ماژول ۴

حریم خصوصی و حفاظت از داده‌های افراد

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

MEDIA DEFENCE

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

فهرست مطالب

ماژول ۴

حریم خصوصی و حفاظت از داده‌های افراد

- **حریم خصوصی با افزایش جریان داده‌ها و نیاز همزمان به حفاظت از اطلاعات شخصی، اهمیت بیشتری پیدا کرده است.**
- **اگرچه جنوب و جنوب شرقی آسیا فاقد یک کنوانسیون منطقه‌ای اختصاصی در مورد حفاظت از داده‌ها هستند و چنین کنوانسیونی برای آسیا به طور کلی وجود ندارد، امکان پیوستن کشورهای غیر اروپایی به کنوانسیون ۱۰۸ شورای اروپا فراهم است.**
- **کشورها باید اطمینان حاصل نمایند که قوانین داخلی آنها استانداردهایی را برای پردازش قانونی اطلاعات شخصی تعیین می‌کنند و این قوانین را با تحولات و پیشرفت‌های حفاظت از داده‌ها همسو نگه می‌دارند.**
- **مفاهیم مرتبط با حریم خصوصی مانند "حق فراموش شدن"، رمزنگاری و محدودیت‌های نظارت دولتی با حفاظت از داده‌ها مرتبط است.**
- **به طور مشخص، افشای منابع خبری در نتیجه نظارت دولتی، تأثیر منفی بر آزادی بیان و آزادی خبرنگاران و روزنامه‌نگاران دارد.**

مقدمه

حق حفظ حریم خصوصی و نیاز همزمان به حفاظت از اطلاعات یا داده‌های شخصی، از آغاز عصر اطلاعات توجه قابل توجهی را به خود جلب کرده است. در حالی که اینترنت و به اشتراک‌گذاری آنلاین اطلاعات و جمع‌آوری داده‌ها به با سرعت فزآینده‌ای افزایش می‌یابد، تحولات قانونی نتوانسته‌اند به همان سرعت پیش رفته و به طور کافی از اطلاعات شخصی حفاظت کنند. با این حال، برخی از کشورها به منظور محافظت از حق حریم خصوصی شهروندان خود، شروع به اتخاذ ابزارها و مقررات مربوط به حفاظت از داده‌ها کرده‌اند.

این ماژول بر حفاظت از داده در آسیا و مفاهیم مرتبط با آن مانند "حق فراموش شدن یا حذف داده‌ها از اینترنت"، رمزنگاری و نظارت متمرکز است.

حق حفظ حریم خصوصی

این موضوع به رسمیت شناخته شده است که حق حفظ حریم خصوصی، به خودی خود و در تسهیل حق آزادی بیان نقش حیاتی ایفا می‌کند. به عنوان مثال، حفاظت از حق حریم خصوصی به افراد امکان می‌دهد تا در شرایطی که ممکن است به دلیل بیان نظرات و دیدگاه‌های خود محکوم و سرزنش شوند، بتوانند به صورت ناشناس آنها را به اشتراک بگذارند. همچنین این حق به افشاگران اجازه می‌دهد تا افشاگری‌های محافظت‌شده انجام دهند و به اعضای رسانه و فعالان این امکان را می‌دهد تا به طور ایمن ارتباطات محرمانه‌ای را فراتر از دسترسی نظارت دولتی برقرار کنند.

حق حفظ حریم خصوصی در ماده ۱۲ اعلامیه جهانی حقوق بشر (UDHR) تضمین شده است. حق حفظ حریم خصوصی همچنین در ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (ICCPR) نیز تضمین شده است که مقرر می‌دارد:

> "(۱) هیچ کس نباید مورد مداخله خودسرانه یا غیرقانونی در حریم خصوصی، خانواده، منزل یا مکاتبات خود قرار گیرد و یا آبرو و حیثیت او مورد تعرض غیرقانونی واقع شود.

(۲) هر کس حق دارد در برابر چنین تعرض و مداخلاتی از حمایت قانون برخوردار شود."
در سال ۲۰۱۲، کشورهای عضو اتحادیه کشورهای جنوب شرقی آسیا موسوم به آ سه آن (ASEAN) با صدور بیانیه‌ای غیرالزام‌آور بر تعهد خود به رعایت و ارتقای حقوق بشر تأکید کردند. ماده ۲۱ اعلامیه حقوق بشر کشورهای عضو اتحادیه کشورهای جنوب شرقی آسیا به طور دقیق حفظ حریم خصوصی در اعلامیه جهانی حقوق بشر را منعکس می‌کند و مقرر می‌دارد که:

"هر شخصی حق دارد از مداخله خودسرانه در حریم خصوصی، خانواده، منزل یا مکاتبات خود، از جمله اطلاعات شخصی، یا تعرض به آبرو و اعتبار شخصی مصون باشد. هر شخصی حق دارد در برابر این تعارض و مداخله‌ها تحت حمایت قانون قرار گیرد."

شایان ذکر است که در سال ۲۰۱۷، دادگاه عالی هند اعلام کرد که حق حریم خصوصی به عنوان بخشی ذاتی از حق زندگی وآزادی شخصی وهمچنین به عنوان بخشی از آزادی‌های بنیادین تضمین شده در بخش سوم قانون اساسی هند حفظ می‌شود. [1] بنابراین، اگرچه قانون اساسی هند صراحتاً شامل حق حفظ حریم خصوصی نیست، با این حال این حق را می‌توان از سایر حقوق وآزادی‌های تضمین شده بر اساس قانون اساسی استنتاج کرد.
همانند حق آزادی بیان، محدودیت در حق حفظ حریم خصوصی باید با آزمون سه‌بخشی برای چنین محدودیت‌هایی مطابقت داشته باشد. همانطور که دیوان عالی هند در حکم صادره در سال ۲۰۱۷ تصریح کرده است:

"حق حفظ حریم خصوصی نمی‌تواند بدون وجود قانونی عادلانه، منصفانه و معقول نقض شود. این محدودیت باید معیار تناسب را برآورده کند، یعنی (۱) باید قانون وجود داشته باشد، (۲) باید در خدمت هدف مشروع دولت باشد و (۳) باید متناسب باشد".[2]

همانطور که در ادامه آمده است، جنبه‌های خاصی از حق حریم خصوصی و تأثیری که اینترنت بر بهره‌مندی از این حق داشته است، مدنظر قرار گرفته است.

حفاظت از داده‌ها و اطلاعات

قوانین حفاظت از داده‌ها با هدف حفظ و حفاظت از پردازش اطلاعات شخصی یا داده‌های شخصی هستند که در مقررات عمومی حفاظت از داده اتحادیه اروپا تحت عنوان "هر گونه اطلاعات مربوط به یک شخص حقیقی شناسایی شده یا قابل شناسایی ('موضوع داده‌ها')" تعریف شده است.[3] یک "شخص حقیقی قابل شناسایی" به نوبه خود به این صورت تعریف می شود:

شخصی که به طور مستقیم یا غیرمستقیم قابل شناسایی باشد، به ویژه با استناد به اطلاعات شناسنامه‌ای مانند نام، شماره شناسایی، داده‌های مکانی، شناسه آنلاین یا با ارجاع به یک یا چند عامل خاص شامل عوامل فیزیکی، فیزیولوژیکی، ژنتیکی، ذهنی، اقتصادی، فرهنگی یا اجتماعی آن شخص حقیقی.

حفاظت از داده‌ها یکی از اقدامات اولیه است که از طریق آن حق حفظ حریم خصوصی تحقق می‌یابد. قوانین حفاظت از داده، علاوه بر تحقق حق حفظ حریم خصوصی، نقش کلیدی در تسهیل تجارت میان

۱- حکم قاضی کی.اس. پوتاسامی و قضات دادگاه عالی هند علیه اتحادیه هند و دیگران، دادخواست شماره 2012/494، ۲۴ آگوست ۲۰۱۷:
http://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf

۲- همان، پاراگراف ۲۳۲ (بند ۶).

۳- مقررات پارلمان اروپا 2016/679 (EU) و شورای اروپا مصوب مورخ ۲۷ آوریل ۲۰۱۶ در مورد حمایت از اشخاص حقیقی با توجه به پردازش داده‌های شخصی و در مورد انتشار آزادانه این داده‌ها و لغو دستورالعمل EC/46/95 ، ماده ۴ (بند ۱):
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

کشورها ایفا می‌کنند، زیرا بسیاری از قوانین حفاظت از داده، به ویژه قوانین اتخاذ شده در داخل اتحادیه اروپا، انتقال فرامرزی داده‌ها را در شرایطی که یک کشور سطح مناسبی از حفاظت از داده را ارائه نمی‌دهد، محدود می‌کنند.
در سال‌های اخیر، توجه روزافزون به موضوع حفاظت از داده منجر به تصویب قوانین جدید حفظ حریم خصوصی در برخی کشورهای آسیایی شده است.[4] از زمان شروع همه‌گیری COVID-19، وابستگی بیشتر به فناوری‌های دیجیتال برای کار از راه دور و ردیابی تماس‌ها، چالش‌های جدیدی را در زمینه حریم خصوصی و حفاظت از داده‌های افراد ایجاد کرده است که منجر شده است الزام تقویت قوانین حفاظت از داده‌ها شتاب و فوریت بیشتری داشته باشد. با این حال، بسیاری از کشورها همچنان به طور ناکافی از حریم خصوصی افراد محافظت می‌کنند، به ویژه در برابر فعالیت‌های نظارتی دولت.[5]

در رابطه با حفاظت از داده‌ها، نظر عمومی شماره ۱۶ در مورد ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (نظر عمومی شماره ۱۶) به شرح زیر است:[6]

> **"جمع‌آوری و نگهداری اطلاعات شخصی در رایانه‌ها، بانک‌های اطلاعاتی و سایر دستگاه، چه توسط مقامات دولتی و چه توسط افراد یا نهادهای خصوصی، باید توسط قانون تنظیم شود. دولت‌ها باید تدابیر مؤثری اتخاذ نمایند تا اطمینان حاصل کنند که اطلاعات مربوط به زندگی خصوصی فرد به دست افرادی نرسد که به موجب قانون مجاز به دریافت، پردازش و استفاده از آن نیستند، و هرگز برای اهداف ناسازگار با میثاق استفاده نمی‌شود. هر فردی به منظور حفاظت حداکثری از زندگی خصوصی خود، باید حق داشته باشد که به صورت معین بداند چه داده‌های شخصی در پرونده‌های داده‌های خودکار ذخیره شده است و برای چه اهدافی ذخیره می‌شود. همچنین هر فردی باید بتواند بفهمد که چه مقامات دولتی یا اشخاص یا نهادهای خصوصی پرونده آنها را کنترل می‌کنند یا ممکن است بر پرونده‌های آنها کنترل داشته باشند. اگر این پرونده‌ها حاوی اطلاعات شخصی نادرست باشند یا برخلاف مقررات قانونی جمع‌آوری یا پردازش شده باشند، هر فردی باید حق درخواست اصلاح یا حذف آنها را داشته باشد."**

جامع‌ترین قوانین حفاظت از داده‌ها، معمولاً اصول زیر را پیش‌بینی می‌کنند:[7]

- **اطلاعات شخصی باید به صورت منصفانه و قانونی پردازش شود و تا زمانی که شرایط مقرر رعایت نشده باشد، نباید پردازش شود..**
- **اطلاعات شخصی باید برای یک هدف (یا اهداف) مشخص به دست آمده باشد و نباید به طریقی که با آن هدف ناسازگار است پردازش شود.**
- **داده‌های شخصی باید کافی، مرتبط و غیر مفرط در ارتباط با هدف (یا اهداف) پردازش باشد.**
- **اطلاعات شخصی باید دقیق باشند و در صورت لزوم به روز نگه داشته شوند.**
- **اطلاعات شخصی نباید بیشتر از آنچه برای جمع‌آوری لازم است، نگهداری شوند.**

۴- برای مرور روندهای منطقه‌ای، مراجعه شود به "راهنمای حریم خصوصی آسیا-اقیانوسیه ۲۰۲۰-۲۰۱۰: قوی‌تر با هم:" (۲۰۲۰) دلویت:
https://www2.deloitte.com/ph/en/pages/risk/articles/asia-pacific-privacy-guide.html
و گراهام گرین لیف، "پیشرفت‌ها در قوانین حریم خصوصی داده‌ها در جنوب آسیا: سریلانکا، پاکستان و نپال" (۲۰۱۹)، قوانین حریم خصوصی و گزارش بین المللی تجارت، صص ۲۲-۲۵:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3549055

۵- دسترسی دیجیتال، "حقوق دیجیتال در آسیای جنوب شرقی، ۲۰۲۱/۲۰۲۲"، (۲۰۲۲):
https://digitalreach.asia/event/report-launch-digital-rights-in-southeast-asia-2021-2022/
اسمیتا کریشنا پراساد و شارنگان آراویندکشان (۲۰۲۱)، "رژیم‌های حریم خصوصی در جنوب آسیا"، مجله بین‌المللی حقوق بشر، جلد ۲۵، شماره ۱، صفحات ۷۹ الی ۱۱۶، ص ۱۰۵:
https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1773442

۶- نظر عمومی شماره ۱۶، بند ۱۰.

۷- دفتر کمیسر اطلاعات، "اصول حفاظت از داده‌ها":
https://ico.org.uk/for-organisations/guide-to-data-protection/data-protection-principles/

- **اطلاعات شخصی باید مطابق با حقوق موضوع داده‌ها که در قانون حفاظت از داده ها پیش بینی شده است پردازش شوند، از جمله حق دسترسی، بازبینی و در صورت لزوم اصلاح داده‌ها.**
- **برای جلوگیری از پردازش غیرمجاز یا غیرقانونی داده‌های شخصی و همچنین جلوگیری از ازدست رفتن تصادفی، نابودی یا آسیب به داده‌های شخصی باید تدابیر فنی و سازمانی مناسب اتخاذ شود.**
- **داده‌های شخصی نباید به کشور دیگری منتقل شود که سطح مناسبی از حمایت از حقوق و آزادی‌های افراد موضوع داده را در رابطه با پردازش اطلاعات شخصی تضمین نمی‌کند.**

کنوانسیون شورای اروپا برای حمایت از افراد در قبال پردازش خودکار اطلاعات و داده‌های شخصی ('کنوانسیون ۱۰۸')[8] در ۲۸ ژانویه ۱۹۸۱ جهت امضا و تصویب گشایش یافت و اولین سند بین‌المللی الزام‌آور برای محافظت در برابر سوءاستفاده‌های ناشی از جمع‌آوری و پردازش داده‌های شخصی بود. هدف کنوانسیون ۱۰۸ "حفاظت از هر فرد، بدون توجه به ملیت یا محل اقامت وی، در رابطه با پردازش داده‌های شخصی وی، و در نتیجه کمک به احترام به حقوق بشر و آزادی‌های بنیادین وی، به ویژه حق حفظ حریم خصوصی" است.[9] کنوانسیون ۱۰۸، گردش آزاد اطلاعات و داده‌های شخصی بین کشورهای عضو کنوانسیون را فراهم می‌کند

امکان پیوستن و الحاق کشورهای غیر عضو شورای اروپا به کنوانسیون ۱۰۸ نیز فراهم است. اگرچه تعدادی از کشورهای غیر اروپایی به آن پیوسته‌اند، اما هیچ کدام از کشورهای جنوب و جنوب شرقی آسیا هنوز چنین کاری را انجام نداده است.

قوانین حفاظت از داده‌ها، علاوه بر تحقق حق حریم خصوصی، معمولاً حق دسترسی به اطلاعات شخصی را نیز تسهیل می‌کنند. در این راستا، بیشتر قوانین حفاظت از داده‌ها، اطلاعاتی که یک کنترل‌کننده در مورد آنها نگهداری می‌کند را درخواست کرده و به آنها اجازه دسترسی داده می‌شود. این مکانیزم می‌تواند این امکان را فراهم نماید تا افراد مشخص کنند که آیا اطلاعات شخصی آنها مطابق با قوانین مربوط به حفاظت از داده پردازش می‌شود، از جمله اینکه آیا اطلاعات نگهداری شده صحیح است و آیا حقوق آنها واقعاً رعایت می‌شود.

حق فراموش شدن یا حذف داده‌ها

آنچه که به عنوان "حق فراموش شدن" شناخته می‌شود (که شاید بهتر است به عنوان "حق پاک کردن داده‌ها" یا "حق حذف از فهرست" توصیف شود)، به حق افراد برای درخواست از موتورهای جستجوی تجاری مانند گوگل برای حذف لینک‌های منتهی به اطلاعات شخصی خود اشاره دارد. این حق، از مفهوم حق زندگی خصوصی نشأت می‌گیرد که شامل حق عدم پروفایل‌سازی برجسته اطلاعات گذشته فرد در نتایج جستجو است، حتی اگر آن اطلاعات همچنان در وب‌سایت‌های مربوطه موجود باشد. این حق به آن معنا است که افراد می‌توانند درخواست کنند اطلاعات شخصی گذشته یا بی‌اهمیت در مورد آنها در نتایج جستجوی موتورهای جستجو حذف شود، مگر اینکه وجود آن اطلاعات برای منافع عمومی ضروری باشد.

پرونده اصلی در این مورد که به آن رسیدگی شده است، مربوط به حکم دیوان دادگستری اتحادیه اروپا (CJEU) در خصوص پرونده نمایندگی گوگل اسپانیا علیه گونزالس در سال ۲۰۱۴ است.[10] در این پرونده، آقای گونزالس، شهروند اسپانیایی، در سال ۲۰۱۰ شکایت خود را به سازمان تنظیم کننده

۸- دسترسی به کنواسیون شماره ۱۰۸ در لینک زیر:
https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

۹- ماده ۱ کنوانسیون ۱۰۸.

۱۰- پرونده شکایت "Google Spain SL و شرکتی دیگر علیه آژانس حفاظت از اطلاعات شخصی اسپانیا (AEPD) و یک شرکت دیگر" با شماره پرونده C-131/12، مورخ ۱۳ ماه می ۲۰۱۴ که توسط دیوان دادگستری اتحادیه اروپا رسیدگی و رأی آن صادر شده است:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

اطلاعات اسپانیا تقدیم کرد. علت شکایت آقای گونزالس این بود که هنگامی که کاربران اینترنتی نام او را در موتور جستجوی گوگل جستجو می‌کردند، به لینک‌هایی از یک روزنامه اسپانیایی در سال ۱۹۹۸ مربوط به پرونده‌های ضمیمه علیه وی برای بازپرداخت برخی بدهی‌ها دسترسی پیدا می‌کردند. آقای گونزالس درخواست کرد که این اطلاعات شخصی مربوط به او حذف یا پنهان شود، زیرا روند رسیدگی به پرونده او به طور کامل حل و فصل شده بود و بنابراین ارجاع به او و ذکر نام او در این زمینه به او لطمه می‌زد.

دیوان دادگستری اتحادیه اروپا، با تکیه بر قانون حفاظت از داده‌های شخصی اتحادیه اروپا که در آن زمان در حال اجرا بود، درخواست آقای گونزالس را تأیید کرد و بر اساس این قانون در آن زمان اقدام کرد. دیوان دادگستری اتحادیه اروپا خاطرنشان کرد که صرف نمایش اطلاعات شخصی در صفحات نتایج جستجو، به منزله پردازش چنین اطلاعاتی محسوب می‌شود[11] و دلیلی ندارد که موتورهای جستجو از الزامات و تضمین‌های قانونی مربوطه مستثنی باشند.[12] همچنین اذعان شد که پردازش اطلاعات شخصی توسط موتورهای جستجو می‌تواند به طور قابل توجهی به حقوق اساسی حریم خصوصی و حفاظت از اطلاعات شخصی آسیب برساند، زیرا امکان دسترسی کاربران اینترنتی به اطلاعات مربوط به افراد و ایجاد پروفایل آنها را فراهم می‌کند.[13] مطابق با نظر دیوان دادگستری اتحادیه اروپا، تأثیر این مداخله به ویژه به دلیل نقش مهم اینترنت و موتورهای جستجو در جامعه مدرن که سبب فراگیری چنین اطلاعاتی می‌شود، افزایش می‌یابد.[14]

دیوان دادگستری اتحادیه اروپا در رابطه با حذف اطلاعات از فهرست، اذعان داشت که حذف لینک‌ها از فهرست نتایج جستجو می‌تواندبر منافع بالقوه مشروع کاربران اینترنتی برای دسترسی به آن اطلاعات و بخشی از حق آزادی بیان آنها تأثیر منفی بگذارد.[15] بنابراین، باید تعادل عادلانه‌ای بین این منافع و منافع صاحب داده‌ها برقرار شود. در این راستا، باید به ماهیت اطلاعات، حساسیت آن برای زندگی خصوصی صاحب داده‌ها و همچنین منافع عمومی برای دسترسی به این اطلاعات که بر اساس نقش صاحب داده‌ها در زندگی عمومی متفاوت است، توجه کرد.[16]

دیوان دادگستری اتحادیه اروپا در ادامه اظهار داشت که در صورتی که با توجه به تمام جوانب و شرایط، اطلاعات فرد برای اهداف پردازش توسط اپراتور موتور جستجو نامناسب واز اساس غیرمرتبط باشد یا دیگرمرتبط نباشد، یا فراتر از اهداف پردازش داده باشد، و با در نظر گرفتن منافع عمومی برای دسترسی به آن اطلاعات، صاحب داده‌ها مجاز است درخواست کند اطلاعات مربوط به وی دیگر در فهرست نتایج جستجو ظاهر نشود.[17] در چنین مواردی، این اطلاعات باید از نتایج موتورهای جستجو حذف شوند.[18]

حق فراموش شدن یا حق حذف اطلاعات شخصی، همچنین در سطح داخلی نیز به رسمیت شناخته شده است. به عنوان مثال، دیوان عالی کشور ایتالیا اعلام کرده است که پس از گذشت دو و نیم سال، منافع عمومی در مورد یک مقاله کاهش می‌یابد و اطلاعات خصوصی حساس نباید به طور نامحدود در دسترس عموم باشد.[19] این پرونده به دادگاه اروپایی حقوق بشر ارجاع شد، که محدودیت اعمال‌شده بر آزادی بیان را پس از خودداری از مداخله در توازن بین این حق و حق احترام به زندگی خصوصی

---

[11] همان، پاراگراف ۵۷.

[12] همان، پاراگراف ۵۸.

[13] همان، پاراگراف ۸۰.

[14] همان

[15] همان، پاراگراف ۸۱.

[16] همان.

[17] همان، پاراگراف ۹۴.

[18] همان، پاراگراف ۹۴.

[19] شکایت PrimaDaNoi علیه X، پرونده شماره 13161، ۲۲ نوامبر ۲۰۱۵: https://globalfreedomofexpression.columbia.edu

توسط دادگاه عالی تجدیدنظر ایتالیا قابل توجیه دانست.[20] همچنین دیوان عالی دادگاه تجدیدنظر بلژیک نیز حق فراموش شدن را به رسمیت شناخته است.[21]

با این حال، حق فراموش شدن یا حذف اطلاعات شخصی محدودیت‌هایی نیز دارد. در سال ۲۰۱۷، دیوان دادگستری اتحادیه اروپا با درخواست صدور رأی اولیه در پرونده "اتاق بازرگانی، صنعت، حرفه و کشاورزی لچه در برابر سالواتوره مانی" مواجه شد.[22] آقای مانی، با استناد به رأی پرونده گونزالس، خواستار صدور دستوری بود که اتاق بازرگانی را ملزم به حذف، ناشناس کردن یا مسدودسازی هرگونه اطلاعات مربوط به او در ثبت شرکت‌هایی کرد که با انحلال شرکتش مرتبط بود. اما دیوان دادگستری این درخواست آقای مانی را رد کرد و اعلام کرد که با توجه به گستره استفاده‌های مشروع احتمالی از داده‌ها در ثبت شرکت‌ها و دوره‌های زمانی متفاوت محدودیت قابل اعمال برای چنین سوابقی، امکان تعیین یک دوره حفظ و نگهداری مناسب وجود ندارد. بنابراین، دیوان بر این اساس نتیجه گرفت که حق عمومی برای فراموش شدن اطلاعات در رابطه با ثبت شرکت‌ها وجود ندارد.

وهمچنین، سایر نظام های قضایی نیز حق فراموش شدن در برابر موتورهای جستجو را به رسمیت نشناخته اند و از حمایت از حق فراموشی در مقابل موتورهای جستجو خودداری کرده‌اند. به عنوان مثال، در برزیل حکم شده بود که موتورهای جستجو را نمی‌توان مجبور به حذف نتایج جستجوی مربوط به یک عبارت یا اصطلاح خاص نمود.[23] همچنین دادگاه عالی ژاپن نیز از اجرای حق فراموش شدن در برابر گوگل خودداری کرده و بیان کرده است که حذف اطلاعات تنها زمانی مجاز است که ارزش حفاظت از حریم خصوصی به طور قابل توجهی بیشتر از ارزش افشای اطلاعات باشد.[24]

در هند، قانون مربوط به حق فراموش شدن همچنان مشخص و معین نیست و حل نشده باقی مانده است. برخی از تصمیمات قضایی، حق فراموش شدن را به عنوان یک نتیجه منطقی از حق حریم خصوصی به رسمیت شناخته‌اند. به عنوان مثال، دادگاه عالی ایالت اوریسا[25] و همچنین دادگاه عالی ایالت کرالا[26] هر دو به این اجماع رسیدند که افراد متأثر از خشونت جنسی حق دارند بخواهند تا برخی از اطلاعات آنلاین شامل تصاویر و ویدئوهای بدون رضایت آنها حذف شوند. در سال ۲۰۲۱، دادگاه عالی دهلی نیز دستور داد نتایج جستجوی مرتبط با حکمی که در اینترنت منتشر شده بود و در آن متقاضی تبرئه شده

---

[20] دادخواست شماره 77419/16، (۲۰۲۲)، ص ۶۹ و ۷۰: https://hudoc.echr.coe.int/eng#{%22fulltext

[21] پرونده پی.اچ علیه اُ.جی، شماره پرونده F/0052/15، ۲۹ آوریل ۲۰۱۶: https://www.huntonprivacyblog.com/wp-content
برای بحث در مورد این پرونده، به "قوانین دادگاه کیفری بلژیک در مورد حق فراموش شدن"، هانتون و ویلیامز، ۱ ژوئن ۲۰۱۶ مراجعه کنید:
https://www.huntonprivacyblog.com/2016/06/01/belgian-court-of-cassation-rules-on-right-to-be-forgotten/

برای اطلاعات بیشتر در مورد حق فراموش شدن، به شکایت NT1 و NT2 علیه Google LLC در بریتانیا (۲۰۱۸) مراجعه کنید:
https://www.judiciary.uk/wp-content/uploads/2018/04/nt1-nt2-v-google-press-summary-180413.pdf

[22] پرونده شماره C-385-15، ۹ مارس ۲۰۱۷: https://curia.europa.eu/juris/document/document...

[23] پرونده Ministra Nancy Andrighi علیه Google Brasil Internet Ltda و سایرین، شماره 6-0307909/2011، ۲۶ ژوئن ۲۰۱۲:
https://www.internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1316921.pdf

[24] ژاپن تایمز، "دادگاه عالی درخواست 'حق فراموش شدن' را رد کرد"، ۱ فوریه ۲۰۱۷:
https://www.japantimes.co.jp/news/2017/02/01/national/crime-legal/top-court-rejects-right-forgotten-demand/#.WqZQXehubIV

[25] *شکایت Subhranshu Rout علیه ایالت اودیسا، دادگاه عالی اوریسا، شماره 4592، (۲۰۲۰):*
https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2021/01/Official-Judgment.pdf

[26] پرونده حق فراموش شدن افراد متأثر از تجاوز جنسی، دادگاه عالی کرالا در دادخواست شماره 9478 در سال ۲۰۱۶ (۲۰۱۷)، که به دلیل در دسترس نبودن حکم اصلی، توسط انجمن آزادی بیان کلمبیا خلاصه شده است:
https://globalfreedomofexpression.columbia.edu/cases/the-case-of-the-rape-survivors-right-to-be-forgotten-india/

بود، مسدود گردد.[27] با این حال، در سال ۲۰۱۷، دادگاه عالی گجرات درخواست مشابهی برای حذف یک حکم را رد کرد.[28] تا آن زمان، هند هنوز چارچوب قانونی جامعی در زمینه حق فراموش شدن نداشت، اگرچه لایحه پیشنهادی در قالب لایحه حفاظت از داده‌های شخصی که اولین بار در سال ۲۰۱۹ معرفی شد، شامل مقرراتی است که این حق را نیز دربر می‌گیرد.[29]
طبق اصول جهانی آزادی بیان و حفظ حریم خصوصی "ماده 19" (اصول جهانی)، [30] حق فراموش شدن (تا حدی که در یک حوزه قضایی خاص به رسمیت شناخته شود)، باید محدود به "حق افراد برای درخواست از موتورهای جستجو برای حذف نتایج جستجوی نادرست یا منسوخ‌شده بر اساس جستجوی نام خود" باشد. [31] همچنین این اصول بیان می‌کنند که درخواست‌های حذف لینک باید "موضوع حکم نهایی دادگاه یا نهاد قضایی مستقل و ذی‌صلاح در زمینه آزادی بیان و قوانین حفاظت از داده‌ها باشد".[32]

رمزنگاری و ناشناس ماندن در اینترنت

رمزنگاری به فرآیند خودکار تبدیل پیام‌ها، اطلاعات یا داده‌ها به فرمی غیرقابل خواندن برای هر کسی به جز گیرنده مورد نظر اشاره دارد و با انجام این کار از محرمانه ماندن و یکپارچگی محتوا در برابر دسترسی یا دستکاری شخص ثالث محافظت می‌شود.[33] با استفاده از "رمزگذاری کلید عمومی" (شکل غالب رمزگذاری سرتاسری داده‌های درحال انتقال)، فرستنده از کد یا کلید عمومی گیرنده برای رمزنگاری اطلاعات استفاده می‌کند و گیرنده از کلید خصوصی خود برای رمزگشایی آن استفاده می‌کند. [34] همچنین رمزگذاری داده‌های ذخیره شده در دستگاه‌های شخصی فرد مانند لپ‌تاپ یا تلفن همراه نیز امکان‌پذیر است.[35]

ناشناس ماندن را می‌توان به عنوان اقدام یا برقراری ارتباط بدون استفاده یا ارائه نام یا هویت خود؛ و یا به عنوان اقدام یا برقراری ارتباط به گونه‌ای تعریف کرد که امکان تعیین نام یا شناسایی هویت فرد را غیرممکن می‌کند، یا استفاده از اسم مستعار یا هر اسم دیگری که با هویت قانونی یا رسمی فرد مرتبط نیست.[36] ناشناس ماندن را می‌توان از شبه‌ناشناس بودن متمایز کرد؛ یعنی ناشناسی به معنای عدم استفاده

---

[27] پرونده شکایت جوراوار سینگ موندی علیه اتحادیه هند و سایرین، شماره پرونده W.P. (C) 3918/ 2020، ۲۰۲۱
https://www.livelaw.in/pdf_upload/161836477429202l-393948.pdf

[28] *پرونده Dharamraj Bhanushankar Dave علیه ایالت گجرات، درخواست مدنی ویژه شماره 1854 در سال ۲۰۱۵ (۲۰۱۷):*
https://indiankanoon.org/doc/156866860/

[29] "لایحه حفاظت از داده‌های شخصی و حق فراموش شدن"، ipleaders، اراچیت گار (۲۰۲۲):
https://blog.ipleaders.in/personal-data-protection-bill-2019-and-the-right-to-be-forgotten/

[30] اصول جهانی توسط جامعه مدنی به رهبری سازمان ماده ۱۹ و با همکاری کارشناسان سطح بالا از سراسر جهان تدوین شده است:
https://www.article19.org/data/files/medialibrary/38657/Expression-and-Privacy-Principles-1.pdf

[31] اصول جهانی، اصل ۱۸ (بند ۱)

[32] همان، اصل ۱۸ (بند ۲).

[33] گزارش گزارشگر ویژه سازمان ملل در مورد آزادی بیان، "گزارش در مورد ناشناس بودن، رمزگذاری و چارچوب حقوق بشر"، A/HRC/29/32، مورخ ۲۲ مه ۲۰۱۵، پاراگراف ۷:
http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx
برای بحث و اطلاعات بیشتر، مراجعه شود به کلینیک بین‌المللی عدالت دانشگاه کالیفرنیا، مرجع منتخب: "گزارش همراه غیررسمی به گزارش گزارشگر ویژه سازمان ملل (گزارش A/HRC/29/32) در مورد رمزگذاری، ناشناسی و آزادی بیان":
http://www.ohchr.org/Documents/Issues/Opinion/Communications/Selected_References_SR_Report.pdf

[34] همان.

[35] همان.

[36] بنیاد مرز الکترونیک، ناشناس بودن و رمزگذاری، ۱۰ فوریه ۲۰۱۶، صفحه ۳:
https://www.ohchr.org/Documents/Issues/Opinion/Communications/EFF.pdf

از هیچ نامی است، در حالی که شبه‌ناشناسی به استفاده از نام مستعار اشاره دارد.[37] در این مورد نیز معمولاً هویت فرد به کاربران منتخب افشا می‌شود.

رمزگذاری و ناشناس بودن ابزارهای ضروری برای بهره‌مندی کامل از حقوق دیجیتال هستند و به دلیل نقش حیاتی آنها در تضمین حق آزادی بیان و حریم خصوصی، از حمایت و محافظت برخوردار هستند. همانطور که گزارشگر ویژه سازمان ملل متحد درباره آزادی بیان تصریح کرده است:[38]

> **"رمزگذاری و ناشناس ماندن، چه به صورت جداگانه یا همراه با هم، محدوده‌ای از حریم خصوصی را برای حفاظت از عقیده و باور ایجاد می‌کنند. به عنوان مثال، ارتباطات خصوصی را میسر کرده و می‌توانند عقاید را در برابر نظارت خارجی حفظ کنند که در محیط‌های متخاصم سیاسی، اجتماعی، مذهبی و قانونی، امری بسیار مهم و ضروری است. در مواردی که دولت ها سانسور غیرقانونی را از طریق فیلترینگ و سایر فناوری‌ها اعمال می‌کنند، استفاده از رمزگذاری و ناشناس بودن به افراد امکان می‌دهد موانع و فیلترینگ را دور بزنند و بدون مداخله مقامات به اطلاعات و ایده‌ها دسترسی داشته باشند. روزنامه نگاران، محققان، وکلا و جامعه مدنی برای محافظت از خود (و منابع، مشتریان و شرکای خود) در برابر نظارت و آزار و اذیت، بر رمزگذاری و ناشناس بودن تکیه می‌کنند. توانایی جستجو در وب، توسعه ایده‌ها و برقراری ارتباط امن ممکن است تنها راهی باشد که بسیاری از افراد از طریق آن بتوانند جنبه‌های اساسی هویتی خود مانند جنسیت، مذهب، قومیت، مبدأ ملی یا نژاد را کشف و کاوش کنند. هنرمندان نیز برای حفظ و محافظت از حق بیان خود به رمزگذاری و ناشناس بودن تکیه می کنند، به ویژه در شرایطی که نه تنها دولت محدودیت ایجاد می‌کند، بلکه جامعه نیز عقاید یا دیدگاه‌های غیرمتعارف را تحمل نمی‌کند."**

رمزگذاری و ناشناس ماندن، به ویژه برای توسعه و به اشتراک‌گذاری عقاید و ابراز نظرات در فضای آنلاین مفید هستند، به خصوص در شرایطی که افراد نگران باشند ارتباطات آنها در معرض تداخل یا حمله عوامل دولتی یا غیردولتی قرار گیرد. بنابراین، این فناوری‌ها ابزارهای خاصی هستند که افراد می‌توانند از طریق آنها از حقوق خود بهره‌مند شوند. بر همین اساس، اعمال هر گونه محدودیت بر رمزگذاری و ناشناس بودن باید با آزمون سه‌بخشی (قانونی‌بودن، ضرورت و تناسب) مطابقت داشته باشد.

طبق اظهارات گزارشگر ویژه سازمان ملل متحد درباره آزادی بیان، در حالی که رمزگذاری و ناشناس ماندن ممکن است موجب ناکامی مقامات اجرای قانون و مبارزه با تروریسم و پیچیده‌سازی نظارت شود، مقامات دولتی به طور کلی در ارائه توجیهات عمومی مناسب برای پشتیبانی از محدودیت‌های استفاده از آنها یا شناسایی مواردی که چنین محدودیت‌هایی برای دستیابی به هدف مشروع ضروری است، شکست خورده‌اند.[39] ممنوعیت‌های صریح و کامل استفاده فردی از فناوری رمزگذاری به طور نامتناسب حق آزادی بیان را محدود می‌کند، زیرا همه کاربران آنلاین در یک حوزه قضایی خاص را از حق استفاده از این ابزارها برای ایجاد فضایی برای ابراز عقیده و بیان، صرف نظر از اینکه آیا برای اهداف غیرقانونی استفاده می‌شوند یا خیر، محروم می‌کند.[40] به همین ترتیب، تنظیم مقررات دولتی در مورد رمزگذاری می‌تواند به منزله ممنوعیت باشد، به عنوان مثال از طریق الزام به دریافت مجوز برای استفاده از رمزگذاری، تعیین استانداردهای فنی ضعیف برای رمزگذاری یا کنترل واردات و صادرات ابزارهای رمزگزارشگر ویژه سازمان ملل متحد درباره آزادی بیان از دولت‌ها خواسته است که رمزگذاری و ناشناس ماندن را ترویج کنند و تأکید کرده است که دستورات رمزگشایی تنها زمانی مجاز باشند که بر اساس قوانین شفاف و قابل دسترس برای عموم و صرفاً به صورت هدفمند و مورد به مورد برای افراد (نه گروه‌ها) اعمال شوند و مجاز و مشروط به حکم قضایی و حفاظت از حقوق قانونی افراد

---

[37] همان.

[38] گزارش گزارشگر ویژه سازمان ملل در مورد ناشناس بودن و رمزگذاری، پاراگراف ۱۲.

[39] همان، پاراگراف ۳۶.

[40] همان، پاراگراف ۴۰.

باشند. به این معنا که دسترسی به محتوای رمزگذاری‌شده افراد باید از طریق مراجع قضایی و مبتنی بر اصول حقوقی حاکم بر حق حریم خصوصی و آزادی بیان صورت گیرد.[41]

کنترل و نظارت دیجیتال توسط دولت

نظارت بر ارتباطات یا نظارت دیجیتال به کنترل وپایش، رهگیری، جمع‌آوری، دستیابی، تجزیه و تحلیل، استفاده، حفظ و نگهداری، دخل و تصرف، دسترسی یا اقدامات مشابه در رابطه با اطلاعات مربوط به مراودات گذشته، حال و آینده افراد اشاره دارد.[42] این نظارت هم شامل محتوای ارتباطات و هم فراداده‌های مربوط به آن مانند موقعیت مکانی و نقاط اتصال است. در خصوص فراداده‌ها یا ابرداده‌ها تصریح شده است که جمع‌آوری و تجمیع این اطلاعات می‌تواند بینش عمیقی در مورد رفتار، روابط اجتماعی، ترجیحات و اولویت‌های شخصی و هویت فرد ارائه دهد. به طور کلی، این امکان وجود دارد که از طریق این مجموعه اطلاعات، نتایج دقیقی در مورد زندگی خصوصی افراد استخراج شود.

نظر عمومی شماره ۱۶ کمیته حقوق بشر سازمان ملل متحد اظهار کرده است که: "رعایت ماده ۱۷ مستلزم تضمین یکپارچگی و محرمانگی مکاتبات به صورت رسمی و عملی است".[43] نظارت، چه به صورت جمع‌آوری انبوه (یا گسترده) داده‌ها [44] و چه جمع‌آوری هدفمند داده‌ها، به طور مستقیم با حریم خصوصی و امنیت لازم برای آزادی عقیده و بیان تداخل دارد و باید در قالب آزمون سه‌بخشی ارزیابی شود تا مشروعیت آن بررسی شود.[45] در عصر دیجیتال، فناوری‌های اطلاعات و ارتباطات ظرفیت دولت‌ها، شرکت‌ها و افراد را برای اجرای نظارت، شنود و جمع‌آوری داده‌ها افزایش داده است، به گونه‌ای که انجام چنین نظارتی دیگر محدود به مقیاس یا مدت زمان نیست.[46]

قطعنامه‌ای که توسط مجمع عمومی سازمان ملل در مورد حق حفظ حریم خصوصی در عصر دیجیتال به تصویب رسید، تأکید کرده است که نظارت غیرقانونی یا خودسرانه و یا شنود ارتباطات، و همچنین جمع‌آوری غیرقانونی یا خودسرانه اطلاعات و داده‌های شخصی، اقداماتی بسیار مداخله‌جویانه هستند که حق حریم خصوصی را نقض می‌کنند و می‌توانند در آزادی بیان مداخله کرده و با اصول یک جامعه

---

41 همان، پاراگراف ۵۹ و ۶۰.

42 ضرورت و تناسب: اصول بین‌المللی در مورد کاربرد حقوق بشر در نظارت بر ارتباطات (اصول ضرورت و تناسب)، ۲۰۱۴، ص ۴:
https://necessaryandproportionate.org/files/2016/03/04/en_principles_2014.pdf

43 نظر عمومی شماره ۱۶، پاراگراف ۸.

44 افشاگری‌های افرادی مانند ادوارد اسنودن نشان داده است که آژانس امنیت ملی ایالات متحده و ستاد ارتباطات عمومی انگلستان، فناوری‌هایی را توسعه داده‌اند که به آنها امکان دسترسی به حجم عظیمی از ترافیک اینترنتی جهانی، از جمله سوابق ایالات متحده، دفترچه‌های آدرس الکترونیکی افراد و حجم زیادی از فراداده‌های دیگر ارتباطات دیجیتالی را می‌دهد. این فناوری‌ها از طریق یک شبکه فرامرزی که شامل روابط استراتژیک اطلاعاتی بین دولت‌ها و سایر عوامل و بازیگران است، مورد استفاده قرار می‌گیرند. این موضوع به عنوان نظارت گسترده یا انبوه شناخته می‌شود. برای اطلاعات بیشتر در مورد نگرانی‌های مربوط به حریم خصوصی که در افشاگری‌های اسنودن مطرح شده است، به گزارش گزارشگر ویژه سازمان ملل درباره حق حریم خصوصی، سند سازمان ملل A/HRC/34/60 (۲۰۱۷) مراجعه کنید:
https://documents-dds-ny.un.org/doc/UNDOC/GEN/G17/260/54/PDF/G1726054.pdf?OpenElement

45 گزارش سال ۲۰۱۶ گزارشگر ویژه سازمان ملل در مورد آزادی بیان و چالش‌های معاصر آزادی بیان، سند سازمان ملل متحد به شماره A/71/373، پاراگراف ۲۰:
https://undocs.org/Home/Mobile?FinalSymbol=A%2F71%2F373&Language=E&DeviceType=Desktop&LangRequested=False

46 گزارش گزارشگر ویژه سازمان ملل در مورد ترویج و حمایت از حق آزادی نظر و بیان، فرانک لا رو، A/HRC/23/40، ۲۰۱۳:
https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

دموکراتیک مغایرت داشته باشند، به ویژه زمانی که در مقیاس گسترده انجام می‌شوند.[47] این قطعنامه همچنین تصریح کرده است که "نظارت بر ارتباطات دیجیتال باید منطبق با تعهدات بین‌المللی حقوق بشری باشد و باید بر اساس یک چارچوب قانونی صورت گیرد که باید برای عموم قابل دسترسی، شفاف، دقیق، جامع و بدون تبعیض باشد."[48]

برای تحقق شرایط قانونی، بسیاری از کشورها اقدام به اصلاح قوانین نظارتی خود کرده‌اند تا فعالیت‌های نظارتی را مجاز نمایند. بر اساس اصول ضرورت و تناسب (مجموعه‌ای از اصول در خصوص اعمال حقوق بشر در نظارت که توسط متخصصان و گروه‌های حفظ حریم خصوصی تدوین شده است)، نظارت بر ارتباطات باید به عنوان اقدامی بسیار مداخله‌جویانه تلقی شود و برای تحقق شرط تناسب، دولت باید حداقل قبل از انجام هر گونه نظارت، موارد زیر را در مقابل یک مقام قضایی ذی‌صلاح ثابت کند:[49]

- به احتمال زیاد یک جرم جدی یا تهدید خاصی به هدف مشروعی انجام شده یا خواهد شد.
- به احتمال زیاد شواهد و مدارک مرتبط ماهوی با چنین جرم جدی یا تهدید خاص، از طریق دسترسی به اطلاعات محافظت شده مورد نظر به دست آید.
- سایر تکنیک‌های کمتر مداخله‌گرانه منسوخ شده یا بی‌فایده خواهند بود، به طوری که تکنیک مورد استفاده کمتر گزینه مداخله‌گرایی باشد.
- اطلاعات به دست آمده تنها محدود به مواردی خواهد بود که مربوط به جرم و جنایت جدی یا تهدید خاص است.
- هرگونه اطلاعات اضافی جمع‌آوری شده نگهداری نخواهد شد، بلکه بلافاصله نابود یا مسترد خواهد شد.
- اطلاعات تنها توسط مرجع مشخص شده و فقط برای هدف و مدت زمانی که مجوز داده شده است، در دسترس بوده و مورد استفاده قرار خواهد گرفت.
- فعالیت‌های نظارتی درخواست شده و تکنیک‌های پیشنهادی ماهیت حق حفظ حریم خصوصی یا سایر آزادی‌های اساسی را تضعیف نمی‌کنند.

نظارت، به منزله مداخله آشکار در حق حفظ حریم خصوصی است. همچنین، این امر مداخله‌ای در حق داشتن عقیده بدون مداخله و حق آزادی بیان محسوب می‌شود. با اشاره به حق داشتن عقیده بدون مداخله، سیستم‌های نظارتی چه هدفمند و چه گسترده، ممکن است حق اظهارنظر را تضعیف کنند، زیرا ترس از افشای ناخواسته فعالیت‌های آنلاین مانند جست‌وجو و مرور، احتمالاً افراد را از دسترسی به اطلاعات مورد نیاز برای ابراز عقیده بازمی‌دارد. به ویژه در مواردی که چنین نظارت‌هایی منجر به نتایج سرکوبگرانه می‌شود.[50]

مداخله در حق آزادی بیان به ویژه در زمینه روزنامه نگاران و اعضای رسانه که ممکن است در نتیجه فعالیت‌های خبری و روزنامه‌نگاری خود تحت نظارت قرار گیرند، محرض و آشکار است. همان‌طور که دبیرکل سازمان ملل متحد اشاره کرده است، این امر می‌تواند اثر بازدارنده‌ای بر بهره‌مندی از آزادی رسانه داشته باشد و ارتباط با منابع و به اشتراک‌گذاری و توسعه ایده‌ها را دشوارتر کند. [51] استفاده از

---

[47] مجمع عمومی سازمان ملل، "قطعنامه حق حفظ حریم خصوصی در عصر دیجیتال"، A/C.3/71/L.39/Rev.1، مصوب ۱۶ نوامبر ۲۰۱۶ (قطعنامه سال ۲۰۱۶ سازمان ملل در مورد حریم خصوصی): https://daccess-ods.un.org/tmp/3401807.84463882.html

[48] همان.

[49] همان مرجع ۴۳، پاراگراف ۸.

[50] گزارش گزارشگر ویژه سازمان ملل در مورد ناشناس بودن و رمزگذاری، مورد مذکور در مرجع ۳۳، پاراگراف ۲۱.

[51] گزارش دبیرکل سازمان ملل متحد به مجمع عمومی سازمان ملل، "گزارش در مورد امنیت روزنامه‌نگاران و موضوع مصونیت از مجازات"، A/70/290، مورخ ۶ آگوست ۲۰۱۵ (گزارش دبیر کل سازمان ملل متحد)، پاراگراف ۱۴ الی ۱۶:

رمزنگاری و سایر ابزارهای مشابه برای کار روزنامه‌نگاران ضروری شده است تا اطمینان حاصل شود که آنها بدون مداخله قادر به انجام کار خود هستند.

افشای منابع خبری از طریق نظارت می‌تواند پیامدهای منفی جدی بر حق آزادی بیان داشته باشد، زیرا منابع محرمانه اعتماد خود را به این که روزنامه‌نگاران قادر به پنهان کردن هویت آنها خواهند بود، از دست خواهند داد. [52] این موضوع در مورد موارد مربوط به افشای اطلاعات کاربران ناشناس نیز صادق است. پس از آنکه محرمانگی اطلاعات به خطر بیفتد با تضعیف شود، دیگر قابل بازیابی نیست. بنابراین، بسیار مهم است که اقدامات تضعیف‌کننده محرمانگی به طور خودسرانه انجام نشوند.

فعالیت‌های نظارتی که علیه روزنامه‌نگاران انجام می‌شود این خطر را دارد که اساساً حق حفاظت از منبع را که روزنامه‌نگاران از آن برخوردارند، تضعیف کند.[53] استفاده روزافزون از فناوری‌های دیجیتال و ابزارهای نظارتی پیشرفته‌تر، چالش‌های بیشتری را برای حفظ ناشناس بودن منابع ایجاد کرده است، از جمله به دلیل خطر افشای ناخواسته منبع در نتیجه نظارت بر دستگاه‌های ارتباطی.[54] به عنوان مثال، برخی منابع خبری در ایالات متحده از طریق سوابق تلفن و ایمیل شناسایی شده‌اند. [55] (برای اطلاعات بیشتر در مورد محافظت از منابع خبری، لطفاً به ماژول ۱۰ این دوره آموزشی مراجعه کنید).

نتیجه‌گیری

با گسترش حوزه آنلاین در سراسر جهان، حفاظت از داده‌ها به طور فزاینده لازم وضروری می‌شود. در جنوب وجنوب شرق آسیا، برخی پیشرفت‌ها در این زمینه حاصل شده است وتعدادی از کشورها اکنون قوانین حریم خصوصی را به اجرا درآورده‌اند. با این حال، با رشد سریع پردازش داده‌ها، قانون‌گذاران هنوز تا حدودی از حفظ کامل حریم خصوصی وحفاظت از اطلاعات شخصی عقب مانده‌اند. همزمان با پیشروی در این مسیر، فعالان حقوق دیجیتال، در تضمین اینکه دولتها در زمینه حفاظت از داده‌ها همگام با آخرین پیشرفتهاعمل کنند وقوانینی تصویب نمایند که به طور کامل از حق حفظ حریم خصوصی محافظت کند، نقش مهمی ایفا خواهند کرد.

https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/247/06/PDF/N1524706.pdf?OpenElement

[52] برای اطلاعات بیشتر، به پرونده Big Brother Watch علیه بریتانیا در دادگاه حقوق بشر اروپا (2018)، مراجعه کنید.
https://globalfreedomofexpression.columbia.edu/cases/big-brother-watch-v-united-kingdom

[53] طبق اصل ۹ اصول جهانی، دولت‌ها باید حفاظت از محرمانه بودن منابع را در قوانین خود فراهم کنند و اطمینان حاصل نمایند که:

- هر گونه محدودیت در حق حفاظت از منابع، مطابق با آزمون سه‌بخشی تحت قوانین بین‌المللی حقوق بشر است.
- محرمانه بودن منابع فقط در شرایط استثنایی و تنها با حکم دادگاه که با الزامات یک هدف مشروع، ضرورت و تناسب مطابقت دارد، باید برداشته شود. همین حمایت‌ها باید برای دسترسی به مطالب خبری اعمال شود.
- حق عدم افشای هویت منابع و حفاظت از مطالب خبری مستلزم آن است که حریم خصوصی و امنیت ارتباطات هر فردی که در حوزه روزنامه‌نگاری فعالیت می‌کند، از جمله دسترسی به داده‌های ارتباطی و فراداده‌های آنها، باید محافظت شود. دور زدن، مانند نظارت مخفیانه یا تجزیه و تحلیل داده‌های ارتباطاتی که توسط مقامات قضایی بر اساس قوانین واضح و محدود قانونی مجاز نیست، نباید برای تضعیف محرمانه بودن منبع مورد استفاده قرار گیرد.
- هر گونه حکم دادگاه فقط باید پس از یک جلسه دادرسی منصفانه صادر شود که به طور مناسب به روزنامه مورد نظر اطلاع داده شده باشد، مگر در موارد اضطراری واقعی.

[54] گزارش گزارشگر ویژه در مورد ترویج و حمایت از حق آزادی عقیده و بیان، A/70/361 (2015)، پاراگراف. ۲۳:
https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/273/11/PDF/N1527311.pdf?OpenElement

[55] برای مثال، به پرونده دولت ایالات متحده آمریکا علیه استرلینگ، 724 F.3d 482 (۲۰۱۳) مراجعه کنید.