مقابله با جرائم تروریستی در عصر دیجیتال؛ چالش‌ها و راهبردها

پیمان نمامیان[۱]، **علیرضا شکربیگی**[۲]

دریافت: ۱۴۰۲/۰۹/۲۱، پذیرش: ۱۴۰۲/۱۰/۱۶
Doi: 10.22034/RCC.2024.2017795.1084

چکیده

زمینه و هدف: فنّاوری‌های دیجیتالی در حال حاضر زندگی ما را به‌شدت تغییر داده است. تقریباً هر حوزه از روابط اجتماعی در حال حاضر هم در سطح ملی و هم در سطح بین‌المللی در حال دیجیتالی شدن است. زیرساخت‌های ارتباطی اطلاعات و همچنین دستگاه‌های دیجیتال در حال حاضر به بخشی جدایی‌ناپذیر از واقعیت امروز تبدیل شده‌اند. دیجیتالی شدن تأثیر بسیار زیادی بر توسعه و رعایت حقوق بشر و همچنین بر وضعیت خود فرد دارد. با رشد فنّاوری‌های دیجیتالی، جرائم تروریستی در فضای مجازی هم گسترش یافت و فرصت‌های زیادی را برای مرتکبان جرائم تروریستی فراهم کرد تا اقدام‌هایی را جهت ورود آسیب جدی به زیرساخت‌ها و بسترهای اجتماعی، سیاسی و حتی امنیتی فراهم نماید.

روش: این پژوهش از حیث روش اجرا توصیفی-تحلیلی است. از این‌رو، داده‌ها به شیوهٔ اسنادی و سنجش مقررات بر پایهٔ اسناد و منابع مکتوب و نیز مطالعه و واکاوی دیدگاه‌های صاحب‌نظران حقوقی با ابزار فیش‌برداری جمع‌آوری و مورد تجزیه‌وتحلیل قرار گرفته است.

یافته‌ها: با توجه به شکست اقدام‌های کنترلی و نظارت مؤثر بر اینترنت و فضای مجازی به دلیل عدم همکاری دولت‌ها، بهره‌گیری گروه‌های تروریستی از فضای مجازی، چالش نوینی برای سازوکارهای ضد تروریستی قلمداد می‌شود. در ضمن، برای توسعه فضای مجازی در چارچوب راهبرد دولت‌ها به‌ویژه دولت‌های دارنده زیرساخت اینترنت پیشرفته، باید در راستای پیشگیری و سرکوب استفاده تروریستی از رسانه‌ها صورت پذیرد. افزون بر این، با توجه به فقدان یک سند حقوقی جامع در حاکمیت بر اینترنت و فضای مجازی به علت عدم اجماع جهانی، ضرورت دارد تا نسبت به هماهنگی در اِعمال واکنش بین‌المللی موفقیت‌آمیز به تحرکات تروریست‌ها در فضای مجازی دولت‌ها با اتخاذ راهبردهایی متناسب و اثرگذار، در این زمینه اقدام کنند.

واژگان کلیدی: دیجیتال، جرائم دیجیتال، جرائم تروریستی، تروریسم دیجیتال، فضای مجازی.

۱. استادیار گروه حقوق دانشکده علوم اداری و اقتصاد دانشگاه اراک، اراک، ایران (نویسنده مسئول)
Email: p-namamian@araku.ac.ir
0000-0001-7681-7293
۲. استادیار گروه حقوق دانشگاه پیام نور، تهران، ایران.
0000-0001-8657-3149

مقدمه

تحولات در فنّاوری اطلاعات و ارتباطات تأثیر قابل توجهی بر افراد و جامعه به عنوان یک کل داشته است. دیجیتالی شدن شیوه عمل و تعامل را در زمینه‌های اجتماعی تغییر داده است. زیرساخت‌های ارتباطی اطلاعات و نیز دستگاه‌های دیجیتال در حال حاضر به بخشی جدایی‌ناپذیر از واقعیت امروز تبدیل شده‌اند. دیجیتالی شدن تأثیر بسیار زیادی بر توسعه و رعایت حقوق بشر و همچنین بر وضعیت خود فرد دارد.[1]

در این راستا، چالش‌های جدیدی برای حقوق فردی و انسجام اجتماعی پدیدار شده است. قانون به عنوان ابزاری برای تضمین حقوق، توزیع تعهدات و فراهم کردن جوامع باثبات، باید مطابق با فنّاوری تغییر کند. پس از اختراع اینترنت، روندهای جدیدتر مانند دیجیتالی شدن، سرمایه‌داری نظارتی و افزایش عملیات مخرب دیجیتال، همگی اعمال حقوق بین‌المللی موجود در فضای دیجیتال را به چالش کشیده‌اند.

فنّاوری‌های دیجیتال ابزار جدیدی برای دفاع و اجرای حقوق بشر فراهم می‌کنند. استفاده از فنّاوری‌های جدید اطلاعات و ارتباطات حتی توسط افراد و نهادهای غیردولتی ممکن است تهدیدی برای صلح و امنیت بین‌المللی باشد. دیجیتالی شدن، سرمایه‌داری نظارتی و افزایش عملیات مخرب دیجیتال، همگی اعمال حقوق بین‌المللی موجود در فضای دیجیتال را به چالش کشیده‌اند. در حال حاضر هیچ ابزار هنجاری خاصی وجود ندارد که به‌طور جامع حقوق بشر قابل اجرا در عصر دیجیتال را تعیین کند. در مقابل، پیشرفت‌های فنّاوری اطلاعات و ارتباطات برای رژیم‌های مختلف بین‌المللی و محلی موجود که به دنبال حمایت از حقوق بشر هستند، پیامدهایی دارد. توسعه فنّاوری‌های دیجیتال همه جنبه‌های زندگی بشر و حقوق بین‌الملل ازجمله دامنه، موضوعات، ابزار و روش‌های تحریم‌های بین‌المللی و یک‌جانبه را تغییر داده و همچنان در حال تغییر است.

دیجیتالی شدن، سرمایه‌داری نظارتی و افزایش عملیات مخرب دیجیتال، همگی اعمال حقوق بین‌المللی موجود در فضای دیجیتال را به چالش کشیده‌اند. جرائم دیجیتال هیچ مرز جغرافیایی ندارد و کل جهان تحت تأثیر قرار خواهد گرفت. در عصر دیجیتال، که در آن فنّاوری‌های دیجیتال نقشی قابل ملاحظه در کلیه ابعاد تعامل انسانی ایفا کرده‌اند، نظارت بر چالش‌های اینترنت در حقوق بین‌الملل امری انکارناپذیر است (Segura-Serrano, 2006: 272). در واقع، فرایندهای تحول دیجیتال تأثیر عمیقی بر بازیگران و ابزارهای روابط بین‌الملل داشته است. شیوه و ابزارهای تثبیت نظم هنجاری بین‌المللی به‌طور قابل توجهی تغییر کرده است. بازیگران خصوصی ظهور کرده‌اند و فضاهای ارتباطی مهمی با نظم‌های هنجاری جانبی ایجاد کرده‌اند (Kettemann, 2020: 81-84).

گسترش فزاینده فنّاوری اطلاعات و ارتباطات منجر به تحوّل و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی شده است. در چنین فضایی که با عنوان فضای مجازی توصیف می‌شود، تهدیدهای نوینی نظیر جنگ مجازی، جنگ اطلاعاتی، جرائم دیجیتال، پدیده هکرها و سرقت اطلاعات محرمانه نهادهای امنیتی و اطلاعاتی، ظهور کرده‌اند تا امنیت ملی کشورها را با چالش جدی مواجه سازند.

فنّاوری‌های دیجیتالی در حال حاضر زندگی ما را به‌شدت تغییر داده است. تقریباً هر حوزه از روابط اجتماعی در حال حاضر هم در سطح ملی و هم در سطح بین‌المللی در حال دیجیتالی شدن است. شورای امنیت سازمان ملل متحد در قطعنامه‌های ۲۴۱۹ (۲۰۱۸)، ۲۴۶۲ (۲۰۱۹) و ۲۴۹۰ (۲۰۱۹) اذعان می‌دارد فعالیت افراد و نهادهای غیردولتی در حوزه دیجیتال ممکن است تهدیدی برای صلح بین‌المللی و نیز موجبات نقض امنیت را در حملات دیجیتال به زیرساخت‌های حیاتی؛ عدم امکان استفاده از سیستم‌های پرداخت برخط، انسداد دسترسی به اینترنت، حساب‌های توییتر و اینستاگرام فراهم نماید.

توسعه فنّاوری‌های دیجیتال کلیه ابعاد زندگی بشر و حقوق بین‌الملل ازجمله گستره، مسائل، ابزار و روش‌های تحریم‌های بین‌المللی و یک‌جانبه را تغییر داده و همچنان در حال تغییر است. فهرست زیر نمونه‌هایی را ارائه می‌دهد اما کامل نیست: پاسخ به حملات مسلحانه و تهدیدات علیه صلح و امنیت بین‌المللی. استفاده از ابزارهای دیجیتال برای تأمین مالی تروریسم؛ فعالیت‌های دیجیتال مخرب، ازجمله حملات به زیرساخت‌های حیاتی که به سطح یک حمله مسلحانه نمی‌رسند. انسداد تجارت برخط کشورهای هدف، شرکت‌ها و افراد و همچنین سایر اتباع. پیشگیری

از دسترسی به سیستم‌عامل‌های برخط عمومی؛ انسداد تجارت با نرم‌افزار یا تجهیزات ارتباطی اطلاعاتی؛ انسداد حساب‌های کاربردی مجازی؛ فهرست ارزهای دیجیتال (Douhan, 2022: 129).

با ظهور جامعه مبتنی بر اطلاعات، خطراتی که تروریست‌های دیجیتال بتوانند با حملات رایانه‌ای به داده‌ها آسیب برسانند، به وجود آمد. از منظر روان‌شناختی، واژه «تروریسم دیجیتال» ترس از اعمال خشونت‌آمیز را با ترس از فنّاوری ترکیب می‌کند. دلیل آن این است که یک تهدید ناشناخته از نظر روانی قدرتمندتر از یک تهدید شناخته‌شده مانند یک بمب تروریستی تلقی می‌شود. به‌علاوه، از طریق تروریسم دیجیتال علیه دولت‌ها، سرورهای خصوصی، شبکه‌ها یا سایر دستگاه‌های الکترونیکی، هکرها می‌توانند با استفاده از ویروس‌ها، کرم‌ها ضمن ایجاد آسیب به سیستم‌ها، وب‌سایت‌ها را مخدوش کنند.[۲] از این‌رو، می‌توان مصداق‌هایی از تروریسم دیجیتال را ذکر کرد:

الف- شبکه‌های تروریستی جهانی که سایت‌های اصلی را با ایجاد مزاحمت‌های عمومی یا توقف ترافیک اینترنتی مختل می‌کنند؛

ب- دسترسی تروریست‌های دیجیتالی بین‌المللی و سپس غیرفعال کردن یا اصلاح سیگنال‌های فنّاوری نظامی؛

ج- تروریست‌های دیجیتالی که سیستم‌های زیرساختی حیاتی مانند تصفیه‌خانه آب یا شبکه برق را هدف قرار می‌دهند؛

د- جاسوسی دیجیتالی که توسط دولت‌ها یا سازمان‌های خصوصی برای جاسوسی از ارتباطات اطلاعاتی انجام می‌شود (Buresh, 2020: 20).

با این همه، نگارنده سعی بر آن دارد تا بهره‌گیری از روش فیش‌برداری اسنادی و با استفاده از منابع کتابخانه‌ای و اینترنتی ضمن مطالعه پیشینه موضوع و تحولات عصر دیجیتال، رویکردها و جلوه‌های تهاجم به جرائم تروریستی را در فضای دیجیتال مورد مداقه قرار دهد. البته این مقاله درصدد یافتن پاسخ به پرسش‌هایی نظیر «در فضای دیجیتال چه تهدیدهایی ناشی از امکان جرائم تروریستی در حال ظهور است؟» و «چگونه می‌توان در قبال جرائم تروریستی در فضای دیجیتال مقابله کرد؟» است. در ضمن این مقاله با استفاده از روش توصیفی تحلیلی، ضمن تبیین قلمرو اینترنت و سنجش ظرفیت آن در ارتکاب جرائم تروریستی، نحوه مقابله با آن در چارچوب موازین حقوق بین‌المللی با رویکردی حقوق بشری مورد سنجش قرار می‌گیرد.

شناخت مفهومی

امروزه فنّاوری‌ها امکان افزایش جرم و جنایت را فراهم می‌کنند. جرائم در فضای دیجیتال، جرائمی هستند که با استفاده از دستگاه‌های دیجیتال، رایانه، تلفن همراه و موارد دیگر مرتبط هستند. جرم دیجیتال به عنوان جرمی تعریف می‌شود که داده‌های رایانه‌ای و سیستم‌های دیجیتال مرتبط با آن را هدف قرار می‌دهد، که در آن دسترسی، سرقت، تغییر، فساد یا اختلال غیرمجاز انجام می‌شود. بااین‌حال، یک جرم دیجیتال تنها زمانی رخ می‌دهد که یک آسیب‌پذیری در سیستم یا برنامه مورد نظر شناسایی و مورد سوءاستفاده قرار گیرد (ر.ک: ملکوتی و خلیل‌زاده، ۱۴۰۱: ۸۳-۸۱). آسیب‌پذیری به عنوان ضعفی تعریف می‌شود که در دستگاه‌ها یا گروهی از دستگاه‌ها (منابع) وجود دارد که می‌تواند توسط یک تهدید مورد سوءاستفاده قرار گیرد. بنابراین، آسیب‌پذیری‌ها منابع را در معرض خطر بزرگی قرار می‌دهند. خطر به عنوان امکانی برای داده‌ها یا یک سیستم تعریف می‌شود که دچار فساد، از دست دادن، سرقت، آسیب، اختلال یا تخریب شود. البته این دسته از جرائم در گونه‌ها و اَشکالی نظیر کلاه‌برداری و سرقت هویت، جنگ اطلاعاتی، کلاه‌برداری‌های فیشینگ و هرزنامه قابل ملاحظه است.[۳]

بنابراین، جرائم دیجیتال جرائمی است که مولود جامعه فنّاور و مدرن بوده و به همین دلیل، ابهامات زیادی در باب ماهیّت و پیشینه این‌گونه جرائم از یک سو و ویژگی‌های این جرائم و مرتکبان آنها از سوی دیگر وجود دارد. با عنایت به این ابهامات و نیز تفاوت‌های موجود بین جرائم دیجیتال و سایر جرائم، پیشگیری و مقابله با جرائم دیجیتال اقدامات تهاجمی خاصّی را می‌طلبد (موسوی، روحانی‌مقدم و آقائی‌بجستانی، ۱۴۰۱: ۳۲۳).

فنّاوری دیجیتال به عنوان ابزاری بسیار پویا برای ارتباطات دارای کاربرد قابل ملاحظه‌ای است. به‌نحوی‌که این فنّاوری هم‌چنین نیروی محرکه‌ای برای سازمان‌های تروریستی و حامیان آنها برای طیف وسیعی از اهداف است. اینترنت به دلیل مزایای بسیاری که ارائه می‌کند، به ابزار مورد علاقه تروریست‌ها تبدیل شده است ازجمله دسترسی آسان،

مقررات اندک یا بدون محدودیت، سانسور ضعیف یا بدون آن یا سایر اشکال کنترل دولتی، مخاطبان بالقوه عظیمی که در سراسر جهان منتشر می‌شوند (Sander, 2022: 295). ناشناس بودن ارتباطات، جریان سریع اطلاعات، تعامل، توسعه و نگهداری ارزان یک حضور وب، یک محیط چندرسانه‌ای، و توانایی تأثیرگذاری بر پوشش در رسانه‌های جمعی سنتی. بنابراین، عصر دیجیتال و گسترش پلتفرم‌های موجود در فضای مجازی، ظهور تروریسم سایبری را تسهیل کرد (Odhiambo, Ochara and Kadymatimba, 2018: 149-151).

با این همه، حمله‌های دیجیتالی در مقیاس بزرگ با سرعت هشداردهنده‌ای در سراسر جهان در حال افزایش است. این حمله‌ها اغلب با تهدیدهای تروریستی دیجیتالی که به‌طور گسترده تبلیغ و عمومی شده است، مرتبط هستند. بااین‌حال، «تروریسم دیجیتالی» یک زمینه تحقیقاتی نسبتاً جوان است و اصطلاحات آن، نظیر اصطلاح اصلی آن، یعنی «تروریسم»، تاکنون به نحو قابل پذیرشی مورد تعریف قرار نگرفته است (Taylor, 2014: 48-50). البته تعریف جدید از تجزیه‌وتحلیل دقیق تعاریف موجود در ادبیات قابل دسترس عموم قابل ملاحظه است، که مشتمل بر کلیه اشتراکات کلیدی شناسایی شده وفق طبقه‌بندی جدید پیشنهادی (یعنی بازیگر، انگیزه، قصد، وسیله، اثر و هدف) است. این رویکرد نوین برای تعریف تروریسم دیجیتالی درک مشترکی از تهدید گسترده‌تر برای استانداردسازی سیاست، همکاری جهانی و تحقیقات ارائه می‌کند، درحالی‌که اجازه می‌دهد زیرمجموعه‌های منحصربه‌فردی از این شاخه از جرائم تروریستی برای کاربردهای قانونی یا تخصصی خاص تعریف شود (Plotnek and Slay, 2021: 136-137).

با این همه، پرسشی که به ذهن متبادر می‌شود این‌که «آیا تروریسم دیجیتال وجود دارد؟» مادامی‌که پرسش‌هایی راجع‌به وجود یک مفهوم مطرح می‌شود، پاسخ به تعریف آن بستگی دارد. با توجه به تعاریف موجود در خصوص جرائم تروریستی، هدف از آن ایجاد ارعاب و هراس افراد یک سازمان یا یک دولت از طریق ایجاد اختلال در فرایندهایی است که در آن سازمان یا دولت عمل می‌کند یا از طریق کشتن یا معلول کردن آن افراد. از این‌رو، نقطه مشترک بین تعریف جرائم تروریستی متعارف و تعریف تروریسم دیجیتال این است که هر دو جرم سعی در ایجاد اختلال در فرایندهای یک سازمان یا دولت دارند. تفاوت در این دو تعریف به این بستگی دارد که آیا قتل و معلول کردن افراد برای معنای تروریسم دیجیتال حیاتی است یا خیر؟ اگر کشتار و معلول کردن افراد یکی از ویژگی‌های ذاتی تروریسم دیجیتال باشد، به‌ظاهر تفاوتی بین هیچ‌یک قابل ملاحظه نیست. در تروریسم دیجیتال، ابزار ارتکاب حمله از یک حمله جنبشی مستقیم به یک حمله دیجیتالی تغییر کرده است، جایی که اثرات جنبشی پیامد حمله دیجیتالی است. یک تفاوت قابل توجه بین جرائم تروریستی متعارف و تروریسم دیجیتال این است که فراوانی حملات تروریستی دیجیتالی از میزان حملات تروریستی سنتی کمتر است (Buresh, 2020: 71-72).

تحولات فنی و حقوقی

در اوایل دهه ۱۹۸۰، سازمان‌های مجری قانون با آغاز عصر رایانه با نگرانی فزاینده در مورد فقدان مقررات کیفری موجود برای مبارزه با جرائم رایانه‌ای نوظهور مواجه شدند (Jarrett and Bailie, 2011: 21). البته جنایات دیجیتال از سال ۱۹۶۰ (در آن زمان سیستم‌های مخابراتی تحت تأثیر حملات قرار گرفتند) تا به امروز متفاوت بودند. در دوران اولیه نظام‌های اطلاعاتی، جرائم رایانه‌ای توسط برخی از کارکنان مرتکب می‌یافت؛ هم‌چنین حملات فیزیکی به سیستم‌های رایانه‌ای در فاصله سال‌های ۱۹۶۰ تا ۱۹۸۰ رایج بود. در سال ۱۹۸۰ نرم‌افزارهای مخرب علیه رایانه‌های شخصی ظاهر شد.[۴]

در آغاز دهه ۱۹۹۰ اینترنت عامل مهمی برای افزایش جرائم دیجیتالی بود. مجرمان با استفاده از روش‌های غیرمجاز معمولاً برای منافع مالی به سیستم‌های ضعیف دسترسی داشتند، مثلاً کلاه‌برداری از کارت اعتباری در اواسط دهه ۱۹۹۰ به‌سرعت رشد کرد. در پایان قرن بیستم و آغاز قرن بیست و یکم، کلاه‌برداری از کارت اعتباری در دسته وسیع‌تری به نام سرقت هویت قرار گرفت. مجرمان هویت افراد دیگر را برای انجام فعالیت‌های غیرقانونی سرقت می‌کردند. در سال ۲۰۰۸ این سریع‌ترین شکل کلاه‌برداری بود. جرائم تلفن همراه در چند سال اخیر در حال افزایش است، در کنار این‌ها، امروزه نوع جدیدی از فعالیت‌های مجرمانه در حال شکل‌گیری است (Kabay, 2008: 64-67) که در این رابطه می‌توان به چهار قاعده مختلف در جرائم

اشاره داشت:

الف- رایانه به عنوان یک هدف جرم (نظیر این‌که رایانه می‌تواند به عنوان خودش به سرقت برود)؛

ب- رایانه به عنوان موضوع جرم، یعنی رایانه محیط جرم است؛

ج- رایانه ممکن است به عنوان ابزاری برای انجام یک جرم استفاده شود (به عنوان نمونه، برای دسترسی به رایانه دیگری و ارتکاب جرم در آنجا)؛

د- استفاده از نماد رایانه برای انجام فعالیت‌های غیرقانونی (Casey, 2011: 149-152).

نگرانی فزاینده‌ای در مورد سوءاستفاده تروریست‌ها از فنّاوری‌های اطلاعات و ارتباطات به‌ویژه اینترنت و فنّاوری‌های دیجیتال جدید برای ارتکاب، تحریک، عضوگیری، تأمین مالی یا برنامه‌ریزی جرائم تروریستی وجود دارد. از این‌رو، سازمان ملل متحد به خطرات استفاده تروریستی از اینترنت پی برده است. در دهه ۱۹۹۰ سازمان از دولت‌های عضو خواست خطر استفاده تروریستی از سیستم‌ها و شبکه‌های الکترونیکی یا مخابراتی با سیم جهت انجام اعمال جنایت‌کارانه را متذکر شوند و سازوکاری برای پیشگیری از چنین جرم و جنایتی و برای ترویج همکاری به تناسب حال پیدا کنند.[۵] پس از آن شورای امنیت از دولت‌های عضو خواست با تبادل اطلاعات مربوط به استفاده گروه‌های تروریستی از فنّاوری ارتباطات و مخابراتی همکاری بین‌المللی را افزایش دهند.[۶] دستیابی به این همکاری به‌طور عملی دشوارتر از آن بود که تصور می‌شد (Archick, 2014: 8-9). بااین‌حال سازمان در سال ۲۰۰۵ مشکل خاص تروریست‌هایی که به‌ویژه در عصر رسانه‌های پرطرفدار شبکه‌سازی اجتماعی همچون فیس‌بوک، تلگرام، توییتر، یوتیوب، فلیکر، و سکوهای وبلاگ‌سازی از اینترنت سوءاستفاده می‌شد و افرادی که خواسته یا ناخواسته مقدار بی‌سابقه‌ای از اطلاعات حساس را از طریق اینترنت انتشار دادند را اعلام کرد.

از سال ۲۰۰۰، در پاسخ به نیاز به استانداردسازی، ارگان‌ها و آژانس‌های مختلف دستورالعمل‌هایی را برای جرم یابی قانونی دیجیتال منتشر کردند. البته یک معاهده بین‌المللی موسوم به «کنوانسیون جرائم رایانه‌ای، مصوب ۲۰۰۱»[۷]، در سال ۲۰۰۴ با هدف تطبیق قوانین ملی جرائم رایانه‌ای، تکنیک‌های تحقیق و همکاری بین‌المللی لازم‌الاجرا شد. این کنوانسیون اولین معاهده بین‌المللی راجع‌به جرائم ارتکابی از طریق اینترنت و سایر شبکه‌های رایانه‌ای است که به‌ویژه با نقض حق چاپ، کلاه‌برداری رایانه‌ای، هرزه‌نگاری کودکان، جرائم ناشی از نفرت، و نقض امنیت شبکه‌ها در ارتباط است.

لازم به ذکر است دولت‌های عضو سازمان ملل متحد وفق قطعنامه ۲۳۴۱ شورای امنیت مصوب سال ۲۰۱۷ و راهبرد جهانی مبارزه با تروریسم سازمان ملل متحد، بر اهمیت همکاری چندجانبه سازمان‌های بین‌المللی، منطقه‌ای و زیرمنطقه‌ای، بخش خصوصی و جامعه مدنی در قبال تهدیدهای ناشی از جرائم تروریستی در فضای دیجیتال، تأکید کردند. البته از دفتر مبارزه با تروریسم و سایر نهادهای مرتبط با پیمان هماهنگی جهانی مبارزه با تروریسم درخواست شد تا به‌طور مشترک از اقدام‌ها و رویکردهای نوآورانه برای ایجاد ظرفیت دولت‌های عضو، در صورت درخواست آن‌ها، برای مقابله این چالش‌ها حمایت کنند.[۸]

کمیته مبارزه با تروریسم شورای اروپا[۹] همایشی دیجیتالی با عنوان «مقابله با ارتباطات تروریستی: تبلیغات تروریستی، تحریک عمومی، استخدام و رادیکالیزه کردن»[۱۰] در محل شورای اروپا در سی‌ویکم ژانویه تا یکم فوریه ۲۰۲۳ برگزار کرد. این همایش بر سازوکارهای عملیاتی نظارت و مقابله با فعالیت‌های گروه‌های تروریستی به‌صورت برخط و غیربرخط[۱۱]، به‌ویژه تلاش‌های گروه‌های تروریستی برای عضوگیری و جلب حمایت در میان حوزه‌های موردنظرشان، و نیز آن‌هایی که با هدف ارائه ابزار و دانش لازم برای انجام فعالیت‌ها انجام می‌شوند، متمرکز بود.[۱۲]

سیاست‌ها و راهبردها

فضای بی‌مرز دیجیتال، جهانی موازی با جهان فیزیکی را به وجود آورده است که درواقع کنترل و ادارهٔ حقوقی آن از حیطهٔ اعمال قدرت یک حاکمیت برنمی‌آید. بنابراین، برای حاکمیت بر این فضا و مقابله با جرائم روزافزون و پیچیدهٔ ارتکابی در فضای دیجیتال همکاری و معاضدت جامعهٔ بین‌المللی برای قاعده‌مندی نیاز است، به‌گونه‌ای که هیچ مجرمی بدون مجازات نماند و این مهم به دست نمی‌آید، مگر با تدوین مقررات هماهنگ و متحدالشکل؛ زیرا جرائم ارتکابی در فضای دیجیتال مرزهای جغرافیایی و سنتی را پشت سر می‌گذارند و به سبب ویژگی‌هایی که دارند،

می‌توان برخی از این‌گونه جرائم را در زمرهٔ آن دسته جرائمی به شمار آورد که برای مقابله با آنها اعمال صلاحیت جهانی ضرورت دارد (جلالی و توسلی‌اردکانی، ۱۳۹۸).

جرائم دیجیتال به‌ویژه طی یک دهه اخیر، به‌مثابه یک راز اطلاق نمی‌شود. جرم دیجیتال زمانی شروع می‌شود که فعالیت غیرقانونی روی داده‌ها یا اطلاعات موجود در رایانه‌ها یا شبکه‌ها انجام شود (Kondo, Katsenga, Zvid-zayi, 2018: 121). در روزهای اولیه جرائم دیجیتال، جرم معمولاً در زمینه مالی انجام می‌شد، اما جرائم دیجیتال اکنون به شکل‌های دیگری تکامل یافته است، به‌عنوان‌مثال سیستم‌های اطلاعاتی به دلایلی می‌توانند توسط برخی از شرکت‌ها به سرقت رفته یا آسیب ببینند. رایانه یا دستگاه‌های تلفن همراه می‌توانند به عنوان ابزاری برای مقابله با جرم مورد استفاده قرار گیرند و به‌طورکلی میزان جرائم دیجیتالی به‌وضوح پس از ظهور اینترنت افزایش می‌یابد. شبکه‌ها نیز نقش بسزایی در افزایش میزان جرائم دیجیتال دارند.

علی‌رغم این‌که اینترنت برای جامعه امری ضروری به شمار می‌رود، اما باید به عنوان ابزاری در مقابله با جرائم تروریستی در نظر گرفت (Yüksel, 2020). همان‌طورکه «بان‌کی مون»[۱۳]، دبیر کل سابق سازمان ملل متحد اظهار داشت: «اینترنت نمونه بارز این است که چگونه تروریست‌ها می‌توانند به شیوه‌ای واقعاً فراملی رفتار کنند. در پاسخ، دولت‌ها باید به شیوه‌ای یکسان فراملی بیندیشند و عمل کنند.»[۱۴]

این در حالی است که اینترنت به ابزاری ضروری برای ارتباطات انسانی تبدیل شده است که اطلاعات فراوان و کاربردهای متنوعی را ارائه می‌دهد. بااین‌حال، وب جهانی فرصت‌های زیادی را برای مرتکبان جرائم تروریستی فراهم می‌کند تا اقدام‌هایی را انجام دهند که باعث آسیب جدی به زیرساخت‌ها و بسترهای اجتماعی، سیاسی و حتی امنیتی می‌شود. از این‌رو، گروه‌های تروریستی معاصر، اولین نسلی هستند که اعضای آن با دسترسی به اینترنت موجبات تهدید برای نقض امنیت بین‌المللی را فراهم آورده‌اند. بنابراین، نباید تعجب‌آور باشد که این پلتفرم‌های برخط نقش مهمی در استخدام افراد آسیب‌پذیر دارند. در واقع، فضای مجازی و اینترنت به تسهیل‌کننده‌های مفیدی برای ترویج، تحریک، ارعاب، و انتخاب مخاطبان بسیار گسترده‌تر و غیرقابل‌دسترس تبدیل شده‌اند.

تروریست‌ها به‌طور روزافزون از فضای مجازی به عنوان ابزاری برای جذب نیرو و شناساندن خود به مردم استفاده می‌کنند. رسانه اجتماعی یک نوآوری جدید است که به افراد اجازه می‌دهد اطلاعات، ایده‌ها، پیام‌های شخصی و محتویات دیگر (مانند فیلم) را در سراسر دنیا با یکدیگر به اشتراک بگذارند.[۱۵] رسانه اجتماعی موجود در فضای مجازی ویژگی‌های مفیدی برای انتشار محتوا، دسترسی آزاد به کاربران، توانایی بازآفرینی و انتقال فوری اطلاعات دارد، اما همین مزیت‌ها موجب شده است تا این‌گونه رسانه‌ها ابزار سودمندی برای تروریست‌ها باشند (Weimann, 2014: 1).

اینترنت و فضای مجازی علاوه بر تأثیرات بنیادین بر حوزه‌های فرهنگی، اجتماعی و اقتصادی جوامع مختلف ابعاد تهدیدآمیزی را نیز آشکار ساخته و زمینه انتقال منابع ناامنی از فضای واقعی به مجازی را فراهم کرده است. امروزه محیط‌های تهدیدآمیز علیه منافع ملت‌ها و دولت‌ها صرفاً به سرزمین محدود نمی‌شود و جهان مجازی نیز محیطی تهدیدزا به شمار می‌آید. ارتکاب جرائم تروریستی در بستر فضای مجازی یکی از مهم‌ترین تهدیدهای نوظهور است که با استفاده از قابلیت‌های اینترنت به فعالیت‌های خود بُعد بین‌المللی داده است. از این‌رو، ماهواره، اینترنت، فضای مجازی و روزنامه‌نگاری سایبر، عامل فضای مجازی در ظهور و گسترش و گروه‌های تروریستی به عنوان بازیگران جدید در عرصه بین‌الملل بیشترین نقش را ایفاء کرده است (برجعلی‌زاده، جعفری و کردی، ۱۳۹۸: ۱۳۹).

اگرچه مزایای اینترنت برای جامعه مدرن بسیار زیاد است، اما باید به این نکته نیز توجه داشت که همان فنّاوری که چنین ارتباطاتی را تسهیل می‌کند، می‌تواند توسط تروریست‌ها نیز مورد سوءاستفاده قرار گیرد. از اینترنت می‌توان برای تمجید و تحریک به ارتکاب جرائم تروریستی، استخدام تروریست‌ها، انتشار محتوای غیرقانونی، تسهیل ارتباط بین عوامل تروریستی و آموزش نیروهای بالقوه استفاده کرد.[۱۶]

در مارس ۲۰۱۲، پس از تصویب قطعنامه ۱۷۸/۶۶ توسط مجمع عمومی، از دفتر مبارزه با مواد مخدر و جرائم سازمان ملل متحد درخواست شد، در چارچوب وظایف خود، «توسعه دانش حقوقی تخصصی در قبال جرائم تروریستی و غیره، به دولت‌های عضو درخواست‌کننده در رابطه با پاسخ‌های عدالت کیفری به تروریسم، ازجمله، در

صورت لزوم، بهره‌گیری از اینترنت برای اهداف تروریستی، کمک کند.»

دفتر مبارزه با مواد مخدر و جرائم سازمان ملل متحد، با هدف ارائه راهنمایی‌های عملی برای سیاست‌گذاران، بازرسان و دادستان‌ها راجع‌به پاسخ‌های عدالت کیفری مؤثر به پرونده‌های مربوط به استفاده از اینترنت برای اهداف تروریستی و مواردی را که از اینترنت به عنوان ابزاری برای تمجید از اقدامات تروریستی، تحریک، عضوگیری، تأمین مالی، آموزش، برنامه‌ریزی و ارتکاب جرائم تروریستی استفاده می‌شود، بررسی می‌کند. در این فرایند، مطابق میثاق بین‌المللی حقوق مدنی و سیاسی، هرگونه محدودیت برای آزادی‌های اساسی، ازجمله حقوق آزادی بیان، آزادی تشکل و حریم خصوصی، باید ضروری و متناسب با تهدید باشد و باید توسط قانون تنظیم شود و شرایط دقیق مداخله را مشخص کند.

البته باید اذعان شود، تا پایان سال ۲۰۲۰ شورای امنیت ملل متحد هرگز تحریم‌هایی را علیه دولت‌ها، اشخاص حقیقی یا حقوقی در پاسخ به بهره‌گیری مخرب از ابزارهای مجازی اعمال نکرده بود؛ این در حالی است که تأکید کرده دولت‌ها موظف به کنترل جریان اطلاعات، پیشگیری از استفاده از اینترنت برای پول‌شویی و تأمین مالی تروریسم، کنترل امور مالی مجازی و مبادله اطلاعات اطلاعاتی مالی لازم[۱۷] یا داده‌های هوانوردی و نام مسافران هستند[۱۸]. در ضمن، مجمع عمومی سازمان ملل متحد برای پیشگیری از بهره‌گیری از اینترنت برای حمایت، ارتکاب، تحریک، عضوگیری، تأمین مالی یا برنامه‌ریزی اقدام‌های تروریستی، قطعنامه ۷۳/۱۷۴ را در سال ۲۰۱۸ صادر کرد.[۱۹]

حقوق بین‌المللی و سازوکارهای مقابله

درحالی‌که در سطح بین‌المللی واضح است که کاربرد و اجرای استانداردهای حقوق بشر باید در کنار تکامل فضاهای دیجیتال تکامل یابد، واقعیت با این درک مطابقت ندارد. فنّاوری‌ها اغلب برای افزایش نظارت، کنترل و طرد بیشتر گروه‌های به حاشیه رانده شده تاریخی استفاده می‌شود.

حقوق بشر در فضای دیجیتال زمینه جدیدی از نگرانی جهانی است. با ظهور اینترنت و محبوبیتی که در سال‌های اخیر به دست آورده است، نظارت بر فضای دیجیتال و حفظ حقوق بشر افرادی که از آن استفاده می‌کنند ضروری است. اینترنت دسته جدیدی از مجرمان یعنی مجرمان دیجیتال را به وجود آورده است. مجرمان دیجیتال به زندگی خصوصی افراد نفوذ می‌کنند و از این طریق حقوق بشر کاربران اینترنت را نقض می‌کنند. اینترنت یک رسانه قوی برای بیان ایده‌ها است و بنابراین باید بدون هیچ محدودیتی باشد. این بستری را برای ما فراهم می‌کند تا از حق آزادی بیان و اطلاعات استفاده کنیم. در زمانی که اینترنت به وجود آمد و فنّاوری هنوز در حال رشد بود، هیچ‌کس هرگز فکر نمی‌کرد که بتواند تا این حد بر حقوق اساسی آنها تأثیر بگذارد (ضیایی، ۱۳۹۶: ۷۹).

با این همه، پیشگیری از نقض حقوق بشر در عصر دیجیتال بر عهده قانون‌گذاران و در چارچوب حاکمیت سرزمینی دولت‌ها از یک‌سو و جامعه بین‌المللی نظیر سازمان ملل متحد از دیگر سو است که باید اطمینان حاصل کنند که مقررات جدید با اسناد هنجاری بین‌المللی و محلی مطابقت دارد. علاوه بر این، بخش خصوصی می‌تواند با طراحی فنّاوری‌های جدید به گونه‌ای که از نقض بالقوه حقوق بشر پیشگیری کرده یا به حداقل می‌رساند، در پیشگیری از سوءاستفاده‌ها نقش داشته باشد. بنابراین، حمایت از حقوق بشر به بهترین وجه از طریق تعامل بین نوآوری‌های تکنولوژیکی و اصلاح سیاست‌ها قابل دستیابی است. اول، توسعه‌دهندگان سخت‌افزار و نرم‌افزار را می‌توان متقاعد کرد که در محصولات جدید راه‌حل‌های فنّاوری برای مشکلات مربوط به حقوق بشر در هنگام توسعه فنّاوری‌های جدید ایجاد کنند. به‌عنوان‌مثال استفاده از نظام‌هایی که از روگرفت غیرقانونی داده‌ها برای محافظت از حق چاپ پیشگیری می‌کند. دوم، مهم است که پیامدهای حقوق بشر فنّاوری‌های نوین پیش از معرفی آنها بررسی شود، نه بعد از آن (Casella, 2003: 92).

رویارویی با جرائم تروریستی به یک مسئله مهم بین‌المللی مبدل گشته است. گروه‌های تروریستی اکنون از فرصت‌های ارائه شده توسط اینترنت و فضای مجازی بهره می‌برند و از منابع برخط برای فرماندهی، کنترل و برقراری ارتباط با شبکه‌های خود استفاده می‌کنند و روایت‌های خود را به گونه‌ای شکل می‌دهند که نگرانی‌های عمومی را بیان می‌کنند و نیروهای جدید جذب می‌کنند (Yüksel, 2020).

سنجش قلمرو حقوق بین‌المللی در حوزه رسانه‌ها به‌ویژه در مسئله فضای مجازی و البته بررسی کارکرد آن‌ها در بستر

فضای مجازی به شکل ساختاری واقعی، به‌مثابه چالشی اطلاق می‌شود که به دلیل نقش استثنایی رسانه‌ها به‌طورکلی و تأثیر مستمر و اساسی آن بر فرایندهای دموکراتیک در حال وقوع در جهان، نیاز به اثبات علمی دارد. در این راستا، توجه ویژه‌ای به تأثیر رسانه‌ها بر روندهای معاصر مربوط به روند ادغام اتحادیه اروپا، توسعه دموکراسی و حاکمیت قانون شده است. این امر به‌ویژه بر آزادی بیان، احترام به ارزش‌ها و اصول استانداردها، حقوق و آزادی‌های بشر تأکید دارد (Ronkova, 2016: 58).

تاکنون، جامعه بین‌المللی ابزارهای قانونی را ایجاد کرده است که سازوکارهایی برای حل چالش‌های ناشی از بهره‌گیری غیرقانونی از اینترنت و فضای مجازی توسط گروه‌های تروریستی ارائه می‌دهد. چنین تلاش‌هایی توسط سازمان ملل متحد، شورای اروپا و اتحادیه اروپا رهبری می‌شود. [۲۰] بااین‌حال، ایجاد مقررات قانونی به دلیل توسعه سریع مؤلفه‌های نوین اینترنت با چالش‌هایی مواجه است. یافتن تعادل عادلانه میان مقررات و حمایت از حقوق فردی و به‌ویژه آزادی بیان امری دشوار به نظر می‌رسد.

با این همه، سازمان ملل متحد نقشی مهم در توسعه آزادی اطلاعات به عنوان یکی از مصادیق حقوق بشر دارد. مهم‌ترین موازین حاکم در چارچوب قواعد بین‌المللی سازمان ملل متحد که حاوی مقررات رسانه‌ای است مشتمل بر «اعلامیه جهانی حقوق بشر»، «میثاق بین‌المللی حقوق مدنی و سیاسی» و «قطعنامه ۵۹/۱ راجع‌به آزادی اطلاعات»، است.

مجمع عمومی سازمان ملل متحد اعلامیه جهانی حقوق بشر را به عنوان معیاری مشترک برای دستاوردهای همه مردم و همه ملت‌ها اعلام کرد تا بدین منظور هر فرد و هر ارگان جامعه، با در نظر داشتن این اعلامیه، با آموزش و تعلیم تلاش کند. این در حالی است که وفق ماده ۱۸ و ۱۹ اعلامیه مزبور مقرر شده است آزادی بیان یکی از ارکان اساسی دموکراسی است؛ یعنی این آزادی از حق افراد برای شکل‌دهی و ابراز عقیده و حق ایجاد انجمن‌هایی حمایت می‌کند که نظرات جمعی آنها را در مورد واقعیت‌ها و تحولات اجتماعی تشویق و منتشر کنند. آزادی بیان به هر فردی این حق را می‌دهد که آزادانه اظهارنظر کند و از هیچ‌کس منع نخواهد شد.

به‌علاوه، ماده ۱۸ میثاق بین‌المللی حقوق مدنی و سیاسی، تصریح می‌کند «هر کس حق آزادی اندیشه، وجدان و مذهب را دارد» و این حق تنها می‌تواند مشمول محدودیت‌هایی باشد که در قانون مقرر شده است. در این رابطه هم حفاظت از امنیت عمومی، نظم، سلامت یا اخلاقیات یا حقوق و آزادی‌های اساسی دیگران به عنوان امری ضروری انگاشته شده است و هم بر اساس ماده ۱۹ حقوق مقرر مشتمل بر آزادی جستجو، دریافت و انتشار اطلاعات و عقاید از هر نوع، بدون توجه به مرزها، اعم از شفاهی، کتبی یا چاپی، و در قالب هنری یا از طریق هر وسیله دیگری که انتخاب می‌کند، است.

در سال ۱۹۴۶، مجمع عمومی سازمان ملل متحد (سازمان ملل متحد) در قطعنامه ۵۹/۱ عبارت «آزادی اطلاعات» را به تصویب رساند که به معنای حق جمع‌آوری، انتقال و انتشار اخبار در هرکجا و همه‌جا بدون محدودیت است. [۲۱]

البته در این میان مهم‌ترین منابع حقوقی که توسط شورای اروپا تصویب شده شامل «کنوانسیون اروپایی حقوق بشر، مصوب ۱۹۵۰»، «منشور اروپایی برای زبان‌های منطقه‌ای یا اقلیت، مصوب ۱۹۹۲» و «کنوانسیون چارچوب برای حمایت از اقلیت‌های ملی، مصوب ۱۹۹۸» است. از این‌رو، بر اساس بند نخست از ماده ۱۰ این کنوانسیون اروپایی حقوق بشر «هر کس حق آزادی بیان دارد» که برای این اهداف، آزادی بیان شامل آزادی عقیده، آزادی دریافت اطلاعات و آزادی در انتشار اطلاعات و عقاید بدون دخالت مقامات دولتی، است. در ماده ۱۱ منشور اروپایی حقوق بشر، برای زبان‌های منطقه‌ای یا اقلیت مقرر شده است که ترویج زبان‌های منطقه‌ای یا اقلیت‌ها در رسانه‌ها برای حفظ آنها حیاتی است. علاوه بر این، مقرر شده که طرفین متعهد می‌شوند که به کاربران زبان‌های منطقه‌ای یا اقلیت اطمینان در مواردی نظیر الف- افتتاح حداقل یک ایستگاه رادیویی و یک کانال تلویزیونی به زبان‌های منطقه‌ای یا اقلیت، ب- تشویق یا تسهیل گشایش مطبوعات، ب- برای اجرای این منشور گزارش‌های دوره‌ای برای دولت‌های امضاکننده توسط کمیته کارشناسان شورای اروپا تهیه می‌شود، حاصل کنند.

افزون بر این، می‌توان برای پیشگیری از انتشار و تبلیغ به ارتکاب جرائم تروریستی در رسانه‌ها به کنوانسیون چارچوب برای حمایت از اقلیت‌های ملی، برای تضمین

و تحقق دسترسی اقلیت‌ها به رسانه‌ها با ترویج تساهل و تکثر فرهنگی در رسانه‌ها اشاره داشت که در این رابطه سازوکارهایی را مقرر نمود: الف- حمایت مالی از صداوسیما که برنامه‌هایی را به زبان‌های اقلیت پخش می‌کند، ب- تأمین بودجه برای برنامه‌هایی که به موضوعات مرتبط با اقلیت‌ها یا گفت‌وگو بین گروه‌های قومی مختلف می‌پردازند، ج- تشویق سردبیران و صداوسیما برای امکان دسترسی اقلیت‌های ملی در برنامه‌های خود.

البته در بند نخست ماده ۹ کنوانسیون اخیر مقرر شده است «طرفین متعهد خواهند شد که نسبت به حق آزادی بیان هر فردی که به یک اقلیت ملی تعلق دارد شامل آزادی داشتن عقیده و دریافت و انتشار اطلاعات و عقاید به زبان اقلیت است، به رسمیت بشناسند، بدون مداخله مقامات دولتی و بدون توجه به مرزها.»

پیش‌نویس گزارش تقریریافته از سوی دفتر مبارزه با مواد مخدر و جرائم سازمان ملل متحد و «گروه ویژه اجرای مبارزه با تروریسم ملل متحد»[۲۲]، حملات سایبری، انتشار اطلاعاتی نظیر تبلیغات و تحریک را به عنوان جرائم تروریستی مدنظر قرار داده است. جامعه بین‌المللی تاکنون اسناد حقوقی بین‌المللی ویژه‌ای را برای مواجه با بهره‌گیری از اینترنت توسط گروه‌های تروریستی تصویب کرده که توسط سازمان ملل متحد، شورای اروپا و اتحادیه اروپا رهبری می‌شود. بااین‌حال، توسعه مقررات قانونی به دلیل ویژگی‌های بدیع اینترنت با چالش‌هایی مواجه است.

نتیجه‌گیری و پیشنهادها

روند افزایش روزافزون هنجارهای حاکمیت دیجیتال بالقوه باعث می‌شود که حقوق بین‌المللی آینده در مورد فضای دیجیتال به‌سختی به طور مؤثر بر بازیگران دولتی تحمیل شود. درصورتی‌که حقوق بین‌المللی آینده در مورد فضای دیجیتال توسط حاکمیت دیجیتال به بهای منافع بازیگران غیردولتی آنها تغییر می‌کند. هر دو سناریو نشان می‌دهند که حقوق بین‌المللی در مورد فضای دیجیتال به‌سختی برای بازیگران دولتی مؤثر است و نیاز به درخواست‌های گسترده‌تری برای تدوین هنجارهای اینترنتی جهانی مبتنی بر قاعده، آزادی‌محور و فراگیر در آینده دارد. ازآنجایی‌که جرائم دیجیتال یک تهدید بزرگ برای همه کشورهای جهان است، باید اقدامات خاصی در سطح بین‌المللی برای پیشگیری از جرائم دیجیتال انجام شود. باید عدالت کامل برای قربانیان جرائم دیجیتال از طریق جبران خسارت و برخورد قاطع با متخلفان برقرار شود تا نمونه‌ای باشد تا بتواند مجرمان جرائم اینترنتی را پیش‌بینی کند.

بنابراین، علی‌رغم عدم امکان تصویب یک سند حقوقی راجع به حاکمیت بر اینترنت و فضای مجازی از سوی جامعه بین‌المللی به جهت نبود اجماع جهانی، اما این امکان برای هماهنگی در اِعمال واکنش بین‌المللی موفقیت‌آمیز به تحرکات تروریست‌ها در فضای مجازی راهبردی است که می‌تواند در مقابله با این‌گونه اقدامات مؤثر واقع گردد. فضای مجازی در عصر نوین دانش و فنّاوری از مزیت‌های برجسته‌ای برخوردار می‌باشند.

البته می‌توان در پاسخ به چالش‌ها و تهدیدهای ناشی از ارتکاب جرائم تروریستی در فضای دیجیتال، راهبردهای زیر را ارائه کرد:

الف- دولت‌ها به‌ویژه دولت‌های دارنده زیرساخت اینترنت پیشرفته برای توسعه فضای مجازی، باید برای پیشگیری و سرکوب استفاده تروریستی از این رسانه با یکدیگر همکاری کنند.

ب- راهبرد دولت‌ها در حوزه سیاست‌گذاری باید به گونه‌ای باشد که حقوق اساسی بشر نقض نشود، موضوع نظارت، نظارت بر ارتباطات، حریم خصوصی، رضایت و فنّاوری باید با تجزیه‌وتحلیل موقعیت و عملکرد قانونی، اخلاقی همراه باشد؛ تنها در این صورت است که فرصتی برای حفاظت از حقوق اولیه بشر و ارتقای مسئولیت در این فضای فنّاورانه وجود خواهد داشت.

پی‌نوشت‌ها

1. UNGA Res 68/167 of 18 December 2013, A/RES/68/167, para. 3.

۲. در این ارتباط می‌توان به هک جایگاه‌های سوخت کشور و اختلال در پمپ بنزین‌ها در ۲۷ آذر ۱۴۰۲ اشاره داشت که این امر به گفته مسئولان امر که توسط خبرگزاری‌های داخلی انعکاس یافت توسط یک گروه هکری صهیونیستی به نام «گنجشک درنده» بوده که مسئولیت هک سیستم سوخت‌رسانی کشور را بر عهده گرفته است. این در حالی است که پیشتر هکرها در چهارم آبان ۱۴۰۰، اطلاعات کارت سوخت شخصی را هدف قرار دادند؛ https://www.farsnews.ir/news/14020927000595/D8

3. https://study.com/academy/lesson/attacks-in-digital-crime-definition-types-vulnerability.html

۴. لازم به ذکر است پیش از دهه ۱۹۷۰ با استفاده از مقرره‌های موجود به جرائم مربوط به رایانه رسیدگی می‌شد. اولین جرائم رایانه‌ای در قانون جرائم رایانه‌ای فلوریدا در سال ۱۹۷۸ به رسمیت شناخته شد که مشتمل بر مقرره‌هایی علیه اصلاح یا حذف غیرمجاز داده‌ها در یک سیستم رایانه‌ای بود.

5. G.A. Res. 51 /210

6. S.C. Res. 1373, para. 3, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

۷. این کنوانسیون که به عنوان «کنوانسیون جرائم رایانه‌ای بوداپست» یا «کنوانسیون بوداپست» نیز شناخته می‌شود، اولین معاهده بین‌المللی است که به دنبال رسیدگی به جرائم اینترنتی و رایانه‌ای از طریق هماهنگ کردن قوانین ملی، بهبود تکنیک‌های تحقیقاتی و افزایش همکاری بین کشورها است و توسط شورای اروپا در استراسبورگ فرانسه و با مشارکت فعال کشورهای ناظر شورای اروپا کانادا، ژاپن، فیلیپین، آفریقای جنوبی و آمریکا تهیه شد.

8. https://www.un.org/counterterrorism/cybersecurity

9. Council of Europe Committee on Counter-Terrorism (CDCT)

10. Digital Conference on “Countering Terrorist Communications: Terrorist Propaganda, Public Provocation, Recruitment and Radicalisation”, 31 January to 1 February 2023.

۱۱. بازیگران تروریست از پلتفرم‌ها و فنّاوری‌های برخط برای استخدام، آموزش، رادیکال‌سازی، تحریک عمومی، تبلیغات یا برنامه‌ریزی، آماده‌سازی و اجرای حملات استفاده می‌کنند. این پدیده با ظهور پلتفرم‌ها و خدمات جدید به تکامل خود ادامه می‌دهد و بازیگران تروریست را قادر می‌سازد تا راه‌های جدید و نوآورانه‌ای برای مهار قابلیت‌های این فنّاوری‌ها بیابند. این شبکه‌ها و بازیگران اغلب به دنبال تقویت ایدئولوژی‌ها و احساساتی هستند که دیدگاه‌های افراطی خشونت‌آمیز را عادی می‌کند و ممکن است دیگران را به ارتکاب جرائم تروریستی الهام یا تشویق کند.

12. https://www.coe.int/en/web/counter-terrorism/-/digital-conference-on-countering-terrorist-communications-terrorist-propaganda-public-provocation-recruitment-and-radicalisation-

13. Ban Ki-Moon

14. UN Secretary-General Ban Ki Moon, United Nations, September 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

15. Social Media, Merriam-Webster, http: //www.merriam-webster.com/dictionary/social / 20media.

16. https://press.un.org/en/2022/sc15141.doc.htm

17. UNSC Res 2462 (n. 5), para. 19.

18. UNSC Res 2482 of 19 July 2019, S/RES/2482, para. 15 (c).

19. UNGA Res 73/174 of 17 December 2018, A/RES/73/174, paras 30–31.

۲۰. لازم به ذکر است اسنادی نظیر «کنوانسیون منطقه‌ای انجمن همکاری‌های منطقه‌ای آسیای جنوبی برای سرکوب تروریسم، مصوب ۱۹۸۷»، «کنوانسیون عربی در مورد سرکوب تروریسم، مصوب ۱۹۹۸»، «معاهده همکاری بین کشورهای عضو کشورهای مستقل مشترک‌المنافع در مبارزه با تروریسم، مصوب ۱۹۹۹»، «کنوانسیون سازمان کنفرانس اسلامی مبارزه با تروریسم بین‌المللی، مصوب ۱۹۹۹»، «کنوانسیون اتحادیه آفریقا راجع به پیشگیری و مبارزه با تروریسم، مصوب ۱۹۹۹»، «کنوانسیون بین آمریکایی علیه تروریسم، مصوب ۲۰۰۲»، «کنوانسیون اتحادیه کشورهای جنوب شرقی آسیا در مورد مبارزه با تروریسم، مصوب ۲۰۰۷»، «دستورالعمل جامعه اقتصادی کشورهای غرب آفریقا راجع به مبارزه با جرائم سایبری، مصوب ۲۰۰۹»، حاوی مقررات راجع به مقابله با کاربرد تروریستی از اینترنت است.

21. A/RES/59 (I), “Calling of an International Conference on Freedom of Information”, UN. General Assembly (1st sess. 1946: London and Flushing Meadow, N.Y.).

۲۲. گروه ویژه اجرای مبارزه با تروریسم (Counter-Terrorism Implementation Task Force) توسط دبیر کل سازمان ملل متحد در سال ۲۰۰۵ تأسیس شد و توسط مجمع عمومی از طریق راهبرد جهانی مبارزه با تروریسم سازمان ملل متحد با اجماع در سال ۲۰۰۶ تأیید شد. مأموریت این گروه ویژه افزایش هماهنگی و انسجام در قبال جرائم تروریستی است (https://www.un.org/victimsofterrorism/en/about/ctitf).

منابع

Barrie, Sander, “International Law in the Age of Digital Media: Reflections on History, the Neoliberal Communication Sphere, and Race”, London Review of International Law, 2022, (10) 2, 295.

Barjalizadeh, Mohammad, Jafari, Ali and Kurdi, Nahid (2018), “Investigating the role of modern media in the spread of terrorism in the international arena”, Soft Power Studies, 1 (9). [In Persian]

Buresh, Donald L (2020), “Does Digital Terrorism Really Exist?”, Journal of Advanced Forensic Sciences, 1 (1): 18-29.

Casella, R, The False Allure of Security Technologies. Social Justice, 2003, 30 (3), p. 92.

Casey, Eoghan, Digital Evidence and Computer Crime (3rd Ed.). Elsevier Inc publisher, 2011.

Douhan, Alena, “The Changing Nature of Sanctions in the Digital Age”, in: Digital Transformations in Public International Law, Angelo Jr. Golia | Matthias C. Kettemann Raffaela Kunz [Eds.], Published by Nomos, 2022, p. 129.

Malkuti, Rasool and Khalilzadeh, Mona (2022), “Legal solutions to ensure cyber security”, Media, 33 (1). [In Persian]

Doi: 10.22034/RCC.2024.2017795.1084

M.E.Kabay, A Brief History of Computer Crime: An Introduction for Students. MSIA School of Graduate Studies, Norwich University, 2008.

Mousavi, Seyyed Jamal, Rouhani Moghadam, Mohammad and Aghaei Bejestani, Maryam (2022), "Measures to prevent cybercrimes with an emphasis on police measures with a jurisprudential approach", Studies of Fiqh and Islamic Law, 14 (26). [In Persian]

Jalali, Mahmoud and Tousli-Ardakani, Saeedeh (2018), "The necessity of creating a coordinated international legal system in dealing with crimes in cyber space", Public Law Studies, 49 (4). [In Persian]

Kettemann, Matthias C., The Normative Order of the Internet, A Theory of Online Rule and Regulation Oxford: Oxford University Press, 2020.

Kettemann, Matthias C. (ed.), Navigating Normative Orders. Interdisciplinary Perspectives, Frankfurt/New York: Campus, 2020.

Kristin, Archick, "U.S.-E.U. Cooperation Against Terrorism", CRS (Dec. 1), 2014.

Kondo T, Katsenga NN, Zvidzayi T, Cybercrime and Human Rights: A case for the due process of internet criminals, Volume 6, Issue 2, 2018, p. 121.

Jarrett, Marshall and Michael W. Bailie, Prosecuting Computer Crimes; Computer Crime and Intellectual Property Section Criminal Division, Published by Office of Legal Education Executive Office for United States Attorneys, 2011, p. 21.

Odhiambo, N. A., Ochara, N. M., and Kadymatimba, A. (2018), "Structuring of the Terrorism Problem in the Digital Age: a Systems Perspective", in Open Innovations Conference, OI 2018 (Johannesburg: IEEE), pp. 148-154.

Plotnek, Jordan J and Jill Slay (2021), "Cyber Terrorism: A Homogenized Taxonomy and Definition", Computers & Security, 102: 102-145.

Weimann, Gabriel, "New Terrorism and New Media", Wilson Center Commons Lab, 2014, 1, available at http: //www.wilsoncenter.org/publication/new-terrorism-and-new-media.

Segura-Serrano, Antonio, 'Internet Regulation and the Role of International Law,' Max Planck UNYB 10 (2006), 191–272 (192).

Ronkova, Nevenka, "International Legal Framework for Media", Journal of Process Management New Technologies, 2016, 4 (2), p. 58.

Ziyai, Sidyaser (2016), "Protection of Human Rights in Cyber Space", Legal Research, 16 (31). [In Persian]

Taylor, Robert W., Eric J. Fritsch, John Liederbach (2014), Digital Crime and Digital Terrorism, Prentice Hall Press.

Yüksel, Cüneyt, "Combating Terrorist Use of the Internet and Social Media: Recommended Solutions within the Scope of International Law", Public and Private International Law Bulletin, 2020, 40 (2), p. 1092.