ماژول ۷

جرایم سایبری

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

MEDIA DEFENCE

ناشر: موسسه دفاع رسانه (www.mediadefence.org)
این مجموعه 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

مقدمه 1

جرایم سایبری چیست؟ 2

تعریف 2

جرایم سایبری در قوانین بین‌المللی 2

جرایم سایبری در قوانین داخلی کشورها 3

انواع جرایم سایبری 3

نقض حریم خصوصی داده‌ها 3

*جرم‌انگاری **گفتار آنلاین*** 6

مزاحمت یا تعقیب سایبری و آزار و اذیت آنلاین 7

زورگویی مجازی 8

سایر جرایم سایبری 9

جرایم سایبری در جنوب و جنوب شرق آسیا 9

گام هایی که برای مقابله با آسیب‌های آنلاین باید برداشته شودد 11

نتیجه‌گیری 12

ماژول ۷

جرایم سایبری

- **با رشد و گسترش سریع دسترسی به اینترنت در آسیا، جرایم سایبری نیز بیش از پیش شایع و خطرناک شده‌اند.**
- **با این حال، قوانین مربوط به فعالیت‌های مجرمانه در اینترنت یا قوانین جرایم سایبری، به طور فزاینده‌ای ابزارهایی را در اختیار دولت‌ها قرار می‌دهند تا مخالفان و رسانه‌ها را سرکوب نمایند.**
- **حریم خصوصی داده‌ها در آسیا، به تدریج در حال جلب توجه گسترده‌تری است و بسیاری از کشورها اخیراً قوانین حمایت از داده‌ها را تصویب کرده‌اند، هرچند اغلب از حمایت کافی از حریم خصوصی برخوردار نیستند.**
- **موضوع نگران کننده این است که بسیاری از جرایم سایبری ماهیتی جنسیتی دارند، مانند مزاحمت و تعقیب سایبری و انتشار غیرقانونی تصاویر خصوصی.**
- **برای مقابله با آسیب‌های آنلاین و تضمین حقوق اساسی برابر در دنیای آفلاین و آنلاین، می‌توان اقدامات عملی مختلفی اتخاذ نمود.**

مقدمه

افزایش دسترسی به اینترنت اخیراً چالش‌های قانونی جدیدی به همراه داشته است. اینترنت ماهیتی فراملیتی و فراگیر دارد و چشم‌انداز ایجاد شده در دنیای دیجیتال، چالش‌های تازه‌ای را در زمینه حفاظت از حقوق بنیادین در عصر دیجیتال ایجاد کرده است. تعاریف سنتی مفاهیمی مانند ناشر یا روزنامه‌نگار پیچیده‌تر شده و ناشناس ماندن در بسیاری از پلتفرم‌های اینترنتی، اگرچه کلید آزادی بیان در بسیاری موارد است، اما در مبارزه با فعالیت‌های آنلاین غیرقانونی و جبران خسارت قربانیان چالش‌برانگیز است. همچنین سوالات جدی درباره مسئولیت انتشار محتوای آنلاین مطرح است که ممکن است بر طرف‌های مختلف در حوزه‌های قضایی گوناگون تأثیرگذار باشد.

تنظیم مقررات و قوانین مربوط به جرایم سایبری و مجازی برای دولت‌ها و نهادهای بین‌المللی دشوار بوده است. در سال ۲۰۲۰ یک گروه متخصص در امنیت سایبری پیش‌بینی کردند هزینه‌های جهانی جرایم سایبری سالانه ۱۵٪ رشد وتا سال ۲۰۲۵ به ۱۰/۵ تریلیون دلار در سال برسد.[1] بدون چارچوب‌های نظارتی قانونی و حمایتی مناسب، گسترش اینترنت، تجارت الکترونیک و توسعه اقتصادی می‌تواند منجر به رشد و گسترش جرایم سایبری شود.

به دنبال افزایش سریع کاربران جدید اینترنت در آسیا، افزایش دسترسی به اینترنت و فناوری‌های اطلاعات و ارتباطات (ICT) نیز منجر به افزایش چشمگیر جرایم آنلاین و فعالیت‌های مجرمانه در فضای مجازی شده است. با این حال، قوانینی که برای مقابله با این جرایم سایبری و تنظیم فعالیت‌های آنلاین وضع می‌شوند، به دلیل ماهیت مبهم و گستره بیش از حد خود، بیشتر به ابزاری برای سرکوب مخالفان، منتقدان و رسانه‌های مستقل توسط دولت‌ها تبدیل شده‌اند.

گزارشگر ویژه سازمان ملل در مورد آزادی بیان در سال ۲۰۱۱ هشدار داد که:

" علارقم تعارض با تعهدات بین‌المللی حقوق بشری، اظهارات مشروع منتشر شده در فضای آنلاین، توسط دولت‌ها جرم‌انگاری می‌شود. این امر یا از طریق اعمال قوانین کیفری موجود بر بیان آنلاین صورت می‌گیرد و یا با ایجاد قوانین جدید که به طور خاص برای جرم‌انگاری اظهارنظر در اینترنت طراحی شده‌اند. چنین قوانینی اغلب با هدف حمایت از آبرو و حیثیت افراد، حفظ امنیت ملی یا مبارزه با تروریسم توجیه می‌شوند، اما در عمل برای سرکوب آزادی بیان و سانسور محتواهایی که مورد پسند دولت‌ها و سایر نهادهای قدرتمند نیستند، مورد استفاده قرار می‌گیرند."[2]

---

[1] گلوبال نیوز وایر، "جرایم سایبری تا سال ۲۰۲۵ سالانه 10.5 تریلیون دلار برای جهان هزینه خواهد داشت"، (۲۰۲۰): https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html

[2] هفدهمین نشست مجمع عمومی سازمان ملل متحد، شورای حقوق بشر، «گزارش گزارشگر ویژه آزادی بیان» صفحه ۱۰، (۲۰۱۱):

متاسفانه این مشکل از زمان هشدار گزارشگر ویژه تاکنون بدتر شده است.

جرایم سایبری چیست؟

تعریف

هیچ تعریف دقیق و جهانی برای اصطلاح "جرم سایبری" وجود ندارد، اما به طور کلی به جرایمی اطلاق می‌شود که با استفاده از شبکه‌های رایانه‌ای یا اینترنت انجام می‌شوند.[3] این تعریف می‌تواند شامل طیف گسترده‌ای از فعالیت‌های مجرمانه از جمله فعالیت‌های تروریستی و جاسوسی با کمک اینترنت، هک و نفوذ غیرقانونی به سیستم‌های رایانه‌ای، جرایم مرتبط با محتوا، سرقت و دستکاری داده‌ها و مزاحمت و تعقیب مجازی شود. به عبارت دیگر، هر گونه فعالیت مجرمانه‌ای که با بهره‌گیری از اینترنت و فضای مجازی و ابزارهای دیجیتال صورت گیرد، در دسته جرایم سایبری یا مجازی قرار می‌گیرد.[4]

جرایم سایبری و امنیت سایبری دو مقوله در فضای دیجیتال هستند که ارتباط تنگاتنگی دارند و غیرقابل تفکیک هستند. امنیت سایبری یا محافظت از دستگاه‌ها، سیستم‌ها وشبکه‌های دیجیتال در برابر جرایم سایبری، به مجموعه‌ای از "ابزارها، سیاست‌ها، مفاهیم امنیتی، تدابیر امنیتی، دستورالعمل‌ها، رویکردهای مدیریت ریسک، اقدامات، آموزش‌ها، شیوه‌های برتر و اطمینان‌بخش و فناوری‌هایی" اشاره دارد که می‌توانند برای محافظت از محیط سایبری، سازمان‌ها و دارایی‌های کاربران مانند دستگاه‌های رایانه‌ای، برنامه‌ها و سیستم‌های مخابراتی مورد استفاده قرار گیرند.[5]

جرایم سایبری در قوانین بین‌المللی

قطعنامه مجمع عمومی سازمان ملل در مورد ایجاد فرهنگ جهانی امنیت سایبری بیان می‌کند که:

> **"امنیت سایبری باید به شیوه‌ای اجرا شود که با ارزش‌های شناخته شده در جوامع دموکراتیک از جمله آزادی تبادل افکار و عقاید، گردش آزاد اطلاعات، محرمانه بودن اطلاعات و ارتباطات، حفاظت مناسب از اطلاعات شخصی، صراحت و شفافیت، سازگار باشد."[6]**

کنوانسیون جرایم سایبری شورای اروپا (CETS No.185)، موسوم به کنوانسیون بوداپست، تنها سند بین‌المللی الزام‌آور در مورد جرایم سایبری است.[7] این کنوانسیون برای کشورهای غیراروپایی نیز قابل اجرا است و تاکنون فیلیپین و سری‌لانکا تنها کشورهای جنوب و جنوب شرق آسیا هستند که به آن ملحق شده‌اند.[8] کنوانسیون بوداپست همچنین به عنوان یک "قانون نمونه" برای قانونگذاران در برخی حوزه‌های قضایی مورد استفاده قرار گرفته است. به عنوان مثال، سری‌لانکا قانون ملی خود در سال ۲۰۰۷ موسوم به قانون جرایم رایانه‌ای را بر اساس کنوانسیون بوداپست و پیش از دعوت به پیوستن به این کنوانسیون در سال ۲۰۱۵، تدوین کرد.[9]

---

https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[3] ماده ۱۹، «آزادی بیان و فناوری اطلاعات و ارتباطات: مروری بر استانداردهای بین‌المللی»، صفحه ۲۵، (۲۰۱۸):
https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf

[4] همان.

[5] تعریف اتحادیه بین المللی مخابرات (ITU) از امنیت سایبری:
https://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/cybersecurity.aspx

[6] پنجاه‌وهفتمین نشست مجمع عمومی سازمان ملل متحد، «قطعنامه ایجاد فرهنگ جهانی امنیت سایبری، ص ۳:
https://digitallibrary.un.org/record/482184?ln=en

[7] شورای اروپا، «کنوانسیون بوداپست و استانداردهای مرتبط»:
https://www.coe.int/en/web/cybercrime/the-budapest-convention

[8] شورای اروپا، «اعضا/ناظران کنوانسیون بوداپست و سازمان‌های ناظر به کمیته کنواسیون جرایم سایبری (T-CY)»
https://www.coe.int/en/web/cybercrime/parties-observers?wpisrc=nl_cybersecurity202

[9] شورای اروپا، کمیته کنوانسیون جرایم سایبری، «کنوانسیون بوداپست در مورد جرایم سایبری: مزایا و تأثیرات در عمل»، (۲۰۲۰)، بخش 4.2.2، ص ۳۰:
https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac

اگرچه این کنوانسیون به عنوان یک "معیار" توسط برخی طرف‌های مذاکرات فعلی برای کنوانسیون جرایم سایبری سازمان ملل متحد مورد استناد قرار گرفته است، اما به دلیل فراهم نکردن حمایت‌های رویه‌ای کافی برای حقوق آزادی بیان و حریم خصوصی و داشتن جرایم محتوایی و کپی‌رایت اضافی و گسترده، مورد انتقاد قرار گرفته است.[10]

جرایم سایبری در قوانین داخلی کشورها

با وجود اینکه تنها دو کشور در جنوب و جنوب شرق آسیا (فیلیپین و سری لانکا) به کنوانسیون بوداپست در زمینه جرایم سایبری پیوسته‌اند، در سال‌های اخیر قوانین مربوط به جرایم سایبری در این مناطق گسترش یافته است.
برای اطمینان از اینکه قوانین جرایم سایبری به طور غیرضروری حقوق اساسی آزادی بیان، حریم خصوصی و دسترسی به اطلاعات را نقض نمی‌کنند، این قوانین باید معیارهای زیر را رعایت کنند:

- ارائه تعاریف محدود و مشخص از جرایم سایبری که برای پیشبرد اهداف مشروع طراحی شده و کمترین محدودیت را بر آزادی بیان و حریم خصوصی اعمال می‌کنند.
- الزام به اثبات احتمال بروز آسیب در نتیجه یک فعالیت مجرمانه مشخص.
- شناسایی ماهیت تهدید حاصل از هر فعالیت مجرمانه.
- عدم وضع قوانین و استانداردهای متفاوت برای رفتارهای آنلاین و آفلاین، مگر اینکه آن رفتار در فضای آنلاین کاملاً متفاوت باشد.
- توجه و دفاع از منافع عمومی در رابطه با کسب و انتشار اطلاعات طبقه‌بندی شده به عنوان اطلاعات محرمانه.
- به عنوان یک اصل کلی، عدم صدور حکم زندان برای جرایم مرتبط با بیان، به جز مواردی که در استانداردهای حقوقی بین‌المللی مجاز شمرده می‌شوند و تضمین و تدابیر کافی برای جلوگیری از سوءاستفاده وجود دارد.[11]

انواع جرایم سایبری

نقض حریم خصوصی داده‌ها

استفاده از داده‌ها و میزان گردش اطلاعات و داده‌ها از جمله داده‌های شخصی در سطح جهانی همواره در حال افزایش است. با این حال، در بسیاری از کشورها مقررات و قوانین کافی برای حفاظت از این داده‌ها وضع نشده است و عدم وجود قوانین مناسب برای جمع‌آوری و پردازش اطلاعات شخصی می‌تواند پیامدهای جدی داشته باشد و همین امر اهمیت وجود قوانین حفاظت از داده‌ها را آشکار می‌سازد. در سال‌های اخیر، توجه روزافزون به موضوع حفاظت از داده‌ها و اطلاعات، منجر به تصویب قوانین حریم خصوصی جدید در تعدادی از کشورهای آسیایی شده است.[12] اما همچنان بسیاری از کشورها از قوانین و مقررات کافی برای حفاظت از اطلاعات و داده‌های کاربران در برابر نقض حریم خصوصی، به‌ویژه از سوی فعالیت‌های نظارتی دولت، برخوردار نیستند.[13]

---

[10] مراجعه شود به جلسه توجیهی ماده ۱۹، "کنوانسیون شورای اروپا در مورد جرایم سایبری و اولین و دومین پروتکل الحاقی" (۲۰۲۲): https://www.article19.org/wp-content/uploads/2022/06/Budapest-Convention-analysis-May-2022.pdf

[11] مؤسسه دفاع رسانه، «راهنمای آموزشی حقوق دیجیتال و آزادی بیان در محیط آنلاین، صفحه ۶۲، (۲۰۲۰) https://www.mediadefence.org/resource-hub/resources/media-defence-training-manual-on-digital-rights-and-freedom-of-expression-online/

[12] برای مرور روندهای منطقه‌ای در زمینه حریم خصوصی داده‌ها و قوانین مربوط به آن، مراجعه شود به گزارش "راهنمای حریم خصوصی آسیا-اقیانوسیه 2020-2021: قوی‌تر با هم"، Deloitte: https://www2.deloitte.com/ph/en/pages/risk/articles/asia-pacific-privacy-guide.html

و گراهام گرینلیف، "پیشرفت در قوانین حریم خصوصی داده‌ها در جنوب آسیا: سریلانکا، پاکستان و نپال"، ۲۰۱۹، گزارش بین‌المللی تجارت و قوانین حریم خصوصی، ص ۲۲-۲۵: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3549055

[13] دسترسی دیجیتال، «حقوق دیجیتال در جنوب شرقی آسیا 2022/2021»، (۲۰۲۲)؛ https://digitalreach.asia/event/report-launch-digital-rights-in-southeast-asia-2021-2022/

ظهور و گسترش فناوری‌های پیشرفته نظارتی و استفاده از فناوری‌های بیومتریک بدون تضمین‌امنیت، تنها بخشی از تهدیدهای متعدد علیه حق حریم خصوصی در آسیا هستند. با این حال، در سال‌های اخیر برخی آرای قضایی امیدوارکننده از سوی دستگاه قضایی در برخی کشورها، حاکی از تمایل به حمایت از حق حریم خصوصی بوده است.

حکم دادگاه عالی هند در مورد بدافزار جاسوسی پگاسوس (Pegasus)

در پرونده "مانوهار لال شارما علیه اتحادیه هند"،[14] دادگاه عالی هند، ادعای دخالت دولت هند در استفاده غیرمجاز از نرم‌افزار جاسوسی پگاسوس را برای نظارت گسترده مورد بررسی قرار داد. در این پرونده، شاکیان (ترکیبی از مدعیان دعاوی منافع عمومی وافراد مدعی قربانی شدن) ادعا کردند که استفاده غیرمجاز دولت از پگاسوس نه تنها نقض حریم خصوصی است، بلکه به دلیل ایجاد اثر "سرکوب کننده"، نقض آزادی بیان نیز محسوب می‌شود.[15]

نرم‌افزار پگاسوس که توسط شرکت اسرائیلی NSO توسعه یافته است، با نفوذ به دستگاه‌های دیجیتال می‌تواند به ایمیل‌ها، پیامک‌ها، تماس‌های تلفنی، دوربین و ضبط صدا دسترسی پیدا کرده و داده‌های ذخیره شده را منتقل کند. در سال ۲۰۱۸، آزمایشگاه تحقیقاتی The Citizen Lab کشف کرد کاربران از بیش از 45 کشور، هدف این نرم‌افزار جاسوسی قرار گرفته‌اند. گزارش‌های تحقیقات بعدی حاکی از این است که حدود ۵۰هزار نفر توسط این ابزار جاسوسی تحت نظر قرار داشته‌اند که حدود ۳۰۰ نفر از آنها شهروندان هندی از جمله روزنامه‌نگاران، پزشکان، فعالان سیاسی و حتی برخی کارکنان دادگاه‌ها بوده‌اند.[16]

در پاسخ به افشاگری‌های رسانه‌ای درباره استفاده از نرم افزار جاسوسی پگاسوس برای نظارت غیرقانونی بر شهروندان، دولت هند توضیحاتی ارائه کرده است و وزیر فناوری اطلاعات این کشور استفاده غیرقانونی از پگاسوس را رد کرد، اما استفاده واقعی از این نرم‌افزار جاسوسی را تکذیب نکرد.[17] این ابهام عمدی و هدفمند در جریان دادرسی پرونده مانوهار نیز منعکس شد؛ جایی که دولت با ارائه یک حکم محرمانه، به طور کلی ادعاهای شاکیان را رد کرد بدون آنکه به جزئیات آنها بپردازد.[18] زمانی که به دولت فرصت ارائه حکم تکمیلی داده شد، سرپرست دادستانی با استناد به نگرانی‌های امنیت ملی از افشای اطلاعات بیشتر خودداری کرد.[19]

دادگاه عالی هند در پرونده مربوط به نرم‌افزار جاسوسی پگاسوس، مجدداً بر رأی قبلی خود در پوتاسوامی[20] مبنی بر "مقدس بودن"[21] حریم خصوصی تأکید کرد و خاطرنشان کرد که میان شاکیان و متهمان در این پرونده، "توافق گسترده حاکی از این است که نظارت یا دسترسی غیرمجاز به داده‌های ذخیره شده در گوشی‌ها و دستگاه‌های شهروندان و به دلایلی غیر از امنیت ملی، امری غیرقانونی، ناپسند و نگران‌کننده است.[22] دادگاه همچنین اذعان کرد که "تهدید به نظارت بر نحوه تصمیم‌گیری شهروندان برای بهره‌مندی از حقوق خود تأثیرگذار است و ممکن است منجر به خودسانسوری شود که برای روزنامه‌نگاران از اهمیت ویژه‌ای برخوردار است.[23] دادگاه همچنین بر اهمیت این پرونده در حفاظت از منابع خبری روزنامه‌نگاران نیز تأکید کرد.[24]

اسمیتا کریشنا پراساد و شارنگان آراویندکشان (2021) «تلاش برای رسیدن – رژیم‌های حریم خصوصی در جنوب آسیا»، مجله بین‌المللی حقوق بشر، دوره ۲۵، شماره ۱، صفحات ۷۹ تا ۱۱۶، صفحه ۱۰۵:
https://www.tandfonline.com/doi/full/10.1080/13642987.2020.1773442

14 دادخواست شماره ۳۱۴ – هند، (۲۰۲۱): https://main.sci.gov.in/pdf/LU/27102021_082008.pdf

15 همان، بند ۲۱.

16 همان، بندهای ۲ و ۳.

17 رجیستر، "وزیر فناوری اطلاعات هند استفاده غیرقانونی از نرم‌افزار جاسوسی پگاسوس شرکت NSO را تکذیب کرد"، (۲۰۲۱):
https://www.theregister.com/2021/07/20/ashwini_vaishnaw_bnso_pegasus_denial/

18 منوهر، شماره ۱۴، بند ۱۲.

19 همان، بند ۱۳ تا ۱۷.

20 حکم کی. اس. پوتاسامی علیه اتحادیه هند، دادخواست کتبی (مدنی) شماره ۴۹۴ سال ۲۰۱۲، (۲۰۱۸):
https://indiankanoon.org/doc/127517806/

21 منوهر، شماره ۱۴، بند ۳۲.

22 همان، بند ۵۲.

23 همان، بند ۳۹.

24 همان، بندهای ۴۰ و ۴۱.

دادگاه عالی هند معتقد بود که با توجه به مبهم بودن حکم ارائه شده از سوی دولت و عدم ارائه اطلاعات کافی، ادعاهای شاکیان در پرونده اولیه قابل بررسی است و آنها موفق شده‌اند دلایل اولیه و ظاهری برای بررسی ادعاهای خود ارائه نمایند و همچنین به دلیل رویکرد ناکافی و عدم شفافیت در ارائه اطلاعات در یک پرونده مربوط به نقض حقوق اساسی مانند حریم خصوصی و آزادی بیان، از دولت شدیداً انتقاد کرد.[25] دادگاه توجیه امنیت ملی به عنوان دلیل عدم افشای اطلاعات دقیق را نپذیرفت و اظهار داشت: "امنیت ملی نمی‌تواند گزندی باشد که قوه قضائیه از آن دوری نماید."[26] در نهایت، دیوان با توجه به فرصت‌های کافی داده شده، به جای الزام دولت به ارائه حکم تکمیلی، دستور تشکیل یک کمیته کارشناسی به ریاست یک قاضی سابق دیوان عالی را برای تحقیق و روشن شدن حقایق مربوط به این پرونده صادر کرد.[27]

در مواردی که به مقامات اختیارات گسترده‌ای برای جمع‌آوری یا حذف گروه خاصی از داده‌ها بدون تضمین‌های کافی اعطا شده است، دادگاه‌ها قوانین مربوط به جرایم سایبری را بیش از حد گسترده تشخیص داده‌اند. به عنوان مثال، در سال ۲۰۱۴ دادگاه عالی فیلیپین در پرونده "دیسینی و دیگران علیه وزیر دادگستری و دیگران" قانونی بودن برخی از مفاد قانون پیشگیری از جرایم سایبری ۲۰۱۲ را مورد بررسی قرار داد.[28] این دادگاه اگرچه بسیاری از مفاد قانون را تأیید کرد، اما برخی مفاد را به دلیل گستردگی بیش از حد، غیرقانونی دانست. به عنوان مثال، ماده ۱۹ که به وزارت دادگستری اجازه محدودسازی یا مسدودسازی دسترسی به داده‌هایی را اعطا کرده بود که "بالقوه ناقض مفاد این قانون تلقی می‌شدند" و با تضمین‌های قانون اساسی در زمینه آزادی بیان و آزادی از تفتیش و توقیف غیرمعقول ناسازگار بود. دادگاه معتقد بود که: "برای یک مقام اجرایی، صرف اعتقاد شخصی به اینکه یک محتوا قانون را نقض می‌کند، دلیل کافی برای ضبط و توقیف یا حذف آن محتوا بدون حکم قضایی نیست؛ زیرا در این صورت آن مقام هم نقش قاضی را برای تشخیص جرم ایفا می‌کند، هم در جایگاه هیئت منصفه و مجری حکم قرار می‌گیرد که مغایر با تفکیک قوا و رعایت تشریفات قانونی است."

یکی دیگر از مفاد قانون پیشگیری از جرایم سایبری فیلیپین که توسط دادگاه عالی این کشور غیرقانونی شناخته شده و مغایر با قانون اساسی تلقی می‌شود، ماده ۱۲ این قانون بود که به مقامات اجرایی اجازه می‌داد "داده‌های ترافیکی مرتبط با ارتباطات رایانه‌ای را به روش‌های فنی یا الکترونیکی و به صورت آنی جمع‌آوری یا ضبط کنند." داده‌های ترافیکی شامل مبدأ، مقصد، مسیر، زمان، تاریخ، اندازه، مدت یا نوع سرویس ارتباطی بود اما شامل محتوای ارتباطات وهویت افراد نمیشد. این ماده همچنین ارائه‌دهندگان خدمات را ملزم می‌کرد "در فرآیند ثبت و جمع‌آوری این داده‌ها" با مقامات اجرایی همکاری کنند. دادگاه در تشخیص گستردگی بیش از حد قانون فعلی و مبهم بودن آن، استدلال خود را به شرح زیر ارائه داده است:

> دلیل جمع آوری داده‌ها دقیقاً مشخص نیست و نمی‌توان استنباط کرد این داده‌ها برای چه اهدافی جمع‌آوری می‌شوند. آیا سازمان‌های مجری قانون از داده‌های جمع‌آوری شده برای شناسایی مجرمان سایبری استفاده خواهند کرد؟ یا از این داده‌ها برای تشکیل پرونده علیه مظنونین شناسایی شده استفاده می‌شود؟ آیا می‌توان از این داده‌ها برای پیشگیری از وقوع جرایم سایبری نیز استفاده کرد؟
>
> اختیاراتی که ماده ۱۲ به مقامات قضایی . مجریان قانون اعطا کرده است، بسیار گسترده و فاقد محدودیت است. گرچه ماده ۱۲ بیان می‌کند که نباید هویت یا محتوای داده‌ها فاش شود، اما این محدودیت صرفاً یک توهم است. چرا که مسلماً هیچ چیز نمی‌تواند مانع از آن شود که مقامات با

---

[25] همان، بندهای ۴۶ و ۵۱.
[26] همان، بند ۴۹.
[27] همان، بندهای ۵۴ و ۵۵.
[28] شماره ثبت کلی: 203335، (۲۰۱۴): https://lawphil.net/judjuris/juri2014/feb2014/gr_203335_2014.html

در اختیار داشتن این داده‌ها، به هویت فرستنده یا گیرنده و محتوای داده‌ها دسترسی پیدا کنند. این امر موجب می‌شود شهروندان و کاربران به طور غیرضروری در معرض افشای اطلاعات یا حتی بدتر از آن، اخاذی از سوی عناصر فاسد در این نهادها قرار گیرند.

اگرچه بخش ۱۲ جمع آوری داده‌ها را به "ارتباطات مشخص شده" محدود می‌کند، اما در عمل این محدودیت فرضی اصلاً به عنوان محدودیت تلقی نمی‌شود. زیرا واضح است که خود مقامات قضایی و مجریان قانون ارتباطات هدف را مشخص می‌کنند. بنابراین قدرت آنها در این زمینه تقریباً نامحدود است و به آنها این امکان را می‌دهد که در یک "بازپرسی قانونی" ارتباطات مشخص و دلخواه خود را انتخاب کنند. این امر به وضوح حق حریم خصوصی افراد را تهدید و نقض می‌کند؛ زیرا مقامات و مجریان قانون می‌توانند به هر اطلاعاتی که بخواهند دسترسی پیدا کرده و آن را کنترل و بررسی کنند که این امر نقض آشکار حریم خصوصی کاربران محسوب می‌شود.

به رسمیت شناخته شدن حق حریم خصوصی در سطح ملی و گسترش آن به حوزه دیجیتال، در پی رشد سریع تصویب قوانین حفاظت از داده‌ها در سراسر جهان پس از اجرایی شدن مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR) در سال ۲۰۱۸ رخ داده است. مقررات عمومی حفاظت از داده اتحادیه اروپا استانداردی جدید برای حفاظت از داده‌های شخصی در فضای مجازی تعیین کرده است و به عنوان الگویی برای قوانین متعدد کشورهای دیگر عمل کرده است. قانون حفظ حریم خصوصی مصرف‌کنندگان کالیفرنیا (CCPA) نیز قواعد گسترده‌ای درباره حقوق مصرف‌کنندگان برای آگاهی از داده‌های شخصی جمع‌آوری شده، درخواست حذف داده‌ها و امتناع از جمع‌آوری داده‌ها دارد.[29] قانون حفظ حریم خصوصی مصرف‌کنندگان کالیفرنیا همچنین با توجه به کاربرد آن در بخش فناوری منطقه *سیلیکون ولی* (Silicon Valley) و همچنین به دلیل پیشرفت و ارتقای وضعیت حفاظت از داده‌ها در سطح جهانی مورد تحسین قرار گرفته است.[30]

جرم‌انگاری گفتار آنلاین

قوانین مرتبط با جرایم سایبری و فعالیت‌های مجرمانه در فضای مجازی معمولاً به دنبال مقابله با طیف گسترده‌ای از محتواهای غیرقانونی یا مضر هستند که در فضای مجازی منتشر می‌شوند. این محتواها ممکن است شامل تحریک به تروریسم، نفرت‌پراکنی یا اظهارات نفرت‌انگیز، محتوای جنسی مانند پورنوگرافی کودکان، و محتوایی باشد که منجر به نقض حقوق مالکیت معنوی می‌شود.[31]
قوانین مرتبط با جرایم سایبری و محدودیت‌های آنها بر محتوای منتشر شده در فضای مجازی، اغلب با حق آزادی بیان و دسترسی به اطلاعات در تعارض است و این حقوق را نقض می‌کند. هرگونه محدودیت بر این حقوق باید مطابق با الزامات ذکر شده در ماده ۱۹(بند ۳) میثاق بین‌المللی حقوق مدنی و سیاسی باشد: یعنی محدودیت‌ها باید به موجب قانون تعیین شده و برای یکی از اهداف مشروع و محدود (احترام به حقوق و اعتبار و حیثیت دیگران، حفاظت از امنیت ملی، نظم عمومی، بهداشت عمومی یا اخلاق عمومی) ضروری باشند. در سال ۲۰۱۱، گزارشگر ویژه سازمان ملل در مورد آزادی بیان، موارد زیر را از جمله انواع اظهاراتی برشمرد که محدودیت آنها تحت اهداف مشروع قرار می‌گیرد: (الف)

---

[29] فوربز، "کالیفرنیا اجرای قانون گسترده حفاظت از حریم خصوصی داده‌ها را آغاز می کند – آنچه باید بدانید" (۲۰۲۰):
https://www.forbes.com/sites/siladityaray/2020/07/01/california-begins-enforcing-broad-data-privacy-law---heres-what-you-should-know/?sh=1279e683de5c

[30] گاردین، "قانون پیشگام حفاظت از حریم خصوصی کالیفرنیا در ژانویه لازم الاجرا می‌شود. این قانون چه کاری انجام می‌دهد؟" (۲۰۱۹):
https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do

[31] ماده ۱۹، «آزادی بیان و فناوری اطلاعات و ارتباطات» (۲۰۱۸):
https://www.article19.org/wp-content/uploads/2018/02/FoE-and-ICTs.pdf

پورنوگرافی کودکان؛ (ب) تحریک مستقیم و علنی به ارتکاب نسل‌کشی؛ (ج) نفرت‌پراکنی و اظهارات نفرت‌انگیز؛ (د) توهین و افترا؛ و (ه) تحریک به تبعیض، خصومت یا خشونت.[32]

حتی قوانینی که برخی انواع بیان را جرم‌انگاری می‌کنند، باید دقیق بوده و از تضمین کافی و مؤثر در برابر سوءاستفاده برخوردار باشند تا الزامات قانونی بودن و ضرورت را برآورده کنند. به عنوان مثال، در مورد محدودیت‌های مربوط به پورنوگرافی کودکان، گزارشگر ویژه تأکید کرد که تدابیر ایمنی باید شامل نظارت و بازبینی توسط یک نهاد قضایی یا نظارتی مستقل و بی‌طرف باشد.[33] در سال ۲۰۱۸، گزارشگر ویژه اظهار داشت: ”قوانین محدودکننده کلی در زمینه "افراطگرایی"، "توهین به مقدسات"، "توهین و افترا"، "اظهارات توهین‌آمیز و نفرت‌پراکنی"، "اخبار جعلی" و "تبلیغات و پروپاگاندا" اغلب به عنوان بهانه‌ای برای درخواست از شرکت‌ها برای سرکوب اظهارات مشروع استفاده می‌شوند.“[34]

جرم‌انگاری اظهارات آنلاین می‌تواند از طریق قوانین خاص جرایم سایبری یا اعمال سایر قوانین کیفری غیرمرتبط به اینترنت صورت پذیرد. یک گزارش در سال ۲۰۱۷ از انجمن ارتباطات پیشرو که قوانین هند، مالزی، میانمار، پاکستان و تایلند را مقایسه می‌کند، نشان می‌دهد:

> تمامی این کشورها یا قوانینی دارند که به طور خاص فضای مجازی را هدف قرار می‌دهند (همراه با مقررات قانونی که بر آزادی بیان در فضای مجازی تأثیر می‌گذارند)، یا در مسیر تدوین چنین قوانینی گام برمی‌دارند. همه این کشورها همچنین از قوانین آفلاین برای جرم‌انگاری و مجازات اظهارات آنلاین استفاده می‌کنند. اکثر آنها از مقرارت قانونی متعددی برای هدف قرار دادن و جرم‌انگاری یک مورد خاص از بیان آنلاین استفاده می‌کنند. آنها همچنین نسبت به گفتار آفلاین، مجازات‌های سنگین‌تری برای "جرایم" آنلاین در نظر می‌گیرند.[35]

برای کسب اطلاعات بیشتر در مورد جرم‌انگاری بیان و اظهارات آنلاین، به ماژول ۳ از مجموعه ماژول‌های پیشرفته موسسه دفاع رسانه در مورد حقوق دیجیتال و آزادی بیان آنلاین مراجعه کنید.

مزاحمت یا تعقیب سایبری و آزار و اذیت آنلاین

پدیده رو به گسترش آزار و اذیت آنلاین یا مجازی و مزاحمت و تعقیب سایبری با رشد شبکه‌های اجتماعی بیشتر ترویج می‌یابد که بستر مناسبی برای چنین رفتارهایی فراهم می‌کند. تعقیب سایبری نوعی آزار و اذیت و ارعاب بی‌رویه از طریق ارتباطات الکترونیکی مانند پیام‌های متنی، تماس‌های تلفنی یا پست‌های ارسالی در شبکه‌های اجتماعی است که می‌تواند بهره‌مندی قربانیان این جرایم از حقوق آنلاین را به شدت محدود نماید؛ به ویژه اگر قربانیان از گروه‌های آسیب‌پذیر و محروم مانند زنان و اقلیت‌های جنسی باشند. تحقیقات نشان داده که آزار و اذیت مجازی اغلب متمرکز بر ویژگی‌های شخصی یا فیزیکی است و دیدگاه‌های سیاسی، جنسیت، ظاهر فیزیکی و نژاد از رایج‌ترین موارد آزار و اذیت آنلاین هستند.[36] علاوه بر این، زنان نسبت به مردان، به میزان بسیار بالاتری در معرض اشکال جنسی آزار و اذیت آنلاین قرار می‌گیرند.[37]

---

[32] گزارشگر ویژه ملل متحد در مورد حق آزادی عقیده و بیان، فرانک لا رو، (۲۰۱۱)، بند ۲۵:
https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[33] همان، بند ۷۱.

[34] گزارشگر ویژه سازمان ملل متحد در مورد حق آزادی عقیده و بیان، (۲۰۱۸)، بند ۱۳:
https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf

[35] انجمن ارتباطات پیشرو، "آزادی بیان: مطالعه‌ای در مورد قوانین جرم‌انگاری بیان و اظهارات آنلاین در آسیا"، (۲۰۱۷)، صفحه ۲۵:
https://www.giswatch.org/sites/default/files/giswspecial2017_web.pdf

[36] مرکز تحقیقات پیو، «آزار و اذیت آنلاین، (۲۰۱۷):
https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

[37] همان.

پدیده نوظهور و نگران‌کننده انتشار غیرمجاز تصاویر خصوصی

شکل خاصی از آزار و اذیت آنلاین که به عنوان یک پدیده نگران کننده ظاهر شده است، به اشتراک‌گذاری و انتشار غیرمجاز تصاویر خصوصی و صریح جنسی (عمدتاً تصاویر زنان) اغلب توسط شریک زندگی یا همسر سابق با انگیزه انتقام از جدایی یا سایر اختلافات، یا با هدف باج‌گیری، اخاذی یا تحقیر است. با این حال، قوانین جرایم سایبری تنها در تعداد کمی از کشورها به طور خاص انتشار غیرمجاز چنین تصاویری را جرم تلقی می‌کنند. این خلأ قانونی اغلب موجب می‌شود قربانیان امکان پیگرد قانونی مناسب علیه عاملان این جرم را نداشته باشند.[38] فیلیپین[39] و سنگاپور[40] از معدود کشورهایی هستند که انتشار غیرمجاز تصاویر خصوصی را به صراحت جرم‌انگاری کرده‌اند.

اهمیت نامگذاری مناسب

انتشار غیرمجاز تصاویر خصوصی اغلب به عنوان "پورنوگرافی انتقامی" نامیده می‌شود. فعالان و پژوهشگران بطور یکپارچه این اصطلاح را به دلایل زیر رد کرده‌اند:[41] اولاً، واژه "انتقام" بدین معناست که قربانی آسیبی را وارد کرده که ارزش انتقام دارد و انتقام‌جویی آن توجیه دارد. ثانیاً، "پورنوگرافی" این رفتار را با تولید توافقی محتوا برای انتشار عمومی یکسان می‌داند، در حالی که انتشار غیرمجاز تصاویر خصوصی قطعاً چنین نیست. ثالثاً، این اصطلاح "یک خسارت یا لطمه قدیمی را به عنوان یک مشکل دیجیتال جدید بازنویسی می‌کند"، در حالی که انتشار غیرتوافقی تصاویر زنان در رسانه‌های مختلف سابقه طولانی دارد.[42] نهایتاً ، این اصطلاح با نادیده گرفتن طیف وسیعی از متجاوزان و انگیزه‌ها، جرم را ساده‌سازی می‌کند و واکنش اخلاق‌گرایانه‌ای علیه قربانی برمی‌انگیزد.[43]

آزار و اذیت مداوم کاربران در شبکه‌های اجتماعی نیز به یک روند نگران کننده تبدیل شده است.

زورگویی مجازی

همچنین شایان ذکر است که جرم زورگویی یا قلدری مجازی (cyberbullying) یکی دیگر از اشکال جرایم سایبری است که عبارت است از ارسال پیام‌های ارعاب‌آمیز یا تهدیدآمیز اغلب از طریق شبکه‌های اجتماعی که در میان کودکان و نوجوانان رایج است. طبق گفته صندوق کودکان سازمان ملل متحد (یونیسف):

" زورگویی مجازی می‌تواند در شبکه‌های اجتماعی، پلتفرم‌های پیام‌رسان، بازی‌های آنلاین و تلفن‌های همراه رخ دهد. این رفتار به صورت مداوم تکرار می‌شود که هدف آن ترساندن، عصبانی کردن یا شرمساری افراد موردنظر است. نمونه‌هایی از آن عبارتند از:

- **پخش شایعات و نشر اکاذیب در مورد یک فرد یا انتشارعکس‌های تحقیرآمیز از فرد در شبکه‌های اجتماعی**
- **ارسال پیام‌های آزاردهنده یا تهدیدآمیز از طریق پلتفرم‌های پیام‌رسان**
- **جعل هویت یک فرد و ارسال پیام‌های نامناسب به دیگران به نیابت از او.**

---

38 به عنوان مثال، نظام قانون‌گذاری در هند در رابطه با انتشار غیرمجاز تصاویر خصوصی، به عنوان یک نظام حقوقی توسعه نیافته مورد انتقاد قرار گرفته است. به عنوان مثال، مراجعه شود به وایشناوی شارما، "درک قوانین انتشار غیرمجاز تصاویر خصوصی در هند با تمرکز بر مسئولیت واسطه‌ها"، مجله حقوقی دانشگاه ملی علوم سیاسی، سال چهاردهم، شماره ۴، ۲۰۲۱.
http://nujslawreview.org/wp-content/uploads/2022/03/14.4-Sharma-1.pdf

39 قانون ضد چشم‌چرانی یا تماشاگری جنسی به عکس و ویدئوی افراد، مصوب سال ۲۰۰۹، قانون جمهوری شماره 9995، بخش ۴:
https://www.lawphil.net/statutes/repacts/ra2010/ra_9995_2010.html).

40 قانون مجازات ۱۸۷۱، (مصوب ۱۵ ژوئن ۲۰۲۲)، بخش 377BC، (ماده ۱، بند الف):
https://sso.agc.gov.sg/Act/PC1871?ProvIds=pr377BC-#pr377BC-
قبل از وضع قوانین خاص مرتبط با انتشار غیرمجاز تصاویر خصوصی و جرم‌انگاری آن، این رفتار تحت عناوین و بندهای کلی‌تری مانند "اعمال علیه عفت زنان" در بخش ۵۰۹ قانون مجازات که اکنون لغو شده است، جرم‌انگاری شده و تحت تعقیب قرار می‌گرفت. به عنوان مثال مراجعه شود به پرونده شکایت "آنگ ژو سی جاشوا علیه دادستان" در دادگاه عالی سنگاپور (۲۰۱۶)، با شماره پرونده SGHC 143
https://www.elitigation.sg/gdviewer/s/2016_SGHC_143

41 وب‌سایت GenderIT، 'پورنوگرافی انتقامی: "پنج دلیل مهم که چرا نباید انتشار غیرمجاز تصاویر خصوصی را با این نام بخوانیم"'، ۲۰۱۹:
https://www.genderit.org/articles/5-important-reasons-why-we-should-not-call-it-revenge-porn

42 همان.

43 انجمن ارتباطات پیشرو، «خشونت و تعرض جنسی آنلاین: گزارش ارسالی انجمن ارتباطات پیشرو به گزارشگر ویژه سازمان ملل در مورد خشونت علیه زنان، علل و پیامدهای آن»، (۲۰۱۷)، صفحه ۲۱:
https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf

زورگویی و آزار و اذیت رودررو و زورگویی مجازی اغلب می‌توانند همزمان اتفاق بیافتند. اما زورگویی مجازی ردپایی دیجیتالی و قابل ردیابی از خود به جای می‌گذارد که می‌تواند به عنوان مدرک شناسایی افراد مرتکب بکار گرفته شود و شواهدی را برای کمک به متوقف کردن این رفتار آزاردهنده فراهم کند.“ [44]

آزار و اذیت آنلاین یا قلدری مجازی در میان جوانان و نوجوانان یک معضل گسترده و در حال گسترش است. بر اساس مطالعه مشترک یونیسف و نماینده ویژه دبیرکل سازمان ملل (SRSG) در امور مربوط به خشونت علیه کودکان، یک سوم از جوانان در ۳۰ کشور قربانی زورگویی آنلاین شده‌اند.[45]

قانون زورگویی سایبری در فیلیپین

فیلیپین از طریق قانون ضد زورگویی و قلدری مصوب سال ۲۰۱۳ به دنبال مقابله با پدیده قلدری مجازی یا آزار و اذیت آنلاین در میان کودکان بوده است.[46] بر اساس این قانون، مدارس ابتدایی و راهنمایی مؤظف هستند خط مشی‌های ضد قلدری را اتخاذ کنند و گزارش‌های سالانه در این زمینه ارائه دهند. در بخش ۲ (د) این قانون، "قلدری" به صورت گسترده‌ای تعریف شده است: "زورگویی یا هرگونه قلدری که از طریق استفاده از فناوری یا وسایل الکترونیکی انجام می‌شود." این رویکرد نوآورانه ممکن است با رویکردهای نامتناسب وگسترده برخی کشورها در جرم‌انگاری زورگویی مجازی در تضاد و تعارض باشد.

سایر جرایم سایبری

کنوانسیون جرایم سایبری بوداپست انواع مختلف جرایم سایبری را به شرح زیر تعریف می‌کند:

- **دسترسی غیرقانونی به یک سیستم رایانه‌ای**
- **رصد و رهگیری غیرقانونی**
- **مداخله در داده‌ها**
- **مداخله در سیستم**
- **سوءاستفاده از دستگاه‌ها**
- **جعل کامپیوتری**
- **کلاهبرداری مرتبط با رایانه**
- **پورنوگرافی کودکان**
- **جرایم مرتبط با نقض حق نشر و کپی‌رایت و حقوق مرتبط**[47]

اگرچه این تعاریف در سال ۲۰۰۱ ارائه شده است، اما بسیاری از آنچه امروزه تحت عنوان جرایم سایبری محسوب می‌شود، هنوز تحت پوشش این دسته‌بندی‌ها و مقررات قرار می‌گیرد.

جرایم سایبری در جنوب و جنوب شرق آسیا

جنوب وجنوب شرقی آسیا در سال‌های اخیر رشد سریع دسترسی به اینترنت را تجربه کرده است. افزایش دیجیتالی شدن جامعه، فرصت‌های بیشتری را برای شهروندان فراهم کرده است تا از حقوق آزادی بیان و دسترسی به اطلاعات بهرمند شوند. اما از سوی دیگر، با گسترش بیشتر فناوری‌های دیجیتال، تهدیدات امنیتی و نگرانی‌های حقوقی جدیدی نیز ظهور کرده است که بسیاری از کشورهای این مناطق در مواجهه با این تهدیدات نوظهور، محدودیت‌هایی را برای حقوق و آزادی‌های مجازی شهروندان خود ایجاد کرده‌اند.

---

[44] یونیسف، "زورگویی سایبری چیست و چگونه می‌توان آن را متوقف کرد":
https://www.unicef.org/end-violence/how-to-stop-cyberbullying

[45] یونیسف، "نظرسنجی یونیسف: طبق گزارش‌ها، بیش از یک سوم جوانان در ۳۰ کشور قربانی زورگویی مجازی شده‌اند"، (۲۰۱۹):
https://www.unicef.org/press-releases/unicef-poll-more-third-young-people-30-countries-report-being-victim-online-bullying

[46] قانون جمهوری شماره 10627: https://lawphil.net/statutes/repacts/ra2013/ra_10627_2013.html

[47] شورای اروپا، "وضعیت قانون جرایم سایبری در آفریقا – مرور کلی" ص ۲، (۲۰۱۵): https://rm.coe.int/16806b8a79

گزارش اینترپل در سال ۲۰۲۱ اشاره کرده است که: "کشورهای عضو اتحادیه کشورهای جنوب شرق آسیا (آسه‌آن) به دلیل رشد سریع اقتصاد دیجیتال، هدف اصلی حملات سایبری قرار گرفته‌اند."[48] در درپاسخ به این تهدیدات امنیتی فزاینده، آسه‌آن اقداماتی را برای همکاری چندجانبه در زمینه امنیت سایبری آغاز کرده است. از جمله این اتحادیه اولین سازمان منطقه‌ای است که اصول یازده گانه رفتار مسئولانه دولت‌ها در فضای سایبری را به صورت داوطلبانه پذیرفته است[49] که مجموعه اصولی است که در گزارش گروه کارشناسان دولتی[50] در سال ۲۰۱۵ تدوین شده و سپس در قطعنامه مجمع عمومی سازمان ملل متحد تأیید شده است.[51]

در کشورهای جنوب و جنوب شرقی آسیا، کشورهای این منطقه به منظور حفاظت بهتر در برابر جرایم آنلاین و همگام شدن با تحولات فناوری، قوانین جدیدی را در زمینه جرایم سایبری در سطح ملی تصویب کرده‌اند. تمامی کشورهای جنوب و جنوب شرق آسیا به استثنای کامبوج، میانمار و مالدیو، به نوعی قانون جرایم سایبری را تصویب کرده‌اند.[52] کامبوج، میانمار و مالدیو نیز در حال تهیه لایحه پیش‌نویس و تدوین چنین قوانینی هستند.[53]

با این حال، قوانین جرایم سایبری کشورهای جنوب و جنوب شرق آسیا، به طور فزاینده‌ای برای محدود کردن آزادی بیان و تنظیم ناعادلانه محتوای اینترنتی، از جمله سرکوب انتقاد یا مخالفت مورد استفاده قرار می‌گیرند. سازمان‌های بین‌المللی مدافع حقوق بشر مانند اکسس ناو (Access Now) که بر موضوع امنیت دیجیتال تمرکز دارند، نگران هستند که انبوه قوانینی که در حال حاضر برای تنظیم جرایم سایبری در حال تصویب هستند، به دلیل تعاریف مبهم و گسترده، مستعد تفسیر و اجرای سلیقه‌ای بوده و محدود کننده آزادی بیان هستند. برخی مفاد این قوانین به طور کلی اقداماتی چون انتشار اطلاعات نادرست یا آسیب به وحدت ملی را جرم تلقی می‌کنند.[54] در نتیجه، فعالان حقوق بشر با موجی از دستگیری‌ها و محکومیت‌ها تحت عنوان جرایم سایبری مواجه شده‌اند که نقض آزادی بیان محسوب می‌شود. این امر نگرانی‌های فزاینده‌ای را در میان مدافعان حقوق بشر در مورد سوءاستفاده از این قوانین برای سرکوب مخالفان و منتقدان ایجاد کرده است.
مثلاً قانون امنیت دیجیتال بنگلادش که به دلیل مفاد و مقررات مبهم و گسترده آن برای سرکوب منتقدان دولت مورد استفاده قرار گرفته است، به شدت مورد انتقاد قرار گرفته است.[55] به عنوان مثال،

---

[48] پلیس بین‌الملل، ارزیابی تهدیدات سایبری اتحادیه کشورهای جنوب شرق آسیا، (۲۰۲۱)، صفحه ۱۳:
https://www.interpol.int/en/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

[49] شبکه خبری کانال آسیا (CNA)، "آسه‌آن چگونه تلاش‌های جهانی امنیت سایبری را مدیریت می‌کند کند؟"، (۲۰۲۱)
https://www.channelasia.tech/article/691880/how-asean-driving-global-cybersecurity-efforts/

[50] مجمع عمومی سازمان ملل، "گزارش گروه کارشناسان دولتی درباره تحولات در زمینه اطلاعات و ارتباطات در چارچوب امنیت بین‌المللی"، سند شماره UN Doc A/70/174، (۲۰۱۵).

[51] مجمع عمومی سازمان ملل، "توسعه اطلاعات و ارتباطات از راه دور در زمینه امنیت بین‌المللی"، UN Doc A/RES/70/237، (۲۰۱۵):
https://undocs.org/Home/Mobile?FinalSymbol=a%2Fres%2F70%2F237&Language=E&DeviceType=Desktop&LangRequested=False

[52] کنفرانس تجارت و توسعه سازمان ملل متحد، "قانون جرایم سایبری در سراسر جهان"، (۲۰۲۱):
https://unctad.org/page/cybercrime-legislation-worldwide

[53] همان. برای تحلیل انتقادی پیش‌نویس لایحه جدید امنیت سایبری میانمار، مراجعه شود به مرکز قانون و دموکراسی، "میانمار: یادداشتی در مورد پیش‌نویس قانون جدید امنیت سایبری"، (۲۰۲۲):
https://www.law-democracy.org/live/wp-content/uploads/2022/05/Myanmar.Cyber-Security-Analysis-English-.pdf

[54] انجمن اکسس ناو (Access Now)، "وقتی قوانین «جرایم سایبری» آزادی بیان را محدود می‌کند: توقف روند خطرناک در سراسر منا (MENA : خاورمیانه و شمال آفریقا)"، (۲۰۱۸):
https://www.accessnow.org/when-cybercrime-laws-gag-free-expression-stopping-the-dangerous-trend-across-mena/

[55] به عنوان مثال مراجعه کنید به دیدبان حقوق بشر، Meenakshi Ganguly، "محدود کردن آزادی بیان، مبارزه با کووید-19 را تضعیف می‌کند"، (۲۰۲۱):
https://www.hrw.org/news/2021/02/24/limiting-free-speech-undermines-fight-against-covid-19

کاریکاتوریست‌ها و روزنامه‌نگارانی که به واکنش دولت به بحران کووید -۱۹ انتقاد کرده و کاریکاتور و مطالبی در این زمینه منتشر کرده‌اند، بر اساس این قانون به اتهام "انتشار تبلیغات، اطلاعات نادرست یا توهین‌آمیز و اطلاعاتی که می‌تواند نظم عمومی را مختل و ناآرامی ایجاد نماید" محکوم شده‌اند.[56]

گام هایی که برای مقابله با آسیب‌های آنلاین باید برداشته شود

این قسمت به رویکردهای عملی در مواجهه با آسیب های انلاین می پردازد

- **داستان را روایت کنید وبه دفاع از آن بپردازید.** ضمن اطمینان کامل از حفظ هویت قربانی یا بازماندگان، آسیب‌های آنلاین را شناسایی و به مطبوعات اطلاع دهید و یک کمپین حمایتی آغاز کنید. اغلب گزارش‌دهی در مورد آسیب‌های آنلاین محدود است که به گسترش این رفتارها کمک می‌کند.
- **چالش‌های حقوقی و قانونی داخلی را در نظر بگیرید.** بسیاری از قوانین جرایم سایبری در آسیا، به ویژه به دلیل ابهام و کلی بودن آنها، احتمالاً حقوق و آزادی‌های اساسی را نقض می‌کنند. در چنین مواردی، رجوع به دادگاه‌ها، به ویژه در نظام‌های دموکراسی مبتنی بر قانون اساسی می‌تواند راه‌حل مناسبی باشد.
- **به مکانیزم‌های سازمان ملل متحد متوسل شوید.** در مواردی که از قوانین جرایم سایبری برای نقض ناعادلانه حقوق و آزادی‌ها استفاده می‌شود و دادگاه‌های داخلی تمایلی به رسیدگی و ارائه راهکارهای مناسب نداشته‌اند، افراد یا گروه‌های متأثر می‌توانند امکان ارائه شکایت انفرادی به یک نهاد بین‌المللی صالح مانند کمیته حقوق بشر سازمان ملل متحد را بررسی کنند. برای ساکنان کشورهایی که صلاحیت نهاد طرف معاهده سازمان ملل را در خصوص شکایات انفرادی به رسمیت نشناخته‌اند، افراد همچنان می‌توانند نگرانی‌های خود را از طریق ارتباطات با گزارشگران ویژه سازمان ملل یا در موارد بازداشت‌های خودسرانه تحت قوانین امنیت سایبری، با کارگروه سازمان ملل در خصوص بازداشت‌های خودسرانه مطرح کنند (برای کسب اطلاعات بیشتر در مورد مکانیسم‌های سازمان ملل، به ماژول ۱۱ این دوره مراجعه کنید).
- **درخواست حکم قضایی موقت یا دائم یا دستور ممانعت از آزار و اذیت را در نظر بگیرید.** دستور قضایی موقت یا دائم یا حکم منع آزار و اذیت می‌تواند یک راه حل مدنی مناسب و کم‌هزینه باشد که در مواردی که رفتار جرم محسوب نمی‌شود اما بر حقوق فرد تأثیر منفی می‌گذارد، مؤثر و مفید است. این دستور یا حکم از آزار و اذیت شدن یک فرد توسط فرد دیگر جلوگیری می‌کند و نقض آن، جرم محسوب می‌شود که مجازات آن معمولاً جریمه نقدی یا حبس است. بسیاری از قوانین ضد آزار واذیت شامل آزار و اذیت آنلاین و زورگویی مجازی نیز می‌شوند. مثلاً قانون حفاظت در برابر آزار و اذیت در سنگاپور، برخی جرایم سایبری مانند "داکسینگ" (انتشار اطلاعات یا تصاویر شخصی با قصد آزار و اذیت و یا ایجاد خشونت) را نیز در بر می‌گیرد.[57]

---

[56] همان، همچنین مراجعه کنید به دیده‌بان حقوق بشر، "بنگلادش باید قانون امنیت دیجیتال که برای سرکوب منتقدان مورد استفاده قرار گرفته است را لغو کند"،(۲۰۲۰):
https://www.hrw.org/news/2020/07/01/bangladesh-repeal-abusive-law-used-crackdown-critics

[57] مراجعه شود به "راهنمای قانون حمایت در برابر آزار و اذیت (POHA) سنگاپور"، (۲۰۲۲):
https://singaporelegaladvice.com/law-articles/singapore-protection-harassment-act/

- **رفتار را به پلتفرم مربوطه گزارش دهید.** اغلب پلتفرم‌ها و شبکه‌های اجتماعی مکانیزم‌هایی برای گزارش رفتارهای غیرقانونی یا غیراخلاقی دارند که می تواند منجر به حذف محتوا یا اقدام علیه کاربر خاطی شود. قبل از گزارش، مرور شرایط و ضوابط استفاده از پلتفرم‌های مربوطه می‌تواند کمک کند تا شرط یا شرایطی که نقض شده است را به وضوح شناسایی کنید. این کار می‌تواند مؤثرتر بودن گزارش را تضمین کند.[58]

نتیجه‌گیری

اگرچه افزایش جرایم سایبری باید مورد توجه قرار گیرد، اما روند رو به رشد استفاده از قوانین جرایم سایبری برای سرکوب مخالفان و آزادی بیان عمیقا نگران کننده است. با اینکه اینترنت فضایی است که به سرعت در حال تحول و تکامل است، اما قوانین می‌توانند و باید به گونه‌ای طراحی شوند که شامل حمایت‌های خاصی در برابر آسیب‌های آنلاین هم در سطح فردی مانند تعقیب و آزار و اذیت‌های سایبری و هم در سطح اجتماعی مانند تنظیم جریان گردش اطلاعات و استفاده از داده‌های شخصی باشند. در این راستا، لازم است کشورهای آسیایی اطمینان حاصل نمایند که هرگونه اقدامی مطابق با استانداردهای حقوق بشری بین‌المللی از جمله عدم محدودیت غیرموجه آزادی بیان و حریم خصوصی باشد. رسانه‌ها و شبکه‌های اجتماعی نیز نقش مهمی در اطمینان از عدم استفاده از پلتفرم‌های خود برای انتشار محتوای غیرقانونی و مضر دارند. علاوه بر این، کشورها، شرکت‌های اینترنتی و جامعه مدنی نیز باید به طور فعال در افزایش سواد رسانه‌ای و دیجیتال، به ویژه آگاهی از ابزارهای موجود برای ارتقای امنیت ارتباطات آنلاین نقش داشته باشند.

---

[58] پلتفرم یا سیستم گزارش محتوای نامناسب و رفتارهای آزاردهنده در شبکه‌های اجتماعی:
فیس‌بوک: https://www.facebook.com/help/263149623790594
اینستاگرام: https://help.instagram.com/192435014247952
توییتر: https://help.twitter.com/en/rules-and-policies/twitter-report-violation
یوتیوب: https://support.google.com/youtube/answer/2802027?co=GENIE.Platform
تیک‌تاک: https://support.tiktok.com/en/privacy-safety/report-inappropriate-content-default.