مجله حقوقی بین‌المللی/ شماره ۵۲/ بهار ـ تابستان ۱۳۹۴/ صفحات ۲۵۴ ـ ۲۲۷

جایگاه حقوق بشر در مبارزه با سایبرتروریسم

غلامعلی قاسمی*

سجاد باقرزاده**

چکیده

با گسترش ارتباطات، تبادل اطلاعات از طریق ابزارهای کارآمد با حداکثر سرعت، دقت و با صرف کمترین وقت و هزینه، ضروری است. فضای مجازی این نقش را به‌خوبی ایفا کرده است اما به‌طور حتم، چنین فضای پرمخاطبی، مخاطرات پیچیده‌ای را نیز به دنبال دارد. سایبرتروریسم، یکی از این مخاطرات و از اشکال تروریسم بین‌المللی است که به‌منظور دستیابی به اهداف خود، امکان آسیب‌رسانی جدی به سامانه‌های زیرساختی و حیاتی کشور مورد هدف، ایجاد تهدیدات هسته‌ای یا هر چیزی که قابلیت تبدیل‌شدن به سلاح کشتار جمعی را داشته باشد، در بردارد. از سوی دیگر، ازآنجایی‌که رعایت حقوق بشر به‌ویژه تأمین حق آزادی و امنیت فردی، حتی برای متهمین و مجرمین تروریستی ازجمله وظایف ذاتی دولت‌ها است، در مبارزه با تروریسم، دولت‌ها برای مراقبت از منافع عمومی، محدودیت‌هایی وضع می‌کنند که نقض آن، تجاوز به حریم خصوصی اشخاص محسوب می‌شود. بااین‌حال، تعهد و تکلیف دولت به‌منظور حفظ و حمایت از حقوق عمومی، نه‌تنها وظیفه هر دولتی است، بلکه ملاکی برای سنجش میزان پایبندی دولت‌ها در تعهد به پیشگیری از وقوع نقض حقوق بشر نیز محسوب می‌شود. مسلماً دولت‌ها نیز در اعمال این حقوق و تکالیف، محدودیت‌هایی دارند.

واژگان کلیدی

حقوق بشر، سایبرتروریسم، فضای مجازی، حق آزادی و امنیت، حریم خصوصی ارتباطات

* استادیار دانشکده حقوق دانشگاه قم g-ghasemig@yahoo.com

** نویسنده مسئول، دانشجوی دکتری حقوق بین‌الملل دانشگاه آزاد اسلامی، واحد علوم‌وتحقیقات تهران
bagherzadeh9920@yahoo.com

مقدمه

یکی از بدیهی‌ترین حقوق شناخته‌شده بشر، حق آزادی و امنیت است و بالتبع، بخشی لاینفک از اسناد حقوق بشری محسوب می‌شود. دولت‌ها نیز همواره علاوه‌بر اسناد جهانی و منطقه‌ای در قوانین داخلی خود، بر لزوم شناسایی و احترام به این حقوق تأکید دارند.[۱] بااین‌حال، سایبرتروریسم که گونه‌ای نوین از تروریسم بین‌المللی بوده و تهدیدی جدی برای بشریت محسوب می‌شود، موجب شده است که دولت‌ها محدودیت‌هایی را برای تأمین این حقوق به‌وجود آورند؛ بدین معنا که همه اشخاص با بهره‌مندی از آزادی، در برابر دخالت‌های غیرقانونی و خودسرانه، مصون هستند. این مصونیت در زمینه تعقیب کیفری و نیز دیگر حوزه‌ها که دولت بر آزادی افراد، تأثیر می‌گذارد، قابل اعمال است. بخشی از تلاش‌های دولت برای مبارزه با تروریسم، عملاً منجر به اتخاذ اقداماتی می‌شود که بر حق آزادی افراد، تأثیرگذار است. برای نمونه می‌توان به اصول محاکمه در جرایم تروریستی، مشتمل بر مقررات مرتبط با قرار تأمین و نگهداشت افراد در بازداشت تا شروع محاکمه اشاره کرد.[۲]

از سوی دیگر، شروع هزاره سوم میلادی با اَشکال جدیدی از تروریسم بین‌المللی همراه بوده است. *کوفی عنان*، دبیرکل پیشین سازمان ملل در گزارش خود با عنوان «ما مردمان در آستانه هزاره سوم میلادی»، دو نوع رهایی عمده را برای مردمان جهان مطرح کرد: رهایی از خواسته و رهایی از ترس؛ به این امید که پیامدهای کوشش‌های بین‌المللی بتواند موجب رهایی از خواسته‌ها و نیازهای بشر ـ که ابعاد اقتصادی، اجتماعی، سیاسی و فرهنگی دارد ـ و رهایی مردم از ترس و خطر جنگ بشود. به‌نظر می‌آید که در حال حاضر، ترس از وقایع تروریستی، بیشتر از هر ترس دیگر در عرصه بین‌المللی وجود دارد.[۳]

اگرچه مبارزه جامعه جهانی علیه تروریسم، پیش از تأسیس سازمان ملل آغاز شد، تردیدی نیست که با وقوع حوادث یازدهم سپتامبر ۲۰۰۱ علی‌رغم ابهامات موجود، پس از تجربه شیوه جدیدی از نقض قواعد بنیادین حقوق بشر، رویکرد دولت‌ها نیز در مبارزه با تروریسم، دچار تغییرات اساسی شد، چرا که دولت‌ها دریافتند حتی در مسافرت هوایی، تروریست‌ها با استفاده از فضای مجازی به‌راحتی امکان اطلاع از تعداد نفرات و مشخصات مسافرین پرواز، کنترل و هدایت هواپیما و ... را خواهند داشت. لذا ابهاماتی را در سطح جوامع مطرح ساخت که آیا واقعاً

---

۱. برای مثال می‌توان به قانون اساسی جمهوری اسلامی ایران اشاره کرد که در ذیل فصل حقوق ملت به‌تفصیل به این موضوع پرداخته است.

2. Office of the United Nations High Commissioner for Human Rights (OHCHR), "Human Rights, Terrorism and Counter-terrorism", United Nations, 2008, p. 36.

۳. مصفا، نسرین؛ سخنرانی با عنوان «مقابله با تروریسم و حقوق بشر» در همایش *تروریسم و دفاع مشروع از منظر اسلام و حقوق بین‌الملل*، انتشارات مرکز مطالعات توسعه قضایی و دانشکده علوم قضایی و خدمات اداری، ۱۳۸۰، ص ۱۹۷.

امکان وقوع حوادث تروریستی از طریق فضای مجازی (سایبرتروریسم) وجود دارد؟ عکس‌العمل دولت‌ها درمقابل اقدامات احتمالی سایبرتروریسم که منجر به نقض تعهدات حقوق بشری می‌شود، با چه ماهیت حقوقی توجیه‌پذیر است؟ پاسخ منطقی به سؤالات یادشده، مستلزم شناختی جامع از سایبرتروریسم و حقوق و تکالیف دولت‌ها برای مبارزه با این پدیده در پرتو قواعد حقوق بشری است.

۱. پیدایش سایبرتروریسم

در دهه ۱۹۸۰ *بری کالین*،[۴] محقق و کارشناس سازمان امنیت و جاسوسی امریکا، اصطلاح تروریسم سایبری را از تلفیق دو واژه فضای سایبر و تروریسم ابداع کرد. این اصطلاح، تعریف و روش واحدی ندارد و از طرف دیگر، برخی موانع در تعریف آن مشاهده می‌شود. *ایمبار- سدون*[۵] درمورد این موانع توضیح می‌دهد که بحث تروریسم سایبری در رسانه‌های عمومی بسیار مطرح شده است و بیشتر بر دسته‌بندی آن تمرکز داشته‌اند تا ارائه تعریف عملیاتی آن.[۶] بااین‌حال می‌توان با بررسی اصطلاحات فضای سایبر و تروریسم به درک جامعی از مفهوم سایبرتروریسم دست یافت.

۱ـ۱. مفهوم فضای سایبر

امروزه اصطلاح «فضای سایبر»، اغلب برای اشاره به شبکه‌ای به‌کار می‌رود که میان مردم به‌عنوان اینترنت شناخته می‌شود. اما تعریف فضای سایبر، فراتر از اینترنت است زیرا هر تعامل یا اتفاقی که در جهان «واقعی» به وقوع نپیوندد، در فضای مجازی (سایبر) رخ می‌دهد.[۷] به عقیده برخی، فضای سایبر، شبکه جهانیِ به‌هم‌پیوستهٔ رایانه‌ها و سامانه‌های ارتباطی است.[۸] فضای سایبر می‌تواند به‌عنوان شبکه به‌هم‌پیوستهٔ جهانی از اطلاعات دیجیتال و زیرساخت‌های ارتباطی، شامل اینترنت، شبکه‌های مخابراتی، سامانه‌های رایانه‌ای و اطلاعات موجود در آن تعریف شود.[۹] دولت‌هایی همچون ایالات متحده، استرالیا، آلمان، هلند، انگلیس و سازمان‌هایی همچون اتحادیه

---

4. Barry Callin

5. Embar-Seddon

۶. عاملی، سیدسعیدرضا؛ *رویکرد دوفضایی به آسیب‌ها، جرایم، قوانین و سیاست‌های فضای مجازی*، امیرکبیر، ۱۳۹۰، ص ۲۳۷.

7. Fenz, Stefan, *Cyberspace Security: A Definition and a Description of Remaining Problems*, University of Vienna - Institute of Government & European Studies, 2005, p 3.

8. Janczewski, Lech J. Andrew M. Colarik, "Cyber Warfare and Cyber Terrorism", *Information Science Reference*, 2007, p. 33.

9. Nils, Melzer, "Cyberwarfare and International Law", *The United Nations Institute for Disarmament Research (UNIDIR) Resources*, 2011, p.4.

اروپا، اتحادیه استانداردسازی مخابرات بین‌المللی،[10] هریک اقدام به ارائه تعریفی از فضای سایبر کرده‌اند. اگرچه در این تعاریف، تفاوت‌هایی وجود دارد، نقطه مشترک همه آن‌ها «مجازی»بودن فضای سایبر است.

۱ـ۲. مفهوم تروریسم

باوجود اشتراک نظر دولت‌ها در مبارزه با تروریسم و علی‌رغم اینکه شورای امنیت در قطعنامه‌های متعدد به ضرورت مبارزه دولت‌ها و سازمان‌های بین‌المللی با تروریسم اشاره کرده است،[11] در اسناد بین‌المللی، تعاریف متفاوتی از تروریسم شده است. برخی از این تعاریف، صرفاً در زمینه بیان مصادیق و جرم‌انگاری برآمده و برخی دیگر به بیان تعاریف کلی روی آورده‌اند. بااین‌حال، برخی معتقدند: «تروریسم، بیشتر بر اساس ماهیت کار تعریف می‌شود تا هویت مرتکبان یا ماهیت هدف آن‌ها. فعالیت‌های همه تروریست‌ها شامل خشونت یا تهدید به خشونت بوده و اغلب با تقاضا همراه است. خشونت، اساساً علیه هدف‌های غیرنظامی صورت می‌گیرد و انگیزه آن‌ها سیاسی است و فعالیت‌ها به شیوه‌ای انجام می‌شود که به عمومیت بالایی دست پیدا می‌کند. این افراد، عموماً اعضای گروه‌های سازمان‌یافته هستند و اغلب مدعی‌اند که فعالیتشان مشروع است. همین طور این کار با هدف اثرگذاری ورای آسیب فیزیکی انجام می‌شود».[12]

اولین سند بین‌المللی که در جهت مقابله با تروریسم تنظیم شده، کنوانسیون پیشگیری و مجازات تروریسم، مورخ ۱۶ نوامبر ۱۹۳۷ است که ۲۴ دولت آن را امضا کردند و فقط یک دولت تصویب کرد. لذا هرگز به مرحله اجرا نرسید. در این کنوانسیون، تعریف جامعی از تروریسم ارائه نشده، لیکن در بند ۲ ماده ۱ آمده است: (در این کنوانسیون، عبارت «اعمال تروریستی» به اعمال جنایی اطلاق می‌شود که علیه دولتی به قصد ایجاد ترس در اشخاص خاص یا گروهی از اشخاص یا افکار عمومی ارتکاب یابد). در کمیسیون حقوق بین‌الملل در سال ۱۹۹۵ در بند ۲ ماده ۲۴ طرح کد (قانون) جنایات علیه صلح و امنیت بشری، تروریسم بین‌المللی این‌گونه تعریف شد: اعمال زیر، تروریسم بین‌المللی محسوب خواهد شد: تصدی، سازماندهی، فرمان‌دادن، تسهیل، تأمین مالی، تشویق یا اداره اعمال خشونت‌آمیز علیه دولتی دیگر که متوجه اشخاص یا اموال باشد و از چنین طبیعتی برخوردار باشد که یک وضعیت ترور، «ترس، وحشت» در تشکل‌ها

10. International Telecommunication Union- Standardization (ITU-T).

۱۱. ن.ک: قطعنامه‌های ۱۲۶۷ (۱۵ اکتبر ۱۹۹۹)، ۱۳۳۳ (۱۹ دسامبر ۲۰۰۰)، ۱۳۶۳ (۳۰ ژوئیه ۲۰۰۱)، ۱۳۸۸ (۱۵ ژوئن ۲۰۰۲)، ۱۳۹۰ (۱۶ ژوئن ۲۰۰۲)، ۱۴۵۲ (۲۰ دسامبر ۲۰۰۲)، ۱۴۵۵ (۱۷ ژوئن ۲۰۰۳)، ۱۴۵۶ (۲۰ ژوئن ۲۰۰۳)، ۱۵۲۶ (۳۰ ژوئن ۲۰۰۴)، ۱۵۶۶ (۸ اکتبر ۲۰۰۴)، ۱۶۱۷ (۲۹ ژوئیه ۲۰۰۵)، ۱۶۹۹ (۸ اوت ۲۰۰۶)، ۱۷۳۰ (۱۹ دسامبر ۲۰۰۶)، ۱۷۳۲ (۲۱ دسامبر ۲۰۰۶).

۱۲. عاملی؛ *همان*، ص ۲۳۶.

یا اشخاص عمومی یا افکار عمومی ایجاد کند تا دولت را به اعطای منافع یا عمل به روش خاص وادارد.[۱۳]

آنچه بیان آن مهم به نظر می‌رسد این است که هنگام به‌کارگیری معنای تروریسم، نباید در مشروعیت مبارزات جنبش‌های آزادی‌بخش ملی شک کرد و اقدامات آنان را در زمره اعمال تروریستی قلمداد نمود. مجمع عمومی سازمان ملل در سال ۱۹۸۹ قطعنامه‌ای با اجماع[۱۴] به تصویب رساند که از جهاتی دارای اهمیت است: نخست اینکه ضمن تأکید بر حق غیرقابل‌نقض «تعیین سرنوشت و استقلال همه ملت‌هایی که تحت استعمار رژیم‌های نژادپرست و دیگر اشکال سلطه بیگانگان و اشغال خارجی به‌سرمی‌برند»، مشروعیت مبارزات آنان به‌ویژه مبارزه جنبش‌های آزادی‌بخش ملی را تأیید می‌کند. این قطعنامه دربردارنده حکم مهم دیگری نیز هست و آن اینکه تمامی اقدامات تروریستی را محکوم می‌کند و چنین اقدامی را توسط هر کس و در هر جا که ارتکاب یابد توجیه‌ناپذیر می‌داند.[۱۵]

یکی دیگر از تعاریف تروریسم در بند ۱ ماده ۲ کنوانسیون بین‌المللیِ سرکوب حمایت مالی از تروریسم[۱۶] آمده است: الف- هر فعلی که منجر به وقوع جرم در قلمرو کنوانسیون یا بر اساس تعاریف یکی از معاهدات ضمیمه این کنوانسیون، جرم تلقی شود؛ یا، ب- انجام هر فعل به قصد کشتار یا ایراد صدمات جسمانی شدید به غیرنظامیان یا دیگر افراد که به‌طور مؤثر، حین مخاصمات مسلحانه، در عملیات جنگی شرکت نداشته باشند، مشروط بر اینکه هدف چنین اقدامی با توجه به ماهیت یا پیش‌زمینه آن، ترساندن جامعه باشد، یا به این قصد صورت گیرد که دولت یا سازمان بین‌المللی را به انجام یا ترک عملی وادار کند. همچنین بر اساس بندهای چهارم و پنجم این ماده، شروع به جرم، شرکت، هدایت یا دستور ارتکاب جرایمِ موضوع بند ۱ نیز در زمره جرایم تروریستی به‌شمار می‌آید.

تعریف فوق‌الذکر، یکی از جامع‌ترین تعاریف است به‌نحوی‌که در برخی از دیگر اسناد بین‌المللی، همچون قطعنامه ۱۵۶۶ شورای امنیت، مجدداً به‌کار رفته است. صرف‌نظر از تعاریف مورد اشعار، تعداد قابل‌توجهی کنوانسیون بین‌المللی برای برخورد با ابعاد مختلف تروریسم منعقد شده است، اما در تمامی این اسناد، تعریف مندرج از تروریسم، موضوع محوری و خاص است.

---

۱۳. سلیمی، صادق؛ *جنایات سازمان‌یافته فراملی*، صدرا، ۱۳۸۲، صص ۴۲ و۴۳.

14. Consensus

۱۵. قربان‌نیا، ناصر؛ «چالش‌های کمک‌های بشردوستانه در دوران جنگ بر ضدتروریسم» در *مجموعه مقالات موضوعی کتاب چالش‌های کمک‌های بشردوستانه در خاورمیانه*، مجری طرح: نسرین مصفا، انتشارات وزارت امور خارجه، ۱۳۸۶، ص ۱۲۵.

16. International Convention for the Suppression of the Financing of Terrorism, 9 December 1999,UN. Doc. A.RES.54.109.

بنابراین تعریف جهانی تروریسم از آن‌ها استنباط نمی‌شود.[۱۷] بااین‌حال به‌نظر می‌رسد، نبود خط‌مشی مشترک میان دولت‌ها در بیان تعریفی واحد از واژه تروریسم، نه از روی تغافل و ناآگاهانه، بلکه کاملاً تعمدی و آگاهانه است تا در صورت مواجهه با هر اتفاقی، امکان انطباق آن را با تعاریف باز و گستردهٔ موجود از واژه تروریسم برای رسیدن به مقاصد خاص سیاسی داشته باشند. به عبارت دیگر، درحالی‌که غالباً اعمال تروریستی را گروه‌های مختلف با انگیزه‌های گوناگون انجام می‌دهند، دولت‌ها و سران حکومت‌ها نیز در بسیاری موارد از آن به‌عنوان ابزاری برای کنترل و سلطه استفاده می‌کنند. بهانه اتخاذ اقدامات ضدتروریستی می‌تواند برای توجیه اعمالی که در دستورالعمل سیاسی قرار دارند، استفاده شود؛ دستورالعمل‌هایی مانند حفظ قدرت سیاسی، حذف مخالفان و سرکوب مقاومت داخلی نسبت به اشغال نظامی.[۱۸]

۱ـ۳. مفهوم سایبرتروریسم و اشکال آن

سایبرتروریسم، یکی از اشکال نوین تروریسم بین‌المللی است و همان گونه که اشاره شد، دولت‌ها در تعاریف تروریسم، غالباً به جرم‌انگاری از طریق بیان مصادیق آن پرداخته‌اند. بااین‌وصف، به‌خوبی می‌توان دریافت که سایبرتروریسم نیز به تبعیت از تروریسم، مفهومی کلی دارد. در سال ۱۹۹۷ *مارک پلیت*،[۱۹] تعریفی از سایبرتروریسم ارائه کرد که بر اطلاق این واژه بر یک حمله عامدانه با اهداف سیاسی اشاره دارد و علیه مدیریت سامانه‌های اطلاعاتی طراحی شده است و می‌تواند علیه اهدافی که در وضعیت مخاصمه نیستند، عواقب جدی وضع کند.[۲۰]

نمی‌توان تعریف بالا را تعریف دقیقی دانست زیرا ممکن است سایبرتروریسم، اهدافی غیر از «اهداف سیاسی» داشته باشد. بنابراین آنچه از تعاریف موجود به‌دست می‌آید، این است که نوع نگرش، بر تعریف واژه، تأثیرگذار است. لذا برای پی‌بردن به مفهوم سایبرتروریسم نمی‌توان به تعاریف موجود اکتفا کرد و حتی می‌توان گفت، تبیین مصادیق و روش‌های ارتکاب، از تعاریف مهم‌تر است. تروریسم سایبری شامل استفاده از روش‌های متداول هک‌کردن مانند دسترسی غیرمجاز به رایانه، ویروس‌ها، بمب‌های ایمیلی و غیره، با هدف آسیب‌رساندن است. با وابستگی بیشتر جامعه به سامانه‌های رایانه‌ای، تروریست‌های سایبری از آسیب‌پذیری این سامانه‌ها استفاده

17. Sorel, Jean-Marc Sorel, "Some Questions about the Definition of Terrorism and the Fight against Its Financing", *European Journal of International Law*, vol. 14, No. 2, 2003, p. 365.

۱۸. سیمبر، رضا؛ «تروریسم بین‌المللی؛ تهدیدات، چالش‌ها و فرصت‌های فراسوی امنیت ملی جمهوری اسلامی ایران»، در مجموعه مقالات موضوعی *امنیت بین‌الملل*، تدوین علی عبدالله‌خانی؛ مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، ۱۳۸۴، ص ۲۸۲.

19. Mark Pollitt

20. Foggetti, Nadia, "Cyber-terrorism and the Right to Privacy in the Third Pillar Perspective", *Masaryk University Journal of Law and Technology* , vol. 3, 2009, p. 366.

می‌کنند. سامانه‌های کنترل ترافیک، تسهیلات پزشکی، نظامی، امنیت عمومی و سامانه‌های ارتباطات، ازجمله حوزه‌های آسیب‌پذیر است. همچنین حملاتی که به مرگ یا صدمه جسمی منتهی می‌شود، انفجار، سقوط هواپیما، آلوده‌کردن آب یا خسارت اقتصادی شدید ازجمله موارد تروریسم سایبری است.[۲۱] این پدیده نوین، قادر است با استفاده از ابزارهای موجود در فضای سایبر، به خشونت هسته‌ای، بیولوژیکی، شیمیایی یا هر چیز دیگری که قابلیت تبدیل‌شدن به سلاح کشتارجمعی را داشته باشد، به‌منظور دستیابی به اهداف خود در همه سطوح دست بزند. این امر، تهدید جدی برای کلیه کشورها چه در سطوح محلی، ملی و بین‌المللی است، به‌طوری‌که دامنه این تهدید، حتی به کشورهایی که ظاهراً از کانون این مسئله دور هستند کشیده شده است. برای یک تروریست، سایبرتروریسم بر روش‌های فیزیکی، برتری‌هایی دارد، ازجمله می‌تواند از راه دور انجام گیرد و احتمال دستگیری توسط طرف مقابل، بسیار پایین است، هزینه آن کم است و نیازی به حمل مواد منفجره و آلات و ادوات مورد استفاده در حملات تروریستی در مأموریت انتحاری یا غیر آن ندارد. تروریست‌های سایبری در اقدام هماهنگ و گسترده در بازه زمانی مشخص می‌توانند آسیب‌های جدی به سامانه‌های زیرساختی و حیاتی کشور مورد هدف وارد آورند.[۲۲]

با توجه به مصادیق یادشده، به نظر *فرد کهن*،[۲۳] اقدامات تروریستی سایبری، روی‌هم‌رفته به چهار شیوه انجام می‌شود: الف) یورش به اطلاعات که همان دگرگونی یا ازمیان‌بردن محتوای فایل‌های الکترونیکی، سامانه‌های رایانه‌ای یا محتویات گوناگون موجود در آن‌ها است. ب) یورش به زیرساخت که بر پایه آن، مرتکب، سخت‌افزارها، پایگاه‌های عملیاتی یا برنامه‌های محیط رایانه را مختل می‌کند یا از بین می‌برد. ج) معاونت فنی در ارتکاب که عبارت است از به‌کارگیری ارتباطات الکترونیکی برای فرستادن نقشه‌ها و طرح‌ها به‌منظور انجام یورش‌های تروریستی یا تحریک به انجام آن‌ها یا توسل به سایر تسهیلات. د) افزایش یا ارتقای منابع مالی که به‌موجب آن، تروریست‌ها با بهره‌گیری از اینترنت برای خشونت سیاسی یا دیگر رفتارها، به گرفتن کمک‌های مالی افراد یا سازمان‌ها می‌کوشند.[۲۴]

در تعریفی که از تروریسم صورت پذیرفت به نظر می‌رسد حضور فرد با سلاح فیزیکی برای ارتکاب عمل ضرورت دارد، درحالی‌که در سایبرتروریسم، فرد، بدون حضور فیزیکی و با استفاده از

---

۲۱. عاملی؛ *همان*، ص ۲۳۹.

۲۲. صفوی‌کوهساره، سیدحامد؛ *قواعد حاکم بر حملات سایبری از منظر حقوق بین‌الملل*، پایان‌نامه کارشناسی ارشد حقوق بین‌الملل، دانشگاه مفید، قم، ۱۳۹۱، ص ۶۴.

23. Fred Cohen

۲۴. عالی‌پور، حسن؛ *حقوق کیفری فناوری اطلاعات*، خرسندی، ۱۳۸۹، ص ۱۱۸.

فضای مجازی اقدام می‌کند. پس آیا این‌گونه اقدامات در فضای سایبر با مفهوم تروریسم قابل‌جمع است؟

نگاهی ژرف به مقاصد و اهداف در جرایم سایبرتروریسم، هم‌پوشانی با اهداف اعمال تروریستی را به اثبات می‌رساند. به عبارت دیگر، سایبرتروریسم می‌تواند با استفاده از شبکه‌های مجازی، ایراد صدمه به زندگی بشر یا با تخریب زیرساخت‌های حیاتی ملی به زندگی بشری صدمه وارد کند. بااین‌وصف آیا سایبرتروریسم، ویژگی‌هایی مشابه با دیگر اشکال تروریسم ندارد که قبلاً به آن پرداختیم؟ اگرچه به‌طور قطع، تفاوت‌هایی میان هواپیماربایی با سلاح و هواپیماربایی از طریق اعمال کنترل بر سامانه رایانه‌ای فرودگاه وجود دارد، برای استفاده از ابزارهای حقوقی در مبارزه با سایبرتروریسم، تأسیس ماهیت حقوقی سایبرتروریسم ضرورت دارد، چرا که در مبارزه با تروریسم، این ماهیت برای جامعه جهانی مشترک است.[۲۵]

۲. نسبت تروریسم سایبری با نقض حقوق بشر

اقدامات تروریستی به‌طور جدی حق بهره‌مندی انسان از حقوق بشر را مختل می‌کند و توسعه اجتماعی و اقتصادی همه دولت‌ها را تهدید و ثبات جهانی و رفاه را تضعیف می‌کند.[۲۶] همان طور که کمیسر عالی سابق حقوق بشر سازمان ملل، خانم *مری رابینسون*[۲۷] اظهار داشت: «اساس حقوق بشر این است که زندگی انسان و کرامت وی نباید به مصالحه گذاشته شود و اعمال خاص دولت‌ها یا غیردولتی‌ها هم هرگز نمی‌تواند هدف را توجیه کند. حقوق بشر بین‌المللی و حقوق بشردوستانه، حد و مرزهایی را که در ارتباط با رفتار نظامی و سیاسی تعریف می‌کنند، دیدگاه بی‌ملاحظه نسبت به زندگی و آزادی انسانی اقدامات ضدتروریستی را زیر سؤال می‌برد».[۲۸]

بااین‌حال، سلسله اقدامات دولت‌ها برای مبارزه با تروریسم، این پرسش را مطرح می‌کند که آیا نمی‌توان اعمال صورت‌گرفته را نقض حقوق بشر محسوب کرد؟ بخصوص اینکه دولت‌ها پیشگیری از وقوع اعمال تروریستی را بهترین نوع مبارزه به حساب می‌آورند و بعضاً با نقض قواعد بنیادین حقوق بشر به‌واسطه اقدامات غیرمتعارف، در صدد تأمین امنیت خویش در چارچوب حفظ حقوق عمومی برمی‌آیند. مبنای قانونمندسازی و به عبارتی، عادی‌سازی دخالت‌ها را می‌توان پس از حوادث ۱۱ سپتامبر ۲۰۰۱ و سخنرانی معروف *جورج بوش*، رئیس‌جمهور پیشین

---

25. Cohen, Aviv, "Cyberterrorism: Are We Legally Ready?, *The Journal of International Business & Law*, 2010, p. 7.

26. See: Resolution 1566, Adopted by the Security Council at its 5053rd meeting, on 8 October 2004.

۲۷. مری رابینسون (Mary Robinson)، رئیس‌جمهور سابق ایرلند و کمیسر عالی سابق حقوق بشر سازمان ملل، از سال ۲۰۰۸ تا ۲۰۱۰ ریاست این کمیسیون را بر عهده داشت.

۲۸. بندک، ولفگانگ و آلیس مانگوپولوس؛ *تروریسم و حقوق بشر*، ترجمه: محمدجعفر ساعد و دیگران، دادگستر، ۱۳۸۹، ص ۸۷.

ایالات متحده در جلسه مشترک کنگره با مردم امریکا و استفاده از اصطلاح «یا با ما یا علیه ما»[۲۹] به‌طور ملموس مشاهده کرد. لذا پی‌بردن به رعایت یا نقض حقوق بشر، مستلزم شناخت صحیح ماهیت حقوق بشر و سپس حقوق و تکالیف دولت‌ها در مبارزه با سایبرتروریسم است.

۲ـ۱. ماهیت حقوق بشر

حقوق بشر، ارزش‌های جهانی و ضمانت‌های حقوقی است که اشخاص و گروه‌ها را در برابر هرگونه فعل و ترک‌فعل دولت‌ها که با آزادی‌های اساسی، حق بهره‌مندی از مقام و کرامت انسانی سروکار دارند، محافظت می‌کند. در یک طیف گسترده‌تر، حقوق بشر شامل احترام، حفاظت و اجرای حقوق مدنی، فرهنگی، اقتصادی، سیاسی و اجتماعی است. حقوق بشر، جهانی است. به عبارت دیگر، این حقوق به‌طور ذاتی به همه بشریت تعلق دارد و به‌هم‌پیوسته و بخش‌ناپذیر است.[۳۰]

جهان‌شمولی، مطلق‌بودن، فسخ‌ناپذیری و انتقال‌ناپذیریِ حق مندرج در قاعده حقوق بشر از اوصاف ماهوی قواعد حقوق بشر است. در رابطه با مطلق‌بودن حق مندرج در قواعد حقوق بشر می‌توان بیان داشت که برخی از قواعد حقوق بشری در زمره قواعد آمره قرار دارد. طبق ماده ۵۳ کنوانسیون ۱۹۶۹ *وین* درباره حقوق معاهدات،[۳۱] قاعده آمره، قاعده‌ای است که به‌وسیله اجماع بین‌المللی دولت‌ها به‌عنوان قاعده‌ای تخلف‌ناپذیر به رسمیت شناخته شده است. خصوصیت بارز و مهم این قواعد، ثبات نسبی آن است. این قواعد، جزء مقررات حقوق عرفی است که نمی‌توان از طریق معاهده یا توافق ضمنی از آن عدول کرد. تنها در صورتی می‌توان آن را کنار گذاشت که یک قاعده عرفی لاحق و مغایر با آن ایجاد شده باشد. حقوق‌دانانی نظیر *مک دوگال*، *لاس ول* و *چن*، قواعد حقوق بشر را به‌عنوان قواعدی که ویژگی آمره دارد، تلقی کرده‌اند. قاضی *تاناکا*[۳۲] در رأی جداگانه خود در قضیه آفریقای جنوب غربی، نظر مشابهی داشته و قواعد مرتبط با رعایت حقوق بشر را در زمره قواعد آمره دانسته است.[۳۳]

واقعیتی که در برخی از اسناد بین‌المللی حقوق بشر به رسمیت شناخته شده این است که انحراف از پاره‌ای حقوق را در شرایط اضطراری جایز دانسته است. بر اساس ماده ۴ میثاق حقوق مدنی و سیاسی: «هرگاه یک خطر عمومی استثنایی (فوق‌العاده) موجودیت ملت را تهدید

29. "Either you are with us, or you are with the terrorists".

30. OHCHR, *op. cit*, p. 3.

31. Vienna Convention on the Law of Treaties, 1969.

32. Judge Tanaka

۳۳. شریفیان، جمشید؛ *راهبرد جمهوری اسلامی ایران در زمینه حقوق بشر در سازمان ملل متحد*، انتشارات وزارت امور خارجه، ۱۳۸۰، ص ۵۷.

کند و این خطر، رسماً اعلام بشود، کشورهای طرف این میثاق می‌توانند تدابیری خارج از الزامات مقرر در این میثاق به میزانی که وضعیت حتماً ایجاب می‌کند اتخاذ نمایند، مشروط بر اینکه تدابیر مزبور با سایر الزاماتی[۳۴] که طبق حقوق بین‌الملل به عهده دارند مغایرت نداشته باشد و منجر به تبعیضی منحصراً بر اساس نژاد، رنگ، جنس، زبان، اصل و منشأ مذهبی یا اجتماعی نشود».[۳۵]

در تفسیری که کمیته حقوق بشر از این ماده به عمل آورده، مقرر شده که «هر ناآرامی یا بلایی که حیات ملت را تهدید نکند، موقعیت اضطراری عمومی نخواهد بود».[۳۶] ضمن اینکه در هنگام اوضاع‌واحوال نامساعد، اضطرار ممکن است به‌عنوان بهانه‌ای برای توجیه عدم سازگاری با تعهدات بخصوصی از حقوق بشر مورد استناد قرار گیرد. پرواضح است که اضطرار نمی‌تواند مستمسکی برای نقض حقوق فاحش بشر باشد. به عبارت دیگر، برخی از حقوق بشر، اساسی‌تر از برخی دیگر محسوب می‌شود. این موضوع را نظام حقوق بین‌الملل بشر عرفی معین می‌کند که تنها در رابطه با تعداد محدودی از حقوق، اجازه عدول یا محدودیت می‌دهد.[۳۷] البته علاوه‌بر مفهوم مخالف ماده ۴ میثاق حقوق مدنی و سیاسی، برخی دیگر از اسناد حقوق بشری همچون ماده ۱۱ کنوانسیون اروپایی حقوق بشر،[۳۸] به بخشی از حقوق بشر به‌عنوان حقوقی اشاره می‌کنند که حتی در وضعیت اضطراری نیز قابل‌تخطی نیست.[۳۹]

رأی مورخ ۳ سپتامبر ۲۰۰۸ دیوان اروپایی حقوق بشر[۴۰] در رابطه با دادخواست تجدیدنظر *یاسین عبدالله کیدی* و مؤسسه بین‌المللی *برکات* علیه شورا و کمیسیون اتحادیه اروپا[۴۱] نیز مبیّن همین امر است. رأی صادره در مرحله بدوی مربوط به ۲۱ دسامبر ۲۰۰۵ است[۴۲] که در این پرونده، شورا و کمیسیون اتحادیه اروپا، اموال خواهان را به‌خاطر ارتباط با القاعده بلوکه کردند و در توجیه این اقدامات به قطعنامه‌های شورای امنیت سازمان ملل برای الزام دولت‌ها به

۳۴. در متن انگلیسی میثاق، واژه «Obligations» درج شده که اینجا به «الزامات» ترجمه شده است، اما به نظر می‌رسد معادل‌سازی آن با واژه «تعهدات» صحیح‌تر باشد.

۳۵. امیر ارجمند، اردشیر؛ *مجموعه اسناد بین‌المللی حقوق بشر*، انتشارات دانشگاه شهید بهشتی، جلد اول، ۱۳۸۰، ص ۹۵.

36. Human Rights Committee, General Comment 29, States of Emergency (article 4), 2001, Para 3.

37. Ryngaert, Cedric, "State Responsibility, Necessity and Human Rights", *Institute for International Law*, K.U.Leuven, Working Paper No 141, 2009, p. 4.

38. European Convention on Human Rights and Fundamental Freedoms, 1950.

۳۹. در این رابطه می‌توان مواردی همچون «حق حیات»، «ممنوعیت شکنجه» و «ممنوعیت بردگی» را ذکر کرد.

40. European Court of Justice

41. *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council and Commission*, Judgment of 3 September 2008.

42. *Yusuf and Al Barakaat Foundation v Council and Case Kadi v Council and Commission*, Judgments of 21 September 2005.

بلوکه‌کردن دارایی‌ها و دیگر اسناد مالی اشخاص حقیقی یا حقوقیِ تعیین‌شده توسط کمیته تحریم‌های شورای امنیت[۴۳] در رابطه با اشخاصی که با اسامه بن‌لادن، القاعده یا طالبان همکاری دارند و نیز به مواد ۶۰، ۳۰۱ و ۳۰۸ شورای اروپا، مقررات پذیرفته‌شده شورای اروپا به شماره ۸۸۱/۲۰۰۲ و لیست ضمیمه در رابطه با بلوکه‌کردن دارایی اشخاص حقیقی و حقوقی مرتبط با شبکه القاعده استناد می‌کنند. لذا خواهان، نزد دادگاه بدوی با ادعای اینکه شورا صلاحیت پذیرش چنین مقرراتی را ندارد و اتخاذ این تدابیر، منجر به نقض حقوق بنیادین متعددی به‌ویژه نقض حق مالکیت و حق دفاع از وی شده است، طرح دعوا می‌کند. بااین‌حال، دادگاه بدوی، دادخواست وی را رد و در بیان دلیل این اقدام، چنین استدلال‌هایی را ابراز کرد: دولت‌های عضو بر اساس منشور سازمان ملل که سند بین‌المللی است و نسبت به قوانین اتحادیه رجحان دارد، ملزم به اعمال قطعنامه‌های شورای امنیت هستند و ... از سوی دیگر، رویکرد هیئت دادرسان دیوان در مرحله بدوی برای بررسی مشروعیت مقررات، صرفاً ملاحظه قوانین عام درجه بالاترِ حقوق بین‌الملل بوده است، به‌طوری‌که با این ملاحظات، یک نظام حقوق بین‌الملل عمومی بنا نهاد که دولت‌های عضو یا دادگاه‌های سازمان ملل متحد، امکان عدول از قواعد آمره را (که در این پرونده نقض نشده بود) ندارند.[۴۴]

متعاقباً خواهان، علیه قضات مرحله نخستین، نزد دیوان دادگستری اتحادیه اروپا[۴۵] اقامه دعوا کرد. دیوان اشعار می‌دارد برای بررسی جامع هر مصوبه که در صلاحیت هیئت داردسان بوده و در پرتو حقوق بنیادین قرار می‌گیرد، تصریح به یک تضمین اساسی وجود دارد که از معاهده شورای اروپا گرفته شده است. البته این حقیقت که ممکن است هیئت دادرسان، مجبور به بررسی مشروعیت یک مصوبه اتحادیه شود که به دنبال اجرای قطعنامه شورای امنیت سازمان ملل متحد است، جوازی برای عدول از آن تضمین اساسی را نمی‌دهد. لذا با تصریح اینکه دادگاه مرحله بدوی، صالح به بررسی مقررات ۸۸۱/۲۰۰۲ با توجه به قواعد آمره نبوده است، قضات مرحله بدوی را از رسیدگی معاف می‌کند. نهایتاً دیوان به ضرورت احترام مطلق به حقوق بنیادین در هنگام اعمال اختیارات اتحادیه و عدم امکان اثبات توجیه‌پذیری تحمیل چنین اقداماتی علیه خواهان اذعان می‌کند.[۴۶]

در اینجا برخی از حقوق بنیادین بشر که احتمال نقض آن در مواجهه با سایبرتروریسم متصور است بررسی می‌شود:

43. Sanctions Committee of the Security Council

44. http://ec.europa.eu/dgs/legal_service/arrets/05c402_en.pdf.

45. European Union Court of Justice.

46. *Ibid*.

الف. حق امنیت

انسان، اساس هستی است تا در این وادی، فرایند تعالی و تکاملی را که لازمه دستیابی به سعادت است، طی کرده و استعدادهای خود را به آزمون عمل بگذارد. یکی از ملزومات بنیادین حصول غایت حیات بشر در گستره کنش‌های متقابل و جمعی که خود مؤلفه‌ای تعیین‌کننده در چنین فرایندی از تعالی‌جویی و کمال‌طلبی است، «امنیت» است.[۴۷] در ماده ۲۲ اعلامیه جهانی حقوق بشر آمده است: «هرکس به‌عنوان عضو اجتماع، حق امنیت اجتماعی دارد و مجاز است به‌وسیله مساعی ملی و همکاری بین‌المللی، حقوق اقتصادی، اجتماعی و فرهنگی خود را که لازمه مقام و نمو آزادانه شخصیت اوست با رعایت تشکیلات و منابع هر کشور به دست آورد». در روابط گوناگون فردی و اجتماعی و خصوصی و عمومی انسان، ممکن است حیات مادی و معنوی افراد، جزئاً یا کلاً در معرض خطر قرار گیرد. در چنین حالتی است که وجود «امنیت» به‌عنوان تأسیس حقوقی، اخلاقی و اجتماعی برای همگان، ضرورت اجتناب‌ناپذیر خواهد داشت. امنیت، اطمینان‌خاطری است که بر اساس آن، افراد در جامعه‌ای که زندگی می‌کنند، نسبت به حفظ جان، حیثیت و حقوق مادی و معنوی خود، بیم و هراسی نداشته باشند. این تأسیس، مستلزم دو تضمین اساسی است:

- تضمین امنیت افراد درمقابل هر نوع توقیف، زندانی‌شدن، مجازات و دیگر تعرضات خودکامه و غیرقانونی حکومتی؛
- تضمین امنیت افراد از طریق حمایت‌های جامعه برای هریک از اعضای خود، به‌منظور حفظ حقوق و تعلقات و برخورداری از آزادی‌های انسانی.

با این ترتیب، امنیت برای افراد و دولت، ایجاد تکلیف می‌کند؛ بدین معنی که افراد مکلف‌اند به حقوق مادی و معنوی یکدیگر احترام بگذارند. دولت نیز مکلف است اولاً، با وضع قانون و تأسیس تشکیلات اداری و قضایی، برای مردم ایجاد امنیت کند تا با اطمینان‌خاطر زندگی کنند و ثانیاً، خود نیز در متابعت از قانون، حقوق و آزادی افراد را محترم شمارد و خودسرانه به آن تعرض نکند.[۴۸] همان گونه که در ماده ۲ کنوانسیون جرایم سایبر مصوب ۸ نوامبر ۲۰۰۱،[۴۹] آمده است: هریک از اعضا باید به‌گونه‌ای اقدام به وضع قوانین و سایر تدابیر کند که در صورت لزوم، بر اساس حقوق داخلی خود، دسترسی عمدیِ بدون حق را به تمام یا بخشی از یک سامانه رایانه‌ای جرم‌انگاری کند. اعضا می‌توانند مقرر دارند این جرم با نقض تدابیر امنیتی و به قصد تحمیل داده‌های رایانه‌ای یا سایر مقاصد ناروا یا نسبت به سامانه رایانه‌ای که با سامانه رایانه‌ای دیگری

۴۷. ولفگانگ و مانگوپولوس؛ *همان*، ص ۱۲.

۴۸. هاشمی، سیدمحمد؛ *حقوق بشر و آزادی‌های اساسی*، میزان، ۱۳۸۴، ص ۲۷۶.

49. The Council of Europe Convention on Cybercrime, Budapest, 2001.

ارتباط دارد، محقق می‌شود. مثلاً دسترسی غیرقانونی[۵۰] شامل جرمی مبنایی می‌شود که تهدیدهای خطرناک و تعرض‌ها علیه امنیت (یعنی محرمانگی، تمامیت و دسترس‌پذیری) سامانه‌ها و داده‌های رایانه‌ای را در برمی‌گیرد. نیاز به حفاظت، منافع سازمان‌ها و افراد در مدیریت، اجرا و کنترل سامانه‌هایشان را بدون وجود مزاحمت و ممانعت، بازتاب می‌دهد. صِرف تعرض غیرمجاز، یعنی «هک‌کردن»، «کرک‌کردن»، یا «ورود به‌عنف رایانه»، اصولاً و فی‌نفسه باید غیرقانونی تلقی شود. این جرایم می‌تواند مانعی برای کاربران مشروع سامانه‌ها و داده‌ها ایجاد کند و تغییرها یا تخریب‌هایی را با هزینه‌های زیاد بازسازی به‌وجود آورد. چنین تعرض‌هایی می‌تواند باعث دسترسی به داده‌های محرمانه (نظیر گذرواژه‌ها، اطلاعات راجع به سامانه‌های هدف) و اسرار برای استفاده از سامانه بدون پرداخت پول یا حتی تشویق نفوذگرها به ارتکاب اشکال خطرناک‌تری از جرایم مرتبط با رایانه شود.[۵۱] مسلماً دسترسی غیرمجاز به اطلاعات مزبور، ناقض امنیت حریم خصوصی افراد، محسوب می‌شود.

ب. حق آزادی

در ماده ۳۰ اعلامیه حقوق بشر آمده است: «هیچ‌یک از مقررات اعلامیه حاضر نباید طوری تفسیر شود که متضمن حقی برای دولتی یا جمعیتی یا فردی باشد که به‌موجب آن بتواند هریک از حقوق و آزادی‌های مندرج در این اعلامیه را از بین ببرد یا در آن راه، فعالیتی بکند». علاوه‌بر اعلامیه جهانی حقوق بشر، در بند سوم ماده ۱ و ماده ۵۵ منشور ملل متحد، بر تشویق احترام به حقوق بشر و آزادی‌های اساسی تأکید شده است. در ماده ۵۶ منشور، دولت‌ها متعهد به انجام اقدامات فردی و جمعی برای حصول آزادی‌های اساسی شده‌اند. به بیان دیگر، تقریباً در همه اسناد بین‌المللی حقوق بشریِ مهم، ازجمله منشور بین‌المللی حقوق بشر، از حق آزادی و امنیت به انحاء مختلف حمایت شده است. این حق به‌طورکلی شامل این موارد است: عدم بازداشت خودسرانه، سلب آزادی صرفاً به‌موجب قانون، حق مطلع‌شدن از علل بازداشت، حق کنترل قضایی بازداشت، حق آزمایش مشروعیت بازداشت، جبران خسارات ناشی از توقیف غیرقانونی و عدم بازداشت در اموری که صرفاً حالت مدنی دارد.[۵۲]

مشابه ماده ۳۰ اعلامیه حقوق بشر، در کنوانسیون اروپایی حقوق بشر نیز درج شده است. در ماده ۱۷ این کنوانسیون آمده است: «هیچ‌یک از مقررات این کنوانسیون نباید به‌صورتی تفسیر شود که به هیچ دولت، گروه یا شخصی به‌طور ضمنی این حق را بدهد تا فعالیت یا اقدامی انجام

50. Illegal Access

۵۱. جلالی فراهانی، امیرحسین؛ *کنوانسیون جرایم سایبر و پروتکل الحاقی آن*، خرسندی، ۱۳۸۸، ص ۲۶.

۵۲. شریفیان؛ *همان*، ص ۴۰۴.

دهد که به قصد ازبین‌بردن هریک از آزادی‌های مقررشده یا ایجاد محدودیت فراتر از مقررات کنوانسیون حاضر باشد».[۵۳]

البته اگرچه حق آزادی افراد، محترم و غیرقابل‌تعرض است، محدودیت‌هایی نیز بر آن وضع شده است. برای مثال، یکی از حقوق شناخته‌شده در اسناد حقوق بشری، حق آزادی بیان است. آزادی بیان، همواره سدی در برابر فساد قدرت محسوب شده است زیرا بدین‌وسیله، قدرت همواره در نظارت افکار عمومی قرار می‌گیرد. ازاین‌روست که آزادی بیان از پایه‌های دموکراسی واقعی شمرده شده است.[۵۴] بااین‌حال، سوءاستفاده از این حق می‌تواند مستمسکی برای مجرمین یا متهمین سایبرتروریسم برای تهدیدات صورت‌گرفته در فضای سایبر باشد. لذا محدودیت‌هایی بر آن وضع شده است.[۵۵] بر این اساس می‌توان بیان داشت: «نظام بین‌المللی حقوق بشر،[۵۶] هم به‌عنوان شمشیر و هم سپر عمل می‌کند. لذا ضرورت جرم‌انگاری (تحدیدشدهٔ) اَشکال افراطی آزادی بیان در عین اینکه از دیگر اَشکال آزادی بیان حمایت می‌کند، اجتناب‌ناپذیر است. تحریک به نسل‌کشی، تنفری که منجر به تحریک به تبعیض، دشمنی یا خشونت می‌شود، تحریک به تروریسم، تبلیغ جنگ، برخی از ممنوعیت‌های مورد نیاز دولت‌های عضو معاهدات نظام حقوق بشر برای آزادی بیان است».[۵۷]

به بیان دیگر، چندین میثاق و اعلامیه ملی و بین‌المللی، ضرورت توازن و تعادل آزادی بیان افراد با حقوق آن‌ها را مبنی‌بر رهایی از اقدامات نفرت‌انگیز که علیه آن‌ها صورت می‌گیرد شناسایی کرده است. این میثاق‌ها شامل منشور حقوق و آزادی‌های کانادا، قانون جزای کانادا، قانون حقوق بشر کانادا، کنوانسیون اروپایی حمایت از حقوق بشر، کنوانسیون رفع کلیه اشکال تبعیض‌نژادی و اعلامیه جهانی حقوق بشر است.[۵۸]

ج. حق بر حریم خصوصی ارتباطات

همان طور که در اسناد بین‌المللی ازجمله ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی ۱۹۶۶[۵۹] آمده است، حریم خصوصی افراد، مصون از تعرض غیرقانونی است. این ماده مقرر

53. European Convention on Human Rights and Fundamental Freedoms, 1950, article 17.

۵۴. کاتوزیان، ناصر و دیگران؛ *آزادی اندیشه و بیان*، انتشارات دانشکده حقوق‌وعلوم‌سیاسی دانشگاه تهران، ۱۳۸۲، صص ۱۰۴و۱۰۵.

۵۵. هیک، استیون و دیگران؛ *حقوق بشر و اینترنت*، ترجمه: سیدقاسم زمانی و دیگران، خرسندی، ۱۳۸۶، ص ۲۲۲.

56. International Human Rights Law

57. UNODC, Comprehensive Study on Cybercrime, United Nations, 2013, p. 107.

۵۸. هیک، استیون و دیگران؛ *همان*.

59. International Covenant on Civil and Political Rights, United Nations, 16 December 1966, article 17.

می‌دارد: «نباید در زندگی خصوصی، خانوادگی، خانه یا مکاتبات هیچ‌کس، مداخله خودسرانه یا خلاف قانون صورت گیرد. همچنین نباید به شرافت و حیثیت او تعرض غیرقانونی شود».[۶۰] در بند ۲ همین ماده به حق حمایت قانونی از شخصی اشاره کرده است که حریم خصوصی‌اش مورد دخالت یا تعرض خودسرانه یا خلاف قانون قرار گرفته است.[۶۱]

در این راستا می‌توان به رأی ۹ آوریل ۲۰۰۹ دیوان اروپایی حقوق بشر اشاره کرد که موضوع آن، طرح دعوای شخص (الف) علیه دولت نروژ به اتهام افترا است. در این پرونده، یکی از روزنامه‌های محلی، دو مقاله علیه (الف) نوشت که یکی از این مقالات در رابطه با تحقیقات مقدماتی پلیس از وی به اتهام قتل و دیگری تجاوز به دو دختر جوان در سال ۲۰۰۰ است. شخص مزبور با ۴۲ سال سن، سابقه حبس به علت ارتکاب قتل و ضرب‌وجرح با چاقو در پرونده‌اش داشته و به‌خاطر اینکه در محل قتل دختران دیده شد، مورد بازجویی پلیس قرار گرفت. بااین‌حال، متهم پس از ده ساعت به‌خاطر فقدان مدارک مثبتهٔ انتساب اتهام، آزاد شد. متعاقباً با تکمیل تحقیقات پلیس، دو مرد دیگر شناسایی و محکوم به ارتکاب قتل شدند. شخص (الف) نیز پس از اثبات بی‌گناهی به‌خاطر اینکه برخی از روزنامه‌های ملی و همچنین شبکه ۲ تلویزیون نروژ به این موضوع پرداخته و با علنی‌کردن جزئیاتی از سوابق و اطلاعات خصوصی او، موجب شناسایی هویتش شدند، در دیوان طرح دعوا کرد. سرانجام، دیوان به این نتیجه رسید که زیان شدیدی به اعتبار و شرف خواهان، خصوصاً به تمامیت روحی و روانی و حریم خصوصی وی در اثر نقض ماده ۸ وارد شده و او، حق دریافت خسارت را دارد.[۶۲]

مسلماً حریم خصوصی ارتباطات هم در برخورداری از چنین حمایت‌هایی مستثنا نمی‌شود. منظور از حریم خصوصی ارتباطات در معنای خاص، مصون‌بودن مراسلات و مکاتبات و مخابرات شهروندان از هرگونه تخریب، تفتیش، شنود و دستیابی غیرمجاز است.[۶۳] بر این اساس، انتظار معقول از قوای حاکم آن است که ضمن حمایت جدی از حقوق و آزادی‌های فردی، از هرگونه تعرض غیرمجاز و ناموجه نسبت به حریم خصوصی و خلوت اشخاص، به‌شدت اجتناب کنند. سوءاستفاده از قدرت برای کنترل ارتباطات و مراسلات و نیز انجام بازرسی‌های غیرضروری و بدون مجوز قانونی از مصادیق نقض حریم خصوصی شهروندان تلقی می‌شود.[۶۴]

این انتظار منطقی در بسیاری از اسناد بین‌المللی نیز تصریح شده است. در ماده ۱۲ اعلامیه

---

60. *Ibid*.

61. *Ibid*.

62. A. V. Norway, "European Court of Human Rights", Judgement of 9 April 2009, *available at:* http://sim.law.uu.nl/SIM/Dochome.nsf?Open.

۶۳. اصلانی، حمیدرضا؛ *حقوق فناوری اطلاعات*، میزان، ۱۳۸۴، ص ۲۸۹.

۶۴. آماده، مهدی؛ *حمایت از حریم خصوصی*، دادگستر، ۱۳۹۲، ص ۸۹.

حقوق بشر آمده است: «نباید در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات هیچ‌کس مداخله‌های خودسرانه شود و نباید به شرافت و اسم و رسمش حمله شود. هرکس حق دارد که درمقابل این‌گونه مداخلات و حملات، از حمایت قانون برخوردار شود»؛ یا اینکه ماده ۸ کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی مقرر می‌دارد: «۱ـ هرکس از حق احترام به زندگی خصوصی و خانوادگی، خانه و مراسلات خود برخوردار است. ۲ـ در اجرای این حق، هیچ مداخله‌ای نباید از سوی هیچ‌یک از مقامات دولتی صورت گیرد مگر مداخلات منطبق بر قانون و مواردی که در جامعه مردم‌سالار به دلایل حفظ امنیت ملی، ایمنی عمومی یا رفاه اقتصادی کشور، پیشگیری از هرج‌ومرج و جرایم، حفاظت از سلامت و اخلاقیات یا حفاظت از حقوق سایرین، ضروری تشخیص داده شود».[۶۵] همچنین در ماده ۱۱ کنوانسیون امریکایی حقوق بشر ۱۹۶۹ و در ماده ۱۸ اعلامیه اسلامی حقوق بشر نیز بر احترام به حریم خصوصی تأکید شده است.

قانون اساسی بسیاری از کشورها نیز در صدد تبیین الزامات و بایسته‌های حفظ حقوق ملت، ازجمله رعایت حریم خصوصی ارتباطات برآمده است. برای مثال، در این رابطه اصل ۲۵ قانون اساسی جمهوری اسلامی ایران مقرر می‌دارد: «بازرسی و نرساندن نامه‌ها، ضبط و فاش‌کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها، استراق‌سمع و هرگونه تجسس ممنوع است مگر به حکم قانون».[۶۶] از سوی دیگر، برخی از دولت‌های دیگر در قانون اساسی‌شان، مستقیماً هیچ اشاره‌ای به رعایت حریم خصوصی نکرده‌اند. در این راستا می‌توان به ایالات متحده امریکا اشاره کرد که در قانون اساسی‌اش، هیچ بیان صریحی مبنی‌بر تضمین حق بر حریم خصوصی وجود ندارد. باوجود این، شناسایی حق شهروندان در امکان برقراری ارتباط به‌صورت ناشناخته، از حق آزادی بیان، حق مخالفت و انتقاد به دست می‌آید.[۶۷]

اما مسئله‌ای که پس از ذکر اهمیت حق بر حریم خصوصی مطرح می‌شود این است که چه‌موقع در فضای سایبر، حریم خصوصی افراد نقض می‌شود؟ در پاسخ به این سؤال گفته می‌شود: هنگامی می‌توان نقض حریم خصوصی فرد را تأیید کرد که او نتواند مخابره اطلاعات راجع به خویش یا استفاده از آن اطلاعات را که در عرصه عمومی قابل دسترس نیست، کنترل کند. هرچه تعداد مردمی که از اطلاعات شخصی آن فرد آگاه می‌شوند بیشتر باشد، گستره نقض

65. The European Convention for the Protection of Human Rights and Fundamental Freedoms, *European Treaty Series*, No.5,213 UNTS221.

۶۶. کنگرانی، مهدی؛ *قانون اساسی و قانون مدنی*، جمال‌الحق، ۱۳۸۵، ص ۳۹.

67. Chawki, Mohamed, "Anonymity in Cyberspace: Finding the Balance between Privacy and Security", *Droit-Tic, Juill*. 2006, p. 18, quoted in C. NICOLL, *Digital Anonymity and the Law: Tensions and Dimensions* (The Hague, T.M.C ASSER PRESS), 2003, p. 294.

حریم خصوصی نیز بیشتر خواهد شد.[۶۸]

د. حق بر ناشناختگی[۶۹]

اگرچه حق بر ناشناختگی را می‌توان در ذیل حق بر حریم خصوصی ارتباطات و به‌عنوان یکی از شاخه‌های آن بررسی کرد، به لحاظ اهمیت حق مزبور در فضای مجازی، آن را به‌طور جداگانه بررسی می‌کنیم. مفهوم ناشناختگی از کلمه‌ای یونانی گرفته شده و به معنای «بی‌نامی» است. در دنیای مدرن و پست‌مدرن جامعه اطلاعاتی، ناشناختگی به‌عنوان یک بُعد حریم خصوصی (اطلاعاتی) تعریف می‌شود. باوجود این حق، داده‌های شخصی، محافظت، و استفاده از آن، قاعده‌مند و با محدودیت‌هایی مواجه می‌شود.[۷۰] در تبیین این مفهوم در عالم معنا می‌توان بیان داشت: این وضعیت، هنگامی حادث می‌شود که فردی در عین حضور در مکانی عمومی، بخواهد آزادی خود را در اینکه ناشناس و مصون از نظارت دیگران باشد، حفظ کند. برای مثال، فردی که از خیابان عبور می‌کند می‌داند که در معرض دید قرار دارد ولی انتظار ندارد که هویتش مشخصاً شناسایی شود و به‌صورت برنامه‌ریزی‌شده در معرض مشاهده دیگران باشد.[۷۱]

بااین‌حال، از دخالت و نظارت دولت‌ها بر اطلاعات شخصی افراد ولو برای پیشگیری از تروریسم سایبری، نقض حق بر ناشناختگی به دست می‌آید. به عبارت دیگر، هنگامی که افراد در کانون توجه دیگران قرار می‌گیرند حریم خصوصی خود را از دست می‌دهند. شناخته‌شدن برای افراد زیاد، به‌تنهایی لطمه به حریم خصوصی است هرچند که بر اثر آن، هیچ اطلاعاتی درباره فرد به دیگران مخابره نشود.[۷۲] از این منظر است که به اعتقاد برخی حقوق‌دانان و پژوهشگران، راه حفاظت از حریم زندگی خصوصی در آینده، همانا پیونددادن اندیشه حریم زندگی خصوصی با اندیشه ناشناختگی و گمنام‌ماندن است. در دنیای رسانه‌ای‌شدهٔ رایانه‌ای، حریم زندگی خصوصی الزاماً این نیست که انسان بتواند برخی از اطلاعات مربوط به خودش را حفظ و برخی دیگر را برملا سازد، بلکه حریم مزبور، عبارت است از داشتن حق حفظ یا اشاعه این واقعیت که اطلاعات موردنظر در واقع به شما تعلق دارد.[۷۳]

---

۶۸. انصاری، باقر؛ *حقوق حریم خصوصی*، سمت، ۱۳۸۶، ص ۱۶.

69. Anonymity

70. Voorhoof, Dirk, "Internet and the Right of Anonymity", Proceedings of the Conference Regulating the Internet, Belgrade, 2010, pp. 2-3.

۷۱. انصاری؛ *همان*، ص ۱۵.

۷۲. *پیشین*، ص ۱۶.

۷۳. نورایی بیدخت، حسن؛ «حریم خصوصی افراد در جریان بین‌المللی داده‌ها»، *رسانه*، شماره ۳۸، تابستان ۱۳۷۸، ص ۲۶.

البته باوجود اینکه برخی از حقوق‌دانان و پژوهشگران،[۷۴] ناشناختگی را به دو دستهٔ ناشناختگی واقعی[۷۵] و ناشناختگی ساختگی[۷۶] دسته‌بندی و از آن حمایت می‌کنند، به نظر می‌رسد با ورود به دهه دوم قرن ۲۱، «ناشناختگی» تحت فشار باشد. درحالی‌که تبلیغات هدفمند رفتاری به گسترش خود ادامه می‌دهد و اطلاعات شخصی به‌طور فزاینده‌ای مشخص می‌شود، مقامات دولتی در سراسر جهان هشدار می‌دهند که ناشناختگی واقعی نه فقط در تعارض با اهداف امنیت ملی محسوب می‌شود، بلکه با گفتمان مدنی خودش هم تعارض دارد.[۷۷] به عبارت دیگر، حق بر ناشناختگی، همچون شمشیر دولبه‌ای است که یک لبه‌اش مربوط به رعایت حقوق بشری مردم و لبه دیگرش، نحوه رعایت چنین تکلیفی از سوی دولت‌هاست که سهل‌انگاری و بی‌مبالاتی در ایفای چنین تکلیفی، این فرصت را برای تروریست‌ها فراهم می‌کند تا در قالب این پوشش با خیال آسوده بتوانند اقدامات تروریستی خویش را از طریق فضای مجازی برای تهدید و ارعاب جامعه هدف، به منصه ظهور برسانند.

به همین دلیل است که برخی، ناشناختگی در اینترنت را همراه با انتقادات فزاینده‌ای می‌دانند و معتقدند این امر، سبب تهدید مدنیت و امنیت عمومی می‌شود.[۷۸] لذا از نظارت دولت‌ها بر فعالیت‌ها در فضای مجازی و شناسایی هویت واقعی افرادی که در این فضا حضور دارند، قویاً حمایت می‌کنند. بااین‌حال، الزامات حقوق بشری ایجاب می‌کند تا دولت‌ها در اعمال حق حاکمیت و ایفای تکالیف خویش به رعایت قواعدی پایبند باشند.

۲ـ۲. حقوق و تکالیف دولت‌ها در مبارزه با سایبرتروریسم

نظام جهانی و منطقه‌ای حقوق بشر تأکید می‌کند که دولت‌ها بنابر صلاحیتشان، هم حق و هم تکلیف حفاظت از افراد در حملات تروریستی را دارند. امروزه قواعد حقوق بشر با نظم عمومی بین‌المللی گره خورده است و نمی‌توان انتظار داشت نادیده‌انگاشتن یا نقض حقوق بنیادین بشر، بدون واکنش جامعه بین‌المللی و تابعان آن، خاتمه پذیرد.[۷۹] برای مبارزه با تروریسم در دوران حضور اینترنت، حفاظت از امنیت بین‌المللی به‌ویژه حقوق بنیادین بشر ضروری است. به‌طور عمده، حفاظت قضایی از اشخاص در برابر سوءاستفاده از اختیارات در مبارزه با تروریسم، ضروری است. در سطح اتحادیه اروپا، شهروندان به دادگاه بدوی و سپس به دیوان دادگستری اتحادیه

74. See: Chawki, *op. cit.*

75. True anonymity

76. Pseudo-anonymity

77. Farrall, Kenneth, "Online Collectivism, Individualism and Anonymity in East Asia", *Surveillance & Society*, 2012, p. 424.

78. *Ibid*.

79. UNODC, *Ibid*.

اروپا مراجعه می‌کنند اما در موارد اخیر، دیده می‌شود که قانون، موقعی که با تروریسم مبارزه می‌کند، مدافع حفاظت از حقوق بنیادین بشر نیست.[۸۰] کنوانسیون شورای اروپا راجع به پیشگیری از تروریسم،[۸۱] که در سال ۲۰۰۷ لازم‌الاجرا شد، مبنای قانونی هماهنگ برای پیشگیری و مبارزه با تروریسم، بخصوص تحریک عمومی به ارتکاب جرایم تروریستی،[۸۲] استخدام[۸۳] و تربیت اشخاص برای تروریسم[۸۴] ازجمله از طریق اینترنت مقرر کرده است.[۸۵]

همچنین سازمان‌هایی مانند دفتر کمیساریای عالی حقوق بشر سازمان ملل متحد،[۸۶] از ارتقا و حفاظت از حقوق بشر و اجرای اقدامات مؤثر ضدتروریسم به‌عنوان موضوعات تقویت‌کننده تکمیلی و دوجانبه حمایت می‌کنند. دفتر از طریق توصیه‌های کلی به دولت‌ها درباره الزامات حقوق بشری، مسئله حفاظت از حقوق بشر را به هنگام مبارزه با تروریسم بررسی می‌کند و نیز مشاوره و مساعدت‌هایی را به دولت‌ها (بر مبنای تقاضا)، به‌ویژه در حوزه ارتقاء آگاهی نظام بین‌الملل حقوق بشر[۸۷] در میان نمایندگان ملی مجری قانون ارائه می‌کند.[۸۸]

با این تفاسیر، در مبارزه با تروریسم، دو تکلیف حقوقی در برابر یکدیگر قرار می‌گیرند: تکلیف به حفاظت از آزادی، حیات و امنیت مردم آن کشور که بیانگر منافع عمومی است و تکلیف به احترام به حقوق بشر افراد و به‌ویژه مظنونان، متهمان یا محکومان به ارتکاب جرایم تروریستی که بیانگر منافع خصوصی و شخصی این افراد است. در چنین شرایطی، نظام حقوق بشر به‌عنوان نظام حقوقی، ناگزیر از حل تعارض است. این نظام حقوقی دو راه پیش رو دارد. می‌تواند تعارض را به نفع یکی از این دو منفعت حل کند یا با ایجاد توازن میان آن‌ها در حفظ و رعایت اصول بنیادین بشری در کلیه شرایط بکوشد. در این خصوص گفته شده که «در جوامع متمدن در موارد تعارض میان منفعت فردی با منافع جمعی، منفعت فردی باید به نفع منافع عمومی کنار گذاشته

80. Foggetti, Nadia, *op. cit*, p.p. 373 – 374.

81. The Council of Europe Convention on the Prevention of Terrorism, 2005.

۸۲. کنوانسیون شورای اروپا درباره پیشگیری از تروریسم، ماده ۵.

۸۳. *همان*، ماده ۶.

۸۴. *همان*، ماده ۷.

85. Akdeniz, Yaman, "Freedom of Expression on the Internet", *Organization for Security and Co-operation in Europe (OSCE)*, 2010, p. 70.

86. The Office of the United Nations High Commissioner for Human Rights (OHCHR)

در سال ۱۹۹۷ برنامه حقوق بشر سازمان ملل متحد به‌منظور تقویت اثرات آن بر هماهنگی فعالیت‌های بشری در همه نظام ملل متحد، مورد تجدیدنظر اساسی قرار گرفت و دبیرکل ملل متحد، دفتر کمیسر عالی و مرکز حقوق بشر سازمان ملل متحد را با هم ادغام کرد که هم‌اکنون تحت نظر کمیسر عالی حقوق بشر اداره می‌شود. ن.ک:

www.unhchr.ch/htm/hchr.htm.

۸۷. نظام بین‌الملل حقوق بشر (International Human Rights Law) منعکس‌کننده تعدادی از معاهدات بین‌المللی اصلی حقوق بشر و حقوق بین‌الملل عرفی است.

88. OHCHR, *op. cit*.

شود. این شرط در زمان‌های دشوار، نیازمند ایجاد توازن میان دو منفعت مذکور تا جایی است که تفاوت‌ها قابل سازش نباشند». نظام بین‌المللی به‌غایت از این دیدگاه سود برده است. در این نظام از طرفی به دولت‌ها اجازه داده شده است که بنابر حفظ آزادی دیگران، حفظ امنیت و بهداشت عمومی، محدودیت‌هایی بر حقوق بشر وضع کنند.[۸۹]

برای مثال، در بند دوم ماده ۹ کنوانسیون شورای اروپا راجع به حمایت از افراد در برابر پردازش خودکار داده‌های شخصی،[۹۰] عمده اختیارات دولت‌های عضو در اعمال محدودیت بر حقوق فردی تشریح شده است: «... هنگامی که عدول از چنین مقرراتی در قوانین دولت‌های عضو، مقرر شده باشد و اقدام ضروری را در جامعه‌ای دموکراتیک برای حمایت از منافع ذیل به‌وجود آورد: الف‌ـ حفاظت از امنیت کشور، امنیت عمومی، منافع پولی دولت یا سرکوب جرایم کیفری؛ ب‌ـ حفاظت از داده‌ها یا حقوق و آزادی‌های دیگران».

در اینجا این سؤال مطرح می‌شود که این محدودیت تا چه میزانی وضع می‌شود؟ در راستای حفظ حقوق عمومی، آیا دستور دادگاه به نظارت بر اطلاعات شخصی برای پیشگیری و مبارزه با سایبرتروریسم، نقض حقوق بشر محسوب نمی‌شود؟

الف. ضوابط ناظر بر تحدید حقوق فردی

با مطالعه اسناد حقوق بشر، حقوق مندرج در این اسناد به دو دسته مطلق و مقید تقسیم می‌شود. حمایت از برخی حقوق، چندان اهمیت دارد که صرف‌نظر از اقلیم جغرافیایی، فرهنگی و سوابق تاریخیِ محل اجرای آن، به‌هیچ‌وجه محدودشدن آن را نمی‌توان تحمل کرد و نباید بر آن قیدی نهاد یا محدوده‌ای برای آن ترسیم کرد. از این قبیل حقوق، مثال‌های متعددی می‌توان آورد. حق حیات، حق برخورداری از محاکمه عادلانه، حق مصونیت در برابر مجازات‌های خشن و غیرانسانی در این دسته جای می‌گیرد و از آن‌ها به‌عنوان «حقوق مطلق» یاد می‌شود. اما حقوق دیگری هست که اجرای مطلق آن به علت برخورد با حقوق فردی دیگران یا منافع اجتماعی، امکان‌پذیر نیست و باید بر آن قید نهاد. این حقوق، قیدپذیر است و در هر نظام حقوقی، محدوده اعمال معینی دارد. آزادی‌های مدنی و سیاسی عمدتاً در این گروه جای دارد. آزادی عقیده و بیان آن و آزادی‌های مذهب، مثال‌هایی مشهور در این زمینه به‌شمار می‌آید که «حقوق مقید» نامیده می‌شود.[۹۱] به عبارت دقیق‌تر، دولت‌ها ملزم به حفاظت از افراد، علیه دخالت اشخاص ثالثی هستند

۸۹. عبدالهی، محسن؛ *تروریسم، حقوق بشر و حقوق بشردوستانه*، شهردانش، ۱۳۸۸، ص ۶۸.

90. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 1981, article 9.

۹۱. ن.ک: کاتوزیان؛ *همان*، صص ۱۸۱ـ۱۷۹.

که مسبب تحدید برخورداری از حق آزادی عقیده و بیان می‌شوند. ایفای تعهد مسلم دولت برای حفاظت از افراد، مستلزم به‌کارگیری اقدامات مناسب و مؤثر برای بررسی اعمال اشخاص ثالث است.[۹۲]

بااین‌حال، مناسب‌ترین پاسخ درباره سؤالات مطروحه این است که در مقام بررسی، دادگاه، منافع عمومی حاصل از حفظ اطلاعات و منافع عمومی حاصل از افشای آن‌ها را ارزیابی می‌کند تا معلوم شود اهمیت کدام‌یک بیشتر است. اگرچه گستره این استثنا در طول زمان، توسعه یافت، می‌توان گفت مبنای آن این قاعده کلی است که «خطرناک‌بودن تعهدی برای عموم جامعه، زائل‌کننده تعهد و نیروی الزام‌آوری آن است».[۹۳] مسلماً حقوق و آزادی‌های فردی، ضمیر حقوق بشر را تشکیل می‌دهد اما این نظام برای بقا، نیازمند ضمیمه‌شدن به فضایل اخلاقیِ شکل‌گرفته در بستر جوامع است تا انعطاف حقوق بشر را بالا ببرد. نتیجه محتوم تأکید بیش از حد بر فردگرایی و دورافتادن از حقوق و آزادی‌های جمعی که امروزه دنیا برای زندگی مسالمت‌آمیز نیازمند آن است، اضمحلال حقوق بشر است. بنابراین اهتمام بیشتر به حقوق جمعی در کنار حقوق فردی، زمینه‌های استحکام حقوق بشر در حال و آینده را فراهم می‌کند.[۹۴]

تعهد و تکلیف دولت به‌منظور حفظ و حمایت از حقوق عمومی، نه‌تنها وظیفه هر دولتی است، بلکه ملاکی برای سنجش میزان پایبندی دولت‌ها در تعهد به پیشگیری از وقوع نقض حقوق بشر نیز محسوب می‌شود. در این راستا دولت‌ها و سازمان‌های بین‌المللی، قبل از هر اقدامی علیه سایبرتروریسم، تکلیف بر تبیین سازوکارهای مناسب پیشگیرانه از طریق مراجع حمایتی تقنینی، آموزشی، فرهنگی، درمانی و ... دارند و پس از اجرای سازوکارهای پیشگیرانه در صورت عدم حصول نتیجه مطلوب، درنهایت باید به مراجع حمایتی پلیسی و امنیتی متوسل شد.[۹۵] این راهکار به‌خوبی در کنوانسیون پیشگیری از جرایم تروریستی، مصوب ۲۰۰۵ شورای اروپا[۹۶] قابل مشاهده است. برخی از کشورها با به‌کارگیری قوانین موجود درباره تروریسم، جرم‌انگاری کرده و تروریست‌هایی را که از اینترنت استفاده می‌نمایند، تعقیب می‌کنند. این کنوانسیون، یکی از این اسناد است.[۹۷]

92. Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Seventeenth Session, 2011, p. 15.

۹۳. استنلی، پائول؛ *حقوق حفظ اسرار*، ترجمه: محمدحسین وکیلی‌مقدم، کتاب همگان، ۱۳۹۱، ص ۵۴.

۹۴. عاشوری، زینب؛ *نسبت فرد و جامعه در حقوق بشر*، پایان‌نامه کارشناسی ارشد حقوق بین‌الملل، دانشگاه مفید قم، ۱۳۹۱، ص ۹۷.

95. Foggetti, Nadia, *op. cit*, p. 368.

96. Council of Europe Convention on Prevention of Terrorism, Warsaw, 2005.

97. Gercke, Marco, "Challenges in Developing a Legal Response to Terrorist Use of the Internet", *Center of Excellence-Defence against Terrorism*, vol. 3, No. 2, 2010, p. 52.

ب. مسئولیت‌های ناشی از نقض بلاوجه حقوق فردی

با توجه به اینکه در مبارزه با سایبرتروریسم، دامنه اعمال حق نظارت بر اطلاعات شخصی بسیار قابل بسط بوده و به عبارت دیگر، تقریباً در چارچوب حفظ حقوق عمومی می‌توان بسیاری از مسائل و موضوعات را جای داد که تدقیق در آن، به عمومی یا شخصی‌بودن منفعت، تردید وارد می‌کند، اگر مقامی دولتی با تمسک به حفظ حقوق عمومی، از اختیارات قانونی خویش برای کسب منافع شخصی سوءاستفاده کند، باید در برابر اقدامات غیرضروری و خارج از حد متعارف خویش، مسئول شناخته شود. در ماده ۱۲ کنوانسیون جرایم سایبر آمده است: «هریک از اعضا باید قوانین و سایر تدابیر را به‌گونه‌ای وضع کند که در صورت لزوم، اطمینان دهد چنانچه اشخاص حقوقی در راستای منافع خود مرتکب جرایم مصوب این کنوانسیون شدند، آن‌ها را تحت تعقیب کیفری قرار خواهد داد. این جرایم را یک شخص حقیقی که شخصاً یا به‌عنوان بخشی از ارگان شخص حقوقی فعالیت می‌کند و مدیریت آن را بر عهده دارد و اختیارات ذیل را داراست مرتکب می‌شود: الف‌ـ اختیار نمایندگی شخص حقوقی، ب‌ـ اختیار تصمیم‌گیری از طرف شخص حقوقی، پ‌ـ اختیار اعمال کنترل بر شخص حقوقی».[۹۸]

به‌هرحال در جنگ علیه تروریسم، معمولاً قواعد حقوق بشر به‌عنوان وظیفه تحمیلی در پاسخ مؤثر به خطر مشاهده می‌شود. برخی دولت‌ها و سازمان‌های بین‌المللی در سطح منطقه‌ای و جهانی مدعی هستند که ماهیت تهدید، دخالت آنان را حتی با صرف هزینه از اصول مبنایی دموکراسی، همچون احترام به آزادی‌های فردی و عدم تبعیض مجاز می‌کند. در این ادعا، حق بر حریم خصوصی اهمیت مضاعفی دارد. یعنی حریم خصوصی یک حق است، اما اقدامات دولت‌ها بسیار مهم است زیرا این اقدامات به حفاظت از دیگر حقوق بنیادین کمک می‌کند.[۹۹] بااین‌حال، این شیوه تا حدودی صرفاً قابلیت اعمال مطلق بر قلمرو داخلی دولت‌ها را دارد اما مشکل، زمانی پیچیده‌تر می‌شود که موضوع به خارج از قلمرو سرزمینی یک دولت تسری نماید. قصور جامعه بین‌المللی در ایجاد سازوکاری جهانی برای مواجهه با تروریسم بین‌المللی، ممکن است واکنش‌های یک‌جانبه دولت‌های قربانی را برانگیزد؛ دولت‌هایی که باز از دیدگاه دیگران ممکن است خود مسبب حرکات تروریستی شناخته شده باشند. در فقدان ابزارهای مناسبی که حقوق بین‌الملل آن‌ها را تضمین کرده باشد، دولت قربانی، اغلب زیر پوشش دفاع مشروع و با توسل به شیوه‌هایی که گاه مشابه همان روش‌هایی است که خود، آن‌ها را تقبیح کرده است، حقوق بین‌الملل را زیر پا می‌گذارد.[۱۰۰]

98. Council of Europe, Convention on Cybercrime, Budapest, 2001, p. 8.

99. Foggetti, Nadia, *op. cit*, p. 368.

۱۰۰. سیمبر؛ *همان*، ص ۲۳۷.

علاوه‌بر اینکه راهبرد جهانی مبارزه با تروریسم سازمان ملل، مصوب سال ۲۰۰۶،[۱۰۱] اهمیت احترام به حقوق بشر و حقوق بشردوستانه و حاکمیت قانون را در قبال همه انسان‌ها به‌عنوان مبنای اساسی برای مبارزه با تروریسم اعلام کرد، عموماً این امر پذیرفته شده است که برخی افعال متخلفانه، موجب مسئولیت دولت متخلف در برابر چندین یا بسیاری از دولت‌ها یا حتی در قبال کل جامعه بین‌المللی می‌شود. گام مهم در این راستا را دیوان بین‌المللی دادگستری در قضیه *بارسلونا تراکشن* برداشت. دیوان در این قضیه اظهار داشت:

باید میان تعهدات دولت در برابر جامعه بین‌المللی در کل و تعهدات او در قبال هر دولت دیگری در زمینه حمایت دیپلماتیک، تمایز اساسی قائل شد. تعهدات دسته قبل به دلیل ماهیت‌اش به تمامی دولت‌ها مرتبط است. نظر به اهمیت حقوق مورد اشاره، تمامی دولت‌ها در حمایت از آن دارای نفع حقوقی هستند. آن‌ها تعهداتی عام‌الشمول[۱۰۲] هستند.[۱۰۳]

دیوان با استناد به حقوق بین‌الملل معاصر، به نمونه‌هایی از این حقوق و تعهدات مشتمل بر غیرقانونی‌بودن اعمال تجاوز، نسل‌کشی و همچنین اصول و قواعد حاکم بر حقوق اساسی شخص انسانی ازجمله حمایت در برابر بردگی و تبعیض نژادی اشاره می‌کند.[۱۰۴]

نتیجه

در نظام حقوق بین‌الملل بشر، دولت‌ها برای رسیدن به راه‌حل مشترک جهانی برای مبارزه با سایبرتروریسم، نیازمند تعریفی واحد و همسان از اصطلاح سایبر تروریسم هستند. «فضای سایبر»، مفهومی روشن و قابل تمییز دارد. فقدان تعریفی واحد از واژه «تروریسم» و اکتفا به جرم‌انگاری از طریق بیان مصادیق، بر پیچیدگی‌های این واژه افزوده است. البته به‌نظر می‌رسد برخی از دولت‌های پیشرفته و قدرتمند، بخصوص پس از حوادث ۱۱ سپتامبر ۲۰۰۱ با سوءاستفاده از این واژه، قواعد حقوق بشری همچون حق آزادی، عدم بازداشت خودسرانه و حق مطلع‌شدن از علل بازداشت را نقض کرده و محدودیت‌های گسترده، جهت دستیابی به منافع خویش اعمال کرده‌اند. تبیین مقررات بین‌المللی جامع، همچون کنوانسیون جرایم سایبری می‌تواند تا حدودی حصول راه‌حل مشترک جهانی را هموارتر سازد، به‌ویژه اینکه چنین اسنادی این قابلیت را دارد که به‌عنوان الگو و نمونه، مورد استفاده قوای تقنینی دولت‌ها قرار گیرد.

مهم‌ترین دلیل مبارزه با سایبرتروریسم، تکلیف دولت‌ها به حفاظت از آزادی و امنیت مردم

101. The UN Global Counter-Terrorism Strategy, adopted in 2006.

102. *Erga omnes*

103. Barcelona Traction, Light and Power Company, Limited, Second Phase, I. C. J. Reports 1970, p 32, para. 33.

104. *Ibid*, at p. 32, para. 34.

کشور است که مبیّن منافع عمومی است. البته در این راستا تعارضی متصور است چون نمی‌توان تکلیف دولت‌ها به رعایت حقوق بشر افراد، خصوصاً متهمان یا محکومان جرایم تروریستی را نادیده انگاشت. برای حل این تعارض، می‌توان این‌گونه استدلال کرد: درصورتی‌که این تفاوت‌ها قابل‌جمع نباشد، منفعت فردی به نفع منفعت عمومی کنار گذاشته می‌شود. مقامات دولتی که در این رابطه اختیاراتی دارند نمی‌توانند برای کسب منافع شخصی از آن سوءاستفاده کنند و لذا در برابر اقدامات غیرضروری و خارج از حد متعارف خویش، مسئول شناخته می‌شوند.

البته نکته حائز اهمیت که در قالب پژوهشی دیگر می‌توان به آن پرداخت این است که آیا دولت‌ها می‌توانند با برداشتی باز و یک‌جانبه از تروریسم، برای تأمین حقوق بنیادین اتباع خویش در برابر سایبرتروریسم، حقوق بنیادین جامعه بشری را نادیده گرفته و آن را نقض کنند؟ در حال حاضر، برخی از دولت‌ها در راستای توجیه اقدامات پیش‌دستانهٔ ناقض حقوق بشر، به این برداشت استناد می‌کنند.

منابع:

الف) فارسی

ـ کتاب

- استنلی، پائول؛ *حقوق حفظ اسرار*، ترجمه: محمدحسین وکیلی‌مقدم، کتاب همگان، ۱۳۹۱.
- اصلانی، حمیدرضا؛ *حقوق فناوری اطلاعات*، میزان، ۱۳۸۴.
- امیرارجمند، اردشیر؛ *مجموعه اسناد بین‌المللی حقوق بشر*، انتشارات دانشگاه شهید بهشتی، جلد اول، ۱۳۸۰.
- انصاری، باقر؛ *حقوق حریم خصوصی*، سمت، ۱۳۸۶.
- آماده، مهدی؛ *حمایت از حریم خصوصی*، دادگستر، ۱۳۹۲.
- بندک، ولفگانگ و آلیس مانگوپولوس؛ *تروریسم و حقوق بشر*، ترجمه: محمدجعفر ساعد و دیگران، دادگستر، ۱۳۸۹.
- جلالی فراهانی، امیرحسین؛ *کنوانسیون جرایم سایبر و پروتکل الحاقی آن*، خرسندی، ۱۳۸۸.
- سلیمی، صادق؛ *جنایات سازمان‌یافته فراملی*، صدرا، ۱۳۸۲.
- سیمبر، رضا؛ «تروریسم بین‌المللی؛ تهدیدات، چالش‌ها و فرصت‌های فراسوی امنیت ملی جمهوری اسلامی ایران»، در *مجموعه مقالات موضوعی کتاب امنیت بین‌الملل*، تدوین علی عبدالله‌خانی؛ مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران، ۱۳۸۴.
- شریفیان، جمشید؛ *راهبرد جمهوری اسلامی ایران در زمینه حقوق بشر در سازمان ملل متحد*، انتشارات وزارت امور خارجه، ۱۳۸۰.
- عالی‌پور، حسن؛ *حقوق کیفری فناوری اطلاعات*، خرسندی، ۱۳۸۹.
- عاملی، سیدسعیدرضا؛ *رویکرد دوفضایی به آسیب‌ها، جرایم، قوانین و سیاست‌های فضای مجازی*، امیرکبیر، ۱۳۹۰.
- عبدالهی، محسن؛ *تروریسم، حقوق بشر و حقوق بشردوستانه*، شهر دانش، ۱۳۸۸.
- قربان‌نیا، ناصر؛ «چالش‌های کمک‌های بشردوستانه در دوران جنگ بر ضدتروریسم»، در *مجموعه مقالات موضوعی کتاب چالش‌های کمک‌های بشردوستانه در خاورمیانه*، مجری طرح: نسرین مصفا؛ انتشارات وزارت امور خارجه، ۱۳۸۶.
- کاتوزیان، ناصر و دیگران؛ *آزادی اندیشه و بیان*، انتشارات دانشکده حقوق‌وعلوم‌سیاسی دانشگاه تهران، ۱۳۸۲.
- کنگرانی، مهدی؛ *قانون اساسی و قانون مدنی*، جمال‌الحق، ۱۳۸۵.
- مصفا، نسرین؛ سخنرانی با عنوان «مقابله با تروریسم و حقوق بشر» در همایش *تروریسم و*

دفاع مشروع از منظر اسلام و حقوق بین‌الملل، انتشارات مرکز مطالعات توسعه قضایی و دانشکده علوم‌قضایی و خدمات اداری، ۱۳۸۰.
- هاشمی، سیدمحمد؛ *حقوق بشر و آزادی‌های اساسی*، میزان، ۱۳۸۴.
- هیک، استیون و دیگران؛ *حقوق بشر و اینترنت*، ترجمه: سیدقاسم زمانی و دیگران، خرسندی، ۱۳۸۶.

ـ مقاله

- نورایی بیدخت، حسن؛ «حریم خصوصی افراد در جریان بین‌المللی داده‌ها»، *رسانه*، شماره ۳۸، تابستان ۱۳۷۸.

ـ پایان‌نامه

- صفوی‌کوهساره، سیدحامد؛ *قواعد حاکم بر حملات سایبری از منظر حقوق بین‌الملل*، پایان‌نامه کارشناسی ارشد حقوق بین‌الملل، دانشگاه مفید، قم، ۱۳۹۱.
- عاشوری، زینب؛ *نسبت فرد و جامعه در حقوق بشر*، پایان‌نامه کارشناسی ارشد حقوق بین‌الملل، دانشگاه مفید قم، ۱۳۹۱.

ب) انگلیسی

- *A. v. Norway*, European Court of Human Rights, Judgement of 9 April 2009, available at: http://sim.law.uu.nl/SIM/Dochome.nsf?Open.
- Akdeniz, Yaman, "Freedom of Expression on the Internet", *Organization for Security and Co-operation in Europe (OSCE)*, 2010.
- Barcelona Traction, Light and Power Company, Limited, Second Phase, I. C. J. Reports 1970.
- Chawki, Mohamed, "Anonymity in Cyberspace: Finding the Balance between Privacy and Security", *Droit-Tic, Juill*. 2006.
- Cohen, Aviv, "Cyberterrorism: Are We legally Ready?, *The Journal of International Business & Law*, 2010.
- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Strasbourg, 1981, available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.
- Council of Europe, Convention on Cybercrime, European Treaty Series - No. 185, Budapest, 2001, available at: Treaty Office on http://conventions.coe.int.
- European Convention on Human Rights and Fundamental Freedoms,

1950, available at: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=4/25/2006&CL=ENG.

- Farrall, Kenneth, "Online Collectivism, Individualism and Anonymity in East Asia", *Surveillance & Society*, 2012.
- Fenz, Stefan, Cyberspace Security: A Definition and a Description of Remaining Problems, University of Vienna - Institute of Government & European Studies, 2005.
- Foggetti, Nadia, "Cyber-terrorism and the Right to Privacy in the Third Pillar Perspective", *Masaryk University Journal of Law and Technology*, vol. 3, 2009.
- Gercke, Marco, "Challenges in Developing a Legal Response to Terrorist Use of the Internet", *Center of Excellence-Defence against Terrorism*, vol. 3, No. 2, 2010.
- Human Rights Committee, General Comment 29, States of Emergency, 2001, abvailbe at: U.N. Doc. CCPR/C/21/Rev.1/Add.11.
- Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Seventeenth session, 2011, Doc. No. A/HRC/17/27.
- International Convention for the Suppression of the Financing of Terrorism, 1999, U.N. Doc. A/RES/54/109, Annex, available at: https://www.unodc.org.
- International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171, available at: http://www.refworld.org/docid/3ae6b3aa0.html.
- Janczewski, Lech J, Andrew M.Colarik, Cyber Warfare and Cyber Terrorism, Information Science Reference, 2007.
- Nils, Melzer, "Cyberwarfare and International Law", *The United Nations Institute for Disarmament Research (UNIDIR) Resources*, 2011.
- Office of the United Nations High Commissioner for Human Rights (OHCHR), Human Rights, Terrorism and Counter-terrorism, Fact Sheet No. 32, United Nations, 2008.
- Resolution 1566, Adopted by the Security Council at its 5053rd meeting, on 8 October 2004, availble at: http://www.unrol.org/files/n0454282.pdf.
- Ryngaert, Cedric, "State Responsibility, Necessity and Human Rights", *Institute for International Law K.U.Leuven*, Working Paper No. 141, 2009.
- Sorel, Jean-Marc, "Some Questions about the Definition of Terrorism and the Fight against Its Financing", *European Journal of International Law*, vol. 14, No. 2, 2003.
- The European Convention for the Protection of Human Rights and Fundamental Freedoms, European Treaty Series No.5, 213 UNTS221.
- United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime, United Nations, 2013.

- Voorhoof, Dirk, "Internet and the Right of Anonymity", Proceedings of the Conference Regulating the Internet, Belgrade, 2010, available at: http://www.psw.ugent.be/Cms_global/uploads/publicaties/dv/05recente_publicaties/Anonymity.Voorhoof.editedjuly2010.pdf.
- www.unhchr.ch/htm/hchr.htm
- *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council and Commission*, Judgment of 3 September 2008, available at: http://ec.europa.eu/dgs/legal_service/arrets/05c402_en.pdf.