نفرت‌پراکنی در وب تاریک از منظر نظام بین‌المللی حقوق بشر

یاسمن صفایی[۱]

[۱]دانشجوی کارشناسی ارشد حقوق بین‌الملل، دانشکده حقوق، دانشگاه قم، قم، ایران
safaie6819@gmail.com

چکیده

وب تاریک به عنوان بخشی از اینترنت تنها از طریق فناوری‌های ناشناس‌کننده مانند تور قابل دسترسی می‌باشد. ناشناس بودن، امکانی که فناوری‌های مذکور به افراد اعطا می‌کنند، زمینه‌ای برای سوء استفاده از این فضا و نقض حقوق بشر را فراهم می‌کند. یکی از این حقوق اساسی، ممنوعیت نفرت‌پراکنی و آزادی از تحریک نفرت نژادی، مذهبی یا ملی بوده که در اسناد بین‌المللی حقوق بشر از جمله ماده ۲۰ میثاق بین‌المللی حقوق مدنی و سیاسی بر آن تاکید شده است. این حق توسط گروه‌های تندرو از جمله داعش، القاعده، نئونازی‌ها و مانند آن‌ها و همچنین افراد در این فضا مورد تجاوز قرار گرفته است. ناشناس ماندن در این فضا به گروه‌های مذکور فرصت می‌دهد تا با برقراری ارتباط ناشناس، تبلیغ ایدئولوژی‌ها و افکار، سربازگیری و پخش اخبار غلط به تحریک افراد به خشونت و نفرت بپردازند. برخی افراد نیز با استفاده از ویژگی بارز این فضا به نفرت‌پراکنی علیه افراد دیگر با نژاد، ملیت و مذهب متفاوت می‌پردازند. در چنین شرایطی، تعهد دولت‌ها به حمایت در نظام بین‌المللی حقوق بشر ایجاب می‌کند که از حقوق افراد در برابر آسیب اشخاص ثالث محافظت کنند. در این راستا، دولت‌ها موظف‌اند که با استفاده از ابزار و شیوه‌های مختلف به مقابله با فعالیت‌های این گروه‌ها و افراد در وب تاریک بپردازند.

کلمات کلیدی: وب تاریک، نظام بین‌المللی حقوق بشر، نفرت‌پراکنی، تعهد به حمایت.

۱ مقدمه

در سال ۲۰۱۱ با تصویب قطعنامه دفاع از آزادی اینترنت در شورای حقوق بشر سازمان ملل، دسترسی به اینترنت یکی از حقوق اساسی بشر اعلام شد. اینترنت فقط به آن بخش که مورد استفاده روزمره افراد است، محدود نشده و از لایه‌های مختلفی تشکیل شده‌است. وب تاریک، یکی از این لایه‌ها تنها از طریق فناوری‌های ناشناس‌کننده مانند تور قابل دسترسی می‌باشد. وجه تمایز وب تاریک از سایر بخش‌های اینترنت، ناشناسی و غیرقابل ردیابی بودن افراد در این فضا است. این ویژگی محیط ایده‌آلی برای افراد و گروه‌های تروریستی فراهم می‌کند؛ چراکه آن‌ها همیشه به‌دنبال برنامه و پلتفرم‌های جدیدتر و بهتر به منظور حفظ حضور آنلاین خود در حداکثر تعداد رسانه ممکن هستند. آن‌ها در چنین محیطی به فعالیت‌های خود از جمله جنگ روانی،

تبلیغات و فریب افکار عمومی، ترویج ایدئولوژی و عقاید خود، سربازگیری، تأمین حمایت مالی پرداخته و فارغ از ترس شناسایی و دستگیر شدن به نفرت‌پراکنی می‌پردازند. از طرفی این نوع اعمال یعنی تبلیغ برای جنگ و یا حمایت از نفرت ملی، نژادی یا مذهبی که تحریک به تبعیض، خصومت یا خشونت کند، براساس ماده ۲۰ میثاق بین‌المللی حقوق مدنی و سیاسی ممنوع شده‌است. از طرفی دیگر، آزادی بیان مندرج در ماده ۱۹ این میثاق نیز به منظور احترام به حقوق و شهرت دیگران و حفاظت از امنیت ملی، نظم عمومی، سلامت عمومی و اخلاق محدود شده و در نتیجه حقی مطلق نخواهد بود. مطابق نظام بین‌المللی حقوق بشر، دولت‌ها در مواجهه با چنین وضعیتی متعهدند از افراد و گروه‌های در معرض آسیب حفاظت کنند. درعین‌حال دولت‌ها در ایفای این تعهد نمی‌توانند دسترسی به این فضا را به‌طور کلی قطع کرده و یا به‌طور دلخواه بر سر راه این دسترسی، مانع ایجاد کنند. علت این امر در بعد دیگر این فضا قابل جستجو است. ناشناس ماندن در این فضا نه‌تنها انشعابی از حق بر حریم خصوصی است بلکه زمینه‌ای برای تحقق دیگر حقوق بشری نیز فراهم می‌کند که دولت‌ها براساس تعهد به احترام و تحقق حقوق بشر موظف به عدم مداخله در برخورداری از این حقوق و همچنین تسهیل آن می‌باشند. بنابراین حریم خصوصی و سایر حقوق بشر نباید فدای مبارزه دولت‌ها با تروریسم در فضای وب تاریک شود. برای نخستین بار در میان منابع انگلیسی و فارسی، این پژوهش به بررسی نفرت‌پراکنی در وب تاریک از منظر نظام بین–المللی حقوق بشر می‌پردازد. برای ارائه این موضوع، در بخش بعدی به مرور مقالات گذشته، در بخش سوم به تعریف وب تاریک و دسترسی به آن، در بخش چهارم نفرت‌پراکنی و تروریسم در این فضا و در نهایت در بخش پنجم به تعهدات دولت‌ها در برخورد با معضل مذکور مطابق نظام بین‌المللی حقوق بشر می‌پردازیم.

۲ مروری بر کارهای دیگران

محققین بسیاری به بحث درباره‌ی تروریسم و افراطی‌گرایی خشن در اینترنت به خصوص در فضای وب تاریک و راه‌های مقابله با آن پرداخته‌اند (Weimann, G. 2015; Pashentsev, E. and bazarkina, D. 2021; Vacca, J. 2020). این پژوهش‌ها از راه‌های جمع‌آوری داده انواع این فعالیت‌ها (Saini, K. and Bansal, D. 2019; Chen, H. 2007) تا بررسی اختصاصی هرکدام از این فعالیت‌ها و چگونگی استفاده از وب تاریک توسط گروه‌های تروریستی (Alayda, S. 2021; Topor, L. 2019) را دربرمی‌گیرد. وجه اشتراک عمده‌ی این تحقیقات، دید کیفری آن‌ها و دسته‌بندی فعالیت‌های تروریستی ذیل عنوان جرائم سایبری می‌باشد. این در حالیست که مقاله حاضر درصدد بررسی این فعالیت‌ها از دریچه حقوق بشر و در چارچوب نظام بین‌المللی آن است.

۳ وب تاریک

بررسی نفرت‌پراکنی در وب تاریک در درجه اول نیازمند آشنایی با این فضا و چگونگی دسترسی به آن خواهد بود که در ذیل به آن می‌پردازیم.

۱.۳ تعریف وب تاریک

اینترنت شامل سه بخش وب سطحی، پنهان و تاریک می‌شود. وب سطحی یا آشکار[۱] مجموعه‌ای از وب سایت‌هایی است که توسط موتورهای جست‌وجو مرسوم مانند گوگل جمع‌آوری و نمایه می‌شوند و متعاقبا از طریق مرورگرهای رایج مانند گوگل کروم[۲] در دسترس عموم قرار می‌گیرند (Chertoff, 2017: 26; Ricardo, 2011; Kaur, 2020, 2). بخش دوم، وب پنهان یا عمیق[۳]، بزرگ‌ترین بخش شبکه گسترده جهانی محسوب می‌شود (Mazi et al., 2020: 3). موتورهای جست‌وجو مرسوم اغلب برای دسترسی به سایت‌های وب سطحی از خزنده‌های وب[۴] استفاده می‌کنند. طی این فرایند، خزنده‌ها وب را جستجو و سایت‌ها را گردآوری کرده و سپس این سایت‌ها توسط موتورهای جستجو طبقه‌بندی و نمایه می‌شوند (Finklea, 2017: 5) در بسیاری از موارد یافتن داده‌های وب پنهان توسط این خزنده‌ها غیرممکن می‌باشد. علت این امر را می‌توان در نوع محتوای وب پنهان جستجو کرد که برای مثال می‌تواند شامل محتوای پویایی که در پاسخ به یک پرسش ایجاد شده، محتوای خصوصی که نیازمند دسترسی با مجوز می‌باشد و محتوای پیوند نشده، باشد (Easttom, 2018: 27). در نهایت، وب تاریک نیز از وب‌سایت‌هایی که با فناوری‌های استاندارد وب ساخته می‌شوند، شکل می‌گیرد؛ با این تفاوت که دسترسی به آن‌ها مستلزم استفاده از مرورگرهای استانداردی (مانند فایرفاکس) است که از طریق بسته‌های نرم‌افزاری ویژه مسیریابی[۵] مسیردهی شده باشند. رایج‌ترین و پرکاربردترین این نرم‌افزارها، چه برای دسترسی به وب تاریک و چه برای مرور ناشناس وب سطحی، تور می‌باشد (Gokhale, 2020: 27). بنابراین در این مقاله، تور به‌عنوان فناوری غیرقابل‌شناسایی کننده معیار در نظر گرفته‌شده و تحقیق بر پایه این شبکه صورت می‌گیرد.

۲.۳ دسترسی به وب تاریک: تور

از اواسط دهه ۹۰ میلادی، آزمایشگاه تحقیقاتی نیروی دریایی ایالات‌متحده[۶] که توسط آژانس پروژه‌های تحقیقاتی پیشرفته دفاعی پنتاگون (دارپا) تامین مالی می‌شد، در حال تحقیق و توسعه بر روی فناوری ناشناس‌کننده خود بود (McCormick, 2013: 22) این تلاش منتج به ساخت تور یا مسیریابی پیازی شد که در سال ۲۰۰۲ به‌عنوان یک نرم‌افزار منبع باز[۷] و رایگان برای استفاده عموم منتشر شد (Dingle-dine, 2004: site) تور با مخفی کردن درخواست‌های اینترنتی و عبور دادن آن‌ها از طریق چندین آدرس آی‌پی[۸] تصادفی قبل از ارتباط با مقصد در شبکه مسیریابی پیازی، امکان غیرمتصل باقی‌ماندن درخواست کاربر به او را فراهم کرده (Jacoby, 2016: 2) و درواقع هویت کاربر و موقعیت سرور را پنهان می‌کند. هر

[1] Clear Web
[2] Google Chrome
[3] Deep Web
[4] Web Crawlers
[5] special routing software packages
[6] United States Naval Research Laboratory (NRL)
[7] Open-source software
[8] Internet Protocol address (IP address)

آدرس آی‌پی که درخواست‌ها از آن عبور می‌کند، یک لایه از رمزنگاری را به سیگنال اضافه کرده که تنها خودش قادر به رمزگشایی آن می‌باشد و همین لایه‌لایه شدن وجه تسمیه این فناوری (مسیریاب پیازی) قرار گرفت (Chertoff, 2017: 27). در سال ۲۰۰۳، قابلیت میزبانی ناشناس وب تاریک نیز به این فناوری اضافه شد که در نتیجه آن علاوه بر بازدیدکننده وب، منتشرکننده سرویس‌های مخفی آن نیز ناشناس باقی می‌ماند. (Moore; Rid, 2016: 18) در حال حاضر تور توسط شرکت غیرانتفاعی پروژه تور[9] اداره شده و از طریق آژانس‌های دولتی، شرکت‌ها، سازمان‌های مردم‌نهاد و کاربران، تامین مالی می‌شود (Jacoby, 2016: 3).

۴ نفرت‌پراکنی در وب تاریک

۱.۴ نفرت‌پراکنی در حقوق بشر بین‌المللی

متون مواد ۱۹ و ۲۰ میثاق بین‌المللی حقوق مدنی و سیاسی گواهی بر این واقعیت است که اگرچه آزادی بیان «یکی از مقبول‌ترین حقوق» است، اما حق مطلق نیست و ممنوعیت‌ها و محدودیت‌هایی برای آن وجود دارد. حق داشتن عقاید بدون مداخله، یک حق مطلق است و «هیچ استثنا یا محدودیتی را مجاز نمی‌داند». تنها در بیان آنهاست که «وظایف و مسئولیت‌های خاص» و در نتیجه محدودیت‌های احتمالی ممکن است اعمال شود. هرچند دولت عضو در اعمال این محدودیت‌ها، «نمی‌تواند خود حق را به خطر بیندازد». مطابق ماده ۱۹ (۳) (ب)، هرگونه محدودیت باید توسط قانون پیش‌بینی شود و باید برای احترام به حقوق یا شهرت دیگران [ماده ۱۹(۳)(الف)]؛ یا حفاظت از امنیت ملی، نظم عمومی، بهداشت عمومی یا اخلاق تحمیل شوند.

ماده ۲۰ میثاق بین‌المللی حقوق مدنی و سیاسی «از شدیدترین محکومیت‌های سخنان مشوق نفرت‌انگیز» توصیف شده‌است، اگرچه به بیان دقیق، این ماده به‌طور کلی به «سخنان مشوق تنفرآمیز» مربوط نمی‌شود، بلکه فقط به «تحریک» مربوط می‌شود. اشاره در ماده ۲۰، هم به «تبلیغ برای جنگ» و هم به «حمایت از نفرت ملی، نژادی یا مذهبی» نشان‌دهنده شدت نفرت مورد نظر است. همچنین نگرانی خود را با نفرتی که مشروط به «تحریک به تبعیض، خصومت یا خشونت» است، توصیف می‌کند (Ghanea, 2012: 301). سخنان تنفرآمیز ممکن است شامل سخنانی باشد که از اعمال خشونت آمیز حمایت، یا به آن‌ها تهدید یا تشویق می‌کند، اما محدود به آن نمی‌شود. امروزه شبکه‌های اجتماعی و سازمان‌های بازنشردهنده سخنان محرک نفرت از فضای مجازی به‌خصوص سطوح پنهان اینترنت همچون وب تاریک استفاده می‌کنند که در نتیجه اقدامات قانونی که برای رسانه‌های دیگر مقرر شده، در این بخش ناکارآمد یا نامناسب خواهد بود. علاوه بر این، در حالی که سخنان نفرت‌پراکنی آنلاین تفاوتی ذاتی با عبارات مشابهی که به صورت آفلاین یافت می‌شود ندارد، چالش‌های عجیبی منحصر به محتوای آنلاین و مقررات آن از جمله ماندگاری، ناشناس بودن و ماهیت بین‌صلاحیتی به‌وجود می‌آورند (Gagliardone, 2015: 13).

[9] The Tor Project

۲.۴ سیر تحول به‌کارگیری اینترنت توسط تروریست‌ها

تروریست‌ها می‌خواهند پیام خود را به گروه بزرگ‌تری از مردم برسانند. آن‌ها به مخاطب جهانی برای گسترش تبلیغات، برقراری ارتباط و جذب اعضای جدید نیاز دارند و اینترنت به‌عنوان یک رسانه ارتباطی جهانی به آن‌ها امکان انجام این کار را می‌دهد (VILIĆ, 2017: 13). آن‌ها با آگاهی به این مطلب در اتخاذ و به‌کارگیری پلتفرم‌های آنلاین نوظهور سریع عمل می‌کنند. در اواخر دهه نود میلادی نوبت استفاده از وب‌سایت‌ها بود. بیش از نیمی از ۳۰ سازمانی که تحت قانون ضدتروریسم ۱۹۹۶ ایالات متحده به‌عنوان سازمان‌های تروریستی خارجی تعیین شده‌بودند، تنها یک وب‌سایت داشتند؛ درحالیکه از سال ۲۰۰۳ تا ۲۰۰۴ صدها وب‌سایت در اختیار تروریست‌ها و حامیان آن‌ها قرار گرفت (VILIĆ, 2017: 15-16). تروریست‌ها علاوه بر راه‌اندازی سایت‌های خودشان، در ادامه از قابلیت‌های تعاملی پلتفرم‌های آنلاین مانند پیام‌رسان‌های سریع، بلاگ‌ها و شبکه‌های اجتماعی مانند توئیتر و یوتیوب استفاده کردند. در نهایت با انباشته شدن دستور العمل، موعظه‌ها، سخنرانی‌ها عملا یک ویکی‌پدیای ترور ساخته‌شد. هرچند که این پایگاه داده در وب سطحی بود، به این معنا که در دسترس آژانس‌های مبارزه با تروریسم، سرویس‌های امنیتی و پلیس قرار داشت و در نتیجه نه‌تنها محتوای بارگذاری‌شده توسط آن‌ها قابل رصد بود، بلکه همچنین تلاش می‌کردند تا افرادی که این محتوا را دانلود کرده‌بودند را شناسایی کرده و حتی محتوا را تغییر داده و دست‌کاری کنند. در نهایت به دنبال بسته‌شدن مکرر شبکه‌های تروریستی در وب سطحی و دستگیری اداره‌کنندگان آن‌ها، افراد و گروه‌های تروریستی فعالیت‌های خود را به وب تاریک، شبکه‌ای ناشناس‌کننده و پنهان که به راحتی در دسترس بوده و در عین حال به‌طور کلی غیرقابل دسترس و نامرئی می‌باشد و به فرار از دستگیری و بسته‌شدن پلتفرم‌هایشان کمک می‌کند ، انتقال دادند (Weimann, 2015: 6-7). در جولای ۲۰۱۵، دفتر تحقیقات فدرال اعلام کرد که داعش برای الهام بخشیدن به حملات تروریستی در سراسر جهان از وب تاریک استفاده می‌کند. این مسئله تنها به داعش اختصاص نداشته و در سال ۲۰۱۷، در تظاهرات علیه تجمع راست‌گرایان آلترناتیو به نام «راست را متحد کنید» شخصی توسط یک سفیدپوست برتری‌طلب کشته‌شد (Katz, Stockman, 2018: site). یکی از نهادهای سازماندهی کننده این تجمع راست، سایت نئونازی دیلی استورمر[۱۰] بود. به‌دنبال این اتفاق شرکت‌هایی مانند گوگل و سایر ارائه‌دهندگان اینترنت و فناوری از دسترسی دادن به این سایت خودداری کرده و همچنین محتوای بسیاری از دیگر گروه‌های برتری‌طلب سفیدپوست و دیگر ملی-راست‌گرایان افراطی از وب سطحی حذف شد (Topor,2019: 28, 36) هرچند که به‌سرعت خانه‌ای جدید و تقریباً بدون هیچ مقرره‌ای یعنی وب تاریک را یافت.

۳.۴ چگونگی تروریسم اینترنتی

اصطلاح تروریسم سایبری اولین‌بار توسط دکتر بری کالین به‌عنوان یک حمله برنامه‌ریزی‌شده توسط تروریست‌ها بر سیستم‌های داده و کامپیوتری تعریف شده‌است. بعدها تمامی فعالیت‌های تروریستی که با استفاده از اینترنت به‌عنوان یک ابزار انجام شده‌است، در این تعریف گنجانده شد. ازاین‌رو تروریسم در وب

[10] Daily Stormer

تاریک از تبلیغات و جنگ روانی تا استفاده‌های بسیار ابزاری مانند جمع‌آوری کمک‌های مالی، سربازگیری، داده کاوی، ارتباطات و شبکه‌سازی و هماهنگی اقدامات را شامل می‌شود که در ذیل در سه دسته کلی به آن‌ها پرداخته‌ایم (Alayda et al., 2021: 3001):

- ارتباطات: تروریست‌ها برای هماهنگی و برنامه‌ریزی عملیات خود از جنبه ناشناس و مبهم وب تاریک استفاده می‌کنند. برای مثال خدمات ایمیل مرورگر تور مانند توراکس[11] و سیگینت[12] در میان جهادیون محبوب هستند، زیرا هم هویت و هم مکان خود را پنهان می‌کنند. نمونه دیگر در یک گزارش انگلیسی با عنوان «دایرةالمعارف ترور داعش» آمده‌است که به سربازهای انگلیسی داعش چگونگی استفاده از وب تاریک به‌منظور ارتباط با شبکه جهانی تروریست‌ها آموزش داده شده‌است (Weimann, 2015: 7, 11).

- ترویج: تروریست‌ها از وب تاریک برای انتشار اظهارات و همچنین ترویج ایدئولوژی‌های خود و انتشار اخبار کذب و شایعات برای تحریک خشونت و اقدامات تروریستی استفاده می‌کنند. از سایت‌های وب تاریک گروه-های برتری‌طلب سفیدپوست می‌توان به بازارها، بلاگ‌ها (سفیدپوست نجات خواهد یافت[13]، هایدن ووت[14])، انجمن‌ها (راشن هیدن انسرز[15]) و شبکه‌های اجتماعی (کانکت[16]، توربوک[17]) اشاره کرد.

- تبلیغات و وعده‌های توخالی: با هدف جذب افراد زیاد و سربازگیری آن‌ها، مخصوصا افراد کم سن و برای دریافت حمایت و منابع مالی. برای مثال می‌توان به «مبارزه‌ی اسلامی بدون برجای‌گذاشتن اثر، کمک مالی کنید»، وب‌سایتی در وب تاریک که به کمک‌های مالی برای جهاد از طریق تراکنش‌های بیت کوین دعوت می‌کند، اشاره کرد. اسناد آنلاینی مانند «بیت کوین و صدقات الجهاد» به‌منظور آموزش انجام چنین تراکنش‌هایی در وب تاریک بر روی وب‌سایت‌های این گروه‌ها قرار داده شده‌است. از این کمک‌های مالی برای انجام انواع فعالیت‌های تروریستی از جمله خرید سلاح از خود بازارهای وب تاریک استفاده می‌شود. برای مثال سلاح‌های استفاده‌شده در حملات نوامبر ۲۰۱۵ پاریس (Jenning et al., 2015) و همچنین حملات چارلی هبدو[18] از این بازارها خریداری شده‌بود (Weimann, 2015: 11-13).

[11] Torbox
[12] Sigaint
[13] White Will Survive
[14] Heidenwut
[15] Russian Hidden Answers (Скрытые Ответы)
[16] Connect
[17] Torbook
[18] Charlie Hebdo attacks

۵ تعهدات دولت در مواجهه با نفرت‌پراکنی در وب تاریک

اهمیت حقوق بشر به‌طور گسترده در نظام بین‌المللی پذیرفته شده (Shaw, 2008: 265) و شناسایی و احترام به آن نیز وظیفه‌ای همگانی است، با این حال نظام بین‌المللی حقوق بشر تکلیف اصلی را بر دوش دولت گذارده و آن را متعهد می‌داند (میرموسوی، ۱۴۰۰: ۲۶). کمیته حقوق اقتصادی،اجتماعی و فرهنگی، تعهدات دولت‌ها را به سه دسته احترام (خودداری از مداخله در برخورداری از حقوق بشر یا محدود کردن آن)، حفاظت (حفاظت از افراد و گروه‌ها در برابر نقض حقوق بشر) و تحقق (اقدام در جهت تسهیل برخورداری از حقوق بشر اساسی) تقسیم‌بندی می‌کند (Committee on Economic, Social and Cultural Rights, 1999). در مواجهه با نفرت‌پراکنی و تروریسم در وب تاریک، تعهد دولت‌ها به خصوص تعهد به حفاظت محل بحث خواهد بود که در ادامه بررسی می‌شود.

۱.۵ احترام

تعهد به احترام و رعایت نوعی تعهد منفی و در جایی است که دولت وظیفه دارد نه تنها از اقداماتی پرهیز کند که باعث محروم شدن افراد از حقوق ناشی از میثاق‌ها می‌شود، بلکه از ایجاد موانع در راه استفاده از حق هم باید خودداری کند (کریون، ۱۳۸۷: ۱۵۴). همان‌طور که اشاره شد، وب تاریک برای بهره‌مندی افراد از تعدادی حقوق بشری بستری فراهم کرده‌است و در راستای مبارزه با تروریسم، دولت نمی‌تواند بر سر راه این برخورداری «فعلی» مانع ایجاد کند و یا آن را محدود نماید، مگر در جایی که چنین اجازه‌ای تصریح شده‌باشد (De Schutter, 2010: 257). بنابراین اقدامات دولت‌ها مانند قطع دسترسی به تور یا سعی در نفوذ به آن و آشکار کردن هویت کاربران به معنای مداخله و ایجاد مانع در بهره‌مندی افراد و یا محروم کردن آن‌ها از این حقوق می‌باشد و نقض تعهد احترام محسوب می‌شود. از طرف دیگر کشورهایی که بر سر راه دسترسی به وب تاریک موانع این چنینی نگذاشته‌اند، تعهد خود را در این زمینه ایفا کرده‌اند. برای مثال درحالی‌که کشورهایی مانند ایالات‌متحده و آلمان به پشتیبانی از تور پرداخته تا جایی‌که از آن حمایت مالی می‌کنند، سایر کشورها مانند چین، روسیه و اتریش به‌شدت مخالف با آن می‌باشند.

۲.۵ تحقق

تعهد به تحقق وظیفه‌ای مثبت است و شامل دو وظیفه می‌شود: نخست فراهم‌سازی و تسهیل برخورداری از حقوق بشر و دوم تامین خدمات. ایفای این تعهد به‌موجب میثاق حقوق مدنی و سیاسی از طریق قانون‌گذاری و حفاظت نهادی از حقوق با تضمین رویه‌ای آن‌ها از راه تأسیس نهادهای قانونی لازم و دیگر اقدام‌های تقنینی، اجرایی، سیاسی و قضایی صورت خواهد گرفت. البته تعهد به تحقق موضوع اصل نسبی بودن قرار خواهد گرفت؛ دولت‌های عضو در اثربخشی به حقوق میثاق از اختیار وسیعی متناسب با توانایی‌های مالی و اقتصادی- اجتماعی‌شان برخوردار می‌باشند. اما اگر بدون دلیل موجهی این تعهدات را اجرا نکنند، ماده ۲ میثاق و همچنین حق مربوطه را نقض کرده‌اند (Nowak, 2005: 39). بر اساس تعهد مذکور، دولت‌ها باید با «تمام ابزار و وسایل مقتضی» برخورداری از حقوق بشر را فراهم کند و مبارزه با نفرت‌پراکنی در وب تاریک

نمی‌تواند توجیهی برای ایجاد مانع در دسترسی به آن باشد.

۳.۵ حفاظت

دولت‌ها نه‌تنها باید از نقض حقوق افراد در حوزه صلاحیتشان از طریق تضمین عدم ارتکاب چنین تخلفاتی از جانب مأمورین دولتی خودداری کنند (تعهد به احترام) بلکه باید همچنین درجایی که نقض این حقوق با اعمال ارتکابی طرفین خصوصی (افراد، گروه‌ها و یا اشخاص حقوقی) تهدید می‌شود، مداخله کرده (De Schutter, 2010: 365) و از حقوق افراد در برابر طرف‌های ثالث حفاظت نمایند (Nowak, 2005: 38) جایی‌که نشانه‌هایی از درخطر نقض بودن حقوق افراد وجود داشته یا موقعیتی وجود دارد که چنین خطری را ایجاد می‌کند، دولت باید اقدامات پیشگیرانه‌ای انجام دهد تا عدم تحقق این خطرات را در بالاترین حد ممکن تضمین کند. زمانی‌که اقدامات صورت‌گرفته مؤثر واقع نشده و بازیگران غیردولتی مرتکب نقض شده‌اند، مقامات دولتی نباید منفعل باقی بمانند؛ چراکه متعهدند جبران‌های مؤثری برای افرادی که حقوقشان نقض شده تضمین کنند و همچنین در موارد معینی برای متخلف مجازات‌های کیفری یا اداری در نظر گیرند (De Schutter, 2010: 365). گاهی میثاق چنین اقداماتی را به‌صراحت تجویز می‌کند از جمله در مورد ممنوعیت تبلیغ برای جنگ یا طرفداری از نفرت ملی، نژادی یا مذهبی مطابق ماده ۲۰.

۴.۵ دولت و ایفای تعهد به حفاظت

تعهد دولت به حفاظت از حقوق افراد در برابر اشخاص ثالث از جمله کسب‌وکارهای مختلف به شکل جامع و دقیقی در قالب ده اصل در اصول راهنما سازمان ملل در کسب‌وکار و حقوق بشر گنجانده شده‌است (Ruggie, 2011: 29). همچنین پروژه فناوری بی[19] در سال ۲۰۱۹، توسط حقوق بشر سازمان ملل راه‌اندازی شد. این پروژه تعهد حفاظت دولت در برابر شرکت‌های فناوری را بر اساس اصول راهنمای سازمان ملل در پنج اصل بیان می‌کند. دولت‌ها در برابر شرکت پروژه تور به‌عنوان یک شرکت فناوری، موظف به اجرای این اصول و درنتیجه ایفای تعهد حفاظتی خود می‌باشند. ازآنجایی‌که اصول راهنمای سازمان ملل در مورد شرکت‌های فراملی و سایر واحدهای کسب‌وکار می‌باشد، رفع دو ابهامی که ممکن است درباره شرکت پروژه تور ایجاد شود، ضروری به‌نظر می‌رسد. پرسش اولی که ممکن است مطرح شود، این خواهد بود که این شرکت فراملی نیست. در پاسخ باید گفت که اصول راهنما صرفاً درباره شرکت‌های فراملی نبوده و شرکت‌های غیرفراملی که ویژگی این نوع شرکت‌ها را داشته باشند مانند بیشتر شرکت‌های فناوری تحت شمول این اصول قرار خواهند گرفت. در درجه دوم به‌حساب آوردن یک پروژه غیرانتفاعی به‌عنوان یک واحد تجاری می‌تواند سوال‌برانگیز باشد. در پاسخ می‌توان به اصل چهاردهم اصول راهنما اشاره کرد که تصریح می‌کند این اصول فارغ از ساختار واحد به آن اعمال می‌شود.[20]

[19] B-Tech Project
[20] Guiding Principles on Business and Human Rights

۵.۵ شرکت‌های فناوری و حقوق بشر

احترام و پاسداری از حقوق بشر وظیفه‌ای همگانی است؛ با این وجود در نظام بین‌المللی حقوق بشر، نقض تعهدات حقوق بشری از سوی اشخاص اعم از حقیقی یا حقوقی عموماً قابل تعقیب و مجازات نیست. در سال‌های اخیر کوشش‌هایی برای شناسایی مسئولیت فردی در نظام بین‌المللی حقوق بشر درحال انجام است. کمیسیون حقوق بین‌الملل در پیش‌نویس جرایم علیه صلح و امنیت نوع بشر، نقش مسئولیت فردی را به‌عنوان ضمانت اجرای حقوق‌بشر مورد توجه قرار داده‌است. این کمیسیون در سال ۱۹۹۱ پیشنهاد کرد نقض‌های نظام‌مند حقوق بشر جرم بین‌المللی تلقی شود و ارتکاب‌کنندگان مسئول شناخته‌شوند (براونلی، ۱۳۹۶: ۴۳۷). افزون بر این گام‌هایی برای پدیدآوردن پیش‌نویس اعلامیه مسئولیت‌های اجتماعی بشری و هنجارهای مربوط به مسئولیت‌های شرکت‌های فراملی و سایر بنگاه‌های تجاری در خصوص حقوق بشر برداشته شده‌است (میرموسوی، ۱۴۰۰: ۴۸). همان‌طور که پیش‌تر بیان کردیم این تلاش‌ها منجر به تدوین اصول راهنمای سازمان ملل در کسب‌وکار و حقوق بشر شد. این اصول درباره‌ی مسئولیت شرکت‌های خصوصی در احترام به حقوق بشر الزام‌آور نبوده اما در سال ۲۰۱۱ توسط شورای حقوق بشر به تایید و امضا رسید و در سال‌های اخیر نیز توسط تعدادی از دولت‌ها به‌تصویب رسیده و در حال اجرایی شدن است.[۲۱]

۶ نتیجه‌گیری

تروریسم در دارک وب یکی از خطرناک‌ترین نقض‌های حقوق بشر محسوب می‌شود و می‌تواند به همان اندازه و چه‌بسا پرگزندتر از تروریسم غیراینترنتی باشد. سازمان‌های تروریستی، افراد و گروه‌های افراطی و نفرت‌پراکن به‌منظور حفظ بقا و فعالیت‌های خود همیشه در پی به‌روزترین و کاربردی‌ترین ابزار بوده‌اند و با پیدایش اینترنت با سوءاستفاده از ویژگی‌های متمایز آن اهداف خود را محقق ساخته‌اند. در واکنش به خطر شناسایی شدن و دستگیری از طریق وب سطحی، این افراد و سازمان‌ها فعالیت‌های خود را به غارهای مجازی وب تاریک انتقال داده و این‌بار با سوءاستفاده از امتیازات این فضا یعنی ناشناسی و نامرئی بودن به نفرت‌پراکنی و تحریک عموم به خشونت، دشمنی و تبعیض می‌پردازند. در مقابله با آن، تعهد دولت به حفاظت از حقوق بشر ایجاب می‌کند تا به مبارزه با این افراد و گروه‌ها بپردازد. جزئیات ایفای این تعهد در اصول راهنمای سازمان ملل تشریح شده که می‌تواند راهگشای خوبی در رسیدن به این هدف محسوب شود. علاوه‌براین، اینترنت شبکه بین‌المللی از کامپیوترها است بنابراین همکاری بین‌المللی برای اثرگذاری کامل اقدامات دولت‌ها ضروری به‌نظر می‌رسد. همچنین روش‌ها و فناوری‌هایی توسط متخصصین حوزه علوم کامپیوتری برای شناسایی موردی تروریست‌ها، تحلیل و بررسی فعالیت‌ها و داده‌ها در این فضا تهیه و ساخته شده‌است. برای مثال می‌توان به ممکس[۲۲] به‌عنوان یکی از این فناوری‌ها اشاره کرد که با هدف روشن‌سازی فضای وب تاریک و کشف الگوها و روابط در داده‌های آنلاین به‌منظور یاری‌رسانی به مجریان قانون و دیگران برای ردیابی فعالیت‌های غیرقانونی ساخته

[21] https://documentsddsny.un.org/doc/RESOLUTION/GEN/G11/144/71/PDF/G1114471.pdf

[22] Memex

شده‌است. این فناوری در اصل برای رصد قاچاق انسان در وب تاریک ساخته شده اما همان اصول را می‌توان تقریباً برای هر نوع فعالیت غیرقانونی در این فضا اعمال کرد. نکته‌ای که توجه به آن بسیار اهمیت دارد این است که درعین دفاع از جامعه در برابر تروریسم، این فرآیند نباید منجر به نابودی کیفیات و ارزش‌هایی شود که در وهله اول آن جامعه را قابل دفاع می‌سازد. اینترنت و وب تاریک به طرق متعددی دربرگیرنده ایده‌آل‌های دموکراتیک آزادی بیان و ارتباطات آزاد می‌باشند. اما اگر به‌خاطر ترس از حملات تروریستی، آزادی خود در استفاده از اینترنت را محدود کنیم درواقع به تروریست‌ها پیروزی را تقدیم کرده و دموکراسی را نادیده گرفته‌ایم. در این راستا، دفتر کمیساریای عالی سازمان ملل با انتشار گزارشی، رمزگذاری داده‌های دیجیتال و ناشناس ماندن ارتباطات در دنیای آنلاین را ضرورتی انکارناپذیر برای تامین آزادی بیان و حقی جهان‌شمول دانسته و از همه دولت‌ها خواسته‌است تا با حفظ این حق، پاسخ‌گوی مقتضیات عصر دیجیتال باشند. چارچوب قانونی برای حمایت از تحقیقات جنایی و همکاری متقابل کشورها در این فضا ضروری است چراکه تحقیقات، اغلب با نقض گسترده حریم خصوصی اشخاص انجام می‌شود و دولت‌ها از ابزارهایی که در قانون شناسایی نشده استفاده می‌کنند. بنابراین سیاست‌های حاکم بر وب تاریک ضمن شناخت صحیح از این فضا باید بتواند میان حریم خصوصی اشخاص و مسئولیت دولت‌ها بر توقف فعالیت‌های مجرمانه تعادل برقرار کند تا از این طریق دولت‌ها علاوه بر ایفای تعهد خود به حفاظت از حقوق بشر، تعهد به احترام و تحقق این حقوق را نیز رعایت کنند.

مراجع

[۱] براونلی، یان، اصول حقوق بین‌الملل عمومی، ترجمه حبیبی مجنده، محمد، ویرایش هشتم، انتشارات دانشگاه مفید، قم، ۱۳۹۶.

[۲] میرموسوی، سیدعلی، «تعهد و مسئولیت های دولت در برابر حقوق بشر»، حقوق بشر، دوره ۱۶، شماره ۱، ۲۶-۵۱، ۱۴۰۰.

[3] O. De Schutter, International Human Rights Law: Cases, Materials, Commentary, Cambridge: Cambridge University Press, 2010.

[4] M. Nowak, U.N. Covenant on Civil and Political Rights – CCPR-Commentary, 2nd ed., Germany: N.P. Engel Publishers, 2005.

[5] M. Shaw, International law, Cambridge: Cambridge University Press, 2008, p. 265.

[6] M. Chertoff, “A public policy perspective of the Dark Web,” Journal of Cyber Policy, vol. 2, pp. 26-38, 2017.

[7] R. Dingeldine, “TOR: The second-generation Onion Router,” Journal of Management Information Systems, vol. 18, pp. 303-319, 2014.

[8] K. Finklea, “Dark Web,” Congressional Research Service, Mar. 2017.

[9] I. Gagliardone, D. Gal, T. Alves ,and G. Martinez, Countering Online Hate Speech, Paris: UNESCO, 2015.

[10] N. Ghanea, “The concept of racist hate speech and its evolution over time,” Paper presented at the 81st session of the United Nations Committee on the Elimination of Racial

Discrimination's Day of thematic discussion on Racist Hate Speech, Geneva, Aug. 2012, p.301.

[11] S. Kaur, S. Randhawa, "Dark Web: A web of crimes," Wireless Pers. Commun. vol. 112, pp. 2131–2158, 2020.

[12] S. Alayda et. al., "Terrorism on dark web," Turkish Journal of Computer and Mathematics Education, vol. 12, pp. 3000-3005, Apr. 2021.

[13] L. Topor, "Dark hatred: antisemitism on the dark web," Journal of Contemporary Antisemitism, vol. 2, pp. 25-42, Dec. 2019.

[14] G. Weimann, "Going dark: terrorism on the dark web," Studies in Conflict and Terrorism, vol. 39, pp. 195-206, Dec. 2015.

[15] V. Vilić, "Dark Web, cyber terrorism and cyber warfare: dark side of the cyberspace," Balkan Social Science Review, vol. 10, pp. 7-25, Dec. 2017.

[16] J. Ruggie, "Guiding principles on business and human rights: implementing the United Nations 'protect, respect and remedy' framework," Netherlands Quarterly of Human Rights, vol. 29, pp. 224-253, 2011.