رویکرد حقوق بین‌الملل در قانون‌گذاری در فضای سایبر

مسعود راعی[۱]، علیرضا آرش پور[۱]، مهدیه شهاب[۲]

[۱]عضو هیئت علمی گروه حقوق بین‌الملل، دانشگاه آزاد اسلامی واحد نجف‌آباد، اصفهان، ایران
masoudraei@yahoo.com,rezaarashpour@gmail.com
[۲]دانشجوی دکتری حقوق بین‌الملل، دانشگاه آزاد اسلامی واحد نجف‌آباد، اصفهان، ایران
mahdieh.shahab@gmail.com

چکیده

توجه بین‌المللی به امنیت سایبری طی سال‌های اخیر به طور چشمگیری افزایش‌یافته است؛ زیرا فضای مجازی به زیرساخت مرکزی جهان تبدیل شده است. این امر امکان توسعه و رشد را ایجاد اما در عین حال فرصت‌های گسترده‌ای را برای منازعات و ارتکاب جرایم فراهم نموده است. کشورها اهمیت فضای سایبر را درک کرده‌اند و همراه با آن، نیاز به همکاری جهانی برای ایجاد ثبات و امنیت بیشتر دارند. سازمان ملل متحد نقشی اساسی در این میان ایفا می‌کند، زیرا اغلب دولت‌ها مسئول اقدامات مخرب و بی‌ثبات‌کننده هستند. این را می‌توان با شمارش ساده حوادث مهم تعیین کرد. این امر به سازمان ملل نقش اساسی در رسیدگی به مسئله اعتماد و امنیت می‌بخشد و اهمیت چارچوب سازمان ملل برای رفتار مسئولانه دولت‌ها در فضای سایبر که در سال ۲۰۱۵ ایجادشده را برجسته می‌کند. جامعه اطلاعات، در حال تبدیل به یک جامعه جهانی بوده، رشد تجارت الکترونیک، باعث توسعه بازارهای جدید صنعتی به‌صورت یکپارچه و جهانی شده است. اما جامعه اطلاعاتی، روی چهارچوب بسیار آسیب‌پذیر (اینترنت) ساخته شده و اینترنت در معرض خطر حملات است. اکنون جامعه مدرن ما از بسیاری جنبه‌ها به فناوری اطلاعات به‌صورت مستقیم یا غیرمستقیم وابسته است.

کلمات کلیدی: امنیت، سایبری، فضای مجازی، توسعه، جرایم، همکاری جهانی، سازمان ملل متحد.

۱ مقدمه

هسته اصلی چارچوب مورد توافق هنجارهای توصیف شده در گزارش ۲۰۱۵ گروه کارشناسان دولتی سازمان ملل متحد (GGE) است. هنجارها تفاهم دولت‌ها بر سر رویه‌هایی است که رفتار مناسب را شناسایی و هدایت می‌کنند. هنجارها تعهدات بین‌المللی را که کشورها پذیرفته‌اند را تعریف می‌کنند. این چارچوب توسط گروه کارشناسی دولتی ایجاد شده است که توسط کمیته اول سازمان ملل متحد تأسیس شده تا تحولات حوزه اطلاعات و مخابرات در زمینه امنیت بین‌المللی را بررسی کند. آخرین مورد از این مجموعه تلاش‌ها تصویب

دو قطعنامه در سال ۲۰۱۸ است و اینکه یک کارگروه کارشناسی جدید و برای اولین بار یک کارگروه بدون محدودیت زمانی ایجاد کرده است (OEWG).

گروه کارشناسان دولتی در توسعه اطلاعات و ارتباطات از راه دور در بستر امنیت بین‌المللی (GGE) تحت نظر کمیته نخست شورای امنیت (کمیته خلع سلاح و امنیت بین‌المللی) تشکیل گردید. این گروه گزارش نخست خود را به تاریخ ۲۴ ژوئن ۲۰۱۳ منتشر نمود. گزارش بر این امر تأکید دارد که امنیت سایبری می‌بایست دوشادوش احترام به حقوق بشر و آزادی‌های بنیادین مندرج در اعلامیه جهانی حقوق بشر و سایر اسناد بین‌المللی توسعه یابد. گزارش مذکور اشعار می‌دارد که دولت‌ها می‌بایست بر میزان همکاری‌ها علیه جرایم سایبری و تروریستی در بستر فناوری اطلاعات را افزایش دهند.

گروه کارشناسان دولتی بر موضوع کاربرد فناوری اطلاعات در مخاصمات و چگونگی اعمال حقوق بین‌الملل بر استفاده از این فناوری توسط دولت‌ها متمرکز شد. گزارش دوم این گروه در ژوییه ۲۰۱۵ منتشر شد. این مباحث در سازمان ملل متحد درک مشترکی در مورد چگونگی رفتار دولت‌ها در فضای مجازی و چگونگی انطباق آن با تعهدات بین‌المللی موجود یک کشور ایجادکرده است. این هنجارها چارچوبی برای رفتار مسئولانه دولت ایجاد می‌کنند. در این گزارش عنوان شد که دولت‌ها می‌بایست در زمینه ممانعت از اعمال خرابکارانه همکاری نموده و نباید آگاهانه اجازه استفاده از سرزمین خود برای اعمال خلاف بین‌المللی با استفاده از فناوری اطلاعات را بدهند؛ تبادل اطلاعات و معاضدت در جهت تعقیب تروریست‌ها و کاربرد مجرمانه فناوری اطلاعات می‌بایست در میان دولت‌ها گسترش یافته و در عین حال احترام کامل به حقوق بشر از جمله حق بر حریم شخصی و آزادی بیان تضمین گردد. هرچند دولت‌ها می‌بایست اقدامات مناسب در راستای حفاظت از زیرساخت‌های حیاتی خود در برابر تهدیدهای فناوری اطلاعات را اتخاذ نمایند، اما نباید رفتاری را در پیش گرفته یا آگاهانه از اقدامات فناوارانه‌ای که عامداً موجب ورود خسارت یا سایر اشکال صدمه به استفاده و کاربرد زیرساخت‌های حیاتی سایر کشورها گردد، حمایت کنند. گروه کارشناسان دولتی پیشنهاد توسل به اقدامات اعتمادساز برای گسترش همکاری‌های بین‌المللی و کاهش خطر تقابل را ارائه نموده است. بخش خصوصی، جامعه دانشگاهی و جامعه می‌توانند نقش مهمی در حمایت از مسئولیت اولیه دولت‌ها در حفظ یک فناوری اطلاعات امن را ایفا نمایند. تهیه‌کنندگان گزارش بر این باور هستند که توانمندسازی اساس همکاری بین‌المللی بوده و منجر به افزایش توان دولت‌ها برای همکاری و اقدام جمعی می‌گردد.

توانمندسازی را می‌توان ستون سوم چارچوب رفتار دولت مسئول دانست. درسال ۲۰۱۰، نماینده آفریقای جنوبی با اشاره به اینکه از جانب کشورهای درحال توسعه سخن می‌گوید، تأکید داشت که توانمندسازی می‌بایست بخشی از هر توافق آتی باشد. از آن پس تاکنون، توانمندسازی سایبری از توسعه طیف وسیعی از ابتکارات، از جمله اجلاس جهانی کارشناسان سایبری، بهره‌مند شده است. توانمندسازی، اقدامات اعتمادساز و هنجارها بسته یکپارچه‌ای را ایجاد می‌کنند که رفتار دولت مسئول را تعریف و شکل می‌دهد. توانایی یک کشور در اجرای هنجارها و اقدامات اعتمادساز به ظرفیت سایبری ملی آن متکی است. توانمندسازی (اعم از فنی و سیاسی) توانایی رعایت هنجارها را تقویت می‌کند؛ در حالیکه اعتمادسازی شواهدی مبنی بر رعایت هنجارها را فراهم می‌آورد. توانمندسازی زمینه را برای حمایت سیاسی مورد نیاز اجماع در مورد چگونگی اجرای هنجارها و اصول رفتار مسئولانه دولت‌ها آماده می‌کند و یکی از راه‌های

اطمینان از انعکاس منافع همه کشورها در بحث امنیت سایبری با پیوند دادن آن به اهداف توسعه پایداراست. گزارش ۲۰۱۵ کارگروه کارشناسان دولتی تأکید می‌کند که کشورها باید «به کشورهای در حال توسعه برای بهبود امنیت در استفاده از فناوری اطلاعات کمک و آموزش دهند». چنان‌که عنوان شده، این امر «می‌تواند از توسعه سیاست‌ها و قوانین مربوط به امنیت سایبری گرفته تا ظرفیت اجرای قانون و کمپین‌های عمومی آگاهی از امنیت سایبری» باشد.

صورت آن‌ها هرچه باشد، روایت غالب پیرامون ظرفیت‌سازی این است که علاوه بر اهداف توسعه، آن‌ها همکاری بین‌المللی و اشتراک اطلاعات را ارتقا می‌بخشند و به عنوان مکانیزمی برای ایجاد یک اجماع جهانی در مورد امنیت سایبری عمل می‌کنند.

۱.۱ مفهوم و کارکردهای فضای مجازی

فضای مجازی محصول پیشرفت‌های جدیدی است که مجموعه به هم پیوسته‌ای از انسان‌ها را از طریق ابزار ارتباط جمعی، صرف نظر از جغرافیای فیزیکی و فرهنگی، گرد هم آورده و تعامل‌های بین فردی یا گروهی را از طریق تبادل اطلاعات دیجیتالی تسهیل کرده است. لکن همزمان با رشد و توسعه این گستره، شکل جدیدی از جرایم نیز پدیدار شده‌اند. ماهیت این جرایم، جدید و با قالب‌های سنّتی جرم متفاوت است، در ضمن بزهکار می‌تواند سن، جنس و هویت خود را پنهان کرده و در زمان و مکان نامشخص با سرعت و سهولت جرم را مرتکب شود. وجوه فنی این پدیده نیز شامل دو جنبه سخت‌افزاری و نرم‌افزاری از قبیل انواع رایانه و ملزومات آن، ماهواره، انواع تلفن همراه،... و انواع شبکه‌ها و رسانه‌های اجتماعی مجازی، نرم‌افزارهای اینترنتی است که با هدف سرعت بخشی به ارتباطات انسانی و تبادل اطلاعات مورد نیاز و ایجاد رفاه و آسایش روزمره زندگی و مفید کردن روند زندگی مورد استفاده هستند. رسانه‌های اجتماعی مجازی، از قبیل فیس بوک، یوتیوب، اینستاگرام، تلگرام، وایبر وجوه مشترکی دارند که مخاطب محور بودن و تولید محتوا در این شبکه‌ها، توسط کاربران از جمله آن است. پدیده فناوری اطلاعات مانند سایر پدیده‌های توسعه‌گری، بلافاصله بعد از ظهور، کارکردهای آشکار و پنهانی را از خود بر جای گذاشت.

فضای مجازی، تبادل اطلاعات و محدودیت‌های ارتباطی را از بین برد و موجب شد تا فعالیت‌های گوناگونی از جمله اقتصاد مجازی، تجارت مجازی، آموزش‌های مجازی و سایر خدمات در این فضا گسترش یابد و تبادلات جدیدی با ماهیت جدید شکل بگیرد. درنتیجه، امروزه ما بر اساس جامعه اطلاعاتی، با سرعت وصف‌ناپذیری در حال توسعه هستیم. از طرفی، کارکردهای پنهان فضای مجازی به‌طور غیرمستقیم، اثرات منفی و زیانباری را به وجود آورده‌اند. برخی از این کارکردهای منفی پنهان از جمله بزهکاری‌های مجازی مانند پول‌شویی، هرزه‌نگاری، قوادی، کلاهبرداری، جعل و ... هستند. درحقیقت کاربران مجازی هستند که با طریقه و روش استفاده از این پدیده، قادرند تا تعریف مثبت یا منفی از فضای سایبری ارائه دهند.

۲.۱ تشریح مفهوم امنیت

امنیت شامل سه عنصر پایه‌ای است: ۱-محرمانگی؛ ۲-یکپارچگی؛ ۳-در دسترس بودن.

نقض محرمانگی: به این معنا که اگر داده‌هایی که در فضای سایبری در حال انتقال هستند، توسط مهاجمین خوانده شوند و محرمانه بودن آن نقض شود.

نقض یکپارچگی: اگر در حین انتقال داده‌ها در فضای سایبری (به عنوان مثال در یک شبکه) اطلاعات توسط مهاجمین دستکاری شده و تغییر داده شوند (به آن چیزی اضافه یا از آن کم شود)

نقض در دسترس بودن: این نوع حملات با هدف خارج کردن منبع اطلاعاتی از سرویس به گونه‌ای که دیگر آن منبع قادر به ارائه سرویس به دیگران نبوده و نتواند تبادل اطلاعات درستی با کاربرانش داشته باشد، انجام می‌شود.

برقراری امنیت در فضای سایبری، به علت ماهیت فضای سایبری کار بسیار دشواری است. از فناوری سایبری بی‌تردید می‌توان همانند ابزارهای جنگ متعارف، برای حمله به تشکیلات دولتی، نهادهای مالی، زیرساخت‌های انرژی، حمل و نقل ملی و روحیه عمومی استفاده کرد؛ فلذا ناامنی در فضای سایبری، صرفاً شامل ناامنی در سیستم‌های اطلاعاتی نیست، بلکه شامل تمام زیرساخت‌هایی می‌شود که به نحوی با فناوری اطلاعات در ارتباطند. در حمله سایبری تحت عنوان ویروس استاکس نت در سال ۲۰۱۰ به تأسیسات اتمی جمهوری اسلامی ایران شد؛ یک بمب منطقی توانست در سیستم کنترل سانتریفیوژهای ایران نفوذ کند، با این هدف که دور سانتریفیوژهارا آن‌قدر زیاد کند تا آن‌ها یا از کار بیفتند و یا منفجر شوند. ایران هیچ‌گاه اطلاعات دقیقی از میزان خسارات وارده توسط این ویروس به تأسیساتش ارائه نداد.

مهم‌ترین مزیت و رسالت شبکه‌های رایانه‌ای، اشتراک منابع سخت‌افزاری و نرم‌افزاری و دست‌یابی سریع و آسان به اطلاعات است. کنترل دست‌یابی و نحوه استفاده از منابعی که به اشتراک گذاشته شده‌اند، از مهم‌ترین اهداف یک نظام امنیتی در شبکه است. با گسترش شبکه‌های رایانه‌ای (خصوصاً اینترنت)، نگرش نسبت به امنیت اطلاعات و سایر منابع به اشتراک گذاشته شده، وارد مرحله جدیدی گردیده است. در این راستا لازم است که هر سازمان برای حفاظت از اطلاعات ارزشمند خود، به یک راهبرد خاص پایبند باشد و براساس آن، نظام امنیتی ر ا اجرا نماید. نبود نظام مناسب امنیتی، بعضاً پیامدهای منفی و دور از انتظاری را به دنبال دارد. توفیق در ایمن‌سازی اطلاعات، منوط به حفاظت از اطلاعات و نظام‌های اطلاعاتی در مقابل حملات است؛ بدین منظور از سرویس‌های امنیتی متعددی استفاده می‌گردد. سرویس‌های انتخابی باید پتانسیل لازم در خصوص ایجاد یك نظام حفاظتی مناسب، تشخیص به موقع حملات و واکنش سریع را داشته باشند. بنابراین می‌توان محور راهبردی انتخاب شده را بر سه مؤلفه حفاظت، تشخیص و واکنش استوار نمود. حفاظت مطمئن، تشخیص به موقع و واکنش مناسب، از جمله مواردی هستند که باید همواره در ایجاد یک نظام امنیتی رعایت شود.

امنیت مجازی شاید به‌شکل قابل توجه آن، موضوع حیاتی برای کشورها باشد. چرا که شرط لازم برای تهدیدپذیری از دنیای مجازی، استفاده گسترده و اتصال به شبکه‌های الکترونیکی اطلاعات است و شرط کافی، دیجیتالی شدن تمامی سیستم‌ها و زیرساخت‌های اقتصادی، اجتماعی و سیاسی یك جامعه می‌باشد. در عین حال نباید فراموش کرد که گسترش ارتباطات و انقلاب تکنولوژیکی، بسیاری از مسائل امنیتی را

جهانی ساخته و شمال و جنوب در این زمینه دارای مسائل مشترکی هستند. از طرفی دیگر تهدید، مفهومی نسبی و ذهنی است و درک آن به مؤلفه‌های گوناگونی بستگی دارد. تهدید در مفهوم گذشته دارای ویژگی‌های مشخصی بوده که می‌توان آن‌ها را این گونه برشمرد:

۱. عمدتاً با منشأ خارجی تصور می‌شد.

۲. مبتنی بر قدرت نظامی بود.

۳. متکی بر حضور فیزیکی دشمن بود.

۴. آگاهی از تهدیدات، گسترده نبود.

۵. دامنه تهدیدات محدود بود.

۶. تهدیدات به‌راحتی قابل تشخیص بود.

۷. در اکثر تهدیدات، دولت‌ها نقش مؤثری را ایفا می‌کردند.

اما در جهان امروز و در عصر جهانی شدن، به واسطه تغییرات تکنولوژی، مفاهیم نیز دستخوش تغییر و تحول شده‌اند. در شرایط نوین ویژگی تهدیدات به شرح زیر است:

۱. اکثر تهدیدات دولت محور نیستند (این قبیل مخاطرات از عوامل و بازیگران ملی یا فراملی نشأت می‌گیرد).

۲. این چالش‌ها، فضای جغرافیایی خاصی ندارند و تهدیدات متنوع، چندسویه و چندجهتی است و در سه سطح جهانی، منطقه‌ای و محلی قابل بررسی است

۳. این تهدیدات را نمی‌توان تنها با اتکا به سیاست‌های دفاعی سنتی مدیریت کرد و مدیریت مؤثر مستلزم طیفی از رهیافت‌های غیرنظامی است.

مسلماً ترسیم یک گفتمان امنیتی خارج از مدار و حریم مفاهیمی چون قدرت، منافع، اهداف، مصالح، ارزش‌ها، تهدیدات و ... دور از دسترس است. اما در شرایطی که تمامی این مفاهیم خود بر ماهیت و شکلی دگرگون شونده و متلون اصرار می‌ورزند و بر مصداق‌های گوناگونی دلالت دارند این امر به‌راحتی امکان‌پذیر نیست.

۲ نظریه حاکمیت در فضای سایبر

از بدو ورود فضای سایبر به زندگی بشریت، مقوله قانونگذاری و شناخت قانونگذار صالح در این فضا، چالش جدی بوده است. شیوه قانونگذاری در فضای سایبر، مبتنی بر دو نوع نگرش متفاوت به حاکمیت در فضای سایبر است. نگرش نخست، مبتنی بر انحصار دولت‌ها در عرصه قانونگذاری فضای سایبر است و نگرش دوم که ملهم از دکترین میراث مشترک بشریت است، مخالف ورود انحصاری دولت‌ها به این عرصه است. هر یک از این دو رویکرد، موجد روش‌های قانونگذاری مختلفی در فضای سایبر است. روش‌های قانونگذاری ملی، بین‌المللی و خودانتظامی در زمره روش‌های قانونگذاری در فضای سایبر به شمار می‌آیند. اگرچه توسل به هر یک از روش‌های قانونگذاری با اشکالاتی در عرصه اجرا روبه‌روست، در این میان می‌توان رویکردی بینابین و مختلط را برگزید تا ضمن رفع نواقص دیگر روش‌ها، زمینه را برای نیل به تفاهم میان کشورها و گروه‌های فعال در زمینه فضای سایبر هموار سازد.

۱.۲ حاکمیت انحصاری بر فضای سایبر

این دیدگاه، حاصل پذیرش مفهوم وستفالیایی حاکمیت در فضای سایبر است.

از آنجا که اینترنت، مرزگذر است، اعمال حاکمیت از سوی همه دولت‌ها می‌تواند مشکلات حقوقی متعددی برای کشورها و افراد ایجاد کند؛ ضمن آنکه فضای سایبر برخلاف دریای آزاد در گذشته، میان چند دولت تقسیم نشده است. هرچند سخت‌افزارهای رایانه‌ای از جمله سرورهای اینترنتی از نظر فیزیکی تحت حاکمیت صلاحیت‌های ملی قرار دارد و همین امر، مستمسک برخی دولت‌ها برای توجیه کنترل سختگیرانهٔ اینترنت شده است، اطلاعات موجود در این سخت‌افزارها و سامانه‌های عامل آن‌ها درحقیقت اینگونه نیست. از آنجا که اینترنت، فاقد حاکمیت مرکزی است، طبق این نظریه، میان حاکمیت‌ها تعارض شکل خواهد گرفت.

۳ روش‌های قانونگذاری در فضای سایبر

قانونگذاری ملی و بین‌المللی از اقسام روش‌های قانونگذاری در فضای سایبر به شمار می‌آیند. روش قانونگذاری ملی، حاکی از رویکرد حاکمیت انحصاری دولت‌ها بر فضای سایبر، و روش بین‌المللی، متأثر از نگرش مبتنی بر دکترین تعمیم نظریه میراث مشترک بشریت بر فضای سایبر است.

۱.۳ روش قانونگذاری ملی

در این روش، نهادهای قانونگذاری ملی نسبت به قانونگذاری و جرم انگاری در فضای سایبر اقدام می‌کنند. باید توجه داشت که در این روش اولاً، نمی‌توان از جرم انگاری تمام جرایم در فضای سایبر، اطمینان خاطر داشت و ثانیاً، این روش می‌تواند موجب تعارض قوانین در فضای سایبر شده و اصل قانونی بودن جرم و مجازات و اصل منع مجازات مضاعف را تحت تأثیر قرار دهد. از آنجا که این روش، مستعد تصویب قوانین فراسرزمینی و انحصاری‌سازی فضای سایبر است، می‌تواند منجر به تصویب قوانین انسدادی توسط کشورها برای جلوگیری

از اعمال صلاحیت کشورهای خارجی شود. از سوی دیگر، عملکرد برخی کشورها ازجمله چین در قانونگذاری حداکثری، منجر به خود سانسوری در فضای سایبر شده است.

۴ روش قانونگذاری بین‌المللی

روش قانونگذاری بین‌المللی با توجه به یکپارچگی اینترنت و مشکلات ناشی از قانونگذاری ملی مطرح شد. این شیوه در بهترین شکل با انعقاد معاهدات بین‌المللی محقق می‌شود. به طور مثال، پروتکل الحاقی به کنوانسیون حقوق کودک، در خصوص فروش، فحشا و هرزه‌نگاری کودکان به صراحت بر نقش اینترنت در توزیع هرزه‌نگاری کودکان اشاره دارد و از کشورها می‌خواهد اینگونه افعال را جرم‌انگاری کنند. همچنین یکی از مهم‌ترین کنوانسیون‌های مربوط به فضای سایبر، کنوانسیون بوداپست در خصوص جرایم سایبری است. با این حال، این کنوانسیون نمی‌تواند به عنوان معاهده‌ای جامع تلقی شود، چون اولاً، تمام جرایم سایبری را در بر نمی‌گیرد و ثانیاً، این کنوانسیون صرفاً برای کشورهای اروپایی لازم‌الاجراست. در هر صورت، معاهدات منطقه‌ای و دوجانبه، پاسخگوی حل مشکلات نبوده و معاهده‌ای اینترنتی در برخی از قواعد آمره، نظیر ممنوعیت دزدی دریایی و نسل‌زدایی نیز در فضای سایبر در سطح بین‌المللی مورد نیاز است.

سازمان‌های بین‌المللی نیز در فرایند بین‌المللی‌سازی قانونگذاری در فضای سایبر، نقش قابل توجهی داشته‌اند. پیش از همه، آنسیترال با تصویب قانون نمونه آنسیترال در خصوص تجارت الکترونیکی در سال 1916 نقش چشمگیری در هماهنگ‌سازی قوانین ملی کشورها درباره مسائل مربوط به تجارت الکترونیک داشته است. گروه هشت نیز در اولین اقدام خود در سال 1917 کمیته فرعی جرایم رایانه‌ای را برای مقابله با جرایم سایبری تأسیس و متعاقباً یک برنامه اصلی را در این رابطه تصویب کرد. مجمع عمومی سازمان ملل متحد در سال‌های 2011 و 2019 برای تنظیم امنیت اطلاعاتی و سایبری اقداماتی انجام داد.

پس از تلاش اتحادیه اروپا برای تصویب کنوانسیون جرایم سایبری، اتحادیه عرب به پیشنهاد ایالات متحده عربی یک مدل قانونی در خصوص همسان‌سازی قوانین ملی کشورهای عربی را در سال 2019 پذیرفت. شورای همکاری خلیج فارس نیز در کنفرانس 2017 به دولت‌ها توصیه کرد که رویکردی متحدانه را در خصوص مواجهه با موضوعات سایبری اتخاذ کنند. سازمان کشورهای امریکایی، سازمان همکاری و توسعه اقتصادی، سازمان همکاری و اقتصادی آسیا ـ اقیانوسیه و سازمان کشورهای مشترک‌المنافع نیز در یکسان‌سازی قواعد بین‌المللی تلاش‌هایی داشته‌اند. اما شاید مهم‌ترین تلاش، اجلاس جهانی جامعه اطلاعات در سال 2019 باشد که در آن تشکیل سازمان بین‌المللی اینترنت و انعقاد معاهده‌ای اینترنتی پیشنهاد شد.

اتحادیه بین‌المللی مخابرات در سال 2017 آژانس جهانی جرائم سایبری و متعاقباً گروه کارشناسان ارشد را با هدف ارائه پیشنهادهایی برای جرم‌انگاری سایبری بنیانگذاری کرد. بالاخره سند اصلاحی مقررات اتحادیه بین‌المللی مخابرات با اعطای وجهه حقوقی بین‌المللی به قانونگذاری در فضای اینترنت با رأی اکثریت کشورها به تصویب رسید. باید توجه داشت که فناوری‌محور بودن فضای سایبر موجب می‌شود که سهم کشورهای مختلف در تنظیم نظام حقوقی حاکم بر فضای سایبر متفاوت باشد. به همین دلیل، یکی از مدل‌های پیشنهادی در قانونگذاری بین‌المللی در فضای سایبر، تقسیم وظایف و امتیازات بر مبنای مؤلفه‌هایی مانند قدرت، ثروت

و تخصص است.

۵ نتیجه‌گیری

دیدگاه حاکمیت انحصاری دولت بر فضای سایبر که متأثر از پذیرش مفهوم وستفالیایی حاکمیت در این فضاست، رفته رفته با پیدایش مفاهیم سیاسی و حقوقی نظیر جهان شمولی، مسئولیت بین‌المللی، اصل عدم مداخله و قواعد حقوق بشری با چالش مواجه شد. متعاقباً رویکرد تعمیم نظریه میراث مشترک بشریت با هدف خارج کردن این فضا از انحصار دولت‌ها مطرح شد. علیرغم این راستا در سطح بین‌المللی تنظیم نشده است. دولت‌ها در حیطه قانونگذاری سایبری، یک یا چند نوع از اقسام روش‌های قانونگذاری را به کار بسته‌اند. اتخاذ منحصرانه هر یک از روش‌ها، مزایا و معایب خاص خود را دارد. امتیازات دیدگاه اخیر، اعمال آن در فضای سایبر با این اشکال همراه است که تا کنون معاهده‌ای انتظام بخش در این راستا در سطح بین‌المللی تنظیم نشده است. دولت‌ها در حیطه قانونگذاری سایبری، یک یا چند نوع از اقسام روش‌های قانونگذاری را به کار بسته‌اند. اتخاذ منحصرانه هر یک از روش‌ها، مزایا و معایب خاص خود را دارد. علی رغم اینکه قابلیت اعمال حقوق بین‌الملل و به طور خاص منشور ملل متحد و اصول و قواعد دیگر حقوق بین‌الملل در مورد فضای سایبری امری پذیرفته شده است، این سؤال به قوت خود باقی است که قواعد و اصول مرتبط چگونه در این زمینه اعمال می‌شوند؟

به‌امید یافتن پاسخ این سؤال، انجمن آکسفورد برای اخلاق، حقوق و مخاصمه مسلحانه، کارشناسان مختلف را در ابتکار «تلاش آکسفورد در مورد حمایت‌های حقوق بین‌الملل در فضای سایبری» گرد هم آورد که برون‌داد این تلاش‌ها، چند بیانیه است که به موضوعات خاص مطرح در حوزه امنیت سایبری پرداخته‌اند. به عبارت دیگر، هسته اصلی این ابتکار یک تلاش مشترک بین کارشناسان حقوقی بین‌المللی از سراسر جهان است که با هدف شناسایی و شفاف‌سازی قواعد حقوق بین‌الملل قابل اجرا در عملیات‌سایبری در زمینه‌های مختلف انجام می‌شود. تا به امروز، این فرآیند پنج بیانیه مختلف را ارائه کرده است: ۱-بیانیه حمایت‌های حقوق بین‌الملل در برابر عملیات سایبری که بخش مراقبت‌های درمانی را هدف قرار می‌دهند؛ ۲- حفاظت از تحقیقات واکسن؛ ۳-حمایت‌های حقوق بین‌الملل در برابر مداخلات انتخاباتی خارجی از طریق ابزارهای دیجیتال؛ ۴- مقررات عملیات و فعالیت‌های اطلاعاتی؛ و ۵- مقررات عملیات‌های باج‌افزار.

در تمامی این بیانیه‌ها بر اعمال حقوق بین‌الملل در این موضوعات تأکید شده است و بیان شده که حقوق بین‌الملل،دولت‌ها را از عملیات سایبری موضو ع هر بیانیه منع می‌کند. به عنوان مثال در بیانیه مربوط به بخش مراقبت‌های درمانی، به صراحت بیان شده است که حقوق بشر دولت‌ها را ملزم می‌کند که حق حیات و حق سلامت همه افراد در قلمروی تحت صلاحیت خود را از طریق اتخاذ تدابیری برای جلوگیری از مداخله اشخاص ثالث در این حقوق با ابزار سایبری تضمین کنند. همچنین، تعهد دولت‌ها را در صورت آ گاهی و اطلاع از یک عملیات سایبری در قلمرو یا زیرساخت‌های تحت صلاحیت یا کنترل آن‌ها، و انجام تمام اقدامات ممکن برای جلوگیری از این اقدامات شناسایی می‌کند.

در بیانیه مربوط به باج‌افزارها نیز، کشورها باید از انجام، هدایت، صدور مجوز یا کمک به عملیات باج‌افزارها

که اصول حاکمیت یا عدم مداخله در امور داخلی یا خارجی یک دولت را نقض می‌کند یا به منزله تهدید یا توسل به زور در معنای منشور است خودداری کنند. به ویژه دولت‌ها باید از عملیات باج‌افزارها با هدفی که منجر به نقض حقوق بشر افراد در حوزه صلاحیت آنهاست جلوگیری کنند و نباید به دولت‌ها یا بازیگران غیردولتی اجازه انجام چنین عملیات‌هایی را در قلمرو و یا با استفاده از زیرساخت‌های خود بدهند.

با وجود تلاش‌ها و اقدامات برشمرده شده توسط کشورهای عضو سازمان ملل و حقوقدانان بین‌المللی در نهایت، دست‌یابی به راه حل اصلی در تنظیم مقررات سایبری دشوار به نظر می‌رسد. از سویی، دولت‌های غربی و ذی‌نفعان عرصه سایبری، بر این نظرند که حقوق بین‌الملل موجود برای تنظیم رفتار دولت‌ها در فضای سایبر کافی است و تنها باید به چگونگی عملیاتی کردن این قواعد پرداخت. اما در مقابل، برخی کشورها مانند ایران، روسیه و کوبا معتقدند در حقوق موجود شکاف‌ها و ناکارآمدی‌هایی وجود دارد که نیازمند تنظیم قواعد جدید در این زمینه از طریق تدوین یک معاهده جدید و یا تحول حقوق بین‌الملل عرفی است. حتی در رویکرد معتقدان به ضرورت قواعد جدید نیز همسویی وجود ندارد. برخی دولت‌ها بر معاهده‌ای متمرکز هستند که از دولت‌ها در برابر مردم محافظت می‌کند و برخی دیگر به دنبال معاهده‌ای هستند که از مردم در برابر دولت‌ها محافظت کند.

از آنجا که مانند هر حوزه دیگر، حقوق بین‌الملل در زمینه فضای سایبری همواره در حال تحول است و روز به روز بر پیچیدگی آن افزوده می‌شود، انتظار می‌رود تا زمان رسیدن به راه حلی جامع و مورد توافق، تلاش‌های مشترک دولت‌ها، سازمان‌های بین‌المللی، جامعه مدنی و دانشگاهیان در این زمینه ادامه یابد. در این راستا، به ویژه دولت‌ها باید برای تقویت اجرای هنجارها و اصول موجود، با تلاش‌های داوطلبانه و رفتار مسئولانه خود برای دستیابی به امنیت سایبری تلاش کنند.

مراجع

[۱] شهاب، مهدیه، پایان‌نامه کارشناسی ارشد، حریم خصوصی و امنیت سایبری: چالش‌ها و راه حل‌ها در حقوق بین‌الملل معاصر، بهمن ۱۳۹۲.

[۲] انصاری، باقر، جزوه درس ارتباطات جمعی، دانشکده علوم ارتباطات دانشگاه علامه طباطبایی، ۱۳۸۳.

[۳] جینا دی آنجلیز، جرایم سایبر، ترجمه عبدالصمد خرم آبادی و سعید حافظی، شورای عالی توسعه قضایی،۱۳۸۲.

[۴] حسن بیگی، ابراهیم، حقوق و امنیت در فضای سایبر، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، چاپ اول ۱۳۸۴.

[۵] اکرمی، سام و سعیده کرمی، پیشگیری غیر کیفری در جرایم اینترنتی، حقوق و فقه، ۱۳۹۵.

[۶] بیگی، جمال، راهبردهای پیشگیری از نقض حقوق شهروندان در فضای مجازی، علم و وکالت، ۱۳۹۷.

[۷] حیدری نژاد، نصرالله، پیشگیری وضعی در جرایم سایبری از منظر حقوق کیفری ایران و جهان، ۱۳۹۷.

[8] Privacy and Human Rights: an International Survey of Privacy Laws and Developments (London Privacy International), 2002.

[9] Explan atory report the convention on cybercrime, 2001.

[10] Houston, Douglas, The Internet Globalization and culture school of business, University of kansas, 2001.