

ماژول ۳
دسترسی به اینترنت

ماژول‌هایی در مورد آزادی بیان و
حقوق دیجیتال در جنوب و جنوب
شرق آسیا



ناشر: موسسه دفاع رسانه (www.mediadefence.org)
این مجموعه آموزشی با همکاری مرکز قانون و دموکراسی (Centre for Law and Democracy) به نشانی اینترنتی: <https://www.law-democracy.org/live/> و با مشارکت ALT Advisory به نشانی اینترنتی <https://altadvisory.africa> تهیه شده است.

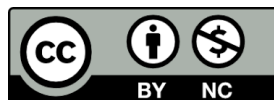
ژوئن ۲۰۲۲

با همکاری سازمان بین‌المللی حقوق غیرانتفاعی



این اثر تحت لیسانس بین‌المللی Commons Attribution-NonCommercial 4.0 منتشر شده است که به این معنی است که اشتراک‌گذاری و اقتباس از این مجموعه آموزشی بلامانع است، به شرطی که به طور مناسب به منبع اصلی ارجاع و به لیسانس موجود در این اثر لینک داده شود و در صورتی که تغییراتی در آن ایجاد شد، اعلام گردد. هرگونه اشتراک‌گذاری یا اقتباس از این مجموعه باید برای اهداف غیرتجاری باشد و باید تحت همان شرایط "اشتراک مشابه" در دسترس قرار گیرد. شرایط کامل مجوز در آدرس اینترنتی زیر قابل مشاهده است:

<https://creativecommons.org/licenses/by-nc/4.0/legalcode.en>



سلب مسئولیت

رسانی و پژوهشی ارائه شده است. این متن مشاوره حقوقی محسوب‌این انتشار صرفاً برای اهداف اطلاع عنوان چنین تلقی یا بر آن تکیه شود. با وجود تلاش فراوان برای اطمینان از دقت‌شود و نباید به‌نمی گونه مسئولیتی در قبال هرگونه خسارت یا زیان ناشی از اتکااطلاعات مندرج در اینجا، مدیا دیفنس هیچ شود پیش از هرگونه اقدام بر اساس اطلاعات موجودپذیرد. به خوانندگان توصیه می‌به این مطالب نمی در این انتشار، مشاوره حقوقی مستقل دریافت کنند.

فهرست مطالب

- 1..... آیا طبق قوانین بین‌المللی حق دسترسی به اینترنت وجود دارد؟
- 4..... اختلال در دسترسی به اینترنت.....
- 5..... قطعی اینترنت چیست؟.....
- 6..... مسدودسازی و فیلترینگ محتوا چیست؟.....
- 7..... بی‌طرفی شبکه چیست؟.....
- 8..... محدودیت حق آزادی بیان.....
- 10..... امنیت ملی به عنوان مبنای توجیه.....
- 12..... مسئولیت واسطه‌های اینترنتی.....
- 14..... نتیجه‌گیری.....

ماژول ۳

دسترسی به اینترنت

- با عنایت به این واقعیت که دسترسی به اینترنت امکان اعمال حق آزادی بیان و سایر حقوق اساسی را میسر می‌کند، تعهد کشورها مبنی بر ترویج دسترسی به اینترنت به عنوان یک حق اساسی در حال ظهور تحت قوانین بین‌المللی به رسمیت شناخته می‌شود.
- اقداماتی همچون قطع اینترنت، مسدودسازی و فیلترینگ محتوا، محدودیت‌های شدیدی بر حق آزادی بیان هستند که اغلب نمی‌توانند به عنوان محدودیت‌های موجه تلقی شوند.
- امنیت ملی اغلب به عنوان توجیهی برای محدود کردن دسترسی به اینترنت و همچنین دیگر مداخلات در حق آزادی بیان استفاده می‌شود. اگرچه امنیت ملی به عنوان یکی از اهداف مشروع برای اعمال محدودیت بر حق آزادی بیان در شرایط مناسب مطرح است، اما اغلب توسط دولت‌ها برای سرکوب مخالفت و سرپوش گذاشتن بر سوءاستفاده‌های دولتی استفاده می‌شود.
- "بی‌طرفی شبکه" به این اصل اشاره دارد که تمام داده‌های اینترنتی باید به طور یکسان و بدون تبعیض بر اساس دستگاه، محتوا، نویسنده، منشأ و یا مقصد محتوا، سرویس یا برنامه مورد بررسی قرار گیرند.
- مسئولیت واسطه‌ها زمانی رخ می‌دهد که واسطه‌های فناوری همچون ارائه دهندگان خدمات اینترنتی (ISP) و وب سایت‌ها ممکن است از نظر قانونی در قبال محتوای غیرقانونی یا مضر ایجاد شده توسط کاربران این خدمات، مسئول انتشار محتوا شناخته شوند. ایجاد چنین مسئولیتی، در رابطه با آزادی بیان در فضای مجازی و آنلاین تأثیر بازدارنده دارد.

آیا طبق قوانین بین‌المللی حق دسترسی به اینترنت وجود دارد؟

اگرچه هیچ معاهده حقوق بشری به طور صریح حق دسترسی به اینترنت را به رسمیت نشناخته است (زیرا این معاهدات اصلی قبل از گسترش استفاده از اینترنت تدوین شده اند)، با توجه به اینکه اینترنت به عنوان ابزار غالب برای انتشار اطلاعات و ایده‌ها، اعم از بیان دیدگاه‌های خود یا دسترسی به اطلاعات، عمل می‌کند؛ در حال حاضر این امر به طور فزاینده‌ای به رسمیت شناخته می‌شود که، اینترنت اکنون مرکزیت یافته است و برای اعمال حق آزادی بیان نقش محوری دارد. به همین دلیل، مجموعه فزاینده‌ای از بیانیه‌های معتبر وجود دارد که بیانگر این است که دولت‌ها موظفند گام‌های مترقی و اساسی در راستای تضمین دسترسی عمومی و همگانی به اینترنت بردارند.^۱

۱- خوان کارلوس لارا، "دسترسی به اینترنت و حقوق اقتصادی، اجتماعی و فرهنگی"، انجمن ارتباطات پیشرو (سپتامبر ۲۰۱۵)، ص ۱۰-۱۱: https://www.apc.org/sites/default/files/APC_ESCR_Access_Juan%20Carlos%20Lara_September2015%20%281%29_0.pdf

گزارش سال ۲۰۱۹ هیأت عالی دبیرکل سازمان ملل متحد در مورد همکاری دیجیتال تصریح می‌کند که: "حقوق بشری جهانشمول به میزان برابر در فضای آنلاین و آفلاین اعمال می‌شوند. آزادی بیان و تجمع همانطور که در میدان شهر اهمیت دارند، به همان اندازه در فضای سایبری نیز اهمیت دارند." صفحه ۱۶:

<https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf>

درک ماهیت حق دسترسی به اینترنت که به تدریج در حال به رسمیت شناخته شدن است، از اهمیت بالایی برخوردار است. این حق بیشتر شبیه به برخی دیگر از حقوق اقتصادی و اجتماعی مانند حق آموزش است، که توسط دولت‌ها "با هدف دستیابی به تحقق کامل" آن در طول زمان و به تدریج به رسمیت شناخته می‌شود، نه بلافاصله^۲. از این منظر، این حق به طور قابل توجهی با حقوق مدنی و سیاسی که انتظار می‌رود دولت‌ها فوراً به آن احترام بگذارند، متفاوت است. با این حال، توسعه تدریجی حقوق به معنای بی اهمیت بودن آنها نیست؛ بلکه بدین معناست که دولت‌ها موظف هستند توجه و منابع کافی را برای دستیابی به این اهداف اختصاص دهند.

اگرچه ممکن است غیرعادی به نظر برسد که دسترسی به یک فناوری خاص را به عنوان یک حق در نظر بگیریم (زیرا هرگز حق دسترسی به رسانه‌های رادیویی/بصری یا مکتوب به رسمیت شناخته نشده است)، اما اینترنت به هیچ وجه با سایر فناوری‌ها قابل مقایسه نیست. به هر اندازه که این فناوری‌ها مهم باشند، هرگز با اهمیت اینترنت در زندگی روزمره و به ویژه به عنوان یک رسانه ابراز بیان و اظهار نظر مطابقت ندارند. تنها بخش ناچیزی از مردم جهان تاکنون از فرصت ابراز خود از طریق رسانه‌های مکتوب یا رادیویی برخوردار بوده‌اند، در حالی که این مورد در خصوص اینترنت صادق نیست. همچنین شایان ذکر است که نظرسنجی‌های جهانی یک نگرش غالب در مورد دسترسی به اینترنت را نشان می‌دهند: اینکه باید به عنوان یک حق به رسمیت شناخته شود^۳.

همچنین باید توجه داشت که به رسمیت شناختن حق دسترسی به اینترنت دو جنبه متفاوت و متناقض دارد و استدلال‌هایی مخالف به رسمیت شناختن این حق وجود دارد. از یک سو، برخی استدلال می‌کنند که این امر با سایر حقوق بشری قابل مقایسه نیست و گسترش دامنه حقوق ممکن است احترام و توجه زیاد به تعداد کمتری از حقوق اصلی را تضعیف کند. همچنین دولت‌ها به دلیل پیامدهای مهم آن، از جمله در زمینه هزینه‌ها، تمایل چندانی ندارند که این حق را صراحتاً به رسمیت بشناسند.

از سوی دیگر، این روند نسبتاً روشن است که به طور فزاینده‌ای دسترسی به اینترنت به عنوان امری ضروری برای برخورداری از طیف گسترده‌ای از حقوق اساسی به رسمیت شناخته می‌شود. در نتیجه افرادی که به اینترنت دسترسی ندارند، از بهره‌مندی کامل از این حقوق محروم می‌شوند که در بسیاری موارد می‌تواند شکاف طبقاتی اجتماعی-اقتصادی موجود را تشدید کند. به عنوان مثال، عدم دسترسی به اینترنت می‌تواند توانایی فرد در کسب اطلاعات کلیدی، تسهیل تجارت، جستجوی شغل یا مصرف کالاها و خدمات را محدود و مختل کند.

دسترسی به اینترنت مستلزم توانایی تکنولوژیکی برای استفاده از اینترنت به شیوه‌ای مقرون به صرفه، ایمن، مؤثر و معنادار است. در سال ۲۰۰۳، یونسکو یکی از اولین نهادهای بین‌المللی بود که از دولت‌ها خواست تا گام‌هایی برای تحقق حق دسترسی به اینترنت بردارند. در این رابطه، یونسکو تصریح کرد که:^۴

در پرونده دلفی علیه استونی در دیوان عالی دادگاه اروپایی حقوق بشر، دادگاه اعلام کرد که: "اینترنت یک بستر بی‌سابقه برای اعمال حق آزادی بیان فراهم کرده است".

<https://globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia/>

۲- ماده ۱۳ میثاق بین‌المللی حقوق اقتصادی، اجتماعی و فرهنگی، مصوب ۱۶ دسامبر ۱۹۶۶، لازم الاجرا در ۳ ژانویه ۱۹۷۶:

<https://www.ohchr.org/sites/default/files/cesr.pdf>

۳- جامعه اینترنت، "بررسی آمار جهانی کاربران اینترنت در سال ۲۰۱۲" (۲۰۱۲):

<https://wayback.archive-it.org/9367/20170907075228>

<https://www.internet-society.org/sites/default/files/rep-GIUS2012global-201211-en.pdf>

۴- یونسکو، "توصیه‌نامه ترویج چندزبانی و استفاده از چندزبانی و دسترسی جهانی به فضای مجازی"، مفاد ۷ و ۱۵:

http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Eng%20-%20Recommendation%20concerning%20the%20Promotion%20and%20Use%20of%20Multilingualism%20and%20Universal%20Access%20to%20Cyberspace.pdf

«دولت‌ها و کشورهای عضو و سازمان‌های بین‌المللی باید دسترسی به اینترنت به عنوان یک خدمت در راستای منافع عمومی را از طریق اتخاذ سیاست‌های مناسب به منظور ارتقای فرآیند توانمندسازی شهروندی و جامعه مدنی ترویج و تقویت کنند، و ضمن در نظر گرفتن نیازهای جوامع روستایی، اجرای صحیح چنین سیاست‌هایی را در کشورهای در حال توسعه تشویق نموده و از آنها حمایت کنند.»

...

دولت‌ها و کشورهای عضو باید حق دسترسی جهانی آنلاین به سوابق عمومی و دولتی، از جمله اطلاعات مرتبط با شهروندان در یک جامعه دموکراتیک مدرن را با در نظر گرفتن ملاحظات محرمانگی، حریم خصوصی و امنیت ملی، همچنین حقوق مالکیت فکری تا حدی که به استفاده از چنین اطلاعاتی مربوط می‌شود به رسمیت بشناسند و از نظر قانونی به آن اعتبار ببخشند. همچنین سازمان‌های بین‌المللی باید حق دسترسی هر کشوری به داده‌های ضروری مربوط به وضعیت اجتماعی یا اقتصادی خود را به رسمیت شناخته و آن را اعلام نمایند.»

در سال ۲۰۱۲، شورای حقوق بشر سازمان ملل متحد (UNHRC) قطعنامه مهمی تصویب کرد که «از همه کشورها خواست تا دسترسی به اینترنت و همکاری بین‌المللی برای توسعه امکانات رسانه‌ای و فناوری اطلاعات و ارتباطات در همه کشورها را تسهیل کنند».^۵

این موضوع در اهداف توسعه پایدار سازمان ملل متحد (SDGs) نیز گسترش یافته است، که به رسمیت می‌شناسد که «گسترش فناوری اطلاعات و ارتباطات و همچنین ارتباطات جهانی، پتانسیل بزرگی برای تسریع پیشرفت بشری، پر کردن شکاف دیجیتال و توسعه جوامع دانش محور دارد».^۶ اهداف توسعه پایدار همچنین از دولت‌ها می‌خواهد که استفاده از فناوری‌های اطلاعات و ارتباطات (ICT) و سایر فناوری‌های توانمند را برای ارتقای توانمندسازی زنان^۷ افزایش دهند و تلاش کنند تا دسترسی جهانی و مقرون به صرفه به اینترنت در کشورهای کمتر توسعه یافته را تا سال ۲۰۲۰ فراهم کنند.^۸

قطعنامه سازمان ملل متحد در سال ۲۰۱۶ در مورد اینترنت که توسط شورای حقوق بشر سازمان ملل متحد به تصویب رسید، اذعان دارد که اینترنت می‌تواند به پیشرفت به سوی توسعه، از جمله در تحقق اهداف توسعه پایدار کمک کند و آن را تسریع کند و بر اهمیت اتخاذ یک رویکرد مبتنی بر حقوق در ارائه و گسترش دسترسی به اینترنت تأکید می‌کند.^۹ قطعنامه، به طور ویژه بر اهمیت اتخاذ و بکارگیری یک رویکرد جامع مبتنی بر حقوق در ارائه و گسترش دسترسی به اینترنت تأیید کرده^{۱۰}، و از دولت‌ها

۵- شورای حقوق بشر سازمان ملل متحد، «قطعنامه ترویج، حمایت و برخورداری از حقوق بشر در اینترنت»، شماره سند A/HRC/20/L.13، مصوب ۲۹ ژوئن ۲۰۱۲، بند ۲:

https://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc

گسترش و تحقق این امر در سال بعد در قطعنامه شورای حقوق بشر سازمان ملل متحد، «قطعنامه ارتقاء، حمایت و برخورداری از حقوق بشر در اینترنت»، شماره سند A/HRC/Res/26/13، مصوب ۱۴ ژوئیه ۲۰۱۴:

https://hrlibrary.umn.edu/hrcouncil_res26-13.pdf

۶- مجمع عمومی سازمان ملل متحد، «دگرگونی جهان ما: دستور کار ۲۰۳۰ برای توسعه پایدار»، به شماره سند A/Res/70/1، مصوب ۲۱ اکتبر ۲۰۱۵، بند ۱۵:

https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang=E

۷- همان، هدف شماره ۵ (b) صفحه ۱۸.

۸- همان، هدف شماره ۹ (c) صفحه ۲۱.

۹- شورای حقوق بشر سازمان ملل متحد، «قطعنامه ترویج، حمایت و برخورداری از حقوق بشر در اینترنت»، شماره سند A/HRC/Res/32/13، مصوب ۱۸ ژوئیه ۲۰۱۶، بند ۲:

<https://www.refworld.org/docid/57e916464.html>

۱۰- همان، بند ۵.

می‌خواهد تدوین و اتخاذ سیاست‌های عمومی ملی مرتبط با اینترنت را با هدف دسترسی همگانی و برخورداری از حقوق بشر در مرکز آن مدنظر داشته و در دستور کار خود قرار دهند.^{۱۱}

در اعلامیه‌های مشترک بعدی، دستورات بین‌المللی ویژه ای مربوط به آزادی بیان در سازمان ملل متحد، سازمان امنیت و همکاری اروپا، سازمان کشورهای آمریکایی و کمیسیون آفریقایی، به وضوح اعلام شده است که این نهادها حق آزادی بیان را شامل تعهد دولت‌ها برای ارتقای دسترسی عمومی به اینترنت می‌دانند. به عنوان مثال، در اعلامیه مشترک خود در سال ۲۰۱۱ در مورد "آزادی بیان و اینترنت"، آنها اظهار داشتند: "تحقق و تأثیر حق آزادی بیان، دولت‌ها را ملزم و متعهد به ارتقای دسترسی همگانی به اینترنت می‌کند."^{۱۲}

در پرونده کالدا علیه استونی (*Kalda v Estonia*)، دیوان عالی دادگاه حقوق بشر اروپا (ECtHR) اعلام کرد که حق آزادی بیان منقاضی از طریق امتناع زندان از دسترسی وی به وبسایت‌های اینترنتی حاوی اطلاعات حقوقی نقض شده است، زیرا این اقدام، حق وی در دریافت اطلاعات را نقض کرده است.^{۱۳} دیوان عالی دادگاه حقوق بشر اروپا خاطر نشان کرد که وقتی یک دولت حاضر است به زندانیان اجازه دسترسی به اینترنت دهد (همانند پرونده مذکور)، باید دلایل خود برای امتناع از دسترسی به سایت‌های خاص را ارائه دهد.^{۱۴}

علاوه بر این تحولات بین‌المللی، چندین کشور (از جمله یونان، استونی، فنلاند، اسپانیا، کاستاریکا و فرانسه) برخی از حقوق دسترسی به اینترنت را در قوانین اساسی، قوانین داخلی یا احکام قضایی خود به رسمیت شناخته‌اند.

فارق از اینکه آیا اینترنت به عنوان یک حق مستقل یا ابزاری توانمند برای تحقق سایر حقوق تلقی می‌شود یا نه، زمینه‌های و اقدامات جدی برای تحقق دسترسی همگانی به اینترنت انجام شده است. در نتیجه، دولت‌ها همگی ملزم هستند که اقدامات لازم برای دستیابی به دسترسی جهانی را انجام دهند. با این حال، در واقعیت، دسترسی جهانی به اینترنت هنوز محقق نشده است. این امر به دلیل ترکیبی از عوامل از جمله فقدان اراده سیاسی برای اولویت دادن به این موضوع، محتوای محلی نامناسب، سطوح ناکافی سواد دیجیتال و چالش‌ها در ارائه دسترسی در بسیاری از زمینه‌ها است.

اختلال در دسترسی به اینترنت

برخی از روش‌هایی که منجر به اختلال در دسترسی به اینترنت می‌شود و دسترسی به اینترنت را مختل می‌کند، شامل قطع اینترنت، اختلال در شبکه‌های آنلاین و سایت‌ها و شبکه‌های اجتماعی، و مسدود کردن و فیلترینگ محتوا است. چنین مداخله‌هایی نمایانگر محدودیت‌های شدید در برخورداری از حق آزادی بیان و همچنین بهره‌مندی از طیف گسترده‌ای از سایر حقوق و خدمات (از جمله بانکداری اینترنتی، همراه بانک، تجارت آنلاین و امکان دسترسی به خدمات دولتی از طریق اینترنت) است.

۱۱- همان، بند ۱۲.

۱۲- مصوب ۱ ژوئن ۲۰۱۱، بند ۶ (الف):

<http://www.law-democracy.org/wp-content/uploads/2011/06/11.06.Joint-Declaration.Internet.pdf>

۱۳- دادخواست شماره ۱۷۴۲۹، ۱۹ ژانویه ۲۰۱۶:

<https://hudoc.echr.coe.int/eng?i=001-160270>

۱۴- همان، بند ۵۳. حکم بعدی یانکوسکیس علیه لیتوانی، دادخواست شماره 08/21575، ۱۷ ژانویه ۲۰۱۷:

<https://hudoc.echr.coe.int/eng?i=001-170354>

همچنین در رابطه با زندانی که از دسترسی به وبسایت حاوی اطلاعات مربوط به آموزش منع شده بود، دیوان عالی دادگاه حقوق بشر اروپا مجدداً ادعای منقاضی را مبنی بر نقض حق آزادی بیان تأیید کرد.

اخلال در اینترنت یا مسدود کردن دسترسی به خدمات و وبسایت‌های اینترنتی، نوعی محدودیت از پیش تعیین شده یا سانسور پیش از انتشار محسوب می‌شود. محدودیت‌های از پیش تعیین شده، اقدامات دولتی هستند که گفتار یا سایر اشکال بیان را قبل از ابراز آنها ممنوع می‌کنند.¹⁵ با توجه به تأثیر سرکوب کننده محدودیت‌های از پیش تعیین شده بر اعمال حق آزادی بیان، معاهده بین‌المللی حقوق مدنی و سیاسی (ICCPR) به گونه‌ای تفسیر شده است که اکثر اشکال محدودیت‌های از پیش تعیین شده در بیان را ممنوع می‌کند.¹⁶ کنوانسیون آمریکایی حقوق بشر نیز ممنوعیت بسیار صریح‌تری بر محدودیت‌های از پیش تعیین شده دارد.¹⁷ بنابراین، توجیه هر گونه اقدامی از این قبیل باید بر اساس آزمون سه بخشی محدودیت‌های آزادی بیان که در ماژول ۱ تشریح شده است، مسئولیت سنگینی در قبال توجیه را به همراه داشته باشد.

قطعی اینترنت چیست؟

قطع اینترنت را می‌توان به عنوان اختلال عمدی در اینترنت یا ارتباطات الکترونیکی تعریف کرد، که طی آن اینترنت برای افراد یا منطقه‌ای خاص غیرقابل دسترسی یا به طور مؤثر غیرقابل استفاده می‌شود، که اغلب به منظور اعمال کنترل بر جریان اطلاعات صورت می‌گیرد.¹⁸ به عبارت دیگر، این امر زمانی رخ می‌دهد که چه دولت و چه عوامل و مقامات بخش خصوصی، به طور عمدی اینترنت، شبکه مخابراتی یا خدمات یک سرویس اینترنتی را مختل کنند، به گونه‌ای که بتوانند بر آنچه مردم می‌گویند یا انجام می‌دهند، کنترل یا نظارت داشته باشند.¹⁹

در برخی موارد، این قطعی ممکن است منجر به قطع کامل شبکه شود، به طوری که دسترسی به اینترنت به طور کامل قطع می‌شود که گاهی اوقات "کیل سوئیچ (kill switch)" نیز نامیده می‌شود. در سایر شرایط، ممکن است دسترسی به شبکه‌های ارتباطی تلفن همراه، وبسایت‌ها یا برنامه‌های شبکه‌های اجتماعی و پیام‌رسان‌ها مسدود، محدود یا به طور مؤثر غیرقابل استفاده شود.²⁰ قطع اینترنت ممکن است کل کشور، شهرها یا مناطق یک کشور و حتی چند کشور را تحت الشعاع قرار دهد و می‌تواند از چند ساعت تا چند ماه به طول بیانجامد.²¹

۱۵- شورای اروپا، "محدودیت‌های از پیش تعیین شده در خصوص آزادی بیان: ضرورت گنجاندن پادمان‌های رویه‌ای در سیستم داخلی" (مصوب ماه مه ۲۰۱۸):

<https://rm.coe.int/factsheet-prior-restraints-rev25may2018/16808ae88c>

۱۶- به عنوان مثال، به مقدمه معاهده بین‌المللی حقوق مدنی و سیاسی (ICCPR) مراجعه کنید؛ همانطور که Marc J. Bossuyt در کتاب "راهنمای سوابق تدوین و تهیه معاهده بین‌المللی حقوق مدنی و سیاسی" که در سال ۱۹۸۷ توسط انتشارات Martinus Nijhoff منتشر شده است، در صفحه ۳۹۸ به تفصیل به این سوابق می‌پردازد.

۱۷- ماده ۱۳ کنوانسیون:

۱. هر فردی حق آزادی اندیشه و بیان دارد. این حق شامل آزادی جست‌وجو، دریافت و انتشار اطلاعات و عقاید از هر نوع و از هر طریقی، بدون توجه به مرزهای جغرافیایی، چه به صورت شفاهی، کتبی، چاپی، هنری یا از طریق دیگر رسانه‌های مورد انتخاب خود او است.

۲. اعمال حق مندرج در بند فوق مشمول سانسور قبل از انتشار قرار نخواهد گرفت، اما منوط به تحمیل مسئولیت‌های بعدی خواهد بود، که صراحتاً توسط قانون تعیین خواهد شد تا حدی که برای تضمین موارد زیر ضروری باشد:

الف) احترام به حقوق یا شهرت دیگران؛ یا

ب) حفاظت از امنیت ملی، نظم عمومی، یا سلامت و اخلاق عمومی.

۱۸- انجمن اکسس نو (Access Now) "قطعی اینترنت چیست؟": <https://www.accessnow.org/keepiton/?ignorelocale>

۱۹- همان.

۲۰- گزارش گزارشگر ویژه سازمان ملل در مورد آزادی بیان به مجمع عمومی سازمان ملل متحد، A/HRC/35/22، مورخه ۳۰ مارس ۲۰۱۷ (گزارش سال ۲۰۱۷ گزارشگر ویژه سازمان ملل در مورد آزادی بیان)، بند ۸:

<https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/077/46/PDF/G1707746.pdf?OpenElement>

۲۱- همان.

لازم به ذکر است که دولت‌ها برای قطع کردن اینترنت معمولاً نیاز به همکاری مقامات و سازمان‌های خصوصی دارند که مدیریت شبکه‌ها را بر عهده دارند و یا ترافیک شبکه را تسهیل می‌کنند.²² همان‌طور که گزارشگر ویژه سازمان ملل متحد در مورد آزادی بیان اشاره کرده است، حملات گسترده به زیرساخت‌های شبکه توسط نهادهای خصوصی، مانند حملات انکار سرویس توزیع شده یا دیداس (DDoS) نیز ممکن است اثرات مشابه قطع اینترنت داشته باشند.

مسدودسازی و فیلترینگ محتوا چیست؟

اگرچه اقداماتی مانند مسدودسازی و فیلترینگ محتوا، به نسبت قطعی کامل اینترنت شدت کمتری دارد، اما این اقدامات نیز می‌توانند همچنان به طور قابل توجهی بر تحقق حق آزادی بیان تأثیر بگذارند و برخورداری کامل از حق آزادی بیان را مختل کنند.

فیلترینگ یا مسدودسازی به صورت زیر تعریف شود:

تفاوت بین «فیلتر کردن» و «مسدود کردن»، موضوع مقیاس و دیدگاه است؛

- فیلترینگ یا فیلتر کردن معمولاً به حالتی اطلاق می‌شود که با استفاده از فناوری، صفحات را با ارجاع به برخی ویژگی‌های خاص مانند الگوهای ترافیک، پروتکل‌ها یا کلمات کلیدی، یا بر اساس ارتباط آنها با محتوای نامناسب یا غیرقانونی، فیلتر و مسدود می‌کند.
- در مقابل، مسدودسازی معمولاً به جلوگیری از دسترسی به وبسایت‌ها، دامنه‌ها، آدرس‌های IP، پروتکل‌ها یا سرویس‌ها و خدمات خاص درج شده در لیست سیاه اشاره دارد.²³

به عنوان مثال، فیلترینگ و قطع اینترنت در بخش‌هایی از میانمار، به مدت طولانی در بخش‌هایی از این کشور رایج بوده است. پس از کودتای فوریه ۲۰۲۱، رژیم نظامی که قدرت را در دست گرفت، مکرراً به قطع اینترنت به عنوان مجموعه‌ای از ابزارهای دیجیتالی سرکوبگرانه متوسل شده است. کاهش سرعت دسترسی به اینترنت در میانمار به اشکال مختلفی از جمله قطع سراسری، قطع منطقه‌ای و محدود کردن دسترسی از طریق محدودیت سرعت و افزایش هزینه‌های داده‌ها انجام شده است.²⁴ این اقدامات رژیم نظامی برای قطع اینترنت و ایجاد سایر موانع برای دسترسی به آن در بیانیه مشترکی در ژوئن ۲۰۲۲ توسط چندین گزارشگر ویژه سازمان ملل به شدت محکوم شد.²⁵

اگرچه اقدامات رژیم نظامی میانمار در زمینه قطع اینترنت و فیلترینگ، به دلیل تکرار و طولانی مدت بودن آن، بیشتر مورد توجه جامعه بین‌المللی قرار گرفته است، اما این تنها نمونه این پدیده در منطقه جنوب و جنوب شرق آسیا نیست. در سال ۲۰۲۱، قطعی اینترنت در هند، بنگلادش، اندونزی و پاکستان نیز ثبت شده است.²⁶

۲۲- همان.

۲۳- ماده ۱۹، "آزادی بیان بدون فیلتر: مسدودسازی و فیلترینگ چگونه بر آزادی بیان تأثیر می‌گذارد"، اکتبر ۲۰۱۶، ص ۷:

https://www.article19.org/data/files/medialibrary/38588/Blocking_and_filtering_final.pdf

۲۴- آتان (Athan) "دسترسی به اینترنت در میان تاریکی و زندگی در میان تهدیدها"، می ۲۰۲۲:

<https://progressivevoicemyanmar.org/wp-content/uploads/2022/06/Internet-Shutdown-Athan-May-2022-Eng.pdf>

۲۵- گزارشگران ویژه سازمان ملل متحد در مورد وضعیت حقوق بشر در میانمار، ترویج و حمایت از آزادی بیان و عقاید، حق حریم خصوصی و حقوق آزادی تجمعات مسالمت‌آمیز و تظاهرات، میانمار: کارشناسان سازمان ملل، "دیکناتور دیجیتال" ارتش را محکوم کردند. (۲۰۲۲):

<https://www.ohchr.org/en/press-releases/2022/06/myanmar-un-experts-condemn-militarys-digital-dictatorship>

۲۶- انجمن اکسس نو، "بازگشت اقتدارگرایی دیجیتال: قطعی اینترنت در سال ۲۰۲۱"، ص ۴:

<https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf>

بی‌طرفی شبکه چیست؟

بی‌طرفی شبکه (Network Neutrality) به این معنی است که نباید در برخورد با داده‌ها و ترافیک اینترنتی، بر اساس دستگاه، محتوا، نویسنده، منشأ و یا مقصد محتوا، سرویس یا برنامه، هیچ گونه تبعیضی صورت گیرد²⁷. به عبارت دیگر، ارائه‌دهندگان خدمات اینترنتی باید با تمام داده‌هایی که از طریق شبکه‌های آنها منتقل می‌شود به صورت منصفانه و بدون تبعیض نادرست به نفع یک برنامه، وبسایت یا سرویس خاص، برخورد کنند²⁸. تبعیض در این زمینه ممکن است به معنای تأثیرگذاری بر اطلاعات به نحوی باشد که انتقال هر گونه داده را متوقف، کند یا دستکاری کند، مگر اینکه با هدف مدیریت قانونی شبکه مانند کاهش ازدحام یا مسدود کردن هرزنامه صورت گیرد²⁹. گزارش سال ۲۰۱۷ گزارشگر ویژه سازمان ملل متحد در مورد آزادی بیان دو روش کلیدی را توصیف می‌کند که از طریق آنها می‌توان بی‌طرفی شبکه را تحت تأثیر قرار داد:³⁰

- **طرح‌های اولویت‌بندی پولی:** در این حالت، ارائه‌دهندگان خدمات اینترنتی در ازای دریافت هزینه یا سایر مزایای تجاری، ترافیک اینترنتی محتواهای خاصی را نسبت به سایر محتواها در اولویت قرار می‌دهند.

- **محتوای رایگان یا نرخ‌گذاری صفر (Zero-rating):** این رویه به این صورت است که ارائه‌دهندگان خدمات اینترنتی برای دسترسی به یک برنامه یا مجموعه‌ای از خدمات خاص، هزینه‌ای دریافت نمی‌کنند، اما برای دسترسی به سایر خدمات یا برنامه‌ها هزینه‌ای اخذ می‌شود.

در کشورهای مختلف آسیا، بحث‌های قابل توجهی پیرامون دسترسی به محتوای رایگان و با نرخ‌گذاری صفر وجود داشته است، زیرا وبسایت‌های شبکه‌های اجتماعی که دسترسی رایگان به کاربران ارائه می‌دهند، از یک طرف استدلال می‌کنند که این امر به افرادی که در غیر این صورت قادر به دسترسی به اینترنت نبودند، امکان دسترسی را فراهم می‌کند و می‌تواند به عنوان دروازه‌ای برای کاربران برای درک فرصت‌های ارائه شده در اینترنت عمل کند. اما در عمل، این افراد اغلب تنها به خدمات ممتاز دسترسی پیدا می‌کنند و ممکن است به اشتباه تصور کنند که این خدمات شامل دسترسی به کل اینترنت است. از سوی دیگر، نرخ‌گذاری صفر منجر به رقابت ناعادلانه می‌شود و می‌تواند درک کاربران را با محدود نمودن دسترسی به برخی سایت‌ها تحریف کند.³¹

هند از جمله کشورهایی است که علیه محتوای رایگان و دارای نرخ‌گذاری صفر اقدام کرده و در واقع آن را ممنوع کرده است. در سال ۲۰۱۶، مقررات جدیدی تصویب شد که ارائه‌دهندگان دسترسی به اینترنت را از ارائه یا دریافت تعرفه‌های تبعیض‌آمیز برای سرویس‌های داده بر اساس محتوا، به استثنای موارد محدود برای محتوای رایگان و دارای نرخ‌گذاری صفر برای خدمات اضطراری، منع می‌کرد³².

۲۷- گزارش سال ۲۰۱۷ گزارشگر ویژه سازمان ملل متحد در مورد آزادی بیان، مرجع شماره ۱۸، بند ۲۳.

۲۸- بنیاد مرزهای الکترونیکی، "بی‌طرفی شبکه": <https://www.eff.org/issues/net-neutrality>

۲۹- اتحادیه آزادی‌های مدنی آمریکا، "بی‌طرفی شبکه چیست؟"

<https://www.aclu.org/issues/free-speech/internet-speech/what-net-neutrality>

۳۰- گزارش سال ۲۰۱۷ گزارشگر ویژه سازمان ملل متحد در مورد آزادی بیان، مرجع ۱۸، بند ۲۴ تا ۲۸.

۳۱- برای مرور و بررسی وضعیت قانونی طرح‌های نرخ‌گذاری صفر در سطح جهانی، به مطالعات و نظرات مشورتی ارائه شده توسط مرکز قانون و دموکراسی در سال ۲۰۳۲، و به احکام دادگاه عالی قانون اساسی در روند رسیدگی به پرونده D-14516 درباره قانون ۱۴۵۰، مصوب سال ۲۰۱۱، بندهای ۱۰۱ تا ۱۱۲ مراجعه کنید:

<https://www.law-democracy.org/live/wp-content/uploads/2022/02/Colombia.Zero-Rating-Brief.CLD.final.pdf>

۳۲- اطلاعیه شماره ۲ سازمان تنظیم مقررات مخابراتی هند در مورد "مقررات ممنوعیت تعرفه‌های تبعیض‌آمیز برای خدمات داده"، (۲۰۱۶) https://tra.gov.in/sites/default/files/Regulation_Data_Service.pdf

این مقررات در پی برگزاری یک کمپین فعال توسط فعالان حقوق دیجیتال در هند وضع شد. این امر عمدتاً تحت تأثیر برنامه Free Basics فیسبوک بود که فعالان آن را به دلیل ارائه دسترسی رایگان به تعداد محدودی از وبسایت‌های از پیش انتخاب‌شده توسط فیسبوک به جای ارائه دسترسی گسترده‌تر به اینترنت برای افراد کم‌درآمد مورد انتقاد قرار داده بودند.³³ هند از آن زمان ممنوعیت محتوای رایگان را در قوانین جدید خود در رابطه با بی‌طرفی شبکه حفظ کرده است.³⁴

محدودیت حق آزادی بیان

در سال ۲۰۱۶، گزارشگر ویژه سازمان ملل در زمینه آزادی بیان خاطرنشان کرد: "مسدود کردن پلتفرم‌های اینترنتی و قطع خدمات و مسدودسازی زیرساخت‌های مخابراتی، تهدیدهای مداوم هستند، زیرا حتی اگر این اقدامات به بهانه امنیت ملی یا برقراری نظم عمومی انجام شوند، اغلب ارتباطات میلیون‌ها نفر را مسدود می‌کند"³⁵. این موضوع محدودیت آشکاری بر حق آزادی بیان تحمیل می‌کند و ممکن است بر طیف گسترده‌تری از حقوق نیز اثر محدودتر داشته باشد.

بیانیه مشترک سال ۲۰۱۱ در مورد آزادی بیان و اینترنت، تأثیر شدیدی که محدودیت‌های اعمال‌شده ایجاد می‌کنند را بیان می‌کند:³⁶

- (الف) مسدود کردن اجباری کل وبسایت‌ها، آدرس‌های IP، درگاه‌ها و پورت‌ها، پروتکل‌های شبکه یا انواع شبکه‌های کاربردی (مانند شبکه‌های اجتماعی) اقدامی افراطی است (شبیه ممنوع کردن یک روزنامه یا یک شبکه تلویزیونی)، که تنها در صورت انطباق با استانداردهای بین‌المللی قابل توجیه است، مانند مواردی که برای محافظت از کودکان در برابر سوءاستفاده جنسی لازم است.
- (ب) سیستم‌های فیلترینگ محتوا که توسط دولت یا ارائه‌دهنده خدمات تجاری تحمیل می‌شوند و توسط کاربران کنترل نمی‌شوند، شکلی از سانسور از پیش تعیین شده هستند و به عنوان محدودیتی بر آزادی بیان قابل توجیه نیستند.
- (پ) محصولات و به منظور تسهیل فیلترینگ توسط کاربران طراحی شده‌اند باید، همراه با اطلاعات واضحی درباره نحوه عملکرد و مشکلات بالقوه آنها در زمینه فیلترینگ گسترده، به کاربران نهایی ارائه شوند.

قطع و محدودیت دسترسی به اینترنت و قطع شبکه‌های مخابراتی و ارتباطی که با هدف اختلال عمدی در دسترسی به اینترنت یا جلوگیری از انتشار اطلاعات آنلاین انجام می‌شود، نقض قوانین حقوق بشر است.³⁷ در قطعنامه سازمان ملل در سال ۲۰۱۶ در مورد اینترنت، شورای حقوق بشر سازمان ملل اعلام کرد که "اقداماتی را که موجب مختل کردن عمدی دسترسی به اینترنت یا مانع انتشار اطلاعات آنلاین می‌شوند و قوانین بین‌المللی حقوق بشر را نقض می‌کنند، به صراحت و به شدت محکوم می‌کند و از تمامی کشورها می‌خواهد چنین اقداماتی را متوقف نمایند."³⁸

۳۳- گاردین، آیوش سونی، "هند در مناقشه بی‌طرفی شبکه، به فیس‌بوک که از سوی مردم تأمین می‌شود، ضربه می‌زند" (۲۰۱۶): <https://www.theguardian.com/technology/2016/feb/08/india-facebook-free-basics-net-neutrality-row>

بی‌بی‌سی، سوتیک بیسواس، "چرا مارک زاکریگ از منتقدان در هند عصبانی است؟" (۲۰۱۵): <https://www.bbc.com/news/world-asia-india-35192184>

۳۴- بی‌بی‌سی، "هند شدیدترین قوانین بی‌طرفی شبکه جهان را تصویب می‌کند" (۲۰۱۸): <https://www.bbc.com/news/world-asia-india-44796436>

۳۵- گزارش سال ۲۰۱۶ گزارشگر ویژه سازمان ملل در زمینه آزادی بیان به مجمع عمومی سازمان ملل، A/71/373، ۶ سپتامبر ۲۰۱۶، بند ۲۲: https://www.un.org/ga/search/view_doc.asp?symbol=A/71/373

۳۶- بیانیه مشترک سال ۲۰۱۱ در مورد آزادی بیان، بند ۳.

۳۷- همان، بند ۶ (ب)

۳۸- همان، بند ۱۰.

همانطور که در نظر عمومی شماره ۳۴، مصوب کمیته حقوق بشر سازمان ملل آمده است: 39

”اعمال هرگونه محدودیت بر عملکرد وبسایتها، وبلاگها یا سایر سیستمهای انتشار اطلاعات مبتنی بر اینترنت، الکترونیکی یا سایر سیستمهایی از این قبیل، از جمله سیستمهای پشتیبان چنین ارتباطاتی مانند ارائهدهندگان خدمات اینترنتی یا موتورهای جستجو، تنها در صورتی مجاز است که با ماده ۱۹ (بند ۳) میثاق بینالمللی حقوق مدنی و سیاسی مطابقت داشته باشد. محدودیتهای مجاز باید معمولاً مرتبط با محتوا باشند؛ ممنوعیتهای کلی بر عملکرد برخی سایتها و سیستمها، با ماده ۱۹ (بند ۳) میثاق بینالمللی حقوق مدنی و سیاسی سازگار نیستند. همچنین ممنوع کردن انتشار مطالب در یک سایت یا سیستم انتشار اطلاعات، صرفاً به دلیل اینکه ممکن است منتقد دولت یا نظام سیاسی-اجتماعی مورد حمایت دولت باشند، با ماده ۱۹ (بند ۳) میثاق بینالمللی حقوق مدنی و سیاسی مغایر است و این اصل را نقض می‌کند.“

گزارشگر ویژه سازمان ملل در زمینه آزادی بیان تأکید کرده است که قطع دسترسی به اینترنت اغلب به صورت مخفیانه و بدون مبنای قانونی صورت می‌گیرد، و این موضوع الزام قانونی بودن محدودیتها را نقض می‌کند.⁴⁰ به همین ترتیب، قطع ارتباطات که بر اساس قوانین و مقررات مبهم انجام می‌شود نیز نمی‌تواند معیار قانونی بودن را برآورده کند و از الزامات قانونی برخوردار نیست.⁴¹ در برخی کشورها، این امر منجر به تصویب قوانین جدید توسط دولت شده است تا به صورت صریح امکان قطع ارتباطات را فراهم کنند. این اقدامات در تعارض با الزامات حقوق بینالملل در زمینه آزادی بیان قرار دارد، زیرا محدودیت‌های وضع‌شده باید مطابق با قوانین موجود و به منظور هدف‌های مشخص و مشروع باشند.⁴²

گزارشگر ویژه سازمان ملل در زمینه آزادی بیان همچنین خاطر نشان کرده است که قطع شبکه، همیشه استانداردهای ضروری را برآورده نمی‌کند و از معیار لازم برخوردار نیست.⁴³ و به طور کلی متناسب نیست.⁴⁴ کشورها اغلب تلاش می‌کنند این اقدامات را با استناد به مسائل امنیت ملی توجیه کنند که در ادامه بیشتر مورد بحث و بررسی قرار می‌گیرد. مثلاً بر اساس گزارش گروه حامی حقوق دیجیتال "Access Now"، سال ۲۰۲۱ چهارمین سال متوالی بود که هند با ۱۰۶ مورد قطعی اینترنت، بیشترین تعداد قطع دسترسی به اینترنت در جهان را ثبت کرده است.⁴⁵ طبق تحقیقات این گروه، ناآرامی‌ها و بی‌ثباتی سیاسی دلیل اصلی اکثر موارد قطع اینترنت در هند بوده است (۸۰ مورد)، و پس از آن اعتراضات (۹ مورد) و خشونت و درگیری‌های دسته‌جمعی (۷ مورد) در رتبه‌های بعدی قرار دارند.⁴⁶

حکم دادگاه عالی هند در رابطه با قطع اینترنت

۳۹- نظریه عمومی شماره ۳۴ کمیته حقوق بشر سازمان ملل، بند ۴۳.

۴۰- گزارش سال ۲۰۱۷ گزارشگر ویژه سازمان ملل متحد در مورد آزادی بیان، بند ۹.

۴۱- همان، بند ۱۰.

۴۲- به عنوان مثال، در هند، پس از بیش از ۴۰ بار قطع اینترنت در سال ۲۰۱۷، وزارت مخابرات مقررات جدیدی را در آگوست ۲۰۱۷ با عنوان "قوانین تعلیق موقت خدمات مخابراتی (اضطرار عمومی یا امنیت عمومی)" وضع کرد که به دولت اجازه می‌داد در شرایط اضطراری عمومی یا به منظور تأمین امنیت عمومی، خدمات تلفن و اینترنت را محدود یا قطع کند. پیش از این، دولت برای اعمال محدودیت‌های اینترنتی، به بند ۱۴۴ قانون جزا استناد می‌کرد که با هدف جلوگیری از "مزاحمت، آزار یا آسیب" تدوین شده بود. این تحول قانونی با واکنش‌های مختلفی روبرو شد. از یک سو، قوانین و مقررات مصوب سال ۲۰۱۷ امکان محدود کردن و قطعی اینترنت توسط دولت را به شکل منسجم‌تری فراهم کرد. از سوی دیگر، نگرانی‌هایی در مورد فقدان تعاریف مشخص برای عبارات "اضطرار عمومی" یا "امنیت عمومی" و پتانسیل قوانین جدید برای سانسور آنلاین مطرح شد. به عنوان مثال به لینک زیر مراجعه کنید:

<http://www.hindustantimes.com/india-news/govt-issues-first-ever-rules-to-carry-out-internet-shutdowns-in-india/story-Drn0MnxJAp58RoZoF17u4L.html>

در عمل، قطعی اینترنت در هند در سال‌های بعد افزایش یافت و این کشور به دلیل عدم اجرای الزامات تحت قوانین مصوب سال ۲۰۱۷ مبنی بر ایجاد یک مخزن متمرکز داده‌ها در مورد قطعی اینترنت مورد انتقاد قرار گرفت. مراجعه شود به انجمن Access Now، "بازگشت اقتدارگرایی دیجیتال: قطعی اینترنت در سال ۲۰۲۱"، ص ۷.

۴۳- گزارش سال ۲۰۱۷ گزارشگر ویژه سازمان ملل متحد در مورد آزادی بیان، بند ۱۴.

۴۴- همان، بند ۱۵.

۴۵- انجمن Access Now، "بازگشت اقتدارگرایی دیجیتال: قطعی اینترنت در سال ۲۰۲۱"، ص ۲.

۴۶- همان، ص ۱۴.

دادگاه عالی هند در حکم خود در سال ۲۰۲۰ در پرونده بهاسین علیه اتحادیه هند، مشروعیت قطع دسترسی به اینترنت در کشمیر را مورد بررسی قرار داده است.⁴⁷ دادگاه عالی در این حکم اعلام کرد که قطع کامل دسترسی به اینترنت، اقدامی "افراطی" است که باید توسط دولت "تنها در صورت ضرورت و اجتناب ناپذیری" در نظر گرفته شود و دولت باید "وجود راهکار جایگزین با شدت کمتر را ارزیابی کند".⁴⁸ دادگاه تأکید کرد که هرگونه تعلیق دسترسی به اینترنت باید با اصل تناسب مطابقت داشته و بیش از میزان لازم ادامه نیابد و تمدید نشود.⁴⁹ اگرچه دادگاه در این حکم رویکردی محتاطانه در قبال قطع اینترنت اتخاذ کرده است، استانداردهای بین‌المللی حتی از این هم فراتر می‌رود. طبق قوانین بین‌المللی حقوق بشر، قطع دسترسی به اینترنت همواره محدودیت غیر قابل توجیه آزادی بیان محسوب می‌شود.⁵⁰

در رابطه با مسدود کردن و فیلترینگ محتوا، در برخی موارد ممکن است شرایطی وجود داشته باشد که چنین اقداماتی قابل توجیه باشند. به عنوان مثال، مسدود کردن وبسایت‌هایی که تصاویر مستهجن و پورنوگرافی کودکان منتشر می‌کنند. اما حتی در این موارد نیز، چنین اقداماتی باید آزمون سه بخشی محدودیت‌ها را برآورده کنند که باید به صورت موردی ارزیابی و بررسی شود.

به همین ترتیب، محدودیت‌های اعمال‌شده بر بی‌طرفی شبکه نیز ممکن است در برخی موارد مشخص، مانند اهداف مشروع مدیریت شبکه، قابل توجیه باشند. با این حال، به عنوان یک اصل کلی، صرف‌نظر از نوع دستگاه، محتوا، نویسنده، منشأ و یا مقصد محتوا، خدمات یا برنامه، نباید در قبال داده‌ها و ترافیک اینترنتی هیچ گونه تبعیضی وجود داشته باشد.⁵¹ علاوه بر این، واسطه‌های اینترنتی باید در مورد هرگونه اقدام مدیریت ترافیک یا اطلاعات که به کار می‌گیرند، شفاف‌سازی کرده و اطلاعات مربوطه باید به نحوی در دسترس همه ذی‌نفعان قرار گیرد.⁵²

امنیت ملی به عنوان مبنای توجیه

امنیت ملی اغلب به عنوان توجیهی برای مداخله و ایجاد اختلال در دسترسی به اینترنت و همچنین سایر محدودیت‌های حق آزادی بیان مورد استناد قرار می‌گیرد.⁵³ اگرچه این استناد ممکن است در شرایط مناسب مشروع باشد، اما این پتانسیل را نیز دارد که برای سرکوب مخالفان و سرپوش گذاشتن بر سوء استفاده‌های دولتی مورد استفاده قرار گیرد.

ماهیت پنهانی بسیاری از قوانین، سیاست‌ها و رویه‌های امنیت ملی، همچنین امتناع دولت‌ها از افشای اطلاعات در مورد تهدیدهای امنیت ملی، این نگرانی را تشدید می‌کند. علاوه بر این، دادگاه‌ها و سایر نهادها، در تعیین آنچه تهدید امنیت ملی محسوب می‌شود، اغلب به شکل نامتناسبی به دولت تمکین کرده‌اند. همانطور که قبلاً اشاره شد:⁵⁴

۴۷- دادگاه عالی هند، دادخواست کتبی (مدنی) شماره 1031/2019 (۲۰۲۰):

https://main.sci.gov.in/supremecourt/2019/28817/28817_2019_2_1501_19350_Judgement_10-Jan-2020.pdf

۴۸- همان، بند ۹۹

۴۹- همان، مفاد بند ۷۱ و ۱۵۲ (ت).

۵۰- گزارش ۲۰۱۷ گزارشگر ویژه سازمان ملل متحد در مورد آزادی بیان، بند ۹ تا ۱۴.

۵۱- اعلامیه مشترک مذکور در مرجع شماره ۱۲، بند ۵ (الف).

۵۲- همان، بند ۵ (ب).

۵۳- برای بحث کامل‌تر در مورد امنیت ملی به طور گسترده‌تر، به "راهنمای آموزشی در مورد رسانه‌های بین‌المللی و تطبیقی و قانون آزادی بیان"، ریچارد کارور، ص ۷۷ الی ۸۸ مراجعه کنید:

<https://www.media-defence.org/resource-hub/resources/media-defence-training-manual-on-international-and-comparative-media-and-freedom-of-expression-law/>

۵۴- گزارش گزارشگر ویژه سازمان ملل در مورد آزادی بیان به دبیر کل سازمان ملل، A/HRC/23/40، ۱۷ آوریل ۲۰۱۳، بند ۶۰:

http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

"استفاده از مفهوم میهم امنیت ملی برای توجیه محدودیت‌های تهاجمی در بهره‌مندی از حقوق بشر، به طور جدی نگران‌کننده است. این مفهوم به طور گسترده تعریف شده است و بنابراین به عنوان ابزاری برای توجیه اقداماتی که به گروه‌های آسیب‌پذیر مانند مدافعان حقوق بشر، روزنامه‌نگاران یا فعالان سیاسی هدف می‌گیرند، توسط دولت مورد سوء استفاده قرار می‌گیرد. همچنین این امر موجب توجیه و تضمین پنهان‌کاری غیرضروری در مورد تحقیقات یا فعالیت‌های اجرای قانون می‌شود که اصول شفافیت و پاسخگویی را تضعیف می‌کند."

همانطور که در اصول ژوهانسبورگ در مورد امنیت ملی، آزادی بیان، گردش آزاد اطلاعات و دسترسی به اطلاعات (اصول ژوهانسبورگ) آمده است:⁵⁵

"(الف) محدودیتی که به دنبال توجیه امنیت ملی باشد مشروع نیست مگر اینکه هدف واقعی و اثر قابل اثبات آن، محافظت از موجودیت کشور یا تمامیت ارضی آن در برابر استفاده و یا تهدید به زور باشد، یا ماهیت آن پاسخ‌گویی به تهدید یا زور باشد، چه از طرف منبع خارجی مانند تهدید نظامی و چه منبع داخلی مانند تحریک به سرنگونی خشونت‌آمیز دولت.

(ب) به طور ویژه، محدودیتی که به دنبال توجیه امنیت ملی است، اگر هدف واقعی یا اثر قابل اثبات آن، حفاظت از منافع غیرمرتبط با امنیت ملی، از جمله محافظت از دولت در برابر شرمساری، آشکارسازی تخلفات یا پنهان کردن اطلاعات درباره عملکرد نهادهای دولتی، تثبیت یک ایدئولوژی خاص یا سرکوب اعتراضات کارگری و اعتصابات باشد، مشروع نیست."

اصل ۷ از اصول ژوهانسبورگ به شرایطی اشاره می‌کند که در آن اعمال حق آزادی بیان به صورت مسالمت‌آمیز نباید به عنوان تهدیدی برای امنیت ملی تلقی شده و مشمول هیچ محدودیت یا مجازاتی شود.

یک دیگر از اصول مهم مندرج در اصول ژوهانسبورگ، اصل ۲۳ است که مقرر می‌دارد: "ابراز عقیده و بیان نباید به منظور حفاظت از امنیت ملی تحت سانسور قبلی یا پیش از انتشار قرار گیرد، مگر در مواقع اضطراری عمومی که حیات کشور را تهدید می‌کند." تدابیری که در بالا توضیح داده شد، اغلب منجر به ایجاد محدودیت‌های قبلی و از پیش تعیین شده بر روی محتوا می‌شوند و به تبع آن، اثری بازدارنده بر بهره‌مندی از حق آزادی بیان دارند.

همانطور که محدودیت‌های ادعایی بر اساس امنیت ملی باید با احتیاط شدید مورد بررسی قرار گیرد، به طور مشابه، در خصوص مبارزه با تروریسم به عنوان توجیهی برای قطع شبکه یا سایر محدودیت‌ها و اختلالات دسترسی به اینترنت نیز باید با احتیاط کامل برخورد شود. همانطور که در نظر عمومی شماره ۳۴ ذکر شده است، رسانه‌ها نقش مهمی در اطلاع‌رسانی به عموم مردم در رابطه با اقدامات تروریستی دارند و باید بتوانند بدون هیچ گونه محدودیتی، عملکرد و وظایف قانونی خود را انجام دهند.⁵⁶ اگرچه دولت‌ها ممکن است استدلال نمایند که قطعی اینترنت برای جلوگیری از انتشار اخبار مربوط به حملات تروریستی و جلوگیری از ایجاد هراس عمومی یا کپی‌برداری ضروری است، اما تجربه نشان داده است که برعکس، برقراری ارتباط و اتصال به اینترنت می‌تواند تأثیرات منفی بر امنیت عمومی را کاهش داده و به حفظ نظم عمومی کمک کند.⁵⁷

۵۵- اصل ۲ از اصول ژوهانسبورگ در مورد امنیت ملی، آزادی بیان و دسترسی به اطلاعات، نوامبر ۱۹۹۶:

<https://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf>

اصول ژوهانسبورگ توسط گروهی از کارشناسان و متخصصان حقوق بین‌الملل، امنیت ملی و حقوق بشر تدوین شد، که بواسطه ماده ۱۹ میثاق گرد هم آمده بودند.

۵۶- نظر عمومی شماره ۳۴، بند ۴۶.

۵۷- گزارش سال ۲۰۱۷ گزارشگر ویژه سازمان ملل در مورد آزادی بیان، بند ۱۴.

در بدترین شرایط، اگر قرار باشد دسترسی به اینترنت محدود شود، باید درباره قوانین، سیاست‌ها و رویه‌های مورد استناد شفاف‌سازی شود، و تعاریف واضح و روشنی از مفاهیمی همچون "امنیت ملی" و "تروریسم" ارائه شود و نظارت مستقل و بی‌طرف بر این اقدامات صورت گیرد.

مسئولیت واسطه‌های اینترنتی

مسئولیت واسطه‌های اینترنتی جایی است که واسطه‌های فناوری مانند ارائه‌دهندگان خدمات اینترنتی و وبسایت‌ها ممکن است در قبال محتوای غیرقانونی منتشر شده توسط کاربران این سرویس‌ها، به لحاظ قانونی مسئول شناخته شوند.⁵⁸ این مسئولیت ممکن است در قبال موارد مختلفی، از جمله نقض حق نشر و کپی‌رایت، سرقت ادبی، اختلافات مربوط به برند تجاری، مدیریت شبکه، ارسال هرزنامه و فیشینگ، "جرایم سایبری"، افترا، نفرت‌پراکنی، پورنوگرافی کودکان و نقض حریم خصوصی ایجاد شود.⁵⁹

گزارشی که توسط یونسکو منتشر شده است، استانداردهای زیر را در رابطه با مسئولیت واسطه‌ها مشخص می‌کند:⁶⁰

- محدود کردن مسئولیت واسطه‌ها در قبال محتوای منتشر شده یا ارسال شده توسط اشخاص ثالث، به منظور رشد و شکوفایی خدمات اینترنتی که تسهیل‌کننده ابراز عقیده و نظر هستند، ضروری است.
- در بسیاری از حوزه‌های قضایی قوانین، سیاست‌ها و مقرراتی که واسطه‌ها را ملزم به اعمال محدودیت‌های محتوا، مسدود کردن و فیلترینگ می‌کنند، با استانداردهای بین‌المللی حقوق بشر در زمینه آزادی بیان سازگار نیستند.
- قوانین، سیاست‌ها و رویه‌های مربوط به نظارت دولتی و جمع‌آوری داده‌ها از واسطه‌ها، در مواردی که با هنجارهای حقوق بشر سازگار نیستند، مانع از توانایی واسطه‌ها در محافظت مناسب از حریم خصوصی کاربران می‌شود.
- در حالی که به دلیل انجام صحیح فرآیندها، اعمال قانون و تصمیم‌گیری‌ها باید شفاف و در دسترس عموم باشد، دولت‌ها اغلب در مورد درخواست‌های شرکت‌ها برای محدود کردن محتوا، ارائه داده‌های کاربران و سایر اقدامات نظارتی، شفافیت لازم را ندارند.

در مورد مسئولیت واسطه‌های اینترنتی، توافق کلی این است که معاف کردن آنها از مسئولیت در قبال محتوای تولید شده توسط دیگران، از حق آزادی بیان به صورت آنلاین محافظت می‌کند. این معافیت می‌تواند یا از طریق یک سیستم مصونیت مطلق از مسئولیت حاصل شود، یا با ایجاد رژیم‌ها باشد که مسئولیت واسطه‌ها را صرفاً پس از امتناع آنها از دستور دادگاه یا سایر نهادهای ذیصلاح برای حذف محتوای مورد اعتراض تعیین می‌کند.

در مورد دسته دوم، بیانیه مشترک ۲۰۱۱ تصریح می‌کند که واسطه‌ها فقط زمانی باید در قبال محتوای شخص ثالث مسئول باشند که به طور خاص در آن محتوا مداخله کرده یا از دستوری که مطابق با

۵۸- آکس کامنینوس، (Alex Comninos)، "مسئولیت واسطه‌های اینترنتی در نیجریه، کنیا، آفریقای جنوبی و اوگاندا: یک منطقه بی‌ثبات" (۲۰۱۲)، ص ۶:

https://www.apc.org/sites/default/files/READY%20%20Intermediary%20Liability%20in%20Africa_FINAL_0.pdf

۵۹- همان.

۶۰- ریکا مک کینون و همکاران، "ارتقای آزادی آنلاین: نقش واسطه‌های اینترنتی" (۲۰۱۴)، صص ۱۷۹ و ۱۸۰:

https://unesdoc.unesco.org/ark:/48223/pf0000231162_eng

ضمانت‌های روند قانونی توسط یک نهاد ناظر مستقل، بی‌طرف و صالح (مانند دادگاه) برای حذف آن محتوا صادر شده است، خودداری کنند⁶¹

دادگاه حقوق بشر اروپا در چند پرونده، مسئولیت واسطه‌های اینترنتی را بررسی و آنها را مسئول دانست:

- در پرونده شکایت دلفی علیه استونیا در سال ۲۰۱۳، دادگاه حقوق بشر اروپا، به موضوع مسئولیت یک پایگاه خبری آنلاین در قبال نظرات توهین‌آمیز خوانندگان که در زیر یکی از مقالات آن منتشر شده بود، پرداخت.⁶² پایگاه خبری به اینکه وقتی اظهار نظر کاربران حق آزادی بیان را نقض کرده است مسئول شناخته شود اعتراض کرده بود. اما دادگاه حقوق بشر اروپا، رأی دادگاه‌های داخلی مبنی بر عدم مسئولیت این پورتال را رد کرد و اعلام کرد این یک محدودیت موجه و متناسب برای آزادی بیان است و این پورتال می‌تواند بابت نظرات توهین‌آمیز کاربران مسئول شناخته شود؛ چرا که این نظرات بسیار توهین‌آمیز بودند، پایگاه خبری نتوانسته بود از انتشار آنها جلوگیری کند، از وجود آنها سود برده بود و به نویسندگان این نظرات اجازه داده بود ناشناس باقی بمانند. دادگاه حقوق بشر اروپا همچنین اشاره کرد که جریمه اعمال شده توسط دادگاه‌های استونی، بیش از حد سنگین نبوده است.

- در پرونده Index.hu Zrt و Magyar Tartalomszolgáltatók Egyesülete علیه مجارستان در سال ۲۰۱۶، دادگاه حقوق بشر اروپا به موضوع مسئولیت یک نهاد خودنظارتی ارائه‌دهندگان محتوای اینترنتی و یک پایگاه خبری آنلاین در قبال نظرات مبتذل و توهین‌آمیز کاربران در وبسایت‌های آنها پرداخت.⁶³ دادگاه حقوق بشر اروپا مجدداً تأکید کرد که اگرچه این پایگاه‌ها ناشر سنتی نظرات کاربران نیستند، اما باید وظایف و مسئولیت‌هایی را بپذیرند. این دادگاه دریافت که اگرچه نظرات توهین‌آمیز و مبتذل بودند، اما سخنان غیرقانونی نبودند و ادعای نقض حق آزادی بیان را تأیید کرد.

- در پرونده Tamiz علیه بریتانیا در سال ۲۰۱۷، دادگاه حقوق بشر اروپا از دلیل کافی برای بررسی حدود مسئولیت واسطه‌های اینترنتی برخوردار بود.⁶⁴ متقاضی که یک سیاستمدار سابق در بریتانیا بود، در دادگاه‌های داخلی ادعا کرده بود که برخی نظرات ارسال شده توسط کاربران ناشناس در Blogger.com گوگل، توهین‌آمیز بوده‌اند. در دادگاه حقوق بشر اروپا، خواهان استدلال کرد که حق او برای رعایت حریم زندگی خصوصی نقض شده است، زیرا دادگاه‌های داخلی از اعطای راه‌حلی علیه واسطه خودداری کرده‌اند. اما ادعای او در نهایت توسط دادگاه اروپایی حقوق بشر رد شد، و

۶۱- اعلامیه مشترک ۲۰۱۱ مذکور در مرجع شماره ۱۲، بند ۲ (الف) - (ب).

۶۲- درخواست شماره 09/64569، ۱۰ اکتبر ۲۰۱۳: <https://hudoc.echr.coe.int/eng?i=001-155105>

۶۳- درخواست شماره 13/22947، ۲ فوریه ۲۰۱۶: <https://hudoc.echr.coe.int/eng?i=001-160314>

۶۴- پرونده شکایت تیمز علیه انگلستان، شماره 14/3877، ۱۹ سپتامبر ۲۰۱۷: <https://hudoc.echr.coe.int/eng?i=001-178106>

مؤسسه دفاع رسانه همراه با ائتلافی از سازمان‌ها، اصول پیشنهادی برای تعیین مسئولیت واسطه‌های اینترنتی بر اساس بهترین رویه‌های موجود در قوانین ملی، دیدگاه‌های کمیته وزرای شورای اروپا و صاحب‌منصبان ویژه، مطالبی را به دادگاه حقوق بشر اروپا ارائه کردند.

در پرونده مذکور در دادگاه اروپایی حقوق بشر، مؤسسه دفاع رسانه همراه با ائتلافی از سازمان‌های دیگر، اصول زیر را پیشنهاد کردند:

- واسطه‌های اینترنتی نباید داور قانونی بودن محتوایی باشند که کاربران خدمات آنها منتشر، ذخیره یا ارسال می‌کنند.
- در صورتی که واسطه‌ها در انتشار محتوا مشارکت نداشته یا آن را تغییر نداده باشند، تا زمانی که به دستور دادگاه یا نهاد ذی‌صلاح برای حذف یا مسدود کردن یک محتوای خاص عمل نکرده‌اند، نباید در قبال محتوای منتشر، ذخیره یا ارسال شده از طریق خدمات خود مسئول شناخته شوند.
- فارغ از موارد فوق، واسطه‌ها به هیچ وجه نباید در قبال محتوا مسئول باشند، مگر اینکه آن محتوا به نحوی به اطلاع آنها رسیده باشد که بتوان تصور کرد که واسطه به طور واقعی از غیرقانونی بودن آن محتوا اطلاع دارد.
- الزام به نظارت مستمر و مداوم بر محتوا با حق آزادی بیان مندرج در ماده ۱۰ کنوانسیون اروپایی حقوق بشر مغایر است.

موارد ارسالی در لینک زیر در دسترس هستند:

<https://www.mediadefence.org/sites/default/files/blog/files/20160407%20Tamiz%20v%20UK%20Inter%20Filing.pdf>

دلیل آن این بود که خدشه وارده به اعتبار او ناچیز بوده است. دادگاه حقوق بشر اروپا بر نقش مهم ارائه‌دهندگان خدمات اینترنتی در تسهیل دسترسی به اطلاعات و مباحثه در زمینه‌های مختلف حقوق سیاسی، اجتماعی و فرهنگی تأکید کرد و به نظر می‌رسید که با این استدلال موافق باشد که این ارائه‌دهندگان نباید ملزم به نظارت بر محتوا یا بررسی فعالیت‌های افتراآمیز احتمالی در سایت‌های خود باشند.

سایر دادگاه‌ها در رابطه با مسئولیت واسطه‌های اینترنتی مواضع قاطع‌تری اتخاذ کرده‌اند. به طور مثال، دادگاه عالی هند قانون داخلی را به گونه‌ای تفسیر کرده است که فقط در مواردی مسئولیت واسطه‌های اینترنتی را پیش‌بینی می‌کند که واسطه از طریق حکم دادگاه یا دولت از ارتکاب یکی از اعمال غیرقانونی مقرر در قانون آگاه شده و در حذف یا قطع دسترسی به چنین اطلاعاتی ناموفق بوده باشد.⁶⁵ همچنین، دادگاه عالی آرژانتین اعلام کرده است که موتورهای جستجو هیچ وظیفه‌ای برای نظارت بر قانونی بودن محتوای شخص ثالثی که به آنها لینک می‌دهند ندارند و تنها در موارد استثنایی که شامل "آسیب آشکار و فاحش" می‌شود، می‌توان واسطه‌ها را ملزم به حذف و غیرفعال کردن دسترسی نمود.⁶⁶ با توجه به نقش حیاتی واسطه‌های اینترنتی در ترویج، ارتقا و حمایت از حق آزادی بیان آنلاین، ضروری است که آنها در برابر هرگونه مداخله غیرموجه (چه از سوی دولت و چه از سوی عوامل و بازیگران خصوصی) که می‌تواند تأثیر مخربی بر این حق داشته باشد، محافظت شوند. به عنوان مثال، از آنجایی که توانایی و آزادی افراد در اعمال حق آزادی بیان آنلاین، به ماهیت منفعلانه واسطه‌های آنلاین وابسته است، هر رژیم حقوقی که موجب شود واسطه‌ها بر محتوای ارسال شده از طریق خدمات خود، محدودیت نابجا یا سانسور عمدی اعمال کنند، در نهایت تأثیر نامطلوبی بر حق آزادی بیان آنلاین خواهد داشت. گزارشگر ویژه سازمان ملل متحد تأکید کرده است که واسطه‌ها می‌توانند به عنوان سپری مهم در برابر نفوذ و مداخله دولت و اشخاص خصوصی عمل کنند، زیرا معمولاً برای مقابله با قطع اینترنت مناسب‌تر هستند.⁶⁷ با این حال این امر فقط زمانی می‌تواند تحقق یابد که واسطه‌ها بدون ترس از تحریم یا مجازات و هر گونه جریمه قادر به انجام این کار باشند.

نتیجه‌گیری

اگرچه حق دسترسی به اینترنت هنوز در مراحل توسعه است، اما یک ابزار حیاتی برای اعمال حق آزادی بیان است و مانند سایر حقوق بشری، تنها در صورت برآورده شدن یک آزمون سه بخشی، می‌توان آن را به طور موجه محدود کرد. همچنین، محدودیت‌های اعمال شده بر دسترسی به اینترنت ممکن است به طور نامتناسبی بر آزادی بیان و حقوق مرتبط با آن تأثیر بگذارد. در دنیای دیجیتالی که به سرعت در حال رشد و توسعه است، اینترنت به فضای مورد مناقشه‌ای تبدیل شده است که هم توسط کسانی که در پی دفاع از حقوق اساسی هستند و هم توسط افرادی که قصد محدود کردن آنها را دارند، استفاده می‌شود. درک صحیح مفاهیمی مانند قطع اینترنت، مسدود کردن و فیلترینگ محتوا، بی‌طرفی شبکه و مسئولیت واسطه‌های اینترنتی برای حمایت کامل و ارتقای حق آزادی بیان در فضای آنلاین، امری واجب و ضروری است.

۶۵- پرونده سینگال علیه اتحادیه هند، درخواست شماره 2012/167، بندهای ۱۱۲ تا ۱۱۸:

<https://www.livewlaw.in/summary-of-the-judgment-in-shreya-singhal-vs-union-of-india-read-the-judgment/>

۶۶- شکایت ماریا بلن رودریگز علیه گوگل، به شماره R.522.XLIX

http://www.stf.jus.br/repositorio/cms/portalStfInternacional/newsletterPortalInternacionalJurisprudencia/anexo/Fallo_R.522.XLIX_Corte_Suprema_da_Argentina_28_oct_2014.pdf

رأی این پرونده در گزارش سال ۲۰۱۶ گزارش ویژه سازمان ملل درباره آزادی بیان در بند ۵۲ توضیح داده شده است.

۶۷- گزارش سال ۲۰۱۷ گزارشگر ویژه سازمان ملل در مورد آزادی بیان، بند ۵۰.