

پالایش (فیلترینگ) اینترنت در اروپا^۱

مترجم: حامد بابازاده مقدم^۲

عمار اسلامخواه^۳

مقدمه

در کمتر از یک دهه، اینترنت در اروپا از محیطی تقریباً بی قید و بند به محیطی تبدیل شد که در آن فیلترینگ در بسیاری از کشورها، به ویژه در سطح اتحادیه اروپا (EU)، هنجار است و نه استثناء. در مقایسه با بسیاری از کشورها در مناطق دیگر که محتوای اینترنت را مسدود می نمایند، ظهور فیلترینگ در اروپا به دلیل جدایی آن از سنت قوی فرآیندهای دموکراتیک و تعهد به آزادی بیان، قابل توجه است.

فیلترینگ در شکل های مختلف انجام می شود، از جمله دستور دولت مبنی بر حذف محتوای غیر قانونی در وب سایت هایی که در داخل کشور میزبانی می شود، مسدود کردن محتوای غیر قانونی که در خارج از کشور میزبانی می شوند، و فیلتر کردن نتایج توسط موتور جستجو مربوط به محتوای غیرقانونی. مانند بسیاری از کشورها در سراسر جهان که درگیر فیلترینگ اینترنت هستند، تفاوت بین فیلترینگ داوطلبانه و الزامی دولت تا حدودی در اروپا مبهم و نامشخص است. در بسیاری از موارد فیلترینگ توسط ارائه دهندگان خدمات اینترنتی^۴، موتورهای جستجو و تامین کنندگان محتوا در اروپا، به صورت "داوطلبانه" با این درک ضمنی انجام شده که همکاری با مقامات دولتی، از مقررات گذاری بیشتر برای فیلترینگ جلوگیری می نماید.

^۱ این نوشتار ترجمه بخش "Internet Filtering in Europe" نوشته خانم Sangamitra Ramachander از مأخذ زیر می باشد:
Access Denied-The Practice and Policy of Global Internet Filtering(London: Cambridge, 2008)

^۲ دانشجوی دکتری حقوق بین الملل دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران
hmoghadam32@yahoo.com

^۳ دانشجوی کارشناسی ارشد روابط بین الملل دانشگاه آزاد اسلامی واحد کرج
eslamiammar@gmail.com

^۴ ISP

دامنه محتوای غیرقانونی که در اروپا فیلتر می شود، تا حد زیادی محدود به پورنوگرافی کودکان، نژادپرستی و مواردی است که به ترویج نفرت و تروریسم می پردازد؛ هر چند اخیراً پیشنهادات و بازنگری هایی در قوانین برخی کشورها انجام شده که با فیلترینگ اینترنت در سایر حوزه ها مانند کپی رایت و قمار مواجه هستند. فیلترینگ همچنین در مورد تهمت و افترا نیز صورت می گیرد؛ این عمل با انتقاداتی مواجه شده است؛ به خصوص در انگلستان برای محدود کردن رفتارهای آنلاین قانونی و ترویج بیش از حد رفتارهای تهاجمی و سیاست خرابکاری، که در آن شرکت های مربوطه بلافاصله محتوای مورد نظر را از ترس اقدام قانونی حذف می نمایند.

شرکت های ارائه دهنده خدمات اینترنتی در اروپا به طور کلی هیچ الزام و تعهدی برای نظارت بر استفاده از اینترنت ندارند و از مسئولیت در مقابل محتوای غیرقانونی در سطح اتحادیه اروپا معاف هستند؛ اما هنگامی که متوجه چنین محتوایی می شوند باید آن را فیلتر کنند. بنابراین درجه فیلترینگ در کشورهای عضو بستگی به تلاش های دولت، پلیس، گروه های حامی، و عموم مردم در شناسایی و گزارش محتوای غیرقانونی دارد.

در طول دهه گذشته تلاش هایی برای ایجاد مجموعه ای از سیاست ها و اقدامات مشترک در سطح اتحادیه اروپا برای مقررات گذاری اینترنت صورت گرفته است. این اقدامات به عنوان یک ضرورت برای ترویج رقابت و تجارت منطقه ای، مقابله با جرایم اینترنتی و تروریسم، و به عنوان یک برنامه محمل برای به اشتراک گذاشتن بهترین شیوه در میان ملت ها دیده می شود. پیشرفت های قابل توجهی در مقررات گذاری در سطح اتحادیه اروپا - هر چند نه به طور مستقیم در حوزه فیلترینگ - شامل تعریف مسئولیت شرکت های ارائه دهنده خدمات نسبت به محتوای غیرقانونی و تعهدات آنها نسبت به حفظ داده ها صورت پذیرفته است.

مقررات منطقه ای

موضوع تکراری در سراسر این بررسی اجمالی، ماهیت قانون در هر کشور با مقررات منطقه ای است که یکدیگر را همپوشانی می دهند. مقابله با فعالیت های جنایی در اینترنت و ترویج رقابت کلی در صنعت اینترنت، دلایل اصلی ذکر شده برای توسعه یک

چارچوب نظارتی منطقه ای بوده است.^۱ رویکرد منطقه ای در اروپا با ارائه درخواستی توسط شورای اروپا به کمیسیون اروپا در ماه آوریل سال ۱۹۹۶ برای تولید "خلاصه ای از مشکلات ناشی از توسعه سریع اینترنت" و ارزیابی نیاز برای تنظیم مقررات گذاری، آغاز شد. کمیسیون گزارشی با عنوان "محتوای غیر قانونی و مضر در اینترنت" و یک گزارش مقدماتی از طرح در مورد "حفاظت از کودکان و کرامت انسانی در خدمات سمعی و بصری" در پاسخ به درخواست شورای اروپا، تدوین نمود.

بر اساس این اسناد "یک چهارچوب مشترک برای خود کنترلی (اینترنت) در سطح اروپا" تهیه شد که در نهایت به یک طرح عملیاتی برای ترویج استفاده امن از اینترنت تبدیل شد. این طرح که در ۲۵ ژانویه ۱۹۹۹ به تصویب رسید و تا سال ۲۰۰۲ عملیاتی بود، اصول اساسی تنظیم محتوای اینترنت در سطح اروپا را تشریح نمود.^۲ از دیدگاه کلی تر، محتوای نامطلوب بر روی اینترنت به "غیر قانونی" و یا "مضر" طبقه بندی می شود. دامنه "غیر قانونی" بودن محتوا بین کشورهای مختلف متفاوت است؛ اگر چه در برخی مسائل اتفاق نظر بیشتری وجود دارد، مانند پورنوگرافی کودکان، قاچاق انسان، ترویج نژاد پرستی و تروریسم و هر گونه کلاهبرداری در اینترنت (مانند کلاهبرداری کارت اعتباری).^۳

موارد "مضر" همانطور که در برنامه تعریف شده، مواردی است که امکان دارد به ارزش ها و احساسات دیگران توهین کند و می تواند به سیاست، مذهب، یا مسائل نژادی مرتبط باشد و ممکن است به طور قابل توجهی میان فرهنگ های مختلف، متفاوت باشد. این طرح بر نیاز به اقدام در پنج حوزه گسترده به منظور جلوگیری از

^۱ برای مطالعه بیشتر نگاه کنید به منبع زیر: <http://europa.eu.int/ISPO/legal/en/internet/communic.html#f10> (accessed May 11, 2007).

^۲ این مسئله با طرح عملیاتی اینترنت امن تر (۲۰۰۵-۲۰۰۲) و برنامه الحاقی اینترنت امن تر دنبال شده است.

^۳ <http://europa.eu.int/ISPO/legal/en/internet/communic.html#f10> (accessed May 11, 2007).

^۴ حتی در موارد پورنوگرافی کودکان، تفاوت هایی مربوط به تعریف پورنوگرافی بین دو کشور طیف وسیعی از مسائل جزایی شامل قانون، روش های کنترل، و مجازات را به همراه دارد. برای یک نمای کلی از این قانون در سطح ملی، طرح مقابله با پورنوگرافی کودکان در کشورهای مختلف را ملاحظه نمایید: <http://www.inhope.org/en/about/about.html> (accessed May 11, 2007).

محتوای غیر قانونی و مضر در اینترنت تاکید دارد:^۱

۱. ترویج داوطلبانه خود کنترلی و رعایت مقررات و نظارت بر محتوای طرح، از جمله استفاده از عناوین ویژه برای گزارش محتوای غیر قانونی یا مضر برای عموم؛
 ۲. ارائه ابزار فیلترینگ و نظام رتبه بندی که پدر و مادر یا معلمان را قادر به تنظیم دسترسی به محتوای اینترنت توسط کودکان در زمانی که تحت مراقبت آنها هستند، می سازد؛ در حالی که به بزرگسالان اجازه می دهد که به محتوای قانونی دسترسی داشته باشند؛
 ۳. بالا بردن سطح آگاهی کاربران در مورد خدمات ارائه شده توسط صنایع که به آنها اجازه می دهد که نهایت استفاده را از اینترنت ببرند؛
 ۴. بررسی پیامدهای حقوقی ترویج استفاده مطمئن تر از اینترنت؛ و
 ۵. تشویق همکاری های بین المللی در حوزه قوانین و مقررات.
- اروپا نیز سیاست های منطقه ای را مقرر داشته که در محدود نمودن مسئولیت ارائه دهنده خدمات اینترنت، تحت رهنمود تجارت الکترونیک EC/۳۱/۲۰۰۰ به طور سخاوتمندانه ای عمل کند. ماده ۱۲، شرط استثنای "صرفاً پوشش محافظ سیم" شرکت های مربوطه را از مسئولیت برای انتقال اطلاعات بر روی شبکه خود تا زمانی که آنها ارسال این پیام را شروع نکرده اند، و یا اطلاعات را انتخاب و اصلاح ننموده، و یا دریافت کنندگان را انتخاب ننموده اند، مبرا می داند. معافیت همچنین برای ذخیره سازی "خودکار، نیمه کاره و موقتی" اطلاعات، به کار می رود و این معافیت را برای "مدت معقول" در نظر می گیرد. مشخص نمودن مورد دومی به اختیار کشورهای عضو قرار داده شده است.
- ماده ۱۳ با حفظ معافیت از مسئولیت، برای "ذخیره سازی خودکار، نیمه کاره و موقت اطلاعات" سر و کار دارد که به منظور هدف منحصر به فرد کارآمدتر ساختن انتقال اجرا می شود. ماده ۱۴، به مسئولیت در ارتباط با محتوای میزبانی وب می پردازد، ابراز می دارد که شرکت های مربوطه «در قبال میزبانی اطلاعات، به شرط آن که واقعاً از غیر قانونی بودن فعالیت ها آگاهی نداشته باشند و در صورت کسب آگاهی،

^۱ <http://europa.eu.int/ISPO/legal/fr/internet/actplan.html> (accessed May 11, 2007)

به سرعت برای حذف اقدام کنند»، مسئولیت قانونی ندارند.^۱ در نهایت ماده ۱۵ شرکت ها را به طور کلی از تعهد برای نظارت بر محتوا، انتقال داده و یا داده های ذخیره شده از طریق خدمات آنها، معاف می دارد. علاوه بر این، لازم نیست شرکت ها به طور فعال به دنبال حقایق و شواهد احتمالی مبنی بر غیر قانونی بودن فعالیت ها باشد.^۲ این مقررات، ایمنی قابل توجهی در برابر مسئولیت برای محتوای غیر قانونی، مطابق با قانون بسیاری از کشورهای دیگر در سراسر جهان که به دنبال گسترش استفاده از اینترنت و ترویج آزادی بیان هستند، به ارائه دهندگان خدمات اینترنت اعطا می کند.

فیلترینگ اجتماعی

اقدام برای مقررات گذاری مربوط به محتوای ناپسند و غیر اخلاقی در سطح کشورها به صورت مستقل و اجرای داوطلبانه فیلترینگ در سطح ارائه دهندگان خدمات اینترنت آغاز شد. اجرای فیلترینگ داوطلبانه اینترنت توسط ارائه دهندگان خدمات در مقیاس بزرگ در اروپا و ابتدا در انگلستان آغاز شد.^۳ بزرگترین ارائه دهنده ی خدمات اینترنت در بریتانیا که بی تی (BT) نام دارد، به حدود یک سوم از کاربران اینترنت خانگی در این کشور خدمات ارائه می دهد. در ماه ژوئن ۲۰۰۴، پروژه Cleanfeed را با مشورت وزارت کشور بریتانیا راه اندازی نمود. تحت نظارت این پروژه، بی تی محتوای اینترنت را طبق لیست سیاهی از وب سایت ها در سراسر نقاط جهان را که مطابق تعریف قانون اصلاحی حمایت از کودکان (مصوب ۱۹۷۸)^۵ حاوی تصاویر سوء استفاده از کودکان بود،

^۱. http://www.jisclegal.ac.uk/pdfs/isp_liability.pdf (accessed May 11, 2007).

^۲. با این حال، کشورهای عضو ممکن است تعهدات اضافی به ارائه دهندگان خدمات اینترنت تحمیل نماید تا به سرعت اطلاعات مربوط به "فعالیت های ادعایی غیر قانونی و یا اطلاعات ارائه شده توسط دریافت کنندگان خدمات آنها" در اختیار مقامات قرار دهند.

http://www.jisclegal.ac.uk/pdfs/isp_liability.pdf (accessed May 11, 2007).

^۳. پروژه Cleanfeed به عنوان "اولین تلاش برای سانسور گسترده اینترنت در دموکراسی غرب" ذکر شده است.

http://observer.guardian.co.uk/uk_news/story/0,6903,1232422,00.html.

^۴. برای اطلاعات بیشتر در مورد این پروژه نگاه کنید به منبع زیر:

<http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf> (accessed May 11, 2007).

^۵. اوایل سال ۲۰۰۶، روزانه ۳۵ هزار تصویر غیرقانونی روزانه مسدود شده و طی چهار ماه در میان مشترکان BT چهار میلیون درخواست دسترسی به این اطلاعات ثبت شده است.

فیلتر نمود. این فهرست توسط سازمان غیر انتفاعی بنیاد نظارت بر اینترنت (IWF) با مشاوره دولت، صنعت، پلیس و مردم تألیف و گردآوری شده است. بنیاد نظارت بر اینترنت این فهرست را برای اعضای خود، که امروز عبارتند از ارائه دهندگان خدمات اینترنت، اپراتورهای شبکه تلفن همراه، تامین کنندگان محتوا و موتورهای جستجو مانند گوگل و یاهو تامین می نماید.^۱ آنهایی که تلاش دارند به محتوای غیر قانونی میزبانی شده در خارج از کشور دسترسی پیدا کنند، یک پیغام خطا دریافت خواهند کرد که اعلام می دارد صفحه خاص به دلیل برخی مشکلات اتصال، قابل دسترسی نیست.^۲ محتوای غیر قانونی که در بریتانیا میزبانی می شود، شامل تصاویر سوء استفاده از کودکان و یا دارای محتوای جنایی، غیر اخلاقی و یا تحریک تنفر نژادی، لازم است که توسط ارائه دهندگان خدمات اینترنت و تامین کنندگان محتوا تحت یک روال اخطار و حذف قرار بگیرند.^۳ اگر چه این نوع از فیلترینگ "داوطلبانه" نامیده می شود، تا پایان سال ۲۰۰۷ انتظار می رود تمام مصرف کننده های پهنای باند ارائه دهندگان خدمات اینترنت در بریتانیا سیستم مشابهی را پیاده سازی نمایند؛^۴ در صورت عدم اجرای این سیستم، ممکن است نظارتی در نظر گرفته شود. کشورهای دیگر، مانند نروژ، سوئد، دانمارک، و ایتالیا، برنامه های مشابهی را اجرا نموده اند، در حالی که فنلاند در حال حاضر اجرای آن را در نظر دارد.^۵

فیلترینگ همچنین از طریق "خود کنترلی داوطلبانه" توسط موتورهای جستجو

^۱. http://www.theregister.co.uk/2006/12/29/iwf_feature/ (accessed May 11, 2007).

^۲. <http://technology.guardian.co.uk/news/story/0,,1704342,00.html> (accessed May 11, 2007).

^۳. <http://www.iwf.org.uk/media/page.70.215.htm> (accessed May 11, 2007).

^۴. <http://publicaffairs.linx.net/news/?p=518> (accessed May 11, 2007).

^۵. http://news.bbc.co.uk/2/hi/uk_news/2445065.stm (accessed May 11, 2007).

^۶. http://press.telenor.com/PR/200505/994781_5.html; http://www.financialmirror.com/more_news.php?id=2574; http://en.wikipedia.org/wiki/Internet_censorship (accessed March 7, 2007); http://www.edri.org/edriagram/number5.1/italy_blocking (accessed May 11, 2007).

انجام می شود. از اوایل سال ۲۰۰۵ تمام موتورهای جستجوی عمده در آلمان^۱ سازمانی را تشکیل داده اند که نتایج جستجو مضر برای افراد زیر سن قانونی را بر اساس لیست ارائه شده توسط یک سازمان دولتی که مسئول طبقه بندی رسانه است، پالایش می کند. این حرکت در پاسخ به فشار اعمال شده برای خود کنترلی داوطلبانه مقرر شده توسط صنایع در سطح اتحادیه اروپا، و مسلماً به دلیل ترس موجود میان صنایع در خصوص افزایش عواقب قانونی در صورت عدم رعایت خود کنترلی داوطلبانه، انجام شده است. با این حال، اقدام مذکور بدلیل عدم شفافیت مورد انتقاد قرار گرفته^۲، زیرا موتورهای جستجو نمی توانند فهرست وب سایت های فیلتر شده را به عموم اعلام نمایند؛ زیرا مطابق تعهدات، آنها مجاز به افشای لیست نیستند.^۳ علاوه بر این، افشا نمودن این لیست هدف از فیلترینگ نتایج جستجو را با شکست مواجه می کند، زیرا سایت ها تنها از نتایج جستجو حذف شده اند و نه از اینترنت.

محتوای اینترنت همچنین از طریق نظارت آنلاین توسط مقامات در انگلیس کنترل می شوند. مرکز حفاظت آنلاین سوء استفاده از کودکان (تاسیس در ۲۰۰۶) پس از آغاز تحقیقات در مورد خدمات پرداخت به ازای بازدید در سال ۲۰۰۶، به سیزده دستگیری اقدام نمود.^۴ همچنین در این کشور پلیس بر اساس اصلاحیه ای الحاقی به قانون حمایت از داده ها (۱۹۹۸)، دارای قدرت دسترسی به بانک اطلاعات شخصی کسانی است که با استفاده از کارت های اعتباری به محتوای غیر قانونی آنلاین دسترسی داشته اند. و در این صورت بانک پس از آن، خدمات به دارندگان این کارت ها را بدلیل نقض قوانین و مقررات خود لغو خواهد نمود.^۵

مردم در نوزده کشور اروپایی در شناسایی و گزارش محتوا به ویژه محتوای غیر

^۱. گوگل، لایکس (Lycos) اروپا، ام اس ان (MSN) آلمان، آ ال (AOL) آلمان، یاهو، تی-آلین و تی-اینفو (t-info)

^۲. <http://blogs.law.harvard.edu/ugasser/2005/03/10#a52> (accessed May 11, 2007).

^۳. <http://www.heise.de/english/newsticker/news/56817> (accessed May 11, 2007).

^۴. <http://news.bbc.co.uk/1/hi/uk/5213058.stm> (accessed May 11, 2007).

^۵.

http://www.theregister.co.uk/2006/06/27/child_convictions_passed_to_banks/ (accessed May 11, 2007).

قانونی در زمینه پورنوگرافی کودکان - از طریق شبکه ای از خطوط تماس ویژه که بر اساس توصیه اتحادیه اروپا در سطح این اتحادیه برقرار شده - همکاری می کنند.^۱ فوریه ۲۰۰۷ در اتریش بر اساس گزارش های یکی از کارمندان شرکت خدمات میزبانی در وین، مقامات یک "شبکه پورنوگرافی کودکان" شامل هفتاد و هفت کشور را کشف نمود.^۲ گزارش های اخیر نشان می دهد که خطوط تماس ویژه نجات کودکان در دانمارک، با تامین مالی به طور مشترک توسط دانمارک و برنامه های اینترنت امن تر کمیسیون اروپا، نزدیک به ۹۰۰۰ گزارش از تصاویر سوء استفاده از کودکان تنها در سال ۲۰۰۶ دریافت نموده اند.^۳ در سال ۲۰۰۴ پلیس در اسپانیا نود نفر را در بزرگترین عملیات این کشور در برابر توزیع پورنوگرافی کودکان که مجهز به خطوط تماس ویژه بود، دستگیر نمود. انجمن INHOPE به عنوان هماهنگ کننده شبکه ای از خطوط تماس ویژه، در کشورهای خارج از اروپا از جمله استرالیا، برزیل، کانادا، کره جنوبی، تایوان، و ایالات متحده عمل می کند.^۴

اگر چه تلاش های اولیه در فیلترینگ محتوای اینترنت برنامه های نسبتاً محدودی داشت، اکنون پیشنهادات و قوانین در خصوص فیلترینگ در سایر حوزه های اجتماعی نظیر قمار و شرط بندی در بسیاری از کشورها در حال ظهور است. در سال ۲۰۰۲ یک پیشنهاد تجدید نظر در قوانین فدرال سوئیس در زمینه قرعه کشی و شرط بندی تهیه شد، به این ترتیب برای افرادی که دسترسی به بازی های غیر قانونی را فراهم می آورند جریمه ای تا ۱ میلیون فرانک سوئیس و یا تا یک سال حبس در نظر گرفته شده است. این تلاش در سال ۲۰۰۴ به حالت تعلیق درآمد، و هیچ اقدام دیگری

^۱. برای مشاهده فهرست کشورها و سازمان های دخیل در طرح تماس به منبع زیر مراجعه نمایید:

http://ec.europa.eu/information_society/activities/sip/projects/hotlines/index_en.htm.

^۲.

<http://www.cnn.com/2007/WORLD/europe/02/07/kids.online.porn.ap/index.html>.

^۳.

http://www.redbarnet.dk/Files/Filer/Seksuelt_misbrug/Pressemedfebruar07_eng.doc(accessed May 11, 2007).

^۴.http://ec.europa.eu/information_society/activities/sip/projects/hotlines/index_en.htm(accessed May 11, 2007).

از آن سال صورت نگرفت. از فوریه ۲۰۰۶، ارائه دهندگان خدمات اینترنت در ایتالیا موظف اند که دسترسی به وب سایت هایی که قمار آنلاین ارائه می کنند را مسدود سازند. فهرست وب سایت هایی که باید مسدود شوند توسط دولت گردآوری و اعلام می شود.^۱ گسترده ترین پیشنهاد برای فیلتر کردن از طرف نروژ بوده است؛ دولت مسدود کردن دسترسی به سایت های قمار خارجی، وب سایت هایی که به "پرچم و نشان ملی یک کشور خارجی بی حرمتی می نمایند"، سایت های که نفرت نسبت به مقامات دولتی را ترویج می کنند (شامل سخنرانی های تنفرآمیز، ترویج نژاد پرستی، پورنوگرافی توهین آمیز، و سایت های همکار که دریافت غیر قانونی موسیقی، فیلم، و یا نمایش های تلویزیون را ارائه می دهند) در نظر می گیرد.^۲

فیلترینگ ملی گرایانه افراطی

در اروپا هیچ نمونه ای از فیلترینگ برای ساکت کردن مخالفان سیاسی وجود ندارد. با این حال، نمونه هایی از فیلترینگ که به دنبال حفظ مشروعیت نهادهای دولتی و حفظ هویت ملی هستند، وجود دارد. در دسامبر ۲۰۰۲ یک دادرس محلی سوئیس، فرانسوا دسواکس، به چندین ارائه دهنده ی خدمات اینترنتی سوئیسی دستور داد سه وب سایت میزبانی شده در ایالات متحده آمریکا که به شدت از دادگاه های سوئیس انتقاد می کنند^۳ مسدود شده و سرور نام دامنه (DNS) خود را برای جلوگیری از دسترسی به دامنه مورد نظر تغییر دهند.^۴ گروه کاربری اینترنت سوئیس و گروه اپراتورهای شبکه این کشور اعتراض کردند که مسدودسازی به راحتی می تواند دور زده شود و این حرکت خلاف قانون اساسی سوئیس است، که "حق دریافت آزادانه اطلاعات، جمع آوری آن از منابع در دسترس عموم و انتشار آن" را به هر فرد تضمین می کند. با این حال،

^۱. <http://www.edri.org/edriagram/number4.12/italybetting> (accessed May 11, 2007).

^۲. <http://www.dagbladet.no/dinside/2007/02/12/491719.html>, cited in: <http://www.opennetinitiative.net/blog/?p=144> (accessed May 11, 2007).

^۳. The contested Web sites were www.appel-aupeuple.org, <http://de.geocities.com/justicecontrol>, and www.swiss-corruption.com.

^۴. <http://www.fitug.de/news/newsticker/newsticker120203210053.html>.

دستور فوق بسیار مقتدرانه اجرا شد و از مدیران ناراضی ارائه دهندگان خدمات اینترنت خواسته شد که شخصاً در دادگاه حاضر شوند، و عدم حضور آنها با اتهام نافرمانی مواجه می شود.

در روز ۷ مارس ۲۰۰۷، وب سایت اشتراک گذاری ویدئو یوتیوب، به دنبال ارسال فیلم های مشخصی در سایت که در مورد بنیانگذار ترکیه، مصطفی کمال آتاتورک بود و به طور کلی برای مردم ترکیه و پرچم ترکیه اهانت آمیز تلقی می شد، با حکم دادگاهی در ترکیه مسدود شد. مسدود نمودن این سایت به استناد ماده ۳۰۱ قانون مجازات ترکیه صورت گرفت، این قانون به عنوان مانع اصلی آزادی بیان شناخته می شود، که توهین نسبت به آتاتورک و همچنین "ترک بودن" را به عنوان یک جرم می شناسد. ارائه دهنده سرویس اینترنت پیشرو در ترکیه، ترک تلکام، مطابق قانون عمل نمود؛ اما درخواستی را برای بازگرداندن اجازه دسترسی به سایت به دادگاه ارائه نمود. دادگاه به شرط حذف شدن این ویدئوی خاص از روی سایت، با درخواست این ارائه دهنده خدمات اینترنت موافقت نمود. مسدود کردن دو روزه سایت یوتیوب، به شدت هم در داخل ترکیه و هم در خارج از کشور مورد انتقاد قرار گرفت و به "بسته شدن یک کتابخانه به دلیل وجود یک کتاب نامناسب" تشبیه شد.^۱

سخنرانی تنفرآمیز

کشورهای اروپایی نیز به طور فزاینده علیه سخنرانی تنفرآمیز آنلاین اقدام می کنند، و سیاست های آفلاین خود را در مورد اینترنت اجرا می کنند. برخی از تلاش ها، مسائل مهمی مانند صلاحیت این دادگاه ها در مورد مسائل موجود بر روی اینترنت را مطرح نمودند. به عنوان مثال، دادگاهی در فرانسه در سال ۲۰۰۰ حکم داد که شرکت یاهو که دفتر مرکزی آن در ایالات متحده است، تحت قانون فرانسه مسئول دسترسی مردم فرانسه به سایت های حراج که شامل یادگاری های نازی ها است، می باشد و خواستار شد که یاهو باید اطمینان حاصل کند که دسترسی به این مطلب از فرانسه غیر ممکن

^۱. <http://www.edri.org/edriagram/number5.5/youtube-turkey> (accessed May 11, 2007).

است یا با جریمه مواجه می شود.^۱ این مورد توسط دو نفر که در سازمانی غیر انتفاعی در فرانسه که با یهودی ستیزی مبارزه می کند^۲، مطرح شد.^۳ یاهو لایحه ای به دادگاه منطقه ای ایالات متحده در سان فرانسیسکو ارائه کرد، با این ادعا که حکم دادگاه فرانسه در ایالات متحده غیرقابل اجرا است. دادگاه آمریکا در نوامبر ۲۰۰۱ به نفع یاهو حکم داد، اما در سال ۲۰۰۴ یک شعبه از دادگاه نهم استیناف ایالات متحده حکم دادگاه بدوی مبنی بر عدم صلاحیت دادگاه فرانسه را رد نمود.^۴ پس از بررسی مجدد این تصمیم، دادگاه نهم استیناف ایالات متحده، قضیه یاهو را در ژانویه ۲۰۰۶ با وجود ادعای عدم صلاحیت دادگاه فرانسه، رد کرد زیرا یاهو این مطالب را از قبل حذف نموده بود و در نتیجه، الزام به مسدودسازی نمی توانست آسیبی به متمم اول قانون اساسی برساند.^۵

به طور مشابه، دادگاه فدرال دادگستری آلمان در دسامبر سال ۲۰۰۰ حکم داد که موارد تجلیل از نازی ها و انکار هولوکاست باید تحت قانون آلمان سانسور شود، بدون در نظر گرفتن این که میزبان سایت در کدام کشور است. این حکم بر اساس پرونده فردی بود که از اینترنت برای گسترش پیام خود برای انکار جنایات جنگ جهانی دوم استفاده می کرد، صادر شد.^۶ در یک مورد دیگر در سال ۲۰۰۲، به هفتاد و هشت ارائه دهنده خدمات اینترنت در Nordrhein-Westfalen دستور داده که از دسترسی به دو وب سایت خارجی که شامل محتوای مربوط به نفو نازی ها بود جلوگیری کنند.^۷ دولت منطقه ای همان منطقه در دوسلدورف نیز فعال ضد سانسور را برای ارسال لینک های

^۱. <http://www.cdt.org/publications/policyposts/2005/5>(accessed May 11, 2007).

^۲. La Ligue Contre Le Racisme Et L Antisemitisme(LICRA) and L Union Des Etudiants Juifs De France

^۳. <http://www.tomwbell.com/NetLaw/Ch03/YahoovLICRA.html> (accessed May 11, 2007).

^۴. <http://www.cdt.org/publications/policyposts/2005/5>(accessed May 11, 2007).

^۵. <http://news.bbc.co.uk/2/hi/technology/4641244.stm> (accessed May 11, 2007).

^۶. http://www.cdt.org/publications/pp_7.06.shtml.

^۷.<http://md.hudora.de/publications/200306-gi-blocking/200306-gi-blocking.pdf>.

سانسور شده با محتوا جناح راست افراطی در وب سایت خود به دادگاه فراخواند.^۱ دیگر کشورهای اروپایی نیز قوانینی برای مقابله با انکار هولوکاست و ممنوعیت محتوای ترویج نفرت نژادی، وضع نموده اند. این قوانین در پروتکل ارائه شده به شورای معاهده جرایم کامپیوتری در اروپا با یکدیگر " هماهنگ " شده اند؛ قوانین مذکور مستلزم آن است که " هر نوشته، هر تصویر، و یا هر ارائه ای از ایده ها و تئوری ها که نفرت، تبعیض و خشونت، در برابر هر فرد یا گروهی از افراد را، بر اساس نژاد، رنگ، نسب یا منشاء ملی یا قومی، و همچنین دینی را طرفداری، ترویج و یا تحریک می کند، اگر به عنوان بهانه ای برای انکار، کم شمردن، تأیید، توجیه و یا جنایات نسل کشی و جنایت علیه بشریت " استفاده شوند، باید توسط امضا کنندگان غیر قانونی اعلام شوند.^۲ همانطور که در مورد تمام محتوای غیر قانونی صدق می کند، یک نوبت که ارائه دهندگان خدمات اینترنت متوجه آن شدند، بسته به اینکه سایت ها در داخل کشور و یا خارج از کشور میزبانی می شوند، باید سایت را حذف یا فیلتر نمایند.

افترا

کشورهای عضو اتحادیه اروپا نیاز به چارچوبی ساده شده را مطرح نمودند، تا با توجه به قوانین مربوط به افترا و تهمت توسط رسانه ها و انتشار آن از طریق اینترنت و دیگر شبکه های الکترونیکی استفاده شود. اصل کلی درباره افترا در رسانه ها که قانون کشوری محل اقامت افترا زنده قابل اعمال است - نشان می دهد سازمان های رسانه ای باید قوانین حفظ حریم خصوصی و افترا در هر کشور اروپایی را بدانند؛ این امر که به عنوان قاعده غیر عملی، مورد انتقاد قرار گرفته است. به عنوان مثال سال ۲۰۰۰ در ایتالیا، مردی در یک دعوی فرامرزی حضانت ادعا کرد همسر سابق او، که در حال حاضر ساکن سرزمین های اشغالی فلسطین است، در قبال بیابیه های ارسال شده و تصاویر قرار گرفته بر روی اینترنت که نسبت به او و توانایی او در مراقبت از دو دختر او توهین آمیز بوده، مسئول می باشد. دیوان عالی کشور ایتالیا، حکم قبلی دادگاه بدوی را

^۱ <http://www.edri.org/edriagram/number2.22/filtering> (accessed May 11, 2007).

^۲ I. Brown, "Internet censorship: Be careful what you ask for." Proc. International Conference on Communication, Mass Media and Culture, Istanbul, October 2006.

لغو نمود، چرا که قوانین ایتالیا در مورد افترا در وب سایت های خارجی که توسط کاربران اینترنت در کشور قابل دسترسی است اعمال می شود.^۱ دادگاه برگزار شد در حالی که اقدامات غیر قانونی در خارج از ایتالیا انجام شده بود، و اثرات آن در داخل کشور احساس می شد و بنابراین موضوع به قوانین ملی مربوط بود.

موضوع نیاز به چارچوب واحد و یکپارچه مجدداً در فوریه ۲۰۰۷ به عنوان بخشی از قرائت دوم پارلمان اروپا از مقررات رم ۲ که در پی ایجاد مقررات در قانون لازم الاجرا پیرامون تعهدات غیر قراردادی مربوط به انتشار محتوا از طریق اینترنت و دیگر شبکه های الکترونیکی می باشد، مطرح شد اصلاحیه پیشنهادی پارلمان این بود که قانون حاکم باید از کشوری باشد که "انتشار و یا پخش محتوا بیشتر با آن ارتباط مستقیم دارد" یا براساس زبان انتشار و یا رسانه پخش کننده محتوا و یا از طریق میزان فروش و یا اندازه مخاطب در یک کشور خاص به عنوان یک نسبت از کل فروش و یا میزان مخاطب و یا ترکیبی از این عوامل "تعیین شود. علاوه بر این قانون اصلاحی پیشنهاد می دهد اگر این موارد به آسانی قابل تعیین نیستند، "قانون حاکم، قانون کشوری خواهد بود که در آن کنترل مقاله اعمال می شود". با توجه به حق پاسخ، پیشنهاد می شود که قانون باید از کشوری باشد که ناشر یا گوینده در آن "اقامت همیشگی" دارد. انتظار نمی رود که متنی که توسط پارلمان به تصویب رسید، به آسانی نفعی از شورای اروپا حاصل کند و باید تحت یک روش استاندارد آشتی جویانه قرار گیرد که در آن کشورهای عضو و اعضای پارلمان اروپا، با داشتن نمایندگی برابر در مورد طرح های پیشنهادی بحث کنند، و اگر به مصالحه قابل قبولی دست یابند، این پیشنهاد به عنوان قانون پذیرفته می شود.^۲

قوانین افترا در شکل کنونی خود و در سطح کشورها به ویژه در انگلیس، به دلیل اینکه منجر به فرهنگ "حذف وب سایت ها" شده، مورد انتقاد قرار گرفته است؛ زیرا ارائه دهندگان خدمات از ترس برخوردهای قانونی، بلافاصله مطالبی را که گمان می رود توهین آمیز باشد حذف می کنند. نگرانی در انگلیس و همچنین سایر کشورها این است که این روند می تواند یک "اثر وحشت زا" (اثری که انجام و اجرای اعمال قانونی را از

^۱. <http://www.cptech.org/ecom/jurisdiction/defamation2.html> (accessed May 11, 2007).

^۲. <http://www.edri.org/edriagram/number5.3/romeII>(accessed May 11, 2007).

ترس مواجه با قانون، کند یا متوقف می کند) بر محتوای آنلاین قانونی و رفتارها داشته باشد^۱.

یک نقطه تحول تاریخی در انگلستان منجر به راهی برای استقرار سیستم اخطار و حذف شد. در قضیه *Laurence Godfrey v. Demon Internet Limited*، بیانیه ای توهین آمیزی به یک گروه خبری ارسال شد، که بر روی سرور *Demon Internet Limited* قابل دسترسی بود. مشخص شد که پیام، جعلی است و به نظر می رسد که پیام تنها از گادفری آمده است. با وجود درخواست های گادفری برای حذف این محتوا، که نسبت به او توهین آمیز بود، ارائه دهنده خدمات اینترنت این درخواست را منطبق ندانست. در نتیجه او به دلیل افترا، تحت قانون افترا سال ۱۹۹۶، ادعای خسارت نمود و با *Demon Internet* خارج از دادگاه مساله را حل و فصل نمود.^۲

قوانین افترا در انگلستان به طور خاص دلسوز شاکیان افترا شناخته می شود، و اغلب در این زمینه با قانون مربوطه در ایالات متحده در تقابل است، به طوری که بسیاری از افراد از کشورهای دیگر برای داشتن شانس بیشتری برای پیروزی و علی رغم انتشار اندک نشریات مورد نظر در انگلستان، در این کشور از نشریات شکایت می کنند. با این حال، مورد مطلوب در برابر وال استریت ژورنال اروپا به طور قابل توجهی حمایت از مطبوعات را در برابر ادعاهای افترا در اکتبر ۲۰۰۶ افزایش داد.^۳ همچنین بحث هایی بر سر اینکه آیا حفاظت از شهرت افراد در تقابل با قانون حقوق بشر سال ۱۹۹۸ است یا خیر وجود داشته است، تا آنجا که ممکن است حفاظت از شهرت افراد حق آزادی بیان را محدود سازد.^۴

^۱. Sarah Lyall, "High court in Britain loosens strict libellaw," The New York Times, October 12, 2006, <http://www.nytimes.com/2006/10/12/world/europe/12britain.html>.

^۲. Yaman Akdeniz, "Case Analysis of *Laurence Godfrey v. Demon Internet Limited*," 1999,

<http://www.cyber-rights.org/reports/demon.htm>;

Consumer Project on Technology, CPT's Page on Defamation and Libel Cases, <http://www.cptech.org/ecom/jurisdiction/defamation2.html>.

^۳. <http://www.nytimes.com/2006/10/12/world/europe/12britain.html>.

^۴. [http://www.lawcom.gov.uk/docs/defamation\(1\).pdf](http://www.lawcom.gov.uk/docs/defamation(1).pdf) (accessed May 11, 2007).

حق کپی رایت

چند کشور در اروپا برای مبارزه با نقض قوانین کپی رایت اقدام به فیلترینگ اینترنت نمودند، که در حال تحول به سوی رویکرد اطلاع و حذف مورد استفاده در ایالات متحده است. در دانمارک، حکم دادگاه کپنهاگ در اکتبر سال ۲۰۰۶، تی دی سی (TDC)، بزرگترین ارائه دهنده خدمات اینترنت کشور، دسترسی به یک وب سایت که موسیقی را به طور غیر قانونی کپی کرده و توزیع می کرد، مسدود نمود.^۱ همانطور که قبلاً ذکر شد در فوریه ۲۰۰۷، نروژ فیلتر در مقیاس بسیار بزرگتر را پیشنهاد کرد، که شامل مسدود کردن از سایت های ارائه دهنده دریافت غیر قانونی موسیقی، فیلم، و برنامه های تلویزیونی بود.^۲

در تاریخ ۱۶ مارس ۲۰۰۷، پلیس مالک سایت www.arenabg.com، که یکی از بزرگترین انتقال دهندگان بیت تورنت^۳ بلغارستان، یکی از ده وب سایت محبوب کشور و فراهم کننده لینک هایی به موسیقی ها، فیلم ها و نرم افزارهای دارای حق کپی رایت می باشد را دستگیر کردند. اگر چه مالک در بیست و چهار ساعت از زندان آزاد شد، وب سایت به دستور پلیس از ۱۶ تا ۱۹ مارس فیلتر شد، به این دلیل که "برای جلوگیری از دخالت خارجی در پیگیری تورنت" لازم بود. دستور فیلتر سایت توسط اداره کل مقابله با جرائم سازمان یافته برداشته شد، اما به دلیل آنچه که رفتار ناعادلانه نسبت به صاحبان و گردانندگان تورنت عنوان می شد، منجر به بروز اعتراضات قابل

^۱ <http://www.flickr.com/photos/jesper/336756697/> (accessed May 11, 2007).

^۲ Article at <http://www.dagbladet.no/dinside/2007/02/12/491719.html> (in Norwegian), cited February 13, 2007, in <http://www.opennetinitiative.net/blog/?p=144>.

^۳ بیت تورنت پروتکلی است که به منظور ارسال پرونده ها و توزیع حجم بزرگی از اطلاعات بدون کاهش در مصرف منابع پر هزینه سرور و پهنای باند طراحی شده است. در واقع نوعی ارتباط همتا به همتا می باشد که کاربران مستقیماً به یکدیگر متصل می شوند و به ارسال و دریافت قسمتی از فایل می پردازند. گر چه فعالیت های تمامی کاربران یک فایل توسط سرور مرکزی به نام Tracker هماهنگ می شود، اما این سرور از محتویات فایل هایی که منتقل می شود بی اطلاع است. در نتیجه تعداد زیادی از کاربران با پهنای باند محدود Tracker مربوطه قابل پشتیبانی هستند. فلسفه کلیدی بیت تورنت این است که کاربران باید هم زمان با دا نلود کردن اطلاعات، آپلود نمایند. در این صورت پهنای باند شبکه با حداکثر کارایی بکار گرفته می شود.

توجهی در میان شهروندان گردید. پس از دستگیری مدیران، دیگر وب سایت های دیگر بسته شدند، برخی در معرض خطر مصادره اموال توسط پلیس قرار گرفتند و یا برای جلوگیری از پیگرد قانونی تحت قانون کپی رایت بلغارستان، سرور خود را به خارج از کشور منتقل نمودند. میزان فیلترینگ واقعی این سایت ها شناخته شده نیست چرا که گزارش های متفاوتی در مورد دسترسی های مختلف ارائه دهندگان سرویس های اینترنت مشترک وجود دارد. با توجه به اینکه بیت تورنت به محتوا دسترسی می دهد اما آن را میزبانی نمی کند، بنابراین منابع قانونی برای مقابله با موارد نقض کپی رایت در این سایت ها به طور خاص روشن نیست.

لویح قانونی در مورد نقض نسخه برداری ادعا شده توسط موتورهای جستجو در چند کشور، با احکام اخیر به نفع سیاست اطلاع و حذف، این موارد قانونی مسلماً می تواند به عنوان پیشینه ای در خدمت کشورهای دیگر در منطقه باشند. در فوریه ۲۰۰۷ دادگاه بروکسل در پرونده مطرح شده توسط Copiepresse بلژیک، یک گروه تجاری به نمایندگی از هفته روزنامه فرانسوی و آلمانی زبان بلژیک، شرکت گوگل را ناقض قوانین کپی رایت ملی دانست و شرکت ۲,۴ میلیون پوند برای نقض قانون کپی رایت جریمه شد. برای هر ترجمه متداول "تولید مجدد و انتشار عناوین خبری و همچنین خلاصه های کوتاه، استفاده از کَش گوگل، داده های ذخیره شده مقالات و اسناد که در دسترس عموم هستند، قانون حقوق نویسندگان را نقض می نماید". مورد قبلی اشاره به خدمات اخبار گوگل دارد، در حالی که دومی به جستجو در وب سایت گوگل اشاره دارد. نتیجه این است که گوگل نمی تواند شامل منبع مقالات، تصاویر، و یا نقاشی های کاربران Copiepress از طریق خدمات اخبار خود بدون موافقت نامه های قبلی باشد و باید مطالب روزنامه بلژیکی را از نتایج جستجوی خود حذف کند. عدم رعایت این حکم با جریمه ۲۵,۰۰۰ یورو در روز مواجه می شود.

گوگل در نظر دارد تا در مورد قضاوت صورت گرفته، درخواست تجدید نظر نماید، با اظهار این که نتایج جستجو در وب و سرویس های خبری در واقع ترافیک بیشتری را به سمت وب سایت روزنامه ها هدایت می کند، و اخبار گوگل هیچ درآمد حاصل از تبلیغاتی از این اقدام کسب نمی کند. با این حال Copiepress بر آن است که با اجازه دادن به کاربران برای دور زدن صفحات اول روزنامه ها و پیوند مستقیم به مقالات، روزنامه ها درآمد حاصل از تبلیغات را از دست می دهد. علاوه بر این، با در

دسترس قرار دادن محتوای روزنامه های قدیمی از طریق ذخیره سازی آن ها، روزنامه ها به طور موثر توانایی متهم ساختن مشتریان برای دسترسی به آرشیو خود را از دست می دهند، در حالی که گوگل در واقع از این سرویس خود درآمد تبلیغاتی کسب می کند. همچنین در حکم دادگاه آمده است که تمام دارندگان کپی رایت می تواند گوگل را در مورد نقض قوانین حق کپی رایت مطلع سازند، و این حکم موتور جستجو را مجبور به حذف مطالب در یک دوره بیست و چهار ساعته و یا پرداخت روزانه ۱۰۰۰ یورو می نماید. این کار می تواند منجر به نگرش ریسک گریزی و رعایت فوری این قانون در بخشی از ارائه دهندگان خدمات اینترنت ، تامین کنندگان محتوا و موتورهای جستجو شود.

گوگل در فرانسه نیز با توجه به سرویس خبری خود، زمانی که خبرگزاری فرانسه (AFP)، مستقر در پاریس برای ۱۷,۵ میلیون دلار در سال ۲۰۰۵ از گوگل شکایت کرده بود به مشکل مشابهی برخورد. این شکایت در آوریل ۲۰۰۷ پس از یک موافقت نامه صدور مجوز حل و فصل شد، که در آن موافقت نامه به گوگل اجازه داده می شود تا از داستان ها و عکس های خبرگزاری فرانسه برای جمع آوری اخبار و برای دیگر سرویس های گوگل از جمله محصولاتتی که انتظار می رود گوگل در آینده راه اندازی نماید، استفاده کند. شرایط مالی این طرح به طور واضح اعلام نشده است. توافق های خارج از دادگاه در اروپا برای نقض قوانین حق نشر نباید تعجب برانگیز باشد، چرا که حمایت قانونی موجود در منطقه برای اتهام نقض قانون حق نشر نسبتاً ضعیف هستند.

در سطح منطقه ای، حقوق مالکیت فکری مربوط به محتوای اینترنت توسط دو دستورالعمل مشخص می شوند: کپی رایت و حقوق مرتبط در جامعه اطلاعاتی به مصوب ۹ آوریل سال ۲۰۰۱، و دستور تجارت الکترونیک EC/۳۱/۲۰۰۰، که در تاریخ ۸ ژوئن ۲۰۰۰ لازم الاجرا شده است. ماده ۵ (۱) کپی رایت دستورالعمل معافیت ارائه دهندگان خدمات اینترنت از مسئولیت برای نقض قوانین حق تکثیر است که در آن "بازتولید محتوا گذرا و یا اتفاقی است" و یا در جایی که در آن کپی بخشی جدایی ناپذیر از فرآیند تکنولوژیک است " که تنها هدف آن قادر ساختن انتقال به بعدی در یک شبکه بین اشخاص ثالث توسط یک واسطه، یا یک استفاده قانونی از کار و یا دیگر موارد" است، می باشد.

دستورالعمل کپی رایت همچنین ارائه دهندگان خدمات اینترنت را از مسئولیت در

زمانی که نسخه‌ها دارای "هیچ اهمیت اقتصادی مستقل" نیستند، معاف می‌دارد؛ این مسئله باید به طور مستقل توسط دادگاه‌های کشورهای عضو مربوطه مورد قضاوت قرار گیرد. به عنوان اولین شرط، ارائه دهندگان خدمات اینترنت و اپراتورهای ارتباطات راه دور نیازی به درخواست مجوز برای انتقال نسخه‌ها در سراسر شبکه خود ندارند. با این حال، شرط دوم نشان می‌دهد که ارائه دهندگان خدمات اینترنت هنوز با وضعیت تفاوت در درجات مسئولیت در سراسر کشورهای عضو اتحادیه اروپا مواجه هستند، و بخشنامه نیز در این زمینه مورد انتقاد قرار گرفته است.

دستورالعمل تجارت الکترونیک با مسئولیت ارائه دهندگان خدمات اینترنت نسبت به محتوا به طور کلی تر، اما با مفاهیم ضمنی مهمی برای حق نشر سرو کار دارد. به طور خاص، این دستورالعمل استثنای اجرای محض، تعهد محدود برای محتوای مرتبط با ذخیره سازی و توابع میزبانی وب فراهم می‌کند، و ارائه دهندگان خدمات اینترنت را از هر گونه تعهد کلی، برای نظارت معاف می‌دارد.

امنیت

نگرانی‌های امنیتی در اروپا منجر به دغدغه‌هایی در مورد قوانین نظارت و کنترل استفاده از اینترنت شده است. اگر چه جدای از فیلترینگ، این تشابه زیادی در اثر بالقوه آنها بر آزادی بیان در اینترنت دارد. حوزه‌های بحث برانگیز قانونی در سطح اتحادیه اروپا در این خصوص، مربوط به نظارت بر ترافیک داده‌ها و حفظ آن است. همانطور که در دستورالعمل اروپایی حفظ داده‌ها، که در ماه مارس ۲۰۰۶ صادر شد، مطرح گردید و باید برای ترافیک اینترنت در ماه مارس ۲۰۰۹ اجرا شود ارائه دهندگان خدمات اینترنت در کشور‌های مختلف ملزم به حفظ اطلاعات خاص مربوط به ارتباطات - بویژه در مورد دسترسی اینترنتی، ایمیل و تلفن - برای یک دوره حداقل شش ماه و نه بیش از دو سال هستند. داده‌هایی که باید حفظ شوند باعث نگرانی در مورد محتوای ارتباطات مربوطه نمی‌شوند.^۱ هدف این است که یک "کد مشترک" حفظ داده‌ها به منظور تسهیل ردیابی محتوای غیر قانونی و منبع حملات علیه سیستم‌های اطلاعاتی و برای

^۱. <http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-63514> (accessed May 11, 2007).

شناسایی افرادی که از شبکه های ارتباطی الکترونیکی برای فعالیت های تروریستی و جرایم سازمان یافته استفاده می کنند، فراهم شود.

با اجرای دستورالعمل در سراسر کشورهای عضو، گروه های حریم خصوصی در مورد توانایی ارائه دهندگان خدمات اینترنت، موتورهای جستجو و شرکتهای وب برای حفظ داده ها و نظارت و کنترل عادات آنلاین مردم هستند. علاوه بر این، دوره نگهداری دوساله به عنوان یک مدت غیرقابل توجهیه زمانی، مورد بحث قرار گرفته است.^۱

نمونه ای از قوانین امنیتی در سطح کشور، قانون پیشنهادی است که پیش نویس آن در مارس ۲۰۰۷ در سوئد مطرح شده است. این قانون به آژانس اطلاعات دفاعی ملی قدرت و اختیار نظارت بر تمام تماس های تلفنی درون و برون مرزی و ترافیک پست الکترونیکی بدون حکم دادگاه را اعطا می کند. این توسط تاسیسات رادیویی دفاع ملی در قالب جستجوهای برای کلمات کلیدی حساس از طریق استفاده از نرم افزارهای کامپیوتری انجام می شود. با برخی از اصلاحات پیشنهاد شده، شورای قانونگذاری سوئدی پیشروی این پیشنهاد به مراحل بعد را تایید کرده است.^۲ نگرانی ها برای حفظ حریم خصوصی، از جمله برای ارتباطات در کشور که اغلب از طریق سرورهای میزبان در خارج از کشور مسیریابی می شوند، بالا گرفت. منتقدان شامل آژانس ملی پلیس امنیت کشور (SAPO)، بودند که این پیشنهاد را ناقض "تمامیت حریم شخصی" دانستند.

نتیجه

فیلترینگ محتوای آنلاین به شکل های مختلفی در میان کشورهای اروپایی انجام می شود. برخی موارد عبارتند از: دستور صادر شده توسط دولت ها به ارائه دهندگان خدمات اینترنت برای حذف وب سایت هایی که شامل مطالب غیر قانونی هستند (زمانی که در داخل کشور میزبانی شده باشند)، دستورات مسدودسازی توسط مقامات اجرایی برای محتوای غیر قانونی میزبانی شده در خارج از کشور، و فیلتر نتایج مربوط به محتوای غیر قانونی توسط موتورهای جستجو که به عنوان یک شکل از خود کنترلی، در

^۱. <http://www.edri.org/edriagram/number5.6/google-data-retention> (accessed May 11, 2007).

^۲. <http://www.edri.org/edriagram/number5.5/sweden-wiretapping> (accessed May 11, 2007).

نظر گرفته می شود. هر چند برخی از موارد و شکل های فیلترینگ توسط موتورهای جستجو و ارائه دهندگان خدمات اینترنت در تعدادی از کشورها اغلب به عنوان "خودکنترلی داوطلبانه" نام برده می شود، به نظر می رسد این اقدام داوطلبانه مبتنی بر این درک ضمنی است که همکاری با دستورات دولتی از عواقب قانونی بعدی ممانعت خواهد کرد.

فیلترینگ در کشورهای اروپایی به برخی از اختلافات حقوقی بر سر مسأله صلاحیت، شامل محتوایی که در خارج از کشور میزبانی می شود، دامن زده است. در حالی که درجه ی فیلترکردن که در میان کشورهای مختلف انجام می شود تا حدی متفاوت است. در بسیاری از کشورها نگرانی هایی در مورد افزایش میزان و گستره کلی فیلترینگ وجود دارد، همانطور که در پیشنهادات و تجدید نظرهای اخیر در قوانین، قابل مشاهده است. با این حال، فیلترینگ در کشورهای اروپایی تا حد زیادی به محتوای غیر قانونی محدود شده است، و دامنه آن بوسیله گفت و گوهای عمومی، پایبندی به قانون، و تعهد به آزادی بیان ملایم تر شده است، هر چند که دومی نسبت به وضعیت موجود در ایالات متحده، مقیدتر است.

در اتحادیه اروپا طی دهه اخیر تلاش هایی برای ایجاد یک پلت فرم مشترک "هماهنگ" مقررات اینترنت وجود داشته است. با توجه به فیلترینگ محتوای آنلاین، تاکید بر همکاری های بیشتر میان صنعت، مقامات دولتی و مقامات مجری درون کشورها و افزایش خودکنترلی داوطلبانه صنعت، بوده است. اگر چه بحث های سطح اتحادیه اروپا در ابتدا بر اشکال مختلف محتوای غیر قانونی آنلاین متمرکز شدند (به ویژه پورنوگرافی کودکان و محتوای نژادپرستانه و ضد بیگانه)، در سال های اخیر توجه بیشتری به استفاده از اینترنت برای تروریسم و جرایم سازمان یافته، شده است. حالت دوم موجب قوانینی در زمینه حفظ داده ها و بحث های زیادی در مورد نیاز به اقدامات امنیتی بیشتری در برابر مفاهیم مرتبط با حفظ حریم خصوصی شده است. همچنین پیشرفت های جدیدی در زمینه مقررات مربوط به افترا، کپی رایت، و تعریف مسئولیت ارائه دهندگان خدمات اینترنت برای محتوای آنلاین در سطح اتحادیه اروپا، صورت گرفته است. نظر به تفاوت های قابل توجه در فرهنگ و قوانین موجود در کشورهای عضو اتحادیه اروپا، ایجاد محملی (جایگاه) مشترک برای قانون گذاری در سطح منطقه، روندی آهسته و پیچیده است.