دوفصلنامه ایرانی مطالعات سازمان ملل متحد
دوره ۵، شماره ۱،زمستان و بهار ۱۴۰۲
صص:۹۸-۱۱۰

کنوانسیون جرایم سایبری: گامی در جهت امنیت یا نقض حقوق بشر؟

حبیبه فرج‌زاده *

DOI: 10.22034/iruns.2024.213200

تاریخ دریافت:۲۰۲۴/۰۴/۱۳ تاریخ پذیرش:۲۰۲۴/۱۲/۰۶

چکیده

پیش‌نویس کنوانسیون مقابله با جرایم سایبری که نخستین سند جامع سازمان ملل متحد در زمینه مقابله با جرایم سایبری به شمار می‌رود و با هدف مقابله با جرایم سایبری و ارتقای همکاری بین‌المللی در این زمینه به تأیید نهایی رسیده است؛ طیف وسیعی از جرایم از جمله دسترسی غیرقانونی، شنود غیرمجاز، تخریب داده‌های الکترونیکی، سوءاستفاده جنسی از کودکان و پول‌شویی عواید ناشی از جرم را جرم‌انگاری می‌کند. بااین‌حال، نگرانی‌های حقوق بشری پیرامون این کنوانسیون از جمله اختیارات گسترده نظارتی، نبود پادمان‌های کافی برای حفاظت از حریم خصوصی و خطر نقض آزادی‌های اساسی به‌وضوح نمایان است. در متن کنوانسیون، اصول و موازین حقوق بشر به‌ویژه در زمینه آزادی بیان و حریم خصوصی به‌طور کامل لحاظ نشده و این موضوع می‌تواند به سوءاستفاده از این معاهده برای نظارت و سرکوب منجر شود. این مقاله تأکید می‌کند که برای جلوگیری از نقض حقوق بشر، ضروری است که مقررات دقیق‌تر و پادمان‌های حفاظتی مؤثرتری در این کنوانسیون گنجانده شود.

واژگان کلیدی: کنوانسیون جرایم سایبری، حقوق بشر، نقض حریم خصوصی، آزادی بیان، اختیارات نظارتی، همکاری بین‌المللی، پادمان‌های حفاظتی.

مقدمه

در دنیای امروز، جرایم سایبری به‌عنوان یکی از چالش‌های نوظهور، نظم و امنیت جوامع را به مخاطره انداخته است. در پاسخ به این چالش، تلاش‌های بین‌المللی برای تدوین قوانین و مقررات ناظر بر جرایم سایبری در جریان است. متن کنوانسیون جرایم سایبری به‌عنوان یکی از مهم‌ترین ابتکارات در این زمینه، در نهایت پس از پنج سال تلاش در تاریخ ۸ اوت ۲۰۲۴ به تأیید رسید و برای تصویب به صحن مجمع عمومی سازمان ملل ارسال شد.[1]

نیک می‌دانیم که رعایت اصول و موازین حقوق بشر در تدوین قوانین و مقررات کیفری از اهمیت بالایی برخوردار است. این اصول، چارچوبی برای تضمین عدالت و انصاف در نظام کیفری و حمایت از حقوق و آزادی‌های افراد در برابر نقض احتمالی آن‌ها از سوی دولت فراهم می‌کنند. اصولی همچون قانونی‌بودن، عدم تبعیض، اصل تناسب، ضرورت، اصل برائت، حق بر دادرسی عادلانه و غیره؛ اما تجربه نشان داده است به دلیل پیچیدگی‌ها و سرعت بالای تغییرات در فناوری‌ها و نقش آن‌ها در جوامع، همچنین به دلیل تعارضاتی که میان منافع مختلف مانند امنیت عمومی و آزادی‌های فردی وجود دارد و نامشخص بودن مرز تعادل میان آن‌ها، همواره قوانینی که برای مقابله با مجرمان و جرایم سایبری وضع شده است، اغلب خود به ابزاری برای کنترل و

---

[1] Draft United Nations convention against cybercrime. A/AC.291/L.15(7 August 2024), Retrieved from: https://documents.un.org/doc/undoc/gen/v24/055/06/pdf/v2405506.pdf?token=xFRKAOaIBUjLgw9c61&fe=true

فرآیند تدوین کنوانسیون جرائم سایبری، از دسامبر ۲۰۱۹ به پیشنهاد روسیه و با قطعنامه ۷۴/۲۴۷ مجمع عمومی آغاز شد. در این قطعنامه، مجمع عمومی تصمیم گرفت به‌منظور تدوین این کنوانسیون «کمیته‌ای اختصاصی» متشکل از تمام گروه‌های دولتی تشکیل دهد. این کمیته در سال ۲۰۲۱ و ۲۰۲۲ دو جلسه مقدماتی برگزار نمود و از تاریخ ۲۸ فوریه ۲۰۲۲ به‌صورت رسمی نشست مذاکراتی اول خود را برگزار نمود. نشست‌های مذاکراتی در ۶ مرحله و تا اوت ۲۰۲۳ ادامه پیدا کرد. در سال ۲۰۲۴ نیز دو جلسه جمع‌بندی برگزار شد و نهایتاً پس از پنج سال پیش‌نویس نهایی کنوانسیون در ۷ اوت ۲۰۲۴ تأیید و برای تصویب به مجمع عمومی ارسال شد.

سرکوب و نه ابزاری برای مقابله با این جرایم تبدیل شده‌اند و اتفاقاً در موارد بسیار، فعالیت‌های مبتنی بر حقوق اساسی افراد و یا فعالیت‌های ضروری برای دفاع از حیات انسانی بوده که از سوی مقامات کشورها در زمره جرایم سایبری و مورد پیگیرد قرار گرفته است.

به‌طورکلی، کنوانسیون جرایم سایبری به جرم‌انگاری طیفی از جرائم اصلی «وابسته به فضای سایبری» و تعداد محدودی از جرائم «تسهیل شده توسط فضای سایبری»[۲] پرداخته است و دولت‌ها را موظف می‌کند که قابلیت‌های تحقیقاتی و اجرایی دیجیتالی را توسعه دهند و این اختیارات جدید را در مورد سایر جرائم انجام‌شده با استفاده از شبکه‌های رایانه‌ای اعمال کنند. دسترسی غیرقانونی به سیستم‌های فناوری اطلاعات (ماده ۷)، شنود غیرمجاز داده‌ها (ماده ۸)، تخریب و تغییر عمدی داده‌های الکترونیکی (ماده ۹)، دخالت در عملکرد سیستم‌ها (ماده ۱۰)، تولید و توزیع دستگاه‌ها یا برنامه‌های مجرمانه (ماده ۱۱)، جعل داده‌های الکترونیکی (ماده ۱۲)، سرقت و کلاهبرداری مرتبط با فناوری اطلاعات (ماده ۱۳)، سوءاستفاده جنسی از کودکان و اغوای آنان برای ارتکاب جرم (ماده ۱۴ و ۱۵)، انتشار غیرمجاز تصاویر خصوصی (ماده ۱۶) و پول‌شویی ناشی از جرایم (ماده ۱۷) اقداماتی است که در این کنوانسیون جرم‌انگاری شده است.[۳]

اما کنوانسیونی که با هدف پیشگیری و مقابله با جرایم سایبری پایه‌ریزی شده و برای آینده اینترنت، حقوق بشر، آزادی‌های دیجیتال و مسیر آتی همکاری بین‌المللی و چندجانبه‌گرایی اهمیت اساسی دارد؛ ظاهراً به نگرانی‌ها در مورد جرم‌انگاری بیان و اختلاف عقیده، ایجاد اختیارات نظارتی گسترده و هموار نمودن سرکوب فرامرزی دامن زده است. به بیان دیگر، پیش‌نویس پیشنهادی که در اصل، هدف آن بهبود همکاری بین‌المللی برای پیشگیری و مقابله با جرایم

[۲] جرائم تسهیل شده توسط فضای سایبری یا غیر وابسته به فضای سایبری (Cyber-enabled crimes)، جرایم سنتی هستند که توسط اینترنت و فناوری‌های دیجیتال تسهیل می‌شوند.

[3] Draft United Nations convention against cybercrime. A/AC.291/L.15(7 August 2024)

سایبری است، اکنون به یک ابزار برای اعمال نظارت‌های گسترده، تضعیف آزادی بیان، نقض حریم خصوصی و سایر استانداردهای حقوق بشر تبدیل شده و تهدیداتی درباره تحقیقات ملی و بین‌المللی را ایجاد کرده است.

نقدها و نگرانی‌های حقوق بشری پیرامون کنوانسیون جرایم سایبری

یکی از این نگرانی‌ها اختلاف نظری است که در مورد دامنه جرایم این کنوانسیون وجود دارد؛ انتظار می‌رود که تمرکز کنوانسیون بر جرایم وابسته به فضای سایبر[4] باشد؛ یعنی جرایمی که در آن‌ها فناوری اطلاعات و ارتباطات هدف مستقیم و یا ابزار ارتکاب جرم هستند. اما ملاحظه پیش‌نویس کنونی نشان می‌دهد که از سه جهت این متن، گسترده‌تر از موارد مورد انتظار برای جرم‌انگاری است. نخست آنکه، فهرست جرایم در پیش‌نویس اصلاحی، فراتر از جرایم وابسته به فضای سایبر است. درعین‌حال، برخی از جرایم جدی و نگران‌کننده از جمله جرایم مربوط به‌افراط گرایی یا جرایم مرتبط با تروریسم را که نمایندگان برخی دولت‌ها پیشنهاد گنجاندن آن‌ها در متن را داده‌اند، شامل نمی‌شود. فقدان تعریف مورد توافق از این جرایم مهم نیز، ناگزیر، اعمال سرکوبگرانه نظیر تعقیب مخالفان سیاسی، مدافعان حقوق بشر، روزنامه‌نگاران و محدودیت‌های غیرقانونی بر آزادی بیان و اجتماع مسالمت‌آمیز را توجیه می‌کند.[5]

دیگر آنکه، تعریف ارائه شده از جرایم در این کنوانسیون «قصد مجرمانه» و «ضرر» را در خود ندارد. درواقع، معیارهایی که در حال حاضر در متن وجود دارند مانند «بدون مجوز»، «بدون داشتن حق» خطر تعقیب افراد به دلیل رفتارهایی که انتظار آسیب از آن رفتارها نمی‌رود یا اصلاً نمی‌توانستند موجب آسیب شوند را به دنبال خواهد داشت. بدین ترتیب اعمالی که با نیت نفع رساندن انجام می‌گیرند از جمله تحقیقات امنیتی، فعالیت‌های افشاگران یا روزنامه‌نگاری تحقیقی با

---

[4] Cyber-dependent crimes

[5] Tomaso Falchetta, "The Draft UN Cybercrime Treaty Is Overbroad and Falls Short On Human Rights Protection" (January 22, 2024), online: Just Security

تعقیب کیفری مواجه خواهند شد. اتفاقی که می‌تواند منجر به کاهش تمایل به چنین فعالیت‌های حیاتی شود و امنیت ارتباطات دیجیتال را تضعیف کند.[۶]

ایراد دیگری که جامعه مدنی و نهادهای حقوق بشری از جمله حریم خصوصی بین‌الملل[۷] به این متن وارد کرده‌اند آن است که نسخه جدید پیش‌نویس در دامنه تحقیق و پیگرد جرایم هم از مواردی که در معاهده آمده، فراتر رفته است. درواقع، بین جرایم مندرج در پیش‌نویس معاهده (فصل دوم) و دامنه اعمال اختیارات برای تحقیق در مورد جرایم و برقراری همکاری بین حوزه‌های قضایی ناهمگونی وجود دارد. مطابق متن فعلی، اختیاراتی که به سازمان‌های مجری قانون داده می‌شود بر رسیدگی به جرایم ارتکابی از طریق سیستم رایانه‌ای و جمع‌آوری شواهد الکترونیکی هر جرم کیفری اعمال می‌شود (ماده ۳۲,۲)[۸]. بنابراین دامنه کاربرد این معاهده از جرایم وابسته به فضای سایبری فراتر رفته است. این موضوع بی تردید این معاهده را به یکی از گسترده‌ترین معاهدات در امور کیفری و همکاری بین‌المللی در زمینه تحقیقات کیفری تبدیل می-کند.[۹]

---

[6] Ibid.

[۷] حریم خصوصی بین‌الملل (Privacy International) یک سازمان غیردولتی است که مقام مشورتی با شورای اقتصادی و اجتماعی سازمان ملل (ECOSOC) دارد. این سازمان با هدف مقابله با سوءاستفاده‌های دولت‌ها و شرکت‌ها از داده‌ها و فناوری فعالیت و تحقیقات جهانی انجام می‌دهد، به افشای آسیب‌ها و سوءاستفاده‌ها می‌پردازد، هم‌پیمانان جهانی را بسیج می‌کند، با همکاری عموم مردم برای یافتن راه‌حل‌ها تلاش می‌کند و به شرکت‌ها و دولت‌ها فشار می‌آورد تا تغییر کنند. این سازمان با نظارت گسترده دولت‌ها و شرکت‌ها مقابله می‌کند تا مردم در سراسر جهان بتوانند از طریق ارتقای حریم خصوصی فردی، امنیت و آزادی بیشتری داشته باشند.

[۸] ماده ۳۳ متن نهایی (۷ اوت ۲۰۲۴).

[9] Privacy International's Comments on the Revised Draft Text of the UN Cybercrime Convention (November 2023), retrieved at: Privacy International.pdf (unodc.org)

افزون بر این، پیش‌نویس کنوانسیون بدون اعمال محدودیت و پادمان‌های مؤثر حقوق بشری، به سازمان‌های مجری قانون اختیارات گسترده‌ای در تجاوز به حریم خصوصی می‌دهد. برای مثال، مقررات مربوط به شرح اختیارات جستجو و ضبط اطلاعات ذخیره شده در دستگاه‌های دیجیتال (بند ۴ ماده ۲۸) به گونه‌ای مقرر شده است که می‌تواند منجر به وادار کردن خدمات دهندگان مخابرات و اینترنت برای افشای نحوه ورود به نرم افزارها و یا فراهم کردن امکان دسترسی مقامات مربوطه به ارتباطات رمزگذاری شده شود که خطر هک دولتی و تضعیف رمزگذاری را به دنبال دارد و حریم خصوصی و امنیت ارتباطات دیجیتال را به خطر می‌اندازد.[۱۰]

یکی از نگرانی‌های اساسی، مسئله اشتراک‌گذاری فرامرزی داده‌ها بدون پادمان‌های حفاظتی مناسب است. این معاهده کشورها را ملزم می‌کند تا در جمع‌آوری و به‌اشتراک‌گذاری داده‌های خصوصی در سطح بین‌المللی، حتی برای جرایمی که به طور مستقیم به فناوری مرتبط نیستند، همکاری کنند. این رویکرد به دولت‌ها اجازه می‌دهد تا بدون درنظرگرفتن تدابیر کافی برای حفاظت از حقوق بشر، داده‌های حساس را به اشتراک بگذارند. به‌ویژه، نگرانی‌های حقوق بشری زمانی افزایش می‌یابد که کشورها می‌توانند داده‌های به‌دست‌آمده از طریق روش‌های نظارتی مداخله‌گرانه و سوءاستفاده آمیز را بدون محدودیت‌های لازم و کافی به اشتراک بگذارند که این خود می‌تواند به نقض گسترده حقوق بشر منجر شود.[۱۱]

---

[10] **28.4.** Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the information and communications technology system in question, the information and telecommunications network, or their component parts, or measures applied to protect the electronic data therein, to provide, as is reasonable, the necessary information to enable the undertaking of the measures referred to in paragraphs 1 to 3 of this article.

[11] Katitza Rodriguez, "The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy" (August 27, 2024), online: Just Security

مواد ۲۹ و ۳۰ کنوانسیون، جمع آوری فوری آمار ترافیک داده و رهگیری محتوای داده‌ها را مقرر کرده است که ویژگی مداخله‌جویانه این اعمال ایجاب می‌کند با مجموعه‌ای از محدودیت‌ها و تدابیر سختگیرانه اعمال شوند و به جرایم جدی حقوق بین‌الملل آن هم با مجوز قضایی پیشین با رعایت ضرورت و تناسب محدود گردند و بدین ترتیب کمترین تزاحم را با حریم خصوصی افراد داشته باشند. این در حالی است که ماده ۲۴ کنوانسیون که شرایط و تضمین‌هایی که کشورها باید برای حفظ حقوق بشر و رعایت اصول تناسب در اعمال اختیارات قانونی فراهم کنند را منعکس کرده است تنها در مورد آیین رسیدگی(دادرسی) اعمال می‌شود. همچنین برخی از شرایط و تضمین‌های مهم حقوق بین‌الملل بشر از جمله اصول قانونی بودن، ضرورت، مجوز قضایی قبلی و حق جبران مؤثر را در نظر نگرفته است.[۱۲]

افزون بر این، بند ۲ ماده ۲۴ با طرح تدابیر حفاظتی اختیاری و مشروط به قوانین داخلی، بسیاری از کشورها را از رعایت استانداردهای بین‌المللی معاف می‌کند. این مشکلات به‌ویژه در نظارت‌های مداخله‌گرانه مانند شنود ارتباطات و جمع‌آوری داده‌های ترافیکی برجسته است، جایی که بسیاری از کشورها نیاز به تأیید قضایی اولیه ندارند و حق اطلاع‌رسانی فردی به‌طور صریح در نظر گرفته نشده است. به این ترتیب، این ماده به‌جای ایجاد همکاری جهانی بر پایه تدابیر حفاظتی قوی، زمینه را برای سوءاستفاده از روش‌های نظارتی غیرقانونی و مخفیانه فراهم می‌آورد.

در مورد همکاری‌های بین‌المللی (فصل پنجم) نیز پیش‌نویس معاهده بسیار گسترده است و نه‌تنها جرایم مندرج در کنوانسیون بلکه جمع‌آوری، حفظ و به‌اشتراک‌گذاری اطلاعات الکترونیکی جرایم جدی را در برمی‌گیرد (ماده ۳۵). ماده ۳۶ انتقال داده‌های شخصی از حوزه

[12] Tomaso Falchetta, Supra note 6.

صلاحیت دولت را به قوانین داخلی و بین‌المللی قابل اعمال منوط کرده است.[۱۳] در این ماده تصریح شده است که اگر نمی‌توان داده‌ها را مطابق با قوانین مربوط به حفاظت از داده‌های شخصی ارائه کرد، کنوانسیون دولت‌های عضو را به انتقال داده‌های شخصی ملزم نمی‌کند. حال اگر قوانین ملی سازوکار مؤثری در قوانین ملی خود برای حفاظت مؤثر نداشته باشد از جمله برای تضمین هدف مشروع و ضرورت و فاقد سازکار نظارتی و جبران مؤثر باشد، این ماده حفاظت مؤثری از حقوق بشر به عمل نیاورده است. در مذاکرات ششمین نشست کمیته ویژه نمایندگان برخی دولت‌ها پیشنهاد کردند که اصول حفاظت از داده‌هایی که در نظر تفسیری کمیته حقوق بشر در مورد ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی، گزارش کمیساریای عالی حقوق بشر سازمان ملل در مورد حق حریم خصوصی در عصر دیجیتال و در قطعنامه‌های مجمع عمومی و شورای حقوق بشر در مورد حق حریم خصوصی در عصر دیجیتال مطرح شده اند در سند پیش نویس گنجانده شوند اما این پیشنهاد در پیش نویس ماده ۳۶ گنجانده نشد و بنابراین استاندارد واضح، دقیق، بدون ابهام و مؤثری به کشورهای عضو برای محافظت از داده‌های شخصی و جلوگیری از پردازش و انتقال داده‌ها به سایر کشورها به گونه ای که حق اساسی حریم خصوصی را نقض نکند، ارائه نشده است.[۱۴]

همچنین، بند ۱ ماده ۴۷ کنوانسیون، به نهادهای اجرای قانون کشورهای عضو اجازه می‌دهد از سیستم‌های پلیس پیش‌بینی‌کننده و پایگاه‌های داده بیومتریک برای تحلیل و تحقیقات جنایی

---

[۱۳] ماده ۳۶ کنوانسیون به حفاظت از داده‌های شخصی در فرآیند انتقال آن‌ها بین کشورهای عضو می‌پردازد و شرایط و الزامات این انتقال را بر اساس قوانین داخلی و تعهدات بین‌المللی کشورها تعیین می‌کند. این ماده تصریح می‌کند که اگر انتقال داده‌ها با قوانین مربوط به حفاظت از داده‌ها سازگار نباشد، دولت‌ها ملزم به انجام این انتقال نیستند و می‌توانند شرایطی برای تطابق با قوانین خود اعمال کنند. همچنین، برای انتقال داده‌ها به کشورهای ثالث، مجوز از دولت اصلی لازم است.

[14] Ibid.

استفاده کنند و اطلاعات حساس بیومتریک را به اشتراک بگذارند. این ماده همکاری نزدیک در اشتراک‌گذاری داده‌های لازم برای تحلیل و تحقیقات را الزام می‌کند، اما به دلیل ابهام در محدودیت‌های آن، خطر استفاده نادرست از این ابزارها برای نظارت و سرکوب وجود دارد. ابزارهای پلیس پیش‌بینی‌کننده و پایگاه‌های داده بیومتریک، به دلیل تهاجمی بودن و تمایل به تبعیض علیه جوامع به حاشیه رانده‌شده، می‌توانند به نقض حقوق بشر منجر شوند. اگرچه پیشنهاداتی برای پادمان‌های قوی‌تر در مذاکرات مطرح شد، این تدابیر در پیش‌نویس نهایی لحاظ نشده و بند۱ (c) ماده۴۷ راه را برای سوءاستفاده‌های احتمالی باز می‌گذارد. عدم اعمال استانداردهای حقوق بشری در این ماده، همراه با ارجاع به قوانین ملی بدون ایجاد تضمین‌های معنادار، موجب ضعف در حفاظت از داده‌های شخصی و حقوق بشر شده است.[۱۵]

نکته قابل‌اشاره دیگر اینکه درخواست‌های داده‌هایی که هدفشان پیگرد یا مجازات افراد به دلیل ویژگی‌های جمعیتی یا عقاید سیاسی آن‌هاست، از همکاری‌های بین‌المللی در کنوانسیون مستثنی شده است (ماده‌های ۴۰,۲۲ و ۳۷,۱۵) و به کشورها اجازه داده شده تا درخواست‌های فرامرزی را به دلایل اختیاری مانند حفظ حاکمیت یا نظم عمومی رد کنند (بند ۲۱ماده ۴۰). همچنین، بند ۸ ماده ۴۰ به کشورهای عضو این اختیار را می‌دهد که اصل دوگانه بودن جرم را به عنوان شرط همکاری اعمال کنند، به این معنا که کشورها می‌توانند در صورتی که جرم در قوانین داخلی‌شان با جرم مورد نظر در کشور درخواست‌کننده هم‌راستا نباشد، از همکاری خودداری کنند. با این حال، کنوانسیون هیچ الزامی برای ارزیابی فعالانه درخواست‌های داده‌ها از منظر نقض حقوق بشر نمی‌گذارد و بسیاری از دلایل رد درخواست، اختیاری هستند. به ویژه، اختیاری بودن اصل دوگانه بودن جرم نگران‌کننده است زیرا کشورها می‌توانند در تحقیقاتی که در یک کشور قانونی و در کشور دیگر جرم محسوب می‌شود، از همکاری امتناع کنند. این وضعیت به ویژه برای

[15] Rodriguez, Supra note 11.

جرایم مرتبط با محتوا یا مواردی که استانداردهای قانونی در آن‌ها متفاوت است، خطرناک است و منافع ژئوپلیتیکی ممکن است تصمیمات همکاری را تحت تأثیر قرار دهد. پیشنهادات برای آنکه جرایم سیاسی، مبنایی برای رد درخواست‌ها در نظر گرفته شوند، رد شد که به تضعیف قابلیت کنوانسیون در محافظت در برابر سوءاستفاده‌های سیاسی انجامیده است. همچنین، بند ۲ ماده ۶ و بند ۲۲ ماده ۴۰ درخواست‌های اشتراک‌گذاری داده‌های فرامرزی که حقوق بشر را نقض می‌کنند یا هدفشان مجازات فرد به دلیل عقاید سیاسی یا ویژگی‌های شخصی اوست را ظاهراً از دامنه کنوانسیون خارج می‌کنند، اما این مقررات فاقد تدابیر اجرایی لازم برای جلوگیری از سوءاستفاده‌های احتمالی هستند.[۱۶]

مورد مهم‌تر آنکه، ماده ۶ که بند ۲ آن اخیراً و در نسخه ۲ مه ۲۰۲۴ افزوده شد،[۱۷] به‌طور کلی به رعایت حقوق بشر اشاره دارد و تصریح می‌کند که هیچ‌چیز در این معاهده نباید به گونه‌ای تفسیر شود که سرکوب حقوق بشر یا آزادی‌های اساسی را مجاز بداند. هرچند این ماده با هدف اطمینان از سازگاری اجرای تعهدات کنوانسیون با تعهدات بین‌المللی حقوق بشری کشورها تدوین شده است و به‌عنوان یک تدبیر حفاظتی اصولی، کشورهای عضو را ملزم می‌کند تا از سوءاستفاده از این کنوانسیون برای سرکوب حقوق اساسی مانند آزادی بیان، عقیده و تجمع جلوگیری کنند؛ اما به‌طور مشخص پادمان‌ها و تدابیر حفاظتی کافی و مؤثری را که برای تضمین حفاظت واقعی از

---

[16] See: INFORMATION NOTE: Human rights and the draft Cybercrime Convention, Office of the High Commissioner for Human Rights, available at: https://www.ohchr.org/en/documents/tools-and-resources/human-rights-and-draft-cybercrime-convention

[17] Article 6. Respect for human rights 1. States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law. 2. Nothing in this Convention shall be interpreted as permitting suppression of human rights or fundamental freedoms, including the rights related to the freedoms of expression, conscience, opinion, religion or belief, peaceful assembly and association, in accordance and in a manner consistent with applicable international human rights law.

حقوق بشر ضروری است، در نظر نمی‌گیرد. از طرف دیگر، این ماده به قدری کلی و مبهم است که کشورهای عضو می‌توانند تفسیری ملی‌گرایانه از آن داشته باشند و بدون تعهد واقعی به حقوق بشر، به سرکوب حقوق اساسی ادامه دهند. ضعف در بند ۲ ماده ۶ به‌ویژه برای کشورهایی که پیش از این نیز تعهدات بین‌المللی حقوق بشری را نادیده گرفته‌اند، فرصت مناسبی برای سوءاستفاده از معاهده فراهم می‌آورد.[۱۸] به‌عبارت‌دیگر، بدون وجود تدابیر حفاظتی خاص و سازوکارهای نظارتی مؤثر، این ماده به‌تنهایی نمی‌تواند مانع از نقض حقوق بشر در چارچوب اجرای این معاهده شود و امکان سوءاستفاده از آن از سوی دولت‌های غیردموکراتیک را افزایش می‌دهد.[۱۹]

بنابراین، متن کنوانسیون تا به اینجا نه‌تنها موجب رفع نگرانی‌ها نشده بلکه به آن‌ها دامن زده است و به کشورها امکان تشکیل شبکه گسترده‌تری برای دسترسی به داده‌های ذخیره شده از سوی شرکت‌های واقع در خارج از قلمروی کشورها می‌دهد که قوانین حریم خصوصی کشورهای دیگر را نقض می‌کند. دامنه آن از جرایم سایبری که به طور خاص در کنوانسیون تعریف شده‌اند فراتر می‌رود و فهرستی طویل از جرایم غیرسایبری را نیز در بر می‌گیرد.[۲۰] روزنامه‌نگاران و اقشار آسیب‌پذیر دیگر با این خطر مواجه‌اند که تحت پیگرد و تحقیق و خطر استرداد به‌خاطر اِعمال حقوق اساسی بشر از طریق فناوری دیجیتال قرار گیرند.[۲۱]

نگرانی اصلی آنجاست که اگر این معاهده همین‌گونه که هست تصویب شود، قوانین کیفری کشورها را تحت‌تأثیر قرار خواهد داد و اختیارات گسترده‌ای را برای تحقیقات کیفری داخلی و

---

[۱۸] بند (۲) ماده ٦: «هیچ چیزی در این کنوانسیون نباید به گونه‌ای تفسیر شود که اجازه سرکوب حقوق بشر یا آزادی‌های اساسی را بدهد.»

[19] Rodriguez, supra note 11.

[20] Katitza Rodriguez, "Latest Draft of UN Cybercrime Treaty Is A Big Step Backward" (December 1, 2023), online: Electronic Frontier Foundation

[21] "As negotiations continue, the proposed UN Cybercrime Convention must not become a tool to undermine press freedom" (February 13, 2024), online: Committee to Protect Journalists

بین‌المللی به نیروهای دولتی اعطا خواهد کرد. زبان مبهم و مقررات گسترده، خطر پیگرد محققان امنیتی که ممکن است برای مقاصد عام‌المنفعه به تحقیق و دورزدن اقدامات امنیتی و کسب اطلاعات اقدام کنند را به دنبال دارد.

نتیجه گیری

با این اوصاف، پیش‌نویس کنوانسیون کاستی‌های زیادی از منظر موازین حقوق بین‌الملل بشر دارد و آزادی بیان، حریم خصوصی و دیگر حق‌های بشری را به خطر می‌اندازد. این پیش‌نویس با دامنه‌ای گسترده‌تر از مقابله با جرایم سایبری، زمینه به‌اشتراک‌گذاری فرامرزی اطلاعات و الزامات همکاری را فراهم ساخته و امنیت آنلاین افراد را کاهش می‌دهد. این معاهده می‌تواند نقش سازمان ملل در صیانت از حقوق بشر را زیر سؤال ببرد و نوید استفاده ابزاری گروهی از کشورها از سازمان ملل به‌عنوان ابزار و توجیهی برای نظارت و سرکوب باشد.

حال که کنوانسیون با تمامی این نگرانی‌ها در آستانه طرح در مجمع‌عمومی ملل متحد است؛ در صورت تصویب، ثمری جز نقض حقوق بشر نخواهد داشت و مقابله با جرایم سایبری به قیمت حقوق بشر و حیثیت افراد تمام خواهد شد. ضروری است برای جلوگیری از احتمال سوءاستفاده از مفاد کنوانسیون به بهانه مقابله با جرایم سایبری، تعاریف دقیق و محدود از جرایم سایبری به عمل آید و این تعاریف فقط شامل اقداماتی شود که به‌طورجدی امنیت سایبری را تهدید می‌کنند. پادمان‌ها و محدودیت‌های قوی و مؤثر ایجاد شود که شوربختانه متن کنونی فاقد آن‌هاست. نمایندگان دولت‌ها باید به دنبال چاره برای گنجاندن مقرراتی باشند که تضمین نماید افشاگران، روزنامه‌نگاران و مدافعان حقوق بشر به‌خاطر فعالیت‌های مشروع خود تحت تعقیب و پیگرد قرار نگرفته و فعالیت‌هایی که به نفع عموم است به مخاطره نمی‌افتد.

نکته پایانی آنکه، اصول حفاظت از داده‌ها که به‌ویژه در جلسه ششم کمیته موقت مورد تأکید نمایندگان برخی دولت‌ها قرار گرفت و موازین دیگر حقوق بشر از جمله اصول عدم تبعیض، قانونی‌بودن هدف مشروع، ضرورت و تناسب بر مقررات کنوانسیون نظارت دارد. تدابیر دیگر نیز،

از جمله اصل مجوز قضایی قبلی برای در دسترس قراردادن یا به‌اشتراک‌گذاری داده‌ها و انجام تحقیقات فرامرزی مطابق با حاکمیت قانون باید اندیشیده شود. هرگونه مقرره نظارتی که می‌تواند در تضعیف امنیت افراد و رمزگذاری مورد سوءاستفاده قرار گیرد، نباید زیر پرچم کنوانسیون مقابله با جرایم سایبری به مجوزی برای نقض حقوق بشر تبدیل شود. در نهایت، لازم و ضروری است که مکانیسم‌های نظارتی قوی و مؤثر برای نظارت بر اجرای کنوانسیون جرایم سایبری و تضمین انطباق آن با حقوق بشر ایجاد شود.