فصلنامه علمی مطالعات بین‌المللی پلیس / دوره دهم / شماره ۳۸ / تابستان ۱۳۹۸ صفحات ۱۴۰ - ۱۱۵

تروریسم سایبری در پرتوی وضعیت بزه‌دیدگان آن

(مطالعهٔ تطبیقی: حقوق ایران و اسناد بین‌المللی)

محمدجواد حیدریان دولت‌آبادی[۱]

رسول مظاهری کوهانستانی[۲]

چکیده

زمینه و هدف: فضای مجازی مانند فضای واقعی، مکانی را برای ارتکاب جرائم توسط بزهکاران فراهم کرده است و کنشگران حاضر در این موقعیت را مورد سوءاستفاده قرار می‌دهند. ماهیت گسترده و فراملی بودن این بزه باعث شده است تا از حیث مقابله با جرم سایبری و حمایت از بزه‌دیدگان آن تاکنون اقدام مؤثری از سوی تابعان فعال حقوق بین‌الملل صورت نپذیرد. با توجه به شیوع حملات سایبری در سراسر جهان، لزوم توجه به بزه‌دیدگان تروریسم سایبری در حقوق موضوعه و اسناد بین‌المللی به شدت دیده می‌شود. هدف این مقاله، مطالعهٔ تطبیقی حقوق ایران و اسناد بین‌المللی در مبارزه با تروریسم سایبری و توجه به حقوق بزه‌دیدگان است.

روش تحقیق: پژوهش حاضر از نظر هدف، کاربردی است که به صورت تحلیلی- توصیفی با استفاده از منابع، اسناد و قوانین داخلی و خارجی موجود انجام گرفته است.

یافته‌ها و نتیجه‌گیری: در راستای حمایت از بزه‌دیدگان تروریسم سایبری در حقوق ایران، هیچگونه مقررهٔ ویژه‌ای اندیشیده نشده است. با تعیین کیفر برای مرتکبان جرائم سایبری فقط حمایت‌های کیفری برای بزه‌دیدگان سایبری اتخاذ شده و دیگر نیازهای بزه‌دیدگان بدون جبران باقی مانده است. بنابراین، جبران خسارت مادی ناشی از بزه‌دیدگی سایبری نیز، فقط با استناد به برخی قواعد عام، همچون قانون مسئولیت مدنی برای جبران خسارت مادی از بزه‌دیدگان سایبری اقدام شده و برای مسئولیت معنوی نیز چاره‌ای اندیشه نشده است. اسناد بین‌المللی نیز با وجود اهتمام ویژه به موضوع تروریسم در قالب قطعنامه‌ها، پروتکلها و اعلامیه‌های الزام‌آور در زمینهٔ جرم‌انگاری رفتارهای بزهکارانهٔ تروریستی، سندی مختص به تروریسم سایبری وجود نداشته و در دیگر اسناد مرتبط با تروریسم، به جرم‌انگاری تروریسم سایبری و حمایت از بزه‌دیدگان پرداخته نشده است.

کلید واژه‌ها: تروریسم سایبری، بزه‌دیدگان، سازمان‌های بین‌المللی، حقوق ایران، اسناد بین‌المللی

---

۱. دانشجوی کارشناسی ارشد حقوق بین‌الملل دانشگاه تهران، (نویسندهٔ مسئول)
mjhd1377@gmail.com

۲. استادیار گروه حقوق دانشگاه اصفهان

مقدمه

تروریســـم سایبری صرف، به اقدامات خشونت‌آمیز سایبری از سوی گروهی با ویژگی‌های خاص اطلاق می‌شـــود که به اهداف مشـــخصی تعرض می‌کنند. اقدامات تروریســـتی باید در حـــدی باشـــند که بتوان معادل جنـــگ اطلاعات را برای آن‌ها بـــکار برد. جنگ اطلاعات یک اقدام تروریســـتی اســـت که برای ایجاد اختلال یا آسیب‌رســـانی یا قطع جدی ارتباطات طرح‌ریزی می‌شود. گستردگی فضای سایبر و به خدمت گرفتن آن توسط اکثر افراد جامعه و زیرساخت‌های کشور، طیف گسترده‌ای از مباحث را پیرامون بزه‌دیدگان این پدیده و چگونگی حمایت و جبران خسارت‌های وارد آمده به آن‌ها را چه در حقوق داخلی کشورمان و کشورهای دیگر و چه در سطح بین‌الملل شکل داده است.

با توجه به شـــیوع حملات سایبری در سرتاســـر جهان، لزوم توجه به بزه‌دیدگان تروریسم سایبری در حقوق موضوعه و اسناد بین‌المللی دیده می‌شود. کشور ما نیز از حملات سایبری مستثنی نبوده، به‌طوری که در سال‌های اخیر به دلیل شدت گرفتن مخالفت سران کشورهای اروپایـــی و غربی به ادامهٔ فعالیت‌های هســـته‌ای در ایران، حملاتی به قصد مختل کردن این تأسیســـات از سوی برخی کشورها از قبیل اسرائیل و آمریکا صورت گرفته است. در خصوص موضع حقوق کیفری ایران در مقابله با تروریســـم می‌توان گفت که قانون‌گذار کیفری ایران فاقد جرم‌انگاری مستقل در مورد تروریسم و جرائم آن است و در واقع سیاست جنایی ایران مبتنی بر سیاســـت مصداقی اســـت و می‌توان مواردی را که با مفهوم تروریسم منطبق است تشخیص داد. از جمله موارد جرم‌انگاری‌شده که می‌توان برای مقابله با تروریسم استناد کرد، محاربه است و البته عده‌ای معتقدند که با جرم‌انگاری عنوان فقهی محاربه می‌توان با تروریسم و اشکال آن مقابله کرد، ولی آشکار است که با توجه به گسترش فناوری‌های نوین و استفادهٔ گروه‌های تروریستی از آن، دیگر محاربه قادر نیست به تمامی این رفتارها پاسخ دهد.

ســـازمان ملل متحد، به عنوان بزرگ‌ترین مرجع بین‌المللی، از ســـال ۱۹۶۳ تاکنون، دربارهٔ تروریســـم و اقدامات تروریستی، سیزده سند بین‌المللی به تصویب رسانده و جالب اینکه تنها در سه سند صراحتاً به عنوان تروریسم اشاره شده و در بقیه تنها مصادیق اقدامات تروریستی برشـــمرده شـــده است. آنچه در اســـناد بین‌المللی در رابطه با عنصر قانونی تروریسم سایبری

می‌توان یافت، جرائمی هستند که بیش‌ترین ظهور را در مفهوم تروریسم سایبری دارند و به‌صورت عام و غیرمستقیم به تروریسم سایبری اشاره کرده‌اند. بنابراین، در زمینهٔ حمایت و پشتیبانی از بزه‌دیدگان تروریسم سایبری، کنوانسیون‌هایی همچون کنوانسیون جرائم سایبر به‌طور عام به حمایت از بزه‌دیدگان سایبری پرداخته‌اند و تنها از طریق تطبیق و مقایسه می‌توان مقررات آن‌ها را برای بزه‌دیدگان تروریسم سایبری استدلال و استخراج کرد. لذا در این مقاله تلاش شده است با روش توصیفی و تحلیلی پس از جمع‌آوری و تبیین مقررات کیفری داخلی و بین‌المللی موجود و تحلیل آن‌ها، با توجه به ضرورت حمایت از بزه‌دیدگان تروریسم سایبری در عرصهٔ حقوق داخلی و حقوق بین‌الملل، چاره‌اندیشی مناسبی شناسایی و ارائه کرد.

حمایت‌های کیفری و مدنی از بزه‌دیدگان تروریسم سایبری در حقوق ایران

حمایت کیفری از بزه‌دیدگان تروریسم سایبری: حمایت کیفری از طریق جرم‌انگاری و کیفرگذاری رفتارهای هنجارشکن، به حمایت از بزه‌دیدگان و جلوگیری از بزهکار شدن افرادی گام برمی‌دارد که در آستانهٔ بزهکاری هستند. با توجه به مطالب فوق، تروریسم سایبری از جهات گوناگون می‌تواند مورد حمایت کیفری قرار گیرد. بنابراین، از آنجایی که بزه تروریسم سایبری دارای مقررهٔ اصلی و عمدهٔ کیفری نیست و نیز با توجه به اینکه ادبیات جزایی کشورمان تحت این عنوان نپرداخته، بلکه در یک یا دو دستهٔ کلی، جرائمی را که بعضاً ظهور در این جرم دارند را مورد بحث قرار داده است، از این‌رو با ضعف ادبیات جزایی مواجه است. در راستای حمایت کیفری از بزه‌دیدگان تروریسم سایبری، در ادامه به شرح سه گونه از این اعمال در رابطه با حمایت از بزه‌دیدگان مذکور پرداخته می‌شود:

– **حمایت کیفری ساده:** حمایت کیفری ساده، یکی از گونه‌های حمایت کیفری محسوب می‌شود که «شامل جرم‌انگاری هر رفتار منع شده‌ای است که به‌طور معمول نیازمند تأسیس ضمانت اجرای کیفری است» (رایجیان اصلی، ۱۳۹۰ الف: ۸۱). حمایت‌های کیفری ساده از بزه‌دیدگان تروریسم سایبری، به مقررات کیفری مرتبط با بزه‌دیدگان مذکور که بیشتر داده‌ها، سیستم‌های رایانه‌ای و مخابراتی و در برخی موارد اشخاص حقیقی هستند، اطلاق می‌شود.

مادۀ ۱۱ قانون جرائم رایانه‌ای به حمایت از تأسیسات رایانه‌ای و مخابراتی که مورد استفادۀ عمومی هستند، پرداخته است. با توجه به مفاد ماده، عنصر مادی شامل افعالی است که به‌صورت غیر حصری منجر به سلب آسایش مردم می‌شود (جلالی فراهانی و باقری اصل، ۱۳۸۷: ۱۳۱). برهم زدن نظم و آسایش عمومی، رکن اصلی بزه‌های تروریستی است که در مادۀ فوق به آن اشاره شده است. با دقت در مادۀ ۱۱ قانون جرائم رایانه‌ای، می‌توان به یکی از ارکان اصلی تروریسم سایبری یعنی ارتکاب افعال عمدی که منجر به مختل شدن رفاه و آسایش عمومی جامعه در اثر وقوع جرم علیه تأسیسات رایانه‌ای و مخابراتی می‌شود، پی برد.

در خصوص تبیین مادۀ قانونی فوق و تطبیق آن با بزه تروریسم سایبری، می‌توان گفت که مادۀ ۱۱ دارای اشکالاتی است. یکی از اشکالات مادۀ فوق این است که نحوۀ ارتکاب بزه علیه تأسیسات مذکور مشخص نشده و به‌صورت کلی هر روشی را که منجر به اختلال آن‌ها می‌شود را مدنظر قرار داده است. در حالی که تروریسم سایبری، باید از طریق و مجرای فضای سایبر، یعنی اینترنت یا محیط شبکه وقوع یابد. براساس مفاد مادۀ فوق، بمب‌گذاری و تخریب فیزیکی تأسیسات عمومی مبتنی بر رایانه و دستگاه‌های مخابراتی نیز مشمول مقررۀ فوق می‌شود (موسوی، ۱۳۹۰: ۱۴). اشکال دیگر مقررۀ فوق این است که فقط به مجازات حبس بزهکار اشاره کرده و به عنوان یک مقررۀ اصلی به حمایت از بزه‌دیدگانی که در اثر افعال مواد ۸ الی ۱۰ این قانون متحمل خسارت می‌شوند، نپرداخته است. بنابراین، تنها بزه‌دیدگان حقوقی را مورد حمایت کیفری قرار داده و برای بزه‌دیدگان حقیقی که ممکن است در اثر حملات تروریستی سایبری متحمل خسارت شوند، تدابیری اندیشیده نشده است. با توجه به مقررات فوق، جا داشت قانون‌گذار در مادۀ ۱۱ به بزه تروریسم سایبری به صراحت اشاره می‌کرد و انواع جبران خسارت برای افراد بزه‌دیده و همچنین به جزای نقدی به‌عنوان مکمل کیفر اشاره می‌کرد.

علاوه بر افعال غیرقانونی در مادۀ ۱۱ این قانون، مواد ۸ الی ۱۰ همین قانون به دسته‌ای دیگر از افعال مادی این بزه پرداخته است. در این سه ماده به‌صورت کامل و غیر حصری، به شایع‌ترین اعمال ارتکابی که علیه تأسیسات حیاتی کشور انجام می‌شود پرداخته شده است. عنصر مادی بزه در سه مادۀ فوق، افعالی هستند که به‌صورت مصداقی برای هدف قرار

دادن سیســـتم‌های رایانه‌ای و مخابراتی که امور اجرایی کشـــور به آن‌ها وابسته است، اشاره شـــده اســـت[۱]. همان‌طور که در ابتدای بحث اشاره شد، مادۀ ۱۱ شباهت خاصی به تروریسم ســـایبری دارد و قانون‌گذار در مواد ۸ الی ۱۰ به‌صورت جامع به افعال غیرمجاز پرداخته که اقدام شایسته‌ای در خصوص جرم‌انگاری غیرمستقیم افعال مرتبط با تروریسم سایبری است.

علاوه بر حمایت‌های ماهوی در این قانون، حمایت شکلی از بزه‌دیدگان یکی از راهکارهایی است که در بیشتر نظام‌های حقوقی به‌منظور رعایت حقوق بزه‌دیده به کار گرفته می‌شود. در خصوص حمایت شکلی از بزه‌دیدگان حقوقی تروریسم سایبری، می‌توان به قواعد مربوط به صلاحیت بند ج مادۀ ۲۸ اشاره کرد که دادگاه‌های ایران را در صورت وقوع حملات رایانه‌ای صالح به رســـیدگی دانســـته اســـت (پوربافرانی، ۱۳۹۶: ۱۶-۱۵). مواد ۶۶۴ و ۶۶۵ آ.د.ک به صلاحیت دادگاههای ایران در رسیدگی به جرائم سایبری با توجه به اصول حمایتی، شخصی، ســـرزمینی و جهانی پرداخته اســـت که بزه‌دیدگان مصرح در بندهای الف، ب، پ و ت مادۀ ۶۶۴ می‌توانند به دادگاه‌های ایران جهت رســـیدگی به جرائم وقوع پیوســـته مراجعه کنند. لذا صرف‌نظر از ایرادات و اشـــکالاتی که به این بخش از آئین دادرســـی جرائم رایانه‌ای مطرح اســـت، آن اســـت که مقنن در بند ت مادۀ ۶۶۴ صرفاً به جرائم رایانه‌ای متضمن سوءاستفاده از اشـــخاص کمتر از ۱۸ ســـال، اعم از اینکه بزه‌دیدۀ ایرانی یا غیرایرانی در ایران یافت شـــود، پرداختـــه اســـت، در حالی که می‌توانســـت تا با توجه به موارد صلاحیـــت جهانی محاکم در رســـیدگی جرائم بین‌المللی مانند جرائم علیه بشـــریت یا نسل‌کشی، چنانچه جرائم رایانه‌ای منتهی به جرائم بین‌المللی مذکور شود مورد توجه قرار می‌گرفت تا از این حیث امکان حمایت از بزه‌دیدگان ســـایبری در صورت تحقق جرائم بین‌المللی نیز فراهم می‌شـــد و آنچه راجع به صلاحیت دادگاه‌های ایران در رســـیدگی به جرائم حاصل از بند ب مادۀ ۶۶۴ مطرح می‌شود

---

۱. این افعال شامل حذف، تخریب، مختل و غیرقابل‌پردازش کردن داده‌ها در سیستم‌های رایانه‌ای و مخابراتی، اقدام به واردکردن، انتقال دادن، پخش کردن، حذف کردن، مختل کردن، متوقف کردن، دست‌کاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری سیستم‌های رایانه‌ای یا مخابراتی، منع دسترسی اشخاص، تغییر گذرواژه یا رمزنگاری داده‌ها، مخفی کردن داده‌ها و اقدام به واردکردن، انتقال دادن، پخش کردن، حذف کردن، مختل کردن، متوقف کردن، دست‌کاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوریِ سیستم‌های رایانه‌ای یا مخابراتی است.

خالی از ایراد و ســـؤال نیســـت. لذا چنانچه بزه‌دیدگان جرم ارتکابی از طریق تارنماهای دارای دامنهٔ مرتبه بالای کد کشور ایران ارتکاب یابد و تبعه‌های کشورهای خارجی باشند، مشخص نیست که رویکرد مقنن و دادگاه‌های ایران در رسیدگی به شکایات بزه‌دیدگان سایبری ساکن در کشورهای بیگانه چگونه است (اسلامی، ۱۳۹۵: ۱۷۷).

اقدام حمایتی دیگر این قانون را می‌توان حفظ داده‌های رایانه‌ای یا ســـامانه‌های رایانه‌ای و مخابراتی دانســـت که ظن قوی به کشـــف جرم یا شناسایی متهم یا ادلهٔ جرم وجود دارد که این حمایت از حمایت‌های تبعی از بزه‌دیدگان مطرح اســـت و برای تحقیق و بازرســـی لازم و ضروری اســـت از سوی مقامات قضایی دســـتور حفاظت یا توقیف و تفتیش آن‌ها صادر شود و چنانچه ضابطان قضایی، کارکنان دولت یا اشـــخاصی که وظیفهٔ حفاظت از داده‌ها به آن‌ها سپرده شده است، خودداری یا افشا کنند، مطابق مواد ۶۶۹ و ۶۷۰ و ۶۷۱ مستوجب مجازات اســـت. این امر مبین آن اســـت که مقنن در حفظ حقوق بزه‌دیده سایبری از حیث جمع‌آوری و نگهداری ادلهٔ جرم و شناسایی مجرمان اهمیت بسزایی قائل است. حمایت کیفری صورت گرفته در قانون تجارت الکترونیکی، شـــامل داده‌هایی است که در بستر مبادلات الکترونیکی مورد اســـتفاده قرار می‌گیرند. این قانون به حمایت از داده‌های شـــخصی پرداخته و هرگونه تعرض به آن‌ها را بدون رضایت دارندهٔ آن‌ها غیرقانونی تلقی کرده و مجازاتی را برای مرتکب در نظر گرفته اســـت (مواد ۵۹ و ۵۸ قانون تجـــارت الکترونیک، مصوب ۱۳۸۲). در مقرراتی دیگر از قانون فوق، به حمایت کیفری ویژه از داده‌پیام‌های شخصی پرداخته که مرتکب این دســـته از جرائم، اشخاص خاصی هســـتند که توسط نهادهای مسئول و دفاتر خدمات صدور گواهی الکترونیکی ارتکاب می‌یابند. در این صورت برای مرتکب حداکثر کیفر تعیین شـــده است (مادهٔ ۷۲ قانون تجارت الکترونیک، مصوب ۱۳۸۲).

به دلیل ابهامات و خلأهای موجود در حمایت از بزه‌دیدگان ســـایبری که مادهٔ ۶۷۸ آ.د.ک بیان می‌دارد، در مواردی که برای رسیدگی به جرائم رایانه‌ای مقررات خاصی پیش‌بینی نشده باشـــد، موضوع تابع قانون آئین دادرســـی کیفری است. گونه‌های سیاست جنایی دولت‌ها در حمایت از بزه‌دیدگان اصولاً در سه حالت حمایت از بزه‌دیده، بلافاصله پس از تحقق جرم، در مرحلهٔ دادرسی و صدور حکم و در مرحلهٔ اجرای احکام و تأمین ضرر و زیان وی است (شمس

ناتری و اسلامی، ۱۳۹۴: ۲۷۶). در مواد ۱۴ و ۱۵ و ۱۷ این قانون اشاره می‌کند که شاکی می‌تواند برای جبران تمام ضرر و زیان‌های مادی و معنوی و منافع ممکن‌الحصول ناشی از جرم را پس از تعقیب متهم و تا قبل از اعلام ختم دادرسی مطالبه کند و دادگاه مکلف است تا ضمن صدور رأی کیفری در خصوص ضرر و زیان وارده به مدعی خصوصی، رأی مقتضی صادر کند. در مواد ۷۰ و ۷۱ این قانون که حمایت از بزه‌دیده محجور است که در صورت دسترسی یا عدم دسترسی به متهم امکان یا شرایط طرح شکایت و پیگیری آن را ندارند، برای تعقیب کیفری متهم مقرر شده است و این امر به‌جز موارد مذکور در مواد ۲۰۱، ۳۶۷ و ۳۶۸ تأکید شده است و همچنین در مادهٔ ۸۱ در زمان صدور دستور تعلیق تعقیب متهم در بند الف مقنن، حفظ حقوق بزه‌دیده را مورد توجه داشته است و اعلام کرده که متهم بایستی در ارائه خدمات به بزه‌دیده در جهت رفع یا کاهش آثار زیانبار مادی یا معنوی ناشی از جرم یا رضایت وی اقدام کند (پوربافرانی، ۱۳۹۶: ۸۲-۷۹).

جهت تضمین حقوق بزه‌دیده برای جبران ضرر و زیان، بازپرس پس از تفهیم اتهام مطابق مادهٔ ۲۱۷ و ۲۴۷ آ.د.ک، یکی از قرارهای تأمین یا نظارت قضایی مصرح در آن را برای متهم صادر می‌کند. بازپرس و دادستان پس از ختم تحقیقات، چنانچه بزه‌دیده بر قرارهای نهایی صادره مثل منع تعقیب یا موقوفی تعقیب و غیره محکوم باشد، می‌تواند مطابق مادهٔ ۲۷۰ به دادگاه اعتراض کند تا چنانچه حقوق وی در این مرحله تضییع شد، مورد رسیدگی قرار گیرد و مطابق تبصرهٔ مادهٔ ۳۴۷ قانون مذکور، هرگاه حضور و دفاع وکیل را برای شخص بزه‌دیده فاقد تمکن مالی را ضروری بداند، برای وی وکیل با هزینهٔ قوه قضائیه انتخاب می‌کند (قربان نیا و نمانیان، ۱۳۹۴: ۱۰۴-۱۰۲).

- **حمایت کیفری ویژه یا افتراقی:** حمایت کیفری ویژه، یعنی جرم‌انگاری بزه با توجه به ویژگی‌های خاص یک بزه‌دیده مانند اشخاص کهن‌سال، زنان و کودکان که به سبب وضعیت خاص آن‌ها باید بیشتر مورد حمایت قرار گیرند (رایجیان اصلی، ۱۳۹۰ الف: ۸۴). حمایت کیفری تشدیدی، از آورده‌های بزه‌دیده‌شناسی حمایتی است که با تشخیص بزه‌دیدگانِ دارای شرایط خاص، به حمایت ویژه از آن‌ها می‌پردازد.

در زمینهٔ حمایت‌های کیفری افتراقی از بزه‌دیدگان تروریسم سایبری، می‌توان به مواد

مختلفی از قانون جرائم رایانه‌ای اشـــاره کرد که به واســـطهٔ موضوع جرم، به تشدید مجازات مرتکب پرداخته است. از جمله حمایت کیفری ویژه در این قانون، «حمایت ویژه از داده‌های سری است که در سیستم‌های رایانه‌ای و مخابراتی یا حامل‌های داده در حال انتقال یا ذخیره هستند» (مادهٔ سه قانون جرائم رایانه‌ای، مصوب ۱۳۸۸).

علاوه بر بیان حمایت‌های کیفری تشـــدیدی در قانون جرائـــم رایانه‌ای، می‌توان به قانون تجـــارت الکترونیکی مصوب ۱۳۸۲ اشـــاره کرد که به حمایت کیفـــری ویژه از داده‌پیام‌های شخصی پرداخته است. این جرائم علیه داده‌ها توسط نهادهای مسئول و دفاتر خدمات صدور گواهی الکترونیکی ارتکاب می‌یابد که در این صورت برای مرتکب، حداکثر کیفرِ تعیین‌شده در مادهٔ ۷۱ را مقرر کرده اســـت. با توجه به حســـاس بودن داده‌های شـــخصی به خصوص در حوزهٔ مالی، قانون‌گذار اشخاصی را که با داده‌های مذکور درگیر هستند، مورد توجه ویژه قرار داده و بدین وســـیله بزهکاران بالقوه را نیز از ارتکاب چنین اعمالی بازداشته است (جاویدنیا، ۱۳۸۶: ۱۲۹).

حمایت مدنی از بزهدیدگان تروریســـم ســـایبری: دســـته‌ای دیگـــر از حمایت‌ها، ســـازوکارهایی هستند که دارای ماهیت کیفری نیستند و بیشتر شامل جبران خسارت از بزه‌دیدگان جرائم می‌شـــود. با توجه به اینکه در قوانین کیفری ایران، جرم‌انگاری صریحی از تروریســـم ســـایبری صورت نگرفته و حتـــی به‌منظور پشـــتیبانی از بزه‌دیدگان جرائم رایانه‌ای، اقدامات شایســـته‌ای اتخاذ نشده اســـت، حمایت‌های غیرکیفری نیز به‌صراحت، چنیـــن بزه‌دیدگانی را مورد توجـــه قرار نداده‌اند. لذا منظور از حمایت مدنی از بزه‌دیدگان تروریســـم سایبری، سازوکارهایی هستند که به‌طور غیرمستقیم و عام به حمایت‌های غیر کیفری از بزه‌دیدگان مذکور می‌پردازند. بنابراین، حمایت‌های مدنی، بیشتر شامل جبران خســـارت مادی است. جبران خسارت مادی شامل هرگونه اقدام به‌منظور جبران و ترمیم آسیب‌های وارده به دارایی‌های بزه‌دیده است که به وسیلهٔ پرداخت پول و هزینه‌های ایجاد شـــده در طی بزه‌دیدگی فرد یا پرداخت غرامت بـــه بزه‌دیدگان تحقق می‌پذیرد (رایجیان اصلی، ۱۳۹۰ الف: ۸۶).

در زمینهٔ بررسی آسیب‌های وارده بر بزه‌دیدگان تروریسم سایبری، خسارات مادی بارزترین

آسیب‌هایی هستند که در اثر وقوع حملات تروریستی سایبری بر بزه‌دیدگان مذکور به خصوص بزه‌دیدگان حقوقی، به دلیل عمده و حساس بودن تأسیسات مذکور وارد می‌شود. البته خسارات مادی، اختصاص به بزه‌دیدگان حقوقی نداشته و اشخاص حقیقی نیز بسته به گستردگی حملات سایبری و آماج جرم، زیان‌های مالی سنگینی را متحمل می‌شوند. در اثر وقوع حملات تروریستی سایبری، بیش‌ترین خسارت وارده بر بزه‌دیدگان، به خسارت‌های اقتصادی اختصاص دارد. به عبارت دیگر، در اثر تخریب تأسیسات زیرساختی کشور که مبتنی بر فناوری اطلاعات هستند، زیان‌های مالی از قبیل اختلال یا توقف در امور اجرایی کشور، هزینه‌های مربوط به اقدامات تشخیصی و اکتشافی در جهت کشف و ردیابی بزهکاران، هزینه‌های توسعه و استقرار تجهیزات پیشگیری، هزینه‌های بازیابی اطلاعات و تعویض سخت‌افزار یا نرم‌افزار آسیب‌دیده، هزینه‌های ایمن‌سازی دوباره، خسارت وارده بر شهروندان در اثر اختلال‌های صورت گرفته مانند مؤسسات مالی و اعتباری و خساراتی از این قبیل، بیش‌ترین هزینه‌های مالی را برای بزه‌دیدگان در پی دارد. بنابراین، با استفاده از سازوکارهای جبران مادی خسارت، می‌توان به بهبود وضع بزه‌دیده و اعادهٔ وضع او به حالت قبل از وقوع بزه اقدام کرد (ساعد، ۱۳۸۹: ۶۷).

با بررسی هزینه‌های تحمیل‌شده بر بزه‌دیدگان مذکور، لزوم جبران کردن آن‌ها توسط بزهکاران و در صورت غیرقابل جبران ماندن، باید توسط دولت جبران شود. بسیاری از خسارت‌های ایراد شده با جبران مادی قابل‌ترمیم هستند. اگرچه در قوانین کشور ما به جبران خسارت قربانیانی که در اثر بدافزارهای رایانه‌ای به آن‌ها خسارت وارد آمده باشد، پرداخته نشده است، اما در خصوص جبران زیان‌های وارده می‌توان به مواردی برخورد کرد که به‌صورت کلی، به جبران خسارت از بزه‌دیده اشاره کرده باشند. مواد عام متعددی از قانون مسئولیت مدنی، قانون مدنی و نیز قانون مجازات اسلامی وجود دارند که می‌توان به جبران خسارت اقدامات تروریستی سایبری اقدام کرد. هرچند اقدام به تفسیر موسع نسبت به برخی مواد قانونی، در نسبت دادن مسئولیت به مرتکبان اعمال تروریستی سایبری، ممکن است قابل ایراد باشد (صارمی، ۱۳۹۲: ۵۴).

در خصوص قوانین موجود، می‌توان به قانون مسئولیت مدنی اشاره کرد که به‌صورت

کلی و قواعد عام در این قانون، به جبران کردن خسارت‌های وارده بر کلیهٔ بزه‌دیدگان اشاره کرده است. بنابراین، اعمالی که توسط تروریست‌های سایبری، علیه داده‌ها، سخت‌افزار، نرم‌افزار، تمامیت جسمانی یا روانی اشخاص ارتکاب می‌یابد، به استناد قاعدهٔ عام مادهٔ یک قانون مسئولیت مدنی، بزهکاران مسئول عمل خود و مکلف به پرداخت غرامت یا جریمهٔ خسارت‌های مذکور هستند. علاوه بر قانون مسئولیت مدنی، مادهٔ ۳۲۸ قانون مدنی، به شکل عام، تلف اموال دیگران را ممنوع و موجب مسئولیت دانسته است (عالی پور، ۱۳۹۰: ۲۳۷). مقررات اشاره‌شده در دو قانون فوق، شامل مواد عامی هستند که با قید عبارات عمومی مانند «هرکسی»، فاعل را مسئول جبران خسارات وارده می‌دانند. اما یکی از قوانینی که به‌طور اختصاصی به جبران خسارت در رابطه با جرائم رایانه‌ای پرداخته است، قانون تجارت الکترونیکی مصوب ۱۳۸۲ است که در مورد جبران خسارت به عین به صراحت در مادهٔ ۷۸ بدان اشاره کرده است. در قسمت پایانی مادهٔ فوق، اشاره به جبران خسارت و مسئولیت اشخاصی دارد که در اثر فعل آن‌ها سیستم‌های دولتی یا خصوصی دچار اختلال یا تخریب شده و متعاقب آن به افراد جامعه ضرر وارد شده است. به نظر می‌رسد این مقرره از قانون تجارت الکترونیکی، تنها مقرره‌ای است که به‌صراحت، اشاره به جبران خسارتی کرده که مرتبط با سیستم‌های رایانه‌ای و مخابراتی هستند. بند ۳ تبصرهٔ ۱۸ لایحهٔ بودجهٔ سال ۱۳۸۵ کل کشور نیز، یکی دیگر از منابع قانونی است که به حمایت و جبران خسارت دولتی از بزه‌دیدگانی اشاره دارد که در اثر اقدامات خصمانهٔ دولت‌های دیگر یا گروه‌هایی که به پشتیبانی دولت‌ها به شهروندان آسیب می‌رسانند، پرداخته است. این تبصره در خصوص جبران خسارت ناشی از اقدامات تروریستی تدوین شده است. هرچند مقررهٔ مذکور دارای ایراداتی به خصوص در اقامهٔ دعوی و چگونگی جبران است، اما گامی مهم در جهت انواع حمایت از بزه‌دیدگان تروریسم و به‌تبع تروریسم سایبری که زیر شاخهٔ تروریسم سنتی است، محسوب می‌شود (پورنقدی و بختیاری، ۱۳۹۲: ۳۵-۳۳).

همچنین، تدوین «لایحهٔ جبران دولتی خسارت از بزه‌دیدگان» که توسط قوهٔ قضائیه تدوین شده است، نمونه‌ای دیگر از تلاش‌های دولت در جهت تحقق اهداف بزه‌دیده‌شناسی و کمک به بزه‌دیدگان است که در این لایحه، صندوق جبران خسارت برای بزه‌دیدگان پیش‌بینی

شـــده است. لایحۀ مذکور، زیان‌های ناشی از جرائم را که قابل حمایت هستند احصاء کرده و چهار دسته از جرائم را مدنظر قرار داده که به بیان آن دسته از مواردی پرداخته می‌شود که با بزه مذکور و بزه‌دیدگان آن قابل تطبیق باشد. دستۀ اول، شامل «جرائم عمدی یا غیرعمدی اســـت که منتهی به قتل شود» (مادۀ ۳ لایحۀ جبران دولتی خسارت از بزه‌دیدگان، ۱۳۸۷). با تطبیق مفاد این مقرره با تبعات تروریســـم ســـایبری، می‌توان مواردی که در اثر فعل یک نفوذگر، قطار مترو از ریل خارج شود یا اینکه در اثر اختلال در تأسیسات راهنمایی و رانندگی از قبیل چراغ راهنمایی، تصادف و به مرگ شهروندان منجر شود، به شمول مقررات این لایحه در خصوص جبران خســـارات مالی بزه‌دیدگان حقیقی تروریسم سایبری اشاره کرد (صارمی، ۱۳۹۲: ۵۸-۵۷).

شیوۀ جبران خسارت از بزه‌دیدگان تروریسم سایبری در حقوق کیفری ایران: در قانون جرائم رایانه‌ای کشورمان راجع به حمایت بزه‌دیدگان سایبری از حیث جبران خسارت وارده و شـــیوه‌های آن موضوعی پیش‌بینی نشـــده است، اما با توجه به اطلاق مادۀ ۱۴ قانون آیین دادرسی کیفری که مقرر داشته شاکی میتواند در صورت وقوع خسارت، جبران ضرر و زیان‌های مادی و معنوی و منافع ممکن‌الحصول ناشی از جرم را مطالبه کند و در صورت وقوع زیان معنوی که شـــامل صدمات روحی، هتک حیثیت، اعتبار شخصی، خانوادگی و اجتماعی اســـت، دادگاه علاوه بر صدور حکم به جبران خســـارت مالی، میتواند متهم را از طریق الزام به عذرخواهی و درج حکم در جراید و امثال آن محکوم کند. از ایرادات وارده به قانون فعلی جرائم رایانه‌ای آن اســـت که با توجه به تأثیرات و اهمیت فزایندۀ فضای مجازی در زندگی روزمرۀ اشـــخاص در دنیا، لازم بود تا مقنن ایران به‌منظور اســـتیفای حقوق حقۀ شاکی و پیشگیری و مقابله با جرائم ارتکابی در فضای مجازی، مصادیق و شـــیوه‌های جبران خسارت وارده را به خوبی مشخص و تبیین کند.

یکی از نکات مهم دیگر در جبران خســـارت از بزه‌دیدگان فضای مجازی که می‌بایســـت در قانون جرائم رایانه‌ای توســـط مقنن ایران مورد توجه قرار گیرد، موضوع حمایت دولت از اتباع بزه‌دیدۀ خویش در صورت عدم شناســـایی متهمان اســـت که جبران خسارت وارده به بزه‌دیدگان از طریق شـــیوه‌هایی چون تأدیه خســـارت به آن‌ها از منابع مالی قانونی جایگزین

پیش‌بینی‌شده در قانون باشد؛ به‌عنوان مثال در قوانین داخلی ایران، صندوق تأمین خسارت-های بدنی در تصادفات در صورت عدم شناسایی متهمان پیش‌بینی شده است یا در مادۀ ۴۳۵ قانون مجازات اسلامی راجع به پرداخت دیه از بیت‌المال به اشخاصی که مورد قتل و ضرب و جرح عمدی واقع می‌شوند و قاتل و ضارب آن‌ها مشخص نیست، به حمایت از این دسته از بزه‌دیدگان پرداخته است که شایسته است تا در این مورد هم چاره‌اندیشی مناسبی اتخاذ شود (اسلامی، ۱۳۹۵: ۱۷۹).

حمایت از بزه‌دیدگان تروریسم سایبری در اسناد بین‌المللی

حمایت کیفری: یکی از مسائل مورد نگرانی و اهتمام جامعۀ بین‌المللی، تدوین یک سری راهکارهایی برای ایفای حق جبران و در نتیجه جبران خسارات وارده بر قربانیان نقض‌های حقوق بشر بود. در همین راستا، بنیادین راجع به حق جبران و غرامت برای قربانیان نقض‌های حقوق بشر و حقوق بشردوستانۀ بین‌المللی (از این به بعد اصول ملل متحد در مورد حق جبران) را در پنجاه و ششمین اجلاسیۀ خود در سال ۲۰۰۰ مورد پذیرش قرار داد (اسلامی، ۱۳۹۵: ۱۶۶).

کنوانسیون جرائم سایبری شورای اروپا مصوب سال ۲۰۰۱، تنها سندی است که جرائم سایبری را مورد بررسی قرار داده و به جرم‌انگاری‌های متعددی از افعال غیرمجاز در محیط سایبری اقدام کرده است. در خصوص حمایت‌های کیفری از بزه‌دیدگان تروریسم سایبری، در این سند می‌توان به جرم‌انگاری‌هایی اشاره کرد که افعال غیرقانونی علیه داده‌ها، سیستم‌های رایانه‌ای و مخابراتی به شمار می‌روند. یکی از افعال جرم‌انگاری شده در این سند، ایجاد اختلال عمدی و من غیر حق در داده‌های رایانه‌ای است که تروریست‌های سایبری نیز از همین طریق به اختلال و تخریب در زیرساخت‌های حیاتی و اطلاعاتی اقدام می‌کنند. با توجه به طبقه‌بندی صورت گرفته در این کنوانسیون، برخی از جرائم در این سند وجود دارد که رکن مادی تروریسم سایبری را تشکیل می‌دهند (روهاس[1]، ۲۰۱۲: ۲۵۵-۲۵۶). ایجاد اختلال در داده یا سیستم‌های رایانه‌ای و دستیابی غیرمجاز، رکن اصلی عملیات تروریستی سایبری

1. Rohas

علیه زیرساخت‌های اطلاعاتی کشور را تشکیل می‌دهند (مادۀ چهار کنوانسیون).

دسته‌ای دیگر از افعال جرم‌انگاری شده در راستای حمایت از بزه‌دیدگان تروریسم سایبری، «سوءاستفاده از وسایل، رمز عبور، کد دستیابی، داده‌ها یا برنامه‌های رایانه‌ای»، هستند که اغلب تروریست‌های سایبری از طریق سوءاستفاده از سیستم‌های رایانه‌ای و مخابراتی یا داده‌ها، به اقدامات خرابکارانۀ خود دست می‌زنند. بنابراین، با ذکر مواضع اتخاذشده در مقررات این کنوانسیون که به‌طور غیرمستقیم به افعال تشکیل‌دهندۀ تروریسم سایبری پرداخته است، می‌توان به حمایت کیفری از بزه‌دیدگان تروریسم سایبری استدلال کرد (مادۀ شش کنوانسیون).

کنوانسیون جلوگیری از بمب‌گذاری تروریستی[1] یکی از بارزترین اسناد بین‌المللی ضد تروریسم است که در سال ۱۹۹۷ تصویب شد (هاشمی، ۱۳۹۰: ۲۵). کنوانسیون فوق، همانند دیگر اسناد بین‌المللی در خصوص تروریسم، با ذکر عبارات مبهم و عام‌الشمول، به ذکر جرائم تروریستی پرداخته که منجر به «کشتن، جراحت یا ایراد خسارات عمدۀ مالی می‌شود» (مادۀ یک کنوانسیون). از آنجا که با استفاده از بدافزارهای رایانه‌ای یا اقدام اشخاص تروریست در تخریب داده‌ها و سیستم‌های رایانه‌ای و مخابراتی، به‌سادگی می‌توان به ایجاد خسارات جبران‌ناپذیر در تأسیسات و زیرساخت‌های کشور از جمله نیروگاه‌های اتمی یا مراکز موشکی اقدام کرد، با استناد به برخی قواعد عام این کنوانسیون، می‌توان به جرم‌انگاری اعمال تروریستی سایبری استدلال کرد (گارسیا، وردیجو[2]، ۲۰۰۹: ۳۸-۴۱).

کنوانسیون سرکوب حمایت مالی از تروریسم[3]، یکی از قطعنامه‌های معروف در زمینۀ منع حمایت مالی از تروریسم است که در ۹ دسامبر ۱۹۹۹ توسط مجمع عمومی سازمان ملل متحد به تصویب رسید (طیبی فرد، ۱۳۸۴: ۲۷۱). با توجه به اینکه منابع مالی، نقش اولیه را در شکل‌دهی عملیات تروریستی ایفا می‌کنند، می‌توان از بزه‌دیده شدن اشخاص به‌طور غیرمستقیم با منع و جرم‌انگاری حمایت‌های مالی، جلوگیری و با تعیین ضمانت اجراهای قوی از آن‌ها حمایت کیفری کرد (مادۀ دو کنوانسیون). در مجموع، از مفاد این کنوانسیون

1. International Convention for the Suppression of Terrorist Bombings
2. Garcı´a., Verdejo
3. International Convention for the Suppression of the Financing of Terrorism

چهار موضوع اساسی استناد می‌شود؛ الزام دولت‌ها به همکاری و معاضدت با یکدیگر به‌منظور سرکوب تروریسم، مقابله با تأمین مالی تروریسم، عدم پشتیبانی مستقیم و غیرمستقیم از تروریسم و جرم‌انگاری و تعقیب کیفری تروریسم از عمده نکاتی است که در این قطعنامه مورد تأکید قرار گرفته است (زرنشان، ۱۳۸۶: ۶۹).

بزه‌دیدگان خاصی در این کنوانسیون مورد حمایت قرار نگرفته‌اند، اما از کلیت اقدامات تروریستی اشاره شده در این قطعنامه، می‌توان نتیجه گرفت که اگر تروریسم سایبری منجر به تخریب تأسیسات حیاتی شود، این بزه‌دیدگان نیز مورد حمایت کیفری این قطعنامه قرار خواهند گرفت. قطعنامهٔ شورای امنیت سازمان ملل متحد به شمارهٔ ۱۳۷۳، یکی دیگر از اسناد بین‌المللی در رابطه با جرم‌انگاری حمایت مالی از اعمال تروریستی است. در این راستا قطعنامهٔ ۱۳۷۳ به ایجاد سازوکارهای بین‌المللی مبارزه با تأمین مالی تروریسم که شامل جرم‌انگاری تأمین مالی اقدامات تروریستی (ردیف‌های «الف» و «ب» بند یک قطعنامهٔ ۱۳۷۳ شورای امنیت، مصوب ۲۰۰۱) و همچنین به مکلف کردن دولت‌ها به‌منظور تلاش برای پیشگیری و مقابله با تأمین مالی تروریسم در قالب فعالیت‌های مختلف اقدام کرده است. به‌طور کلی، شورای امنیت در ارتباط با تأمین مالی تروریسم، هشت قطعنامه را تصویب کرده است که مهم‌ترین آن‌ها عبارت‌اند از: قطعنامهٔ شمارهٔ ۱۳۷۷ در دسامبر ۲۰۰۱ و قطعنامهٔ ۱۳۹۰ در ۲۸ ژانویهٔ ۲۰۰۲. قطعنامه‌های فوق، از جمله اسناد بین‌المللی در رابطه با تعهدات حقوقی بین‌المللی دولت‌ها برای منع حمایت مالی و ایمن ساختن سرزمین‌های دولت‌ها از حامیان مالی تروریست‌ها هستند (پاکزاد، ۱۳۹۰: ۲۲۸).

اتحادیهٔ کشورهای اروپایی، سیاست‌های متعددی را در خصوص حملات علیه شبکه‌های رایانه‌ای، انتشار ویروس‌ها، کرم‌های رایانه‌ای، تروجان‌ها، هرزنامه‌های اینترنتی، حملات فیشینگ و سرقت هویت صادر کرده است. با توجه به اینکه موارد فوق به‌طور غالب در تروریسم سایبری مورد استفاده قرار می‌گیرند، بنابراین اتحادیهٔ اروپا یکی از مهم‌ترین سازمان‌هایی است که به‌منظور جرم‌انگاری افعال غیرمجاز در محیط سایبری گام برداشته است (دوون، مائر[1]، ۲۰۰۶: ۱۸۲-۱۸۳). کنوانسیون اروپایی مقابله با تروریسم[2]، در واکنش به افزایش

1. Dunn&Mauer
2. European Convention on Fighting Terrorism

نگرانی‌های حاصل از اقدامات تروریستی، به تصویب کنوانسیون اقدام کرد که از شاخص‌ترین اسناد منطقه‌ای در خصوص تروریسم به شمار می‌رود. دامنهٔ شمول این کنوانسیون در مقایسه با دیگر اسناد ضد تروریسم وسیع‌تر است و تقریباً تمامی جرائم مذکور در کنوانسیون‌های بین‌المللی ضد تروریسم را شامل می‌شود. هرچند این کنوانسیون به جرم‌انگاری صریحی از اقدامات تروریستی اشاره نکرده است، اما کلیت مفاد این سند، جا را برای جرم‌انگاری سایر جرائم تروریستی باز گذاشته و با تأکید بر شمول قواعد سایر کنوانسیون‌های بین‌المللی، می‌توان به حمایت از بزه‌دیدگان تروریسم سایبری از جمله تأسیسات حیاتی و اشخاص حقیقی استدلال کرد (تقی زاد و زمردی، ۱۳۹۶: ۱۰۸).

کنوانسیون منطقه‌ای سازمان همکاریهای آسیای جنوبی[1]، یکی دیگر از تلاش‌های منطقه‌ای کشورهای جهان در مبارزه با تروریسم است که در سال ۱۹۸۷ در کاتماندو به تصویب رسید (زمانی، ۱۳۸۰: ۱۳۸). با توجه به بررسی مجموعه‌ای از جرائم اشاره‌شده در این سند، جرم‌انگاری افعالی که از طریق رایانه یا اینترنت به اقدامات تروریستی منتج می‌شود، دیده نمی‌شود. اما با استدلال به قواعد عام ارتکاب جرائم تروریستی که در کنوانسیون‌های متعددی از جمله کنوانسیون مقابله با اقدامات غیرقانونی علیه امنیت هواپیمایی کشوری، می‌توان به اشارهٔ غیرمستقیم این کنوانسیون‌ها به افعال تشکیل‌دهندهٔ تروریسم سایبری و در مقابل به حمایت از بزه‌دیدگان این جرم استدلال کرد (موسوی و حیدری، ۱۳۹۲: ۱۴).

حمایت‌های مدنی: حمایت‌های مدنی از بزه‌دیدگان تروریسم سایبری، شامل بررسی مجموعه‌ای از اسناد بین‌المللی است که به حمایت از بزه‌دیدگان جرائم پرداخته‌اند و بدین علت که از بزه‌دیدگان تروریسم سایبری، حمایت غیرکیفری صریحی صورت نگرفته، به اسنادی رجوع می‌شود که کلیت بزه‌دیدگان جرائم را مورد چتر حمایتی خود قرار داده‌اند. بنابراین، حمایت‌های مدنی از بزه‌دیدگان تروریسم سایبری، عبارت‌اند از: حمایت مادی، عاطفی و حیثیتی، پزشکی، شکلی.

حمایت مادی از بزه‌دیدگان جرائم، به عنوان برجسته‌ترین گونه‌های حمایت به شمار می‌رود. اینگونه از حمایت‌ها، «در همهٔ سطوح قانون‌گذارانه، قضایی و اجرایی و هم در سطوح

1. Convention of the Organization of Regional Co-operation of South-Asia (1987)

سیاســـت جنایی مشـــارکتی از قبیل راه‌اندازی صندوق‌های ملّی پرداخت غرامت امکان‌پذیر اســـت» (رایجیان اصلی، ۱۳۹۰ الف: ۸۶). کنوانسیون پیشـــگیری از تروریسم شورای اروپا، بارزترین سند منطقه‌ای در خصوص جبران خسارت از بزه‌دیدگان جرائم تروریستی و حمایت از بزه‌دیده و خانواده‌های آن‌ها است. وسیع بودن جرائم مشمول این کنوانسیون، دلیلی بر آن است که قواعد حمایتی آن را در خصوص بزه‌دیدگان مورد بحث گسترش دهد. در این راستا، کنوانسیون مذکور اعلام می‌دارد که حمایت از بزه‌دیدگان باید براساس یک برنامه‌ریزی ملی و بر مبنای قانون‌گذاری داخلی کشـــورهای عضو، شامل کمک‌های مالی و پرداخت خسارت به بزه‌دیدگان تروریسم و خانواده‌های آن‌ها باشد (مادۀ ۱۳ کنوانسیون پیشگیری از تروریسم شورای اروپا، مصوب ۲۰۰۵).

در کنوانســـیون منع حمایت مالی از تروریســـم در راستای حمایت و جبران خسارت مادی از بزه‌دیدگان تروریســـم، به کشـــورهای عضو توصیه کرده که در صورت توقیف منابع مالیِ اعمال تروریستی که در مادۀ دو به این اعمال اشاره‌شده، آن‌ها را برای بزه‌دیدگان مذکور در کنوانسیون صرف کنند. راهبرد جهانی ضد تروریسم سازمان ملل متحد، نیازهای بزه‌دیدگان تروریسم و خانواده‌هایشان را مورد توجه قرار داده و به تسهیل زندگی آن‌ها اشاره کرده است. با توجه به گســـترده بودن مفاد این راهبرد، جبران خســـارت‌های مادی بزه‌دیدگان تروریسم سایبری نیز در حوزۀ این راهبرد قرار می‌گیرند[1].

پیوســـت اعلامیۀ اصول بنیادین عدالت برای بزه‌دیدگان و قربانیان سوءاســـتفاده از قدرت اعلامیه، سندی الزام‌آور نیست، اما با توجه به خصیصۀ بین‌المللی و سازمان صادرکنندۀ آن، می‌تواند در ارتقای حقوق بزه‌دیده و ترویج اصول و ملاک‌های جهانی بزه‌دیده‌شناسی حمایتی مؤثر واقع شـــود. براســـاس مقررات این اعلامیه، «بزهکار یا به‌طور کل مسئول عمل مجرمانه، باید به‌طور مقتضی آثار ناشی از بزه را در بزه‌دیده یا اطرافیان آن به وسیلۀ بازگرداندن مال یا پرداخت پول برای آســـیب یا زیان وارد آمده و به‌طور کل هزینه‌هایی که در اثر بزه‌دیدگی بر قربانی حاصل شـــده بپردازد (بند هشـــتم اعلامیه). در ادامه، این اعلامیه در راستای پرداخت

1. http://www.un.org/terrorism/strategy-counter-terrorism.shtml, retrieved at : 10/01/2018

غرامت به بزه‌دیدگان، راه‌اندازی منابعی برای جبران خسارت اندیشیده است که شامل تشویق دولت‌ها به راه‌اندازی صندوق ملی پرداخت غرامت برای فراهم کردن پرداخت غرامت به بزه‌دیدگان، به خصوص در مواردی که دولت متبوع بزه‌دیده قادر به این جبران خسارت نباشد، پرداخته است (بند ۱۲). همچنین، اعلامیه به پرداخت غرامت دولتی پرداخته و بنا به شرایطی، بزه‌دیده را مورد حمایت قرار داده است (احمری و کحلکی، ۱۳۹۵: ۳۱۲). سند مذکور که از زمرهٔ اسناد بین‌المللی در خصوص بزه‌دیده شناسیِ حمایتی به شمار می‌رود، حقوق بزه‌دیدگان جرائم را مورد توجه قرار داده و حمایت‌های متعددی از جمله حمایت‌های پزشکی را مورد اشاره قرار داده است (بند ۱۴ اعلامیه). اعلامیه به انواع حمایت‌ها از جمله مداخله‌های بهداشت روانی- اجتماعی و روحی- معنوی در قالب مشاوره‌های خانوادگی یا عاطفی و غیره به بزه‌دیدگان پرداخته که نشان‌دهندهٔ اهتمام ویژهٔ این سند بین‌المللی در خصوص توجه به آسیب‌های روانی و عاطفی بزه‌دیدگان جرائم است. در ادامه همین مقرره، به تمهید راهکارهایی برای اعادهٔ حیثیت و جایگاه بزه‌دیده در میان خانواده یا اجتماع می‌پردازد (مادهٔ هشت).

قطعنامهٔ شمارهٔ ۶۰/۱۴۷ که عنوان کامل آن، اصول اساسی و رهنمودهای حق دادخواهی و جبران خسارت از قربانیان نقض فاحش قوانین بین‌الملل حقوق بشر و نقض جدی حقوق بین‌الملل بشردوستانه است، دستاورد تلاش سازمان ملل متحد و دولت‌ها در زمینهٔ شناسایی حق‌های بزه‌دیدگان به شمار می‌رود. قطعنامهٔ مذکور، حقوق متعددی را برای جبران خسارت زیان‌های وارده بر بزه‌دیدگان به رسمیت شناخته که به‌تبع، این حمایت‌ها مشمول بزه‌دیدگان مورد بحث خواهد شد. عمده‌ترین حق‌های شناخته‌شده در این قطعنامه شامل «جبران خسارت، پرداخت غرامت، توان‌بخشی و اعادهٔ حیثیت، اقناع‌سازی بزه‌دیده و تضمین‌هایی برای تکرار نکردن بزه‌دیدگی دوبارهٔ افراد هستند» (رایجیان اصلی، ۱۳۹۰: ۲۶۲-۲۶۰).

در خصوص حمایت پزشکی از قربانیان تروریسم سایبری، هیچ سند بین‌المللی را نمی‌توان یافت که به موضوع حمایت پزشکی، حتی بزه‌دیدگان سایبری پرداخته باشد. بزه‌دیدگی سایبری، موضوعی نوین در میان نظام‌های حقوقی است و در اغلب موارد به‌طور غیرمستقیم به جبران خسارت مادی بزه‌دیدگان ناشی از جرائم سایبری، پرداخته نشده و جنبه‌های دیگر

همچنان مسکوت مانده است. شاید دلیل چنین نقیصه‌ای، بالا بودن رقم سیاه بزهکاری و عدم گزارش بزه توسط بزه‌دیدگان سایبری است. بنابراین، هم در سطح حقوق داخلی کشورها و هم در حقوق بین‌الملل، نیاز به توجه بیشتر نسبت به بزه‌دیدگان سایبری و به خصوص جرائم خشونت‌باری چون تروریسم سایبری احساس می‌شود (دهشیری، ۱۳۹۵: ۱۴۷).

کنوانسیون اروپایی پیشگیری از جرائم تروریستی به‌عنوان بارزترین سند منطقه‌ای در خصوص حمایت‌های عاطفی است. در همین راستا، این کنوانسیون با ایجاد ابزارها و سازوکارهای لازم توسط دولت‌ها در قالب برنامه‌ها و قانون‌گذاری‌های ملی، برای محافظت، جبران خسارت و کمک‌های همه‌جانبه برای قربانیان تروریسم اشاره کرده است که کمک‌های همه‌جانبه شامل قواعد حمایتی از نوع عاطفی خواهد بود (مادۀ ۱۳ کنوانسیون اروپایی پیشگیری از تروریسم، مصوب ۲۰۰۵).

در خصوص مسائل شکلی مربوط به جرائم رایانه‌ای، همانند حقوق داخلی کشورها، اسناد بین‌المللی نیز به‌وفور با مشکلات آیین دادرسی مواجه هستند. در جرائم فراملی مانند تروریسم سایبری و به‌طورکلی حملات سایبری، بزهکاران از کشورهای دیگر برای پایه‌ریزی حملات استفاده می‌کنند؛ زیرا از ضعف قوانین بین‌المللی و همچنین عدم وجود رویۀ یکنواخت و منسجمی در زمینۀ مساعدت و پیگرد ادله و مجرمان سایبری در بین کشورها آگاه‌اند. کنوانسیون جرائم سایبر، در زمینۀ حقوق شکلی و قواعد آیین دادرسی مدارِ مربوط به جرائم سایبر، مقررات مختلفی را به‌عنوان برجسته‌ترین سند در خصوص جرائم سایبری تدوین کرده است. از جمله حمایت‌های شکلی در خصوص بزه‌دیدگان سایبری، می‌توان به مواردی اشاره کرد که این کنوانسیون به محافظت از داده‌های رایانه‌ای ذخیره‌شده پرداخته که احتمال نابودی یا تغییر آن‌ها وجود دارد (مادۀ ۱۶). با توجه به اینکه تروریسم سایبری در فراسوی مرزها قابل ارتکاب است، در مواد ۲۲ تا ۳۵ این کنوانسیون، در خصوص همکاری و معاضدت‌های بین‌المللی به‌منظور همکاری دولت‌های عضو با یکدیگر در زمینۀ استرداد مجرمان، اعطای اطلاعات به‌صورت داوطلبانه از سوی کشورهای عضو بدون درخواست رسمی، حفظ فوری داده‌های رایانه‌ای ذخیره‌شده در قلمرو دولت‌ها، افشای فوری دادۀ ترافیک حفاظت‌شده مبنی بر درخواست دولت‌های دیگر، دسترسی به داده‌های رایانه‌ای،

جمع‌آوری زندهٔ دادهٔ ترافیک و شـــنود دادهٔ محتوا در این مقررات مورد اشـــاره قرار گرفته‌اند (قربان نیا و نمانیان، ۱۳۹۴: ۱۰۶-۱۰۴).

سندی دیگر که به‌صورت کلی به حمایت‌های شکلی از بزه‌دیدگان پرداخته است، اعلامیهٔ اصـــول بنیادین عدالت برای بزه‌دیدگان و قربانیان سوءاســـتفاده از قدرت، مصوب ۲۹ نوامبر ۱۹۸۵ است که به فراهم کردن و تقویت ابزارهای کشف، پیگرد و صدور حکم محکومیت برای بزهکاران، توصیه کرده اســـت. همچنین، پیش‌نویس کنوانســـیون سازمان ملل متحد دربارهٔ عدالت و پشتیبانی از بزه‌دیدگان و قربانیان سوءاستفاده از قدرت، سازوکارهای شکلی را برای حمایت از بزه‌دیدگان جرائم مورد توجه قرار داده اســـت. در خصوص حمایت‌های شـــکلی از بزه‌دیدگان در این کنوانســـیون، می‌توان به مقرره‌ای اشاره کرد که به اقداماتی نظیر «کشف، پیگرد، تعیین کیفر و اصلاح و تربیت مرتکبان، هماهنگ با هنجارهای بین‌المللی و به فراهم کردن خدمات برای بزه‌دیدگانی که آسیب بیشتری دیده‌اند اشاره می‌کند» (مادهٔ چهار).

شیوه جبران خسارت از بزه‌دیدگان تروریسم سایبری در حقوق بین‌الملل

– **اعادهٔ وضع به حالت سابق:** جبران خسارت باید در حد امکان تمام آثار عمل غیرقانونی را از بین ببرد و وضعیت را به حالت قبل از ارتکاب عمل غیرقانونی بازگرداند و در صورتی که این امر ممکن نباشد باید غرامتی به ارزش اعاده به وضع سابق پرداخت شود. منظور از اعاده به وضع ســـابق این اســـت که مرتکب حقوق قربانی را که در اثر اقدام مجرمانه نقض شده‌اند، بازگرداند. البته این اعاده زمانی ممکن اســـت که مال یا پول از دســـت رفته هنوز موجود باشد (روزنهان و سالیگمن، ۱۳۸۹: ۲۸۸).

– **پرداخت غرامت:** ادعای پرداخت غرامت در کنار یا به جای اعاده به وضع ســـابق مطرح می‌شـــود و غالباً با تقاضای جلب رضایت همراه اســـت. غرامـــت در مقابل زیان‌های مادی یا غیرمادی ناشـــی از نقض تعهد که عینی و بالفعل باشـــد، پرداخت می‌شود. کمیسیون حقوق بین‌الملل در مادهٔ ۳۶ بیان می‌دارد که غرامت باید تمامی خســـارات مالی قابل ارزیابی شامل منافع بالفعل را در برگرفته که به سه شکل غرامت اسمی، غرامت برای خسارت مادی و مالی و غرامت برای خسارت معنوی قابل دریافت است.

- **جلب رضایت زیان‌دیده:** اگر بزه ارتکابی از طریق اعداه وضع یا پرداخت غرامت قابل جبران نباشد، مرتکب مکلف به جلب رضایت زیان‌دیده نسبت به خسارت وارده است. جلب رضایت می‌تواند به‌صورت اعتراف به نقض، اظهار پشیمانی، عذرخواهی رسمی یا هر روش مناسب دیگری باشد. جلب رضایت زیان‌دیده جنبه‌ای از جبران عمل نامشروع و در مفهوم موسع کلمه است؛ این شکل از جبران برای خسارت‌های غیرمادی مناسب است (ووترز[1]، ۲۰۱۳: ۱۲۹)

- **مساعدت:** علاوه بر نیازهای متعدد مالی، قربانیان یک جرم خشونت‌بار ممکن است نیازمند مراقبت پزشکی فوری یا حتی درازمدت و همچنین دیگر اشکال مساعدت باشند و براساس آن‌ها، قربانیان باید مساعدت‌های لازم مادی، پزشکی، روان‌شناختی و اجتماعی را از رهگذر ابزار دولتی، داوطلبانه، اجتماعی و بومی دریافت کنند. اشکال متعدد مساعدت نه‌تنها از طرف دولت، بلکه از طرف جامعه و اجتماعات تخصصی نیز قابل پیش‌بینی است. بخش عمده‌ای از این خدمات و مساعدت‌ها می‌تواند با توسعهٔ انجمن‌ها یا نهادهای محلی دارای کارکنان متخصص و آشنا با نیازهای خاص قربانیان جرم بهبود یابد.

- **رجوع به دادگاه‌های بین‌المللی:** دیوان بین‌المللی دادگستری، اصولاً صلاحیت رسیدگی به عمل متخلفانهٔ بین‌المللی دولتی را دارد که صلاحیت دیوان را برای رسیدگی پذیرفته باشد. منظور از عمل متخلفانهٔ بینالمللی، فعل یا ترک فعل دولت است که با تعهد بین‌المللی لازم‌الاجرای دولت متخلف در زمان نقض همخوانی و سازگاری نداشته باشد (مادهٔ ۱ و ۲ معاهدهٔ مسئولیت کشورها در برابر اعمال متخلفانهٔ بین‌المللی، مصوب ۲۰۰۱). دیوان اصولاً صلاحیت رسیدگی به پرونده‌های کیفری را ندارد. پس اگر یک جرم سایبری صرف ارتکاب یابد، قطعاً دیوان صلاحیت رسیدگی نخواهد داشت، اما چنانچه فضای سایبری ابزاری برای نقض یک تعهد بین‌المللی باشد که منجر به عمل متخلفانهٔ بین‌المللی برای آن دولت می‌شود، ممکن است دیوان بتواند اعمال صلاحیت کند. مثلاً در مورد کنوانسیون نسل‌زدایی، همانگونه که در مادهٔ ۹ آن آمده است، دیوان صلاحیت رسیدگی دارد. البته عمل متخلفانهٔ مزبور یا باید قابل انتساب به دولت متخلف باشد یا دولت مزبور عملی را که اساساً قابل انتساب به آن نیست را پذیرفته یا مورد تأیید قرار داده باشد (الین[2]، ۲۰۱۶: ۵۶۳).

1. Wouters
2. Elain

نتیجه‌گیری و پیشنهادها

در راستای حمایت از بزه‌دیدگان تروریسم سایبری در حقوق کیفری ایران، هیچ‌گونه مقررهٔ خاصی اندیشـــیده نشده اســـت و حتی برای بزه‌دیدگان سایبری به معنای اخص، حمایت‌های ویژه‌ای تخصیص نیافته اســـت. شاید با تعیین کیفر برای مرتکبان جرائم سایبری، بتوان گفت که فقط حمایت‌های کیفری برای بزه‌دیدگان ســـایبری اتخاذ شده و دیگر نیازهای بزه‌دیدگان از جمله نیازهای عاطفی یا جبران خسارت‌های متناسب با بزه‌دیدگی آن‌ها بدون جبران باقی مانده اســـت. این نکتهٔ روشن است که بزه‌دیدگان سایبری، یکی از بی‌دفاع‌ترین و بی‌گناه‌ترین اشخاصی هستند که در اثر فرایند بزه‌دیدگی، متحمل خسارت‌های مادی، عاطفی، اجتماعی و در برخی موارد پزشکی می‌شوند، اما به دلیل برخی ویژگی‌های فضای سایبر، چالش‌های تعقیب مجرمان و فقدان مقررات کافی، نیازهای آن‌ها بدون جبران باقی می‌ماند. در راســـتای جبران خسارت مادی ناشی از بزه‌دیدگی سایبری نیز، فقط با استناد به برخی قواعد عام، همچون قانون مسئولیت مدنی برای جبران خسارت مادی از بزه‌دیدگان سایبری اقدام می‌شود، در صورتی که به دلیل متفاوت بودن محیط ارتکاب جرم و شرایط بزه‌دیده و بزهکار، نمی‌توان از قواعد و آیین دادرسی سایر جرائم که در محیط فیزیکی تحقق می‌یابند، استفاده کرد.

اســـناد بین‌المللی نیز با وجود اهتمام ویژه به موضوع تروریسم در قالب قطعنامه‌ها و اعلامیه‌های الزام‌آور و غیرالزام‌آور در زمینهٔ جرم‌انگاری رفتارهای بزهکارانهٔ تروریستی، سندی مختص به تروریسم سایبری وجود ندارد و در دیگر اسناد مرتبط با تروریسم، به جرم‌انگاری تروریسم سایبری و حمایت از بزه‌دیدگان آن پرداخته نشـــده اســـت. آنچه در اسناد بین‌المللی در رابطه با عنصر قانونی تروریسم ســـایبری می‌توان یافت، جرائمی هســـتند که بیش‌ترین ظهور را در مفهوم تروریسم سایبری دارند و به‌صورت عام و غیرمســـتقیم به تروریســـم سایبری اشـــاره کرده‌اند. بنابراین، در زمینهٔ حمایت و پشتیبانی از بزه‌دیدگان تروریسم سایبری، کنوانسیون‌هایی همچون کنوانسیون جرائم سایبر به‌طور عام به حمایت از بزه‌دیدگان ســـایبری پرداخته‌اند و تنها از طریق تطبیق و مقایسه می‌توان مقررات آن‌ها را برای بزه‌دیدگان تروریســـم سایبری استدلال و استخراج کرد. نمونه‌ای از اسنادی که به‌طور اختصاصـــی بـــه حمایت از بزه‌دیدگان جرائم پرداخته‌اند، اصـــول بنیادین عدالت برای بزه‌دیدگان و قربانیان سوءاستفاده از قدرت و کنوانسیون مبارزه با جرائم خشونت‌بار هستند که به‌صورت کلی به

انواع حمایت‌های مادی، پزشکی، عاطفی، اجتماعی از بزه‌دیدگان اشاره کرده‌اند. بنابراین، سازمان‌های بین‌المللی که در رأس آن‌ها سازمان ملل متحد وجود دارد و همچنین شورای وزرای اروپا که نقش فزاینده‌ای را در جهت تقویت و گسترش جرم‌انگاری جرائم سایبری در دهۀ اخیر ایفا کرده‌اند، می‌توانند با استفاده از کمیته‌های تخصصی و استفاده از متخصصان دیگر کشورها که در زمینۀ تروریسم سایبری و جرم‌انگاری آن پیشتاز بوده‌اند، برای تدوین کنوانسیون‌های الزام‌آور بین‌المللی در خصوص پیشگیری از تروریسم سایبری و حمایت ویژه از بزه‌دیدگان آن اقدام کنند.

در این راستا، تبیین و ارائه پیشنهادهای زیر ضروری به نظر میرسد:

- اگرچه با توجه به نوظهور بودن جرائم سایبری، مرجع قضایی بین‌المللی مشخصی تاکنون برای رسیدگی این جرم پیش‌بینی نشده است، ولی با توجه به نحوۀ احراز صلاحیت دیوان بین‌المللی دادگستری در رسیدگی به جرائم، بدیهی است که در صورت تحقق شرایط مذکور، دیوان به عنوان یک دادگاه بین‌المللی قضایی می‌تواند در حمایت از بزه‌دیدۀ یک جرم سایبری وارد رسیدگی شود.
- با توجه به تخصصی بودن فضای سایبری، قضاتی که به جرائم مرتبط به این فضا رسیدگی می‌کنند، باید در حوزۀ فناوری اطلاعات و سایر فناوری‌های مرتبط متخصص باشند. بنابراین، اگرچه با نوظهور بودن تروریسم سایبری تاکنون مرجع قضایی بین‌المللی مشخصی پیش‌بینی نشده است، به نظر میرسد ضرورت دارد تا یک دادگاه ویژه جرائم سایبری تشکیل شود یا در دیوان کیفری بین‌المللی شعب تخصصی برای رسیدگی به این جرم تشکیل شود.
- حضور گسترده و فعال ضابط قضایی بین‌المللی تحت عنوان پلیس بین‌الملل، با ابعاد و شمول گسترده جهت مقابله با این پدیدۀ نامیمون، کشف، شناسایی و در نهایت تعقیب مجرمان در این عرصه، گامی ضروری به نظر میرسد.

منابع

منابع فارسی

- احمری، حسین و کحلکی، غلامرضا (۱۳۹۵). تحلیل سازه‌انگارانهٔ تروریسم سایبری و رویکرد نظام حقوقی به آن. *فصلنامهٔ پژوهش‌های روابط بین‌الملل*. شمارهٔ شانزدهم، دورهٔ نخست.

- اسلامی، ابراهیم (۱۳۹۵). جایگاه حمایت از بزه‌دیدگان جرائم سایبری در مقررات کیفری حقوق داخلی و حقوق بین‌الملل. *پژوهشنامهٔ حقوق اسلامی*. شمارهٔ اول، سال هفدهم.

- پاکزاد، بتول (۱۳۹۰). ماهیت تروریسم سایبری. *مجلهٔ تحقیقات حقوقی*. شمارهٔ ۴.

- پوربافرانی، حسن (۱۳۹۶). *حقوق جزای بین‌الملل*. تهران: انتشارات جنگل.

- پوربافرانی حسن، امیدی علی، قلی زاده بهروز (۱۳۹۶). درآمدی بر یکسان‌انگاری جرم دزدی دریایی با تروریسم. *مجلهٔ مطالعات حقوقی*. دورهٔ دوم، شمارهٔ نهم.

- پورنقدی، بهزاد و بختیاری، ارشد (۱۳۹۲). تروریسم سایبری و اهمیت آن در برهم‌زدن امنیت بین‌المللی. *مطالعات بین‌المللی پلیس*. دورهٔ چهارم، شمارهٔ ۱۴.

- تقی زاد، مهرداد و زمردی، کیوان (۱۳۹۵). نقش اتحادیهٔ اروپا در قاعده‌مندسازی جرائم سایبری. *مطالعات بین‌المللی پلیس*. سال ششم، شمارهٔ ۲۵.

- جاویدنیا، جواد (۱۳۸۶). نقد و بررسی جرم‌های مندرج در قانون تجارت الکترونیکی. *مجلهٔ حقوقی دادگستری*. شمارهٔ ۵۹.

- جلالی فراهانی، امیرحسین و باقری اصل، رضا (۱۳۸۶). پیشگیری اجتماعی از جرائم و انحرافات سایبری. *مجلس و پژوهش*. سال ۱۴، شمارهٔ ۵۵.

- جلالی فراهانی، امیرحسین و باقری اصل، رضا (۱۳۸۷). پیشگیری اجتماعی از جرائم سایبری راهکاری اصلی برای نهادینه‌سازی اخلاق سایبری. *اطلاع‌رسانی و کتابداری رهآورد نور*. شمارهٔ ۲۴.

- جلالی فراهانی، امیرحسین (۱۳۸۹). *کنوانسیون جرائم سایبر و پروتکل الحاقی آن (به همراه گزارش‌های توجیهی آن‌ها)*. تهران: خرسندی. چاپ اول.

- دهشیری، محمدرضا (۱۳۹۵). بررسی و تحلیل تروریسم سایبری با رویکرد پیشگیری وضعی. *فصلنامهٔ دانش انتظامی لرستان*. سال؟ شماره؟ صص؟

- رایجیان اصلی، مهرداد (۱۳۹۰ الف). *بزه‌دیده شناسی حمایتی*. تهران: دادگستر. چاپ دوم.

- روزنهـــان دیوید ال. و ســـلیگمن مارتیـــن. ای. بی. (۱۳۸۹). *روان‌شناســـی نابهنجاری؛ آسیب‌شناسی روانی* (سید یحیی محمدی). جلد اول. تهران: ساوالان. چاپ دوازدهم.

- زرنشـــان، شهرام (۱۳۸۶). *شورای امنیت و تعهد دولت‌ها برای مقابله با تروریسم*. تهران: مرکز امور حقوقی بین‌المللی معاونت حقوقی و امور مجلس ریاست جمهوری.

- ساعد، نادر (۱۳۸۹). *منابع حقوق مبارزه با تروریسم در ایران*. تهران: خرسندی.

- شـــمس ناتری، ابراهیم و اســـلامی، داود (۱۳۹۴). ماهیت کیفری تأمین مالی تروریسم. *مطالعات حقوق کیفری و جرم‌شناسی*. شمارۀ ۵ و ۶.

- صارمی، احمد (۱۳۹۲). رسیدگی به جرائم هواپیمایی در نظام کیفری بین‌المللی و ملی. *مطالعات بین‌المللی پلیس*. شمارۀ ۱۴.

- طیبی‌فرد، امیرحسین (۱۳۸۴). مبارزه با تأمین مالی تروریسم در اسناد بین‌المللی. *دفتر خدمات حقوقی بین‌المللی جمهوری اسلامی ایران*. شمارۀ ۳۲.

- عالی پور، حسن(۱۳۹۰). *حقوق کیفری فناوری اطلاعات*. تهران: خرسندی. چاپ اول.

- قانون تجارت الکترونیک، مصوب ۱۳۸۲.

- قانون جرائم رایانه‌ای، مصوب ۱۳۸۸.

- قربـــان نیا، ناصر و نمامیان، پیمان (۱۳۹۴). جایگاه حمایت از بزه‌دیدگان تروریســـم در نظام حقوق بین‌المللی. جلد ۱۲. *مجلۀ حقوق تطبیقی*. شمارۀ ۲.

- موسوی، محمدرضا و حیدری، خدیجه (۱۳۹۲). تأثیر تهدیدات امنیتی تروریسم سایبری بر امنیت ملی جمهوری اســـلامی ایران و راهکارهای مقابله با آن. *مجلۀ مطالعات بین‌المللی پلیس*. دورۀ چهارم، شمارۀ ۱۴.

- موســـوی، سید رضا (۱۳۹۰). پیشـــگیری وضعی از جرائم سایبری در قالب تدابیر فنی و محدودیت‌هـــای پیش‌روی آن. *همایـــش منطقه‌ای چالش‌های جرائم رایانه‌ای در عصر امروز*. انجمن‌های علمی، ادبی و هنری دانشگاه آزاد اسلامی واحد مراغه.

- هاشـــمی، سید حســـین (۱۳۹۰). *تروریسم از منظر حقوق اسلام و اسناد بین‌المللی*. قم: پژوهشگاه حوزه و دانشگاه. چاپ اول.

اسناد بین‌المللی

- راهبرد جهانی ضد تروریسم سازمان ملل متحد در سال ۲۰۰۵.

- قطعنامـــهٔ راجع به حمایت از قربانیان نقض‌های فاحش حقوق بین‌المللی حقوق بشـــر و نقض شدید حقوق بشردوستانهٔ بین‌المللی، مصوب ۲۰۰۵.

- قطعنامهٔ شمارهٔ ۱۳۷۳ شورای امنیت، مصوب ۲۰۰۱.

- کنوانسیون اروپایی پیشگیری از تروریسم مصوب ۲۰۰۵.

- کنوانسیون اروپایی مقابله با تروریسم، مصوب ۱۹۹۹.

- کنوانسیون بین‌المللی حقوق مدنی و سیاسی، مصوب ۱۹۶۶.

- کنوانسیون پیشگیری و سرکوب اعمال تروریستی سازمان کشورهای آمریکایی، مصوب ۱۹۷۱.

- کنوانسیون جلوگیری از بمب‌گذاری تروریستی، مصوب ۱۹۹۷.

- کنوانســـیون راجع بـــه جلوگیری از اعمال غیرقانونی علیه امنیت هواپیمایی کشـــوری، مصوب ۱۹۷۱.

- کنوانسیون منع حمایت مالی از تروریسم، مصوب ۱۹۹۹.

- Dunn. Myriam, Mauer, V. (2006). (eds.) International CIIP Handbook, ETH Zurich: Center for Security Studies,Vol. II.

- Elain, Fahey (2016). The EU cybercrime &cyber – security Rule-Making: Maping the Internal & External Dimensions of EU Security, University of Amesterdam, Forthcoming European Journal of Risk Resoloution, vol 1.

- Rohas. N. (2012). Cyber Terrorism in the Context of Globalization, II World Congress on Informatics and Law Madrid, Spain. pp. 1-26. Retrieved From: www.barzaloo.com.

- Teodoro. P. Garcı´a., Verdejo. J. Dı´az., Ferna´ndez. G. Macia., Vazquez. E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges, computers & security vol 28, Issues 1–2.

- Wouters, Jan & Sanderjin, Duquet (2013). The UN, The European Union and multilateral actions against terrorism, Leuven center for global Governance studies, working paper No.113.

منابع انگلیسی

Documents

- United Nation Resolutions:45/121:1998.
- United Nation Resolutions:Con.Annex to Res.No. 26/59/P, 1999.
- United Nation Resolutions:SC/1373, 2001.
- United Nation Resolutions:56/121, 2001.
- United Nation Resolutions:56/121, 2002.
- United Nation Resolutions:57/239, 2003.
- United Nation Resolutions:58/199, 2004.
- United Nation Resolutions:58/199, 2004.
- United Nation Resolutions:64/211, 2010.