تقابل حق حریم خصوصی اشخاص و امنیت ملی، در مقابله با تروریسم سایبری

یونس فتحی*

خیرالله شاهمرادی**

تاریخ دریافت: ۱۳۹۶/۷/۵ تاریخ پذیرش: ۱۳۹۶/۹/۵

چکیده

مقوله امنیت ملی و تلاش برای تحقق همه جانبهٔ آن در یک جامعه از اصلی‌ترین مباحث در هر نظام سیاسی می‌باشد. تروریسم، یکی از جدی‌ترین تهدیدها برای امنیت یک نظام سیاسی محسوب می‌شود که به مدد پیشرفت تکنولوژی در چند دهه اخیر از قالب سنتی خارج شده و به شکل خطرناک‌تر و پیشرفته‌تری در بستر فضای سایبر مجال بروز پیدا کرده است و امنیت دولت‌ها را در معرض تهدید جدی قرار می‌دهد. تحقق امنیت ملی در مواردی با اعمال مجازات نسبت به تروریست‌ها و در مواردی با اتخاذ سیاست‌های پیشگیری از جرم شکل می‌گیرد. اما اتخاذ تدابیر مذکور در مواردی باعث می‌شود که حفاظت از امنیت ملی در تقابل با حق حریم خصوصی افراد قرار گیرد. این موضوع در فضای سایبر، تقابل میان حق حریم خصوصی و امنیت ملی را به عنوان موضوعی پرسش‌برانگیز مطرح کرده و این نوشتار در پی پاسخ به آن است تا مشخص کند که در این تعارض، کدام مقوله مقدّم می‌باشد.

واژگان کلیدی: *تروریسم، سایبر، امنیت ملی، حق حریم خصوصی.*

*استادیار دانشکده ادبیات و علوم انسانی دانشگاه بوعلی سینای همدان(نویسنده مسؤول).

fathi3320@gmail.com

**کارشناسی ارشد حقوق جزا و جرم‌شناسی دانشگاه قم.

shahmoradikhirollah@yahoo.com

مقدمه

بیش از دو دهه است که اینترنت نقش بسزایی در ارتباطات جهانی ایفا می‌کند و به‌طور روزافزونی با زندگی مردم جهان عجین شده است. نوآوری‌ها و هزینه کم در این زمینه باعث شده است تا دسترسی، استفاده و عملکرد اینترنت به میزان قابل توجهی افزایش یابد، چنانکه امروزه اینترنت در سراسر دنیا در حدود دو میلیارد کاربر دارد. اینترنت شبکه وسیع جهانی را به وجود آورده که سالانه میلیاردها دلار برای اقتصاد جهانی سودآوری داشته است. با وجود این، اینترنت دولت‌ها را در مقابل چالش‌های جدید امنیتی قرار داده است. هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده است که بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و حتی افراد، به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، جرایم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آنها را به وجود آورند(خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱، ص۱۶۸).

یکی از بدیهی‌ترین حقوق شناخته شدهٔ بشر حق حریم خصوصی است و به عنوان بخش لاینفک اسناد حقوق بشری محسوب می‌شود. دولت‌ها نیز همواره علاوه بر اسناد جهانی و منطقه‌ای، در قوانین داخلی خود بر لزوم شناسایی و احترام به این حق تأکید دارند. با این حال، تروریسم سایبری که گونه‌ای نوین از تروریسم بین‌المللی بوده و تهدیدی جدی برای بشریت محسوب می‌شود، موجب شده است که دولت‌ها محدودیت‌هایی را برای تأمین این حق به وجود آورند. بخشی از تلاش‌های دولت برای مبارزه با تروریسم عملاً منجر به اتخاذ اقداماتی می‌شود که بر حق حریم خصوص افراد تأثیرگذار است.

اگرچه مبارزه جامعه جهانی علیه تروریسم، پیش از تأسیس سازمان ملل متحد آغاز شد اما 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 گردید؛ چراکه دولت‌ها دریافتند که حتی در مسافرت هوایی، تروریست‌ها با استفاده از فضای مجازی به راحتی امکان اطلاع یافتن 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 امکان وقوع حوادث تروریستی از طریق فضای مجازی (تروریسم سایبری) وجود دارد؟

در دنیای امروز، تروریست‌های اطلاعاتی می‌توانند به صورت غیر مجاز وارد سیستم‌های رایانه‌ای امنیتی شوند. برای مثال، با تداخل در سیستم ناوبری هوایی باعث سقوط هواپیما شده یا باعث قطع برق سراسری یا مسموم کردن منابع غذایی شوند(سلمانی‌زاده، ۱۳۸۰، ص۱۲۰) و به‌طورکلی آسیب‌های امنیتی جدی ایجاد می‌کنند که می‌تواند منجر به ایجاد بحران‌های حاد گردد. به گفته *فرید ذکریا* (در کتاب آینده آزادی)، دستیابی سریع تروریست‌ها به اطلاعات موررد نیاز عملیاتی خود از طریق فضای سایبری، از جمله آفت‌های فضای سایبر است که امنیت دولت‌ها را در معرض تهدید جدی قرار می‌دهد. مورد *دیوید کوپلند* می‌تواند در تأیید گفته *ذکریا* مورد استناد قرار گیرد. دیوید کوپلند در سال 1999 به دلیل نژادپرستی و انگیزه‌های جنسی، سه مورد بمب‌گذاری را در لندن صورت داد. بخشی از شواهد دادگاه حاکی از این بود که او اطلاعات مربرط به ساخت بمب را از منابع اینترنتی به دست آورده است. برای مثال، کتاب «راهنمای تروریستی» و نسخه دوم کتاب «چگونگی ساخت بمب» از این نمونه‌اند. این‌گونه منابع و سایر منابع نظیر کتاب‌های «ساخت مواد منفجره آشوب طلبان» و «تخلفات بزرگ»، که به راحتی و با استفاده از موتورهای جستجوگر اینترنتی قابل دستیابی می‌باشند، دولت‌ها را در معرض تهدیدهای جدید امنیتی قرار داده است(Walker, 2006, p.645).

بنابراین، امروزه اهمیت درک چنین فضایی در ارتباط با مفهوم امنیت ملی، از مهم‌ترین ادراکات ضروری برای جوامع مختلف است. تروریسم سایبری با هدف نابودسازی ساختارهای اساسی یک کشور، از جمله تهدیدات علیه منافع و امنیت ملی کشور است و از مهم‌ترین جرایم فراملی در فضای مجازی می‌باشد.

۱. مفاهیم و تعاریف

۱-۱. مفهوم حریم خصوصی[1]

از دیدگاه بسیاری از اندیشمندان، برای شناخت حریم خصوصی از همان ابتدا با یک

1. Privacy.

ژولیدگی و بی‌نظمی مفهومی مواجه می‌شویم. اندیشمدانی مانند *ویلیام بی نی*،[1] *تام گرتی*،[2] *آرتور میلر*،[3] *دنیل سولو*[4] و دیگران در آثار خود به این مهم اشاره کرده‌اند(انصاری، ۱۳۸۶، ص۱۲).

ویلیام بی نی، مشکلات حریم خصوصی را از جهت تعریف به ذات و قلمرو آن مربوط می‌سازد. *میلر*، دشواری تعریف را در ابهام و شکنندگی آن می‌داند و از دیدگاه *گرتی*، حریم خصوصی مفهومی متلوّن و متغیری است. از نظرگاه *سولو* نیز جامع‌ترین و با ارزش‌ترین حق شهروندی، حق بر حریم خصوصی است. در واقع، در یک جامعه دموکراتیک باید توانایی لازم برای ایجاد و حفظ اشکال مختلف از روابط اجتماعی بین شهروندان با مردم وجود داشته باشد. ابزار لازم برای این مقوله آن است که مردم زندگی مستقل از یکدیگر داشته باشند و آنچه در این میان مهم تلقی می‌گردد آسودگی ذهن و آرامش فیزیکی است. *سولو* در کتاب خود تحت عنوان «فهم حریم خصوصی»[5] باور دارد که هیچ‌کس نمی‌تواند معنای حریم خصوصی را به صورت شمرده بیان دارد؛ چراکه مفهومی سیّال و در جریان است(Solve, 2008, p.1).

حریم خصوصی به عنوان یک مفهوم هم‌پوشان، حوزه‌های مختلف مجزّایی از مطالعه و موقعیت‌های رویه‌ای را در بر می‌گیرد. حریم خصوصی، معنایی فراتر از «خصوصی» دارد و محدود به حفاظت از یک «امر نهان» نمی‌شود. این مقوله مدعی پوشش دادن به اطلاعات و فعالیت‌هایی مانند اعتبار بانکی افراد، تجویز دارو توسط پزشک یا داروساز و ... است که اشخاص هر روز با آن سر و کار دارند. همچنین، گفته شده است که حریم خصوصی مشمول موقعیت فیزیکی افراد (مانند خانه و محل کار) و اطلاعات (مانند ارزش خانه و میزان دستمزد) نیز می‌شود. حریم خصوصی از جمله مفاهیمی است که نسبیت در مورد آن مطرح می‌شود؛ چراکه با فرهنگ، اقتصاد و حتی نوع رژیم سیاسی حاکم بر یک کشور مرتبط است. لذا می‌توان گفت که حریم خصوصی امری نسبی است که مفهوم آن از کشوری به کشور دیگر ممکن است متفاوت باشد(رحمدل، ۱۳۸۴، ص۱۲۹).

1. Villiam beaney.
2. Tom gerety.
3. Arthur miller.
4. Daniel solve.
5. Understanding privacy.

۱-۲. مفهوم امنیت[1]

همزمان با به وجود آمدن دولت – ملت و گسترش کارویژه‌های آن، امنیت ملی به عنوان یکی از مهم‌ترین این کارویژه‌ها در دستور کار دولت‌ها قرار گرفت، به‌طوری که اکثریت قریب به اتفاق تحلیل‌گران بر این باورند که ماهیت وجودی دولت‌ها به تأمین امنیت داخلی و خارجی آنها و چگونگی تعریف، بسط و گسترش مفهوم امنیت ملی گره خورده است. در این راستا، دیدگاه‌های متفاوتی راجع به بحث امنیت ملی و چگونگی تأمین آن در میان دولت‌ها و محافل دانشگاهی وجود دارد(خلیلی‌پور رکن‌آبادی و نورعلی‌وند، ۱۳۹۱، ص۱۷۵).

مفهوم امنیت مانند سایر مفاهیم اساسی و رایج در علوم انسانی نظیر صلح، عدالت و آزادی در معرض تفسیرها و تعبیرهای گوناگونی قرار دارد و در طول تاریخ بشری با تغییر و تحولات گسترده‌ای مواجه شده است و مکاتب متعددی نظریات خود را پیرامون این مفهوم ارائه کرده‌اند.

باری بوزان،[2] آن را برابر با رهایی از تهدید تعریف می‌نماید و معتقد است که امنیت در نبود مسئله دیگری به نام تهدید درک می‌شود(عبدالله‌خانی، ۱۳۸۳، ص۱۳۵).

از دید *آرنولد ولفرز*،[3] امنیت در یک مفهوم عینی، به فقدان تهدیدها نسبت به ارزش‌های اکتسابی تلقی می‌شود و در یک مفهوم ذهنی، بر اساس دلهره و نگرانی از به مخاطره افتادن ارزش‌ها و توانمندی‌های لازم در کسب نتایج منصفانه ارزیابی می‌شود(چگینی‌زاده، ۱۳۷۹، ص۶۸).

بنابراین، یکی از دلایل پیچیدگی مفهوم امنیت و ماهیت ابهام‌آمیز آن، چند وجهی بودن مفهوم امنیت است. وجوه و ابعاد مختلف امنیت را می‌توان در محورهای سیاسی، اقتصادی، نظامی، فرهنگی و زیست محیطی دسته‌بندی کرد(ماندل، ۱۳۷۹، صص۸۳-۷۱).

از سوی دیگر، امنیت صرفاً در یک قلمرو یا محدوده خاص قابل پیگیری و دستیابی نیست، بلکه امنیت در قلمروهای مختلف که در عین حال به هم پیوسته و وابسته و دارای تأثیرات متقابل نسبت به یکدیگر می‌باشند، قابل پیگیری و تحلیل است. قلمروهای گوناگون امنیت عبارت است از امنیت فردی، ملی، منطقه‌ای و بین‌المللی. امنیت در لغت،

1. Secyrity.
2. Barri buzan.
3. Arnold wolfers.

حالت فراغت از هرگونه تهدید یا حمله و یا آمادگی برای رویارویی با هـر تهدیـد و حملـه تعریف شده است و در اصطلاح سیاسی و حقوقی به صورت امنیت فردی، اجتماعی، ملـی و بین‌المللی به کار می‌رود، به‌گونه‌ای که امنیت فردی حالت فراغت یک فـرد از تهدیـد و حمله، امنیت اجتماعی، حالت فراغت همگانی از تهدید، امنیت ملی، حالت فراغتی از تهدید یک ملت و امنیت بین‌المللی حالـت فراغـت از تهدیـد قـدرت‌هـا در صـحنه بـین‌المللـی است(آشوری، ۱۳۸۳، صص۳۸ و ۳۹).

۱-۳. مفهوم تروریسم سایبری[1]

این واژه نخستین بار از سوی *کالین باری*،[2] در دهه ۱۹۸۰ مطرح شـد و بیشـتر بـه معنـای حمله یا تهدید به حمله علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آنهـا است، هنگامی که به منظور ترساندن یا مجبور کردن دولـت یـا اتبـاع آن بـرای پیشـبرد اهداف سیاسی یا اجتماعی خاص اعمال می‌شود. به گفته *کانوی*،[3] تروریسم سایبری عبارت است از حمله عمدی و آگاهانه با انگیزه‌های سیاسی به وسیله گروه‌های فرو ملی یا عوامل پنهانی علیه اطلاعات، سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌ها که منتهـی بـه خشونت علیه افراد غیر نظامی و سایر اهداف شود(Seddon, 2004, p.20).

دولت‌ها در تعریف تروریسم غالباً به جرم‌انگاری از طریق بیان مصادیق آن پرداخته‌اند. با این وصف، به خوبی می‌توان دریافت که تروریسم سایبری مفهومی کلی دارد. «آژانـس مدیریت فوق‌العاده فدرال»،[4] تروریسم سایبری را این‌گونه تعریف می‌کند: «تهدید و حمله غیر قانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن، زمانی که برای ترساندن یا مجبور کردن حکومت یـا مـردم آن در پیشـبرد اهـداف سیاسـی یـا اجتمـاعی صـورت می‌گیرد»(Chertoff, 2008, p.4).

تروریست‌ها با از دست دادن پایگاه‌های فیزیکی کلیدی (مانند افغانسـتان)، بـه عامـل کلیدی برای اقدام در فضای سایبری تبدیل شده‌اند. این اقدام‌ها می‌تواند شـامل افـزایش منابع برای حمایت از عملیات‌های خـود، برنامـه‌ریـزی عملیـات (اسـتفاده از ابزارهـای در

1. Cyber terrorism.
2. Calin bari.
3. Kanvey.
4. Federal Emergency Management Agency.

دسترس همانند Google earth)، فرماندهی و کنترل عملیات، انجام عملیات‌های نفوذی و آموزش به هواداران خود (استقرار وسایل انفجاری) باشد(Starr, 2009, p.18).

در تعریف دیگری، تروریسم سایبری عبارت است از: «بهره‌گیری از اینترنت و شبکه‌های رایانه‌ای و امکاناتی که این شبکه‌ها پدید می‌آورند با هدف نابود ساختن ساختارهای زیربنایی یک جامعه مانند انرژی، حمل و نقل، فعالیت‌های دولتی و تأثیر گذاشتن بر یک دولت، شهروندان، گروه‌ها و ...»(عباسی، ۱۳۸۳، ص۳۰).

مارک پلیت در سال ۱۹۹۷ تعریفی از تروریسم سایبری 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. نمی‌توان تعریف بالا را تعریف دقیقی دانست؛ زیرا ممکن است تروریسم سایبری، اهدافی غیر از «اهداف سیاسی» داشته باشد. بنابراین، آنچه از تعاریف موجود به دست می‌آید این است که نوع نگرش، بر تعریف واژه تأثیرگذار است. لذا برای پی بردن به مفهوم تروریسم سایبری نمی‌توان به تعاریف موجود اکتفا کرد و حتی می‌توان گفت که تبیین مصادیق و روش‌های ارتکاب، از تعاریف مهم‌تر است. تروریسم سایبری شامل استفاده از روش‌های متداول هک کردن مانند دسترسی غیر مجاز به رایانه، ویروس‌ها، بمب‌های ایمیلی و غیره، با هدف آسیب رساندن است.

سایبر تروریسم می‌تواند ابعاد داخلی داشته باشد یا شامل موارد بین‌المللی شود. امروزه تروریسم سایبری خطرناک‌تر از تروریسم سنّتی است، به این دلیل که ساختار اقتصادی و خدمات‌رسانی بسیاری از کشورها مبتنی بر فناوری‌های اطلاعاتی و ارتباطی شده است. با وابستگی بیشتر جامعه به سامانه‌های رایانه‌ای، تروریست‌های سایبری از آسیب‌پذیری این سامانه‌ها استفاده می‌کنند. سامانه‌های کنترل ترافیک، تسهیلات پزشکی، نظامی، امنیت عمومی و سامانه‌های ارتباطات از جمله حوزه‌های آسیب‌پذیر است. همچنین، حملاتی که به مرگ یا صدمه جسمی منتهی می‌شوند انفجار، سقوط هواپیما، آلوده کردن آب یا خسارت اقتصادی شدید از جمله موارد تروریسم سایبری است. این پدیده نوین قادر است با استفاده از ابزارهای موجود در فضای سایبر، به خشونت هسته‌ای، بیولوژیکی، شیمیایی و یا هر چیز دیگری که قابلیت تبدیل شدن به سلاح کشتار جمعی را داشته باشد، به منظور دستیابی به اهداف خود در همه سطوح دست بزند. این امر، تهدید جدی برای کلیه

کشورها چه در سطوح محلی، ملی و بین‌المللی است، به‌طوری که دامنه این تهدید حتی به کشورهایی که ظاهراً از کانون این مسئله دور هستند نیز کشیده شده است. برای یک تروریست، تروریسم سایبری بر روش‌های فیزیکی برتری‌هایی دارد، از جمله می‌تواند از راه دور انجام گیرد و احتمال دستگیری توسط طرف مقابل بسیار پایین است و 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. درباره میزان خطرناکی این جرم، یک متخصص تروریسم در مرکز مطالعات استراتژیک و بین‌المللی آمریکا با اشاره به ادعای یک مقام رسمی سیا می‌نویسد که تروریست در فضای سایبر قادر است با یک میلیارد دلار هزینه و ۲۰ هکر شایسته، ایالات متحده را فلج کند. *والتر لاکور*[1] نیز یادآوری می‌کند که اگرچه هدف تروریست‌ها معمولاً قتل سران سیاسی و گروگان‌گیری و ... است اما صدمه‌ای که با حمله الکترونیکی به شبکه‌های رایانه‌ای وارد می‌آید ممکن است بسیار غم‌انگیزتر باشد و اثرات آن تا مدت‌ها باقی بماند(درآنجلیز، ۱۳۸۳، ص۱۶).

۲. شیوه‌های تروریسم سایبری

به نظر *فردِ کهن*،[2] اقدامات تروریستی سایبری روی هم رفته به چهار شیوه انجام می‌شود:

الف) یورش به اطلاعات؛ که همان دگرگونی یا از میان بردن 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 و یا از بین می‌برد.

ج) معاونت فنی در ارتکاب؛ که عبارت است از به‌کارگیری ارتباطات الکترونیکی برای فرستادن نقشه‌ها و طرح‌ها به منظور انجام یورش‌های تروریستی یا تحریک به انجام آنها یا توسل به سایر تسهیلات.

د) افزایش یا ارتقای منابع مالی؛ که به موجب آن، تروریست‌ها با بهره‌گیری از اینترنت

1. Walter lacver.
2. Fred cohen.

برای خشونت سیاسی یا دیگر رفتارها، به گرفتن کمک‌های مالی افراد یا سازمان‌ها می‌کوشند(عالی‌پور، ۱۳۸۹، ص۱۱۸).

۳. تقابل میان حق حریم خصوصی و امنیت ملی در مقابله با تروریسم سایبری

اقدامات تروریستی به‌طور جدّی 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 می‌نماید. همان‌طور که کمیسر عالی سابق حقوق بشر سازمان ملل خانم مری رابینسون اظهار داشت: «اساس حقوق بشر این است که زندگی انسان و کرامت وی نباید به مصالحه گذاشته شود و اعمال خاص دولت‌ها یا غیر دولتی‌ها 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 ضد تروریستی را زیر سؤال می‌برد»(قاسمی و باقرزاده، ۱۳۹۴، ص۲۴۰).

با این حال، سلسله اقدامات دولت‌ها برای مبارزه با تروریسم این پرسش را مطرح می‌کند که آیا نمی‌توان اعمال صورت گرفته را ناقض حق حریم خصوصی محسوب کرد؟ بخصوص این که دولت‌ها پیشگیری از وقوع اعمال تروریستی را بهترین نوع مبارزه به حساب می‌آورند و بعضاً با نقض قواعد بنیادین حقوق بشر به واسطه اقدامات غیر متعارف درصدد تأمین امنیت خویش در چهارچوب حفظ حقوق عمومی بر می‌آیند. مبنای قانونمندسازی و به عبارتی، عادی‌سازی دخالت‌ها را می‌توان پس از حوادث ۱۱ سپتامبر ۲۰۰۱ و در سخنرانی معروف جورج بوش رئیس جمهور پیشین ایالات متحده در جلسه مشترک کنگره با مردم امریکا و استفاده از اصطلاح «یا با ما یا علیه ما» به‌طور ملموس مشاهده کرد(قاسمی و باقرزاده، ۱۳۹۴، ص۲۴۰).

از جمله مهمترین حقوق بشری که به دنبال خنثی کردن اقدامات ضد تروریستی توسط دولت‌ها در معرض نقض قرار می‌گیرد «حق حریم خصوصی» است. همان‌طور که در اسناد بین‌المللی از جمله ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی ۱۹۶۶،[1] آمده

1. International Covenant on Civil and Political Rights, United Nations, 16 December 1966, Article 17.

است حریم خصوصی افراد مصون از تعرض غیر قانونی است. این ماده مقرر 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 غیر قانونی شود». 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. آن قسم از حریم خصوصی که به‌طور خاص در جریان اقدامات ضد تروریستی دولت به بهانه حفظ امنیت ملی مورد خدشه قرار می‌گیرد «حریم خصوصی ارتباطات» است. منظور از حریم خصوصی ارتباطات در معنای خاص، مصون بودن مراسلات و مکاتبات و مخابرات شهروندان از هرگونه تخریب، تفتیش، شنود و دستیابی غیر مجاز است. بر این اساس، انتظار معقول از قوای حاکم آن است که ضمن حمایت جدی از حقوق و آزادی‌های فردی، از هرگونه تعرض غیر مجاز و ناموجه نسبت به حریم خصوصی و خلوت اشخاص، به شدت اجتناب کنند. سوء استفاده از قدرت برای کنترل ارتباطات و مراسلات و نیز انجام بازرسی‌های غیر ضروری و بدون مجوز قانونی، از مصادیق نقض حریم خصوصی شهروندان تلقی می‌شود. این انتظار منطقی در بسیاری از اسناد بین‌المللی نیز تصریح شده است. در ماده ۱۲ اعلامیه حقوق بشر آمده است: «در زندگی خصوصی، امور خانوادگی، اقامتگاه یا مکاتبات هیچ‌کس نباید مداخله‌های خودسرانه شود و نباید به شرافت و اسم و رسمش حمله شود. هر کس حق دارد در مقابل این‌گونه مداخلات و حملات، از حمایت قانون برخوردار شود». همچنین در ماده ۱۱ کنوانسیون آمریکایی 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، از جمله رعایت حریم خصوصی ارتباطات بر آمده است. برای مثال، در این رابطه اصل ۲۵ قانون اساسی جمهوری اسلامی ایران مقرر می‌دارد: «بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آنها، استراق سمع و هرگونه تجسس ممنوع است مگر به حکم قانون»(کنگرانی، ۱۳۸۵، ص۳۹).

مسئله‌ای که پس از ذکر اهمیت حق بر حریم خصوصی مطرح می‌شود این است که چه موقع در فضای سایبر، حریم خصوصی افراد نقض می‌شود؟ در پاسخ به این پرسش

گفته می‌شود که 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 حریم خصوصی نیز بیشتر خواهد شد(انصاری، ۱۳۸۶، ص۱۶).

در معرض خطر قرار گرفتن یا ایراد خدشه به منافعی همچون امنیت ملی، حکومت را ناچار به اتخاذ تدابیر مقابله‌گر یا نظارت پیشگیرانه برای برقراری نظم و امنیت می‌کند که گاهاً ممکن است نقض حریم خصوصی و آزادی‌های افراد را نیز در بر داشته باشد. اصولاً رژیم‌های توتالیتر، به اقتضای ماهیت خود خواستار قدرت نامحدودند و این قدرت تنها در صورتی به دست می‌آید که همه انسان‌ها بدون استثنا در تمام ابعاد زندگی‌شان تحت یک چیرگی قابل اطمینان در آیند. امنیت‌محوری دولت‌ها نیز زمینه‌ساز نقض خلوت شهروندان است؛ بدین معنا که در تزاحم بین حریم خصوصی با امنیت، پیوسته یا بیشتر مواقع امنیت مرجّح شناخته می‌شود. میزان اهمیت امنیت در مبحث جرایم علیه امنیت ملی و تعارض آن با سایر مصالح و منافع از همین جا مشخص می‌شود(محسنی، ۱۳۸۹، ص۵۳۱).

گذشته از رژیم‌های توتالیتر و امنیت‌محوری دولت‌ها، در برخی موارد آنچه که با حریم خصوصی در تعارض است مصالح اجتماعی به معنای واقعی کلمه می‌باشد. به عنوان مثال، می‌توان به تزاحم حق بر خلوت با مصالح و منافع عمومی در پیگیری و کشف جرایم اشاره کرد. این مباحث در مسئله رهگیری ارتباطات اینترنتی افراد از سوی دولت به بهانه‌های مختلف و تعارض آن با حق حریم خصوصی شهروندان نیز مطرح می‌گردد. «رهگیری ارتباطات در فضای سایبر» به معنای آن است که ارگان‌های قانونی و اطلاعاتی، به دلایل مهم و در صورتی که ضرورت قانونی وجود داشته باشد، این امکان و اجازه را پیدا کنند که محتوای در حال انتقال در سامانه‌های مخابراتی و الکترونیکی را زیر نظر قرار دهند. در اعلامیه جهانی حقوق بشر و میثاق بین‌المللی حقوق مدنی و سیاسی، حفظ امنیت ملی، نظم عمومی، سلامت و اخلاق عمومی، حقوق و آزادی‌های دیگران، خطوط قرمز حق خلوت ذکر شده‌اند. ماهیت بسیاری از جرایم مهم، به خصوص جرایم سازمان‌یافته یا جرایم ضد امنیتی، علی‌الخصوص تروریسم و عواقب شوم آنها که متوجه جامعه می‌شود، به‌گونه‌ای نیست که در منظر عموم اتفاق افتد. لذا ذات مخفیانه این‌گونه جرایم از یک سو و آسیب‌های شدید ناشی از آنها از سوی دیگر موجب تجویز رهگیری ارتباطات سایبری

افراد از سوی حاکمیت در این‌گونه موارد می‌شود. از این رو، همیشه بیم آن می‌رود که منافع عمومی به عاملی برای مشروع دانستن تجاوز به حریم خصوصی افراد از سوی حاکمیت تبدیل گردد و حقوق اساسی افراد نادیده گرفته شود؛ زیرا قدرت عمومی اغلب به بهانه ایجاد نظم و امنیت و یا شرایط اضطراری (که معیار عینی و تعریف شده‌ای نیز ندارد) با تصویب قوانین خاص یا وارد کردن استثنائات و تبصره‌هایی به قوانین حمایت‌کننده از حریم خصوصی افراد، به محدود کردن آزادی‌ها و از جمله دخالت در حوزه خصوصی افراد در جهت نیل به اهدافش مبادرت می‌کند. بنا به یک نظر، «دولت‌ها یکی از جدی‌ترین تهدیدکنندگان و ناقضین حریم خصوصی تلقی می‌گردند که در پاره‌ای موارد نیز به مصالح اجتماعی و اخلاق عمومی برای توجیه عملکرد خود استناد می‌کنند»(نوبهار، ۱۳۸۷، ص۲۵۴).

رهگیری ارتباطات سایبری نیز یکی از همین اقداماتی است که در بسیاری از کشورها اعمال می‌شود و دولت‌ها بعضاً به بهانه‌های فوق به آن متوسل می‌گردند. به عنوان مثال، در آمریکا مطابق قانون «برنامه نظارت محرمانه خارجی»، دولت آمریکا می‌تواند بدون دریافت مجوز قانونی و قضایی، ارتباطات الکترونیکی اعم از مکالمات تلفنی و ایمیل‌های اتباع خارجی و آمریکایی‌هایی را که مظنون به عضویت در گروه‌های تروریستی و یا جاسوسی برای دیگر کشورها هستند، رهگیری کند. بر اساس ماده ۸ کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های اساسی ۱۹۵۰، همه حق دارند به حریم خصوصی و زندگی خانوادگی، خانه و مکاتبات آنان احترام گذاشته شود. هیچ مقام دولتی نباید به استفاده از این حق تعرض کند، مگر مطابق قانون و در صورتی که این کار برای مصالح امنیت ملی، امنیت جامعه، پیشگیری از بی‌نظمی یا تبهکاری، حفظ سلامت اخلاقی یا برای حمایت از حقوق و آزادی‌های دیگران در یک جامعه دموکراتیک ضروری باشد.

در حقیقت، پس از دستیابی بشر به رایانه و استفاده گسترده وی از اینترنت، امروزه دیگر نظارت‌ها محدود به جهان فیزیکی نیست و مرز بی‌نهایت فضای مجازی نیز مشمرل حیطه رصدگری دولت شده است. امروزه گروه‌های تروریستی با استفاده از فضای سایبری، تروریسم را گسترش می‌دهند و از فضای مجازی برای استخدام نیرو و افزایش بودجه فعالیت‌هایشان استفاده کرده و راه‌هایی برای همکاری با یکدیگر و نوع جدیدی از تهدید را به وجود می‌آورند. لذا با دگرگونی ابزارهای تهدید، مقابله با آنها نیازمند رویکردها، راهبردها و ابزارهای جدیدی است. با توجه به این که جرایم ارتکابی در فضای سایبر نظیر تروریسم

سایبری، جرایم سازمان‌یافته سایبری و ... به صورت گروهی و «بـر خـط»[1] در حـال رشـد می‌باشند، واکنش در برابر آنها مستلزم استفاده از نیروهای ناظر به منظور پیشگیری است. جهانی شدن جرایم سایبری همچون تروریسم و پر مخاطره شدن جوامع در برخورد با این جرایم، تمایل سیاست‌گذاران را به اولویت بخشیدن امنیت بـر آزادی شـدت بخشـیده کـه تحت تأثیر ورود مجموعه اقدامات کنترلی به نظام حقرقی و سیاسی بوده که در این فضـا اعمال شده و آزادی‌های مدنی را دستخوش تزلزل قرار مـی‌دهنـد(احمـدی و شـمعی، ۱۳۹۵، ص۳۴).

این موضوع در فضای سایبر، تقابل میان حق حریم خصوصی و امنیـت را بـه عنـوان موضوعی چالش‌برانگیز مطرح کرده است. شواهد زیادی مبنی بر نقض حریم خصوصـی و محرمانگی مردم در فضای سایبر توسط دولت به بهانه حفظ امنیت ملی وجود دارد. بـرای مثال، پس از حادثه یازدهم سپتامبر در آمریکا، دولت به منظور بالا بـردن امنیـت داخلـی، قانونی موسوم به «قانون پاتریوت»[2] به تصویب رسانید که به واسطه آن امکان دسترسی به ایمیل‌های شهروندان آمریکایی وجود داشت. مـی‌تـوان گفـت، «در صـورتی کـه منفعـت عمومی حاصل از امنیت ملی بیش از منفعت حاصل از اطلاعات محرمانه باشد، اطلاعـات مورد حمایت واقع نمی‌شوند و به‌طورکلی دادگاه‌ها به امنیت ملی چنان اهمیتی مـی‌دهنـد که بر اساس آن حکم به افشای اطلاعات محرمانه می‌نمایند»(شمعی، ۱۳۹۲، ص۶۲).

ویژگی مشترک تمام سیاست‌های ضد تروریستی این است که برآنند تا اختیارات قـوه مجریه را گسترش دهند و از طرفی پاسخ‌گویی آنها را کاهش دهند، به نحوی که برخی از پرونده‌های مربوط به تنش میان حقوق و آزادی‌هـای فـردی و اقـدامات قـوه مجریـه در کشورهای اروپایی، به دادگاه اروپایی حقوق بشر کشیده شد(هاشمی، ۱۳۹۰، ص۱۶).

۴. ضوابط ناظر بر تحدید حقوق فردی

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 نادیده انگاشتن یا نقض حقوق

1. Online.
2. Patriot Act.

بنیادین بشر بدون واکنش جامعه بین‌المللی و تابعان آن خاتمه پذیرد. در مبارزه با تروریسم دو تکلیف حقوقی در برابر یکدیگر قرار می‌گیرند، یکی تکلیف به حفاظت از آزادی، حیات و امنیت مردم آن کشور، که بیانگر منافع عمومی می‌باشد و دیگری تکلیف به احترام به حقوق بشر و به‌ویژه مظنونان، متهمان و یا محکومان به ارتکاب جرایم تروریستی، که بیانگر منافع خصوصی و شخصی این افراد است. در چنین شرایطی، نظام حقوق بشر به عنوان 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(عبداللهی، ۱۳۸۸، ص۶۸).

با مطالعه اسناد حقوق بشر، حقوق مندرج در این اسناد به دو دسته مطلق و مقید تقسیم می‌شوند. حمایت از برخی حقوق چندان اهمیت دارد که صرف‌نظر از اقلیم جغرافیایی، فرهنگی و سوابق تاریخی محل اجرای آن به هیچ وجه محدود شدن آن را نمی‌توان تحمل کرد و نباید بر آن قیدی نهاد یا محدودهایی برای آن ترسیم کرد. از این قبیل حقوق مثال‌های متعددی می‌توان مطرح کرد. حق حیات، حق برخورداری از محاکمه عادلانه، حق مصونیت در برابر مجازات‌های خشن و غیر انسانی در این دسته جای می‌گیرد و از آنها به عنوان «حقوق مطلق» یاد می‌شود. اما حقوق دیگری هست که اجرای مطلق آنها به علت برخورد با حقوق فردی دیگران یا منافع اجتماعی امکان‌پذیر نیست و باید بر آنها قید نهاد. این حقوق، قید پذیرند و در هر نظام حقوقی، محدوده اعمال معینی دارند. آزادی‌های مدنی و سیاسی عمدتاً در این گروه جای دارند. آزادی عقیده و بیان آن و آزادی‌های مذهب، مثال‌هایی مشهور در این زمینه به شمار می‌آیند که «حقوق مقید» نامیده می‌شوند(قاسمی و باقرزاده، ۱۳۹۴، ص۲۴۶).

در این راستا برخی معتقدند که هیچ قاعده مطلقی وجود ندارد که بدون هیچ استثنایی پذیرفته شود و در شرایطی که تعارض میان دو مصلحت (حفظ امنیت ملی و حفظ حقوق فردی) وجود داشته باشد می‌توان به نفع مصلحت عظیم‌تر حکم کرد که ممکن است بقای نظام و امنیت کشور باشد(آقابابایی، ۱۳۸۹، ص۵۴).

اما پرسش این است که محدوده نقض باید تا چه میزان باشد؟ آنچه که از اسناد و رویه‌های بین‌المللی و بررسی حقوق سایر کشورها بر می‌آید این است که این موارد نقض همواره باید به صورت استثنایی و با شرایطی خاص صورت گیرد؛ یعنی اولاً این

محدودیت‌ها قانونی و به موجب قانون پیش‌بینی شده باشد. ثانیاً با حسن نیت باشد؛ یعنی چون احراز موارد تزاحم با حکومت است، حکومت نباید از آن به عنوان ابزاری برای نیل به منافع صرفاً سیاسی خود بهره‌گیری کند. ثالثاً متناسب باشد؛ یعنی محدودیت‌ها با خطری که در صورت نبودن محدودیت جامعه را تهدید می‌کند، تناسب داشته باشد(قربان‌نیا، ۱۳۸۵، ص۲۰). این خطر معمولاً ناظر به شرایط بحران است و نه وضعیت‌های فشار(صدر توحیدخانه، ۱۳۸۸، ص۴۶۷). رابعاً به دلیل ابزاری بودن مصلحت عمومی، اگر زمانی بتوان در ادامه تطور و تکامل زندگی جمعی انسان بدون تمسک به مفهوم و نهاد مصلحت عمومی از کیان جمعی و اصل زندگی گروهی حفاظت کرد، دیگر نیازی به آن نخواهد بود(راسخ و بیات کمیتکی، ۱۳۹۳، ج۲، ص۵۶۶).

در ایالات متحده رویکرد سختگیرانه نسبت به جرایم تروریستی و محدود کردن حقوق بنیادین متهمین این جرایم پس واقعه ۱۱ سپتامبر با لحاظ همین رویکرد صورت گرفته است، به‌گونه‌ای که متهمین این جرایم دیگر شهروند محسوب نشده، بلکه دشمن‌اند که باید با آنها جنگید و این جنگ بر اساس حق مشروع شهروندان یعنی حق برخورداری آنان از امنیت رخ می‌دهد. این جنگ در پی طرد و اخراج دشمن است و همانند کیفر نیست که کیفرشونده نسبت به آن حقی داشته باشد(یزدیان جعفری، ۱۳۹۵، ص۷۷)، اگرچه دیوان عالی این کشور نیز پس از چند سال به فکر وارد کردن اصول انسانی و بشری در گفتمان حقوقی جرایم تروریستی افتاده است(یزدیان جعفری، ۱۳۹۵، ص۴۷۷).

در مقابل، اعتقاد دیگری وجود دارد مبنی بر این که نقض برخی از حقوق حتی در شرایط سخت مطلقاً نادرست است؛ زیرا اگرچه ممکن است شر کمتری ایجاد کند اما همچنان شر است و هرکس مرتکب آن شود مقصر است(تبیت، ۱۳۸۴، ص۱۷۳).

هیچ دولتی نمی‌تواند با استناد به دلایل مبتنی بر منافع امنیتی، حیاتی، ملی و خصوصی از شمول تعهدات برگرفته از اصول ذاتی و لایتغیر تخطی کند(ممتاز و شریفی طرازکوهی، ۱۳۹۰، ص۲۰).

در چنین دیدگاهی، حق نسبت به خیر عمومی مقدّم است. دغدغه اصلی حکومت، حفظ حقوق افراد است و برای تحدید یا تضییق آن، دلیل قوی‌تری از خیر عمومی لازم است. در جوامع لیبرال، برخی حقوق آن‌قدر صبغه بنیادین دارند که قانون نه تنها در آنها دخالت نمی‌کند، بلکه خود را ملزم به حمایت از آن می‌بیند. بنابراین، تأکید حتی بر خواست عمومی و جمعی بدون توجه به مبانی و آثار حقوق اساسی و بنیادین فرد نمی‌تواند دقیق

باشد. لذا باید قلمروی تعیین کرد که هیچ قدرت سیاسی یا اجتماعی، مشروع یا نامشروع، تفکیک شده یا یکپارچه، حق هیچ‌گونه مداخله‌ای در آن را نداشته باشد(فلاحی، ۱۳۹۳، ص۹۰). به علاوه، منفعت عموم نه منفعت دولت است و نه منفعت قانونگذار. منفعت عمومی چیزی جز منفعت افراد نیست و به عقیده *رز*[1] فیلسوف انگلیسی، منفعت عمومی و فردی درهم تنیده و یکی است و به نظر او، خیر عمومی به معنای خیر همگان است که شامل خیر صاحبان فردی حق نیز می‌شود. از این رو، با حمایت از خیر و منفعت فرد، در حقیقت به حفظ و حمایت از منفعت عمومی پرداخته‌ایم و در مقابل با تضمین منفعت عمومی، در واقع خیر فرد را نیز تضمین کرده‌ایم(راسخ، ۱۳۹۳، ج۲، ص۹۴). به عبارت دیگر، مرکز ثقل امنیت، عدالت است و بدون آن امنیت لرزان و سست خواهد بود(آقابابایی، ۱۳۸۹، ص۵۳). حتی در حوزه حدود اسلامی نیز سختگیری و شدت عمل در مورد رفتارهای مجرمانه‌ای است که امنیت و آسایش عمومی شهروندان را هدف قرار می‌دهند(مانند حد محاربه) و در جرایم علیه دولت و حاکم، مسالمت و مدارا و توجه به مطالبات مخالفان توصیه می‌شود(آقابابایی، ۱۳۸۴، ص۳۷).

حقوق کیفری در جوامع مردم‌سالار نسبت به کسانی که امنیت حکومت را مورد خدشه قرار داده‌اند نه تنها کمتر نیست، بلکه مورد تأکید بیشتری است؛ زیرا یکی از شاخص‌های سنجش میزان اعتقاد حکومت به عدالت را باید در شیوه برخورد با مخالفان سنجید(آقابابایی، ۱۳۸۴، ص۱۸). حق بر امنیت سایر شهروندان نمی‌تواند نقض حقوق مشروع مظنونین، متهمین و مجرمین را توجیه کند(رضوانی، ۱۳۹۱، ص۱۹).

در حقیقت، کسانی که نقض حقوق فردی را موجه می‌دانند عمدتاً به مصلحت متوسل می‌شوند و مراد از مصلحت را یکی از این سه معنا می‌دانند:

۱- مصلحت یعنی نفع عظیم‌تر

۲- مصلحت یعنی یک حق رقیب

۳- مصلحت یعنی ضرورت

در مورد معنای نخست این‌گونه استدلال می‌شود که با فدا کردن حق فرد، حق جامعه در تأمین امنیت حفظ می‌شود و این در مجموع نفع بیشتری را نصیب افراد بیشتر می‌کند. اما باید توجه داشت که منفعت عمومی نمی‌تواند دلیل خوبی برای محدود کردن حق فرد

1. Ros.

باشد؛ زیرا این نفع احتمالی است و حتی نمایندگان مردم ممکن است درباره خواست‌های جامعه داوری نادرستی داشته باشند و بر اساس ملاحظاتی کاملاً بی‌ربط با ارتقای حداکثری خیر عمومی عمل کنند(بودنهایمر، ۱۳۹۳، ص۱۰۸). به علاوه، سیاست‌های مصلحت عمومی باید در پی تقویت کرامت انسان باشد و نه خواری او. فدا کردن حقوق فردی در مقابل مصلحت عمومی حاکی از آن است که حقوق ریشه در احترام به شخصیت انسانی ندارند، بلکه صرفاً برخاسته از ملاحظات سودگرایانه حکومت است. حال آن که باید حمایت از آزادی‌های فردی هدف انحصاری حکومت بوده و قلمرو مصلحت عمومی به همین کارکرد فرو کاسته شود(بودنهایمر، ۱۳۹۳، صص۱۱۳و۱۱۴). حتی از دید سودانگارانه ممکن است اگر حکومت به نفع فرد خطا کند، صرفاً کمی بیش از آن چیزی که بر آن مصمم شده بود باید برای نظام اجتماعی هزینه کند، اما اگر علیه فرد مرتکب اشتباه شود، اهانتی بر او روا داشته شده که هزینه بسیار زیادتری باید بشود تا جلوی آن اهانت گرفته شود(دورکین، ۱۳۹۳، ص۲۳۳).

در مورد معنای دوم، فدا کردن حقوق بدان دلیل صورت می‌گیرد که در رقابت با سایر حقوق، مغلوب می‌شوند و در اینجا حق جامعه به نگهداری درجه‌ای از امنیت مطلوب خود است. این استدلال نیز مردود است؛ زیرا حقوق در صورتی می‌توانند رقیب یکدیگر باشند که از یک سنخ محسوب شوند. حق فرد را تنها حق افراد دیگر می‌تواند محدود کند و نه حقوق جامعه و امنیت اجتماعی(دورکین، ۱۳۹۳، ص۲۲۴).

در مورد معنای سوم، یک موقعیت اضطراری، توجیه خوبی برای نقض حقوق فردی است. در این دیدگاه، به خاطر وجود یک خطر جدی که البته به صورت موقتی است، برای دفع آن خطر، حقوق افراد محدود می‌شود. پس یک اقدام دائمی نخواهد بود و به محض رفع خطر، محدودیت‌ها نیز باید رفع شود. اینجا نیز لازم است این موقعیت واقعی باشد و هیچ دلیل و مدرک واقعی وجود ندارد که تساهل در برابر نافرمانی مدنی موجب ازدیاد نافرمانی شود، چه رسد به این که موجب ازدیاد جرم گردد. بر عکس، معقول به نظر می‌رسد که بگوییم تساهل موجب افزایش احترام به مقامات شده یا لااقل جلوی رشد بی‌احترامی را خواهد گرفت. پس این که تساهل منجر به نابودی جامعه شود کاملاً بی‌پایه است(دورکین، ۱۳۹۳، ص۲۲۷). به علاوه، حکومت‌هایی که به این توجیه متوسل می‌شوند، با قانونگذاری‌های دائمی خود عملاً راه برداشتن محدودیت‌ها را سد می‌کنند.

در واقع، توسل به مفهوم مصلحت در مقابل حقوق فردی ناشی از عدم تفکیک میان مقام نظر و عمل است. در مقام عمل، میان میزان قدرت واقعی ما در عملی ساختن نمونه آرمانی فاصله هست. باید فاصله موجود را شفاف کرد و تصمیمی به فراخور امکانات واقعی گرفت و همچنان به نظریه قابل دفاعی که ارائه شده است وفادار ماند. مهم حرکت به سمت نظریه و الگو است. لذا نباید محدودیت‌های عملی را به جای نظر نشاند و نام مصلحت بر آن نهاد(راسخ، ۱۳۹۳، ج۲، ص۲۶۴).

آنچه که از فقه اسلامی نیز بر می‌آید آن است که ورود به بحث مصلحت در فضای حکومتی بنی‌امیه، بنی‌عباس و پادشاهان بعدی وجود داشته است؛ یعنی برای توجیه دینی دادن به عملکرد حکومت، آموزه مصلحت را به کار گرفته‌اند(آقابابایی، ۱۳۸۴، ص۱۸۷).

اصل مصلحت زمانی می‌تواند راهگشا باشد که با معیارهای عینی و نظارت‌پذیر همراه باشد و الا زمینه سوء استفاده دولت در محدود کردن آزادی‌های بنیادین را فراهم خواهد ساخت(آقابابایی، ۱۳۸۴، ص۱۹۳).

در این زمینه شورای قانون اساسی فرانسه، نظام افتراقی حتی برای جرایم تروریستی را با اجتماع دو شرط قبول کرده است؛ یکی ناشی نشدن این تفاوت‌ها از تبعیض‌های ناموجه و دیگری تضمین‌های برابر برای اصحاب دعوا به ویژه رعایت حقوق دفاعی. این در حالی است که این شورا تعمیم این سیستم را برای جرایم علیه امنیت کشور رد کرده است؛ زیرا معتقد است که جرایم اخیر، خصوصیات مشابهی با جرایم تروریستی ندارند(مارتی، ۱۳۹۳، ص۴۲۷).

به نظر می‌رسد که از جمع‌بندی مطالب پیش‌گفته می‌توان این نتیجه را پذیرفت که گاهی اوقات شکستن حریم حقوق فردی لازمه پیشگیری یا اصلاح معضلی است که از طریق دیگر قابل اصلاح نیست و به نظر می‌رسد که نمی‌توان دولت را به‌طور کلی از مداخله در امور شخصی افراد ممنوع نمود. لذا بهترین راه ممکن جهت حفظ و صیانت حریم خصوصی افراد در فرآیند اقداماتی همچون رهگیری ارتباطات سایبری شهروندان در موارد ضروری همچون پیشگیری یا کشف اقدامات تروریستی، به‌کارگیری حداقلی و ضابطه‌مند کردن حداکثری این‌گونه اقدامات و تعیین دقیق شرایط و ضوابط و حدود و ثغور آن می‌باشد. به عبارت دیگر، برای ممانعت از بازگشت تاریخ به نفع اختیارات مقامات عمومی برای دست‌اندازی به حقوق فردی باید موارد منافع جمعی مهم که نسبت به حریم خصوصی افراد به‌طور استثنایی اولویت دارد، به صراحت مشخص گردد؛ زیرا در غیر این

صورت ممکن است از یک سو حریم خصوصی افراد دچار خدشه گردد و از سوی دیگر، این مسئله موجب بی‌اعتمادی شهروندان نسبت به دستگاه قضایی و دولت شود.

نتیجه

با گسترش انقلاب‌های تکنولوژیک و ظهور فضای سایبر، از یک سو مفهوم قلمرو زدایی مطرح شده است و از سوی دیگر تغییر ماهیت تهدیدهای امنیتی و مفهوم مرز و حراست از آن به مسئله‌ای حیاتی مبدل گردیده است. ویژگی جهانی و بدون مرز بودن چنین فضایی با توسل به فناوری اطلاعات، امنیت ملی را با چالشی جدی مواجه کرده است. هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری موجب شده است تا بازیگران اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و حتی افراد به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، جرایم سایبری، تروریسم سایبری، جاسوسی سایبری و ... را به وجود آورند. در این بحبوحه، حقوق کیفری زمانی می‌تواند به رسالت خود عمل کرده باشد که بتواند میان حفظ نظم و امنیت اجتماعی از یک سو و حقوق و آزادی‌های فردی از سوی دیگر توازن ایجاد کند.

حریم خصوصی به اندازه امنیت ملی مقوله‌ای مهم تلقی می‌شود. بنابراین، نمی‌توان راه افراط و تفریط پیمود و یکی را فدای دیگری کرد. استفاده دولت از حق خود برای مقابله با تروریسم سایبری و یا پیشگیری از آن و حفظ امنیت خویش نمی‌تواند به بهای نقض فراگیر حریم خصوصی تمام شود مگر با دلایل و توجیهات ویژه.

تمسک به اصل مصلحت در این زمینه زمانی می‌تواند راهگشا باشد که با معیارهای عینی و نظارت‌پذیر همراه باشد و الا زمینه سوء استفاده دولت در محدود کردن آزادی‌های بنیادین را فراهم خواهد ساخت. به عبارت دیگر، موارد نقض حق حریم خصوصی افراد به بهانه پیشگیری از تهدیدات امنیتی همچون تروریسم سایبری یا مقابله با آنها همواره باید به صورت استثنایی و با شرایطی خاص صورت گیرد؛ یعنی اولاً این محدودیت‌ها قانونی و به موجب قانون پیش‌بینی شده باشد. ثانیاً با حسن نیت باشد؛ یعنی چون احراز موارد تزاحم با حکومت است، حکومت نباید از آن به عنوان ابزاری برای نیل به منافع صرفاً سیاسی خود بهره‌گیری کند. ثالثاً متناسب باشد؛ یعنی محدودیت‌ها با خطری که در صورت نبودن محدودیت، جامعه را تهدید می‌کند، تناسب داشته باشد. همچنین، در صورتی که به هنگام ترسیم قلمرو قانونی حمایت از حریم خصوصی افراد رویکرد موسعی اتخاذ شود، ممکن است در عمل برای مجریان قانون مشکلات عدیده‌ای به وجود آید. تردیدی نیست که این

حریم محترم و خدشه‌ناپذیر است، اما نباید به‌گونه‌ای تعریف شود کـه مجریـان قـانون در مقابل مجرمان سایبری خلع سلاح شوند و عملاً از تعقیب و کیفر آنان بازماننـد کـه ایـن خود به تجری آنها و ترغیب به ارتکاب جرایم شدیدتر و گسترده‌تر منجر خواهد شد.

فهرست منابع

الف. کتاب‌های فارسی

۱. آشوری، داریوش؛ *دانشنامه سیاسی*، انتشارات مروارید، چاپ دهم، تهران، ۱۳۸۳.

۲. آقابابایی، حسین؛ *قلمرو امنیت در حقوق کیفری*، پژوهشگاه فرهنگ و اندیشه اسلامی، چاپ اول، تهران، ۱۳۸۹.

۳. انصاری، باقر؛ *حقوق حریم خصوصی*، سمت، تهران، ۱۳۸۶.

۴. بودنهایمر، ادگار؛ *درآمدی بر نظریه مصلحت عمومی*، ترجمه محمد راسخ، مندرج در مجموعه مقالات حقوق و مصلحت، انتشارات طرح نو، چاپ چهارم، ۱۳۹۳.

۵. تبیت، مارک؛ *فلسفه حقوق*، ترجمه حسن رضایی خاوری، انتشارات دانشگاه علوم اسلامی رضوی، چاپ اول، مشهد، ۱۳۸۴.

۶. درآنجلیز، جینا؛ *جرایم سایبر*، ترجمه سعید حافظی و عبدالصمد خرم‌آبادی، دبیرخانه شورای عالی اطلاع‌رسانی، ۱۳۸۳.

۷. دورکین، رونالد؛ *جدی گرفتن حق‌ها*، ترجمه محمد راسخ، مندرج در مجموعه مقالات حقوق و مصلحت، انتشارات طرح نو، چاپ چهارم، تهران، ۱۳۹۳.

۸. راسخ، محمد؛ *حقوق اقتضای حداقلی عدالت*، مندرج در مجموعه مقالات حق و مصلحت، جلد دوم، نشر نی، چاپ سوم، تهران، ۱۳۹۳.

۹. راسخ، محمد و بیات کمیتکی، مهناز؛ *مفهوم مصلحت عمومی*، مندرج در مجموعه مقالات حق و مصلحت، جلد دوم، نشر نی، چاپ سوم، تهران، ۱۳۹۳.

۱۰. رضوانی، سودابه؛ *مدیریت انسان‌مدار ریسک جرم*، با دیباچه علی‌حسین نجفی ابرندآبادی، میزان، چاپ اول، ۱۳۹۱.

۱۱. شمعی، محمد؛ *درآمدی بر جرم‌انگاری و جرم‌زدایی*، انتشارات جنگل، تهران، ۱۳۹۲.

۱۲. صدر توحیدخانه، محمد؛ *حقوق در چنبره دشمن از سیاست آمریکایی جنگ با ترور تا نظریه آلمانی حقوق کیفری دشمنان*، تازه‌های علوم جنایی، نشر میزان، چاپ اول، ۱۳۸۸.

۱۳. عالی‌پور، حسن؛ *جرایم ضد امنیت ملی*، انتشارات خرسندی، تهران، ۱۳۸۹.

۱۴. عبدالله‌خانی، علی؛ *نظریه‌های امنیت مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی(۱)*، مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر، چاپ نخست، تهران، ۱۳۸۳.
۱۵. عبدالهی، محسن؛ *تروریسم، حقوق بشر و حقوق بشردوستانه*، شهردانش، تهران، ۱۳۸۸.
۱۶. فلاحی، احمد؛ *اصل ضرورت در جرم‌انگاری*، نشر دادگستر، چاپ اول، تهران، ۱۳۹۳.
۱۷. کنگرانی، مهدی؛ *قانون اساسی و قانون مدنی*، جمال الحق، تهران، ۱۳۸۵.
۱۸. مارتی، میری دلماس؛ *نظام‌های بزرگ سیاست جنایی*، ترجمه علی‌حسین نجفی ابرندآبادی، نشر میزان، چاپ دوم، ۱۳۹۳.
۱۹. ماندل، رابرت؛ *چهره متغیر امنیت ملی*، ترجمه پژوهشکده مطالعات راهبردی، پژوهشکده مطالعات راهبردی، تهران، ۱۳۷۹.
۲۰. محسنی، فرید؛ *حریم خصوصی اطلاعات*، نشر دانشگاه امام صادق، چاپ اول، ۱۳۸۹.
۲۱. ممتاز، جمشید و شریفی طرازکوهی، حسین؛ *حداقل قواعد بشردوستانه قابل اجرا در آشوب‌ها و شورش‌های داخلی مذکور در حقوق بشردوستانه بین‌المللی*، نشر میزان، چاپ اول، تهران، ۱۳۹۰.
۲۲. نوبهار، رحیم؛ *حمایت حقوق کیفری از حوزه‌های عمومی و خصوصی*، انتشارات جنگل، چاپ اول، تهران، ۱۳۸۷.
۲۳. هاشمی، سیدحمید؛ *تروریسم از منظر حقوق اسلام و اسناد بین‌المللی*، پژوهشگاه حوزه و دانشگاه، تهران، ۱۳۹۰.

ب. مقاله‌های فارسی

۲۴. آقابابایی، حسین؛ *گفتمان فقهی و جرم‌انگاری در حوزه جرایم علیه امنیت و دولت*، مجله فقه و حقوق، شماره پنجم، ۱۳۸۴.
۲۵. احمدی، سیدمحمدصادق و شمعی، محمد؛ *نظارت پیشگیرانه دولت: تقابل امنیت و آزادی*، فصلنامه راهبرد، شماره ۷۹، ۱۳۹۵، صص۴۶-۲۹.
۲۶. چگینی‌زاده، غلامعلی؛ *رویکردی نظری به مفهوم امنیت ملی در جهان سوم*، مجله سیاست خارجی، سال ۱۴، شماره ۱، ۱۳۷۹.

۲۷. خلیلی‌پور رکن‌آبادی، علی و نورعلی‌وند، یاسر؛ *تهدیدات سایبری و تأثیر آن بر امنیت ملی*، فصلنامه مطالعات راهبردی، شماره ۵۶، ۱۳۹۱، صص۱۹۶-۱۶۷.
۲۸. رحمدل، منصور؛ *حق انسان بر حریم خصوصی*، مجله دانشکده حقوق و علوم سیاسی، شماره ۷۰، ۱۳۸۴.
۲۹. سلمانی‌زاده، محمود؛ *جنگ اطلاعات و امنیت*، خبرنامه انفورماتیک، سازمان برنامه و بودجه کشور، شماره ۸۰، آذر و دی ۱۳۸۰.
۳۰. عباسی، مهدی؛ *اینترنت ابزار سیاست تروریسم مجازی*، نشریه فرهنگی و فناوری، سال اول، شماره سوم، دی و بهمن۱۳۸۳.
۳۱. قاسمی، غلامعلی و باقرزاده، سجاد؛ *جایگاه حقوق بشر در مبارزه با سایبر تروریسم*، مجله حقوقی بین‌المللی، شماره ۵۲، ۱۳۹۴، صص۲۵۴-۲۲۷.
۳۲. قربان‌نیا، ناصر؛ *تحدید حقوق و آزادی‌ها*، مجله فقه و حقوق، شماره ۱۰، ۱۳۸۵.
۳۳. یزدیان جعفری، جعفر؛ *تقابل امنیت فردی و ملی در جرایم علیه امنیت*، پژوهش حقوق کیفری، شماره چهاردهم، ۱۳۹۵، صص۸۱-۵۹.

ج. منابع خارجی

34. Chertoff, Michael; "*The cyber security Challenge*", Regulation & Governance. Congressional Research Service(CRS) (2008); *"Botnets, Cybercrime and Cyber terrorism: Vulnerabilities and Policy Issues for Congress"*, Available at: www.crs.org, (accessed by July 23, 2011).
35. Seddon, Embar; "*Cyber terrorism*", Edited Alan Oday, Ash gate Publishing company, 2004.
36. Solve, Leinad; "*Understanding privacy*", Harvard university press, Londen, Englnd, 2008.
37. Starr, Stuart H.; "*Towards an Evolving Theory of Cyber power*", Center for Technology and National Security Policy(CTNSP), National Defense University(NDU), 2009.
38. Walker, Clive; *"Cyber Terrorism: Legal Principle and Law in the United Kingdom"*, Penn State Law Review, Vol.110, 2006.

Judgment, No.91, Autumn 2017

The Confrontation between the Right to Privacy and National Security against Cyber Terrorism

Younes Fathi [*]
Kheirollah Shahmoradi[**]

Received: 27/09/2017 *Accepted: 26/11/2017*

***Abstract**:*
National security and the attempts for substantiating and protecting it, are of the main tasks in any political system. However, terrorism, as one of the most serious threats to the security of any political system, has evolved from its traditional form with the help of technological advances in recent decades and found a new place in cyberspace that comparing to its previous form, it becomes even more advanced and dangerous. In fact, terrorism, in its new place and form, has increasingly put the security of countries at risk. National security may be protected by such measures as punishment of the terrorists and/or implementation of crime prevention policies, but, measures taken for protecting security may conflict with the right to privacy in some cases. Thus, such conflict has raised a question regarding which one is prior to the other and therefore, should be put first. This article seeks to answer such question.

Key words: *Cyber, Terrorism, National Security, Right to Privacy.*

[*]Assistant Professor at Literature and Humanities Faculty of Bu-Ali Sina University.
fathi3320@gmail.com
[**]M.A in Criminal Law and Criminology at Qom University.
shahmoradikhirollah@yahoo.com