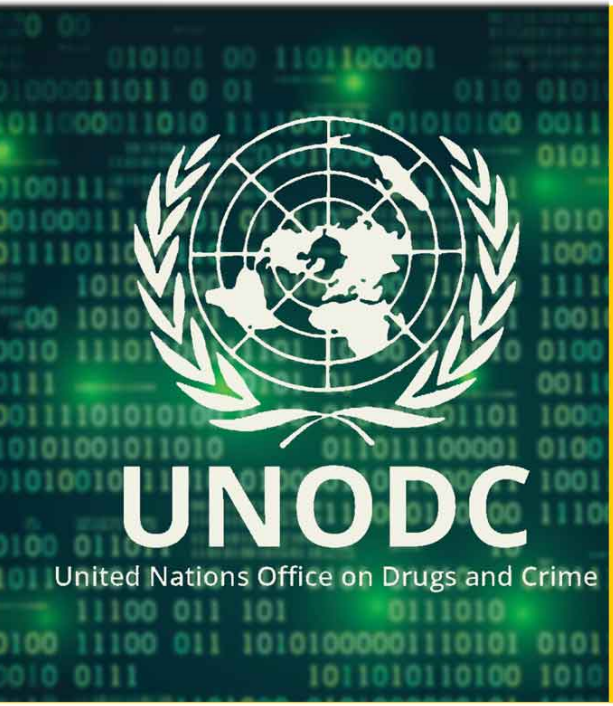
مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

گزارش سریع
سی و نهم



تحلیل و بررسی طرح کنوانسیون مبارزه با جرائم سایبری

Analysis and review of the draft on convention of fighting against cybercrime

بسم الله الرحمن الرحیم

گزارش سریع

گزارش شماره ۳۹
اردیبهشت ۱۴۰۱

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

تحلیل و بررسی طرح کنوانسیون مبارزه با جرائم سایبری

گزارش سریع که با عنوان Rapid Report شناخته می‌شود، نوعی گزارش کوتاه است که صرفاً برای اطلاع کلی از موضوع یا پدیده‌ای خاص در بازه زمانی محدود تهیه می‌شود. هدف عمده چنین گزارش‌هایی ایجاد تصویری اجمالی برای آشنایی ابتدایی سیاست‌گذاران و برنامه‌ریزان در موضوعات مورد علاقه آنان است.

تهیه شده در پژوهشگاه فضای مجازی
(گروه مطالعات حقوقی و مقرراتی فضای مجازی)

تهیه‌کننده: امیرعباس رکنی (کارشناسی ارشد حقوق جزاوجرم‌شناسی دانشگاه علوم‌قضایی)
ناظر علمی: سید امین پیشنماز (دانشجوی دکتری حقوق خصوصی دانشگاه شهید بهشتی)
محمدمهدی نصر هرندی (مدیر گروه مطالعات اخلاقی فضای مجازی)

نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶ غربی، پلاک ۲۰
تلفن: ۸۶۱۵۱۰۶۱-۰۲۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

فهرست

سخن نخست

سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سیدابوالحسن فیروزآبادی

دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

چکیده

چکیده

با گذشت بیش از بیست سال از تصویب کنوانسیون جرائم سایبری بوداپست، جامعه جهانی دست‌به‌گریبان با جرائم سایبری، شاهد اقدامی جدید، کارآمد و متناسب با جرائم نوپدید و شدید سایبری و به‌روزرسانی سیاست کیفری رژیم حقوق بین‌الملل در پاسخ به این نوع از جرائم خطرناک نبوده است. دولت فدراسیون روسیه با درک صحیح از نیاز مبرم جهان به ارتقای نظام کیفر گذاری بین‌المللی جرائم سایبری و با هدف جلوگیری از رشد فزاینده جرائم سایبری در عرصه بین‌الملل، اقدام به طراحی یک کنوانسیون جهانی جهت مبارزه با جرائم سایبری نموده است. طرح پیشنهادی دولت روسیه به سازمان ملل متحد، حاوی نوآوری‌ها و نکات قابل‌توجهی است که می‌تواند در سیاست‌گذاری‌های داخلی نیز مورد توجه قرار بگیرد. نمایندگان کشورهای عضو سازمان ملل، بنا بر سیاست‌های ملی و بین‌المللی، ملاحظات فنی و رابطه خود با کشور روسیه واکنش‌های مختلفی به این طرح ارائه داده‌اند. برخی از کشورها همچون ایالات‌متحده آمریکا با برخی از ابعاد این طرح مخالفت کرده و برخی از کشورها نیز با روسیه هم‌نظر هستند. بااین‌حال، برجستگی‌های معتنابه این طرح در نهایت منجر به این شده است که کمیته موقت

تدوین کنوانسیون بین‌المللی جامع سازمان ملل در مورد مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد جنایی چندین جلسه در سال ۲۰۲۲ تشکیل دهد و با یک‌صدا کردن کشورهای مختلف جهان در مسیر مبارزه با جرائم سایبری، گامی جدید و استراتژیک در ایجاد یک رژیم حقوقی بین‌المللی حاکم بر فضای مجازی بردارد. در نوشتار پیش رو، با در نظر داشتن متن اصلی کنوانسیون که ترجمه آن ضمیمه این گزارش شده‌است، مروری بر زمینه‌ها و دلایل اهمیت تصویب این کنوانسیون، رویکرد کشورهای مختلف به پیشنهاد روسیه، ابعاد مهم این طرح و دامنه جرم انگاری در آن انجام خواهد شد. نتیجه حاصل از این نوشتار، نهایتا ثابت می‌کند که با مد نظر قرار دادن چند ذی نفعی بودن فضای اینترنت و حضور بازیگران مختلف و با منافع متعارض در این بستر، ضروری به نظر می رسد تا دولت-ملت‌ها در موسع‌ترین معنا و دامنه خود، در راستای تداوم جریان تامین منفعت همگانی و ایجاد یک خیر عمومی، در مسیر ایجاد یک نظام حقوقی چند ذی نفعی، تنظیم‌گر و بازدارنده گام برداشته و منافع ناشی از امنیت جمعی سایبری را به عنوان نظم امنیتی جدید در جهان سایبر به رسمیت بشناسند.

واژگان کلیدی: جرائم سایبری، کنوانسیون، سازمان ملل، حقوق بین‌الملل، روسیه

مقدمه

مقدمه

بعـد از پایـان جنـگ جهانی دوم و شـکل‌گیری سـازمان ملل متحد، جامعه بین‌المللـی بـه ایـن نتیجـه رسـید کـه برخـی از موضوعـات بنـا بـر ماهیت و ذات خـود، پتانسـیل تبدیـل بـه معضـلات همه‌گیـر و چالـش آفریـن دارنـد. بـر همیـن اسـاس، علی‌رغـم آنکـه جهـان در تاریـخ سیاسـی معاصـر خـود منازعـات مختلفـی همچـون دوقطبـی شـدن شـرق و غـرب، جنـگ سـرد و کنش‌هـای جنگی و میان جنگی متعددی را پشـت سـر گذاشـته اسـت، برای فائـق آمـدن بـر چالش‌هایـی کـه در قامت یـک تهدید وجـودی علیـه امنیت ملـی و جمعـی خودنمایـی می‌کنـد، بـه سـمت راه‌حل‌هـای متکـی بـر جمع سـپاری و مشـارکت حداکثـری اعضای جامعـه بین‌المللی حرکت کرده اسـت. مـواردی همچـون قاچـاق مـواد مخـدر، اسـلحه و انسـان، پول‌شـویی، تأمیـن مالی تروریسـم، محدودسـازی اسـتفاده از تسـلیحات هسـته‌ای و شـیمیایی و جرائـم سـازمان‌یافته مـواردی از ایـن قبیل هسـتند. رشـد و توسـعه روزافزون فنـاوری و تبدیل‌شـدن اینترنـت بـه یـک کالای همگانـی و نیاز اولیـه زندگی بشـر، هرچنـد کـه تأثیـرات چشـم‌گیری برافزایـش کیفیـت زندگـی فـردی و اجتماعـی انسـان‌ها داشـته و عوایـد مـادی و معنـوی ناشـی از آن بـر تمـام سـطوح و شـئون زندگـی بشـریت اثر گذاشـته، اما از سـوی دیگر، ایـن امر نیز

حقیقتی انکارناپذیر است که چالش‌های مختلفی نیز برای افراد و دولت‌ها به همراه داشته و دارد؛ و از سوی دیگر، با تبعیت از ویژگی اساسی فناوری که همان پیشرفت و تحول لحظه‌به‌لحظه است، این چالش‌ها نیز به شکلی مستر پیشرفت کرده و گسترش می‌یابد. از همین رو، کارشناسان و صاحب‌نظران امنیتی، تهدیدات و معضلات ناشی از اینترنت را در قالب تهدیدات امنیتی نوظهور طبقه‌بندی می‌کنند و کارگزاران دولتی را به این امر مهم رهنمون می‌سازند که باید در راستای کنترل و مدیریت این چالش حرکت کنند.

مسلم امر آن است که نخستین گام در این خصوص همانند هر امر دیگری که مربوط به زندگی اجتماعی است، در سطح ملی برداشته می‌شود و دولت‌ها با قانون‌گذاری داخلی، در مسیر کنترل و مدیریت شرایط گام برمی‌دارند؛ اما ازآنجایی‌که اینترنت و چالش‌های آن دارای یک حوزه وجودی محدود نیستند و سرتاسر جهان را درنوردیده و جهان تحت سلطه خود را تبدیل به یک کلیت واحد می‌کنند، کنترل و مدیریت آن نیز در چنین مقیاسی نیازمند استقرار یک رژیم حقوقی جهانی هست. با در نظر داشتن این امر، توجه به چند نکته از اهمیت بسزایی برخوردار است؛ نخست آنکه اینترنت و نظام بین‌الملل هر دو جزو مفاهیم آنارشیک هستند. این آنارشیک بودن، به تعبیر باری بوزان[1] بنیان‌گذار مکتب امنیتی کوپنهاگ، نه به معنی بی‌نظمی و آشوب هابزی است، چراکه در اینجا سطح تحلیل هر دو مفهوم روابط بین آدمیان نیست و آنارشیک بودن نظام بین‌الملل و اینترنت به معنای فقدان حکومت مرکزی است. اگرچه این امر نیز به‌نوبه خود به معنای فقدان خود حکومت نیست؛ زیرا حکومت‌ها در نظام بین‌الملل و اینترنت در درون واحدهای سیستم

1. Barry Buzan

جای دارند. بر همین مبنا، ازآنجایی‌که در جهان نمی‌توان هیچ اقتدار سیاسی بالاتر از دولت دارای اقتدار حاکمیت یافت، سیستم سیاسی مرکب از دولت‌های دارای حاکمیت، ساختاری همراه با آنارشی سیاسی خواهد بود. نکته مهم دیگر آن است که هنگامی‌که دنبال تأمین امنیت در محیط آنارشیکی همچون اینترنت هستیم، نیازمند تعیین مرجع امنیت هستیم. چراکه در این مقام، مهم‌ترین پرسشی که باید پاسخ داده شود عبارت از این است که امنیت چه چیزی قرار است تأمین شود؟ در پاسخ باید گفت که مکاتب سیاسی-امنیتی متقدم و متأخر رهیافت‌های گوناگونی در این زمینه دارند. یکی از پاسخ‌های متداول و متعارف آن است که امنیت دولت‌ها باید در این فضای آنارشیک تأمین شود، اما به دلایلی که در ادامه مطرح خواهد شد، به‌زودی خواهیم فهمید که این پاسخ سطحی برای این پرسش به‌هیچ‌وجه کافی به نظر نمی‌رسد. دولت‌ها ابژه‌هایی بی‌شکل، چندوجهی و جمعی هستند که امنیت را از راه‌های مختلفی می‌توان بدان اطلاق کرد، از سوی دیگر باید توجه داشت که دولت‌ها زیادند و امنیت یکی را نمی‌توان بدون ارجاع به دیگران موردبحث و بررسی قرارداد. جستجو برای یافتن مرجع امنیت در اینترنت، سرانجام ما را به این نقطه می‌رساند که امنیت می‌تواند مراجع بالقوه زیادی داشته باشد. این مرجع‌ها نه‌تنها با افزایش تعداد اعضای جامعه دولت‌ها بیشتر می‌شود، بلکه از سطح دولت‌ها به سطح افراد پایین آمده و نیز از آن فراتر رفته تا سطح سیستم بین‌المللی به‌عنوان یک کل بالا می‌رود. چون امنیت هر مرجع، در انزوای از دیگران قابل حصول نیست و امنیت هرکدام به‌صورت شرطی برای امنیت همگان درمی‌آید[1]. این مراجع امنیت نیز به انواع و اقسام گوناگونی تقسیم می‌شوند، اما بر اساس یک تقسیم‌بندی معروف و

۱. بوزان، باری، مردم، دولت‌ها و هراس، پژوهشکده مطالعات راهبردی، چاپ ششم، تهران، ص ۳۹.

تقریباً پذیرفته‌شده در میان اکثر مکاتب امنیتی مدرن، مراجع امنیت را در سه سطح افراد، دولت‌ها و نظام بین‌المللی می‌توان طبقه‌بندی کرد. درنهایت، بر اساس آنچه گذشت، باید توجه داشت که هر زمان که به دنبال تأمین امنیت در فضای آنارشیک هستیم، باید به این امر توجه داشته باشیم که رهایی از تهدید، با برقراری امنیت جمعی میسر خواهد بود و چنانچه هر یک از مراجع و سطوح تحلیل دچار ناامنی یا حتی احساس ناامنی شوند، بر اساس نظریه آشوب، کل سیستم دچار آشوب شده و تمامی سطوح و مراجع درگیر خواهند شد. این امر، آنجا پدیدارتر می‌شود که به این نکته مهم توجه کنیم که اینترنت همانند نظام بین‌المللی، یک مفهوم چند ذی‌نفعی است و نمی‌توان صرفاً برای آن ذی‌نفعی در یک سطح در نظر گرفت. این ویژگی اخیر نیز همانند آنارشیک بودن جزو شباهت‌های اینترنت و نظام بین‌المللی است.

کنوانسیون‌های بین‌المللی متداول‌ترین ابزار ایجاد قوانین با استانداردهای بین‌المللی هستند که دولت‌ها و سایر بازیگران جامعه جهانی باید از آن‌ها پیروی کنند. در طول چند دهه اخیر، اهمیت کنوانسیون‌ها در چارچوب حقوق بین‌الملل به‌شدت افزایش‌یافته است. در حقوق بین‌الملل مدرن، اهمیت معاهدات بین‌المللی در ایجاد قواعد بین‌المللی خود را نمایان ساخته است. از تأثیرات مهم کنوانسیون‌ها می‌توان به ایجاد نهاد ها یا سازوکارهای بین‌المللی به‌منظور اجرای قوانین بین‌المللی اشاره نمود. بااین‌وجود، بسیاری از نظریه‌پردازان کلاسیک حقوق بین‌الملل کیفیت اجرای کنوانسیون‌ها را به‌عنوان یک نقطه‌ضعف و محل مناقشه شناسایی کرده‌اند. اغلب گفته می‌شود که حقوق بین‌الملل به دلیل نبود مکانیسم و ضمانت اجرا، نتوانسته است تأثیر مطلوبی از خود به‌جای گذاشته

و رسالت ذاتی خود را انجام دهد؛ اما به نظر می‌رسد آنچه در طول دهه‌های گذشته در اثر روند رو به رشد انعقاد کنوانسیون‌های متعدد در زمینه موضوعات مهم و حساس بین‌المللی پیش‌آمده است، مکانیسم‌های استواری به‌منظور اجرای قواعد پذیرفته‌شده جهانی ایجاد کرده است.

نکته مهم دیگری که در خصوص کنوانسیون‌ها قابل‌ذکر است، تبعیت این معاهدات از مفهوم حاکمیت است. حقوق بین‌الملل بر این باور است که هیچ اقدامی را نمی‌توان بدون یا برخلاف میل یک کشور مستقل انجام داد. به‌بیان‌دیگر، علی‌رغم آنکه معاهدات بین‌المللی کشورها عضو و حتی غیر عضو را ملزم به ایفای تعهدات و انجام تکالیف خاصی می‌کنند، توانایی وارد آوردن خدشه به تمامیت یک نشان سیاسی را ندارد. در واقع، معاهدات بین‌المللی نقطه تلاقی محدودیت در حاکمیت و حمایت از حاکمیت هستند. در این گفتمان، مهم‌ترین هدف حقوق معاهدات بین‌المللی، تنظیم گری موضوعات مشخص است و به دنبال آن فضایی ایجاد می‌گردد که در آن استفاده از زور در امور بین‌المللی منتفی شده و جای خود را به‌حق و تکلیف می‌دهد؛ بنابراین، حاکمیت دولت همواره یکی از نقاط ثقل حقوق بین‌الملل است و نمی‌توان انتظار داشت که یک معاهده مقرراتی را پیش‌بینی کند که بر حاکمیت یک دولت تأثیر منفی بگذارد. انعقاد معاهدات، جزء مهم‌ترین شیوه‌های ایجاد و تکامل رژیم حقوق بین‌الملل است. ازآنجایی‌که فرایند انعقاد معاهده بستری برای بحث و مشورت آگاهانه درباره موضوعاتی که باید چاره‌ای برای آن تمهید شود را ایجاد می‌کند، اعتقاد بر این است که خروجی نهایی این بستر تعاملی، ملموس‌ترین و کاربردی‌ترین قواعد را در مورد آن موضوع ارائه می‌کند. درنتیجه، باید گفت که وضع قوانین بین‌المللی از طریق انعقاد

معاهد، مطلوب‌ترین شیوه تولید قوانین بین‌المللی است.

افزایش شدت حملات سایبری مخرب در طول سال‌های گذشته، فرار مجرمان سایبری از چنگال عدالت، اثرپذیری قابل‌توجه امنیت داخلی، امنیت ملی و امنیت بین‌المللی از جرائم سایبری و بسیاری دیگر از عوامل تحت تأثیر جرائم سایبری، اهمیت چاره‌اندیشی در خصوص مبارزه با جرائم سایبری را بیش از هر زمان دیگری در میان رهبران جهان برانگیخته است. در دسامبر سال ۲۰۱۴ میلادی، هنگامی باراک اوباما، رئیس‌جمهور وقت ایالات‌متحده آمریکا در مقابل دوربین‌ها علناً کره شمالی را به هک کردن سونی پیکچرز متهم کرد، به‌وضوح مشخص گردید که ضرورت تأمین امنیت سایبری جمعی به اوج اهمیت خود رسیده است. اصولاً تعداد کمی از مسائل سیاسی در جهان وجود دارد که تمامی رهبران جهان را متفق‌القول می‌کند؛ اما جرائم سایبری و اثرپذیری امنیت سایبری به دنبال این جرائم، تنها در عرض چند سال از نخستین تلاش‌های کارشناسان برجسته‌ای همچون ریچارد کلارک[1]، نویسنده رساله جنگ سایبری[2]، توانست با جلب نظر رئیس‌جمهور آمریکا، منجر به توافق میان چین و آمریکا و بیانیه معروف گروه ۲۰ در سال ۲۰۱۵ و تأکید بر لزوم ایجاد هنجارهای امنیت سایبری گردد.

جهان به‌وضوح متوجه شده است که باید در خصوص مدیریت اینترنت و مبارزه با مجرمان ناشناس آن چاره‌ای اضطراری بی اندیشد. از زمان تجاری‌سازی اینترنت در اواسط دهه ۱۹۹۰ میلادی، اینترنت به‌سرعت در میان مردم گسترش یافت. در اوایل قرن ۲۱ بیش از یک‌سوم جمعیت جهان به این فناوری دسترسی داشتند و اکنون در سال ۲۰۲۲ آمارها حکایت از آن دارد که بیش از چهار و نیم میلیارد نفر در جهان به اینترنت

1. Richard Clarke
2. Cyber War monograph

دسترسی دارند[1]. درنتیجه این افزایش سریع دسترسی کاربران به اینترنت، انگیزه‌های اقتصادی و سیاسی برای بهره‌برداری مخرب و غیرقانونی از شبکه نیز به‌سرعت افزایش پیدا می‌کند و اعمال مجرمانه شکل جدیدی به خود می‌گیرند. به‌موازات نگرانی رهبران جهان، پژوهش‌ها و مطالعات مجموعه‌های دانشگاهی، سیاسی و نظامی نیز در طول این سال‌ها چند برابر شده است. محققان و صاحب‌نظران روابط بین‌الملل به‌ویژه شاخه‌های مطالعات امنیتی و مطالعات استراتژیک به شکل فزاینده‌ای بر پیامدهای جرائم سایبری بر امنیت ملی و بین‌المللی تأکید می‌کنند. خروجی علمی این مجموعه‌های مطالعاتی بر تأثیر اینترنت بر مفاهیمی مانند قدرت، حاکمیت، حکمرانی جهانی و امنیتی سازی است. در میان طیف گسترده‌ای از تهدیدات و خطرات سایبری، جرائم سایبری در کانون توجهات قرارگرفته و آثار آن بر مفاهیم پیش‌گفته، آن را هم‌طراز موضوعاتی همچون تروریسم سایبری، جنگ سایبری، جاسوسی سایبری قرار داده است.

درحالی‌که محققان پیامدهای جرائم سایبری بر امنیت ملی و بین‌المللی را به طرز فزاینده موردتوجه قرار می‌دهند، همچنان در مورد سطح و ماهیت این تهدید و همچنین سیاست‌های مناسبی که دولت‌ها و سایر ذی‌نفعان اینترنت باید اتخاذ کنند، اختلاف‌نظر دارند. تلاش‌های ملی و بین‌المللی، بر تدوین قوانین تخصصی حاکم بر فضای سایبری، شناسایی خلأهای قانونی، توسعه هنجارها و عرف‌های سایبری، اعتمادسازی، بازدارندگی و از همه مهم‌تر ایجاد یک رژیم حقوق سایبری بین‌المللی متمرکز است. جوزف نای[2]، دانشمند و پژوهشگر سیاسی اهل ایالات‌متحده در این خصوص معتقد است که یک مجموعه رژیم امنیت سایبری تکامل‌یافته شامل چندین نهاد منطقه‌ای و بین‌المللی است

1. Internet users in the world 2021 | Statista. (2022). Retrieved 3 April 2022, from https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=How20%many20%people20%use20%the,the20%internet20%via20%mobile20%devices.
2. Joseph Nye

کـه نقش‌هـای محـوری و کلیـدی در شـکل‌دهی واکنش‌هـای سیاسـتی ایفـا می‌کننـد. ازنظـر نـای، در جهـان کنونـی اینترنـت همه‌جـا و همه‌چیـز را در برگرفتـه و پیشـرفت‌های فنـاوری تاکنـون از توانایی نهادهـای حاکمیتی برای پاسـخگویی و مدیریـت پیشـی گرفتـه اسـت. او بـا تمایـز قائـل شـدن میـان حکمرانـی اینترنتـی و حکمرانی سـایبری، اعتقـاد دارد کـه حکمرانی اینترنت در قلـب فضـای مجـازی قـرار دارد و تنها یکـی از زیرمجموعه‌هـای حکمرانی سـایبری است.

سیاسـت کیفـری و سیاسـت جنایـی، اکنون یکی از مهم‌تریـن ضرورت‌های حکمرانـی سـایبری اسـت. جرائـم و مجرمـان سـایبری روزبـه‌روز بیشـتر و خطرناک‌تـر می‌شـوند و بـا بهره‌منـدی از ویژگـی فرامـرزی اینترنـت، دامنـه اثرگـذاری خـود را بسـیار وسـیع کرده‌انـد. همان‌طـور کـه اشاره‌شـده، صاحب‌نظـران در خصـوص نحـوه پاسـخ‌دهی مناسـب بـه جرائـم سـایبری همچنـان اتفاق‌نظـر پیـدا نکرده‌انـد، امـا شـکل‌گیری نظم‌هـای امنیتـی منطقـه‌ای و جهانـی، تنها راه پیش روی بشـر را انعقاد یک کنوانسـیون فراگیر و دارای ضمانـت اجـرای قـوی قـرار داده اسـت. اولیـن تـلاش جهـان بـرای انعقـاد یـک کنوانسـیون به‌منظـور مبـارزه بـا جرائـم سـایبری، بـه سـال‌های ابتدایـی ۲۱ بازمی‌گـردد. کنوانسـیون جرائم سـایبری معروف به «کنوانسـیون جرائـم سـایبری بوداپسـت» نخسـتین معاهـده بین‌المللـی اسـت کـه بـه جرائـم رایانـه‌ای و اینترنتـی می‌پـردازد و می‌کوشـد قوانیـن ملـی را سـازگار کـرده، روش‌هـای تحقیقـات را ارتقـا دهـد و همـکاری بیـن کشـورها را بهبود بخشـد. ایـن کنوانسـیون توسـط شـورای اروپـا در سـال ۲۰۰۱ ارائه شـد و از ۲۳ نوامبـر ۲۰۰۱ کشـورها می‌توانسـتند آن را امضـا کننـد. از ابتـدای ژوئیـه ۲۰۰۴ کنوانسـیون بـه اجـرا درآمـد. بااین‌حـال، ایـن کنوانسـیون بـه دلایـل

مختلفی نتوانست آن‌چنان‌که انتظار می‌رفت مؤثر واقع شود. نخستین و اصلی‌ترین دلیل این امر، ناشی از این نکته مهم است که مرجع تصویب این کنوانسیون شورای اروپا است و از همین رو سطح مقبولیت پایین‌تری نسبت به کنوانسیون‌های سازمان ملل دارد. از سوی دیگر، نزدیک به بیست سال از نگارش اولیه و تنظیم متن این کنوانسیون گذشته و طبیعی است که پاسخگوی چالش‌های کنونی جاریم سایبری و سرعت رشد فزاینده آن را نداشته باشد. عدم مشارکت کشورهای غیراروپایی در تهیه پیش‌نویس متن این کنوانسیون و اعمال نظرات آن‌ها نیز ازجمله دیگر دلایل کاهش مقبولیت این کنوانسیون است.

با توجه بر آنچه گفته شد، یک نیاز شدید به سندی اجماع ساز میان کشورهای مختلف جهان که با ایجاد وحدت رویه، نقشه راه مبارزه با جرائم سایبری را مشخص سازد، به‌شدت احساس می‌شود. دولت فدراسیون روسیه، به‌عنوان یکی از کشورهای ابرقدرت جهان که نظام حکمرانی سایبری مختص به خود را داشته و از شخصیت‌های حقوقی مؤثر در جهان واقع و سایبر است، به‌خوبی این احساس نیاز را درک کرده و بر همین اساس، به دستور دادستان کل روسیه، جمعی از حقوق دانان، کارشناسان و متخصصان روسی چند سالی است که موظف به تهیه و تنظیم متن یک کنوانسیون جهت طرح در سازمان ملل متحد شده‌اند. در همین ایام، سازمان ملل به‌موجب قطعنامه ۲۴۷/۷۴ دستور تشکیل یک کمیته موقت به‌منظور تدوین کنوانسیون بین‌المللی مبارزه با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه را صادر کرده است. در همان قطعنامه، مجمع عمومی، تصمیم گرفت که کمیته موقت حداقل شش جلسه، هر جلسه ۱۰ روزه، تشکیل دهد تا در ژانویه ۲۰۲۲، یک جلسه پایانی در

نیویورک به‌منظور پایان دادن به ارائه پیش‌نویس کنوانسیون به مجمع عمومی در هفتاد و هشتمین جلسه آن برگزار کند که این جلسه به دلیل محدودیت‌های ناشی از بیماری کرونا به تعویق افتاده است.

کمیته موقت، متشکل از ۱۵ عضو است. این اعضا، هرکدام به‌عنوان نمایندگان منطقه‌ای در کمیته حضور دارند. این نمایندگان عبارت‌اند از: گروه آفریقایی: الجزایر و مصر و نیجریه، گروه آسیا و اقیانوسیه: چین و ژاپن و اندونزی، گروه اروپای شرقی: استونی و لهستان گروه اروپای و فدراسیون روسیه، گروه آمریکای لاتین و حوزه کارائیب: جمهوری دومینیکن، نیکاراگوئه، برزیل، گروه اروپا و اعضای دیگر: استرالیا و پرتغال و ایالات‌متحده.

دولت روسیه با توجه به آمادگی خود، نخستین پیش‌نویس را ۲۹ ژوئن ۲۰۲۱ تقدیم به کمیته موقت کرد. طرح پیشنهادی دولت روسیه چندین هدف بلندپروازانه دارد. بر اساس مفاد این کنوانسیون، دولت روسیه به‌تمامی کشورهای عضو پیشنهاد می‌کند که جرائم سایبری را به‌عنوان جرمی مستقل در نظام حقوقی خود مورد جرم انگاری قرار دهند. این کنوانسیون رویه‌های جدید را در خصوص نحوه همکاری‌های بین‌المللی جهت مبارزه با جرائم سایبری تعریف می‌کند. روسیه پیشنهاد کرده است تا یک گروه فنی بین‌المللی برای مبارزه با جرائم فناوری اطلاعات و ارتباطات تشکیل شود تا به دولت‌های عضو جهت بررسی کنوانسیون کمک کند. یکی از ویژگی‌های اصلی طرح پیشنهادی دولت روسیه، تأکید بر حاکمیت ملی است. این نکته مهم در مقدمه نیز مورداشاره قرارگرفته است. این نکته ازآن‌جهت مهم است که یکی از دلایل اصلی نپیوستن دولت روسیه به کنوانسیون بوداپست، عدم توجه این کنوانسیون به مسئله

حاکمیت است، چراکه بر اساس آن کنوانسیون، عملیات سایبری فرامرزی به‌طورکلی و بدون لحاظ هیچ قید شرطی تجویزشده است. البته پایبندی روسیه به اصل حاکمیت، چالش‌هایی را نیز در متن پیشنهادی به وجود آورده است. مسئله استرداد مجرمین سایبری یکی از همین چالش‌ها است. بر اساس متن پیشنهادی روسیه، دولت‌های عضو تحت شرایطی می‌توانند از استرداد مجرمان سایبری خودداری کنند. جرم انگاری پاره‌ای از جرائم که جرم سایبری محض نیست، از دیگر محل‌های مناقشه طرح روسی است. هرچند دولت روسیه در طرح پیشنهادی خود نسبت به کنوانسیون بوداپست دامنه جرائم را توسعه داده و برخی از جرائم سایبری نوظهور را نیز مورد شناسایی قرار داده، اما در خصوص نکته پیش‌گفته، انتقادات جدی‌ای وجود دارد. از سوی دیگر، در طرح پیشنهادی، فعالیت‌های مخرب سایبری عملیات سایبری باهدف تغییر آراء یا از کار انداختن زیرساخت‌های و فناوری‌های مربوط به برگزاری انتخابات و در نتیجه محروم کردن یک کشور از توانایی برگزاری انتخابات به شکل عجیبی ازقلم‌افتاده و جرم انگاری نشده است.

با مرور این مقدمات، در ادامه با توجه به متن اصلی کنوانسیون که ترجمه آن ضمیمه گزارش شده است، به بررسی پروپزوال کنوانسیون مبارزه با جرائم سایبری خواهیم پرداخت. همانطور که گفته شد،این طرح توسط نماینده کشور روسیه در سازمان ملل مطرح‌شده است و پس از طی تشریفات قانونی، به کمیته‌های بررسی واگذارشده و چندین نوبت نیز بر اساس نظر کشورهای مختلف مورد اصلاح و تغییر قرارگرفته و با قطعی شدن این اصلاحات، باید انتظار را آن را داشت که به تصویب مجمع عمومی سازمان ملل رسیده (هرچند با توجه به شرایط موجود و

تحریم همه‌جانبه روسیه توسط اکثر اعضای جامعه جهانی به دلیل حمله به اکراین بعید به نظر می‌رسد) و کشورهای مختلف جهان بر اساس سیاست‌های خود به آن پیوسته و کنوانسیون لازم‌الاجرا شود. همچنین در این گزارش، ضمن بررسی پیش‌زمینه و چرایی ارائه چنین طرحی از سوی دولت روسیه، مروری بر اولویت‌های جمهوری اسلامی ایران در این کنوانسیون خواهد شد و پیشنهادهایی متناسب با وضعیت کنونی و نیازمندی‌های ضروری نظام حقوقی کشور مطرح می‌شود.

بخش اول

بخش اول

طرح بحث

روسیه باهدف جلوگیری از وقوع جرائم سایبری، اولین پیش‌نویس یک کنوانسیون جهانی برای افزایش و بهبود قوانین علیه جرائم سایبری را به سازمان ملل متحد ارائه کرده است. یکی از اهداف این کشور از تهیه این پیش‌نویس گسترش فهرست انواع جرائم سایبری تعیین‌شده بین‌المللی است؛ روسیه معتقد است که جرائم سایبری شناخته‌شده در سطح بین‌المللی که در حال حاضر کوتاه و ناقص است. به گزارش خبرگزاری دولتی اسپوتنیک، روسیه در این پیش‌نویس تعداد جرائم سایبری را از ۹ مورد به ۲۳ مورد افزایش داده است. به گزارش خبرگزاری روسی تاس، «پیش‌نویس روسیه از کنوانسیون مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه» رسماً در ۲۷ جولای[1] ارائه شد. متن کنوانسیون روسی، مشتمل بر ۸۹ ماده است که در ۷ فصل مطرح‌شده است. فصل اول به توضیح اهداف کنوانسیون، صلاحیت‌های اجرایی و اصطلاحات به‌کاررفته در متن، فصل دوم به جرم انگاری، مقررات ناظر بر آیین دادرسی کیفری و شیوه اجرای قانون، فصل سوم به اقدامات لازم جهت پیشگیری و مبارزه با جرائم سایبری، نحوه همکاری‌های بین‌المللی، استرداد مجرمان سایبری و همکاری‌های سازمان‌های مجریان قانون و

۱. ۱۴۰۰/۵/۵

تمهیدات لازم جهت مصادره اموال ناشی از جرم، فصل پنج به کمک‌های فنی و آموزشی، فصل ششم به سازوکارهای اجرای کنوانسیون و در نهایت فصل هفتم به برخی از مقررات نهایی می‌پردازد.

هیئت روسی به رهبری پتر گورودوف معاون دادستان کل و دنیس تاچایچاوالیت، سرپرست دفتر مبارزه با مواد مخدر و جرم سازمان ملل در دفتر ژنو سازمان ملل این پیش‌نویس را ارائه کرد. گورودوف، رهبر هیئت روسی، دراین‌ارتباط گفت که «کنوانسیون بوداپست در مورد جرائم سایبری شورای اروپا»[1] منسوخ‌شده است، زیرا تنها ۹ نوع مشخص‌شده از جرائم سایبری را به رسمیت می‌شناسد. این کنوانسیون که در سال ۲۰۰۱ تنظیم شد، انواع جدید جرائم سایبری را شامل نمی‌شود. کنوانسیون جرائم سایبری معروف به «کنوانسیون جرائم سایبری بوداپست» یا به‌اختصار «کنوانسیون بوداپست» نخستین معاهده بین‌المللی است که به جرائم رایانه‌ای و اینترنتی می‌پردازد و می‌کوشد قوانین ملی را سازگار کرده، روش‌های تحقیقات را ارتقا دهد و همکاری بین کشورها را بهبود بخشد. این کنوانسیون توسط شورای اروپا در سال ۲۰۰۱ ارائه شد و از ۲۳ نوامبر ۲۰۰۱ کشورها می‌توانستند آن را امضا کنند.

کنوانسیون بوداپست که بیشتر به‌عنوان کنوانسیون جرائم سایبری شناخته می‌شود، در سال ۲۰۰۱ توسط کشورهای آفریقای جنوبی، کانادا، ژاپن و ایالات‌متحده امضا شد و در جولای ۲۰۰۴ لازم‌الاجرا شد. این کنوانسیون اولین معاهده بین‌المللی بود که برای رسیدگی به جرائم ارتکابی با استفاده از اینترنت و سایر شبکه‌های کامپیوتری منعقدشده بود. بااین‌حال، ازآنجایی‌که این معاهده در اوایل قرن ۲۱ تنظیم شد، فقط آن دسته از جرائم سایبری را پوشش می‌داد که در آن زمان به رسمیت

1. The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention

شناخته‌شده بودند.

۹ جرم اصلی تعیین‌شده توسط کنوانسیون بوداپست شامل دسترسی غیرقانونی، شنود غیرقانونی، تداخل داده‌ها، تداخل در سیستم، سوءاستفاده از دستگاه‌ها، جعل رایانه‌ای، کلاه‌برداری با استفاده از رایانه، جرائم مربوط به پورنو گرافی کودکان و جرائم مربوط به نقض حق چاپ و حقوق مرتبط با آن است.

در سال ۲۰۲۰، ایگور کراسنوف، دادستان کل روسیه، گروهی از افراد متخصص را برای بررسی جرائم مرتبط با فناوری اطلاعات گرد هم آورد. این گروه بود که وظیفه تدوین یک کنوانسیون بین‌المللی جهانی برای مقابله با جرائم سایبری را بر عهده گرفت. این پیش‌نویس شامل جرائم سایبری جدیدتری می‌شود که در چند سال اخیر شایع شده‌اند، ازجمله جرائم مربوط به ارزهای دیجیتال، محصولات پزشکی تقلبی و حتی مشارکت خردسالان در فعالیت‌های غیرقانونی.

این پیش‌نویس چالش‌ها و تهدیدهای امروزی را در حوزه امنیت اطلاعات بین‌المللی (ازجمله استفاده مجرمانه از ارزهای رمزنگاری‌شده) را نیز در نظر می‌گیرد و نگاهی به جرائم جدیدی که با استفاده از فناوری‌های اطلاعات و ارتباطات (بازاریابی محصولات پزشکی جعلی، قاچاق مواد مخدر) انجام می‌شود؛ دارد. این مسائل در بیانیه دادستانی کل کشور روسیه هم شناسایی‌شده بود. این پیش‌نویس همچنین به دنبال تقویت «همکاری بین‌المللی درزمینه کمک‌های حقوقی در پرونده‌های جنایی، ازجمله ردیابی، دستگیری، ضبط و استرداد دارایی‌ها» نیز هست.

با معرفی پیش‌نویس قطعنامه در ابتدای نشست سازمانی کمیته موقت برای تدوین کنوانسیون بین‌المللی جامع در مورد مقابله با استفاده از

فناوری اطلاعات و ارتباطات برای مقاصد جنایی، حامی اصلی آن، نماینده فدراسیون روسیه، آن را نتیجه توافقی توصیف کرد که در جریانات اخیر منعقدشده است. وی با اشاره به اینکه زبان آن بر اساس اسنادی است که توسط فدراسیون روسیه و ایالات‌متحده به‌عنوان نمایندگان گروه‌هایی از کشورها ارائه‌شده است، گفت که تهیه پیش‌نویس آن به دنبال چندین ماه کار سخت بوده و از حمایت اکثریت قاطع کشورهای عضو برخوردار است. او با توصیف این پیش‌نویس به‌عنوان «متن مصالحه‌ای بسیار متعادل و ظریف»، گفت که پیش‌بینی می‌کند که برای بررسی بیش‌تر این پیش‌نویس کمیته موقت هم در وین و هم در نیویورک تشکیل جلسه دهد. نیاز به تأمین مالی برای این پیش‌نویس، مشارکت هیئت‌هایی را که فاقد نمایندگی در کمیته موقت هستند و همچنین کشورهای درحال‌توسعه به‌طور گسترده‌تر را موردتوجه قرار می‌دهد و تصمیم‌گیری مبتنی بر اجماع را ضروری می‌سازد. وی با بیان این‌که اساس کار خود را نیز بر اساس آیین‌نامه داخلی مجمع عمومی قرار می‌دهد، خاطرنشان کرد: این بدان معناست که هیچ هیئتی نمی‌تواند مانع اجماع بر سر این پیش‌نویس شود. وی با اشاره به اینکه فدراسیون روسیه به‌منظور اطمینان از حمایت گسترده‌تر از پیش‌نویس، تغییرات عمده‌ای در متن ایدئال خود ایجاد کرده است، بر اهمیت وحدت جهانی در مورد تهدید جدی جرائم سایبری تأکید کرد و از همه هیئت‌ها خواست به این متن رأی مثبت دهند.

مسئله اصلی این است که اکثر کشورها تمایل زیادی دارند تا با استفاده از یک معاهده جهانی با جرائم سایبری مبارزه کنند، اما نمی‌توانند بر سر تعریف مناسبی از «جرم سایبری» توافق کنند. طبق مفاد این قطعنامه،

کمیته موقت چندین جلسه ۱۰ روزه برای شروع در ژانویه ۲۰۲۲ تشکیل داد و مقرر شده است که پیش‌نویس کنوانسیون مقابله با جرائم سایبری در هفتاد و هشتمین جلسه آن در سال ۲۰۲۳ به مجمع عمومی ارائه شود. همچنین مقرر شد روش‌هایی را برای مشارکت سازمان‌های بین‌المللی و منطقه‌ای و دعوت و تأیید گروه‌های متخصص در زمینه جرائم سایبری تعیین شود. بخشی از قطعنامه، قبل از تصویب، با اصلاحیه‌ای که توسط نماینده بریتانیا پیشنهاد شد تغییر یافت که با رأی ثبت‌شده اعضا به تصویب رسید.

بخش دوم

بخش دوم

دلایل اهمیت کنوانسیون مبارزه با جرائم سایبری

در اواسط ژانویه سال جاری، سازمان ملل به‌طور رسمی فرآیندی را برای تدوین یک معاهده جهانی در مورد جرائم سایبری آغاز نمود. تدوین این معاهده جهانی با پیش‌نویسی از کشور روسیه بود اما با توجه به اتفاقات متعدد در سال ۲۰۲۱ در مورد حملات باج افزار به زیرساخت‌ها، از دستگاه‌های مراقبت‌های بهداشتی در ایرلند گرفته تا اتفاقات مرتبط با خطوط سوخت در ایالات‌متحده، می‌توان تصور کرد که روند این معاهده توسط ایالات‌متحده و متحدان غربی آن نیز حمایت می‌شود.

شیوع ویروس کرونا عمدتاً بر مشاغل در سراسر جهان تأثیر گذاشته است، اما بازار کسب‌وکار جرائم سایبری در حال رونق است. ازآنجایی‌که افراد بیشتری مجبور به کار در خانه هستند و افراد هرروز بیشتر به دنبال یکپارچگی دیجیتالی عمیق‌تر زندگی خود هستند، مجرمان پایگاه کاربری بزرگ‌تری برای حمله و سو استفاده دارند. در اوت ۲۰۲۰، پلیس بین‌الملل افزایش «هشداردهنده» حملات سایبری در یک دوره چهارماهه را گزارش کرد. این سازمان می‌گوید هر چه تعداد بیشتری از افراد زمان خود را به‌صورت آنلاین سپری می‌کنند، مجرمان بیشتر از آسیب‌پذیری‌های امنیتی، برای سرقت داده‌ها، ایجاد اختلال و سودآوری استفاده می‌کنند».

اینترپل گفت: «ازآنجایی‌که احتمال ناپدید شدن ویروس کرونا به‌زودی کم است، افزایش بیشتر جرائم سایبری در آینده نزدیک نیز بسیار محتمل است»، زیرا کار از خانه آسیب‌پذیری‌های امنیتی سامانه‌ها را در معرض دید قرار می‌دهد و منجر به افزایش پیشروی مجرمان سایبری و طراحی جدیدتر روش‌های هوشمندانه برای فریب کاربران ناآگاه و حملات سایبری می‌شود.[1]

در ژوئیه ۲۰۲۱، روسیه پیش‌نویس کنوانسیون جرائم سایبری را به رئیس کمیته ویژه که وظیفه تدوین معاهده سازمان ملل در مورد جرائم سایبری را بر عهده داشت، ارائه کرد و پیشنهاد کرد که از آن به‌عنوان مبنای معاهده آینده استفاده شود. چارچوب این پیش‌نویس به‌طور قابل‌توجهی از چارچوب جرائم سایبری موجود در کنوانسیون بوداپست متفاوت است، چراکه در این کنوانسیون جرم انگاری گسترده وجود دارد؛ با این وجود، ابهام و ناهماهنگی در برخی از مفاد آن و محدودیت در همکاری‌های بین‌المللی ازجمله موضوعاتی است که نیازمند بررسی دقیق است. این پیش‌نویس اولین پیش‌نویسی نیست که روسیه در این زمینه تهیه‌کرده است. درواقع، این کشور یک مورد دیگر را در سال ۲۰۱۸ قبل از شروع فرآیند سازمان ملل منتشر کرده بود.

رویکرد روسیه به فضای سایبری رویکردی مبتنی بر حاکمیت و کنترل گسترده دولت بوده است. تلاش‌های اخیر روسیه مبتنی بر منزوی کردن اینترنت در حوزه‌های قضایی خود از سایر نقاط جهان بوده است و پیشنهاد اخیر این کشور هم با رویکردی که در محدوده مرزهای جغرافیایی‌اش اتخاذ نموده، هماهنگ است، اگرچه باید گفت این پیش‌نویس تفاوت‌های قابل‌توجهی با پیش‌نویس قبلی دارد.

1. https://www.firstpost.com/tech/news-analysis/explained-russias-proposal-to-the-un-for-expanding-list-of-designated-cybercrimes9843901-.html

باوجود پیش‌نویس روسی، رأی‌گیری نمایندگان مختلف کشورها در سازمان ملل متحد، اصلاحیه‌های سه کشور بریتانیا، برزیل و هاییتی و جلسات گوناگون مذاکره در رابطه با موضوع جرائم سایبری، حقیقت این است که تاکنون هیچ تصمیم اساسی و مناسبی درباره این معاهده گرفته نشده است؛ نه دامنه، مقدمه یا ساختار آن مشخص‌شده و نه این‌که چه اعمالی تحت این معاهده جرم سایبری محسوب می‌شوند تعریف‌شده است.

قرار بود در اولین جلسه کمیته موقت در مورد حدود و ثغور این موضوعات و ابزارهای بالقوه برای مقابله با جرائم سایبری بحث شود، برخی از دولت‌ها نیز اسنادی را ارائه کرده‌اند که بینش و انتظارات آن‌ها را نشان می‌داد؛ اما دولت‌ها هنوز به انگیزه پشت این پیش‌نویس بی‌اعتمادند، آن‌ها معتقدند که راه‌اندازی فرآیند مرتبط با این معاهده دشوار و ثقیل است و به‌طور خلاصه برای ایجاد یک معاهده موردحمایت جهانی با یکدیگر اختلافات اساسی دارند که باید بر آن‌ها غلبه کرد، لذا دولت‌ها به‌سختی پای میز مذاکره می‌آیند.

بخش سوم


تلاش آرمان گرایانه برای مقابله
با جرائم سایبری در سطح جهانی
UNODC

بخش سوم

تلاش آرمان‌گرایانه برای مقابله با جرائم سایبری در سطح جهانی

به طور کلی باید گفت که در خصوص ادبیات مربوط به طراحی یک کنوانسیون به منظور مبارزه با جرائم سایبری دو دیدگاه رقیب وجود دارد. اولین دیدگاه تقریباً جهانی است و می‌گوید باید کاری برای افزایش همکاری جهانی در مورد جرائم سایبری و ایجاد درک مشترک از مسائل انجام شود. این دیدگاه بر پیش‌نویس روسیه حاکم است؛ گروهی از دولت‌ها، ازجمله چین و روسیه، استدلال می‌کنند که کنوانسیون بوداپست نگرانی‌های آن‌ها را در خصوص جرائم سایبری منعکس نمی‌کند؛ به‌ویژه، این دیدگاه را دارند که دسترسی فرامرزی به داده‌ها و شواهد الکترونیکی به حاکمیت ملی ضربه می‌زند[1]. داده‌ها در سراسر حوزه‌های قضایی و اغلب توسط شرکت‌های خصوصی ذخیره می‌شوند، ازجمله محتوای نگهداری شده در فضای ابری، سابقه جستجوهای وب یا پیام‌های متنی. دولت‌هایی مانند روسیه و چین تلاش کرده‌اند تا داده‌های شهروندان خود را تحت صلاحیت دولت قرار دهند و نسبت به بندهایی که دسترسی سایر دولت‌ها به داده‌ها را اجباری می‌کند، محتاط هستند.

دیدگاه دوم اصلاً چنین نگاهی ندارد و نگران است که تعاریف جرائم سایبری به‌قدر کافی مناسب نباشد و همکاری بین‌المللی برای بازپس‌گیری

1. Walker, S. (2022). The Quixotic Quest to Tackle Global Cybercrime. Retrieved 2 April 2022, from https://foreignpolicy.com/11/02/2022/un-cybercrime-treaty-russia-hacking/

مجرمان، آزادی بیان را تحت‌الشعاع قرار دهد؛ اما حقیقت این است که دیدگاه دوم نمی‌تواند برای عصر حاضر و شرایط کنونی اینترنت کافی باشد؛ چراکه از اوایل سال ۲۰۰۱، زمانی که اولین کنوانسیون منطقه‌ای جرائم سایبری، کنوانسیون بوداپست شورای اروپا، تصویب شد، اینترنت و دامنه استفاده از آن بیش‌ازحد تصور سیاست‌مداران گسترده شده است. دیدگاه دوم، همچنین شامل بی‌اعتمادی بین دولت‌ها درباره انگیزه‌های پشت یک معاهده جهانی است که کل فرآیند را به نفع خود می‌کند. از همان ابتدا، کشورهای غربی، ازجمله کشورهای عضو اتحادیه اروپا، ایالات‌متحده، بریتانیا و کانادا، در برابر فرآیند سازمان ملل برای توسعه ابزار جرائم سایبری مقاومت کردند. همه اعضای کنوانسیون بوداپست، خواهان یک معاهده رقیب نبودند و احساس می‌کردند که با افزودن الحاقیه به آن، این کنوانسیون همچنان کاربردی است و برای هر دولتی مناسب است.

حملات باج افزاری کسب‌وکارها و مؤسسات دولتی را ویران کرده است. جنایاتی مانند استثمار جنسی آنلاین کودکان به سطح هشداردهنده رسیده است. قرنطینه‌های کرونا که باعث می‌شد مردم، از کودکان گرفته تا افراد مسن، منزوی‌تر و آنلاین‌تر باشند، جنایات آنلاین را نیز تشدید کرد. دامنه‌های مخرب، کلاه‌برداری‌های فیشینگ، فروش محصولات تقلبی مرتبط با ویروس کرونا به‌صورت آنلاین، ازجمله خونی که ادعا می‌شد از بیماران کرونایی بهبودیافته گرفته‌شده و در دارک وب[1] فروخته می‌شد هرروز بیش‌تر و بیش‌تر شد. بسیاری از کشورها احساس می‌کنند که یک معاهده جهانی از طریق گنجاندن پشتیبانی ظرفیت فنی به افزایش توانایی آن‌ها در پاسخگویی به این نوع تهدیدات کمک می‌کند. دیگر کشورها احساس می‌کنند که می‌توانند همکاری حقوقی بهتری را ایجاد کنند.

1. Dark Web

اگرچه برخی از دولت‌ها زمزمه‌هایی مبنی بر خروج کامل از روند معاهده روسی کرده‌اند، اما بازهم جلسات کمیته موقت برای بررسی این موضوع برگزار شد. اکنون همه جناح‌های سیاسی به این روند متعهد و آماده دفاع از اولویت‌های خود هستند. مسائل اساسی حل‌نشده کلیدی شامل تعریف جرائم (ازجمله جرائم مرتبط با محتوا)، حاکمیت دیجیتال، همکاری بین‌المللی و دسترسی به داده‌ها، همکاری فنی و ظرفیت‌سازی است.

شاید سخت‌ترین چیز این باشد که دولت‌ها جرم سایبری را چگونه تعریف می‌کنند. در حال حاضر هنوز هیچ تعریف مشترکی وجود ندارد و دولت‌ها دیدگاه‌های بسیار متفاوتی در مورد آنچه این تعریف باید در برگیرد، دارند. این اختلاف‌نظرها از دیدگاه‌های متفاوت در مورد اهمیت حفاظت از هنجارهای حقوق بشر و نگرانی‌ها در مورد جرم‌انگاری ارتباطات شخصی، سخنرانی سیاسی آنلاین و آزادی بیان و اجتماع ناشی می‌شود. درحالی‌که دولت‌ها بیشتر بر سر گنجاندن جرائم وابسته به فضای سایبری مانند بدافزارها و باج افزارهایی که محرمانگی، یکپارچگی و در دسترس بودن داده‌ها و سامانه‌ها را تهدید می‌کنند به توافق می‌رسند، توافق بسیار کمی در مورد جرائم سایبری وجود دارد، جرائم سایبری جرائمی هستند که آفلاین نیز اتفاق می‌افتند اما مجرمان ممکن است در آن از فناوری برای دستیابی به اهداف خود استفاده کنند، مانند تجارت آنلاین غیرقانونی حیات‌وحش.

اتحادیه اروپا بیشتر علاقه‌مند است این معاهده را به جرائم با فناوری پیشرفته و جرائم وابسته به فضای سایبری محدود کند و احتمالاً معتقد است بیان فهرستی از اقدامات مجرمانه در این معاهده مثل جعبه پاندورا[1] خواهد بود، به این معنا که وقتی تمام این موارد را به‌عنوان جرم تلقی کنیم، اتفاقات پیش‌بینی‌نشده و بدی در انتظار خواهد بود. از سوی دیگر،

1. Pandora›s box

چین رویکرد گسترده‌تری را پیشنهاد کرده است که شامل جرائم وابسته به فضای سایبری و همچنین جرائم مرتبط با محتوا ازجمله «استفاده از اینترنت برای تحریک و ارتکاب اقدامات تروریستی، انتشار و اطلاعات مضر»، فروش و توسعه و انتشار فناوری اطلاعات و ارتباطات و داده‌ها برای ارتکاب جرم و جنایت و تشکیل «زنجیره محصول تاریک» می‌شود. روسیه در پیش‌نویس معاهده جهانی خود خواستار جرم انگاری «اقدامات غیرقانونی باانگیزه نفرت پراکنی یا دشمنی سیاسی، ایدئولوژیک، اجتماعی، نژادی، قومی یا مذهبی، حمایت و توجیه چنین اقداماتی یا ارائه دسترسی به آن‌ها» شد[1] که باعث می‌شود اکثر سخنرانی‌ها و پلتفرم‌هایی که آن را منتشر می‌کنند موظف به جرم انگاری این موارد شوند.

1. Article -21 Extremism-related offences, United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Draft 29 June 2021

بخش چهارم


دیدگاه مجامع حقوق بشری نسبت به
کنوانسیون مبارزه با جرائم سایبری
UNODC

بخش چهارم

دیدگاه مجامع حقوق بشری نسبت به کنوانسیون مبارزه با جرائم سایبری

هم کمیسیونر عالی حقوق بشر و هم نمایندگان سازمان‌های حقوق بشری همواره تاکید می‌کنند که هر معاهده‌ای علیه جرائم سایبری جدید باید شامل پادمان[1] های صریحی برای منافع عمومی باشد، زیرا این بیم وجود دارد که قوانین ناظر بر جرائم سایبری برای سرکوب فعالیت‌های مشروع استفاده شود. کمیسیونر عالی حقوق بشر نسبت به گنجاندن هرگونه جرم محتوایی در این معاهده هشدار می‌دهد و به این خطر اشاره می‌کند که این نوع جرائم به‌طور نامتناسب در سطح ملی اعمال شود. برای مثال، قوانینی که مدعی مبارزه با اطلاعات نادرست و حمایت آنلاین یا تمجید از تروریسم و افراط‌گرایی هستند، برای زندانی کردن وبلاگ نویسان یا مسدود کردن کل پلتفرم‌ها در برخی کشورها همچون بحرین، عربستان و مصر مورد سوءاستفاده قرارگرفته‌اند.

نامه بیش از ۱۳۰ گروه جامعه مدنی نگرانی‌های کمیسیونر عالی حقوق بشر در مورد جرائم مبتنی بر محتوا را منعکس می‌کند و همچنین به نیاز به گنجاندن پادمان های صریح برای محافظت از مردم اشاره دارد؛ زیرا تاکنون قوانین جرائم سایبری در بسیاری از کشورها برای سرکوب رفتار قانونی استفاده‌شده است. به گفته کمیسیونر عالی حقوق بشر، استفاده

1. Safeguard

از جرائم سایبری برای هدف قرار دادن روزنامه‌نگاران، افشاگران، فعالان سیاسی، محققان امنیتی، جوامع اقلیتی و مدافعان حقوق بشر یک عمل کاملاً اثبات‌شده است؛ بنابراین نتیجه می‌گیریم تعریف دقیق رفتاری که جرم انگاری می‌شود ضروری خواهد بود تا زمانی که این معاهده درنهایت توسط دولت‌های مختلف در سراسر جهان در سطح ملی اعمال می‌شود، حقوق بشر به حاشیه نرود[1].

قوانین جرائم سایبری مبهم مانند قوانینی که دسترسی غیرمجاز به دستگاه‌های رایانه‌ای را جرم انگاری می‌کند، برای هدف قرار دادن محققان امنیت دیجیتال، افشاگران، فعالان و روزنامه‌نگاران استفاده‌شده است و برخی از دولت‌ها استدلال می‌کنند که هرگونه افشای اطلاعات در خصوص یک شرکت یا سیاست دولتی می‌تواند به‌عنوان جرم سایبری تلقی شود[2]. همان‌طور که توسط کمیسیونر عالی حقوق بشر هم گفته‌شده است، اصل قانونی بودن مقررات حقوق کیفری ایجاب می‌کند که تعاریف جرائم سایبری «در دسترس عموم، واضح و دقیق» باشد، به‌طوری‌که افراد بتوانند به‌طور منطقی تشخیص دهند که کدام رفتار ممنوع است و رفتار خود را بر اساس آن تنظیم کنند. تعاریف مبهم و نادرست از این جرائم، فضایی را برای تفسیرهای خودسرانه و خطر نقض حقوق بشر باقی می‌گذارد.

بسیاری از طرح‌های اولیه دولت‌ها نیز شامل درخواست‌هایی برای اطمینان از پایبندی به استانداردهای حقوق بشر و توجه ویژه به تأثیر نامطلوب بالقوه بر آزادی بیان و سایر حقوق بشر است. با توجه به ماهیت جهانی معاهده پیشنهادشده توسط روسیه، ضروری است که حقوق بشر در محور مذاکرات معاهده قرار گیرد.

1. Katitza Rodriguez, a. (2022). Nearly 130 Public Interest Organizations and Experts Urge the United Nations to Include Human Rights Safeguards in Proposed UN Cybercrime Treaty. Retrieved 2 April 2022, from https://www.eff.org/deeplinks/01/2022/nearly-130-public-interest-organizations-and-experts-urge-united-nations-include

2. U.S. whistleblower Chelsea Manning challenging secrecy laws barring her from Canada | National Post. (2022). Retrieved 2 April 2022, from https://nationalpost.com/news/canada/u-s-whistleblower-chelsea-manning-challenging-secrecy-laws-barring-her-from-canada

بخش پنجم


نگاهی به نقاط ضعف و قوت طرح پیشنهادی
کنوانسیون مبارزه با جرائم سایبری
UNODC

بخش پنجم

نگاهی به نقاط ضعف و قوت طرح پیشنهادی کنوانسیون مبارزه با جرائم سایبری

این پیش نویس طیفی از موضوعات مربوط به حقوق ماهوی، اسناد فرآیندی، همکاری‌های بین‌المللی، کمک‌های حقوقی متقابل و اقدامات پیشگیرانه را پوشش می‌دهد. ساختار و دامنه مقابله با مشکل جرائم سایبری به روشی فراگیر و جامع در این کنوانسیون دیده‌شده است. این سند به موضوعاتی که در اسناد جرائم سایبری موجود مانند کنوانسیون بوداپست شورای اروپا، کامل‌ترین سند بین‌المللی موجود در مورد جرائم سایبری، پرداخته می‌شود هم رسیدگی می‌کند، اما به روشی متفاوت. این سند ۶۹ صفحه‌ای بسیار فراتر از ابزارهای موجود است، به‌ویژه در جرائمی که به‌عنوان جرائم سایبری در نظر گرفته می‌شود. همچنین به مسائل مربوط به پیشگیری، ظرفیت‌سازی، کمک‌های فنی و موارد دیگر نیز می‌پردازد.

قطعنامه‌ای که روند معاهده را در دسامبر[1] ۲۰۱۹ ایجاد کرد، به‌صراحت اشاره می‌کند که اسناد بین‌المللی موجود باید به‌طور کامل موردتوجه قرار گیرند. بااین‌حال، پیش‌نویس روسیه به‌طور قابل‌توجهی با اصطلاحات پذیرفته‌شده، مانند اصطلاحات موجود در کنوانسیون بوداپست، مغایرت دارد و اصطلاحات و تعاریف جدیدی را معرفی می‌کند. پیش‌نویس روسی

۱. آذر ماه ۱۳۹۸

به‌جای استفاده از اصطلاحات جاافتاده‌ای مانند «داده‌های رایانه‌ای» و «سیستم رایانه‌ای»، اصطلاحات جدیدی مانند «اطلاعات الکترونیکی» را به کار می‌برد که در بخش «استفاده از اصطلاحات» تعریف‌نشده‌اند (ماده ۴ پیش‌نویس)؛ اما مورداستفاده قرار می‌گیرند. در سراسر متن سند این پیش‌نویس از واژگان جدید به‌طور متناقض همراه با اصطلاحات دیگری مانند «داده»، «سیستم» یا «اطلاعات دیجیتال» استفاده شده که باعث ایجاد سردرگمی در حوزه کاربرد آن‌ها می‌شود. به‌عنوان‌مثال، ماده ۶ دسترسی به «اطلاعات دیجیتالی» را جرم انگاری می‌کند، اما عنوان ماده «دسترسی غیرمجاز به اطلاعات الکترونیکی» است. ماده ۱۸ پیشنهاد می‌کند که «ایجاد و استفاده از داده‌های دیجیتال برای گمراه کردن کاربر»، بدون این‌که مشخص شود «داده‌های دیجیتال» همان «اطلاعات دیجیتالی» است یا خیر، جرم محسوب بشود. بی‌دقتی در این موارد با اصول بنیادین حقوق کیفری که مستلزم قطعیت و وضوح در تعریف اعمال مجرمانه و تعیین مرزهای جرم انگاری است، در تضاد است.

این پیش‌نویس ازنظر دامنه جرم انگاری گسترده است. اولین پیشنهاد روسیه در سال ۲۰۱۸ عمدتاً به اعمالی اشاره داشت که قبلاً در چارچوب‌های قانونی موجود و باکمی تفاوت جرم انگاری می‌شدند. این متن برخی از جرائم ذکرشده در پیشنهاد قبلی (مانند هرزنامه و فیشینگ) را کنار می‌گذارد، اما فهرست گسترده‌تری از جرائم ازجمله تشویق یا اجبار به خودکشی، جرائم مربوط به مشارکت خردسالان در ارتکاب اعمال غیرقانونی که حیات آن‌ها را به خطر می‌اندازد، مسائل مربوط به زندگی یا سلامتی، تروریسم و جرائم مرتبط با افراط‌گرایی و بسیاری موارد دیگر را پیشنهاد می‌کند. علاوه بر این، در ماده ۸۶ این پیش‌نویس، به

امضاکننـدگان اجـازه داده نمی‌شـود در مـورد جرائم مندرج در برخـی از مواد خـود ازجملـه هرزه‌نـگاری کـودکان، تشـویق یا اجبـار به خودکشـی، جرائمی کـه جان یا سـلامت افـراد زیر سـن قانونی را به خطـر می‌اندازند، (مـاده ۱۵)، (مـاده ۱۷) و تحریـک بـه فعالیت‌های خرابکارانـه و جرائم مرتبط با تروریسـم (مـواد ۱۹، ۲۲-۲۶...) و همچنیـن در رابطـه بـا برخـی از مقـررات مربـوط بـه اسـترداد، شـرطی قائـل شـوند (بنـد ۱۱ مـاده ۴۷). لـذا در مواد صدرالاشـاره مقامـات کشـورها بایـد بـدون اسـتثناء از وقـوع جرائم سـایبری مرتبـط با این موضوعـات جلوگیـری بـه عمل‌آورنـد. بسـیاری از جرائـم پیشـنهادی به‌طـور مبهـم تعریف‌شـده‌اند. به‌عنوان‌مثـال، مـاده ۱۸ در مـورد «ایجـاد و اسـتفاده از داده‌هـای دیجیتـال بـرای گمراه کردن کاربـر» قابلیت تفسـیرهای مختلفی را دارد و می‌توانـد بـرای غیرقانونـی کردن هرگونه مخالفـت و جلوگیری از آزادی بیـان اسـتفاده شـود. همان‌طور که در تعدادی از کشـورها مشـاهده می‌شـود، ابهـام در قوانیـن، تفسـیر خودسـرانه و اسـتفاده از قوانیـن کیفـری را بـرای تعقیـب مخالفـان سیاسـی، روزنامه‌نـگاران و دفـاع از حقـوق بشـر امکان‌پذیـر کـرده اسـت. ایـن پیش‌نویس به دلیـل پیشـنهاد «ممنوعیت امتنـاع از کمک حقوقـی متقابـل و اسـترداد»؛ بـه دلیل تلقی یـک جرم به‌عنوان جرم سیاسـی (ماده ۴۶,۴)، پتانسـیل اسـتفاده از تحقیقات جرائم سـایبری را در سـطح ملی و فرامـرزی به‌عنـوان ابـزاری برای سـرکوب سیاسـی ایجـاد می‌کند.

به‌عـلاوه، پیش‌نویـس روسـیه بـرای مبارزه بـا جرائم سـایبری فاقد مبنایی درخـور هنجارها و اسـتانداردهای بین‌المللی حقوق بشـر اسـت. به‌عنوان‌مثال، مـاده ۲۱ بنـد ۱ در مـورد افراط‌گرایـی بـر «اقدامات غیرقانونی بـا انگیزه نفرت یـا دشـمنی سیاسـی، ایدئولوژیـک، اجتماعـی، نـژادی، قومـی یـا مذهبـی، حمایـت و توجیـه چنیـن اقداماتـی یا ارائه دسترسـی بـه آن‌ها» تمرکـز دارد،

بدون اشاره به چگونگی این اعمال یا این‌که این اعمال توسط چه کسی انجام‌شده است. غالباً اتفاق می‌افتد که دولت‌ها افراط‌گرایی را به معنای دیدگاه‌های سیاسی، ایدئولوژی‌ها و هویت‌هایی که با آن مخالف‌اند تعریف می‌کنند. همین ماده از افراط‌گرایی به‌عنوان «تحقیر با استفاده از فناوری اطلاعات و ارتباطات» یاد می‌کند. تحقیر یک مفهوم شخصی و فرهنگی است که برای پیش‌نویس یک سند بین‌المللی مناسب نیست و اگر در یک معاهده الزام‌آور گنجانده شود، عاملی خطرناک برای سرکوب سیاسی است.

درحالی‌که برخی از مقررات مبهم و دارای پتانسیل تفسیرهای مختلف هستند، برخی دیگر بسیار محدود هستند. به‌عنوان‌مثال، ماده ۶ پیشنهاد می‌کند که دسترسی غیرمجاز را فقط در موارد مسدود کردن، تغییر، تخریب یا کپی جرم انگاری کند و جرم دسترسی غیرقانونی صرف را پوشش نمی‌دهد. دسترسی غیرقانونی صرف به‌عنوان یک جرم در چارچوب‌هایی مانند کنوانسیون بوداپست و دستورالعمل اتحادیه اروپا در مورد حملات علیه سامانه‌های اطلاعاتی در سال ۲۰۱۳ وجود دارد؛ بنابراین، پیش‌نویس روسیه از این استانداردها متفاوت است. حذف مجوزهای دسترسی صرف در خارج از مرزهای فعالیت‌های مجرمانه، مانند نفوذ برای مطالعه سیستم هدف یا خواندن اطلاعات محرمانه بدون کپی کردن یا از بین بردن آن‌ها است که گویا در این کنوانسیون مورد تائید است.

تعدادی از دولت‌ها ابراز نگرانی کرده‌اند که معاهده پیشنهادی روسیه ممکن است درنهایت شامل همه‌چیز، از جنگ سایبری گرفته تا امنیت ملی و مجموعه‌ای از قوانین جدید برای حاکمیت اینترنت باشد. این نگرانی‌ها باعث شده است که این معاهده همچنان بر جرم و جنایت و

اجرای قانون متمرکز بماند.

تعدادی از کشورها، ازجمله برزیل، جمهوری دومینیکن، لیختن‌اشتاین، نروژ، سوئیس، بریتانیا و ایالات‌متحده آمریکا، از تمرکز محدودتر بر جرم انگاری حمایت می‌کنند و نسبت به استفاده از این معاهده هشدار می‌دهند. اعمال کنترل‌های گسترده‌تری بر روی اینترنت در سطح جهانی، هماهنگی فنی و خط‌مشی اینترنت در حال حاضر از طریق طیفی از نهادهای چند ذینفعی مانند انجمن حاکمیت اینترنت انجام می‌شود. تلاش‌های گذشته دولت‌ها برای «تحت تسلط گرفتن» کنترل بر این نهادهای چند ذی‌نفعی، نفاق انگیز و نامناسب بوده است.

بسیاری از همان دولت‌ها از گنجاندن امنیت سایبری، امنیت ملی یا جنگ سایبری در محدوده معاهده پیشنهادی روسیه هشدار می‌دهند. به‌عنوان‌مثال، اتحادیه اروپا و کشورهای عضو آن بر لزوم حذف عبارات «امنیت ملی» یا «مسائل رفتار دولتی» تأکید می‌کنند، کشور برزیل هم معتقد است عبارات «صلح و امنیت بین‌المللی» و «دفاع سایبری» باید حذف شود. آنچه واضح به نظر می‌رسد، در این کنوانسیون مرز بین جرائم سایبری از یک‌سو و امنیت ملی، امنیت سایبری و جنگ سایبری از سوی دیگر، محوشده است و سازمان‌های نظامی و امنیتی به‌طور فزاینده‌ای درگیر رسیدگی به جرائم آنلاین خواهند شد. اجماع نظر دولت‌ها بر سر تعریف «اقدامات جنگی در فضای سایبری» نیز مبهم و دشوار است و موضوع را برای یک معاهده بین‌المللی مناسب نمی‌کند. یکی دیگر از کمیته‌های سازمان ملل (گروهی از کارشناسان دولتی در مورد رفتار مسئولانه دولت‌ها درفضای سایبری) در تلاش است تا بین دولت‌ها در مورد نحوه رفتار مسئولانه در هنگام درگیری بین‌المللی در فضای سایبری

اجماع نظر ایجاد کند.

حتی درجایی که دولت‌ها موافقت می‌کنند که تمرکز بر جرم‌انگاری را حفظ کنند (شیلی، ایالات‌متحده آمریکا، بریتانیا، کانادا، اتحادیه اروپا و کشورهای عضو آن، کلمبیا، نیوزیلند، استرالیا، نروژ، سوئیس، نیجریه و اندونزی)، سؤالاتی در مورد این‌که چه جرائمی باید به‌طور خاص جرم انگاری شود، مطرح می‌شود. بسیاری از جنایات، اگر نگوییم اکثر آن‌ها، اکنون می‌توانند جنبه تکنولوژیکی داشته باشند و دامنه ماهوی این معاهده را به‌طور بالقوه وسیع می‌کند. درواقع، یکی از معاهده‌های منطقه‌ای جرائم سایبری (کنوانسیون بوداپست شورای اروپا) حتی نقض کپی‌رایت را به‌عنوان یکی از اصلی‌ترین ممنوعیت‌های کیفری خود در برمی‌گیرد.

برخی از جرائم ذاتاً شامل فناوری‌های اطلاعاتی می‌شوند و به نظر می‌رسد که اکثر دولت‌ها موافق هستند که این جرائم سایبری «خالص» باید در چارچوب کنوانسیون ثبت شوند. برای مثال، این موارد شامل جنایاتی است که داده‌ها یا یک سیستم رایانه‌ای، هدفِ جرم هستند (نیجریه، ایالات‌متحده آمریکا و تا حدی اتحادیه اروپا).

اکثر دولت‌های دیگر فراتر از این هم می‌روند. به‌عنوان‌مثال، استرالیا، اتحادیه اروپا، نیوزلند، نیجریه، سوئیس و ایالات‌متحده آمریکا بر لزوم گنجاندن جرائم سایبری فعال در این معاهده تأکید می‌کنند؛ اما تعیین این‌که چه چیزی به معنای «جرائم سایبری فعال» است می‌تواند مشکل باشد. بسیاری از جرائم (فساد، قاچاق مواد مخدر و تروریسم) قبلاً در سطح بین‌المللی ممنوع شده‌اند و تعدادی از اسناد بین‌المللی قبلاً چارچوب‌هایی را برای همکاری ایجاد کرده‌اند (مانند کنوانسیون سازمان ملل متحد علیه

جرائم سازمان‌یافته فراملی و کنوانسیون سازمان ملل متحد علیه فساد). تکثیر این ابزارها درحالی‌که سعی می‌شود بخش منحصربه‌فرد «سایبری» هر جرم را به تصویر بکشد، ممکن است به تکرار (همان‌طور که توسط ژاپن، لیختن‌اشتاین، نیوزلند و سوئیس اشاره‌شده است) یا حتی اختلال در تلاش‌های بین‌المللی موجود (همان‌طور که نیوزلند هشدار می‌دهد) منجر شود.

بنابراین، برخی از دولت‌ها پیشنهاد کرده‌اند که تنها جرائمی که در آن دامنه، سرعت و مقیاس جرم با استفاده از فناوری‌های اطلاعاتی و ارتباطاتی افزایش می‌یابد، باید جرم انگاری شوند (نیوزیلند، استرالیا، بریتانیا و ایالات‌متحده آمریکا). در این میان فناوری‌ها یک عامل هستند. ایالات‌متحده آمریکا و استرالیا خاطرنشان می‌کنند که یک جرم آنلاین که به‌طور ناشناس انجام می‌شود، ممکن است در تعیین مشتقات جرم در محدوده معاهده نقش داشته باشد.

برخی از دولت‌ها نیز خواستار گنجاندن جرایم مرتبط با محتوا، مانند تحریک به ترور (چین و روسیه)، اطلاعات نادرست و اخبار جعلی (چین و اندونزی) و نقض حق کپی‌رایت (اندونزی، لیختن‌اشتاین، مکزیک، نروژ، روسیه و ایالات‌متحده آمریکا) شده‌اند. در مقابل، دفتر کمیساریای عالی حقوق بشر سازمان ملل متحد استدلال کرده است که هرگونه گنجاندن جرائم تسهیل‌شده توسط فناوری (در مقابل جرائم سایبری «اصلی»)[1] باید محدود شود.

نمایندگان کشورهای فعال در فرایند رایزنی و بررسی ماهوی کنوانسیون، هر کدام بر جرم انگاری صریح برخی از جرایم مهم در متن کنوانسیون، تاکید دارند. این جرایم عبارتند از: دسترسی غیرقانونی به رایانه یا سیستم رایانه‌ای

1. core cybercrimes

(چین، اتحادیه اروپا، اندونزی، لیختن‌اشتاین، نروژ، مکزیک، روسیه، ایالات‌متحده آمریکا)، ره‌گیری غیرقانونی ارتباطات یا ترافیک داده‌ها (اندونزی، لیختن‌اشتاین، نروژ، روسیه، ایالات‌متحده آمریکا)، تداخل داده یا سیستم (شیلی، اتحادیه اروپا، اندونزی، لیختن‌اشتاین، نروژ، پاناما، روسیه، ایالات‌متحده آمریکا)، سوءاستفاده از دستگاه‌ها (لیختن‌اشتاین، نروژ، روسیه، ایالات‌متحده آمریکا)، کلاه‌برداری سایبری، (استرالیا، چین، اندونزی، مکزیک، نیوزیلند، نروژ، روسیه، ایالات‌متحده آمریکا)، جرائم مربوط به نقض کپی‌رایت و حقوق مرتبط (اندونزی، لیختن‌اشتاین، مکزیک، نروژ، روسیه، ایالات‌متحده آمریکا) و جرائم مربوط به پورنو گرافی کودکان (استرالیا، اتحادیه اروپا، اندونزی، چین، روسیه، نیوزیلند، نروژ، مکزیک، بریتانیا، ایالات‌متحده آمریکا).

فهرستی شاخص از سایر جنایات خاص که توسط برخی از دولت‌ها ارائه‌شده است عبارت‌اند از: استفاده از اینترنت برای تحریک و ارتکاب اقدامات تروریستی (چین، روسیه). اطلاعات نادرست، توطئه، فریب (چین، اندونزی)؛ مطالبی که حاوی خصومت‌های نژادی، ملیت، مذهب یا سیاسی (اندونزی)، جرائم مرتبط با قاچاق اسلحه (مکزیک، روسیه)، استفاده از ارزهای دیجیتال و دارایی‌های دوگانه برای مقاصد مجرمانه (مکزیک)، دسترسی غیرمجاز به داده‌های شخصی (روسیه) است. ایالات‌متحده آمریکا، جرائم مربوط به توزیع مواد مخدر و روان‌گردان (روسیه) و توزیع غیرقانونی داروها و محصولات پزشکی تقلبی (روسیه).

به‌غیراز موارد پیش‌گفته، بسیاری از کشورها علاقه‌مند هستند تا تلاش برای ارتکاب جرائم تحت پوشش، کمک و مشارکت در آن‌ها، یا حتی پول‌شویی عواید حاصل از جرائم سایبری نیز جرم انگاری شود

(شیلی، چین، نیجریه، نروژ، روسیه، ایالات‌متحده آمریکا). مسئله مسئولیت کیفری برای اشخاص حقوقی (برخلاف اشخاص حقیقی) نیز ممکن است جرم انگاری شود و در متن اصلی معاهده پیشنهادشده توسط روسیه نیز آمده است، به این معنی که شرکت‌ها ممکن است مرتکب جرم شوند (مکزیک، روسیه، ایالات‌متحده).

درنهایت، بسیاری از کشورهای عضو تأکید می‌کنند که کارایی این معاهده در آینده و با توسعه سریع فناوری‌ها و استقرار روش‌های خلاقانه جدید برای ارتکاب جنایات در فضای سایبری، اثبات خواهد شد. استرالیا، ژاپن، لیختن‌اشتاین، نیجریه، بریتانیا و ایالات‌متحده هم از این ایده حمایت می‌کنند. این معاهده باید به نحوی تنظیم شود که با پیشرفت فناوری از نیاز به اصلاح مکرر این معاهده جلوگیری کند.

چندین رویکرد ملی برای مقابله با جرائم سایبری، بین جرائم وابسته به فضای سایبری (جرائمی که فقط از طریق فناوری اطلاعات و ارتباطات قابل ارتکاب هستند) و جرائم مبتنی بر فضای سایبری (جرائم سنتی تسهیل‌شده توسط فناوری اطلاعات و ارتباطات که به‌موجب آن، فناوری اطلاعات و ارتباطات به‌عنوان ابزار استفاده می‌شود) تفاوت قائل می‌شوند. جرائم مبتنی بر فضای سایبری طیف گسترده‌ای از جرائم، مانند بهره‌کشی آنلاین از کودکان، سرقت هویت، کلاه‌برداری‌های مالی، جرائم مرتبط با محتوا و عملاً هر جرمی با بعد فناوری اطلاعات و ارتباطات را در برمی‌گیرد.

پیش‌نویس روسیه هم از نظر جنایات مرتبط با تروریسم و افراط‌گرایی گسترده است و هم در گنجاندن انواع دیگر جرائم سایبری گزینشی است. به‌عنوان‌مثال، ماده ۲۲ در مورد جرائم مربوط به توزیع مواد مخدر و

روان‌گردان صحبت می‌کند و ماده ۲۵ بر توزیع غیرقانونی داروها و فرآورده‌های پزشکی تقلبی تمرکز دارد. مشخص نیست چرا این گروه منتخب از جرائم نسبتاً سنتی که در آن فناوری اطلاعات و ارتباطات به‌عنوان وسیله‌ای برای ارتکاب جرم استفاده می‌شود، نیاز دارند به‌عنوان یک جرم سایبری صرف تلقی شوند و نمی‌توان با استفاده از قوانین کیفری موجود، مانند قوانین عمومی مرتبط با قاچاق مواد مخدر، به آن‌ها پرداخت. این رویکرد انتخابی، تمرکز خودسرانه بر برخی از جرائم و نه برخی دیگر، خطر امکان‌پذیری و نهادینه کردن پاسخ جزئی به مشکلات کلی را به همراه دارد؛ جرم انگاری موازی جدید و در نظر گرفتن مجازات برای جرائمی که قبلاً در سیستم حقوقی فعلی برایشان پاسخ مناسبی وجود دارد، ممکن است کارکرد حقوق کیفری را تضعیف کند و فرصت بهره‌برداری از نقاط ضعف این موضوع و کاربرد سلیقه‌ای قوانین را باز کند.

پادمان‌ها نیز یکی دیگر مسائل مناقشه‌برانگیز در طرح روسی است. بخش پیش‌نویس در مورد ابزارهای رویه‌ای شامل اقدامات شناخته‌شده‌ای مانند دستور تولید، جمع‌آوری و افشای جزئی داده‌های ترافیک، ره‌گیری داده‌های محتوا، جستجو و ضبط است. بااین‌حال، فاقد دقت و تمایز در سازوکارها و ابزارهای موجود است. درحالی‌که کنوانسیون بوداپست تمایز واضحی بین انواع مختلف داده‌ها و پادمان های قابل‌اجرا ارائه می‌دهد، این پیش‌نویس همه آن‌ها را باهم گروه‌بندی می‌کند. به‌عنوان‌مثال، ماده ۳۳ در مورد «جمع‌آوری اطلاعات منتقل‌شده از طریق فناوری اطلاعات و ارتباطات» به شنود محتوا و هر داده دیگری اشاره دارد. این فقدان دقت مباحث در مورد تدابیر لازم و متناسب با مداخله‌گری، مانند محدود کردن ره‌گیری به جرائم جدی، کار را پیچیده می‌کند.

دامنه کاربرد چارچوب‌های تحقیقاتی، علاوه بر جرائم ذکرشده در پیش‌نویس، تحقیقات سایر جرائم ارتکابی با استفاده از فناوری اطلاعات و ارتباطات را نیز در برمی‌گیرد. حتی اگر به طرفین اجازه داده شود که برای محدود کردن دامنه وسیع مواد مربوط به اقدامات تحقیقاتی، شرطی قائل شوند، امکان اعمال این مقررات در مورد هر جرم کیفری، مسئله تدابیر مناسب را مطرح می‌کند. بسیاری از اقدامات تحقیقاتی دیجیتال، یکپارچه و درعین‌حال مزاحم هستند که این مسئله می‌تواند حق حریم خصوصی را نقض کند؛ بنابراین، مهم است که تضمین شود تداخل اقدام خاص ضروری و متناسب با جدیت جرم، مطابق با استانداردهای حقوق بشر است. این موضوع به‌ویژه برای کشورهایی که قبلاً طرف کنوانسیون بوداپست که سطح مشخصی از استانداردها و پادمان ها را ایجاد کرده است، هستند؛ بسیار مهم است.

درحالی‌که پیش‌نویس شامل مقرراتی در مورد شرایط و ضمانت‌های مربوط به اختیارات رویه‌ای است (ماده ۳۲)، به نظر می‌رسد اهمیت کمتری نسبت به استانداردهای کنوانسیون بوداپست به این موضوع می‌دهد. به‌عنوان‌مثال، ماده ۳۳ شنود داده‌ها را به هر جرمی در معاهده تعمیم می‌دهد، درحالی‌که کنوانسیون بوداپست آن را به جرائم جدی محدود می‌کند. درنهایت، اما مهم‌تر از آن، کنوانسیون بوداپست به‌طرف اجازه می‌دهد تا زمانی که درخواست مربوط به جرمی است که طرف درخواست شونده آن را جرم سیاسی می‌داند، از کمک حقوقی متقابل امتناع کند. پیشنهاد روسیه مستقیماً امتناع از کمک حقوقی متقابل و استرداد به این دلیل را ممنوع می‌کند و طرفین را مجبور می‌کند تا کمک حقوقی متقابل را ارائه دهند حتی اگر دولت درخواست‌کننده از

تحقیقات دیجیتالی خاصی به‌عنوان ابزاری برای سرکوب سیاسی استفاده کند.

این پیش‌نویس ظرفیت‌سازی، به‌ویژه، آموزش کارکنان و ارائه کمک‌های فنی برای پیشگیری و مبارزه با جرائم فناوری اطلاعات و ارتباطات (ماده ۷۶) را در متن خود برجسته می‌کند. همچنین برافزایش آگاهی عمومی در مورد جرائم سایبری تأکید زیادی دارد (ماده ۴۴). این‌که همکاری بسیار موردنیاز بین دولت‌ها در سطح بین‌المللی و همچنین در سطح ملی بین ذی‌نفعان در این پیش‌نویس تسهیل شده است؛ یک توسعه خوشایند و قابل توجه است. پیوند دادن این موضوع با فرآیندهای اخیر سازمان ملل که تأکید مشابهی داشتند و اجماع همه کشورها را به دست آورده است، هر دو تلاش را تحت تأثیر قرار می‌دهد و رویکرد جامع‌تری برای ظرفیت‌سازی در مقابله با تهدیدات ناشی از سوء استفاده از فناوری اطلاعات و ارتباطات را به تصویر می‌کشد.

با این وجود، یکی از استدلال‌ها علیه معاهده سازمان ملل در مورد جرائم سایبری این است که زمان زیادی طول می‌کشد تا کشورها بر سر محتوای آن توافق کنند. رویکرد روسیه به فرآیند سازمان ملل که به دلیل جرم انگاری گسترده، ابهام و ناهماهنگی در برخی مفاد خود و محدودیت‌های همکاری بین‌المللی و موضوعات دیگر به‌طور قابل‌توجهی از چارچوب‌های بین‌المللی موجود در مورد جرائم سایبری، فاصله می‌گیرد؛ ممکن است این مسئله را تائید کند. علاوه بر این، پیشنهاد پیش‌نویس معاهده قبل از شروع فرآیند ممکن است ازنظر بسیاری به‌عنوان تضعیف روح فرآیند سازمان ملل و اجماع شکننده‌ای که در مورد روش‌های این فرآیند به دست آمد، تلقی شود. برخلاف مذاکرات در اولین کمیته سازمان

ملـل متحد در زمینه فناوری اطلاعـات و ارتباطات و صلح و امنیت بین‌المللی، نتیجـه ایـن رونـد الـزام‌آور خواهد بـود. این بدان معناسـت که کشـورهایی که تصمیـم بـه پیوسـتن بـه معاهـده می‌گیرنـد بایـد ایـن کنوانسـیون را امضا و تصویـب کننـد و آن را در سیسـتم حقوقـی ملـی خـود اجـرا کننـد. ایـن امر هرگونـه توافقـی را کـه به‌طـور قابل‌توجهـی از رویه‌های رایج موجـود منحرف شـود بسـیار بعیـد می‌کند.

پیشرفت قابل‌توجهی در چند سال گذشته در تدوین قوانین و سیاست‌های ملی برای رسـیدگی به خطرات فزاینده ناشـی از جرائم سـایبری حاصل‌شـده اسـت. ازایـن‌رو، رویکرد مکمل به‌جـای رویکرد رقیب، پتانسـیل جلب حمایت مردمـی را دارد، نـه این‌کـه آنچـه قبـلاً توافـق شـده اسـت را از بیـن ببـرد و منجـر بـه یک ابزار واقعـاً جهانی و فراگیر بـرای حمایت از دولت‌ها در سـطوح مختلـف ظرفیـت برای پیوسـتن بـه مبارزه جهانی علیه جرائم سـایبری شـود. رویکردهـای رقابتـی بـه تلاش برای رسـیدگی به یک مشـکل فرامرزی کمکی نخواهـد کـرد. درواقـع، ایـن رویکردهـا بـا تکه‌تکـه کـردن تلاش‌هـای جهانی بـرای مقابلـه بـا جرائم سـایبری به نتیجه معکوس دسـت خواهنـد یافت. [1]

1. https://directionsblog.eu/russias-vision-for-a-cybercrime-treaty/

بخش ششم

بخش ششم

دیدگاه نمایندگان کشورهای مختلف درخصوص کنوانسیون[1]

با آغاز به کار دولت روسیه در اواخر ژانویه و ارائه قطعنامه در مجمع عمومی سازمان ملل، برای بررسی پیش‌نویس ارائه‌شده توسط این کشور جلسات متعددی در نیویورک برگزار شد. البته، معاهده روسی با مقاومت زیادی از سوی تعدادی از کشورها نیز از همان ابتدا مواجه شد. جمهوری دومینیکن، با حامیان عمدتاً اروپایی و آمریکای مرکزی همراه با استرالیا، ژاپن، نیوزیلند و ایالات‌متحده ازجمله مخالفان اصلی این طرح بودند. با برگزاری جلسات کارشناسی، سپس اصلاحیه‌هایی ارائه شد که طرحی کاملاً متفاوت را پیشنهاد می‌کرد. لذا پیش‌نویس روسیه در جریان رأی‌گیری دست‌خوش تغییرات زیادی شد. این دومین باری است که روسیه سعی می‌کرد به اولویت‌های خود برای این دستور کار بپردازد اما در رأی‌گیری شکست خورد. درحالی‌که روسیه آشکارا خود را رهبر این ابتکار می‌داند، وقتی‌که می‌کوشد ترجیحات خود را تحمیل کند، با مقاومت فزاینده‌ای از سوی سایر کشورها مواجه می‌شود.

نماینده بریتانیا با ارائه اصلاحیه‌ای، تمایل خود را برای یک معاهده جرائم سایبری که از گسترده‌ترین حمایت ممکن برخوردار باشد و اقدامات ملموسی را ارائه کند، ابراز کرد. او گفت که برای این منظور، طیفی

1. https://www.un.org/press/en/2021/ga12328.doc.htm

از ذینفعـان و کارشناسـان بایـد بتواننـد نظـرات خـود را به‌صـورت شـفاف بـا کمیتـه موقـت در میـان بگذارنـد. وی درباره الفاظ منسوخ‌شـده‌ای کـه در این کنوانسـیون به‌کاررفته اسـت ابـراز تعجب کـرد و تأکید کرد: «مقابلـه با جرائم سـایبری نبردی اسـت کـه دولت‌ها به‌تنهایـی نمی‌توانند در آن پیروز شـوند». چالشـی کـه در پیش‌نویـس فعلـی وجـود دارد ایـن اسـت کـه بنـد ۹ [1] آن به هـر یک از کشـورهای عضـو در مورد مشـارکت یک سـازمان غیردولتی خاص یـا عضـو جامعـه مدنی، حـق وتـو می‌دهـد. نماینـده بریتانیا در ایـن خصوص خواسـتار اصلاحیه شد.

وی بـا اشـاره گسـترده‌تر به‌پیـش نویـس قطعنامـه تأکیـد کـرد: متنی که پیـش روی مـا اسـت، بـه معنـای نتیجـه کار در کمیتـه و توافق نیسـت. بلکه نتیجـه مذاکـرات دوجانبـه بیـن فدراسـیون روسـیه و ایالات‌متحده اسـت که حتـی روسـیه اکنـون به آن اعتـراض دارد. او گفـت: من تنها متوجه شـدم که اکثریـت نسـبت بـه متن ابـراز نگرانـی می‌کردند. نبایـد برای تائیـد یک «متن غافلگیرکننـده» در کوتاه‌مـدت و به قیمت رایزنی‌های غیررسـمی بیشـتر بین کشـورهای عضـو عجله کرد. البته در سرتاسـر جلسـه، بسـیاری از سـخنرانان ایـن ایـرادات را تکـرار کردنـد و چندیـن سـخنران، به‌ویژه در مـورد روش‌های پیش‌نویـس قطعنامـه برای سـاختار تصمیم‌گیـری کمیته موقـت، اختلاف‌نظر داشتند.

در همیـن راسـتا، نماینـده برزیـل اصلاحیـه‌ای را ارائه کـرد که بخش‌هایی از بنـد ۵ [2] اجرایـی را بـا بیانـی جدیـد جایگزیـن می‌کنـد و همـه تصمیمـات کمیتـه موقـت در مـورد موضوعـات اساسـی را همراه بـا تأیید و اجمـاع نظر با

1. 9. Requests the Chair of the Ad Hoc Committee, in consultation with the United Nations Office on Drugs and Crime, to draw up a list of additional organizations with expertise in the field of cybercrime that may attend sessions of the Ad Hoc Committee as observers, and to submit the proposed list to Member States for their consideration on a non-objection basis; A/75/L.87/Rev.1, Distr.: Limited 24 May 2021.
2. 5. Also decides that the Ad Hoc Committee shall hold its six negotiating sessions in Vienna and shall be guided by the rules of procedure of the General Assembly, while exhausting all efforts to adopt substantive decisions by consensus; Ibid.

اکثریت دوسوم نمایندگان حاضر و رأی‌دهنده لازم می‌داند. وی با تأکید بر این‌که ردیابی جرائم سایبری جرمی دشوار و بدون مرز فیزیکی است و از حوزه‌های قضایی ملی می‌گذرد، گفت بنابراین همکاری بین‌المللی در این زمینه بسیار حیاتی است. او گفت که پیش‌نویس کنونی فاقد شمولیت و شفافیت لازم است و در مورد این‌که این پیش‌نویس «پشت درهای بسته» و بدون رایزنی کافی و با این فرض اشتباه که موردحمایت همه هیئت‌ها قرار می‌گیرد، تهیه‌شده است، ابراز نگرانی کرد.

او گفت که در غیاب رایزنی‌های گسترده‌تر، برزیل تصمیم گرفت اصلاحیه‌ای را ارائه کند که برای تصمیم‌گیری کمیته موقت نیاز به اکثریت اعضا دارد. وی خاطرنشان کرد که چنین اکثریتی در بسیاری از نهادهای تهیه‌کننده معاهده‌های سازمان ملل، ازجمله اجلاس بین دولتی اخیر برای ایجاد یک سند بین‌المللی الزام‌آور قانونی در زمینه تنوع زیستی دریایی در مناطق خارج از صلاحیت ملی، از سابقه زیادی برخوردار است. نماینده کوبا این معاهده را به‌عنوان یک موازنه ظریف توصیف کرد که «نماینده بهترین سازش موجود است»، حمایت خود را از این پیش‌نویس اعلام کرد، همچنین پیشنهاد ایجاد آستانه تصمیم‌گیری اکثریت دوسوم را رد کرد.

نماینده نیکاراگوئه گفت: سازمان ملل متحد نمی‌تواند در برابر چالش‌های نوظهور جرائم سایبری غیرفعال بماند. به‌منظور شروع سریع کار کمیته موقت، او گفت که هیئت او از امروز پیش‌نویس روسیه در مجمع حمایت می‌کند و به دیگران در این زمینه هشدار داد. درحالی‌که نیکاراگوئه موافق اصلاحیه پیشنهادی هائیتی در مورد مشارکت گسترده‌تر کشورهای درحال‌توسعه است، از اصلاحیه پیشنهادی بریتانیا حمایت نمی‌کند، زیرا

معتقد است پیش‌نویس اولیه سابقه مشارکت سازمان‌های غیردولتی را نیز نشان می‌دهد.

نماینده کشور کریباتی با اشاره به این‌که کشورش به‌شدت تحت تأثیر جرائم سایبری قرارگرفته است، از مجلس خواست تا «نفسی بکشد و در مسیر صبر، خرد و همکاری» در این موضوع بسیار مهم قدم بگذارد. وی تأکید کرد: «ما خواهان معاهده‌ای هستیم که مورد تشویق و تجلیل همه انسان‌های روی کره زمین قرار گیرد.»

نماینده چین گفت پیش‌نویس، یک متن مصالحه‌ای است که منعکس‌کننده اجماع همه کشورهای عضو است. او با توصیف این پیش‌نویس به‌عنوان «سندی به‌سختی تهیه‌شده است» گفت که هدف آن دستیابی به یک کنوانسیون گسترده و عملی در مورد جرائم سایبری با مشارکت گسترده است. او با عطف به اصلاحات پیشنهادی، گفت: این پیش‌نویس همراه با اصلاحاتش نگرانی‌های همه هیئت‌ها را به شیوه‌ای معقول برطرف می‌کند. اصلاحاتی که «این توازن را بر هم می‌زند»، مانند اصلاحات برزیل برای روح این معاهده مناسب نیست؛ بنابراین چین از اصلاحیه برزیل حمایت نمی‌کند.

وی در خصوص مشارکت سازمان‌های مردم‌نهاد نیز گفت: این پیش‌نویس منعکس‌کننده نگرش باز نسبت به این موضوع است و به گروه‌هایی که وضعیت مشورتی با سازمان‌های اقتصادی و اجتماعی دارند و سایرین با وضعیت ناظر مشارکت می‌کنند، اجازه کار می‌دهد. به همین دلیل، چین از اصلاحیه پیشنهادی بریتانیا نیز حمایت نمی‌کند. ازآنجایی‌که مقابله با جرائم سایبری مستلزم فرآیند مذاکره‌ای است که همه کشورهای عضو را در برمی‌گیرد، چین از کشورهای درحال‌توسعه، به‌ویژه کشورهایی که فاقد

نمایندگی در وین هستند، حمایت می‌کند و امیدوار است سایر کشورها نیز همین کار را انجام دهند.

نماینده هلند که موضع کشورش مطابق با موضع اتحادیه اروپا است، گفت که هیئت او آماده حمایت از پیش‌نویس ارائه‌شده به جلسه سازمانی کمیته موقت در دوازدهم ماه مه است. وی با تأکید بر اهمیت فراگیری این معاهده، از اقدامات انجام‌شده در جلسه ابراز تأسف کرد. عجله در تصویب پیش‌نویس در مجلس در چنین مهلت کوتاهی، درحالی‌که رایزنی‌ها با رئیس مجلس همچنان در جریان بود، عادی نیست. هلند از اصلاحیه پیشنهادی برزیل برای آستانه تصمیم‌گیری اکثریت دوسوم حمایت می‌کند، چراکه تضمین می‌کند صدای کل اعضای سازمان ملل شنیده می‌شود.

نماینده ونزوئلا بر تعهد کشورش به مبارزه با جرائم سایبری تأکید کرد و خواستار آغاز هر چه سریع‌تر کار کمیته موقت شد. وی با اشاره به این‌که بیش از یک سال است که بحث‌های جامعی دراین‌باره انجام‌شده است، گفت ونزوئلا از هر ابتکاری که هدف آن تقویت مشارکت فراگیر و آغاز کار کمیته موقت باشد، حمایت می‌کند؛ بنابراین، از پیش‌نویس مذکور و این ایده که آیین‌نامه داخلی مجمع باید کمیته موقت را نیز اداره کند، حمایت می‌کند.

همچنین نمایندگان استرالیا، کلمبیا، کانادا، نروژ، کاستاریکا و گواتمالا نگرانی‌ها را در مورد روند تهیه پیش‌نویس تکرار کردند. بااین‌حال، چندین کشور نیز در حمایت از پیش‌نویس مذکور صحبت کردند و آن را «مصالحه‌ای با دقت و متعادل» نامیدند که بنا به‌ضرورت، نمی‌تواند به‌طور کامل هیچ هیئتی را راضی کند.

1. https://www.un.org/press/en/2021/ga12328.doc.htm

نماینده رومانی گفت که روند کار در هفته‌های اخیر با بی‌توجهی به فراگیری و مشورت همراه بوده است. وی با ابراز حمایت از پیشنهاد اکثریت دوسوم ارائه‌شده توسط برزیل، گفت هرگونه تلاش برای رد آن نشان می‌دهد که قصد واقعی برخی از کشورها تمسخر مذاکرات کمیته موقت است.

نماینده سوئیس که از طرف لیختن‌اشتاین نیز صحبت می‌کرد، از این‌که این پیش‌نویس دیدگاه طیف وسیعی از کشورهای عضو را در نظر نمی‌گیرد، ابراز تأسف عمیق کرد. چراکه اجماع نظرات بهترین رویکرد است، اصلاحیه در مورد سیستم اکثریت دوسوم پیشنهادشده توسط برزیل بهترین سازش را بین کسانی که برای تصمیم‌گیری اجماع استدلال می‌کنند و کسانی که خواستار این فرآیند نیستند؛ ارائه می‌کند. وی انتظار داشت که مذاکرات به‌صورت باز و شفاف و بر اساس اسناد بین‌المللی موجود انجام شود. او همچنین از اصلاحیه پیشنهادی بریتانیا حمایت کرد. او که در مقام نماینده دولت خود صحبت می‌کرد، از انجام کل فرآیند مذاکره در وین که مرکز حقوقی سازمان ملل است، حمایت کرد.

نماینده ایالات‌متحده گفت که هیئت او از این پیش‌نویس به شکل کنونی آن حمایت نمی‌کند و همچنین از تلاش برای دور زدن گفتگو یا عجله در رأی‌گیری درزمانی که رایزنی‌های غیررسمی هنوز برنامه‌ریزی نشده است، حمایت نمی‌کند. وی با تأکید بر این‌که چنین اقداماتی کارایی دفتر و کمیته موقت را تضعیف می‌کند، گفت که ایالات‌متحده در حمایت خود از یک فرآیند متوازن، فراگیر و مبتنی بر اجماع که منجر به یک معاهده جهانی جرائم سایبری می‌شود، شفاف بوده است.

او با تأکید بر این‌که متنی که امروز به‌سرعت به مجمع ارائه شد،

«بسیار از آن استاندارد فاصله دارد»، گفت که اقدامات حامی اصلی متن یعنی روسیه تنها نشان می‌دهد که اجماع نظر دولت‌ها هدف آن نیست. او با عطف به اصلاحیه پیشنهادی برزیل، گفت که دلیل خوبی برای دوسوم اکثریت وجود دارد که می‌تواند به ایجاد اعتماد در میان کشورهای عضو به سمت اجماع کامل‌تر کمک کند. در این زمینه، او از هر دو اصلاحیه ارائه‌شده توسط برزیل و بریتانیا استقبال کرد.

نماینده شیلی، سال ۲۰۲۰ را ازنظر افزایش حملات سایبری و توانایی‌های شتاب‌دهنده هکرها بی‌سابقه توصیف کرد. وی با تأکید بر این‌که هر ۳۹ ثانیه یک حمله سایبری رخ می‌دهد، شکاف دیجیتالی را نیز موردتوجه قرارداد و حمایت خود را از توسعه یک معاهده جهانی الزام‌آور اعلام کرد. او گفت متأسفانه، روند منتهی به مذاکرات فراگیر و شفاف نبوده است. به‌این‌ترتیب، شیلی از اصلاحیه ارائه‌شده توسط نماینده برزیل به‌عنوان راهی برای تضمین نمایندگی گسترده کشورهای عضو حمایت می‌کند.

اصلاحیه دیگری هم توسط نماینده هائیتی به نمایندگی از جامعه کارائیب ارائه و معرفی شد و با هدف تسهیل بهتر مشارکت کشورهای درحال‌توسعه در مذاکرات کمیته موقت، چندین تغییر در پیش‌نویس، ازجمله انتقال برخی از جلسات به نیویورک، به‌جای وین را ارائه کرد. وی با موافقت با این موضوع که جرائم سایبری یک مشکل جهانی است که نیاز به یک واکنش واقعاً جهانی دارد، گفت که کشورهای درحال‌توسعه اغلب فاقد چارچوب‌های قانونی و قابلیت‌های امنیتی مؤثر موردنیاز برای مبارزه با آن هستند؛ بنابراین بسیار مهم است که نظرات کشورهای درحال‌توسعه در تهیه پیش‌نویس هر معاهده جهانی موردتوجه قرار گیرد. او همچنین طرحی را بر اساس ماده ۹۱ آیین‌نامه داخلی مجلس پیشنهاد

کرد که در آن هیئت‌ها پیش از دو اصلاحیه دیگر، به اصلاحیه پیشنهادی او رأی می‌دادند.

نماینده سوریه با ناکافی بودن اسناد بین‌المللی موجود به دلیل عدم توجه به استفاده از فناوری اطلاعات و ارتباطات (ICT) توسط گروه‌های تروریستی، از پیش‌نویس فدراسیون روسیه حمایت کرد. وی با اشاره به این‌که این متن منعکس‌کننده همه بحث‌هایی است که در طی مراحل آماده‌سازی در هفته‌های اخیر انجام‌شده است، گفت: برای ما، این متن مبنای قانونی و واقع‌بینانه‌ای برای حرکت به جلو است. در مورد اصلاحیه پیشنهادی برزیل، وی گفت که کمیته موقت باید از قوانین داخلی مجمع عمومی در تصمیم‌گیری با اکثریت ساده یا با اکثریت دوسوم در صورت لزوم پیروی کند. وی از اصلاحیه پیشنهادی هائیتی به نمایندگی از حوزه کارائیب استقبال کرد و درعین‌حال از اصلاحیه بریتانیا استقبال نکرد.

نماینده اتریش که خود را نیز با اتحادیه اروپا همراهی می‌کرد، این نکات را تکرار کرد. او گفت: «امید ما این بود که از دوقطبی شدن پرهیز کنیم و روند را باروحیه مثبت اجماع آغاز کنیم. در دوازدهم ماه مه، چندین هیئت نگرانی‌های خود را در مورد متن موردتوافق ایالات‌متحده و فدراسیون روسیه ابراز کردند. وی با ابراز ناامیدی از این‌که تلاش‌های رئیس مجمع برای حل این اختلافات با ورود سریع این پیش‌نویس به مجمع کاهش یافت، از اصلاحات ارائه‌شده توسط برزیل و بریتانیا حمایت کرد. وی همچنین با ابراز تأسف از این‌که موضوع محل برگزاری مذاکرات باعث ایجاد تفرقه شده است، تأکید کرد: هیچ سلسله مراتبی بین کرسی‌های سازمان ملل وجود ندارد.

ده ها هیئت در توضیح موضع خود درباره این پیش‌نویس، هم قبل

و هم بعد از رأی‌گیری صحبت کردند. نماینده پرتغال به نمایندگی از اتحادیه اروپا گفت که هیئت او در ابتدا نگران این بود که اقدامات کمیته موقت بدون اجماع کامل می‌تواند منجر به دوقطبی شدن بیشتر و عدم توافق شود، شکاف دیجیتالی را بدتر کند و توانایی کشورها برای مبارزه با جرائم سایبری را از بین ببرد. وی با اشاره به نگرانی‌های جدی بسیاری از هیئت‌ها که احساس می‌کردند نمی‌توانند دیدگاه‌های خود را در طول جلسه سازمانی به اشتراک بگذارند، به‌ویژه به دلیل این‌که چندین جلسه غیررسمی که وعده داده‌شده بود هرگز برگزار نشد، تصمیم یک‌جانبه برای ارائه متن اصلاح‌شده پیش از موعد به مجمع را «بسیار نگران‌کننده» توصیف کرد.

او گفت که این اقدامات، به‌ویژه نادیده گرفتن تلاش‌های رئیس کمیته برای برگزاری رایزنی‌های غیررسمی، بی‌احترامی به نظرات مختلف اعضا را نشان می‌دهد و اعتماد به نحوه انجام این فرآیند را از بین می‌برد. نماینده پرتغال گفت درحالی‌که اتحادیه اروپا ترجیح می‌دهد رئیس یک متن مصالحه آمیز را پیشنهاد کند، از اصلاحیه برزیل برای افزودن یک‌بند درباره اکثریت دوسوم در تصمیم‌گیری حمایت می‌کند.

درنهایت این کنوانسیون با عنوان «مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه» به‌اتفاق آرا پس از بحث و بررسی فشرده با سه اصلاحیه تصویب شد که دو مورد از آن‌ها مستلزم رأی‌گیری ثبت‌شده بود. در ادامه، مجمع هر اصلاحیه را به ترتیبی که دریافت کرد، موردبررسی قرارداد. با رأی‌گیری ابتدا به پیشنهاد برزیل، این اصلاحیه با ۸۸ رأی موافق در مقابل ۴۲ مخالف و ۳۲ رأی ممتنع به تصویب رسید. کشورهای عضو اصلاحیه پیشنهادی هائیتی به نمایندگی

از کشورهای حوزه کارائیب را بدون رأی به تصویب رساندند. آن‌ها سپس اصلاحیه پیشنهادی بریتانیا را با ۸۲ رأی موافق در مقابل ۳۳ مخالف و ۴۳ رأی ممتنع به تصویب رساندند. اگر تلاش‌ها بر سر تنظیم تصویب نهایی این معاهده شکست بخورد، همکاری در زمینه مبارزه با جرائم سایبری به‌صورت نظام‌های منطقه‌ای، پراکنده و حتی موقتی باقی خواهد ماند و یک رژیم قضای بین‌المللی و دارای فرایند شفاف در سراسر حوزه‌های قضایی شکل نخواهد گرفت.[1]

1. https://foreignpolicy.com/2022/02/11/un-cybercrime-treaty-russia-hacking/

بخش هفتم


موضوعات وملاحظات مبتنی بر منافع
ملی جمهوری اسلامی در کنوانسیون
UNODC

بخش هفتم

موضوعات و ملاحظات مبتنی بر منافع ملی جمهوری اسلامی در کنوانسیون

حرکت جامعه بین‌المللی به‌سوی انعقاد کنوانسیون‌هایی که در صدد ایجاد یک وحدت رویه جهت جرم انگاری و کیفر گذاری جرائم شدید است را باید بخشی از تلاش‌های جمعی در راستای برقراری یک سیستم حقوق کیفری بین‌المللی دانست. صاحب‌نظران دلایل مختلف و متعددی برای آغاز چنین جنبش حقوقی بزرگی نام می‌برند. جهانی‌شدن، افزایش سرعت رشد فناوری، جرائم نوپدید، عبور مجرمان از حصار مرزهای جغرافیایی و خطرناک شدن آثار جرائم نسبت به گذشته ازجمله مهم‌ترین دلایل است؛ اما سؤال مهمی که خود تبدیل به یک محل مناقشه است، بحث در خصوص این است که حقوق کیفری بین‌المللی دقیقا چیست؟ در پاسخ باید گفت که حقوق کیفری بین‌المللی یا حقوق بین‌الملل کیفری[1] در ادبیات حقوق بین‌الملل اصطلاحی است که بیانگر سه بحث کلی هست: ۱- مقررات حاکم بر دادرسی‌های مراجع بین‌المللی مثلاً دیوان کیفری بین‌المللی ۲- اجرای فرامرزی قوانین کیفری در مواردی که مجاز است ۳- حقوق کیفری داخلی در مواجهه با جرائم مهم بین‌المللی و یا الزام‌آور درنتیجه معاهدات. از سوی دیگر لازم به ذکر است که حقوق کیفری نظام بین‌المللی درواقع چیز جدایی از نظام‌های داخلی نیست.

۱. این اختلاف و تمایز در اصطلاح ناشی از اختلاف‌نظر میان علمای حقوق بین‌الملل است. بااین‌وجود، مطالعه آثار حقوق دانان فرانسوی ازآن‌جهت که ترتیب استعمال صفت و موصوف در زبان فرانسه شبیه به زبان فارسی است، نشان می‌دهد که ایشان غالباً تمایزی بین این دو اصطلاح قائل نشده‌اند.

درواقع، جامعه دولت‌ها توافق نموده‌اند که مجرمان بین‌المللی را در هر کجایی که یافتند محاکمه نمایند و این جیزی جز ذات حقیقی و فلسفه وجودی حقوق کیفری بین‌المللی نیست.

نکته مهم دیگری که نیازمند بذل‌توجه است، عبارت از این می‌باشد که تاکنون، نظامی مستقل از دادرسی کیفری داخل کشورها به عرصه وجود پا ننهاده است و دیوان کیفری بین‌المللی جدید التاسیس نیز دارای صلاحیت تکمیلی است و اعمال صلاحیت آن منوط به مواردی است که محاکم داخلی نخواهند و یا نتوانند به جرائم مذکور در اساس‌نامه آن دیوان رسیدگی نمایند و این نیز تأکیدی بر اجرای حقوق کیفری برای مهم‌ترین جرائم بین‌المللی در سطح جهان است. بر همین اساس، هنگامی‌که یک کنوانسیون بین‌المللی به تصویب می‌رسد، باید توجه داشت که در وهله نخست جامعه جهانی به یک اجماع و توافق جمعی در خصوص جدی بودن موضوع جرم رسیده است؛ این نکته مهم به‌خوبی در بند ب ماده ۲ کنوانسیون پالرمو و استعمال اصطلاح جرم شدید "Serious crime" معتنابه است. در وهله دوم، ایجاد یک سیاست جنایی مشترک باهدف حفاظت از جامعه در برابر آن جرم شدید به‌ویژه با استقرار وحدت رویه، تصویب قوانین مناسب و از همه مهم‌تر تقویت همکاری‌های بین‌المللی و محافظت از امنیت ملی و جمعی اعضا است.

با پایان یافتن جنگ سرد و آغاز فصل جدیدی از تاریخ روابط بین‌الملل، کارشناسان امنیتی اقدام به شناسایی گونه‌های جدیدی از تهدیدات امنیت ملی کردند که ماهیت متفاوتی با تهدیدات سنتی امنیت ملی داشته و از آن به تهدیدات امنیتی نوظهور تعبیر می‌شود. ماهیت این تهدیدات امنیتی خاص، آثار و پیامدهای آن‌ها و تبعات گسترده آن‌ها جامعه جهانی

را بـر آن داشـت تـا به‌منظـور مبـارزه مؤثـر با آن‌هـا اقدام بـه ایجـاد نظام‌های همـکاری بین‌المللـی و مبـارزه همه‌جانبـه بـا این‌گونـه از تهدیـدات کنـد. در شـرایط کنونی جرائم سـایبری به‌عنـوان جدیدترین نسـل از تهدیدات امنیتی بـا ویژگی‌هایی بسـیار متمایـز از جرائم سـنتی نیازمند انعقاد یک کنوانسـیون معتبـر و اکثریتـی بین‌المللـی و ضمانـت اجراهـای قطعی اسـت. بـرای تحقق ایـن موضـوع بایـد توجـه داشـت کـه تقویت مبانـی نظـری و مطالعاتـی برای این کنوانسـیون بسـیار حائز اهمیت اسـت؛ زیرا اهمیت موضوع سـبب خواهد شـد تـا حتی در صـورت انعقاد یک کنوانسـیون حداکثـری، بسـیاری از موارد منشـأ ایجـاد اختـلاف میان کشـورهای مختلف و یـا ابزاری برای سوءاسـتفاده کشـورهای قدرتمنـد و اثرگـذار بر جریان تنظیم متن کنوانسـیون شـود.

بـا توجـه بـه آنچـه گذشـت، در ادامه بـا در نظر داشـتن ایجـاد یک تحول پارادایمـی در زمینـه سیاسـت‌گذاری کیفـری در عرصـه بین‌المللـی بـه دلیل ظهـور بازیگـران فـرا دولتـی کـه معـارض بـا حکومت‌ها عمـل می‌کننـد و در برخـی مـوارد حاکمیـت و وفـاق ملـی را هـدف قـرار داده و کانون‌هـای قدرت بزرگـی بـرای خـود ایجـاد کرده‌انـد، بـه اولویت‌هـای مهـم جمهوری اسـلامی ایـران در کنوانسـیون جرائـم سـایبری پرداخته می‌شـود.

پیش از آغاز بحث، ذکر یک نکته ضروری به نظر می‌رسـد. کنوانسـیون‌های بین‌المللـی همانطـور کـه گفتـه شـد درصـدد ایجـاد یک وحـدت رویـه میان کشـورهای عضـو در خصـوص ایجـاد سـاختارهای یکسـان در جـرم انـگاری، شـیوه‌های کشـف جرم، تعقیب متهم و رسـیدگی قضایی هسـتند. هرچند هر کنوانسـیونی بنـا بر شـرایط خـاص حاکم بـر روح و متن خود برای کشـورهای عضـو حـق تحفـظ در نظـر می‌گیـرد، امـا ایـن حـق منجـر بـه نپذیرفتـن و اجرایی نکردن کلیت کنوانسـیون توسـط کشـور عضو نخواهد شـد. هر کشـور

عضو مستلزم است تا قوانین داخلی خود را اصلاح‌کرده و در صورت فقدان قوانین داخلی، قوانین کنوانسیون را در موضوع جرم اجرایی کند. درواقع ضمانت اجرایی هر کنوانسیونی همین پایبندی اعضا بر مفاد کنوانسیون است و چنانچه این اتفاق نیافتد به‌نوعی نقض غرض خواهد بود و اهداف کنوانسیون محقق نخواهد شد. این موضوع در قانون مدنی کشور ما نیز به‌عنوان یک اصل از حقوق بین‌الملل پذیرفته‌شده است طبق ماده ۹ قانون مدنی ایران، «مقررات عهودی که بر طبق قانون اساسی بین دولت ایران و سایر دول منعقدشده باشد در حکم قانون است».

البته لازم به ذکر است که در راستای این ماده، تنها معاهدات بین‌المللی - نه سایر منابع ایجاد تعهدات بین‌المللی ازجمله عرف - موردتوجه قرار می‌گیرند. معاهدهٔ موردنظر نیز باید به لحاظ بین‌المللی لازم‌الاجرا شده باشد و مراحل تصویب در نظام حقوقی ایران را طی کرده باشد. همچنین، اساس‌نامه یا سند مؤسس سازمان‌های بین‌المللی که دولت ایران به عضویت آن درمی‌آید، در چارچوب ماده ۹ قرار می‌گیرد؛ اما معاهداتی که ایران با سازمان‌های بین‌المللی منعقد می‌کند چنین ویژگی‌ای ندارند. همچنین است معاهداتی که مفاد آن به‌واسطهٔ اقتضائات خاص حقوق بین‌الملل برای دولت ایران لازم‌الاجراست[۱].

بر اساس آنچه گفته شد، جمهوری اسلامی ایران باید توجه داشته باشد که در خصوص کنوانسیون جرائم سایبری، بنا بر اولویت‌های خود و در راستای تأمین منافع و تحقق انتظارات از پیوستن به چنین کنوانسیون مهمی، در فرایند مذاکرات اصلاح و تصویب کنوانسیون با بهره‌گیری از بدنه کارشناسی و مشورت متخصصان برجسته داخلی، با چانه‌زنی شرایط ایده آلی در این کنوانسیون برای خود فراهم کند؛ زیرا در صورت عدم

۱. بذار، وحید، محدودهٔ اعمال ماده ۹ قانون مدنی نسبت به تعهدات بین‌المللی دولت ایران، فصلنامه قضاوت، دوره ۱۹، شماره ۹۷،خرداد ۱۳۹۸، صفحه ۴۹-۶۷

چنین اقدامی، شرایطی پیش خواهد آمد که شاید با اصول و ضوابط مدنظر نظام فاصله داشته و حتی در مواقعی مانع از پیوستن کشور به این کنوانسیون شود.

با طرح این مقدمه، به سراغ مرور برخی از اولویت‌های مهم جمهوری اسلامی ایران در کنوانسیون جرائم سایبری خواهیم رفت. محدوده و حوزه شمول کنوانسیون یک از موضوعات مهم و قابل‌بحث است. در خصوص محدوده و حوزه شمول کنوانسیون، به شکل دقیق‌تر و تخصصی‌تری باید از اصطلاح صلاحیت استفاده نمود. صلاحیت خود به دو نوع ذاتی و نسبی یا محلی تقسیم می‌شود. درباره صلاحیت ذاتی کنوانسیون مسلماً باید گفت که طیف وسیعی از جرائم سایبری قابل‌شناسایی است که کنوانسیون می‌تواند بنا بر تصریح در متن خود ناظر و صالح نسبت به آن جرائم سایبری باشد؛ اما باید توجه داشت که بر اساس عرف قانون‌گذاری، قانون‌گذار نمی‌تواند و منطقی هم نیست که تمامی جرائم موجود را مورد شناسایی قرار داده و آن‌ها را لیست کند. در مقابل راهکارهای گوناگونی وجود دارد که با توسل به آن می‌تواند صلاحیت و حوزه شمول کنوانسیون و یا هر متن قانونی را توسعه داد. یکی از بهترین راهکارها استفاده از معیار نوعی است. به‌عنوان‌مثال، بر اساس تجربه موفق کنوانسیون پالرمو می‌توان از معیار جرائم شدید استفاده نمود. درنتیجه ضروری است که یک تعریف جامعه و مانع از جرائم شدید سایبری در متن کنوانسیون ارائه گردد. صلاحیت تکمیلی، یکدیگر از تأسیسات حقوقی کاربردی و البته کار آزمایی شده است. به‌عنوان‌مثال، صلاحیت دیوان کیفری بین‌المللی تکمیلی است. منظور از صلاحیت تکمیلی این است که چنانچه جرائم مطروحه در کنوانسیون از سوی دادگاه‌های داخلی کشورهای عضو مورد

رسیدگی قرار نگیرد، یک مرجع رسیدگی‌کننده که آن نیز باید در متن کنوانسیون باید مشخص‌شده باشد، صالح به رسیدگی به آن جرم سایبری است. درنتیجه، دولت‌های عضو کنوانسیون که مایل هستند جرائم ارتکابی در قلمرو یا توسط اتباع آن‌ها در کشور خودشان مورد رسیدگی قرار گیرد، باید دادگاه صالح و نحوه رسیدگی به جرائم را در قانون داخلی مشخص کنند.

نکته مهم دیگر که نیازمند توجه است، موقعیت جغرافیایی و درواقع محل ارتکاب جرم است. در اینجا باید توجه داشت که گرچه جرائم سایبری در اینترنت اتفاق می‌افتد، اما باید میان بستر ارتکاب جرم و مکان خارجی که در جهان واقع مجرم در آنجا مستقر بوده و اقدام به ارتکاب جرم کرده است تفاوت قائل شد. در ادامه همین نکته، سیل متعددی از مسائل و چالش‌های مختلف در خصوص جرائم سایبری مطرح خواهد شد که یکی از مهم‌ترین آن‌ها، ایجاد تفکیک میان جرائم سایبری ملی و جرائم سایبری فراملی است. گاهی اوقات یک جرم سایبری در داخل مرزهای یک کشور اتفاق می‌افتد و صرفاً زیرساخت‌های همان کشور را مورد هدف قرار می‌دهد؛ اما موارد متعددی در سال‌های اخیر مشاهده‌شده است که یک موج حمله سایبری از مبدأ یک یا چند کشور، یک یا چند کشور را مورد هدف قرار می‌دهد.

از سوی دیگر، به رسمیت شناسی مسئولیت کیفری برای شخصیت‌های حقوقی و خصوصاً دولت‌ها مهم ترین بخش مبحث مسئولیت است. این نکته مهم در مذاکرات پیش‌نویس اساس‌نامه دیوان کیفری بین‌المللی خود را نشان داد. علی‌رغم آنکه نمایندگان بسیاری از کشورها موافق آن بودند که برای شخصیت‌های حقوقی و کشورها نیز مسئولیت کیفری در

نظر گرفته‌شده و دیوان صالح به رسیدگی به جرائم دستگاه‌ها یا نمایندگان آن‌ها هنگامی‌که جرم را به نام آن‌ها انجام می‌دهند باشد، نماینده کشور فرانسه مانع از تصویب بند ۵ ماده ۲۳ پیش‌نویس اساس‌نامه شد؛ اما در خصوص جرائم سایبری، یکی از مسائل قابل‌توجهی که به‌شدت به امنیت ملی کشورها آسیب می‌رساند و جمهوری اسلامی نیز قربانی این طیف از جرائم سایبری است، جرائم سایبری دولتی و شرکتی است. در شرایط کنونی، این جرائم علاوه بر ارتکاب از سوی شخصیت‌های فرا دولتی، به شکل سازمان‌یافته از سوی بسیاری از دولت‌ها نیز ارتکاب می‌یابد. از سوی دیگر، بسیاری از شخصیت‌های حقوقی همچون شرکت‌های بزرگ فناوری نیز در برخی موارد مرتکب جرائم سایبری می‌شوند که این چالش نیز به‌خوبی باید با به رسمیت شناسی مسئولیت کیفری شخصیت‌های حقوقی تدبیر شود.

نکته مهم دیگری که باید در خصوص آن تعیین تکلیف شود، شناسایی جنس جرائم سایبری دولتی است. ملاحظه رویه‌های اخیر برخی از سازمان‌های مهم بین‌المللی همچون سازمان پیمان آتلانتیک شمالی بیانگر آن است که رفته‌رفته جرائم سایبری دولتی به‌عنوان یک جرم جنگی تلقی شده و به کشور یا کشورهای قربانی جواز اقدام متقابل به شکل سخت و نظامی می‌دهد. این موضوع به شکل جدی در اجلاس‌های سالیانه ناتو موردبررسی قرارگرفته و بر همین مبنا ناتو فضای مجازی را به‌عنوان یک بستر عملیات نظامی مورد شناسایی قرار داده است.

اصلی‌ترین و قابل‌توجه‌ترین موضوع برای جمهوری اسلامی ایران در کنوانسیون مبارزه با جرائم سایبری فعالیت اثرگذار و پیگیرانه است. جمهوری اسلامی چنانچه خواهان تأمین حداکثری منافع ملی خود

در چنین کنوانسیون مهم و اثرگذاری است، نیازمند آن است تا با یک برنامه‌ریزی دقیق و حساب‌شده، در مقام یک عضو کلیدی در مرحله تهیه پیش‌نویس کنوانسیون ظاهر شود تا از این طریق بتواند منافع ملی خود را تأمین کند. بدون ایفای نقش و ایجاد گفتمان، مسلماً نمی‌توان انتظار تأمین منافع قابل‌توجهی برای کشور داشت. برای تحقق این امر مهم، در نخستین گام پیشنهاد می‌شود که در داخل کشور یک کارگروه ویژه متشکل از متخصصین فضای مجازی، جرم شناسان و کارشناسان حقوقی و همچنین افراد باتجربه و مسلط بر عرف تنظیم کنوانسیون‌های بین‌المللی و حقوق سازمان‌های بین‌المللی تشکیل شود. از سوی دیگر ضروری است تا این کارگروه در تعامل و ارتباط مستقیم با شورای عالی فضای مجازی، وزارت امور خارجه، قوه قضائیه و قوه مقننه باشد. اولویت و وظیفه اصلی این کارگروه نیز می‌بایست تهیه یک پیش‌نویس علمی و استاندارد و پیشنهاد آن در مذاکرات مقدماتی و جلسات کارشناسی کنوانسیون باشد.

ایجاد چنین پرستیژی طی فرایند شکل‌گیری این کنوانسیون زمینه آن خواهد شد تا جمهوری اسلامی با اثرگذاری به‌مراتب بیشتری بتواند منافع ملی خود و شرکای هم‌سود خویش را پیگیری کند و البته در همین زمینه با اولویت قرار دادن منافع ملی باید در تعامل و مشورت با شرکای خود نیز باشد.

دلیل تأکید مؤکد به حضور فعال جمهوری اسلامی ایران در فرایند تهیه پیش‌نویس و امور مقدماتی کنوانسیون از یک‌سو ناشی از این امر مهم هست که یقیناً این کنوانسیون با توجه به اهمیت و توسعه روزبه‌روز فضای مجازی و ضریب نفوذ آن در زندگی بشریت تبدیل به یکی از مهم‌ترین کنوانسیون‌های قرن حاضرشده و از سوی دیگر به این دلیل است که

عدم مشارکت فعال، ابراز نظر کارشناسی و رویکرد منفعلانه کشور در فرایندهای مقدماتی مهم‌ترین کنوانسیون‌های سالیان گذشته همچون کنوانسیون‌های پالرمو و مریدا سبب شده است که نه‌تنها جمهوری اسلامی ایران نتوانسته است گفتمان خویش را در عرصه قانون‌گذاری بین‌المللی مطرح کرده و از این طریق منافع خویش را تأمین کند، بلکه این رویکرد انفعالی عرصه بسیاری مناسبی برای دشمنان و رقبای جمهوری اسلامی ایران فراهم کرده است تا بتوانند با ایجاد ضمانت اجرای بین‌المللی برای خواسته‌ها و منافع ملی خود، ایران را تحت‌فشار و تنگنا قرار دهند؛ به‌عبارت‌دیگر، کنوانسیون مبارزه با جرائم سایبری را باید به‌عنوان یک فرصت مناسب برای عملیاتی سازی فاز دیپلماسی سایبری جمهوری اسلامی ایران در نظر گرفت. دیپلماسی دیجیتال از یکسو محصول گسترش نفوذ فضای مجازی و تأثیرات فن‌آوری‌های نوین اطلاعاتی و ارتباطاتی بر ماهیت، اهداف، ابزارها و فرآیندهای دیپلماسی سنتی و از سوی دیگر محصول واکنش طبیعی و پاسخ هوشمندانه ساختارهای دیپلماتیک کشورها به فرصت‌ها و تهدیدات ناشی از تحولات و روندهای بین‌المللی اکوسیستم فضای مجازی ازجمله تضعیف حاکمیت‌های ملی و تأثیرات عمیق و گسترده آن بر روابط بین‌الملل و ژئوپلیتیک قدرت است. دیپلماسی دیجیتال به‌عنوان قلمرو جدیدی در سیاست خارجی کشورها و ابزاری برای تحقق اهداف و منافع ملی با بهره‌گیری از ظرفیت‌های فضای سایبری شناخته‌شده و در ابعادی چون دستگاه دیپلماسی دیجیتال، دیپلماسی دیجیتال رسمی، دیپلماسی عمومی سایبری و دیپلماسی سایبری شرکتی مطرح هست.

با توجه به آنچه گذشت، برخی از مهم‌ترین ملاحظات و موضوعات

مهمی که جمهوری اسلامی ایران باید در کنوانسیون مبارزه با جرائم سایبری پیگیری نماید، عبارت است از:

۱. «ماهیت جهانی و بدون مرز اینترنت»

۲. «ساختار توزیع‌شده آن و تنوع ذینفعان آن»

۳. «روند وابستگی متقابل دیجیتال میان کشورها»

۴. «بین‌المللی شدن ماهیت تهدیدات، حملات و جرائم سایبری»

۵. «گسترش ساخت، اشاعه و استفاده از تسلیحات سایبری توسط قدرت‌ها»

۶. «انتقال بی‌ضابطه بین مرزی داده‌ها و نقض حریم خصوصی و حفاظت از داده‌ها»

۷. «تشدید سوءاستفاده از فضای مجازی به‌عنوان ابزار اِعمال فشار و مداخله در امور داخلی کشورها و تشدید اقدامات سازمان‌یافته باهدف بی‌ثبات‌سازی، ضربه به منافع ملی، امنیت ملی، فرآیندهای انتخاباتی، سلامت اجتماعی و اقتصادی کشورها بر بستر آن»

۸. «تأکید بر شکل‌گیری نظم جدید در نظام بین‌الملل فضای مجازی در حوزه توسعه قلمروی بومی و مکانیسم حکمرانی بین‌المللی فضای مجازی مبتنی بر قواعد، چندجانبه، شفاف، عادلانه، اخلاق‌مدار، مبتنی بر اصول حاکمیت ملی کشورها، مزایا و منافع مشترک با مشارکت برابر همه کشورها در چارچوب کنوانسیون»

۹. «واکنش به انتساب حملات سایبری به کشورهایی مانند ایران از سوی آمریکا در جهت اِعمال فشار و زمینه‌سازی تداوم و تشدید تحریم‌های سایبری و غیر سایبری و تشدید و توجیه فرآیند تحریم اشخاص حقیقی و حقوقی ایرانی به بهانه دست داشتن در فعالیت‌های

مخرب سایبری علیه منافع و امنیت ملی آمریکا و محدودسازی ارائه خدمات پایه و کاربردی به آن‌ها.»

۱۰. «ظهور فناوری‌های دولت گریز و قانون‌گریز»

۱۱. «آسیب‌ها و مخاطرات فضای مجازی برای کودکان و نوجوانان»

مصادیق مدنظر برای جرم انگاری در کنوانسیون نیز از دیگر مبحث‌های مناقشه برانگیز کنوانسیون است که نیازمند چانه‌زنی فعال و حضور پر رنگ جمهوری اسلامی ایران در فرایند تنظیم سند است. همان‌گونه که گفته شد، ماهیت چنین کنوانسیون‌هایی اقتضا می‌کند که وارد جزئیات نشده و لیست طول و درازی از جرائم را طرح نکند. در عوض، جرم انگاری جرائم شدید و با دامنه اثرگذاری گسترده و مخرب که امنیت ملی و جمعی کشورهای مختلف را مورد تهدید قرار می‌دهد، چالاکی و کارایی کنوانسیون را به‌شدت افزایش می‌دهد. چراکه بر اساس اصل صلاحیت ملی، این وظیفه کشورها است که در وهله نخست با جرم انگاری جرائم اقدام به برقرار امنیت و محافظت از جامعه کنند. از همین رو، ذکر جرائمی همچون سرقت هویت، کلاه‌برداری اینترنتی، دزدی اطلاعات و امثالهم صرفاً تکرار مکررات است و ارزش‌افزوده‌ای برای کنوانسیون ایجاد نمی‌کند. کنوانسیون مبارزه با جرائم سایبری باید بیشتر در مسیر ایجاد امنیت و حفاظت جمعی حرکت کرده و قابلیت بازدارندگی در قبال جرائم شدید سایبری که از سوی بازیگران اصلی فضای سایبر ارتکاب می‌یابد را داشته باشد؛ بر همین اساس توصیه می‌شود بیشتر بر جرم انگاری موارد ذیل تأکید شود:

۱. جرم انگاری جرائم سایبری دولتی.

۲. جرم انگاری جرائم سایبری شرکتی.
۳. جرم انگاری و تشدید مجازات جرائم سایبری سازمان‌یافته.
۴. جرم انگاری خریدوفروش حجم قابل‌توجه داده‌های خام یا تجزیه‌شده به‌منظور اهداف نامشروع و غیراخلاقی.
۵. جرم انگاری سوءاستفاده از داده‌های گردآوری‌شده به‌منظور اهداف نظامی، ایجاد ناآرامی و شورش در کشورهای مختلف.
۶. پیش‌بینی سازوکار عادلانه و موردتوافق حداکثری به‌منظور انتساب جرائم سایبری.

جمع‌بندی

جمع‌بندی

علی‌رغم آنکه اینترنت و فناوری‌های مربوط به آن در طول قرن بیست و یکم نسبت به بسیاری از فناوری‌های دیگر رشد و توسعه سریع‌تری داشته و جرائم مربوط به آن نیز با همین سرعت درحرکت بوده و تمامی کشورهای جهان را کم‌وبیش متأثر ساخته است تاکنون شاهد یک عزم همگانی برای ایجاد یک سیاست جنایی واحد در مبارزه با جرائم سایبری نبوده‌ایم. کنوانسیون بوداپست نیز با توجه به آنکه نتوانست مشارکت کشورهای مختلف جهان را جلب کند و بیشتر در کانون توجه کشورهای اروپایی قرار دارد، توفیق چندانی در زمینه مبارزه با جرایم سایبری کسب نکرد؛ مضاف بر این، مرجع تصویب این کنوانسیون نیز شورای اروپا است و مسلما مقبولیت کمتری نسبت به کنوانسیون های تحت نظر سازمان ملل متحد دارد. عدم شکل گیری یک توافق همه جانبه و با مقبولیت حداکثری با گذشت سال ها از ظهور اینترنت و تبدیل شدن آن به یک بستر استراتژیک می‌تواند متأثر از موارد مختلفی باشد. بدون شک کشورهای مختلف دارای منافع تعریف‌شده متفاوتی در اینترنت هستند. بسیاری از کشورهای جهان با نظامی سازی اینترنت آن را تبدیل به یک جنگ‌افزار کرده و بر ضد دشمنان خود

استفاده می‌کنند. برخی از کشورها با ارتکاب جرائم سایبری اقدام به کسب درآمدهای هنگفت می‌کنند و برخی دیگر از کشورها، به دلایلی همچون توسعه‌نیافتگی و یا ناآرامی‌های داخلی انگیزه و توانی برای مبارزه با جرائم سایبری ندارند؛ اما آن چیز که مسلم است، این است که اینترنت یک موضوع چند ذی‌نفعی است. افراد، سازمان‌ها و شرکت‌ها، دولت‌ها و شخصیت‌های نوظهور فرا دولتی همگی جز ذی‌نفعان اینترنت هستند و شرط اصلی تأمین جریان ثابت منفعت در این فضای نظارت گریز و آنارشیک، بدون شک برقراری امنیت است. جرائم سایبری، تمامی ذی‌نفعان اینترنت را تحت تأثیر قرار می‌دهند و ادامه فعالیت در بستر آن را با اخلال مواجه می‌کنند. با مرتبط شدن بخش‌های بیشتری از زندگی بشر به اینترنت، این وابستگی و به شکل متقابل، آسیب‌پذیری از جرائم سایبری نیز بیشتر و بیشتر خواهد شد. برای برقراری و تأمین امنیت در این فضای جمعی، جامعه جهانی نیازمند آن است که بر موانع مهمی فائق آمده و حتی در مواقعی با کاستن از برخی منافع، در راستای برقراری یک نظام حقوقی جمعی، تنظیم‌گر و بازدارنده گام بردارد. تعارض منافع کشورهای جهان با سطوح بالای قدرت و قابلیت حکمرانی در فضای مجازی یکی از مهم‌ترین موانع دست‌یابی به این هدف است.

همان‌طور که در اثنای این گزارش اشاره شد، اینترنت یک عرضه آنارشیک است که نمی‌توان در آن هیچ قدرت غالب و حکمران را مورد شناسایی قرارداد. شاید پذیرش این واقعیت، جهان را وارد مرحله جدیدی از قرارداد اجتماعی کند. به این معنا که تمامی اعضا، از برخی از حقوق و آزادی‌های خویش چشم‌پوشی کنند تا در مقابل به یک امنیت و آزادی جمعی مداوم دست پیدا کنند. مسلماً این ایده در بادی امر به‌شدت

آرمان‌گرایانه خواهد بود و با توجه به شرایط کنونی جهان بسیار دور از ذهن به نظر برسد؛ اما به‌عنوان یک‌راه حل نهایی باید به آن توجه کرد و در راستای آن گام برداشت. شرایط حاکم بر حال حاضر عرصه بین‌الملل، خود یکی از اصلی‌ترین موانع پیش روی دست‌یابی به چنین توافقی است. حتی اگر درصدد دست‌یابی به چنین آرمانی هم نباشیم و بخواهیم به آنچه موجود است بسنده کنیم بازهم به نظر می‌رسد که نهایی شدن این کنوانسیون بر اساس آن طرح اولیه که از سوی دولت روسیه پیشنهادشده است کمی بعید باشد. روسیه با حمله به اکراین در ضعیف‌ترین موقعیت سیاسی خود در عرصه روابط بین‌المللی قرارگرفته و به نظر می‌رسد بیش از هرزمانی قدرت چانه‌زنی خود را در مقابل رقیب سنتی‌اش یعنی ایالات‌متحده آمریکا و دولت‌های غربی ازدست‌داده است. با توجه به آنکه سازمان ملل متحد در سال گذشته به طرح روسی رأی مثبت داده است، دور از ذهن نیست که تجدیدنظرهای اساسی در خصوص این طرح انجام بگیرد. از سوی دیگر، اختلاف نظر های عمیق و تفاوت های بنیادین در نظام های حکمرانی بر اینترنت ابرقدرت هایی همچون روسیه و چین در شرق از یک سو و ایالات‌متحده آمریکا و شرکایش در غرب دست‌یابی به چنین توافقی را به‌شدت دشوار و شکننده می‌کند. ابرقدرت‌های شرقی به‌شدت تحت تأثیر تنظیم گری دولتی و کنترل اینترنت قرار دارند و دغدغه‌های آن‌ها نسبت به جرائم سایبری نیز طبیعتاً متأثر از این شیوه حکمرانی است. درحالی‌که در غرب نگرانی در خصوص آسیب‌پذیری ارزش‌هایی مثل آزادی بیان و حریم خصوصی کاربران از توسعه دامنه جرائم در اولویت نمایندگان کشورها قرار دارد (همانگونه که در بررسی مشروح مذاکرات نمایندگان دیده شد) و رویکرد تفسیر مضیق

قوانین جزایی، تحدید دامنه جرم انگاری و حداقلی کردن عناوین مجرمانه به‌منظور عدم ایجاد تورم قضایی به چشم می‌خورد. بااین‌حال و فارغ از جمیع این اوصاف، آنچه قطعی و حتمی است، نیاز مبرم کنونی جامعه جهانی به ایجاد یک کنوانسیون قدرتمند جهت مبارزه با جرائم سایبری است.

ضمیمه

ضمیمه

پروپوزال کنوانسیون سازمان ملل متحد در مورد مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه

کشورهای طرف این کنوانسیون با مواردی به شرح زیر موافقت می کنند:

اعتقاد دارند فضای اطلاعاتی باید با رعایت دقیق اصول و هنجارهای اصلی حقوق بین‌الملل از جمله اصول احترام به حقوق و آزادی‌های بشر و اصول حل‌وفصل مسالمت‌آمیز اختلافات ساخته شود،

این نکته را که هر کشوری دارای حق حاکمیت و اعمال صلاحیت قضایی بر قلمرو خود با توجه به فضای اطلاعاتی مطابق با قوانین داخلی خود است را در نظر دارند،

برای جدی بودن مشکلات و تهدیدات ناشی از جرائم حوزه فناوری اطلاعات و ارتباطات، برای ثبات و امنیت جامعه که نهاد ها و ارزش‌های دموکراتیک و عدالت را تضعیف کرده و بر توسعه پایدار و حاکمیت قانون تأثیر منفی می‌گذارد اهمیت قائل‌اند،

همچنین در خصوص سوءاستفاده مجرمانه از فناوری اطلاعات و ارتباطات که فرصت‌های فراوانی را برای دیگر اشکال فعالیت‌های مجرمانه از جمله حملات رایانه‌ای به تأسیسات زیرساختی حیاتی، جاسوسی سایبری، بهره‌کشی آنلاین جنسی از کودکان، تروریسم، کلاه‌برداری، قاچاق داده‌های

شخصی و پول‌شویی نگران‌اند.

در مورد افزایش تعداد جرائم فناوری اطلاعات و ارتباطات که مقادیر زیادی از دارایی که ممکن است بخش قابل‌توجهی از منابع دولت‌ها را تشکیل دهد در برمی‌گیرد و ثبات سیاسی و توسعه پایدار آن کشورها را تهدید کند نگرانی زیادی دارند،

اعتقاد دارند که جرائم فناوری اطلاعات و ارتباطات یک پدیده فراملی است که جامعه و اقتصاد همه کشورها را تحت تأثیر قرار داده و همین امر همکاری بین‌المللی برای پیشگیری و مبارزه با چنین جرائمی را ضروری می کند.

در خصوص نیاز به کمک‌های فنی در مقابله با جرائم فناوری اطلاعات و ارتباطات که نقش مهمی در افزایش ظرفیت دولت‌ها برای پیشگیری مؤثر از این جرائم و ارتقای سطح امنیت اطلاعات ایفا می‌کند متقاعد شده‌اند،

این نکته را در نظر دارند که پیشگیری و ریشه‌کنی جرائم فناوری اطلاعات و ارتباطات به عهده همه دولت‌ها است و دولت‌ها باید برای اطمینان از اثربخشی تلاش‌های خود در این زمینه با حمایت و مشارکت همکاری‌های عمومی و خصوصی، مشاغل و افراد و گروه‌های خارج از بخش عمومی، مانند جامعه مدنی با یکدیگر همکاری کنند، زیرا امنیت کلی محیط اطلاعاتی به تلاش‌های جمعی هر کشور بستگی دارد،

در پیشگیری، کشف و سرکوب مؤثر نقل و انتقالات بین‌المللی دارایی‌هایی که به‌طور غیرقانونی در نتیجه جرائم فناوری اطلاعات و ارتباطات به‌دست‌آمده و همچنین در تقویت همکاری بین‌المللی در بازیابی دارایی‌ها مصمم هستند،

اصل انصاف، برابری در برابر قانون و نیاز به پرورش یک فضای فرهنگی در جامعه که جرائم فناوری اطلاعات و ارتباطات را تحمل نکند را در نظر دارند،

قطعنامه شماره ۲۷۴/۷۴ مجمع عمومی سازمان ملل متحد مورخ ۲۷ دسامبر ۲۰۱۹ با عنوان (مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه) که یک کمیته بین‌دولتی موقتی از کارشناسان برای تدوین کنوانسیون بین‌المللی جامع در مورد مقابله با استفاده از فناوری اطلاعات و ارتباطات برای مقاصد مجرمانه است را، در نظر دارند.

ماده ۱- اهداف کنوانسیون

اهداف کنوانسیون به این شرح است:

ترویج و تقویت اقدامات پیشگیرانه و مبارزه مؤثر با جرائم و سایر اقدامات غیرقانونی در زمینه فناوری اطلاعات و ارتباطات، جلوگیری از:

-اقدامات علیه محرمانگی، یکپارچگی و در دسترس بودن فناوری اطلاعات و ارتباطات؛

-سوءاستفاده از فناوری اطلاعات و ارتباطات؛

از طریق:

- جرم انگاری اعمال مشمول این کنوانسیون؛

-ارائه اختیارات کافی برای مبارزه مؤثر با این‌گونه جرائم و سایر اعمال غیرقانونی از طریق تسهیل در کشف، تحقیق و بررسی آن‌ها؛ پیگرد قانونی در سطح داخلی و بین‌المللی؛

-ایجاد ترتیباتی برای همکاری بین‌المللی؛

بهبود کارایی همکاری‌های بین‌المللی و توسعه این همکاری‌ها به‌ویژه در زمینه آموزش کارکنان و ارائه کمک‌های فنی برای پیشگیری و مبارزه با این جرائم.

ماده ۲- دامنه کاربرد

هر کشور عضو بدون تعصب به قوانین داخلی خود باید تلاش کند تا اقداماتی را اتخاذ کند تا به ابتکار خود و مشروط بر این که به تحقیقات یا اقدامات قضایی انجام شده توسط مقامات ذیصلاح خود لطمه ای وارد نکند، اطلاعات مربوط به اموال به دست آمده از ارتکاب یک جرم مطابق این کنوانسیون را در زمانی که فکر می‌کند افشای چنین اطلاعاتی ممکن است زمینه‌ای را برای مقامات ذیصلاح دولت عضو پذیرنده فراهم کند تا تحقیقات یا رسیدگی قضایی را آغاز کنند یا ممکن است منجر به درخواست آن کشور برای این کار شود ارسال کند. این کنوانسیون، مطابق با مفاد آن، در مورد پیشگیری، کشف، سرکوب، تحقیق و تعقیب جرائم و سایر اعمال غیرقانونی مقرر در مواد ۶ تا ۲۹ این کنوانسیون و اجرای اقداماتی برای از بین بردن پیامدهای این کنوانسیون از طریق تعلیق معاملات مربوط به دارایی های به دست آمده در نتیجه ارتکاب جرم یا سایر اعمال غیرقانونی مطابق این کنوانسیون و توقیف، مصادره و استرداد عواید حاصل از این جرایم باید اعمال شود.

به منظور اجرای این کنوانسیون، لازم نیست که جرایم و سایر اعمال غیرقانونی مطابق این کنوانسیون منجر به خسارت مالی شود، مگر در مواردی که در این کنوانسیون به نحو دیگری مقرر شده است.

ماده ۳- حفاظت از حاکمیت

دولت‌های عضو تعهدات خود را طبق این کنوانسیون مطابق با اصول حاکمیت دولت‌ها، برابری حاکمیتی کشورها و عدم‌مداخله در امور داخلی سایر کشورها انجام خواهند داد. این کنوانسیون به مقامات صلاحیت‌دار یک دولت عضو اجازه نخواهد داد که در قلمرو کشور دیگر امور قضایی و وظایفی را که طبق قوانین داخلی آن دولت منحصراً برای مقامات خودش محفوظ است، اعمال کنند، البته به‌غیراز مواردی که در این کنوانسیون پیش‌بینی‌شده باشد.

ماده ۴-تعریف اصطلاحات

الف) «توقیف اموال» به معنای ممنوعیت موقت انتقال، تبدیل، واگذاری یا جابجایی اموال، یا بر عهده گرفتن موقت نگهداری یا کنترل اموال به‌موجب حکم دادگاه یا سایر مراجع ذیصلاح است.

ب) «بات‌نت»[1] به دو یا چند دستگاه فناوری اطلاعات و ارتباطات گفته می‌شود که نرم‌افزارهای مخرب روی آن‌ها نصب‌شده و بدون اطلاع کاربران به‌صورت مرکزی کنترل می‌شوند.

ج) «نرم‌افزار مخرب» به نرم‌افزاری اطلاق می‌شود که هدف آن اصلاح، تخریب، کپی و مسدود کردن غیرمجاز اطلاعات یا خنثی‌سازی نرم‌افزار مورداستفاده برای ایمن کردن اطلاعات دیجیتال است.

د) «هرزه‌نگاری کودکان» مطابق ماده ۲ (ج) پروتکل اختیاری ۲۵ مه ۲۰۰۰ کنوانسیون حقوق کودک در مورد فروش کودکان، فحشا و هرزه‌نگاری کودکان به‌کاررفته است.

ه) «عواید» به معنای هرگونه دارایی است که مستقیم یا غیرمستقیم

1. Botnet

بات‌نت‌ها شبکه‌هایی هستند که با در اختیار گرفتن مجموعه‌ای از کامپیوترها که بات(bot) نامیده می‌شوند، تشکیل می‌شوند. این شبکه‌ها توسط یک یا چند مهاجم که botmasters نامیده می‌شوند، با هدف انجام فعالیت‌های مخرب کنترل می‌گردند. به عبارت بهتر، ربات‌ها کدهای مخربی هستند که بر روی کامپیوترهای میزبان اجرا می‌شوند تا امکان کنترل نمودن آن‌ها از راه دور را برای botmasterها فراهم نمایند و آن‌ها بتوانند این مجموعه را وادار به انجام فعالیت‌های مختلف نمایند.

از طریق ارتکاب جرم یا سایر اعمال غیرقانونی مقرر در این کنوانسیون به‌دست‌آمده و همچنین درآمد یا سایر منافع حاصل از این عواید، از دارایی چنین درآمدهایی تبدیل‌شده‌اند یا از اموالی که چنین عوایدی با آن مخلوط شده است کسب‌شده‌اند.

و) «فناوری اطلاعات و ارتباطات» (ICT) به فرآیندها و روش‌های تولید، پردازش و توزیع اطلاعات و همچنین راه‌ها و روش‌های اجرای آن‌ها اطلاق می‌شود.

ز) «شبکه‌های اطلاعاتی و مخابراتی» به مجموعه‌ای از تجهیزات مهندسی اطلاق می‌شود که برای کنترل فرآیندهای فناوری از طریق فناوری رایانه و مخابرات طراحی‌شده‌اند.

ح) «اموال» عبارت است از هر نوع دارایی، اعم از مادی یا غیرمادی، منقول یا غیرمنقول، مشهود یا نامشهود، ازجمله پول در حساب‌های بانکی، دارایی‌های مالی دیجیتال، ارز دیجیتال و رمز ارزها و اسناد قانونی یا اسنادی که مالکیت دارایی یا هر بخشی از آن را نشان می‌دهد.

ط) «اطلاعات» به معنای هرگونه داده (پیام‌ها، سوابق) است، صرف‌نظر از شکلی که در آن ارائه‌شده است.

ی) مصادره به معنای سلب اجباری اموال بدون غرامت به‌موجب حکم دادگاه یا سایر مراجع ذیصلاح است.

ک) «حمله رایانه‌ای» به معنای تداخل هدفمند نرم‌افزار و (یا) سخت‌افزار و نرم‌افزار با سیستم‌های اطلاعاتی یا شبکه‌های اطلاعاتی و مخابراتی برای مختل کردن و (یا) خاتمه دادن به عملکرد آن‌ها و (یا) تهدید امنیت اطلاعات پردازش‌شده توسط این امکانات است.

ل) «اطلاعات دیجیتالی» به هرگونه داده (سوابق) اطلاق می‌شود

که صرف‌نظر از شکل و مشخصات موجود و پردازش‌شده در سامانه‌ها، دستگاه‌ها و شبکه‌های اطلاعاتی و مخابراتی است.

م) «زیرساخت اطلاعات حیاتی» به مجموعه‌ای از تأسیسات زیرساخت اطلاعات حیاتی و شبکه‌های مخابراتی که برای اتصال تأسیسات زیرساخت اطلاعات حیاتی استفاده می‌شوند، اطلاق می‌شود.

ن) «تأسیسات زیرساختی حیاتی» به سیستم‌های اطلاعاتی و شبکه‌های اطلاعاتی و ارتباطی مقامات دولتی و سیستم‌های اطلاعاتی و سیستم‌های کنترل فرآیند خودکار فعال در بخش‌های دفاعی، بهداشتی، آموزشی، حمل‌ونقل، ارتباطات، انرژی، بانکی و مالی، هسته‌ای و غیره اطلاق می‌شود که حوزه‌های مهم زندگی دولت و جامعه را تشکیل می‌دهند.

و) «ارائه‌دهنده خدمات» به این معناست: ۱) هر نهاد دولتی یا خصوصی که توانایی برقراری ارتباط از طریق فناوری اطلاعات و ارتباطات را در اختیار کاربران خدمات خود قرار می‌دهد؛ و ۲) هر نهاد دیگری که اطلاعات الکترونیکی را از طرف یک‌نهاد ذکرشده در بخش (۱) یا کاربران خدمات ارائه‌شده توسط آن نهاد پردازش یا ذخیره می‌کند.

ه) «داده‌های ترافیکی» به معنای هرگونه اطلاعات الکترونیکی (به‌استثنای محتویات داده‌های انتقال‌یافته) مربوط به انتقال داده‌ها از طریق فناوری اطلاعات و ارتباطات است و به‌ویژه مبدأ، مقصد، مسیر، زمان، تاریخ، اندازه، مدت و نوع سرویس شبکه زیربنایی.

ی) «دستگاه فناوری اطلاعات و ارتباطات» به معنای مجموعه (گروه) اجزای سخت‌افزاری است که برای پردازش خودکار، ذخیره‌سازی و انتقال اطلاعات الکترونیکی استفاده می‌شود.

ر) «ادله الکترونیکی» به هرگونه اطلاعات ادله و مدارکی اطلاق

می‌شود که به شکل دیجیتال (بر روی یک رسانه الکترونیکی) ذخیره یا منتقل‌شده است.

ز) اصطلاح «خسارت اساسی» باید مطابق با قوانین داخلی دولت عضو درخواست شونده تعیین شود.

فصل دوم

جرم انگاری، دادرسی کیفری و اجرای قانون

ماده ۵- هر دولت عضو، اقدامات قانونی و سایر اقدامات لازم را اتخاذ می‌نماید و این کنوانسیون برای دولت‌ها ایجاد مسئولیت می‌کند تا طبق قوانین داخلی خود چنین مواردی را به‌عنوان جرم اعلام کند. مواد این کنوانسیون، ضمن اعمال مجازات کیفری و سایر مجازات، ازجمله حبس، سطح خطر عمومی ناشی از یک جرم معین و وسعت آن را نیز در نظر می‌گیرد.

ماده ۶- خسارت ایجادشده ناشی از دسترسی غیرمجاز به اطلاعات الکترونیکی

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا طبق قوانین داخلی خود دسترسی غیرمجاز و عمدی به اطلاعات دیجیتال را که منجر به تخریب، مسدود کردن، تغییر یا کپی کردن آن شده است، به‌عنوان یک جرم اعلام کند.

ماده ۷- شنود غیرمجاز

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ

کند تا ره‌گیری عمدی اطلاعات دیجیتالی را که بدون مجوز مناسب و/ یا با نقض قوانین تعیین‌شده، برای ره‌گیری داده‌های ترافیکی و داده‌های پردازش‌شده که برای استفاده عمومی در نظر گرفته نشده‌اند و با استفاده از فناوری اطلاعات و ارتباطات صورت می‌پذیرد، بر اساس قوانین داخلی خود به‌عنوان جرم تلقی کند.

ماده ۸- مداخله غیرمجاز نسبت به اطلاعات دیجیتالی

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا مداخله عمدی غیرمجاز در اطلاعات دیجیتال از طریق آسیب رساندن، حذف، تغییر، مسدود کردن، اصلاح یا کپی کردن آن را تحت قوانین داخلی خود به‌عنوان یک جرم تلقی کند.

ماده ۹- اخلال در شبکه‌های اطلاعاتی و ارتباطی

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا هر عمل غیرمجاز عمدی باهدف ایجاد اختلال در شبکه‌های اطلاعاتی و ارتباطی که منجر به عواقب جدی شده را به‌عنوان جرم به رسمیت بشناسد.

ماده ۱۰- ایجاد، استفاده و توزیع نرم‌افزارهای مخرب

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا ایجاد عمدی، انطباق، استفاده و توزیع نرم‌افزارهای مخرب برای کشور، تخریب غیرمجاز، مسدود کردن، تغییر، کپی، انتشار اطلاعات دیجیتال، یا خنثی کردن ویژگی‌های امنیتی آن، به‌استثنای تحقیقات قانونی را بر اساس قوانین داخلی خود به‌عنوان یک جرم اعلام کند.

هر کشور عضو، اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا ایجاد یا استفاده از یک بات نت به‌منظور ارتکاب هر یک از اعمال پیش‌بینی‌شده در مواد ۶ تا ۱۲ را، بر اساس قوانین داخلی خود به‌عنوان جرم تلقی کند.

ماده ۱۱- مداخله غیرمجاز در زیرساخت‌های اطلاعاتی حیاتی

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا ایجاد، توزیع و (یا) استفاده عمدی از نرم‌افزار یا سایر اطلاعات دیجیتالی، تداخل غیرمجاز در زیرساخت‌های اطلاعاتی حیاتی، تخریب، مسدود کردن، اصلاح، کپی کردن اطلاعات موجود در آن، یا خنثی کردن ویژگی‌های امنیتی که آگاهانه برخلاف قانون طراحی‌شده‌اند به‌عنوان جرم تلقی کند. هر کشور عضو، بایداقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا نقض قوانین عملکرد رسانه‌های طراحی‌شده برای ذخیره‌سازی، پردازش و انتقال داده‌های دیجیتالی محافظت‌شده موجود در زیرساخت‌های اطلاعاتی حیاتی یا سیستم‌های اطلاعاتی شبکه‌های اطلاعاتی و ارتباطی که به زیرساخت‌های اطلاعاتی حیاتی تعلق دارند را بر اساس قوانین داخلی خود به‌عنوان جرم تلقی کند.

ماده ۱۲- دسترسی غیرمجاز به داده‌های شخصی

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا طبق قوانین داخلی خود دسترسی غیرمجاز به داده‌های شخصی به‌منظور از بین بردن، تغییر، کپی یا اشتراک‌گذاری آن‌ها را به‌عنوان یک جرم تلقی کند.

ماده ۱۳- قاچاق غیرمجاز دستگاه‌ها

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا طبق قوانین داخلی خود، ساخت، فروش، خرید غیرقانونی برای استفاده، واردات، صادرات یا سایر اشکال انتقال برای استفاده از وسایلی که اساساً به‌منظور ارتکاب هر یک از جرائم مقرر در مواد ۶ تا ۱۲ این کنوانسیون طراحی یا اقتباس‌شده‌اند را، به‌عنوان یک جرم تلقی کند. مفاد این ماده زمانی که ساخت، فروش، خرید برای استفاده، واردات، صادرات یا سایر اشکال انتقال برای استفاده از دستگاه‌ها، به دلیل آزمایش مجاز یا حفاظت از سیستم‌های رایانه‌ای باشد قابل‌اجرا نخواهد بود.

ماده ۱۴- سرقت مرتبط با فناوری اطلاعات و ارتباطات

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا طبق قوانین داخلی خود سرقت یا کسب غیرقانونی مربوط با آن، از طریق کلاه‌برداری، تخریب، مسدود کردن، اصلاح یا کپی داده‌های دیجیتال یا تداخل دیگر با عملیات فناوری اطلاعات و ارتباطات. به‌عنوان جرم تلقی کند.

هر دولت عضو ممکن است این حق را برای خود محفوظ نگه دارد که سرقت‌های مرتبط با فناوری اطلاعات و ارتباطات یا کسب حقوق غیرقانونی آن، ازجمله از طریق کلاه‌برداری را به‌عنوان یک وضعیت تشدیدکننده مجازات تلقی کند.

ماده ۱۵- جرائم مرتبط با فناوری اطلاعات و ارتباطات مربوط به تولید و توزیع محتوا یا اشیاء با تصاویر مستهجن خردسالان

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند که

طبق قوانین داخلی خود ارتکاب عمدی و بدون حق رفتارهای زیر به‌عنوان یک جرم شناخته شود: الف) تولید پورنو گرافی کودکان به‌منظور توزیع آن از طریق شبکه‌های اطلاعاتی و ارتباطی، ازجمله اینترنت؛ ب) ارائه یا در دسترس قرار دادن پورنو گرافی کودکان از طریق شبکه‌های اطلاعاتی و ارتباطی، ازجمله اینترنت؛ ج) توزیع، مخابره، نمایش عمومی یا تبلیغ هرزه‌نگاری کودکان با استفاده از شبکه‌های اطلاعاتی و ارتباطی، ازجمله اینترنت؛ د) تهیه پورنو گرافی کودکان از طریق فناوری اطلاعات و ارتباطات برای خود یا برای شخص دیگری. ه) داشتن پورنو گرافی کودکان در یک سیستم رایانه‌ای یا در دستگاه‌های ذخیره‌سازی الکترونیکی داده‌های دیجیتال.

برای اهداف بند ۱ فوق، اصطلاح «هرزه‌نگاری کودک» شامل مطالب مستهجنی است که به‌صورت بصری موارد زیر را به تصویر می‌کشد: الف) یک خردسال درگیر رفتار صریح جنسی. ب) شخصی که به نظر می‌رسد صغیر باشد و درگیر رفتارهای صریح جنسی است. ج) تصاویر واقع‌گرایانه که نشان‌دهنده یک کودک خردسال است که درگیر رفتار جنسی صریح است. ازنظر این ماده، اصطلاح «صغیر» شامل همه افراد زیر ۱۸ سال می‌شود.

ماده ۱۶ -تشویق یا اجبار به خودکشی

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا بر اساس قوانین داخلی خود تشویق یا اجبار به خودکشی، به‌خصوص در بین افراد کم سن و سال، از طریق فشار روانی یا فشار های دیگر در جریان اطلاعات و شبکه‌های مخابراتی ازجمله اینترنت را به‌عنوان یک جرم تلقی کند.

ماده ۱۷ -جرائم مربوط به دخالت افراد زیر سن قانونی در ارتکاب اعمال غیرقانونی که جان یا سلامت آن‌ها را به خطر می‌اندازد

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا طبق قوانین داخلی خود دخالت افراد زیر سن قانونی و ارتکاب اعمال غیرقانونی تهدیدکننده حیات آن‌ها از طریق فناوری اطلاعات و ارتباطات را به‌عنوان یک جرم در نظر بگیرد؛ البته به‌استثنای اعمالی که در ماده ۱۶ این کنوانسیون پیش‌بینی‌شده است.

ماده ۱۸ -ایجاد و استفاده از داده‌های دیجیتال برای گمراه کردن کاربر

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا بر اساس قوانین داخلی خود ایجاد و استفاده غیرقانونی عمدی از داده‌های دیجیتال را که می‌تواند با داده‌هایی که قبلاً توسط کاربر شناخته‌شده و مورد اعتماد است، اشتباه گرفته‌شده و باعث آسیب قابل‌توجهی شود، به‌عنوان جرم تلقی کند.

هر کشور عضو ممکن است این حق را برای خود محفوظ نگه دارد که چنین اعمالی را درصورتی‌که در ارتباط با سایر جرائم تحت قوانین داخلی خود بوده یا متضمن قصد عمدی برای ارتکاب چنین جرائمی باشد، مجرمانه تلقی کند.

ماده ۱۹-تحریک به فعالیت‌های خرابکارانه یا مسلحانه

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا به‌موجب قوانین داخلی خود، جرمی را که از طریق فناوری اطلاعات و ارتباطات برای فعالیت‌های خرابکارانه یا مسلحانه در جهت سرنگونی

خشونت‌آمیز رژیم یک کشور دیگر صادرشده است، جرم‌انگاری کند.

ماده ۲۰- جرائم مرتبط با تروریسم

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا طبق قوانین داخلی خود استفاده از فناوری اطلاعات و ارتباطات برای فعالیت‌های تروریستی، تحریک، استخدام یا هرگونه دخالتی در فعالیت‌های تروریستی و توجیه تروریسم، جمع‌آوری یا تأمین بودجه برای تأمین مالی آن به‌عنوان جرم تلقی شود.

ماده ۲۱ -جرائم مربوط به افراط‌گرایی

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا اعمال غیرقانونی باانگیزه سیاسی یا دشمنی ایدئولوژیک، اجتماعی، نژادی، قومی یا مذهبی، حمایت و توجیه این‌گونه اقدامات یا فراهم آوردن امکان دسترسی به آن‌ها با استفاده از فناوری اطلاعات و ارتباطات، بر اساس قوانین داخلی خود به‌عنوان جرم تلقی شود.

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا تحقیر یک شخص یا گروهی از مردم به دلیل نژاد، قومیت، زبان، خاستگاه، نگرش دینی، از طریق فناوری اطلاعات و ارتباطات را بر اساس قوانین داخلی خود به‌عنوان یک جرم اتخاذ کند.

ماده ۲۲ -جرائم مربوط به توزیع مواد مخدر و روان‌گردان

هر دولت عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا طبق قوانین داخلی خود قاچاق غیرقانونی و عمدی مواد مخدر و روان‌گردان و همچنین مواد موردنیاز برای ساخت آن‌ها (پیش ساز)، با

استفاده از فناوری اطلاعات و ارتباطات را به‌عنوان یک جرم تشخیص دهد.

ماده ۲۳ -جرائم مربوط به قاچاق اسلحه

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا تجارت غیرقانونی عامدانه اسلحه، مهمات و مواد منفجره از طریق فناوری اطلاعات و ارتباطات را طبق قوانین داخلی خود به‌عنوان یک جرم اعلام کند.

ماده ۲۴ -بازسازی نازیسم، توجیه نسل‌کشی یا جنایات علیه صلح و بشریت

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا طبق قوانین داخلی خود انتشار عمدی مطالبی را که موضوعات صدر الاشاره را رد، تأیید یا توجیه می‌کند و از طریق فناوری اطلاعات و ارتباطات منتشر می‌شود، به‌عنوان یک جرم تلقی کند. این اقدامات شامل اقداماتی است که به‌منزله نسل‌کشی یا جنایت علیه صلح و بشریت است و توسط حکم دادگاه نظامی بین‌المللی بر اساس توافقنامه لندن در ۸ اوت ۱۹۴۵ بیان‌شده است.

ماده ۲۵- توزیع غیرقانونی داروها و فرآورده‌های پزشکی تقلبی

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا بر اساس قوانین داخلی خود توزیع غیرقانونی عمدی داروها و محصولات پزشکی تقلبی از طریق فناوری اطلاعات و ارتباطات را به‌عنوان جرم اعلام کند.

ماده ۲۶- استفاده از فناوری اطلاعات و ارتباطات برای ارتکاب اعمالی که طبق حقوق بین‌الملل به‌عنوان جرم شناخته‌شده‌اند

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا طبق قوانین داخلی خود استفاده از فناوری اطلاعات و ارتباطات به‌منظور ارتکاب عمل تعیین‌شده به‌عنوان جرم توسط هر یک از معاهدات بین‌المللی را جرم انگاری کند.

یک دولت عضو این کنوانسیون هنگام تصویب، پذیرش، تصویب یا الحاق این سند در صورتی که عضو معاهده ای که در ضمیمه این کنوانسیون ذکر شده است نباشد، می‌تواند در رابطه با آن معاهده (معاهدات) برای خود اعلامیه‌ای صادر کند. این اعلامیه به محض لازم‌الاجرا شدن معاهده برای آن دولت عضو باید متوقف شده و دولت عضو باید این واقعیت را به امان‌گذار اطلاع دهد.

هنگامی که یک دولت عضو از عضویت در یکی از معاهده مندرج در ضمیمه این کنوانسیون خارج شود، می‌تواند در رابطه با آن معاهده (معاهدات)، همانطور که در بند ۲ فوق پیش‌بینی شده است، اعلامیه صادر کند.

ماده ۲۷- نقض حق تکثیر و حقوق مرتبط با استفاده از فناوری اطلاعات و ارتباطات

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا بر اساس قوانین داخلی خود نقض حق چاپ و حقوق مربوطه را که توسط این قانون تعریف‌شده است، به‌عنوان یک جرم یا اقدام غیرقانونی دیگر به رسمیت بشناسد. قوانین آن کشور عضو باید زمانی که چنین

اعمالی عمداً با استفاده از فناوری اطلاعات و ارتباطات، ازجمله استفاده غیرقانونی از نرم‌افزار برای سیستم‌ها یا پایگاه‌های اطلاعاتی رایانه‌ای دارای حق چاپ و تخصیص حق تألیف صورت می‌گیرد آن را جرم انگاری کنند.

ماده ۲۸- کمک، آماده‌سازی و تلاش برای ارتکاب جرم

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا طبق قوانین داخلی خود، هرگونه تلاش برای ارتکاب جرم را توسط مفاد این کنوانسیون، جرم انگاری کند.

هر کشور عضو باید اتخاذ تدابیر قانونی و سایر اقدامات لازم را برای خود در نظر بگیرد تا طبق قوانین داخلی خود، ساخت یا تطبیق ابزارهای جرم، جلب همدستان، توطئه برای ارتکاب جرم یا ارتکاب آن یا هرگونه اقدام عمدی دیگر برای ارتکاب جرائم گفته‌شده در این کنوانسیون را جرم انگاری کند.

هر دولت عضو اقدامات قانونی و سایر اقدامات لازم را طبق قوانین داخلی خود اتخاذ خواهد کرد تا برای سازمان دهنده، عامل یا کمک‌کننده به این جرائم ایجاد مسئولیت کند و همچنین مسئولیت کیفری ارتکاب جرائم جمعی، ازجمله گروه‌های سازمان‌یافته و انجمن‌های جنایی را تشدید کند.

ماده ۲۹- سایر اعمال غیرقانونی

این کنوانسیون مانع از آن نخواهد بود که یک کشور عضو هر عمل غیرقانونی دیگری را که عمداً از طریق فناوری اطلاعات و ارتباطات ارتکاب یافته و موجب خسارت قابل‌توجهی می‌شود، به‌عنوان جرم تلقی کند.

ماده ۳۰ -مسئولیت اشخاص حقوقی

هر دولت عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا اطمینان حاصل شود که اشخاص حقوقی می‌توانند برای یک جرم جنایی یا سایر اقدامات غیرقانونی مقرر در این کنوانسیون درصورتی‌که جرمی به نفع آن‌ها و توسط هر شخص حقیقی که به صورت انفرادی یا به عنوان بخشی از ارگان شخص حقوقی مربوطه فعالیت می کند و به موجب موارد زیر در آن سمت رهبری دارد انجام شود مسئول شناخته شوند:

الف) وکالتنامه شخص حقوقی؛

ب) اختیار تصمیم گیری از طرف شخص حقوقی.

ج) اختیار اعمال کنترل در شخص حقوقی.

علاوه بر موارد پیش‌بینی شده در بند ۱ این ماده، هر کشور عضو باید اقدامات لازم را برای اطمینان از اینکه شخص حقوقی می‌تواند در مواردی که به دلیل عدم نظارت یا کنترل توسط شخص حقیقی مذکور در بند ۱ باعث شده است، اتخاذ کند و این شخص حقوقی رامسئول بداند. ممکن است ارتکاب یک جرم جنایی یا سایر اعمال غیرقانونی که مطابق با مفاد این کنوانسیون به نفع آن شخص حقوقی ایجاد شده است توسط یک شخص حقیقی که تحت اقتدار آن عمل می کند انجام شده باشد.

با رعایت اصول حقوقی دولت عضو، مسئولیت یک شخص حقوقی ممکن است کیفری، مدنی یا اداری باشد. دولت عضو باید تضمین کند که اشخاص حقوقی مسئول، مشمول تحریم‌های مؤثر، متناسب و بازدارنده ازجمله تحریم‌های مالی می‌شوند.

در نظر گرفتن این مسئولیت برای اشخاص حقوقی به مسئولیت اشخاص حقیقی که مرتکب جرم یا عمل غیرقانونی دیگری شده‌اند، لطمه‌ای وارد نمی‌کند.

بخش ۲
رویه‌های کیفری و اجرای قانون

ماده ۳۱- محدوده مقررات آیین دادرسی

هر دولت عضو اقدامات قانونی و سایر اقدامات لازم را برای ایجاد اختیارات و رویه‌های پیش‌بینی‌شده در این بخش به‌منظور پیشگیری، شناسایی، سرکوب، کشف و رسیدگی به جرائم و سایر اعمال غیرقانونی و انجام اقدامات قضایی در رابطه با این جنایات پیش می‌گیرد.

به‌استثنای مواردی که در ماده ۳۳ این کنوانسیون مقررشده باشد، هر دولت عضو باید اختیارات و رویه‌های ذکرشده در بند ۱ این ماده را در موارد زیر اعمال کند: الف) جرائم جنایی و سایر اعمال غیرقانونی که مطابق با مواد ۶ تا ۲۹ این کنوانسیون ایجادشده است. ب) سایر جرائم جنایی و سایر اعمال غیرقانونی که از طریق فناوری اطلاعات و ارتباطات انجام می‌شود. ج) جمع‌آوری مدارک اعم از مدارک الکترونیکی مربوط به ارتکاب جرائم کیفری و سایر اعمال غیرقانونی.

الف) هر دولت عضو ممکن است حق اعمال اقدامات مندرج در ماده ۳۸ این کنوانسیون را فقط در مورد جرائم جنایی یا دسته‌هایی از جرائم جنایی برای خود حفظ کند، مشروط بر اینکه دامنه این‌گونه جرائم جنایی، محدودتر از دامنه جرائم جنایی که اقدامات مذکور در مفاد ماده

۳۳ این کنوانسیون در مورد آن‌ها اعمال می‌شود، نشود. هر کشور عضو، اعمال چنین شرطی را محدود خواهد کرد تا امکان اجرای گسترده‌ترین تدابیر مقرر در ماده ۳۸ این کنوانسیون را فراهم کند. ب) اگر یک کشور عضو، به دلیل محدودیت‌هایی در قوانین داخلی خود که در زمان تصویب این کنوانسیون لازم‌الاجرا بود، نتواند تدابیر ذکرشده در مواد ۳۳ و ۳۸ این کنوانسیون را در مورد داده‌های ارسال‌شده در یک قرارداد اعمال کند و آن سیستم

الف) به نفع گروه محدودی از کاربران در حال بهره برداری است، و

ب) از شبکه اطلاعاتی و مخابراتی استفاده نمی کند و با سایر سیستم های اطلاعاتی مرتبط نیست.

آن کشور عضو ممکن است این حق را برای خود محفوظ نگه دارد که این اقدامات را برای چنین انتقال اطلاعاتی اعمال نکند.

ماده ۳۲- شرایط و ضمانت‌ها

هر دولت عضو باید تضمین کند که ایجاد، اجرا و اعمال اختیارات و رویه‌های پیش‌بینی‌شده در این بخش مشروط به شرایط و ضمانت‌های پیش‌بینی‌شده در قوانین داخلی خود است که حفاظت کافی از انسان و حقوق و آزادی‌های او را، ازجمله حقوق ناشی از تعهداتی که دولت عضو تحت میثاق بین‌المللی حقوق مدنی و سیاسی مورخ ۱۶ دسامبر ۱۹۶۶ و سایر اسناد بین‌المللی حقوق بشر قابل‌اجرا برعهده‌گرفته است را، تضمین می‌کند.

با توجه به ماهیت اختیارات و رویه‌های مربوط، این شرایط و تضمین‌ها، نظارت قضایی یا سایر نظارت‌های مستقل، دلایل توجیه‌کننده اعمال و

محدودیت دامنه و مدت چنین اختیارات یا رویه‌هایی را نیز شامل می‌شود. دولت عضو باید تأثیر اختیارات و رویه‌های پیش‌بینی‌شده در این بخش را تا حدی که با منافع عمومی، به‌ویژه در مورداجرای عدالت سازگار باشد، بر حقوق، مسئولیت و منافع مشروع شخص ثالث در نظر بگیرد.

ماده ۳۳- جمع‌آوری اطلاعات منتقل‌شده از طریق فناوری اطلاعات و ارتباطات

هر کشور عضو اقدامات قانونی و سایر اقدامات لازم را در رابطه با جرائم پیش‌بینی‌شده توسط این کنوانسیون و بر اساس قوانین داخلی خود اتخاذ خواهد کرد تا مقامات ذی‌صلاح خود را در موارد زیر مختار کنند: الف) جمع‌آوری یا ثبت اطلاعات از طریق فناوری اطلاعات و ارتباطات و استفاده از ابزارهای فنی، در قلمرو آن کشور عضو. ب) موظف کردن و مسئول دانستن هر شرکت ارائه‌دهنده خدمات اینترنتی تا حدی که توانایی فنی لازم برای انجام امور زیر را داشته باشد:

ب-۱) اطلاعات الکترونیکی را که شامل داده‌های محتوایی است و از طریق استفاده از ابزارهای فنی در قلمرو آن کشور از طریق فناوری اطلاعات و ارتباطات منتقل می‌شود، جمع‌آوری یا ثبت کند.

یا ب-۲) همکاری و کمک به مقامات ذیصلاح کشور عضو در جمع‌آوری یا ضبط فوری اطلاعات الکترونیکی، شامل داده‌های محتوایی است و از طریق فناوری اطلاعات و ارتباطات در قلمرو دولت عضو منتقل می‌شود.

درصورتی‌که یک دولت عضو، به دلیل اصول قدیمی نظام حقوقی داخلی خود، نتواند تدابیر مندرج در بند ۱ (الف) این ماده را اتخاذ کند، در عوض می‌تواند اقدامات قانونی دیگری را به‌منظور اطمینان از جمع‌آوری

یا ضبط فوری اطلاعات الکترونیکی (شامل داده‌های مربوط به محتوا) را با استفاده از فناوری اطلاعات و ارتباطات در قلمرو خود اتخاذ کند.

هر کشور عضو، اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا هر شرکت ارائه‌دهنده خدمات اینترنتی را ملزم به محرمانه نگه‌داشتن هرگونه اختیارات مقرر در این ماده و هرگونه اطلاعات مربوط به آن کند. اختیارات و رویه‌های مذکور در این ماده مشمول مقررات مواد ۳۱ و ۳۲ این کنوانسیون خواهد بود.

ماده ۳۴ -نگهداری سریع اطلاعات الکترونیکی انباشته

هر کشور عضو باید اقدامات قانونی لازم را اتخاذ کند تا مقامات ذیصلاح خود را قادر سازد تا دستورات یا دستورالعمل‌های کافی برای حفظ سریع اطلاعات الکترونیکی مشخص، ازجمله داده‌های ترافیکی را صادر کنند. به‌ویژه در مواردی که این باور وجود داشته باشد که داده‌ها در برابر حذف، کپی یا اصلاح یا به دلیل انقضای دوره نگهداری داده‌ها آسیب‌پذیر هستند.

اگر یک دولت عضو مقررات بند ۱ این ماده مبنی بر حفظ اطلاعات ذخیره‌شده را به‌وسیله دستوری به شخصی (ازجمله اشخاص حقوقی) اجرا کند، دولت عضو باید اقدامات قانونی لازم برای الزام آن شخص به حفظ این اطلاعات و حفظ یکپارچگی آن را برای مدت‌زمانی که لازم است و نه بیشتر، توسط قانون داخلی کشور خود، به کار گیرد. افشای داده‌ها یک دولت عضو ممکن است متعاقباً تمدید چنین دستوری را در پی داشته باشد.

هر کشور عضو اقدامات قانونی لازم را اتخاذ خواهد کرد تا شخصی را

کـه وظیفـه حفـظ اطلاعـات را بـر عهـده دارد ملـزم کند ایـن رویه‌هـا را برای مدتـی کـه در قوانیـن داخلـی خود پیش‌بینی‌شـده اسـت، محرمانه نگـه دارد. اختیـارات و رویه‌هـای مذکـور در ایـن ماده مطابـق با مفاد مـواد ۳۱ و ۳۲ این کنوانسـیون ایجاد خواهد شد.

ماده ۳۵- حفظ سریع و افشای جزئی داده‌های ترافیک

هـر کشـور عضـو، در رابطـه بـا داده‌هـای ترافیکـی که طبق مفـاد ماده ۳۴ ایـن کنوانسـیون بایـد حفـظ شـود، اقدامـات قانونـی و سـایر اقدامـات لازم را اتخـاذ خواهـد کرد:

الـف) اطمینـان حاصـل شـود کـه نگهـداری سـریع داده‌هـای ترافیـک، صرف‌نظـر از اینکـه چـه تعـداد از ارائه‌دهنـدگان خدمـات در انتقـال چنیـن اطلاعاتـی دخیـل بوده‌انـد، امکان‌پذیـر اسـت.

ب) از افشـای سـریع حجـم کافی از داده‌های ترافیکـی به مقامات ذیصلاح کشـور عضـو اطمینـان حاصـل کنـد تـا دولـت مربوطـه بتوانـد ارائه‌دهندگان خدمـات و مسـیری را کـه اطلاعات ذکرشـده از طریق آن مخابره شـده اسـت شناسـایی کند.

اختیـارات و رویه‌هـای مذکـور در ایـن مـاده مطابـق با مفاد مـواد ۳۱ و ۳۲ این کنوانسـیون ایجاد خواهد شـد.

ماده ۳۶- دستور تولید

برای اهداف مندرج در بند ۱ از ماده ۳۱ این کنوانسـیون، هر کشـور عضو اقدامـات قانونـی لازم را بایـد اتخـاذ کنـد تـا به مقامـات ذیصلاح خـود اختیار دهـد تـا در موارد زیـر دسـتورات لازم را بدهند:

۱- الف) شخصی در قلمرو خود اطلاعات الکترونیکی مشخصی که در اختیار یا کنترل آن شخص است ارائه کند؛

۱- ب) به ارائه‌دهنده خدماتی که خدمات خود را در قلمرو آن کشور عضو ارائه می‌کند دستور دهد تا اطلاعات مشترکی را که در اختیار یا کنترل آن ارائه‌دهنده خدمات است، ارسال کند.

۲) اختیارات و رویه‌های مذکور در این ماده مطابق با مفاد مواد ۳۱ و ۳۲ این کنوانسیون ایجاد خواهد شد.

۳) ازنظر این ماده، اصطلاح «اطلاعات مشترک» هرگونه اطلاعاتی به‌غیراز داده‌های ترافیکی یا داده‌های محتوایی است که توسط یک ارائه‌دهنده خدمات اینترنتی به مشترکین سرویس‌هایش داده می‌شود، که بر اساس آن امکان ایجاد موارد زیر وجود دارد:

۳-الف) نوع خدمات اطلاعاتی و ارتباطاتی مورداستفاده، مفاد فنی اتخاذشده در آن و مدت خدمت.

۳- ب) هویت مشترک، آدرس‌های پستی یا سایر آدرس‌ها، تلفن و سایر شماره‌های دسترسی، ازجمله آدرس‌های IP و اطلاعات صورت‌حساب، اطلاعات موجود در قرارداد.

۳-ج) اطلاعات مربوط به موقعیت مکانی تجهیزات اطلاعاتی و مخابراتی که با قرارداد خدمات ارتباط دارد.

ماده ۳۷- جستجو و ضبط اطلاعات ذخیره‌شده یا پردازش‌شده به‌صورت الکترونیکی

هر دولت عضو باید اقدامات قانونی و سایر اقدامات لازم را برای دسترسی مقامات صلاحیت‌دار خود به موارد زیر در قلمرو آن کشور به کار

گیرد: الف) دستگاه‌های فناوری اطلاعات و ارتباطات و اطلاعات ذخیره‌شده در آن. ب) رسانه ذخیره‌سازی اطلاعات که اطلاعات الکترونیکی موردنظر ممکن است در آن ذخیره شود.

هر کشور عضو، اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا اطمینان حاصل شود که در مواردی که مقامات صلاحیت‌دار آن‌که به‌موجب مفاد بند ۱ (الف) این ماده اطلاعات یا مواردی را جستجو می‌کنند، بتوانند به‌سرعت جستجو کرده و به اطلاعات دسترسی یابند.

هر دولت عضو اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا اقداماتی را برای توقیف اطلاعات الکترونیکی در قلمرو یا تحت صلاحیت دولت عضو یا به‌طور مشابه ایمن‌سازی چنین اطلاعاتی اتخاذ کنند. این اقدامات شامل ارائه اختیارات زیر به مقامات ذی‌صلاح آن کشور خواهد بود: الف) توقیف دستگاه فناوری اطلاعات و ارتباطات که برای ذخیره اطلاعات یا ایمن‌سازی آن به روش دیگری استفاده می‌شود. ب) تهیه و نگهداری از این اطلاعات به‌صورت الکترونیکی و دیجیتال. ج) حفظ یکپارچگی اطلاعات ذخیره‌شده مربوطه. د) برای حذف اطلاعات ذخیره‌شده یا پردازش‌شده الکترونیکی از دستگاه فناوری اطلاعات و ارتباطات.

هر کشور عضو، اقدامات قانونی لازم را اتخاذ خواهد کرد تا مقامات ذیصلاح خود را طبق رویه‌ای که در قوانین داخلی خود تعیین‌شده است مختار کند تا به هر شخصی که دانش خاصی در مورد عملکرد سیستم اطلاعاتی موردنظر و شبکه مخابراتی یا اجزای سازنده آن‌ها دارد، برای ارائه اطلاعات لازم و/یا کمک در انجام اقدامات مذکور دربندهای ۱ تا ۳ این ماده دستور دهد.

اختیارات و رویه‌های مذکور در این ماده مطابق با مفاد مواد ۳۱ و ۳۲

این کنوانسیون ایجاد خواهد شد.

ماده ۳۸- جمع‌آوری بی‌درنگ داده‌های ترافیک:

هر کشور عضو باید اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا مقامات ذی‌صلاح خود به موارد زیر دسترسی یابند:

الف) جمع‌آوری یا ثبت اطلاعات و داده‌های ترافیکی مرتبط با استفاده از ابزار فنی و فناوری اطلاعات و ارتباطات در قلمرو کشور عضو.

ب) موظف کردن ارائه‌دهندگان خدمات به انجام موارد زیر تا حدی که توانایی فنی لازم برای انجام آن را دارند: (۱) جمع‌آوری یا ثبت داده‌های ترافیکی در قلمرو کشور عضو، با استفاده از ابزارهای فنی برای این منظور. یا (۲) همکاری و کمک به مقامات ذیصلاح دولت عضو در جمع‌آوری یا ثبت فوری داده‌های ترافیکی مرتبط با اطلاعات مشخص در قلمرو کشور عضو.

درصورتی‌که یک دولت عضو، به دلیل اصول دیرینه نظام حقوقی داخلی خود، نتواند تدابیر مقرر در بند ۱ (الف) این ماده را اتخاذ کند، در عوض می‌تواند اقدامات قانونی و سایر اقدامات لازم، مانند جمع‌آوری یا ثبت فوری داده‌های ترافیکی در قلمرو خود از طریق استفاده از ابزارهای فنی را اتخاذ کند.

هر کشور عضو، اقدامات قانونی و سایر اقدامات لازم را اتخاذ خواهد کرد تا یک ارائه‌دهنده خدمات اینترنتی را ملزم به محرمانه نگه‌داشتن اعمالِ اختیارات مقرر در این ماده و هرگونه اطلاعات مربوط به آن کند. اختیارات و رویه‌های مذکور در این ماده مشمول مقررات مواد ۳۱ و ۳۲ این کنوانسیون خواهد بود.

ماده ۳۹- صلاحیت قضایی

هـر دولـت عضـو باید تمام اقدامات لازم را بـرای ایجاد صلاحیت قضایی در مـورد جرائـم جنایـی و سـایر اعمـال غیرقانونی که مطابـق با این کنوانسـیون ایجادشـده اسـت، اتخاذ کند:

الف) در قلمرو آن دولت عضو باشد.

ب) روی کشـتی‌ای کـه پرچـم آن کشـور عضـو را در هنـگام ارتـکاب جرم حمـل می‌کنـد، یا سـوار بر هواپیمایی کـه در آن زمان تحت قوانین آن کشـور عضو ثبت‌شـده اسـت، باشد.

با رعایت ماده ۳ این کنوانسیون، یک دولت عضو می‌تواند صلاحیت خود را در مـورد هرگونـه جرم و سـایر اعمال غیرقانونی دیگر بـه کار بگیرد؛ زمانی که:

الـف) جـرم علیـه اتبـاع آن دولـت عضو یا یک فرد بـدون تابعیت که به‌طور دائـم در قلمـرو آن اقامت دارد، یا یک شـخص حقوقی کـه در قلمرو خود، یک دولـت یا تأسیسـات دولتی، ازجملـه اماکن یک نمایندگـی دیپلماتیک یا دفتر کنسـولی آن کشـور عضو، دارای نمایندگی دائمی اسـت؛ ارتکاب یافته باشـد.

ب) جـرم توسـط اتبـاع آن دولـت عضو یا شـخص بـدون تابعیتی که محل اقامت معمول آن در قلمرو آن کشـور اسـت، انجام شـود.

ج) جرم علیه آن دولت عضو انجام‌شده باشد.

د) جـرم به‌طـور کامـل یا جزئـی در خارج از قلمـرو آن دولت عضو ارتکاب یافتـه اسـت، اما آثـار آن در قلمـرو آن دولت عضو، جرم محسـوب می‌شـود یا منجر بـه ارتکاب جرم می‌شـود.

بـرای اهـداف ماده ۴۷ این کنوانسـیون، هر کشـور عضو بایـد تمام اقدامات لازم را بـرای ایجـاد صلاحیـت قضایـی خـود در مـورد جرائمـی کـه طبق این کنوانسـیون ایجادشـده اسـت، اتخاذ کند، زمانی که متهم در قلمرو آن کشـور

حضورداشته باشد و دولت عضو نمی‌تواند چنین شخصی را صرفاً به این دلیل که او به آن کشور پناهنده شده است مسترد نکند.

هر کشور عضوی که متهم در قلمرو آن حضور دارد و چنین شخصی را استرداد نمی‌کند، در موارد پیش‌بینی‌شده در بندهای ۱ و ۲ این ماده، بدون استثنا و صرف‌نظر از اینکه جرم در قلمرو کشورش ارتکاب یافته باشد یا خیر، موظف خواهد بود پرونده را به‌منظور پیگرد قانونی بدون تأخیر بیشتر مطابق با قوانین به کشور دیگری ارسال کند.

اگر یک کشور عضوی که صلاحیت خود را طبق بند ۱ یا ۲ این ماده اعمال می‌کند متوجه شده باشد که سایر کشورهای عضو در رابطه با همان عمل در حال تحقیق، تعقیب یا اجرای یک دادرسی قضایی هستند، مقامات ذیصلاح دیگر کشورهای عضو، در صورت لزوم، به‌منظور هماهنگی اقدامات خود با یکدیگر مشورت خواهند کرد.

این کنوانسیون بدون لطمه به حقوق بین‌الملل عمومی، اعمال هیچ‌گونه صلاحیت کیفری یا اداری را که توسط یک دولت عضو مطابق با قوانین داخلی خود ایجادشده است، مستثنا نخواهد کرد.

فصل سوم
اقدامات برای پیشگیری و مبارزه با جرائم و سایر اعمال غیرقانونی در فضای سایبری

ماده ۴۰- سیاست‌ها و شیوه‌های پیشگیری و مبارزه با جرائم و سایر اعمال غیرقانونی مرتبط با استفاده از فناوری اطلاعات و ارتباطات

هر کشور عضو باید مطابق با اصول اساسی نظام حقوقی خود،

برای مبارزه با جرائم و سایر اعمال غیرقانونی مرتبط با استفاده از فناوری اطلاعات و ارتباطات، سیاستی مؤثر و هماهنگ را توسعه داده، اجرا نموده یا دنبال کند.

هر دولت عضو باید تلاش کند تا شیوه‌های مؤثری را برای جلوگیری از تخلفات و سایر اعمال غیرقانونی مربوط به استفاده از فناوری اطلاعات و ارتباطات ایجاد و ترویج کند.

دولت‌های عضو، در صورت اقتضا و مطابق با اصول اساسی نظام‌های حقوقی خود، با یکدیگر و با سازمان‌های بین‌المللی و منطقه‌ای مربوطه در ترویج و توسعه اقدامات مذکور در این ماده همکاری خواهند کرد.

ماده ۴۱- نهادهای مسئول پیشگیری و مبارزه با جرائم و سایر اعمال غیرقانونی مرتبط با استفاده از فناوری اطلاعات و ارتباطات

هر کشور عضو باید کلیه اقدامات قانونی و سایر اقدامات قانونی لازم را در تعیین مقامات مسئول در راستای فعالیت برای پیشگیری و مبارزه با جرائم و اقدامات غیرقانونی مربوط به استفاده از فناوری اطلاعات و ارتباطات انجام دهد و رویه‌هایی را برای تعاملات بین این مقامات ایجاد کند.

هر کشور عضو باید نام و آدرس مقام/مقاماتی را که ممکن است به سایر کشورهای عضو در توسعه و اجرای اقدامات خاص برای جلوگیری از تخلفات و سایر اعمال غیرقانونی مربوط به استفاده از فناوری اطلاعات و ارتباطات کمک کنند، به دبیر کل سازمان ملل اطلاع دهد.

ماده ۴۲- بخش خصوصی

هر کشور عضو باید اقداماتی را مطابق با اصول اساسی قوانین داخلی

خود برای جلوگیری از جرائم و سایر اعمال غیرقانونی مربوط به استفاده از فناوری اطلاعات و ارتباطات در بخش خصوصی، ارتقای استانداردهای امنیت اطلاعات در بخش خصوصی و در صورت اقتضا، مجازات مدنی، اداری و کیفری مؤثر، متناسب و بازدارنده را برای عدم رعایت چنین اقداماتی اعمال کنند.

اقدامات باهدف دستیابی به این اهداف ممکن است شامل موارد زیر باشد:

الف) ارتقای همکاری بین سازمان‌های مجری قانون دولت عضو و نهادهای خصوصی مربوطه‌ی آن دولت عضو.

ب) ترویج توسعه استانداردها و رویه‌های تضمین امنیت اطلاعات.

ج) ترویج برنامه‌های آموزشی برای مقامات انتظامی، تحقیقاتی، قضایی و دادسرا در رابطه با استفاده از فناوری اطلاعات و ارتباطات.

ماده ۴۳- اصول و ضوابط رفتاریِ شرکت‌های خصوصی خدمات مخابراتی

هر شرکت خصوصی خدمات مخابراتی (یا گروهی از ارائه‌دهندگان این‌گونه خدمات) واقع در قلمرو یک دولت عضو، در محدوده اختیارات خود و در چارچوب اختیارات خود، مطابق با قوانین کشوری که در آن واقع‌شده است، برای حمایت از ایجاد و اجرای اصول و استانداردهای استفاده از فضای سایبری بین‌المللی و بر اساس احترام به حقوق بشر که توسط اسناد اساسی سازمان ملل تضمین‌شده است، اقدامات مقتضی را انجام خواهد داد.

اقدامات لازم برای دستیابی به این اهداف ممکن است شامل موارد زیر باشد:

الف) همکاری بین شرکت خصوصی خدمات مخابراتی با یکدیگر.

ب) همکاری در تدوین اصول و استانداردها برای ایجاد محیطی مناسب برای ساخت جامعه متمدن به‌عنوان بخشی جدایی‌ناپذیر از فضای سایبری بین‌المللی.

ماده ۴۴- افزایش آگاهی عمومی در مورد پیشگیری از جرائم سایبری

هر کشور عضو باید اقدامات مقتضی را در محدوده اختیارات خود و مطابق با اصول اساسی قوانین داخلی خود برای ترویج مشارکت فعال سازمان‌های عمومی در پیشگیری از جرائم و سایر اقدامات غیرقانونی مرتبط با استفاده از فناوری اطلاعات و ارتباطات و افزایش آگاهی عمومی در مورد این جرائم، علل و میزان جدیت آن‌ها و همچنین تهدیدات این جرائم اتخاذ کند. این مشارکت باید با اقدامات زیر پشتیبانی شود:

الف) فراهم کردن دسترسی عمومی به اطلاعات به‌صورت مؤثر.

ب) انجام فعالیت‌های افزایش آگاهی عمومی در راستای عدم تحمل جرائم و سایر اعمال غیرقانونی مربوط به استفاده از فناوری اطلاعات و ارتباطات و همچنین انتشار بهترین شیوه‌ها.

ج) اجرای برنامه‌های آموزشی عمومی در زمینه امنیت فناوری اطلاعات و ارتباطات.

هر کشور عضو باید اقدامات مقتضی را اتخاذ کند تا اطمینان حاصل شود که عموم مردم از نهادهای مربوطه مسئول مبارزه با جرائم مربوط به استفاده از فناوری اطلاعات و ارتباطات اشاره‌شده در این کنوانسیون مطلع هستند و امکان دسترسی به این نهاد ها را برای گزارش هرگونه رویدادی که ممکن است طبق این کنوانسیون جرم تلقی شود فراهم می‌کند.

ماده ۴۵- اتخاذ تدابیر قانونی لازم برای ارائه حمایت مؤثر از شهود هر دولت عضو

الف) افرادی که با حسن نیت و بر اساس دلایل معقول اطلاعات مربوط به اعمال غیرقانونی را طبق مواد ۶ و ۲۸ این کنوانسیون اطلاعاتی را ارائه می‌کنند یا به نحوی با مراجع تحقیق یا قضایی همکاری دارند.

ب) شاهدانی که در مورد اعمال غیرقانونی مندرج در مواد ۶ تا ۲۸ این کنوانسیون شهادت می‌دهند و نیز قربانیان آن.

ج) در صورت اقتضا، اعضای خانواده اشخاص مذکور در بندهای (الف) و (ب) این ماده.

فصل چهارم

همکاری‌های بین‌المللی

استرداد، کمک‌های حقوقی متقابل و همکاری بین سازمان‌های مجری قانون

ماده ۴۶- اصول کلی همکاری‌های بین‌المللی

کشورهای عضو باید تا حد امکان مطابق با مفاد این فصل و بر اساس سایر اسناد بین‌المللی در مورد همکاری بین‌المللی در امور کیفری و توافقات حاصل‌شده بر اساس اصل عمل متقابل و همچنین قوانین داخلی باهدف پیشگیری، سرکوب، کشف و بررسی جرائم مربوط به استفاده از فناوری اطلاعات و ارتباطات با یکدیگر همکاری کنند.

زمانی که درخواستی از یکی از کشورهای عضو برای پیگیری و همکاری بین‌المللی صادر می‌شود، فارغ از این‌که آن اقدام یا اعمال در کشور دیگر عضو جرم تلقی می‌شود یا خیر، کشور درخواست شونده نیز باید آن را

جرم انگاری نموده و به همکاری بین‌المللی خود ادامه دهد. به رسمیت شناختن متقابل جرائم، یک الزام است، صرف‌نظر از اینکه قانون دولت عضو درخواست شونده آن اقدام را جرم تعریف می‌کند یا نمی‌کند.

کشورهای عضو باید در صورت اقتضا و طبق سیستم‌های حقوقی داخلی، در تحقیق و تعقیب قضایی پرونده‌های مدنی و اداری مرتبط با جرائم مربوط به استفاده از فناوری اطلاعات و ارتباطات، کمک متقابل را در نظر بگیرند.

در بین کشورهای عضو، به‌منظور استرداد و کمک حقوقی متقابل در امور کیفری، ازجمله مصادره و بازیابی اموالی که از راه کیفری به‌دست‌آمده است، هیچ‌یک از جرائم مذکور در مواد ۶ تا ۲۸ این کنوانسیون جرم سیاسی، جرمی که با یک جرم سیاسی یا یک جرم باانگیزه سیاسی مرتبط است تلقی نخواهد شد. بر این اساس، درخواست استرداد یا معاضدت حقوقی در امور کیفری، ازجمله تفتیش، ضبط، مصادره و بازیابی اموالی که از طرق مجرمانه به‌دست‌آمده است، صرفاً به این دلیل رد نخواهد شد که مربوط به یک جرم سیاسی، جرم مرتبط با یک جرم سیاسی یا یک جرم باانگیزه سیاسی است. در ایجاد و پاسخگویی به درخواست‌های طبق این کنوانسیون، کانال‌های سازمان پلیس جنایی بین‌المللی، اینترپل، نیز ممکن است در موارد فوری و زمانی که توافق بین کشورهای عضو درخواست‌کننده و درخواست شونده حاصل می‌شود، استفاده شود.

هر کشور عضو دارای حق برابر برای حفاظت از منابع اطلاعاتی و زیرساخت‌های اطلاعاتی حیاتی خود در برابر سوءاستفاده و تداخل غیرمجاز، ازجمله حملات رایانه‌ای علیه آن‌ها خواهد بود.

ماده ۴۷- استرداد

این ماده در مورد جرائمی که طبق این کنوانسیون ایجادشده است اعمال می‌شود، درصورتی‌که شخصی که موضوع درخواست استرداد در قلمرو کشور عضو درخواست شونده حضورداشته باشد، طبق قوانین داخلی هر دو کشور عضو درخواست‌کننده و دولت درخواست شونده حداقل یک سال حبس یا مجازات سنگین‌تر قابل مجازات است.

جرائم جنایی مندرج در مواد ۶ تا ۲۸ این کنوانسیون طبق هر معاهده استرداد موجود بین کشورهای عضو، جرائم قابل‌استرداد تلقی خواهند شد. کشورهای عضو متعهد می‌شوند که چنین جرائمی را به‌عنوان جرائم قابل‌استرداد در هر معاهده استرداد آتی بین خود لحاظ کنند. دولت عضوی که قانون داخلی آن اجازه می‌دهد، درصورتی‌که از این کنوانسیون به‌عنوان مبنای استرداد استفاده کند، هیچ‌یک از جرائم ایجادشده بر اساس این کنوانسیون را جرم سیاسی تلقی نخواهد کرد.

اگر درخواست استرداد مربوط به چندین جرم جداگانه باشد که حداقل یکی از آن‌ها طبق این ماده قابل‌استرداد است، درحالی‌که بقیه به دلیل مجازات اعمال‌شده در مورد آن‌ها قابل‌استرداد نیستند، اما به‌عنوان جرائمی که طبق این کنوانسیون تعیین‌شده است تلقی می‌شوند، دولت درخواست شونده نیز می‌تواند این ماده را در مورد چنین جرائمی اعمال کند.

اگر کشور عضوی که استرداد را مشروط به وجود معاهده می‌کند، درخواست استرداد را از کشور دیگر عضوی که با آن معاهده استرداد ندارد دریافت کند، این کنوانسیون ممکن است به‌عنوان مبنای قانونی برای استرداد در رابطه با هر جرم این کنوانسیون اعمال شود.

دولت عضوی که استرداد را مشروط به وجود معاهده می‌کند:

الف) هر کشور هنگام تودیع سند تصویب، پذیرش یا الحاق به این کنوانسیون، به دبیر کل سازمان ملل اطلاع خواهد داد که آیا کنوانسیون را به‌عنوان مبنای قانونی برای همکاری در زمینه استرداد با سایر کشورهای عضو این کنوانسیون اعمال خواهد کرد یا خیر.

ب) اگر این کنوانسیون را به‌عنوان مبنای قانونی برای همکاری در زمینه استرداد اعمال نمی‌کند، در صورت لزوم، به‌منظور اعمال این ماده، به دنبال انعقاد معاهداتی با سایر کشورهای عضو این کنوانسیون در مورد استرداد باشد.

کشورهای عضوی که استرداد را مشروط به وجود معاهده نمی‌دانند، جرائمی را که این ماده در مورد آن‌ها اعمال می‌شود، به‌عنوان جرائم قابل‌استرداد بین خود به رسمیت می‌شناسند.

استرداد تابع شرایطی خواهد بود که در قوانین داخلی دولت درخواست شونده یا در معاهدات مربوط به استرداد، ازجمله شرایط مربوط به حداقل شرایط مجازات برای استرداد در آن کشور وجود داشته باشد.

کشورهای عضو، با رعایت قوانین داخلی خود، تلاش خواهند کرد تا مراحل استرداد را تسریع بخشند و الزامات شواهد مربوط به آن را، در صورت وجود، در مورد هر جرمی که این ماده در مورد آن اعمال می‌شود، ساده کنند.

دولت عضو درخواست شونده می‌تواند از استرداد درصورتی‌که به حاکمیت، امنیت، نظم عمومی یا سایر منافع عمومی اساسی خودش لطمه وارد کند، امتناع کند.

دولت عضو درخواست شونده، با رعایت مقررات قوانین داخلی خود و

معاهدات استرداد، پس از اطمینان از این‌که شرایط اقتضا می‌کند و فوری است، می‌تواند بنا به درخواست کشور عضو درخواست‌کننده، شخصی را که باید مسترد شود، بازداشت کند، تحت تعقیب قرار دهد یا اقدامات مناسب دیگری را، ازجمله تسلیم شخص به دولت عضو درخواست‌کننده، اتخاذ کند.

اگر کشور عضوی که در قلمرو آن مجرم ادعاشده پیدا شده است، چنین شخصی را استرداد نکند، بدون استثنا، بنا به درخواست کشور عضو خواهان استرداد، موظف است پرونده را بدون تأخیر به مقامات ذیصلاح خود به‌منظور تعقیب این فرد ارسال کند. این مقامات تصمیم خود را اتخاذ خواهند کرد و روند رسیدگی خود را به همان روشی که در مورد هر جرم دیگری که ماهیت سنگینی دارد طبق قوانین داخلی آن دولت عضو انجام خواهد داد. کشورهای عضو ذینفع باید با یکدیگر همکاری کنند تا اطمینان حاصل شود که این تعقیب مؤثر است.

در مواردی که یک کشور عضو طبق قوانین داخلی خود مجاز است یکی از اتباع خود را استرداد کند یا به نحو دیگری تسلیم کند، تنها به شرطی که شخص برای اجرای مجازات تعیین شده در نتیجه محاکمه یا روند استرداد به آن کشور بازگردانده شود، دولت عضو درخواست شونده و کشور عضو درخواست‌کننده در مورد رویه و سایر شرایط آن مطابق بند ۱۰ این ماده باید به توافق برسند.

هر شخصی که در رابطه با هر یک از جرائم مربوط به این ماده مورد رسیدگی قرار می گیرد، باید در تمام مراحل دادرسی، از کلیه حقوق و تضمین‌های مقرر در معاهده بین‌المللی حقوق سیاسی و مدنی[1] و قوانین داخلی کشور عضوی که آن شخص در قلمرو آن حضور دارد برخوردار شود.

1. International Covenant on Civil and Political Rights

هیچ‌یک از مواد این کنوانسیون نباید به‌عنوان تحمیل تعهد به استرداد تفسیر شود، مگر درصورتی‌که دولت عضو درخواست شونده دلایل قابل‌توجهی داشته باشد که درخواست استرداد به‌منظور تعقیب یا مجازات شخصی به دلیل جنسیت، نژاد، زبان، مذهب، ملیت یا منشأ قومی آن شخص انجام‌شده است یا انطباق با این درخواست به هر یک از این دلایل باعث آسیب به موقعیت آن شخص می‌شود.

قبل از امتناع از استرداد، دولت عضو درخواست‌کننده، در صورت لزوم، با دولت عضو درخواست‌کننده مشورت خواهد کرد تا فرصت‌های کافی برای ارائه دیدگاه‌های خود و ارائه اطلاعات مرتبط با حقایق مندرج در درخواستش فراهم شود.

کشورهای عضو باید به دنبال انعقاد معاهدات یا ترتیبات دوجانبه و چندجانبه برای اجرای استرداد یا افزایش اثربخشی آن باشند.

هر کشور عضو یک مقام مرکزی را تعیین خواهد کرد که مسئولیت دریافت درخواست‌های استرداد و اجرای آن‌ها را دارد. درزمانی که یک دولت عضو سند تصویب، پذیرش یا تائید یا الحاق خود به این کنوانسیون را به امانت بگذارد، از سوی مقام مرکزی تعیین‌شده به دبیر کل سازمان ملل متحد اطلاع‌رسانی خواهد شد.

ماده ۴۸- عدم وجود دو حکم در یک‌زمان

اگر حکم نهایی توسط مقامات صلاحیت‌دار دولت عضو درخواست شونده در مورد شخص مورد اتهام در رابطه با جرمی که برای آن درخواست استرداد شده است، صادرشده باشد، استرداد صادر نخواهد شد. درصورتی‌که مقامات صلاحیت‌دار دولت عضو درخواست شونده تصمیم به

عدم تعقیب یا خاتمه دادرسی در رابطه با همان جرم‌گرفته باشند، ممکن است استرداد رد شود.

استرداد شخصی که در کشور ثالث طرف کنوانسیون جرمی مرتکب شده که به خاطر آن درخواست استرداد صادرشده و برای این فرد حکم قطعی صادرشده است، صادر نمی‌شود:

الف) درصورتی‌که حکم مذکور موجب برائت وی شود.

ب) درصورتی‌که مدت حبس یا مجازات دیگری که به آن محکوم‌شده است:

اولاً) به‌طور کامل اجراشده است.

ثانیاً) به‌طور کامل یا نسبت به بخشی که اجرانشده است، مورد عفو قرارگرفته باشد.

ج) درصورتی‌که دادگاه مرتکب را بدون تعیین مجازات محکوم کرده باشد.

بااین‌حال، در موارد مذکور در بند ۲، حکم استرداد ممکن است صادر شود:

الف) اگر جرمی که در رابطه با آن حکم صادرشده است، علیه شخص، مؤسسه یا هر عاملی که یک مقام دولتی در کشور درخواست‌کننده است رخداده باشد.

ب) اگر شخصی که در مورد او حکم صادرشده است، خود یک مقام دولتی در کشور درخواست‌کننده باشد.

ج) اگر جرمی که در مورد آن حکم صادرشده است، به‌طور کامل یا جزئی در قلمرو دولت درخواست‌کننده یا در محلی که به‌عنوان قلمرو آن تلقی می‌شود، انجام‌شده باشد.

مفاد بندهای ۲ و ۳ مانع از اعمال مقررات داخلی گسترده‌تر مربوط به اثر عدم وجود دو حکم در یک‌زمان ملحق به احکام کیفری خارجی نخواهد بود.

ماده ۴۹- مساعدت حقوقی متقابل

کشورهای عضو باید کمک حقوقی متقابل را به‌منظور تحقیقات، پیگرد قانونی یا رسیدگی قضایی در رابطه با جرائم مربوط به استفاده از فناوری اطلاعات و ارتباطات به یکدیگر ارائه کنند.

هر دولت عضو اقدامات قانونی و سایر اقدامات لازم را برای رعایت تعهدات مقرر در مواد ۵۵، ۵۶، ۵۹ تا ۶۲ و ۶۶ این کنوانسیون اتخاذ خواهد کرد. هر کشور عضو تمدید (یا عدم تمدید) یک محدودیت زمانی را برای جلوگیری از فرار از مسئولیت در نظر خواهد گرفت.

جز در مواردی که به‌طور خاص در مواد این فصل پیش‌بینی‌شده باشد، کمک حقوقی متقابل تابع مقررات مندرج در قوانین داخلی کشور عضو درخواست شونده یا در موافقت‌نامه‌های مربوط به معاضدت حقوقی متقابل، ازجمله فهرست دلایل عدم همکاری کامل یا جزئی خواهد بود که دولت عضو درخواست شونده می‌تواند به آن رجوع کند.

هر دولت عضو یک مقام مرکزی را تعیین خواهد کرد که مسئولیت دریافت درخواست‌های کمک حقوقی متقابل و اجرای آن‌ها را دارد. درزمانی که یک دولت عضو سند این کنوانسیون تصویب کرده و بپذیرد، مقام مرکزی تعیین‌شده خود را به دبیر کل سازمان ملل متحد اطلاع خواهد داد.

ماده ۵۰- کمک‌های اضطراری متقابل

ازنظر این ماده، وضعیت اضطراری به وضعیتی اطلاق می‌شود که خطر جدی و قریب‌الوقوع برای جان یا ایمنی هر فردی را در پی داشته باشد.

هر کشور عضو می‌تواند در صورت وجود شرایط اضطراری در کوتاه‌ترین زمان ممکن از یک کشور دیگر درخواست کمک متقابل کند. درخواست تحت این ماده باید در میان سایر مطالب ضروری، شرح حقایقی را که نشان می‌دهد وضعیت اضطراری وجود دارد و ارتباط آن با کمک درخواستی را شامل شود.

دولت عضو درخواست شونده چنین درخواستی را به‌صورت الکترونیکی می‌پذیرد. بااین‌حال، ممکن است درخواست کند که سطح مناسبی از امنیت و احراز هویت قبل از پذیرش درخواست تضمین شود.

دولت عضو درخواست شونده می‌تواند در کوتاه‌ترین زمان ممکن، خواهان اطلاعات بیشتری را برای ارزیابی درخواست شود. دولت عضو درخواست‌کننده باید اطلاعات اضافی را در کوتاه‌ترین زمان ممکن ارائه دهد.

دولت عضو درخواست شونده، پس از اطمینان از وجود شرایط اضطراری و برآورده شدن سایر الزامات کمک متقابل، باید در کوتاه‌ترین زمان ممکن به درخواست پاسخ دهد.

هر کشور عضو باید اطمینان حاصل کند که با مقام مرجع ذیصلاح خود به درخواست‌های کمک متقابل طبق مواد ۴۹ و ۵۲ این کنوانسیون پاسخ می‌دهد و می‌توان به‌صورت ۲۴ ساعته برای پاسخ به درخواست‌ها تماس گرفت.

مقامات صلاحیت‌دار مسئول مساعدت متقابل در هر دو طرف درخواست‌کننده و درخواست شونده ممکن است توافق کنند که نتایج درخواستی که مطابق با این ماده، از طریق کانال ارتباطی جایگزینی غیر ازآنچه معمولاً برای درخواست کمک حقوقی متقابل استفاده می‌شود در اختیار دولت عضو درخواست‌کننده قرار گیرد.

در مواقع اضطراری، درخواست‌ها ممکن است مستقیماً توسط مقامات صلاحیت‌دار دولت عضو درخواست‌کننده به مقامات ذی‌صلاح دولت عضو درخواست شونده یا از طریق اینترپل یا شبکه ۲۴ ساعته مطابق با ماده ۶۶ این کنوانسیون ارائه شود. در چنین مواردی، یک نسخه از درخواست باید هم‌زمان از طریق مقام مرکزی دولت عضو درخواست‌کننده به مقام مرکزی دولت عضو درخواست شونده ارسال شود. اگر درخواست مستقیماً به مقام مرکزی دولت عضو درخواست شونده ارائه شود و آن مقام مرجع صالح برای اجرای درخواست نباشد، باید درخواست را به مقام صلاحیت‌دار ارجاع داده و مرجع مرکزی دولت عضو درخواست‌کننده را از ارجاع مطلع کند. هر کشور عضو می‌تواند در زمان امضا سند این کنوانسیون، به دبیر کل سازمان ملل متحد اطلاع دهد که به‌منظور کارآمدی، درخواست‌هایی که طبق این کنوانسیون ارائه‌شده است باید فقط به مقام مرکزی ارسال شود.

ماده ۵۱- ارائه اطلاعات مناسب

یک دولت عضو می‌تواند، مطابق با قوانین داخلی خود و بدون درخواست قبلی دولت عضو دیگر، اطلاعات جمع‌آوری‌شده در جریان تحقیقات خود را، درصورتی‌که معتقد است افشای چنین اطلاعاتی می‌تواند به آن دولت دیگر کمک کند، ارسال کند.

قبل از ارائه چنین اطلاعاتی، دولت مربوطه ممکن است بخواهد محرمانه بودن اطلاعات حفظ شود یا شرایط خاصی برای استفاده از آن رعایت شود. اگر دولت عضو پذیرنده در موقعیتی نباشد که به چنین درخواستی بپیوندد، باید به دولت عضو ارائه‌دهنده اطلاع دهد تا تصمیم بگیرد که آیا اطلاعات همچنان باید ارائه شود یا خیر. اگر دولت عضو پذیرنده اطلاعات را تحت شرایط فوق بپذیرد، این شرایط برای آن دولت عضو الزام‌آور خواهد بود.

ماده ۵۲- روش‌های ارسال درخواست کمک حقوقی متقابل در صورت عدم وجود معاهدات بین‌المللی قابل‌اجرا

در مواردی که معاهده حقوقی متقابل بین دولت عضو درخواست‌کننده و دولت عضو درخواست شونده وجود نداشته باشد، مفاد بندهای ۲ تا ۸ این ماده اعمال خواهد شد. در صورت وجود چنین معاهده‌ای، مفاد این ماده اعمال نخواهد شد، مگر اینکه کشورهای عضو ذینفع موافقت کنند که به‌جای اسناد فوق‌الذکر، یک یا تمام مقررات این ماده را که در زیر آمده است، اعمال کنند.

الف) هر دولت عضو یک مقام یا مقامات مرکزی را برای ارسال درخواست‌های کمک حقوقی متقابل و پاسخ به آن‌ها، اجابت این درخواست‌ها یا ارجاع آن‌ها به مقامات ذیصلاح تعیین خواهد کرد.

ب) مقام یا مقامات مرکزی مذکور در جزء (الف) فوق باید مستقیماً با یکدیگر ارتباط برقرار کنند.

ج) هر دولت عضو پس از تصویب این کنوانسیون، اسامی و نشانی مقامات تعیین‌شده طبق این بند را به اطلاع دبیر کل سازمان ملل متحد

خواهد رساند.

د) دبیر کل سازمان ملل متحد باید لیست مقامات مرکزی تعیین‌شده توسط کشورهای عضو را گردآوری و به‌روز کند. هر کشور عضو باید به‌طور منظم اطمینان حاصل کند که اطلاعات موجود در لیست اسامی به‌روز است.

هنگام اعطای درخواست برای کمک حقوقی متقابل، مقامات کشورهای عضو درخواست شونده قوانین آن کشور را اعمال خواهند کرد. در صورت درخواست مقام درخواست‌کننده، رویه‌های قانونی دولت درخواست‌کننده می‌تواند اعمال شود؛ مشروط بر این‌که با مفاهیم اساسی نظام حقوقی دولت عضو درخواست شونده مغایرت نداشته باشد.

دولت عضو درخواست شونده می‌تواند از ارائه کمک حقوقی امتناع کند اگر:

الف) درخواست مربوط به جرمی باشد که دولت عضو درخواست شونده آن را جرم علیه دولت یا جرم مرتبط با آن بداند.

ب) انجام درخواست ممکن است، حاکمیت، امنیت، نظم عمومی یا سایر منافع حیاتی او را تضعیف کند.

دولت عضو درخواست شونده می‌تواند درصورتی‌که احساس کند کمک حقوقی در تحقیقات جنایی یا رسیدگی‌های قضایی که توسط مقامات ذیصلاح تداخل ایجاد کند؛ پاسخ به درخواست را به تعویق بی اندازد.

دولت عضو درخواست شونده، قبل از امتناع یا به تعویق انداختن مساعدت حقوقی، با مشورت دولت عضو درخواست‌کننده، می‌تواند درخواست را تا حدی یا مشروط به شرایطی که مناسب بداند بررسی کند.

دولت عضو درخواست شونده باید در اسرع وقت، نتایج اجرای درخواست

کمک حقوقی را به کشور درخواست‌کننده اطلاع دهد. در صورت رد درخواست یا به تعویق افتادن اجرای آن، دولت عضو درخواست‌کننده باید از دلایل رد یا به تعویق انداختن آن مطلع شود.

دولت عضو درخواست‌کننده می‌تواند از دولت عضو درخواست شونده بخواهد که از محرمانه بودن واقعیت و موضوع درخواستی که مطابق با مفاد این فصل ارائه‌شده است اطمینان حاصل کند، اما فقط تا جایی که با تحقق درخواست مطابقت داشته باشد. اگر دولت عضو درخواست شونده نتواند درخواست محرمانه بودن را انجام دهد، باید فوراً دولت عضو درخواست‌کننده را در این مورد مطلع کند. پس‌ازآن دولت عضو درخواست‌کننده تصمیم خواهد گرفت که آیا درخواست همچنان باید برآورده شود یا خیر.

ماده ۵۳- انجام بازجویی‌ها و سایر اقدامات رویه‌ای با استفاده از سیستم‌های کنفرانس ویدیویی یا تلفنی

مقامات صلاحیت‌دار یک دولت عضو می‌توانند با توافق دوجانبه، از طریق استفاده از سیستم‌های کنفرانس ویدیویی یا تلفنی کمک حقوقی ارائه کنند.

سیستم‌های کنفرانس ویدیویی یا تلفنی باید مطابق با قوانین دولت عضو درخواست شونده استفاده شود. اگر دولت عضو درخواست شونده به ابزارهای فنی لازم برای برگزاری کنفرانس ویدئویی دسترسی نداشته باشد، این ابزار ممکن است توسط دولت عضو درخواست‌کننده با توافق دوجانبه ارائه شود.

ماده ۵۴- اختیارات نمایندگی‌های دیپلماتیک و دفاتر کنسولی

کشورهای عضو حق دارند اسناد را از طریق نمایندگی‌های دیپلماتیک یا دفاتر کنسولی به شهروندان خود ابلاغ کنند.

کشورهای عضو این حق را خواهند داشت که تحت دستور مقامات ذیصلاح خود، از شهروندان خود از طریق نمایندگی‌های دیپلماتیک یا دفاتر کنسولی خود، ازجمله از طریق استفاده از سیستم‌های کنفرانس ویدیویی یا تلفنی، بازجویی کنند.

در موارد مندرج در بندهای ۱ و ۲ این ماده از هیچ وسیله اجبار یا تهدیدآمیز نمی‌توان استفاده کرد.

ماده ۵۵ محرمانه بودن و محدودیت‌های استفاده از اطلاعات

در مواردی که توافقنامه معاضدت حقوقی متقابل بین دولت‌های عضو درخواست‌کننده و دولت‌های عضو درخواست شونده، بر اساس یک قانون واحد یا موردتوافق وجود نداشته باشد، مفاد این ماده اعمال نخواهد شد. در صورت وجود چنین توافقنامه یا قانونی، مفاد این ماده اعمال نخواهد شد، مگر این‌که کشورهای عضو ذینفع توافق کنند که به‌جای آن، یک یا همه مفاد این ماده را که در زیر آمده است، اعمال کنند.

در پاسخ به درخواست، دولت عضو درخواست شونده می‌تواند شرایط زیر را برای ارائه اطلاعات یا مطالب تعیین کند:

الف) اطلاعات یا مطالب باید محرمانه بماند؛ در صورت عدم وجود چنین شرایطی، درخواست کمک حقوقی متقابل ممکن است امکان‌پذیر نباشد.

ب) اطلاعات یا مطالب نباید برای هیچ تحقیق یا رسیدگی قانونی دیگری به‌غیراز موارد ذکرشده در درخواست استفاده شود.

اگر دولت عضو درخواست‌کننده نتواند هیچ‌یک از شرایط مندرج در بند (۲) این ماده را رعایت کند، باید فوراً به دیگر دولت عضو اطلاع دهد. سپس دیگر دولت عضو تصمیم خواهد گرفت که آیا چنین اطلاعاتی قابل‌ارائه است یا خیر. اگر دولت عضو درخواست‌کننده موافقت کند که این شرایط را رعایت کند، این شرایط برای آن دولت عضو الزام‌آور خواهد بود.

هر کشور عضوی که اطلاعات یا مطالبی را با توجه به شرایط مندرج در بند ۲ این ماده ارائه می‌کند، می‌تواند از دولت عضو دیگر توضیحاتی در مورداستفاده از این اطلاعات یا در رابطه با هر یک از شرایط تحمیلی درخواست کند.

ماده ۵۶- حفاظت از داده‌های شخصی

داده‌های شخصی ارسال‌شده از یک دولت عضو به کشور عضو دیگر بنا به درخواستی که طبق این کنوانسیون ارائه می‌شود، می‌تواند فقط برای اهداف جنایی، اداری یا دادرسی مدنی و سایر رویه‌های قضایی یا اداری که مستقیماً با آن رسیدگی‌ها مرتبط است و همچنین برای جلوگیری از تهدید جدی و قریب‌الوقوع برای امنیت عمومی افرادی که اطلاعات شخصی آن‌ها مخابره می‌شود، استفاده شود.

چنین داده‌های شخصی را نمی‌توان بدون رضایت کتبی قبلی کشور عضو انتقال‌دهنده داده‌ها و در موضوع داده‌های شخصی با رضایت شخص ثالث به اشتراک گذاشت.

دولت عضوی که داده‌های شخصی را بنا به درخواستی که طبق این کنوانسیون ارائه می‌شود، ارسال می‌کند، می‌تواند به کشور عضوی که داده‌ها به آن منتقل‌شده است، اطلاعاتی در مورداستفاده از آن‌ها ارائه دهد.

ماده ۵۷- انتقال دادرسی کیفری کشورهای عضو

انتقال دادرسی و تعقیب کیفری جرائم این کنوانسیون، درصورتی‌که چنین انتقالی به نفع اجرای صحیح عدالت تلقی شود، به ویژه در مواردی که مشتمل بر چندین حوزه قضایی باشد، با هدف اطمینان از ادغام دادرسی کیفری انجام می‌شود.

ماده ۵۸- انتقال محکومین دولت‌های طرف کنوانسیون

انعقاد موافقت‌نامه‌های دوجانبه یا چندجانبه یا سایر ترتیبات مربوط به انتقال افرادی که به دلیل جرائم این کنوانسیون به حبس یا سایر اشکال محرومیت از آزادی محکوم‌شده‌اند کمک می‌کند این افراد بتوانند مجازات خود را در قلمرو کشورهای عضو مربوطه سپری کنند.

ماده ۵۹- حفظ تسریع اطلاعات الکترونیکی

هر کشور عضو می‌تواند از کشور دیگر عضو درخواست کند که جهت اطمینان از حفظ سریع اطلاعاتی که با استفاده از فناوری اطلاعات و ارتباطات در قلمرو آن کشور عضو و در رابطه با موضوعی که دولت عضو درخواست‌کننده قصد دارد در چارچوب کمک حقوقی متقابل درخواستی برای جستجو یا توقیف یا درخواست دیگری برای حفظ یا کسب آن اطلاعات ارسال کند؛ دستوراتی را صادر کند یا اقداماتی را انجام دهد.
در درخواست حفظ اطلاعاتی که طبق بند ۱ این ماده انجام می‌شود باید موارد زیر مشخص شود:

الف) نام مرجع درخواست‌کننده.

ب) خلاصه‌ای از حقایق اساسی و ماهیت تحقیق، تعقیب یا رسیدگی

قضایی که درخواست مربوط به آن است.

ج) اطلاعات الکترونیکی که باید حفظ شود و ارتباط آن با جرم یا عمل غیرقانونی که در رابطه با آن درخواست ارائه‌شده است.

د) هرگونه داده موجود که مالک اطلاعات یا مکان دستگاه فناوری اطلاعات و ارتباطات را شناسایی می‌کند.

ه) توجیه نیاز به حفظ اطلاعات.

و) اطلاعیه‌ای مبنی بر اینکه دولت عضو قصد دارد در چارچوب مساعدت حقوقی متقابل، درخواستی برای جستجو، توقیف یا سایر اقدامات لازم برای حفظ اطلاعات موردنظر ارائه کند.

به‌محض دریافت چنین درخواستی از یک کشور عضو دیگر، دولت عضو درخواست شونده باید اقدامات مقتضی را مطابق با قوانین داخلی خود انجام دهد تا فوراً از حفظ اطلاعات مشخص‌شده در بند ۱ این ماده اطمینان حاصل کند. دولت عضو درخواست شونده می‌تواند به‌طور کامل یا جزئی، درخواست تضمین حفظ اطلاعات را انجام دهد، حتی اگر عملی که مبنای درخواست را تشکیل می‌دهد در کشور درخواست شونده جرم انگاری نشده باشد.

اگر دولت عضو درخواست شونده احساس کند که اجرای درخواست می‌تواند به حاکمیت، امنیت یا سایر منافع اساسی آن لطمه وارد کند، ممکن است درخواست حفظ اطلاعات رد شود.

درصورتی‌که دولت عضو درخواست شونده معتقد باشد که اجرای درخواست مذکور در بند ۱ این ماده حفظ آینده اطلاعات را تضمین نمی‌کند یا محرمانگی را به خطر می‌اندازد یا به نحو دیگری به تحقیقات، تعقیب یا رسیدگی قضایی لطمه می‌زند، باید فوراً نسبت به این موضوع

اطلاع‌رسانی کند. دولت عضو درخواست‌کننده تصمیم خواهد گرفت که آیا درخواست باید اجرا شود یا خیر.

هرگونه حفاظت از اطلاعات که در پاسخ به درخواست مذکور در بند ۱ این ماده انجام می‌شود، برای مدت حداقل ۹۰ روز خواهد بود تا دولت عضو درخواست‌کننده بتواند درخواستی برای جستجو، توقیف یا سایر اقدامات ارائه کند. پس از دریافت چنین درخواستی، دولت عضو درخواست شونده باید آن اطلاعات را تا زمان تصمیم‌گیری در مورد آن درخواست حفظ کند.

ماده ۶۰- افشای سریع داده‌های ترافیکی حفظ‌شده

هنگامی‌که در جریان اجرای یک درخواست برای حفظ اطلاعات ارائه‌شده به‌موجب ماده ۵۹ این کنوانسیون، دولت عضو درخواست شونده متوجه می‌شود که ارائه‌دهنده خدمات از کشور دیگری در انتقال اطلاعات شرکت داشته است باید به‌سرعت به کشور عضو درخواست‌کننده مقدار کافی از داده‌های ترافیکی را فاش کند تا امکان شناسایی آن شرکت ارائه‌دهنده خدمات و مسیری که از طریق آن اطلاعات منتقل‌شده است وجود داشته باشد.

اگر دولت عضو درخواست شونده فکر کند که اجرای این درخواست می‌تواند به حاکمیت، امنیت یا سایر منافع اساسی آن لطمه وارد کند، ممکن است درخواست کشور خواهان را رد کند.

ماده ۶۱- کمک متقابل در مورد جمع‌آوری فوری داده‌های ترافیکی

یک دولت عضو، بنا به درخواست دولت عضو دیگر، جمع‌آوری بی‌درنگ

داده‌های ترافیکی را در قلمرو خود یا در قلمرو تحت صلاحیت خود انجام خواهد داد و اطلاعات جمع‌آوری‌شده را طبق رویه‌های تعیین‌شده توسط قانون داخلی خود و به‌شرط وجود دلایل مرتبط، به دولت عضو درخواست‌کننده ارسال می‌کند.

در درخواستی که مطابق بند (۱) این ماده انجام می‌شود، باید موارد زیر مشخص شود:

الف) نام مرجع درخواست‌کننده.

ب) خلاصه‌ای از حقایق اساسی و ماهیت تحقیق، تعقیب یا رسیدگی قضایی که درخواست مربوط به آن است.

ج) اطلاعات الکترونیکی که جمع‌آوری داده‌های ترافیکی در رابطه با آن موردنیاز است و ارتباط آن با جرم مربوطه یا سایر اعمال غیرقانونی.

د) هرگونه داده موجود که مالک/کاربر اطلاعات و مکان دستگاه فناوری اطلاعات و ارتباطات را شناسایی می‌کند.

ه) توجیه نیاز به جمع‌آوری داده‌های ترافیکی؛ توجیه انتخاب دوره مشخص‌شده برای جمع‌آوری داده‌های ترافیکی.

و) دوره جمع‌آوری داده‌های ترافیکی.

ماده ۶۲- کمک متقابل در مورد جمع‌آوری اطلاعات الکترونیکی

یک دولت عضو باید در قلمرو خود یا در قلمرو تحت صلاحیت خود، جمع‌آوری بی‌درنگ اطلاعات را به‌صورت دیجیتالی و الکترونیکی و از طریق فناوری اطلاعات و ارتباطات، ازجمله داده‌های مربوط به محتویات پیام‌ها، مطابق با رویه‌های تعیین‌شده توسط قانون داخلی خود انجام دهد. چنین اطلاعاتی باید مطابق با قوانین داخلی کشور عضو جمع‌آوری‌کننده

اطلاعات و همچنین موافقت‌نامه‌های موجود کمک حقوقی به کشور دیگر عضو ارائه شود.

ماده ۶۳- تحقیقات مشترک

مقامات صلاحیت‌دار دو یا چند دولت عضو می‌توانند با توافق دوجانبه، گروه‌های تحقیقاتی مشترکی را برای یک هدف خاص و برای مدت محدودی که ممکن است با توافق دوجانبه تمدید شود، تشکیل دهند تا تحقیقات جنایی در یک یا بیشتر کشورهای عضوی که گروه را تشکیل داده‌اند انجام شود. برای این منظور، کشورهای عضو باید انعقاد موافقت‌نامه‌های دو یا چندجانبه را بررسی کنند. ترکیب گروه باید در توافقنامه مشخص شود. درخواست برای تشکیل یک گروه تحقیقاتی مشترک ممکن است از طرف هر کشور عضو ذینفع صادر شود. گروه باید دریکی از کشورهای عضوی که تحقیقات در آنجا انجام شود تشکیل می‌شود. کشورهای عضو باید اطمینان حاصل کنند که حاکمیت کشور عضوی که چنین تحقیقاتی در قلمرو آن انجام می‌شود کاملاً محترم شمرده می‌شود.

ماده ۶۴- روش‌های تحقیقاتی ویژه

به‌منظور مبارزه مؤثر با جرائم مربوط به استفاده از فناوری اطلاعات و ارتباطات، هر کشور عضو تا حدی که اصول اساسی قوانین داخلی خود اجازه می‌دهد و با رعایت شرایط مقرر در قوانین خود، باید به بهترین نحو ممکن عمل کند، با توجه به توانایی خود، اقدامات لازم را انجام دهد تا امکان استفاده مناسب توسط مقامات ذیصلاح خود مانند نظارت الکترونیکی یا سایر اشکال نظارتی و همچنین برای انجام عملیات مخفی

توسط مقام صلاحیت‌دار خود را فراهم کند و اطمینان حاصل شود که شواهد جمع‌آوری‌شده از طریق این روش‌ها در دادگاه قابل‌قبول است. به‌منظور بررسی جرائم مشمول این کنوانسیون، کشورهای عضو تشویق می‌شوند تا در صورت لزوم، موافقت‌نامه‌ها یا ترتیبات مناسب دوجانبه یا چندجانبه را برای استفاده از چنین فن‌های تحقیقاتی در چارچوب همکاری در سطح بین‌المللی منعقد کنند. چنین موافقت‌نامه‌هایی باید با رعایت کامل اصل برابری حاکمیت دولت‌ها منعقد و اجرا شود و کاملاً مطابق با شرایط آن موافقت‌نامه‌ها اجرا شود.

در صورت عدم وجود توافق یا ترتیبی که در بند ۲ این ماده پیش‌بینی‌شده است، تصمیمات مربوط به استفاده از چنین روش‌های تحقیقاتی ویژه‌ای در سطح بین‌المللی باید به‌صورت موردی و در صورت لزوم با در نظر گرفتن ترتیبات مالی و تفاهم‌های مربوط به اعمال صلاحیت قضایی توسط کشورهای عضو مربوط اتخاذ شود.

ماده ۶۵- همکاری بین سازمان‌های مجری قانون

دولت‌های عضو باید با یکدیگر همکاری نزدیک داشته باشند و بر اساس سیستم‌های حقوقی و اداری داخلی خود عمل کنند و باهدف افزایش کارایی اقدامات مجری قانون برای مبارزه با جرائم مشمول این کنوانسیون عمل کنند. برای مثال، دولت‌های عضو باید اقدامات مؤثری را با اهداف زیر انجام دهند:

الف) تقویت یا در صورت لزوم ایجاد کانال‌های ارتباطی بین مقامات، آژانس‌ها و مراجع ذی‌صلاح خود برای تضمین تبادل امن و سریع اطلاعات در مورد تمام جنبه‌های جرائم تحت پوشش این کنوانسیون.

ب) همکاری با سایر کشورهای عضو در انجام تحقیقات در رابطه با جرائم مشمول این کنوانسیون به‌منظور تعیین موارد زیر:

ب-۱) هویت، محل نگهداری و فعالیت‌های افراد مشکوکی که در چنین جرائمی دست داشتند یا محل نگهداری سایر افراد درگیر عملیات مجرمانه.

ب-۲) جابجایی عواید ناشی از جرائم یا اموال حاصل از ارتکاب چنین جرائمی.

ب- ۳) جابجایی اموال، ابزار، تجهیزات یا سایر وسایل مورداستفاده یا در نظر گرفته‌شده برای استفاده در ارتکاب چنین جرائمی.

ب-۴) انتقال اقلامی که برای ارتکاب جرم استفاده‌شده است، ازجمله ابزار جرم؛ اقلامی که درنتیجه جرم یا به‌عنوان پاداش برای آن ارتکاب جرم‌ها به‌دست‌آمده است یا اقلامی که مجرم در ازای جرم از این طریق به دست آورده است. و مواردی که ممکن است به‌عنوان مدرک در یک پرونده جنایی کمک کنند.

ب-۵) تبادل اطلاعات با سایر کشورهای عضو در مورد ابزارها و روش‌های خاصی که برای ارتکاب جرائم مشمول این کنوانسیون به کار می‌رود، ازجمله نمونه‌هایی از نرم‌افزارهای مخرب، استفاده از هویت‌های جعلی، اسناد جعلی، تغییریافته و سایر ابزارهای پنهان کردن فعالیت‌های غیرقانونی؛

ب- ۶) تسهیل هماهنگی مؤثر بین مقامات، آژانس‌ها و خدمات ذی‌صلاح خود و تشویق تبادل کارکنان و کارشناسان و اعزام افسران رابط، مشروط به انعقاد موافقت‌نامه‌ها یا ترتیبات دوجانبه بین دولت‌های مربوطه؛

ب- ۷) تبادل اطلاعات موردعلاقه و انجام اقدامات هماهنگ برای کشف زودهنگام جرائم تحت پوشش این کنوانسیون.

به‌منظور اجرای این کنوانسیون، دولت‌های عضو می‌توانند به انعقاد موافقت‌نامه‌ها یا ترتیبات دوجانبه یا چندجانبه در مورد همکاری مستقیم بین سازمان‌های مجری قانون خود مبادرت نموده و در صورت وجود چنین موافقت‌نامه‌ها یا ترتیباتی، بهبود آن‌ها را در نظر بگیرند. در مواردی که چنین توافقنامه‌ها یا ترتیباتی بین دولت‌های مربوطه وجود نداشته باشد، دولت‌های عضو می‌توانند این کنوانسیون را به‌عنوان مبنایی برای همکاری متقابل اجرای قانون در رابطه با جرائم تحت پوشش این کنوانسیون در نظر بگیرند. کشورهای عضو، در صورت لزوم، از توافق‌ها یا سازوکارهای سازمان‌های بین‌المللی یا منطقه‌ای، برای تقویت همکاری بین سازمان‌های مجری قانون خود، استفاده کامل خواهند کرد. هر کشور عضو ممکن است در شرایط اضطراری از طریق وسایل ارتباطی سریع، ازجمله دورنگار یا پست الکترونیکی، درخواست کمک را ارسال کند، البته اگر چنین وسایلی سطح مناسبی از امنیت و احراز هویت (ازجمله رمزگذاری، در صورت لزوم) را تضمین کند. دولت عضو درخواست شونده چنین درخواستی را می‌پذیرد و با هر وسیله ارتباطی سریع مشابهی به آن پاسخ می‌دهد. دولت عضو درخواست شونده می‌تواند پس از دریافت درخواست اصلی، حق ارسال پاسخ را برای خود محفوظ نگه دارد و مراتب را به مقام ذی‌صلاح اطلاع خواهد داد.

ماده ۶۶- شبکه ۷/۲۴

هر کشور عضو باید یک نقطه تماس ۷/۲۴(بیست‌وچهار ساعتِ هفت روز هفته) را برای ارائه کمک سریع در تحقیقات، تعقیب قضایی یا رسیدگی قضایی در رابطه با جرائم مربوط به سیستم‌ها و داده‌های رایانه‌ای یا در

جمع‌آوری شواهد مرتبط با جرم تشکیل دهد. چنین کمکی باید شامل حمایت یا در مواردی که طبق قانون یا رویه داخلی آن‌ها مجاز باشد، اعمال مستقیم اقدامات زیر باشد:

الف) ارائه مشاوره فنی.

ب) اطمینان از امنیت داده‌ها برای جمع‌آوری شواهد و همچنین موافقت‌نامه‌های کمک حقوقی متقابل.

هر کشور عضو باید اقداماتی را برای تأمین کارکنان و تجهیزات واجد شرایط برای تسهیل عملیات چنین شبکه‌ای انجام دهد.

بخش ۲

اقدامات برای بازیابی اموال

ماده ۶۷- مقررات عمومی کشورهای طرف کنوانسیون

کشورهای عضو با رعایت مقررات این کنوانسیون و قوانین داخلی خود، بیشترین همکاری و مساعدت حقوقی متقابل را برای بازیابی اموالی که از طرق مجرمانه به‌دست‌آمده است به یکدیگر ارائه خواهند کرد. هم‌چنین باید معاهدات مربوط به سازمان‌های بین‌المللی منطقه‌ای و بین منطقه‌ای در زمینه مبارزه با پول‌شویی در نظر گرفته شود.

ماده ۶۸- پیشگیری و کشف و انتقال عواید حاصل از جرم

یک دولت عضو باید تمام اقدامات لازم را انجام دهد تا بتواند مطابق با قوانین داخلی خود از مؤسسات مالی و همچنین سازمان‌هایی که دارایی‌های مالی دیجیتال و ارز دیجیتال دارند اطلاعات به دست آورد. در

حوزه قضایی، اطلاعات هویت مشتریان و مالکان ذینفع در ارتکاب جرائم پیش‌بینی‌شده اهمیت دارد.

یک دولت عضو باید تمام اقدامات لازم را اتخاذ کند تا مطابق با قوانین داخلی خود از مؤسسات مالی و همچنین سازمان‌هایی که در فعالیت‌های مربوط به گردش دارایی‌های مالی دیجیتال و ارز دیجیتال فعالیت می‌کنند، بخواهد حساب‌ها را موردبررسی منطقی قرار دهند.

اقدامات مذکور در بندهای ۱ و ۲ این ماده باید به‌طور منطقی برای کشف معاملات مشکوک و گزارش آن به مقامات ذیصلاح طراحی شود و نباید به‌گونه‌ای تعبیر شود که مؤسسات مالی را از انجام تجارت با مشتری منع کند.

هر کشور عضو باید تدابیری اتخاذ کند تا اطمینان حاصل کند مؤسسات مالی و سازمان‌هایی که در فعالیت‌های مربوط به دارایی‌های مالی دیجیتال و ارز دیجیتال فعالیت می‌کنند، در طی یک دوره زمانی مناسب، سوابق کافی از حساب‌ها و تراکنش‌های مربوطه را حفظ می‌کنند. هر دولت عضو، بر اساس قوانین داخلی خود، ایجاد سیستم‌های مؤثری را برای افشای اطلاعات مالی در مورد اشخاص مشکوک به ارتکاب جرائم این کنوانسیون بررسی خواهد کرد و برای عدم رعایت الزامات مذکور در این ماده، مجازات مناسبی را پیش‌بینی خواهد کرد. هر کشور عضو نیز اقدامات لازم را در نظر خواهد گرفت تا به مقامات ذیصلاح خود اجازه دهد در صورت لزوم آن اطلاعات را با مقامات ذیصلاح در سایر کشورهای عضو به اشتراک بگذارند.

با هدف جلوگیری و کشف نقل و انتقال عواید ناشی از جرائم ایجاد شده مقرر در این کنوانسیون، هر کشور عضو باید اقدامات مناسب و مؤثری

را بـا کمـک نهادهـای نظارتـی و نظارتـی خـود بـرای جلوگیـری از تأسـیس بانک‌هایـی کـه حضـور فیزیکـی ندارنـد و بـه یـک گـروه مالـی تحـت نظارت وابسـته نیسـتند به اجـرا بگذارد. عـلاوه بر این، کشـورهای عضو ممکن اسـت در نظر داشـته باشـند که مؤسسـات مالی خود و همچنین سـازمان‌هایی را که در فعالیت‌هـای مربـوط بـه گردش دارایی‌هـای مالی دیجیتـال و ارز دیجیتالی فعالیـت می‌کننـد، ملـزم کننـد از ورود یـا ادامـه روابـط بانکی وابسـته به این مؤسسـات خـودداری کننـد و از ایجـاد روابـط بـا موسسـات مالـی خارجی که اجـازه می‌دهنـد حساب‌هایشـان توسـط بانک‌هایـی اسـتفاده شـود کـه هیـچ حضـور فیزیکـی ندارنـد و بـه یک گـروه مالـی تحت نظارت وابسـته نیسـتند محافظـت کنند.

هـر کشـور عضـو، طبـق قوانیـن داخلی خـود، باید سیسـتم‌های مؤثر برای افشـای اطلاعـات مالـی را در مـورد اشـخاصی کـه در رابطـه با آنهـا اطلاعاتی در مـورد اتهـام بـه دخالـت آنهـا در جرائم مشـمول مقـررات این کنوانسـیون وجـود دارد، ایجـاد کنـد و باید تحریم های مناسـب برای عـدم رعایت الزامات موضـوع ایـن مـاده را پیش‌بینی کنـد. همچنین هر کشـور عضو بایـد اقدامات لازم را در بگیـرد تـا بـه مقامـات ذیصـلاح خـود اجـازه دهـد در صـورت لزوم بـرای تحقیـق و اقـدام بـه منظـور بازیابـی عوایـد ناشـی از جرایـم مقـرر در ایـن کنوانسـیون در صـورت لـزوم آن اطلاعـات را بـا مقامـات ذیصـلاح سـایر کشـورهای عضـو به منظور تحقیق و اقـدام برای بازیابی عواید ناشـی از جرایم مقـرر در این کنوانسـیون بـه اشـتراک بگذارند.

ماده ۶۹- تدابیر برای بازیابی مستقیم اموال هر کشور عضو

هـر کشـور مطابـق بـا قوانیـن داخلی خـود، موظف اسـت اقدامـات قانونی

لازم را در راستای موارد زیر اتخاذ کند:

الف) به دولت دیگر عضو، اتباع خود و افراد بدون تابعیت که به‌طور دائم در قلمرو خود اقامت دارند و اشخاص حقوقی تأسیس‌شده یا دارای دفتر مقیم در قلمرو آن، اجازه اقامه دعوای مدنی در دادگاه‌های آن کشور عضو برای احراز حق مالکیت اموالی که در نتیجه ارتکاب یک جرم به‌دست‌آمده است را بدهد.

ب) به دادگاه‌های خود اجازه دهد که به پرداخت غرامت یا خسارات ناشی از ارتکاب این‌گونه جرائم، دستور دهند.

ج) به دادگاه‌ها یا مقامات ذی‌صلاح خود اجازه دهد، در هنگام تصمیم‌گیری در مورد مصادره اموال ناشی از جرم، ادعای کشور عضو دیگر، اتباع آن یا افراد بدون تابعیت را که به‌طور دائم در قلمرو آن ساکن هستند و اشخاص حقوقی مستقر در قلمرو خود را به‌عنوان مالک قانونی اموالی که از طریق ارتکاب جرم به‌دست‌آمده است، به رسمیت بشناسند.

ماده ۷۰- سازوکارهای مصادره اموال از طریق همکاری بین‌المللی در مصادره

هر دولت عضو به‌منظور ارائه کمک حقوقی متقابل در رابطه با اموالی که از طریق ارتکاب جرم طبق این کنوانسیون به‌دست‌آمده است مطابق با قوانین داخلی خود: الف) باید اقدامات لازم را اتخاذ کند تا مقامات ذیصلاح خود را قادر سازند و حکم مصادره که توسط دادگاه یک کشور عضو دیگر صادرشده است را اجرا کنند. ب) اقدامات لازم را در محدوده صلاحیت خود اتخاذ کند تا مقامات صلاحیت‌دار خود را قادر سازد تا اموال با منشأ خارجی را با دستور قضایی در رابطه با قانونی شدن عواید

حاصل از جرم مصادره کنند. ج) تدابیری اتخاذ کنند را که امکان مصادره غیر محکومیتی این اموال در دادرسی کیفری در مواردی که مجرم به دلیل مرگ، فرار یا غیبت یا در سایر موارد مقتضی قابل‌تعقیب نباشد، میسر باشد.

هر دولت عضو، به‌منظور ارائه کمک حقوقی متقابل، بنا به درخواست دولت دیگر عضو این کنوانسیون، باید مطابق با قوانین داخلی خود:

الف) به مقامات ذیصلاح خود اجازه دهد اموال را به‌موجب دستور توقیف صادرشده توسط دادگاه یا سایر مقامات ذیصلاح دولت درخواست‌کننده توقیف کنند. البته درصورتی‌که مبنای معقول و دلایل کافی برای کشور درخواست شونده ارائه شود، این اموال درنهایت مشمول مصادره خواهد شد. دستور برای اهداف بند ۱ (الف) این ماده؛

ب) به مقامات ذیصلاح خود اجازه دهد تا اموال را در صورت درخواست با مبنای معقول توقیف کنند. این دارایی درنهایت مشمول یک دستور مصادره برای اهداف بند ۱ (الف) این ماده خواهد شد؛

ج) به مقامات ذیصلاح خود اجازه دهد تا در مواردی مانند دستور توقیف خارجی یا اتهامات جنایی در ارتباط با تحصیل چنین اموالی، دارایی را برای مصادره نگه دارند.

مطابق بند ۲ این ماده در صورت درخواست مربوطه به‌صورت کتبی، مساعدت حقوقی ارائه می‌شود.

اگر در صحت یا محتوای درخواست تردید وجود داشته باشد، ممکن است تأییدیه اضافی درخواست شود.

درخواست باید حاوی اطلاعات زیر باشد:

الف) نام درخواست‌کننده و مرجع صالح درخواست شونده.

ب) مبنای واقعی پرونده.
ج) هدف و توجیه درخواست.
د) شرح محتوای کمک درخواستی.
ه) کپی دستور توقیف در صورت وجود.
و) هرگونه اطلاعات دیگری که می‌تواند برای اجرای صحیح درخواست مفید باشد.

۶. درخواست ارسالی یا تائید شده به‌صورت کتبی باید توسط مقام مجاز مرجع ذیصلاح امضا و مهر شود.

ماده ۷۱- همکاری بین‌المللی برای مصادره

دولت عضوی که درخواستی را از کشور عضو دیگری که صلاحیت رسیدگی به جرمی را که مطابق این کنوانسیون برای مصادره اموال مندرج در بند ۱ ماده ۷۳ کنوانسیون دریافت کرده است باید: الف) به‌منظور اخذ حکم مصادره و در صورت صدور حکم، اجرای آن درخواست را به مقامات ذیصلاح خود ارائه کند. یا

ب) به مقامات صلاحیت‌دار خود دستور مصادره دادگاه دولت درخواست کننده را با هدف اثربخشی به درخواست و اموال مربوطه واقع در قلمرو دولت عضو درخواست شونده که در نتیجه ارائه جرایم مقرر در این کنوانسیون به دست آمده است، ارائه کند.

پس از درخواست توسط دولت عضو دیگری که صلاحیت رسیدگی به جرم را دارد، دولت عضو که درخواست شونده اقداماتی را برای شناسایی یا توقیف اموال به‌دست‌آمده در نتیجه ارتکاب جرائم مقرر در این کنوانسیون یا ابزارهای مورد استفاده برای جرایمی که در بند ۱ (ب) این ماده

ذکر شده اتخاذ خواهد کرد تا دستور مصادره نهایی توسط دولت عضو درخواست کننده یا بنا به درخواست آن دولت عضو طبق بند ۱ این ماده صادر شود.

تصمیمات یا اقدامات پیش‌بینی‌شده در بندهای ۱ و ۲ این ماده توسط دولت عضو که درخواست مصادره از او شده است مطابق با مفاد قوانین داخلی خود و هرگونه موافقت‌نامه یا ترتیبات دو یا چندجانبه‌ای اتخاذ خواهد شد که به‌موجب آن ممکن است در روابط با کشور متعهد شود. هر دولت عضو باید نسخه‌هایی از قوانین و مقررات خود را که مفاد این ماده و هرگونه اصلاحیه بعدی در این قوانین و مقررات یا شرح آن را اعمال می‌کند، به دبیر کل سازمان ملل ارائه کند.

درصورتی‌که دولت عضو درخواست شونده دستور مقامات ذی‌صلاح دولت عضو درخواست‌کننده یا مدارک موردنیاز برای مقامات صلاحیت‌دار دولت درخواست شونده را به‌موقع دریافت نکند، درخواستی که طبق این ماده ارائه می‌شود، ممکن است رد شود یا اقدامات موقتاً لغو شود.

قبل از لغو هرگونه اقدام موقت اتخاذشده به‌موجب این ماده، دولت عضو که درخواست مصادره از او شده است در صورت امکان، فرصتی را برای دولت درخواست‌کننده فراهم می‌کند تا دلایل خود را در مورد ادامه اقدامات ارائه دهد.

مقررات این ماده نباید به‌عنوان لطمه به حقوق اشخاص ثالث با حسن نیت تعبیر شود.

ماده ۷۲- همکاری ویژه

بدون غرض ورزی نسبت به قوانین داخلی خود، هر کشور عضو باید اقداماتی

را اتخاذ کند تا به ابتکار خود مشروط بر این که به تحقیقات یا اقدامات قضایی انجام شده توسط مقامات ذی صلاح خود لطمه ای وارد نکند، اطلاعات مربوط به اموال حاصل از ارتکاب جرمی را که طبق این کنوانسیون مقرر شده است، به یکی دیگر از کشورهای عضو ارسال کند، در صورتی که گمان می کند افشای چنین اطلاعاتی ممکن است زمینه را برای مقامات صلاحیتدار دولت عضو پذیرنده فراهم کند تا تحقیقات یا رسیدگی قضایی را آغاز کنند یا ممکن است منجر به چنین درخواستی از سوی آن دولت عضو طبق این سر فصل شود.

ماده ۷۳- استرداد و دفع اموال

دولت عضوی که طبق مقررات این فصل اموال را مصادره کرده است، باید این اموال را از طریق بازگرداندن به صاحبان قانونی اولیه‌اش، مطابق بند ۳ این ماده و قوانین داخلی خود، کنار بنهد.

هر کشور عضو باید کلیه اقدامات قانونی و سایر اقدامات لازم را اتخاذ کند تا هنگام درخواست دولت دیگر عضو، مقامات ذیصلاح آن کشور با در نظر گرفتن حقوق اشخاص ثالث، با حسن نیت و مطابق با قوانین داخلی خود قادر به بازگرداندن اموال مصادره شده باشند.

مطابق ماده ۷۱ این کنوانسیون و بندهای ۱ و ۲ این ماده، دولت عضو که از او درخواست شونده باید:

الف) در مورد اختلاس اموال عمومی مصادره شده طبق ماده ۶۸ این کنوانسیون و بر اساس حکم نهایی صادرشده در دولت عضو درخواست‌کننده، اموال مصادره شده را به دولت عضو درخواست‌کننده بازگرداند. ب) در سایر موارد، اولویت را به بازگرداندن اموال مصادره شده

بـه صاحبـان قانونـی قبلی آن یا پرداخـت غرامت یا خسـارات وارده به قربانیان جرم بدهد.

در صـورت اقتضـا، دولـت عضـو درخواسـت شـونده می‌توانـد هزینه‌هـای معقولـی را کـه در جریـان تحقیقـات یـا رسـیدگی‌های قضایی هزینه شـده را کسـر کند.

به‌منظـور دسـتیابی بـه ترتیبات قابل‌قبـول دوجانبه در مورد دفـع نهایی اموال مصادره شـده، کشـورهای عضـو می‌تواننـد مشـورت کـرده و موافقت‌نامه‌های جداگانـه منعقد کنند.

ماده ۷۴- هزینه‌ها

هزینه‌هـای عـادی مربوط به درخواسـت باید توسـط دولتی که درخواسـت مصـادره از او شـده اسـت پوشـش داده شـود، مگـر اینکـه کشـورهای عضـو ذی‌ربـط بـه نحـو دیگـری توافق کننـد. اگـر هزینه‌های اساسـی یـا فوق‌العاده بـرای انجـام درخواسـت موردنیـاز باشـد، کشـورهای عضـو بایـد بـرای تعیین شـرایط و ضوابـط اجـرای درخواسـت و همچنیـن نحـوه پرداخـت هزینه‌هـا مشـورت کنند.

فصل پنجم
کمک فنی و آموزش

ماده ۷۵- اصول کلی کمک فنی

دولت‌هـای عضـو بایـد تـا حـدی کـه می‌تواننـد بـه یکدیگـر بیشـترین میـزان کمک‌هـای فنـی را بخصـوص بـه نفـع کشـورهای درحال‌توسـعه برای

مبارزه با جرائم فناوری اطلاعات و ارتباطات، ازجمله آموزش در زمینه‌های اشاره‌شده در ماده ۷۶ این کنوانسیون و همچنین آموزش و کمک و تبادل متقابل تجربه و تخصص مرتبط که همکاری بین‌المللی بین کشورهای عضو در مورد استرداد و کمک‌های حقوقی متقابل را تسهیل می‌کند، ارائه دهند.

کشورهای عضو باید تا حد ضرورت تلاش‌ها را برای به حداکثر رساندن اثربخشی فعالیت‌های عملیاتی و آموزشی در سازمان‌های بین‌المللی و منطقه‌ای و در چارچوب موافقت‌نامه‌ها یا ترتیبات دوجانبه و چندجانبه تقویت کنند.

کشورهای عضو در صورت درخواست، کمک به یکدیگر را در انجام ارزیابی‌ها، مطالعات و تحقیقات مربوط به انواع، علل و آثار جرائم فناوری اطلاعات و ارتباطات ارتکابی در کشورهای متبوع خود، با هدف توسعه استراتژی‌ها و برنامه‌های اقدام برای مبارزه با این نوع جرائم، با مشارکت مقامات ذی‌صلاح بررسی خواهند کرد.

کشورهای عضو وظیفه ارائه کمک‌های فنی تخصصی به دولت‌های عضو را به‌منظور ارتقای اجرای برنامه‌ها و پروژه‌های مبارزه با جرائم فناوری اطلاعات و ارتباطات و سایر جرائم به دفتر مبارزه با مواد مخدر و جرائم سازمان‌یافته سازمان ملل واگذار خواهند کرد.

ماده ۷۶- آموزش

هر دولت عضو باید در صورت لزوم برنامه‌های آموزشی خاصی را برای کارکنان خود که مسئول پیشگیری و مبارزه با جرائم فناوری اطلاعات و ارتباطات هستند، توسعه داده، اجرا کرده یا بهبود بخشد. چنین برنامه‌های آموزشی می‌تواند در زمینه‌های زیر باشد:

الف) اقدامات مؤثر برای پیشگیری، کشف و تحقیق جرائم فناوری اطلاعات و ارتباطات و همچنین مجازات و مبارزه با آن‌ها، ازجمله استفاده و جمع‌آوری شواهد الکترونیکی و تکنیک‌های تحقیق.

ب) ظرفیت‌سازی برای توسعه و برنامه‌ریزی یک سیاست راهبردی برای مبارزه با جرائم فناوری اطلاعات و ارتباطات.

ج) آموزش کارکنان مقامات صلاحیت‌دار در تهیه درخواست استرداد، حمایت از اجرای قانون و کمک حقوقی متقابل که الزامات این کنوانسیون را برآورده می‌کند.

د) جلوگیری از انتقال عواید ناشی از جرائم ایجادشده بر اساس این کنوانسیون و بازیابی این عواید.

ه) کشف و مسدود کردن معاملات مربوط به انتقال عواید ناشی از جرائم مطابق این کنوانسیون.

و) نظارت بر جابجایی عواید ناشی از جرائم ایجادشده طبق این کنوانسیون و روش‌های مورداستفاده برای انتقال و مخفی کردن این عواید.

ز) سازوکارها و روش‌های قانونی و اداری مناسب و کارآمد برای تسهیل توقیف و مصادره عواید ناشی از جرائم بر اساس این کنوانسیون.

ح) روش‌های مورداستفاده در حمایت از قربانیان و شاهدانی که با مقامات قضایی و مجری قانون همکاری می‌کنند.

ط) آموزش کارکنان در مقررات ملی و بین‌المللی و آموزش زبان.

با حمایت دفتر مبارزه با مواد مخدر و جرائم سازمان ملل متحد، کشورهای عضو می‌توانند باهدف ارتقای اجرای برنامه‌ها و پروژه‌های ملی برای مبارزه با جرائم فناوری اطلاعات و ارتباطات به دیگر کشورهای عضو کمک‌آموزشی تخصصی ارائه کنند.

ماده ۷۷- تبادل اطلاعات

هر کشور عضو باید با مشورت با کارشناسان مربوطه، روند جرائم فناوری اطلاعات و ارتباطات در قلمرو خود و همچنین شرایطی را که در آن چنین جرائمی ارتکاب یافته است، بررسی کند.

کشورهای عضو تا حد امکان، باید انتشار آمار و تحلیل‌های مربوط به جرائم فناوری اطلاعات و ارتباطات را باهدف توسعه، تعاریف، استانداردها و اشتراک‌گذاری بهترین روش‌ها برای پیشگیری و مبارزه با چنین جرائمی، بررسی کنند و آن‌ها را با یکدیگر و از طریق و سازمان‌های منطقه‌ای بین‌المللی به اشتراک بگذارند.

هر کشور عضو باید نظارت بر سیاست‌ها و اقدامات عملی خود را برای مبارزه با جرائم فناوری اطلاعات و ارتباطات و همچنین ارزیابی اثربخشی آن‌ها در نظر بگیرد.

فصل ششم

مکانیسم‌های اجرای کنوانسیون

ماده ۷۸ -کنفرانس کشورهای عضو کنوانسیون

بدین‌وسیله کنفرانسی از کشورهای عضو کنوانسیون به‌منظور بهبود ظرفیت و همکاری بین کشورهای عضو برای دستیابی به اهداف مندرج در این کنوانسیون و ارتقاء و بازنگری اجرای این کنوانسیون تشکیل می‌شود. دبیر کل سازمان ملل متحد کنفرانس کشورهای عضو را حداکثر یک سال پس از لازم‌الاجرا شدن این کنوانسیون دعوت خواهد کرد. پس‌ازآن، جلسات منظم کنفرانس طبق آیین‌نامه‌ای که توسط کنفرانس دولت‌های

عضو تصویب می‌شود، برگزار خواهد شد.

کنفرانس کشورهای عضو آیین‌نامه‌ها و قوانین ناظر بر عملکرد فعالیت‌های مندرج در این ماده، ازجمله قوانین مربوط به پذیرش و مشارکت ناظران و پرداخت هزینه‌های انجام‌شده در انجام آن فعالیت‌ها را تصویب خواهد کرد.

کنفرانس کشورهای عضو در مورد فعالیت‌ها، رویه‌ها و روش‌های کار برای دستیابی به اهداف مندرج در بند ۱ این ماده است، ازجمله:

الف) تسهیل فعالیت‌های کشورهای عضو طبق مواد ۷۶-۷۷ و فصل‌های این کنوانسیون، ازجمله از طریق تشویق کمک‌های داوطلبانه.

ب) تسهیل مبادله اطلاعات بین کشورهای عضو در مورد الگوها و روندهای مربوط به جرائم فناوری اطلاعات و ارتباطات و شیوه‌های موفق برای پیشگیری و مبارزه با آن‌ها، به‌استثنای اطلاعاتی که حاوی داده‌هایی است که طبق قوانین دولت عضو یکی از اسرار دولتی است.

ج) همکاری با سازمان‌ها و سازوکارهای بین‌المللی و منطقه‌ای ذی‌ربط و سازمان‌های غیردولتی بین‌المللی.

د) استفاده مناسب از اطلاعات مربوطه تولیدشده توسط سایر سازوکارهای بین‌المللی و منطقه‌ای برای مبارزه و پیشگیری از جرائم فناوری اطلاعات و ارتباطات، به‌منظور جلوگیری از تکرار کار های غیرضروری.

ه) بررسی دوره‌ای اجرای این کنوانسیون توسط کشورهای عضو آن و ارائه توصیه‌هایی برای بهبود این کنوانسیون و اجرای آن.

ز) شناسایی الزامات کمک فنی کشورهای عضو در رابطه با اجرای این کنوانسیون و توصیه هر اقدامی که ممکن است در این زمینه ضروری باشد.

به‌منظور اجرای بند ۴ این ماده، کنفرانس کشورهای عضو باید از طریق اطلاعات ارائه‌شده توسط کشورهای عضو، آگاهی لازم را در مورد اقدامات انجام‌شده توسط دولت‌های عضو در اجرای این کنوانسیون و مشکلاتی که در اجرای این کنوانسیون با آن مواجه می‌شوند، کسب کند.

هر دولت عضو باید اطلاعاتی را در مورد اقدامات قانونی و اداری و سایر اقدامات و همچنین در مورد برنامه‌ها، طرح‌ها و شیوه‌های خود برای اجرای این کنوانسیون، همان‌طور که توسط کنفرانس کشورهای عضو موردنیاز است، در اختیار کنفرانس کشورهای عضو قرار دهد. کنفرانس کشورهای عضو، مؤثرترین راه‌های دریافت و اقدام بر اساس اطلاعات، ازجمله، اطلاعات دریافتی از دولت‌های عضو و سازمان‌های بین‌المللی ذی‌صلاح را بررسی خواهد کرد. ورودی‌های دریافتی از سازمان‌های بین‌المللی غیردولتی مربوطه که طبق رویه‌هایی که باید توسط کنفرانس دولت‌های عضو در مورد آن تصمیم‌گیری می‌شود، معتبر باشند، نیز ممکن است موردبررسی قرار گیرند.

بر اساس بندهای ۴ تا ۶ این ماده، کنفرانس کشورهای عضو، در صورت لزوم، مکانیسم یا نهاد مناسبی را برای کمک به اجرای مؤثر کنوانسیون ایجاد خواهد کرد.

ماده ۷۹- کمیسیون فنی بین‌المللی

کنفرانس کشورهای عضو، کمیسیون فنی بین‌المللی مبارزه با جرائم فناوری اطلاعات و ارتباطات را برای کمک به کشورها در بازنگری اجرای کنوانسیون ایجاد و تأسیس خواهد کرد.

کمیسیون یک ارگان دائمی متشکل از ۲۳ عضو خواهد بود و بر اساس

اصول نمایندگی مختلط ایجاد خواهد شد. دو سوم اعضا نماینده کنفرانس کشورهای عضو خواهند بود و یک سوم اعضا نماینده هیئت‌های حاکم مانند اتحادیه بین‌المللی مخابرات خواهند بود.

اعضای کمیسیون باید کارشناسانی باشند که تجربه مستقیم قابل‌توجهی در زمینه دیپلماسی، حقوق بین‌الملل و کیفری، فناوری‌های ارتباطی یا تحقیقات مرتبط داشته باشند.

اعضای کمیسیون برای مدت پنج سال خدمت می‌کنند و می‌توانند مجدداً منصوب شوند.

جلسات کمیسیون حداقل سالی یک‌بار تشکیل می‌شود و در مقر اتحادیه بین‌المللی مخابرات در دفتر مبارزه با مواد مخدر و جرائم سازمان ملل متحد یا در زمان و مکانی که توسط کنفرانس کشورهای عضو مشخص یا تائید شده است، تشکیل خواهد شد.

کمیسیون آیین‌نامه داخلی خود را که باید توسط کنفرانس کشورهای عضو تصویب شود، تدوین خواهد کرد.

کمیسیون باید پیشرفت‌های تکنولوژیکی در زمینه ICT را ارزیابی کند.

کمیسیون از طریق کنفرانس کشورهای عضو، نتایج کار خود را به کشورهای عضو و سازمان‌های بین‌المللی ذینفع گزارش خواهد داد.

ماده ۸۰- دبیرخانه

دبیر کل سازمان ملل متحد خدمات دبیرخانه‌ای لازم را به کنفرانس کشورهای عضو کنوانسیون ارائه خواهد کرد.

دبیرخانه باید:

الف) ترتیبات و خدمات لازم را برای جلسات کنفرانس کشورهای عضو

و کمیسیون ارائه دهد.

ب) در صورت درخواست، به کشورهای عضو در ارائه اطلاعات به کنفرانس کشورهای عضو و کمیسیون کمک کند.

ج) اطمینان از هماهنگی لازم با دبیرخانه‌های سایر سازمان‌ها و سازوکارهای بین‌المللی و منطقه‌ای ذی‌ربط.

فصل هفتم مقررات نهایی

ماده ۸۱- اجرای کنوانسیون

هر دولت عضو باید اقدامات لازم ازجمله اقدامات قانونی و اداری را مطابق با اصول اساسی حقوق داخلی خود برای تضمین اجرای تعهدات خود به‌موجب این کنوانسیون انجام دهد.

هر دولت عضو می‌تواند تدابیر سخت‌گیرانه یا شدیدتری نسبت به آنچه در این کنوانسیون برای پیشگیری و مبارزه با جرائم فناوری اطلاعات و ارتباطات پیش‌بینی‌شده است اتخاذ کند.

ماده ۸۲- حل‌وفصل اختلافات

در صورت بروز اختلاف بین دولت‌های عضو در مورد تفسیر یا اجرای این کنوانسیون، آن‌ها باید راه‌حلی را از طریق مذاکره، سازش یا داوری یا از طریق سایر روش‌های مسالمت‌آمیز موردتوافق طرفین اختلاف جستجو کنند.

ماده ۸۳- امضا، تصویب، پذیرش و تصویب

این کنوانسیون برای امضای همه کشورهای عضو سازمان ملل مفتوح خواهد بود.

این کنوانسیون برای امضای سازمان‌های همگرایی اقتصادی منطقه‌ای نیز مفتوح خواهد بود، مشروط بر اینکه حداقل یکی از اعضای آن این کنوانسیون را مطابق بند ۱ این ماده امضا کرده باشد.

این کنوانسیون منوط به تصویب و پذیرش خواهد بود. اسناد تصویب، پذیرش یا تأیید رسمی نزد دبیر کل سازمان ملل متحد سپرده خواهد شد. یک سازمان ادغام اقتصادی منطقه‌ای می‌تواند سند تصویب، پذیرش یا تأیید رسمی خود را درصورتی‌که حداقل یکی از کشورهای عضو آن اقدام مشابهی انجام داده باشد، تودیع کند. در آن سند تصویب، پذیرش یا تأیید رسمی، چنین سازمانی میزان صلاحیت خود را در رابطه با موضوعاتی که توسط این کنوانسیون اداره می‌شود، اعلام خواهد کرد. چنین سازمانی همچنین باید هرگونه تغییر مربوطه در حدود صلاحیت خود را به امانت‌دار اطلاع دهد.

ماده ۸۴- لازم‌الاجرا شدن

این کنوانسیون در نودمین روز پس از تاریخ تودیع سی‌امین سند تصویب، پذیرش یا تائید رسمی لازم‌الاجرا خواهد شد. برای اهداف این بند، هرگونه اسنادی که توسط یک سازمان ادغام اقتصادی منطقه‌ای سپرده‌شده است، به‌عنوان اسنادی که توسط کشورهای عضو آن سازمان سپرده‌شده است، اضافی محسوب نمی‌شود.

برای هر کشور عضو یا سازمان‌های ادغام اقتصادی منطقه‌ای که این کنوانسیون را پس از تودیع سی‌امین سند چنین اقدامی تصویب، پذیرفته یا تأیید می‌کنند، این کنوانسیون در سی روز پس از تاریخ تودیع سند مربوطه توسط آن دولت یا سازمان مربوطه یا در تاریخ لازم الاجرا شدن

ایـن کنوانسـیون طبـق بنـد ۱ این مـاده، هرکدام کـه موخر باشـد، لازم الاجرا می شـود.

ماده ۸۵- اصلاحات

سـه سـال پـس از لازم‌الاجـرا شـدن ایـن کنوانسـیون، یـک دولـت عضـو می‌توانـد اصلاحیـه‌ای را پیشـنهاد کنـد و آن را نـزد دبیـر کل سـازمان ملـل متحـد تسـلیم کنـد، دبیـر کل سـازمان ملـل متعاقبـاً اصلاحیـه پیشـنهادی را بـه کشـورهای عضـو و کنفرانـس سـازمان ملـل متحـد ابـلاغ خواهـد کرد. کشـورهای عضـو کنوانسـیون به‌منظـور بررسـی و تصمیم‌گیری در مـورد این پیشـنهاد. کنفرانـس کشـورهای عضـو تمـام تلاش خـود را برای دسـتیابی به اجمـاع در مـورد هـر اصلاحیـه انجـام خواهـد داد. اگـر تمـام تلاش‌هـا بـرای دسـتیابی بـه اجمـاع بـه پایـان رسـیده باشـد و توافقـی حاصل نشـده باشـد، اصلاحیـه به‌عنـوان آخریـن راه‌حـل، بـرای تصویـب آن بـا اکثریـت دو سـوم کشـورهای عضـو نیـاز خواهد داشـت.

سـازمان‌های ادغـام اقتصـادی منطقـه‌ای، در موضوعاتـی کـه در صلاحیت خـود اسـت، حـق رأی خـود را طبـق ایـن مـاده بـا تعـداد آرا برابـر بـا تعـداد کشـورهای عضـو خود اعمـال خواهنـد کـرد. درصورتی‌که کشـورهای عضو از حـق رأی خـود اسـتفاده کنند، چنین سـازمان‌هایی از حق رأی خود اسـتفاده نخواهنـد کـرد و بالعکس.

اصلاحیـه‌ای کـه مطابـق بنـد ۱ ایـن ماده به تصویب رسـیده اسـت، منوط بـه تصویـب، پذیـرش یـا تأیید توسـط کشـورهای عضـو و سـازمان‌های ادغام اقتصـادی منطقـه‌ای مربوطـه خواهد بود.

اصلاحیـه‌ای کـه مطابـق بنـد ۱ ایـن مـاده اتخاذشـده اسـت، در مورد یک

دولت عضو یا یک سازمان ادغام اقتصادی منطقه‌ای ۹۰ روز پس از تاریخ تودیع سند به دبیر کل سازمان ملل متحد لازم‌الاجرا خواهد شد. تصویب، پذیرش یا تصویب چنین اصلاحیه‌ای با اکثریت دو سوم آرا.

هنگامی‌که اصلاحیه لازم‌الاجرا می‌شود، برای آن دسته از دولت‌های عضو یا سازمان‌های یکپارچه اقتصادی منطقه‌ای که رضایت خود را برای التزام به آن ابراز کرده‌اند، الزام‌آور خواهد بود. سایر کشورهای عضو همچنان به مقررات این کنوانسیون یا هر اصلاحیه قبلی که تصویب، پذیرفته یا تائید کرده‌اند، ملزم خواهند بود.

ماده ۸۶- ملاحظات

هر کشور عضو ممکن است اعلام کند که در هنگام امضا یا تودیع سند تصویب یا الحاق خود، از طریق یک اطلاعیه کتبی خطاب به دبیر کل سازمان ملل متحد، از حق شرط در مورد اعمال این کنوانسیون استفاده خواهد کرد. این مورد برای مواد ۱۵-۱۷، ۱۹-۲۰، ۲۲-۲۶ و ماده ۴۷، بند ۱۱، پذیرفته نخواهد شد.

ماده ۸۷- بازنگری پیوست

هر دولت عضو می‌تواند اصلاحاتی را برای فهرست اسناد حقوقی بین‌المللی مندرج در ضمیمه این کنوانسیون پیشنهاد کند.

دبیرخانه مسئول نظارت بر اسناد حقوقی بین‌المللی جدید تصویب‌شده است که ممکن است بر دامنه کاربرد این کنوانسیون تأثیر بگذارد و اصلاحات پیشنهادی را برای ضمیمه به جلسه بعدی کنفرانس کشورهای عضو ارائه خواهد کرد.

اصلاحات پیشنهادی باید فقط مربوط به اسناد حقوقی بین‌المللی جهانی و منطقه‌ای باشد که لازم‌الاجرا شده و مستقیماً با جنایات بین‌المللی مرتبط است.

دبیر کل پیش‌نویس اصلاحات پیشنهادی مطابق بند ۱ این ماده را به کشورهای عضو ارسال خواهد کرد. اگر یک سوم یا بیشتر از تعداد کل کشورهای عضوی که این کنوانسیون را تصویب کرده‌اند، اعتراض خود را نسبت به لازم‌الاجرا شدن اصلاحیه ظرف شش ماه از تاریخ ارسال پیش‌نویس اصلاحیه، به دبیر کل سازمان ملل اعلام کنند، چنین اصلاحیه‌ای لازم‌الاجرا نخواهد شد.

سازمان‌های ادغام‌شده اقتصادی منطقه‌ای در موضوعاتی که در صلاحیت خود هستند، حق رأی خود را طبق این ماده با تعداد آرا برابر با تعداد کشورهای عضو خود اعمال خواهند کرد. اگر کشورهای عضو از حق رأی خود استفاده کنند، چنین سازمان‌هایی نباید از حق رأی خود استفاده کنند و بالعکس.

اگر ظرف شش ماه از ارسال پیش‌نویس اصلاحیه کمتر از یک سوم کل کشورهای عضوی که این کنوانسیون را تصویب کرده‌اند، اعتراض خود را نسبت به لازم‌الاجرا شدن این اصلاحیه نزد دبیر کل سازمان ملل متحد ارسال کنند. اصلاحیه برای کشورهای عضوی که به آن اعتراض نمی‌کنند ۳۰ روز پس از پایان دوره شش‌ماهه برای تسلیم اعتراض لازم‌الاجرا می‌شود.

کنفرانس کشورهای عضو اصلاحیه‌ای را با اکثریت دو سوم کلیه کشورهای عضوی که این کنوانسیون را تصویب کرده‌اند تصویب خواهد کرد. چنین اصلاحیه‌ای برای کشورهای عضوی که رضایت خود را برای

اعمال این اصلاحیه اعلام کرده‌اند ۳۰ روز پس از تاریخ تصویب اصلاحیه لازم‌الاجرا می‌شود.

دولت عضوی که قبلاً به اصلاحیه اعتراض کرده است، می‌تواند تصمیم خود را تغییر داده و پذیرش آن را به امانت‌گذار اطلاع دهد. در آن صورت، اصلاحیه برای کشور عضو مربوطه ۳۰ روز پس از تاریخی که پذیرش اصلاحیه را به اطلاع دبیر کل سازمان ملل می‌رساند، لازم‌الاجرا خواهد شد.

ماده ۸۸- فسخ

یک دولت عضو می‌تواند این کنوانسیون را با اطلاعیه کتبی به دبیر کل سازمان ملل متحد فسخ کند. این فسخ شش ماه پس از تاریخ دریافت اطلاعیه توسط دبیر کل نافذ خواهد شد.

یک سازمان ادغام‌شده اقتصادی منطقه‌ای زمانی که تمام کشورهای شرکت‌کننده در چنین سازمانی این کنوانسیون را فسخ کرده باشند عضو این کنوانسیون نخواهد بود.

ماده ۸۹- امین و زبان‌ها

دبیر کل سازمان ملل متحد به‌عنوان امین این کنوانسیون تعیین می‌شود.

اصل این کنوانسیون که متون عربی، چینی، انگلیسی، فرانسوی، روسی و اسپانیایی آن به یک اندازه معتبر است، نزد دبیر کل سازمان ملل متحد سپرده خواهد شد.

منابع

[1] A/75/L.87/Rev.1, Distr.: Limited 24 May 2021.

[2] and Communications Technologies for Criminal Purposes, Draft 29 June 2021

[3] Article 21- Extremism-related offences, United Nations Convention on Countering the Use of Information

[4] https://directionsblog.eu/russias-vision-for-a-cybercrime-treaty/

[5] https://foreignpolicy.com/2022/02/11/un-cybercrime-treaty-russia-hacking/

[6] https://www.eff.org/deeplinks/2022/02/un-committee-begin-negotiating-new-cybercrime-treaty-amid-disagreement-among

[7] https://www.firstpost.com/tech/news-analysis/explained-russias-proposal-to-the-un-for-expanding-list-of-designated-cybercrimes-9843901.html

[8] https://www.un.org/press/en/2021/ga12328.doc.htm

[9] Internet users in the world 2021 | Statista. (2022). Retrieved 3 April 2022, from https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=How%20many%20people%20use%20the,the%20internet%20via%20mobile%20devices.

[10] Katitza Rodriguez, a. (2022). Nearly 130 Public Interest Organizations and Experts Urge the United Nations to Include Human Rights Safeguards in Proposed UN Cybercrime Treaty. Retrieved 2 April 2022, from https://www.eff.org/deeplinks/2022/01/nearly-130-public-interest-organizations-and-experts-urge-united-nations-include

[11] The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention

[12] U.S. whistleblower Chelsea Manning challenging secrecy laws barring her from Canada | National Post. (2022). Retrieved 2 April 2022, from https://nationalpost.com/news/canada/u-s-whistleblower-chelsea-manning-challenging-secrecy-laws-barring-her-from-canada

[13] United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, first draft Convention, Draft 29 June 2021, available in: https://ccdcoe.org/library

[14] Walker, S. (2022). The Quixotic Quest to Tackle Global Cybercrime. Retrieved 2 April 2022, from https://foreignpolicy.com/2022/02/11/un-cybercrime-treaty-russia-hacking/

[۱۵] بـذار، وحیـد، محـدودۀ اعمـال مـاده ۹ قانـون مدنـی نسـبت بـه تعهـدات بین‌المللی دولـت ایران، فصلنامـه قضـاوت، دوره ۱۹، شـماره ۹۷، خـرداد ۱۳۹۸، صفحـه ۴۹-۶۷

[۱۶] بـوزان، بـاری، مـردم، دولت‌هـا و هـراس، پژوهشـکده مطالعات راهبـردی، چاپ ششـم، تهران، ص ۳۹.

csri.majazi.ir

حوزه فضای مجازی به اندازه انقلاب اسلامی اهمیت دارد. این فضا مثل یک رودخانه پر از آب و خروشان است که می آید و دائماً هم بر آب آن افزوده و خروشان تر می شود. اگر ما بر این رودخانه تدبیر کنیم و برنامه داشته باشیم، زه‌کشی کنیم و هدایت کنیم این رودخانه را تا به سد بریزد، می‌شود فرصت. اگر رهایش کنیم و برنامه‌ای برای آن نداشته باشیم می‌شود یک تهدید.

csri.majazi.ir