته باشند، کارمندان ما خود را ملزم به ارائه اطلاعات به ارباب رجوع بدانند، و مردم هم مطلع باشند که دسترسی آزاد

به اطلاعات چیست و براساس این قانون چه حق و حقوقی برای آنها ایجاد می‌شود. پس برای اینکه فهم عمومی از این قانون ایجاد شود، فرهنگ‌سازی و آموزشی عمیق لازم است. اگر این قانون به‌عنوان گفتمان رایج جا بیفتد و همه درباره آن حرف بزنند خودبه‌خود به مطالبه عمومی تبدیل می‌شود. از طرفی قانون دسترسی آزاد به اطلاعات همان قدر که می‌تواند نتایج مثبتی در زمینه جلوگیری از فساد داشته باشد، ممکن است ابزاری شود برای آبروبری و آبرودهی و نوعی فوتبال سیاسی؛ بنابراین باید زمینه‌های فرهنگی این قانون فراهم شود. رسانه‌ها به‌عنوان یکی از ابزارهای اجرایی این قانون، هم در ایجاد مطالبه بین مردم و دستگاه‌ها و هم گفتمان‌سازی برای آن، سهم مهم و موثری دارند. طبیعی است داشتن فضای آزاد رسانه‌ای و نزدیک شدن فضاهای خبری و رسانه‌ای به استانداردهای جهانی پیش‌زمینه‌ای برای اجرای این قانون است. یکی دیگر از الزامات جهت اجرای این قانون، در دسترس

بودن اطلاعات به صورت الکترونیکی و تحقق دولت الکترونیک است. بهترین شیوه تکریم ارباب رجوع، حرکت دولت به سمت الکترونیکی شدن است که سبب حذف مسیر پیچیده بوروکراسی اداری است. هر چند محوریت اجرای این قانون وزارت فرهنگ و ارشاد اسلامی است، اما از آنجا که قرار است وزارت ارتباطات بستر فنی رسیدن اطلاعات به دست مردم را فراهم کند، مرتب‌ترین وزارتخانه با اجرای این قانون است و البته تکرار و تاکید چندین باره وزیر ارتباطات بر اجرای قانون دسترسی آزاد به اطلاعات خود حکایت از جایگاه این وزارتخانه در برقراری جریان آزاد اطلاعات دارد. (نمک دوست تهرانی، ۱۳۸۴)

به نظر می‌رسد تغییر قوانین دیگر برای هماهنگ شدن با این قانون و تعریف شفاف و دقیق از مفاهیم و خط قرمزهایی نظیر هتک حرمت، حریم خصوصی، منافع و امنیت ملی و یکپارچه سازی

آرشیوهای سازمان‌های دولتی و خصوصی و فراهم آوردن امکان دسترسی آرشیو ملی به همه اسناد، از اقدامات دیگریست که برای اجرایی شدن این قانون ضروری است. با توجه به این نکته که جریان آزاد اطلاعات یا آزادی اطلاعات در سال‌های آغازین قرن بیست و یکم جایگاه ویژه‌ای دارد و از آن به عنوان اکسیژن دموکراسی نام برده می‌شود و اجرای این قانون در ایران را می‌توان در حکم انقلابی اساسی در نظام اداری، اجرایی و مدیریتی کلان کشور ارزیابی نمود، پژوهش حاضر بر آن است که بررسی سازکارهای مهم بر دسترسی آزاد بر اطلاعات پردازد

فصل اول :

مفهوم شناسی و مبانی حاکم بر فیلترینگ

مفهوم فیلترینگ یا محدود کردن اطلاعات بسیار قدیمی تر و گسترده تر از اینترنت است. این مفهوم را می‌توان در «سانسور» جستجو کرد. فرهنگ انگلیسی آکسفورد (۲۰۱۴) سانسور را اینگونه تعریف می‌کند: «یک قدرت ذهنی یا نیرویی است که عناصر خاصی را در ناخودآگاه، سرکوب می‌کند و مانع پدیدار شدن آنها در

ذهن خود آگاه می‌شود. سانسور به عنوان یک مقام رسمی در برخی از کشورها، وظیفه بازبینی تمام کتاب‌ها، نشریات، آثار نمایشی و غیره را قبل از انتشار بر عهده دارد تا تضمین کند که آنها شامل چیزی غیر اخلاقی، بدعت، یا توهین آمیز نباشند.» در ادبیات، سانسور به عنوان کنترل اطلاعات و انتشار یا گردش ایده‌ها در یک جامعه تعریف شده است. (بیتسو، ۲۰۱۴: ۴۲). اما سانسور اینترنت به خوبی تعریف نشده است و به سمت مخدوش‌سازی، سواستفاده و تبلیغات در حال تغییر است. (بارنت و فیمستر، ۲۰۱۳: ۸۴)

گسترش اینترنت زمینه‌ای را به وجود آورد که طیف وسیعی از اطلاعات بدون هیچگونه محدودیتی و فراتر از مرزهای جغرافیایی در سراسر جهان منتشر شود و به نحو چشمگیری به یک رسانه ارتباطی و اطلاعاتی تبدیل گردد. ضمن اینکه مخاطبان و کاربران اینترنت هم به همان اندازه

افزایش مداومی داشته اند. خصوصیت و ویژگی اینترنت و سهولت انتشار مطالب و اطلاعات و علاوه بر آن راحتی دستیابی به انواع مختلف اطلاعات در وب اعم از متن، صوت و تصویر و داده‌های گرافیکی متنوع، به اندازه ای شدت یافته است که در برخی موارد اطلاعات حاوی مطالب مخرب و زیانباری نیز در وب منتشر می‌شود که زمینه سوء استفاده‌های مختلف را فراهم آورده است. هرزه نگاریهای جنسی بخصوص در زمینه سوء استفاده از کودکان، ترویج خشونت و فساد، خرید و فروش مواد مخدر و زیانبار، اشاعه اطلاعات خصوصی افراد و سازمانها، استفاده از اطلاعات وب در جهت اهداف تروریستی و موارد مشابه، ضرورت کنترل محتوای وب را ناگزیر ساخته است، ولی این کنترل و نظارت برانتشار اطلاعات در جوامع مختلف و بر حسب خط مشی‌های سیاسی و فرهنگی هر جامعه ای نمودهای متفاوتی داشته است. در برخی جوامع غربی تاکید بیشتر بر عدم سوء استفاده از اطلاعات

خصوصی افراد و جلوگیری از انتشار تصاویر جنسی کودکان و ممانعت از دسترسی سازمانهای تروریستی به اطلاعات خاص و مهم است اما کنترل محتوای اینترنت در جوامع شرقی و مذهبی فراتر از موارد فوق است و نظارت شدید بر اشاعه افکار و عقاید سیاسی در شبکه جهانی را نیز شامل می‌شود. به‌طور مثال در کشور چین که مقام اول را در جهان از نظر تعداد کاربران اینترنت داراست، نظارت گسترده‌ای بر محتوای اطلاعات سیاسی صورت می‌گیرد و سانسور شدید بر عقاید و اندیشه‌های متضاد با حکومت کمونیستی چین در وب حاکم است و به این منظور “پلیس اینترنت” در این کشور نیز با این هدف شکل گرفته است. (ولایتی، ۱۳۸۵: ۱)

در تعریفی دیگر سانسور یا فیلترینگ اینترنت، عبارت است از محدود کردن دسترسی کاربران اینترنت به وبگاه‌ها و خدمات اینترنتی که از

دیدگاه متولیان فرهنگی و سیاسی هر کشور برای مصرف عموم مناسب نیست، اعمال فیلتر به وسیله ارائه دهندگان خدمات اینترنتی انجام می‌شود ولی تعیین سطح، مصادیق و سیاست‌های فیلترینگ با حکومت‌هاست. (مولایی، ۱۳۸۵: ۱۲۴)

در این پژوهش نیز منظور از فیلترینگ، محدود سازی اطلاعات و محتوای سایت‌های اینترنتی است که با توسل به مصوبات و قوانین دولتی نامناسب تشخیص داده شده است.

۱-۱- فیلترینگ اینترنت؛ انواع و روش‌ها

هر چند شیوه‌های متعددی برای اعمال فیلترینگ در جهان وجود دارد اما در گذشته به طور کل دو روش فیلترینگ، یعنی فیلترینگ بر اساس بانک اطلاعات ثابت و فیلترینگ بر اساس

محتوای صفحات در جهان اعمال می‌شد که در سال‌های اخیر این دو روش به طور یکپارچه ترکیب شده‌اند. در سیستم جدید تمام مواردی که توسط کاربران دیده می‌شود دوباره در مورد آنها تصمیم‌گیری می‌شود. اگر دیدن صفحه‌ای درست نباشد و صفحه برای کاربر فیلتر نشده باشد در مشاهده مجدد دسترسی به صفحه غیرممکن می‌شود. (بصیریان جهرمی، ۱۳۹۲: ۴۲) از بعد فنی روش‌هایی که فیلترینگ و محدودسازی اطلاعات و محتوای سایت‌ها انجام می‌شود، عبارتند از:

۱-۲- فیلترینگ از طریق DNS

سرویس DNS نام هر دامنه را به IP آدرس متناظرش ترجمه می‌کند. آدرس سروری که سرویس DNS را ارائه می‌دهد، به طور اتوماتیک و در هنگام برقراری اتصال به اینترنت از طریق ISP در اختیار کامپیوتر شما گذاشته می‌شود.

اگر این سرور DNS ، سانسور کننده باشد، کلید درخواست‌ها برای سایت‌های غیرمجاز را بی‌پاسخ می‌گذارد.

۱-۳- فیلترینگ به وسیله پروکسی

در این روش ISP دسترسی مستقیم به اینترنت را محدود کرده و شما را ملزم به استفاده از پروکسی می‌کند. باید در تنظیمات مرورگر، آدرس پروکسی سروری را که ISP داده را وارد کنید. کلید_درخواست‌ها به پروکسی فرستاده می‌شود و در صورت مجاز بودن درخواست، پروکسی آن را از اینترنت گرفته و برایتان ارسال می‌کند.

۱-۴- فیلترینگ به کمک سانسور افزارها

این نرمافزارها بیشتر در منزل (برای کنترل والدین بر فرزندان)، مدارس و دانشگاهها استفاده می‌شوند و در حقیقت نوعی فیلترینگ سفارشی هستند که در کشورهای مثل آمریکا به کار گرفته می‌شوند. مانند: نت نی، سایبر پورتال، سایبر ستر

۱-۵- فیلترینگ به کمک مسدود کردن پورت‌ها

پورت‌ها مانند درهایی هستند که سرور از طریق آنها سرویس‌هایش را ارائه می‌دهد. اگر پورتی بلوک شود، تمام سرویس‌هایی که از طریق آن پورت ارائه می‌گردد، غیر قابل دسترس است. بیشتر پورت‌های ۸۰، ۳۱۲۸، ۸۰۸۰ مسدود می‌شوند، زیرا پورت‌های متداول برای پروکسی‌ها هستند.

۱-۶- لیست سیاه و لیست سفید

لیست سیاه: شامل آدرس مجموعه سایت‌هایی است که دسترسی به آن‌ها مجاز نیست. گاهی هم از کلمات کلیدی استفاده می‌شود به طوری که اگر در سایت مورد درخواست این کلمات وجود داشته باشد، بلوک می‌شود. لیست سفید: شامل آدرس مجموعه سایت‌هایی است که دسترسی به آنها مجاز می‌باشد. در سازمان‌هایی استفاده می‌شود که می‌خواهند کارمندانشان فقط به تعداد معدودی سایت دسترسی داشته باشند.

۱-۷- فیلترینگ معکوس

این نوع فیلترینگ در مقصد انجام می‌شود. سرور شرکت ارائه دهنده خدمات، قبل از ارائه هر گونه سرویسی، ابتدا IP مشتری را چک می‌کند و در صورتی که متعلق به یک کشور تحریم شده

باشد، از ارائه سرویس سرباز می‌زند.

۱-۸- فیلترینگ هوشمند

اما آنچه اخیراً بحث‌های گوناگونی پیرامون آن مطرح شده است، نوع جدیدی از فیلترینگ موسوم به «فیلترینگ هوشمند» است. بنا بر نظر کارشناسان، فیلترینگ هوشمند برنامه‌ای است که در صورت اجرا، به کاهش نارضایتی مردم از فیلترینگ کمک خواهد کرد و ضمن جلوگیری از سرقت اطلاعات ملی، خلل وارد شده به فعالیت افراد را به حداقل ممکن می‌رساند.

طبق تعاریف موجود و نمونه‌های تطبیقی سایر کشورها، یکی از مواردی که قرار است در فیلترینگ هوشمند مورد توجه قرار گیرد، این است که در برخورد با یک صفحه، به جای فیلتر کردن تمام آدرس، بخشی از آن مسدود شود. در نتیجه

چنین روندی، در یک سایت هم چون فیس بوک، تنها برخی صفحات مسدود شده و دسترسی به سایر صفحات، آزاد خواهد بود.

از سوی دیگر، در فیلترینگ هوشمند قرار است میان دسترسی‌های افراد، تمایزاتی ایجاد شود و سطحی از دسترسی بیش تر یا دسترسی کم تر، برای افراد متناسب با سن، شغل و تخصص شان، در نظر گرفته شود. برای مثال سطح دسترسی به اینترنت برای یک پژوهشگر در مقایسه با یک دانش آموز متفاوت خواهد بود که البته با توجه به اینکه اجرای این عملکرد، به تشخیص هویت افراد نیاز دارد، ابعاد اجرایی این بخش از پیشنهاد، همچنان در مرکز ملی فضای مجازی در دست بررسی است.

از دیگر الزامات فیلترینگ هوشمند، امکان درک و پردازش تصویر است که در نتیجه آن می‌توان امیدوار بود که تنها برخی از تصاویر مغایر

با اخلاق سایت‌ها فیلتر شوند، بی آن که قرار باشد تمام آدرس آن سایت مسدود شود. نرم‌افزار فیلترینگ هم چنین باید قادر باشد که بر اساس محتوا مسدود سازی را انجام دهد. برای مثال باید بتواند میان یک مطلب پزشکی که در آن از برخی کلمات خاص استفاده شده است و مطالب دیگری که از همان کلمات استفاده می‌کنند، تمایز قائل شود.

فاریس و ویلنثو دسته بندی دیگری از «گزینه‌های فیلترینگ محتوا»^۱ را اینگونه برشمرده اند: فیلترینگ سیاسی، فیلترینگ اجتماعی و فیلترینگ امنیتی/متعارض^۲ فیلترینگ سیاسی شامل دیدگاه‌ها و اطلاعاتی می‌شود که در فضای اینترنت در مخالفت با حکومتی بر سر قدرت است و نسبت به مصادیقی همچون حقوق بشر،

1. Content filtering choices

2. Political, social, and security/conflict filtering

آزادی بیان، حقوق اقلیت‌ها و جنبش‌های مذهبی و نظایر آن اعمال می‌گردد. فیلترینگ اجتماعی بر رویکردهای اخلاقی، هنجارها و نظام ارزشی جامعه متمرکز است که اغلب به هرزه‌نگاری، قمار، مواد مخدر، مشروبات الکلی و مسائلی از این دست می‌پردازد. (فاریس و ویلنئو، ۲۰۰۸: ۹)

فیلترینگ امنیتی نیز ناظر بر انسداد اطلاعات و محتواهایی است که به مناقشات مرزی، درگیری‌های مسلحانه، جنبش‌های جدایی طلبانه و گروه‌های شبه نظامی پرداخته‌اند. با این حال در کنار این سه مورد، نوع دیگری از فیلترینگ نیز مشهور به فیلترینگ «ابزارهای اینترنتی»^۱ وجود دارد که به اختلال در ایمیل، الگوریتم موتورهای جستجو، خدمات صدا روی اینترنت و روش‌های دور زدن فیلترینگ و سانسور منجر می‌شوند و مکمل فنی آن روش‌ها است.

1. Internet tools

۱-۹- مبانی قانونی فیلترینگ

قانون جرایم رایانه‌ای و فهرست مصادیق محتوای مجرمانه حدود محدودیت‌ها بر فضای اینترنت را تعیین می‌کنند هر چند که بسیاری از محدودیت‌های اعمال شده در فضای اینترنت خارج از این چارچوب‌ها و گاهی بر اساس اعمال سلیقه انجام می‌گیرد اما بررسی این قوانین ضروری است.

بر اساس ماده ۲۱ قانون جرائم رایانه‌ای ارائه دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی «کارگروه (کمیته) تعیین مصادیق» موضوع ماده ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرائم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می‌رود را پالایش (فیلتر) کنند.

طبق این فهرست محتوای مجرمانه شامل محتوا علیه عفت و اخلاق عمومی، محتوا علیه مقدسات اسلامی، محتوا علیه امنیت و آسایش عمومی، محتوا علیه مقامات و نهادهای دولتی و عمومی، محتوا مرتبط با جرایم رایانه ای، محتوای مرتبط با سایر جرایم، محتوا مجرمانه مربوط به امور سمعی و بصری و مالکیت معنوی، محتوای مجرمانه مرتبط با انتخابات مجلس شورای اسلامی و محتوای مجرمانه مرتبط با انتخابات ریاست جمهوری هستند. این مصادیق با استناد به قانون مجازات اسلامی، قانون مطبوعات، قانون جرایم رایانه ای، قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی، قانون بازار و اوراق بهادار، قانون جامع کنترل و مبارزه ملی با دخانیات، قانون حمایت از حقوق پدیدآورندگان نرم افزارهای رایانه ای، قانون تجارت الکترونیکی، قانون انتخابات مجلس شورای اسلامی، قانون انتخابات ریاست جمهوری و قانون اخلال در نظام اقتصادی کشور تنظیم شده

است.^۱

بر فهرست فوق نقدهایی نیز وارد شده است، باقر انصاری عضو هیئت علمی دانشکده حقوق دانشگاه شهید بهشتی در گفتگویی با مرضیه خلقتی خبرنگار حقوقی خبرگزاری دانشجویان ایران (ایسنا) این فهرست را مورد نقد و بررسی قرار می‌دهد، که در ادامه به بخشی از این نقد و بررسی اشاره می‌کنیم؛

این فهرست بیش از آنکه به مصادیق مجرمانه پرداخته باشد، به گردآوری عناوین مجرمانه که پیش از آن در قوانین دیگر وجود داشت پرداخته است، فهرست منتشره از نظر یک کاسه کردن عناوین مجرمانه اقدامی جدید محسوب می‌شود اما نتوانسته وظیفه اصلی خود را در تعیین روشن و واضح مصادیق محتوای مجرمانه به انجام برساند.

۱. فهرست مصادیق محتوای مجرمانه و قوانین مورد استناد در پیوست شرح داده شده است.

به گفته انصاری وظایف کارگروه تعیین مصادیق محتوای مجرمانه عبارتند از: تهیه فهرست مصادیق محتوای مجرمانه و انتشار آن ، دوم تشخیص مصادیق محتوای مجرمانه است که در صورت تشخیص مبنی بر مجرمانه بودن محتوا، دستور فیلتر یا پالایش آن داده می شود. «تشخیص، کار قضایی است و بر اساس آن، آنچه منتشر شده با آنچه که قبلا منع شده، تطبیق داده می شود. اگر مطلبی در زمره مصادیق محتوای مجرمانه تشخیص داده شد دستور فیلترینگ داده می شود که البته در خصوص این دستور هم ابهاماتی وجود دارد مثلا پس از صدور دستور پالایش، آیا فقط مطلب فیلتر می شود یا کل سایت فیلتر می شود که این موضوع چندان روشن نشده و محل بحث است.»

سومین وظیفه کارگروه رسیدگی به شکایات ناشی از فیلترینگ فهرستی که این کارگروه منتشر می کند، در اختیار ارائه دهندگان خدمات اینترنتی