



وضعیت بزهدیدگان تروریسم سایبری در پرتو حقوق کیفری ایران

محسن قدیر

هیئت علمی، استادیار، دکترای حقوق بین الملل، دانشگاه قم، دانشگاه قم، قم، ایران

حسین کاظمی فروشانی^۱

دانش آموخته کارشناسی ارشد حقوق بین الملل، دانشگاه قم، قم، ایران

نرگس اکبری

دانش آموخته دکتری حقوق بین الملل، دانشگاه آزاد تهران جنوب، تهران، ایران

(تاریخ دریافت: ۱۳۹۷/۱۰/۱۲ تاریخ پذیرش: ۱۳۹۷/۱۲/۲۴)

چکیده

فضای مجازی همچون فضای حقیقی، محلی را برای ارتکاب جرایم توسط بزهداران فراهم آورده است و آن‌ها دیگر کنش‌گران حاضر در این فضا را مورد سوءاستفاده قرار می‌دهند ماهیت گسترده و فرامرزی بودن این جرم باعث شده است تا از حیث مقابله با جرم سایبری و حمایت از بزهدیدگان آن تاکنون اقدام مؤثری از سوی کشورها صورت نپذیرد. با توجه به شیوع حملات سایبری در سرتاسر جهان، لزوم توجه به بزهدیدگان تروریسم سایبری در حقوق موضوعه دیده می‌شود. در راستای حمایت از بزهدیدگان تروریسم سایبری در حقوق ایران، هیچ گونه مقرره خاصی اندیشیده نشده است. با تعیین کیفر برای مرتکبان جرایم سایبری فقط حمایت‌های

کیفری برای بزه‌دیدگان سایبری اتخاذ شده و دیگر نیازهای بزه‌دیدگان بدون جبران باقی مانده است. لذا 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. موضوع مسئولیت کیفری و تبیین گستره آن در حقوق جرایم رایانه‌ای از اهمیت بسیار زیادی برخوردار است و ممکن است سؤالات زیادی در رابطه با گستره مسئولیت افراد در محیط مجازی مطرح شود که قانون‌گذار ایران فصل ششم از قانون جرایم رایانه‌ای را به موضوع مسئولیت کیفری اختصاص داده است.

واژگان کلیدی

تروریسم سایبری، بزه دیدگان، مسئولیت کیفری، حقوق ایران، فضای سایبری

victims situations support according to Iran criminal law

Abstract

Cybernetic terrorism today has become one of the major challenges for legal systems, particularly criminal systems. finally terrorism crime, changed from traditional approaches and turned into new technologies. in most countries, especially developed countries, computers and communications facilities carrying out daily activities such as credit and financial affairs, office automation, controls and supervision in the field of industrial infrastructure, military, healthcare, and etc. critical and informationa infrastructure as the main victims of cyber terrorism, are the most attractive and desirable. looking at the increasing incidents of cyber attacks against developed countries and the incidence of severe damage to critical infrastructure, cyber attacks against the system, results can be disastrous, and have a strong impact on the physical security of assets, safety of the national economy and general safety. In recent years, use of this kind attacks against government critical and vital installations increased and due to offender's identity to remain hidden feature, these terrorism have been special concerned with governments and individuals. by considering the current situation and the rise of political and economic tensions between governments, special protection from cybernetic.

Keywords

cyber terrorism, victims, International organizations, Iran law, International documents



مقدمه

تروریسم سایبری صرفاً، به اقدامات خشونت آمیز سایبری از سوی گروهی با ویژگی های خاص اطلاق می شود که به اهداف مشخصی تعرض می کنند. اقدامات تروریستی باید در حدی باشند که بتوان معادل جنگ اطلاعات را برای آنها بکار برد. جنگ اطلاعات یک اقدام تروریستی است که برای ایجاد اختلال یا آسیب رسانی یا قطع جدی ارتباطات طرح ریزی می شود (جلالی فراهانی، ۱۳۸۵ : ۹۶-۹۵). گستردگی فضای سایبر و به خدمت گرفتن آن توسط اکثر افراد جامعه و زیرساخت های کشور، طیف گسترده ای از مباحث را پیرامون بزه دیدگان این پدیده و چگونگی حمایت و جبران خسارت های وارد آمده به آن ها را چه در حقوق داخلی کشورمان و کشورهای دیگر و چه در سطح بین الملل شکل داده است.

با توجه به شیوع حملات سایبری در سرتاسر جهان، لزوم توجه به بزه دیدگان تروریسم سایبری در حقوق موضوعه ایران دیده می شود. کشور ما نیز از حملات سایبری مستثنی نبوده به طوری که در سال های اخیر، به دلیل شدت گرفتن مخالفت های سران کشورهای اروپایی و غربی به ادامه فعالیت های هسته ای در ایران، حملاتی به قصد مختل کردن این تأسیسات، از سوی برخی کشورها از قبیل اسرائیل و آمریکا صورت گرفته است. در خصوص موضع حقوق کیفری ایران در مقابله با تروریسم می توان گفت که قانونگذار کیفری ایران فاقد جرم انگاری مستقل در مورد تروریسم و جرایم آن است و در واقع سیاست جنایی ایران مبتنی بر سیاست مصداقی است و می توان مواردی را که با مفهوم تروریسم منطبق است تشخیص داد. از جمله موارد جرم انگاری شده که می توان برای مقابله با تروریسم استناد کرد، محاربه است و البته عده ای معتقدند که با جرم انگاری عنوان فقهی محاربه می توان با تروریسم و اشکال آن مقابله کرد ولی آشکار است که با توجه به گسترش فن آوری های نوین و استفاده گروه های تروریستی از آن، دیگر محاربه قادر نیست به تمامی این رفتارها پاسخ دهد.

جرایم مختلفی ممکن است در محیط اینترنت به وقوع بپیوندند و در نتیجه مجرمین متعددی اقدام به ارتکاب جرم در محیط اینترنت می نمایند، عدم هماهنگی حقوق جزاء با این پدیده ها یعنی عدم جرم انگاری جرایمی که در محیط اینترنت به وقوع می پیوندند، عدم ایجاد مسئولیت برای بزه کارانی که از این محیط برای انجام رفتارهای بزه کارانه خویش بهره می جویند و ... مطمئناً راه را برای ارتکاب جرایم بسیار زیادی در محیط اینترنت و سایبر فراهم خواهد نمود، بر این اساس باید اذعان داشت که پیشرفت فن آوری نباید بتواند جلوی

جلوگیری و مقابله با جرایم را در حقوق جزا بگیرد، بنابراین مهم‌ترین مسئله‌ای که در پیش روی نظام‌های کیفری مختلف وجود دارد ایجاد و پذیرش تغییرات در راستای مبارزه و مقابله با جرایم مختلفی است که با استفاده از اینترنت و یا در محیط مجازی به وقوع می‌پیوندند و مبحث شناخت مسئولیت کیفری برای مجرمینی که در این محیط اقدام به ارتکاب رفتارهای بزهکارانه می‌نمایند، است. متأسفانه قواعد موجود و سازوکارهای فعلی در چارچوب حقوق کیفری موثر و کافی نمی‌باشد اما دادگاه‌های ملی می‌توانند با توسل به اصول مختلف حاکم بر صلاحیت بویژه اصل صلاحیت جهانی در حمایت از بزه دیدگان موثر باشند. لذا در این مقاله تلاش شده است با روش توصیفی و تحلیلی پس از جمع‌آوری و تبیین مقررات کیفری داخلی موجود و تحلیل آنها با توجه به ضرورت حمایت از بزه دیدگان تروریسم سایبری در عرصه حقوق داخلی چاره‌اندیشی مناسبی شناسایی و ارائه گردد.

۱- حمایت‌های کیفری و مدنی از بزه‌دیدگان تروریسم سایبری در حقوق ایران

۱-۲. 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 بر می‌دارد که در آستانه بزه‌کاری هستند. با توجه به مطالب فوق، تروریسم سایبری از جهات گوناگون می‌تواند مورد حمایت کیفری قرار گیرد. بنابراین از آن جایی که بزه تروریسم سایبری دارای مقررۀ اصلی و عمدۀ کیفری نیست و نیز با توجه به این که ادبیات جزایی کشورمان تحت این عنوان نپرداخته، بلکه در یک یا دو دسته کلی، جرایمی را که بعضاً ظهور در این جرم دارند را مورد بحث قرار داده است، از این رو با ضعف ادبیات جزایی مواجه هستیم. در راستای حمایت کیفری از بزه‌دیدگان تروریسم سایبری، در ذیل به شرح سه گونه از این اعمال در رابطه با حمایت از بزه‌دیدگان مذکور پرداخته می‌شود:

۱-۱-۲. حمایت کیفری ساده

حمایت کیفری ساده، یکی از گونه‌های حمایت کیفری محسوب می‌شود که "شامل جرم‌انگاری هر رفتار منع شده‌ای است که به طور 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 می‌گردد.

ماده ۱۱ قانون جرائم رایانه ای به حمایت از تأسیسات رایانه‌ای و مخابراتی که مورد استفاده عمومی هستند، پرداخته، که بزه دیده عمده تروریسم سایبری به شمار می‌آیند. با توجه به مفاد ماده، عنصر مادی شامل افعالی است که به صورت غیر حصری منجر به سلب آسایش مردم می‌شود (جلالی فراهانی - باقری اصل، ۱۳۸، ص ۱۳۱). برهم زدن نظم و آسایش عمومی، رکن اصلی بزه‌های تروریستی است که در ماده فوق به آن اشاره گردیده است. اما آن چه ماده فوق را به جرم‌انگاری تروریسم سایبری نزدیک کرده است، سلب امنیت و آسایش عمومی در اثر افعال ارتكابی غیر حصری در مواد هشت الی ۱۰ علیه زیرساخت‌های عمومی و ضروری کشور است. بنابراین با دقت در ماده ۱۱ قانون جرایم رایانه‌ای، می‌توان به دو رکن از ارکان اصلی تروریسم سایبری، یعنی ارتكاب افعال عمدی که منجر به مختل شدن رفاه و آسایش عمومی جامعه در اثر وقوع جرم علیه تأسیسات رایانه‌ای و مخابراتی پی برد. همچنین این ماده به بزه‌دیدگان حقوقی، یعنی تأسیسات ضروری مورد استفاده عمومی اشاره کرده اما تنها حمایت اندیشیده شده فقط شامل حمایت کیفری است (سلامتی، ۱۳۸۷: ۳۲۵).

در خصوص تبیین ماده قانونی فوق و تطبیق آن با بزه تروریسم سایبری، می‌توان گفت که ماده ۱۱ دارای اشکالاتی است. یکی از اشکالات ماده فوق این است که نحوه ارتكاب بزه علیه تأسیسات مذکور مشخص نشده و به صورت کلی هر روشی را که منجر به اختلال آن‌ها می‌شود را مد نظر قرار داده است. در حالی که تروریسم سایبری، باید از طریق و مجرای فضای سایبر، یعنی اینترنت یا محیط شبکه وقوع یابد. بر اساس مفاد ماده فوق، بمب گذاری و تخریب فیزیکی تأسیسات عمومی مبتنی بر رایانه و دستگاه‌های مخابراتی نیز، مشمول مقررۀ فوق می‌گردد (موسوی، ۱۳۹۰، ۱۴). اشکال دیگر مقررۀ فوق این است که فقط به مجازات حبس بزهکار اشاره نموده و به عنوان یک مقررۀ اصلی به حمایت از بزه‌دیدگانی که در اثر افعال مواد هشت الی ده 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 ماده ۱۱ به بزه تروریسم سایبری به صراحت اشاره می‌کرد و انواع جبران خسارت برای افراد بزه‌دیده و همچنین به جزای نقدی به عنوان مکمل کیفر اشاره می‌نمود (عالی پور، ۱۳۹۰، ۲۱۴).

علاوه بر افعال غیرقانونی در ماده ۱۱ این قانون، مواد هشت الی ۱۰ همین قانون به دسته‌ای دیگر از افعال مادی این بزه پرداخته است. در این سه ماده به صورت کامل و غیر حصری، به شایع‌ترین اعمال ارتكابی که علیه تأسیسات حیاتی کشور انجام می‌شود پرداخته است. عنصر مادی بزه در سه ماده فوق، افعالی هستند که به صورت مصداقی برای هدف قرار دادن سیستم‌های رایانه‌ای و مخابراتی که امور اجرایی کشور به آن‌ها وابسته است، اشاره شده است^۱. همان طور که در ابتدای بحث اشاره گردید، ماده ۱۱ شباهت خاصی به تروریسم سایبری دارد و قانون‌گذار در مواد هشت الی ۱۰ به صورت جامع به افعال غیرمجاز پرداخته که اقدام شایسته‌ای در خصوص جرم‌انگاری غیرمستقیم افعال مرتبط با تروریسم سایبری است (باطنی - پارچی آبادی، ۱۳۹۰، ۱۰۰).

علاوه بر حمایت‌های ماهوی در این قانون، حمایت شکلی از بزه‌دیدگان یکی از راهکارهایی است که در بیشتر نظام‌های حقوقی به منظور رعایت حقوق بزه‌دیده به کار گرفته می‌شود. در خصوص حمایت شکلی از بزه‌دیدگان حقوقی تروریسم سایبری، می‌توان به قواعد مربوط به صلاحیت بند ج ماده ۲۸ اشاره نمود که دادگاه‌های ایران را در صورت وقوع حملات رایانه‌ای صالح به رسیدگی دانسته است (پوربافرانی، ۱۳۹۶، ۱۶-۱۵). مواد ۶۶۴ و ۶۶۵ آ.د.ک به صلاحیت دادگاه‌های ایران در رسیدگی به جرائم سایبری باتوجه به اصول حمایتی، شخصی، سرزمینی و جهانی پرداخته است. که بزه دیدگان مصرح در بندهای الف، ب، پ و ت ماده ۶۶۴ می‌توانند به دادگاه‌های ایران جهت رسیدگی به جرائم وقوع پیوسته مراجعه نمایند لذا صرف نظر از ایرادات و اشکالاتی که به ایت بخش از آئین دادرسی جرایم رایانه‌ای مطرح است، آن است که مقنن در بند ت ماده ۶۶۴ صرفاً به جرایم رایانه‌ای متضمن سوء استفاده از اشخاص کمتر از ۱۸ سال، اعم از اینکه بزه دیده ایرانی یا غیرایرانی در ایران یافت شود، پرداخته است. درحالی که می‌توانست تا با توجه به موارد صلاحیت جهانی محاکم در رسیدگی جرائم بین‌المللی مانند جرائم علیه بشریت یا نسل‌کشی، چنانچه جرایم رایانه‌ای منتهی به جرائم بین‌المللی مذکور گردد مورد توجه قرار می‌گرفت تا از این حیث امکان حمایت از بزه‌دیدگان سایبری در صورت

۱- این افعال شامل: حذف، تخریب، مختل و غیرقابل پردازش کردن داده‌ها در سیستم‌های رایانه‌ای و مخابراتی، اقدام به وارد کردن، 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، اقدام به وارد کردن، انتقال دادن، پخش کردن، حذف کردن، مختل کردن، متوقف کردن، دست‌کاری یا تخریب داده‌ها یا امواج الکترومغناطیسی یا نوری سیستم‌های رایانه‌ای یا مخابراتی است.

تحقق جرائم بین المللی نیز فراهم می گردید و آنچه راجع به صلاحیت دادگاه های ایران در رسیدگی به جرائم حاصل از بند ب ماده ۶۶۴ مطرح می شود خالی از ایراد و سوال نمی باشد. لذا چنانچه بزه دیدگان جرم ارتكابی از طریق تارنماهای دارای دامنه مرتبه بالای کد کشور ایران ارتكاب یابد تبعه های کشورهای خارجی باشند مشخص نیست که رویکرد مقنن و دادگاه های ایران در رسیدگی به شکایات بزه دیدگان سایبری ساکن در کشورهای بیگانه چگونه است (اسلامی، ۱۳۹۵، ۱۷۷).

اقدام حمایتی دیگر این قانون را می توان حفظ داده های رایانه ای یا سامانه های رایانه ای و مخابراتی دانست که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود دارد که این حمایت از حمایت های تبعی از بزه دیدگان مطرح می باشد و برای تحقیق و بازرسی لازم و ضروری است از سوی مقامات قضایی دستور حفاظت و یا توقیف و تفتیش آنها صادر شود و چنانچه ضابطان قضایی، کارکنان دولت و یا اشخاصی که وظیفه حفاظت از داده ها به آنها سپرده شده خودداری یا افشا نمایند مطابق مواد ۶۶۹ و ۶۷۰ و ۶۷۱ مستوجب مجازات است. این امر مبین آن است که مقنن در حفظ حقوق بزه دیده سایبری از حیث جمع آوری و نگهداری ادله جرم و شناسایی مجرمین اهمیت بسزائی قائل است (دهشیری، ۱۳۹۵: ۵۸).

حمایت کیفری صورت گرفته در قانون تجارت الکترونیکی، شامل داده‌هایی است که در بستر مبادلات الکترونیکی مورد استفاده قرار می‌گیرند. این قانون به حمایت از داده‌های شخصی پرداخته و هرگونه تعرض به آن‌ها را بدون رضایت دارنده آن‌ها غیرقانونی تلقی کرده و مجازات‌هایی را برای مرتکب در نظر گرفته است (مواد ۵۸ و ۵۹ قانون تجارت الکترونیک، مصوب ۱۳۸۲). در مقرراتی دیگر از قانون فوق، به حمایت کیفری ویژه از داده پیام‌های شخصی پرداخته که مرتکب این دسته از جرایم اشخاص خاصی هستند که توسط نهادهای مسئول و دفاتر خدمات صدور گواهی الکترونیکی ارتكاب می‌یابند؛ در این صورت برای مرتکب حداکثر کیفر تعیین شده است (ماده ۷۲ قانون تجارت الکترونیک، مصوب ۱۳۸۲).

به دلیل ابهامات و خلاهای موجود در حمایت از بزه دیدگان سایبری که ماده ۶۷۸ آ.د.ک بیان می دارد در مواردی که برای رسیدگی به جرائم رایانه ای مقررات خاصی پیش بینی نشده، موضوع تابع قانون آئین دادرسی کیفری است، گونه های سیاست جنایی دولت‌ها در حمایت از بزه دیدگان اصولاً در سه حالت حمایت از بزه دیده، بلافاصله پس از تحقق جرم، در مرحله دادرسی و صدور حکم و در مرحله اجرای احکام و تأمین ضرور و زیان وی می باشد (شمس ناتری - اسلامی، ۱۳۹۴، ۲۷۶). در مواد ۱۴ و ۱۵ و ۱۷ این قانون اشاره می‌کند

که شاکی می تواند برای جبران تمام ضرر و زیان های مادی و معنوی و منافع ممکن الحصول ناشی از جرم را پس از تعقیب متهم و تا قبل از اعلام ختم دادرسی مطالبه کند و دادگاه مکلف است تا ضمن صدور رای کیفری در خصوص ضرر و زیان وارده به مدعی خصوصی، رای مقتضی صادر نماید (زرخ، ۱۳۹۱: ۲۴). در مواد ۷۰ و ۷۱ این قانون که حمایت از بزه دیده محجور می باشد که در صورت دسترس ییا عدم دسترسی به متهم امکان یا شرایط طرح شکایت و پیگیری آن را ندارند، برای تعقیب کیفری متهم مقرر نموده است و این امر بجز موارد مذکور در مواد ۲۰۱، ۳۶۷ و ۳۶۸ تاکید شده است و همچنین در ماده ۸۱ در زمان صدور دستور تعلیق تعقیب متهم در بند الف مقنن حفظ حقوق بزه دیده را مورد توجه داشته است و اعلام نموده که متهم بایستی در ارائه خدمات به بزه دیده در جهت رفع یا کاهش آثار زیانبار مادی یا معنوی ناشی از جرم یا رضایت وی اقدام نماید (زوارجلالی، ۱۳۹۴، ۸۲-۷۹).

جهت تضمین حقوق بزه دیده برای جبران ضرر و زیان، بازپرس پس از تفهیم اتهام مطابق ماده ۲۱۷ و ۲۴۷ آ.د.ک، یکی از قرارهای تامین یا نظارت قضایی مصرح در آن را برای متهم صادر می نماید. بازپرس و دادستان پس از ختم تحقیقات، چنانچه بزه دیده بر قرارهای نهایی صادره، مثل منع تعقیب یا موقوفی تعقیب و محکوم باشد، می تواند مطابق ماده ۲۷۰ به دادگاه اعتراض کند تا چنانچه حقوق وی در این مرحله تضییع گردید، مورد رسیدگی قرار گیرد و مطابق تبصره ماده ۳۴۷ قانون مذکور هرگاه حضور و دفاع وکیل را برای شخص بزه دیده فاقد تمکن مالی را ضروری بدانند، برای وی وکیل با هزینه قوه قضائیه انتخاب می کند (قربان نیا - نمانیان، ۱۳۹۴، صص ۱۰۴-۱۰۲).

بزه دیدگان مورد حمایت در لایحه مبارزه با تروریسم، تأسیسات مورد استفاده عمومی دولتی و غیردولتی هستند که در اثر تخریب اشخاص تروریست، منجر به تخریب یا اختلال در کارکرد آنها می شود (بند دو لایحه مبارزه با تروریسم). از آن جایی که با پیشرفت تکنولوژی، تأسیسات عمومی کشور به شدت به فناوری اطلاعات وابسته شده است، بر اساس مقرره فوق هر گونه عملی که منجر به تخریب تأسیسات عمومی شود، عمل تروریستی محسوب می شود. اگر چه در این لایحه از بزه دیدگان تروریسم سایبری، عنوانی به میان نیامده؛ اما همانند دیگر مقررات اشاره شده در این بخش، از مفاد عام این لایحه می توان به حمایت کیفری از برخی بزه دیدگان بزه مذکور اشاره نمود.

۲-۱-۲. حمایت کیفری ویژه یا افتراقی

حمایت کیفری ویژه، یعنی جرم‌انگاری بزه با توجه به ویژگی‌های خاص یک بزه‌دیده، مانند اشخاص کهن سال، زنان و کودکان که به سبب وضعیت خاص آن‌ها باید بیشتر مورد حمایت قرار گیرند (رایجیان اصلی، ۱۳۹۰، الف، ص ۸۴). حمایت کیفری تشدید، از آورده‌های بزه‌دیده شناسی حمایتی است که با تشخیص بزه‌دیدگان دارای شرایط خاص، به حمایت ویژه از آنان می‌پردازد.

در زمینه حمایت‌های کیفری افتراقی از بزه‌دیدگان تروریسم سایبری، می‌توان به مواد مختلفی از قانون جرائم رایانه‌ای اشاره نمود که به واسطه موضوع جرم، به تشدید مجازات مرتکب پرداخته است. از جمله حمایت کیفری ویژه در این قانون، "حمایت ویژه از داده‌های سرّی است که در سیستم‌های رایانه‌ای و مخابراتی یا حامل‌های داده در حال انتقال یا ذخیره هستند" (ماده سه قانون جرایم رایانه‌ای، مصوب ۱۳۸۸). تروریست‌های سایبری، به منظور طرح ریزی و انجام عملیات‌های خود نیاز به اطلاعاتی دارند که بتوانند هدف را به خوبی شناسایی نموده و به نقاط ضعف سیستم‌های رایانه‌ای و مخابراتی پی ببرند؛ لذا جاسوسی رایانه‌ای رکن اصلی، برای تحقق این بزه به شمار می‌آید. در این ماده نیز به سبب سرّی بودن داده‌ها، حمایت کیفری ویژه‌ای برای آن‌ها در نظر گرفته شده است. قانون‌گذار نیز در این راستا، این مسئله را مورد توجه قرار داده است و به جرم‌انگاری این عمل غیر قانونی اقدام نموده است. یکی از ایراداتی که در خصوص ماده سه وارد است این است که به زیرساخت‌های اطلاعاتی کشور اشاره‌ای ننموده و فقط به سرّی بودن داده‌ها اشاره گردیده که جا داشت در ماده ۱۱ یا ماده ۲۶، به منظور تشدید مجازات مرتکب به زیرساخت‌های اطلاعاتی کشور اشاره می‌شد (کدخدایی - ساعد، ۱۳۹۰: ۳۸).

علاوه بر بیان حمایت‌های کیفری تشدید در قانون جرایم رایانه‌ای، می‌توان به قانون تجارت الکترونیکی مصوب ۱۳۸۲ اشاره نمود که به حمایت کیفری ویژه از داده پیام‌های شخصی پرداخته است. این جرایم علیه داده‌ها توسط نهادهای مسئول و دفاتر خدمات صدور گواهی الکترونیکی ارتکاب می‌یابد که در این صورت برای مرتکب، حداکثر کیفر تعیین شده در ماده ۷۱ را مقرر کرده است. با توجه به حساس بودن داده‌های شخصی به خصوص در حوزه مالی، قانون‌گذار اشخاصی را که با داده‌های مذکور درگیر هستند، مورد توجه ویژه قرار داده و بدین وسیله بزهکاران بالقوه را نیز از ارتکاب چنین اعمالی باز داشته است (جاویدنیا، ۱۳۸۶، ص ۱۲۹).

۲-۲. حمایت مدنی از بزه دیدگان تروریسم سایبری

دسته‌ای دیگر از حمایت‌ها سازوکارهایی هستند که دارای ماهیت کیفری نیستند و بیشتر شامل جبران خسارت از بزه‌دیدگان جرایم می‌شود. با توجه به این که در قوانین کیفری ایران، جرم‌انگاری صریحی از تروریسم سایبری صورت نگرفته و حتی به منظور پشتیبانی از بزه‌دیدگان جرایم رایانه‌ای، اقدامات شایسته‌ای اتخاذ نشده است، حمایت‌های غیر کیفری نیز به صراحت، چنین بزه‌دیدگانی را مورد توجه قرار نداده‌اند. لذا منظور از حمایت مدنی از بزه‌دیدگان تروریسم سایبری، سازوکارهایی هستند که به طور غیرمستقیم و عام به حمایت‌های غیر کیفری از بزه‌دیدگان مذکور می‌پردازند. بنابراین حمایت‌های مدنی، بیشتر شامل جبران خسارت مادی است. جبران خسارت مادی، شامل هرگونه اقدام به منظور جبران و ترمیم آسیب‌های وارده به دارایی‌های بزه‌دیده است که به وسیلهٔ پرداخت پول و هزینه‌های ایجاد شده در طی بزه‌دیدگی فرد یا پرداخت غرامت به 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 (Gonzalez, 2013: 97). 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 وارد بر بزه‌دیدگان، به خسارت‌های اقتصادی اختصاص دارد (Cherif, 2015: 145). 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 سخت افزار یا نرم افزار آسیب دیده، هزینه‌های ایمن سازی 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 نمود (ساعد، ۱۳۸۹، ۶۷).

با بررسی هزینه های تحمیل شده بر بزه‌دیدگان مذکور، لزوم جبران نمودن آنها توسط بزهکاران و در صورت غیرقابل جبران ماندن، باید توسط دولت جبران گردد. بسیاری از خسارت‌های ایراد شده با جبران مادی قابل ترمیم هستند اگر چه 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 که به صورت 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 نمود. 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 نمود که به صورت کلی و قواعد عام در این قانون، به جبران نمودن خسارت‌های وارده بر کلیه بزه‌دیدگان اشاره نموده است. بنابراین اعمالی که توسط تروریست‌های سایبری، علیه داده‌ها، سخت افزار، نرم افزار، تمامیت جسمانی یا روانی اشخاص ارتکاب می‌یابد، به استناد قاعده عام ماده یک قانون مسئولیت مدنی، بزهکاران مسئول عمل خود و مکلف به پرداخت غرامت یا جریمه خسارت‌های مذکور هستند. علاوه بر قانون مسئولیت مدنی، ماده ۳۲۸ قانون مدنی، به شکل عام، تلف اموال دیگران را ممنوع و موجب مسئولیت دانسته است (عالی پور، ۱۳۹۰، ۲۳۷). مقررات اشاره شده 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 به طور اختصاصی به جبران خسارت در رابطه با جرایم رایانه‌ای پرداخته است، قانون تجارت الکترونیکی مصوب ۱۳۸۲ است که در مورد جبران خسارت به عین به صراحت در ماده ۷۸ بدان اشاره کرده است. در قسمت پایانی ماده 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 مقرر از قانون تجارت الکترونیکی، تنها مقرره‌ای است که به صراحت، اشاره به جبران خسارتی نموده که مرتبط با سیستم‌های رایانه‌ای و مخابراتی هستند. بند ۳ تبصره ۱۸ لایحه بودجه 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 خصمانه 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 مقررۀ مذکور دارای ایراداتی به خصوص در اقامۀ دعوی و چگونگی جبران است، اما گامی مهمی در جهت انواع حمایت از بزه دیدگان تروریسم و به طبع تروریسم سایبری که زیر شاخۀ تروریسم سنتی است، محسوب می شود (پورنقدی - بختیاری، ۱۳۹۲، ۳۵-۳۳).

همچنین تدوین «لایحۀ جبران دولتی خسارت از بزه دیدگان» که توسط قوه قضاییه تدوین شده است، نمونه ای دیگر از تلاش های دولت در جهت تحقق اهداف بزه دیده شناسی و کمک به بزه دیدگان است که در این لایحه، صندوق جبران خسارت برای بزه دیدگان پیش بینی شده است. لایحۀ مذکور، زبان های ناشی از جرایم را که قابل حمایت هستند احصاء نموده و چهار دسته از جرایم را مد نظر قرار داده که به بیان آن دسته از مواردی پرداخته می شود که با بزه مذکور و بزه دیدگان آن قابل تطبیق باشد. دسته اول، شامل "جرایم عمدی یا غیر عمدی است که منتهی به قتل گردد" (ماده سه لایحۀ جبران دولتی خسارت از بزه دیدگان، ۱۳۸۷). با تطبیق مفاد این مقررۀ با تبعات تروریسم سایبری، می توان مواردی که در اثر فعل یک نفوذگر، قطار مترو از ریل خارج گردد 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 خسارات مالی بزه دیدگان حقیقی تروریسم سایبری اشاره نمود (صارمی، ۱۳۹۲، ۵۸-۵۷).

پیش بین سازوکار جبران آثار ناشی از بزه دیدگی یکی از مهم ترین مولفه های حقوق کیفری در راستای حمایت از بزه دیدگان تروریسم سایبری می باشد. برخلاف مولفه های حمایتی پیشین، آثار ساز و کار جبران بطور مستقیم بر بزه دیدگان مذکور تبلور می یابد و هرچه گسترده تر باشد از گسترش آسیب وارده در اثر ارتکاب جرم علیه بزه دیدگان جلوگیری می کند. لذا در کنار جبران خسارت های مادی حمایت های معنوی هم نسبت به بزه دیدگان تروریسم سایبری باید مورد توجه قرار بگیرد. مشخص است هرچرمی علاوه بر خسارت های مادی، آزرده گی خاطر بزه دیده را نیز به همراه دارد. این آزرده گی خاطر که از آسیب به عواطف و احساسات فرد یا حیثیت شخص برمی خیزد و در جرم های مختلف بازتاب های گوناگون دارد، درد و رنج عاطفی و حیثیتی نامیده می شود (Cox, 2016: 427).

جبران درد و رنج های عاطفی به دلیل برآوردناپذیری مالی از جبران خسارت مادی جداست. حمایت عاطفی کمک های روانشناسانه ای است که برای ترمیم درد و رنج های عاطفی بزه دیدگان انجام می شود و پیش از هر چیز نقش روانکاو و روانشناسان در آن برجسته است. حمایت عاطفی از بزه دیدگان را می توان از گذر

مراکز خصوصی روان درمانی بهره مند از روانشناسان متخصص تضمین کرد. از نظر سیاست جنایی، مقنن قانون جرایم رایانه ای به جبران خسارت معنوی توجه چندانی نداشته است به نحوی که در برخی موارد به صرف جرم انگاری اعمالی که علیه حیثیت افراد است، امتفا شده است (مواد ۱۸-۱۶) و به جبران ضرر و زیان معنوی ناشی از بزه دیدگی جرایم مذکور توجه خاصی نشده است و صرفاً در ماده ۱۸، آن‌هم بصورت مردد بر جبران خسارت معنوی نظر شده است (تقی زاد - زمردی، ۱۳۹۵ : ۷۷).

نکته ای که در راستای سیاست جنایی ایران در قبال حمایت از بزه دیدگان بطور کلی می توان اشاره کرد "دستورالعمل و ضوابط اجرایی حمایت از بزه دیدگان" است که توسط وزارت دادگستری در مورخ ۱۳۸۸/۴/۲۱ به تصویب رسیده است که نقطه عطف مثبتی در راستای حمایت مادی و معنوی از تمام اقشار بزه دیده است. ولی نکته قابل تامل در این دستورالعمل، این است که اجرای آن بصورت آزمایشی تا پایان سال ۱۳۸۸ بوده و پس از پایان مدت اجرای آزمایشی و برای سال های بعد منوط به تامین بودجه شده است که بنظر می رسد اصل وجود چنین مقرراتی ضروری بوده ولی نه به شکل فعلی که قابل اجرا نباشد بلکه لوازم اجرای چنین مقرراتی فراهم شود که انتظار می رود در راستای اجرای بهتر، سطح قانونی آن از " دستورالعمل " به " قانون " ارتقا یابد.

همچنین مصوبه ای تحت عنوان "بسته اجرایی وزارت دادگستری" موضوع ماده ۲۱۷ قانون برنامه پنج ساله پنجم توسعه جمهوری اسلامی ایران، منتشر شد که بر اساس آن یکی از راهبردهای اساسی بسته فوق اجرای تکالیف بیت المال در پرداخت دیه و سائر حقوق آسیب دیده های از جرائم، معرفی شده است و در راستای آن سیاست های اجرایی متناظر با راهبرد فوق ایجاد سازو کار لازم برای پرداخت دیه و اجرای آرای محاکم قضایی و ایجاد سازوکارهای لازم برای حمایت از بزه دیدگان شناخته شده است که وجود و اجرای چنین مقرراتی نقطه عطف مثبت در راستای حمایت مادی و معنوی از بزه دیدگان جرائم می توان تلقی نمود (پورقهرمانی، ۱۳۹۶ : ۱۳).

۲-۳. شیوه جبران خسارت از بزه دیدگان تروریسم سایبری در حقوق کیفری ایران

در قانون جرایم رایان های کشورمان راجع به حمایت بزه دیدگان سایبری از حیث جبران خسارت وارده و شیوه های آن موضوعی پیش بینی نشده است اما با توجه به اطلاق ماده ۱۴ قانون آیین دادرسی کیفری که

مقرر داشته شاک می‌تواند در صورت وقوع خسارت جبران ضرر و زیان نهایی مادی و معنوی و منافع ممکن الحصول ناشی از جرم را مطالبه نماید و در صورت وقوع زیان معنوی که شامل صدمات روحی، هتک حیثیت، اعتبار شخصی، خانوادگی و اجتماعی هست، دادگاه علاوه بر صدور حکم به جبران خسارت مالی می‌تواند متهم را از طریق الزام به عذرخواهی و درج حکم در جراید و امثال آن محکوم نماید. از ایرادات وارده به قانون فعلی جرایم رایانه ای آن است که با توجه به تأثیرات و اهمیت فزاینده فضای مجازی در زندگی روزمره اشخاص در دنیا لازم بود تا مقنن کشورمان به منظور استیفای حقوق حقه شاک و پیشگیری و مقابله با جرایم ارتكابی در فضای مجازی، مصادیق و شیوه های جبران خسارت وارده را به خوبی مشخص و تبیین نماید.

یکی از نکات مهم دیگر در جبران خسارت از بزه دیدگان فضای مجازی که می‌بایست در قانون جرایم رایانه ای توسط مقنن کشورمان مورد توجه قرار گیرد موضوع حمایت دولت از اتباع بزه دیده خویش در صورت عدم شناسایی متهمین

می باشد که جبران خسارت وارده به بزه دیدگان از طریق شیوه هایی چون تأدیه خسارت به آن ها از منابع مالی قانونی جایگزین پیش بینی شده در قانون باشد به عنوان مثال : در قوانین داخلی کشورمان صندوق تأمین خسارت های بدنی در تصادفات در صورت عدم شناسایی متهمین پیش بینی شده است و یا در ماده ۴۳۵ قانون مجازات اسلامی راجع به پرداخت دیه از بیت المال به اشخاصی که مورد قتل و ضرب و جرح عمدی واقع می شوند و قاتل و ضارب آنها مشخص نیست به حمایت از این دسته از بزه دیدگان پرداخته است که شایسته است تا در این مورد هم چاره اندیشی مناسبی اتخاذ گردد (اسلامی، ۱۳۹۵، ۱۷۹).

با توجه به فنی و نوظهور بودن جرم مذکور در فضای سایبری شایسته است تا در خصوص این بزه هم مانند سایر جرایم که مقنن عقیده به رسیدگی تخصصی آن ها به لحاظ محاسن حاصله در محاکم قضایی کشورمان و سایر کشورها دارد، از قضاتی که دارای آگاهی و تخصص لازم در رسیدگی به جرایم سایبری را دارند در شعب تخصصی دادسرا و دادگاه ها استفاده نماید که این امر اولاً مستلزم فراهم آوردن تمهیدات لازم از حیث آموزش به قضات علاقمند به خدمت در این حوزه و ثانیاً اختصاص شعبی از دادسرا یا دادگاه های کیفری یک و دو و نظامی و اطفال بر حسب درجه های مجازات ارتكابی در فضای سایبری رسیدگی نمایند می باشد که متأسفانه در کشورمان علی‌رغم فراهم شدن جنبه تقنینی این موضوع، تاکنون زمینه اجرایی آن فراهم نشده است که این امر یکی از ایرادات و اشکالات مهم به عملکرد دستگاه قضایی کشورمان است و بدیهی است که با

اجرای مقررات ماده ۶۶۶ و تبصره ذیل آن زمینه مناسب و مؤثری در جهت حمایت از بزه دیدگان سایبری فراهم می‌گردد.

۳- مسئولیت کیفری در قانون جرایم رایانه‌ای ایران

مسئولیت اعم از کیفری و مدنی، مستلزم پاسخگویی شخص مسئول است و این پاسخگویی یا به دلیل تقصیر است یا به دلیل وارد کردن زیان، مخاطب پاسخ نیز یا جامعه است یا زیان دیده و هدف از آن هم یا بازدارندگی و تنبیه شخص مسئول است یا به حالت اول برگرداندن وضعیت زیان دیده. البته در نظام‌های حقوقی قدیمی، موارد و هدف‌های فوق‌الذکر از هم تفکیک نشده بود و مجازات فرد مسئول هم هدف بازدارندگی داشت و هم موجب جبران خسارت و همین گذشته مشترک تنها نقطه عطف مفاهیم مسئولیت مدنی و کیفری است (Clarke, 2013: 208). قانون‌گذار ایران در قانون جرایم رایانه‌ای فصل ششم از قانون را به موضوع مسئولیت کیفری اختصاص داده است، شاید بتوان گفت مهم‌ترین تغییری که قانون فوق‌الذکر در رابطه با مسئولیت کیفری ایجاد نموده، شناسایی و ایجاد مسئولیت کیفری برای اشخاص حقوقی است، ماده ۱۹ و ۲۰ قانون فوق‌الذکر در رابطه با مسئولیت کیفری اشخاص حقوقی است.

در این رابطه ممکن است این سؤال مطرح شود که تأکید قانون‌گذار ایران بر بحث مسئولیت کیفری اشخاص حقوقی چه معنایی در پی دارد؟ و آثار آن چیست؟

یکی از مهم‌ترین سؤالاتی که ممکن است در این زمینه مطرح شود در واقع بحث شناخت مسئولیت کیفری برای اشخاص حقوقی و تأثیر آن بر مسئولیت افراد حقیقی است، آیا رویه قانون‌گذار ایران بر این بوده که اصل را بر مسئولیت کیفری اشخاص حقوقی قرار دهد؟ یا به دنبال نفی مسئولیت کیفری اشخاص حقیقی در محیط سایبر بوده است؟ پاسخ مطمئناً منفی است، با توجه به اینکه تبصره دو ماده ۱۹ مقرر می‌دارد: «مسئولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود»، بنابراین اینکه قانون‌گذار ماده نخست از مبحث ششم قانون جرایم رایانه‌ای را به بحث مسئولیت کیفری اختصاص داده، به معنای نفی مسئولیت کیفری اشخاص حقیقی نیست.

مسئله دیگری که باید در این مقوله مورد بررسی قرار بگیرد بحث تناسب مسئولیت‌ها و رابطه مسئولیت کیفری اشخاص حقیقی و حقوقی است، همان‌طور که گفتیم تبصره دو ماده ۱۹ مسئولیت کیفری اشخاص حقوقی را مانعی برای مجازات اشخاص حقیقی ندانسته، اما متن ماده فوق تا اندازه‌ای همراه کننده است، زیرا عملاً صحبتی از ارتباط دو مسئولیت با یکدیگر نشده است، به‌هرحال باید اذعان داشت تا زمانی که کسی مسئولیت نداشته باشد اعمال مجازات بر ایشان امکان‌پذیر نیست، بنابراین متن تبصره ۲ فوق‌الذکر به معنای امکان وجود مسئولیت همزمان برای شخص حقوقی و اشخاص حقیقی عضو آن مجموعه است. بحث ارتباط میان مسئولیت اشخاص حقیقی و مسئولیت اشخاص حقوقی، به اشکال ارتباط میان این دو نوع مسئولیت می‌پردازد، باید توجه داشت که این دو مسئولیت از پیشینه و ریشه‌ی مشترکی برخوردارند، آن‌ها بر اثر نقض جدی تعهداتی که به‌طور کلی در برابر جامعه وجود دارند ایجاد می‌شوند (Andrew, 2010: 24). البته این دو مسئولیت عواقب یکسانی ندارند، به‌هرحال باید گفت که وجود مبنای مشترک به معنای آن نیست که قواعد کلی مسئولیت اشخاص حقیقی در رابطه با مسئولیت اشخاص حقوقی قابلیت کاربرد دارند، در اینجا تنها می‌توانیم به این مسئله اشاره کنیم که یکسان بودن این دو نوع مسئولیت در قواعد اولیه به معنای آن است که هر دو بر اثر نقض هنجارهای اساسی که مورد حمایت جامعه است ایجاد می‌شوند، البته در قواعد ثانویه این ارتباط کمرنگ خواهد شد. در هر حال شناخت اشتراکات و ارتباط میان مسئولیت اشخاص بررسی مبانی مسئولیت در این زمینه است (رضوی فرد - موسوی، ۱۳۹۵، ۴۰).

یکی از نکات مهم دیگر در جبران خسارت از بزه دیدگان فضای مجازی که می‌بایست در قانون جرایم رایانه‌ای توسط مقنن کشورمان مورد توجه قرار بگیرد موضوع حمایت دولت از اتباع بزه دیده خویش در صورت عدم شناسایی متهمین می‌باشد که جبران خسارت وارده به بزه دیدگان از طریق شیوه‌هایی چون تادیه خسارت به آنها از منابع مالی قانونی جایگزین پیش‌بینی شده در قانون باشد به عنوان مثال در قوانین داخلی کشورمان صندوق تامین خسارت‌های بدنی در تصادفات در صورت عدم شناسایی متهمین پیش‌بینی شده است و یا در ماده 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 بزه دیدگان پرداخته است که شایسته است تا در این مورد هم چاره‌اندیشی مناسبی اتخاذ گردد.

۴- بحث و نتیجه گیری

در راستای حمایت از بزه‌دیدگان تروریسم سایبری در حقوق کیفری کشورمان، هیچ گونه مقررۀ خاصی اندیشیده نشده است و حتی برای بزه‌دیدگان سایبری به معنای اخص، حمایت‌های ویژه‌ای تخصیص نیافته است. شاید بتوان با تعیین کیفر برای مرتکبان جرایم سایبری گفت که فقط حمایت‌های کیفری برای بزه‌دیدگان سایبری اتخاذ شده و دیگر نیازهای بزه‌دیدگان، از جمله نیازهای عاطفی یا جبران خسارت‌های متناسب با بزه‌دیدگی آن‌ها بدون جبران باقی مانده است. این نکته روشن است که بزه‌دیدگان سایبری، یکی از بی دفاع‌ترین 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 آنان بدون جبران باقی می‌ماند. در راستای 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 جرایم که در محیط فیزیکی تحقق می‌یابند، استفاده نمود.

مهم‌ترین ابزارهایی که برای مبارزه با جرایم نوین در برابر حقوق جزا وجود دارد. راهکارهایی مانند جرم‌انگاری، ایجاد و توسعه مسئولیت کیفری، استفاده از راهکارهای نوین حل اختلاف و مجازات‌های نوین و... است، در رابطه با مسئولیت کیفری در جرایم سایبری قانون‌گذار ایران اقدام به توسیع و گسترش مسئولیت کیفری در برابر اشخاص حقوقی نموده است. تا قبل از تصویب قانون فوق‌الذکر بحث مسئولیت کیفری اشخاص حقوقی در قوانین کیفری ایران چندان مطرح نشده بود و قانون جرایم رایانه‌ای نخستین بار این موضوع یعنی مسئولیت کیفری اشخاص حقوقی را موردپذیرش قرار داده است، می‌دانیم بسیاری از جرایم رایانه‌ای معمولاً توسط اشخاص حقوقی واقع می‌شوند و این اقدام قانون‌گذار ایران در رابطه با ایجاد مسئولیت کیفری برای این اشخاص امری کاملاً طبیعی بوده و درواقع استفاده از ابزار گسترش مسئولیت کیفری برای مبارزه با جرایم جدید است.

منابع و مأخذ

الف) کتاب ها

- ۱- اردبیلی، محمدعلی (۱۳۸۱)، «مفهوم تروریسم»، گزیده مقالات همایش تروریسم از دیدگاه اسلام و حقوق بین الملل، چاپ اول. تهران: مرکز مطالعات توسعه قضایی و دانشکده علوم قضایی و خدمات اداری.
- ۲- باستانی، برومند (۱۳۹۰)، جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، چاپ سوم. تهران: بهنامی.
- ۳- پوربافرانی، حسن (۱۳۹۶)، حقوق جزای بین الملل، تهران: انتشارات جنگل.
- ۴- تقی زاده انصاری، مصطفی (۱۳۸۸)، سازمان جهانی پلیس جهانی اینترپل، چاپ اول، تهران: خرسندی.
- ۵- جلالی فراهانی، امیرحسین و باقری اصل، رضا (۱۳۸۷)، پیشگیری اجتماعی از جرایم سایبری راهکاری اصلی برای نهادینه سازی اخلاق سایبری، اطلاع رسانی و کتابداری «ره آورد نور»، شماره ۲۴
- ۶- رایجیان اصلی، مهرداد (۱۳۹۰)، الف. بزه‌دیده شناسی حمایتی، چاپ دوم. تهران: دادگستر.
- ۷- زرنشان، شهرام (۱۳۸۶)، شورای امنیت و تعهد دولت ها برای مقابله با تروریسم، مرکز امور حقوقی بین‌المللی معاونت حقوقی و امور مجلس ریاست جمهوری.
- ۸- ساعد، نادر (۱۳۸۹)، منابع حقوق مبارزه با تروریسم در ایران، تهران: خرسندی.
- ۹- صنوبر، ناصر (۱۳۹۳)، اقتصاد تروریسم، تهران: انتشارات بورس.
- ۱۰- عالی پور، حسن (۱۳۹۰)، حقوق کیفری فناوری اطلاعات، چاپ اول. تهران: خرسندی.
- ۱۱- فامیلی زوار جلالی، امیر (۱۳۹۴)، مسئولیت بین المللی دولت‌ها ناشی از تامین مالی دهشت افکنی با تاکید بر گروه دهشت افکن داعش، پایان نامه کارشناسی ارشد حقوق بین الملل، دانشگاه تهران
- ۱۲- کدخدایی، عباسعلی و ساعد، نادر (۱۳۹۰)، تروریسم و مقابله با آن، چاپ اول. تهران: مجمع جهانی صلح جهانی.
- ۱۳- نمایان، پیمان (۱۳۹۰)، واکنش‌های عدالت کیفری به تروریسم، چاپ اول. تهران: میزان.

ب) مقالات

- ۱۴- الهویی نظری حمید (۱۳۹۶)، فامیل زوارجلالی امیر، "مسئولیت بین المللی دولت های تأمین کننده مالی تروریسم"، شماره ۳، دوره چهل و هفتم، تهران: مجله مطالعات حقوق عمومی.
- ۱۵- احمری، حسین، کحلکی، غلام رضا (۱۳۹۵)، تحلیل سازه انگارانه تروریسم سایبری و رویکرد نظام حقوقی به آن، دوره نخست، شماره شانزدهم، فصلنامه پژوهش های روابط بین الملل.
- ۱۶- اسلامی، ابراهیم (۱۳۹۵)، "جایگاه حمایت از بزه دیدگان جرائم سایبری در مقررات کیفری حقوق داخلی و حقوق بین الملل"، سال هفدهم، شماره اول، پژوهشنامه حقوق اسلامی.
- ۱۷- پاکزاد، بتول (۱۳۹۰)، "ماهیت تروریسم سایبری"، شماره ۴، تحقیقات حقوقی.
- ۱۸- پورقهرمانی، بابک (۱۳۹۶)، "مطالعه تطبیقی سازکارهای حمایت از بزه دیدگان جرائم رایانه ای در حقوق کیفری ایران و اسناد بین المللی با تاکید بر کنوانسیون بوداپست"، شماره ۱۵، سال هشتم، پژوهشنامه حقوق کیفری.
- ۱۹- پوربافرانی حسن، امیدی علی، قلی زاده بهروز (۱۳۹۶)، "درآمدی بر یکسان انگاری جرم دزدی دریایی با تروریسم"، شماره نهم، دوره دوم، شیراز: مجله مطالعات حقوقی.
- ۲۰- تقی زاد، مهرداد، زمردی، کیوان (۱۳۹۵)، نقش اتحادیه اروپا در قاعده مندسازی جرائم سایبری، سال ششم، شماره ۲۵، مطالعات بین المللی پلیس.
- ۲۱- رضوی فرد، بهزاد، موسوی، سید نعمت الله (۱۳۹۵)، "مسئولیت کیفری در فضای سایبر در حقوق ایران"، دوره ۵، شماره ۱۶، فصلنامه پژوهش حقوق کیفری.
- ۲۲- جلالی فراهانی، امیرحسین، باقری اصل، رضا (۱۳۸۶)، "پیشگیری اجتماعی از جرائم و انحرافات سایبری"، مجلس و پژوهش، سال ۱۴، شماره ۵۵.
- ۲۳- جلالی فراهانی، امیرحسین (۱۳۸۵)، "تروریسم سایبری"، سال سوم، شماره ۱۰، مجله فقه و حقوق.
- ۲۴- خرم آبادی، عبدالصمد (۱۳۸۶)، "کلاهبرداری رایانه ای از دیدگاه بین الملل و وضعیت ایران"، فصلنامه حقوق مجله دانشکده حقوق و علوم سیاسی، سال ۳۷، شماره ۲.

۲۵- دهشیری، محمدرضا (۱۳۹۵)، " بررسی و تحلیل تروریسم سایبری با رویکرد پیشگیری وضعی "،

لرستان: فصلنامه دانش انتظامی.

۲۶- زررخ، احسان (۱۳۹۱)، " بزه‌دیده شناسی سایبری "، مجلس و پژوهش. سال ۱۷، شماره ۶۴

۲۷- شمس ناتری ابراهیم، اسلامی داود (۱۳۹۴)، " ماهیت کیفری تامین مالی تروریسم "، شماره ۵، ۶،

تهران: مطالعات حقوق کیفری و جرم شناسی.

۲۸- صارمی، احمد (۱۳۹۲)، رسیدگی به جرائم هواپیمائی در نظام کیفری بین المللی و ملی، شماره ۱۴،

مطالعات بین المللی پلیس.

۲۹- طیبی فرد، امیرحسین (۱۳۸۴)، "مبارزه با تأمین مالی تروریسم در اسناد بین‌المللی "، دفتر

خدمات حقوقی بین‌المللی جمهوری اسلامی ایران، شماره ۳۲

۳۰- علیزاده، اکبر، باباپور، مهدی (۱۳۹۲)، تروریسم هسته‌ای و راهکارهای مقابله با آن از منظر حقوق

بین‌الملل، دوره چهارم، شماره ۱۶، مطالعات بین المللی پلیس.

۳۱- قربان نیا، ناصر، نمایان، پیمان (۱۳۹۴)، "جایگاه حمایت از بزه دیدگان تروریسم در نظام حقوق

بین المللی"، جلد ۱۲، شماره ۲، مجله حقوق تطبیقی.

۳۲- کیهانلو، فاطمه، رضادوست، وحید (۱۳۹۳)، "حملات سایبری به مثابه توسل به زور در سیاق منشور

سازمان ملل متحد"، شماره ۶۹، فصلنامه تحقیقات حقوقی.

۳۳- ماه پیشانیان، مهسا (۱۳۹۰)، "فضای سایبر و شیوه های نوین درگیری ایالات متحده آمریکا با

جمهوری اسلامی ایران "، نامه پژوهش فرهنگی، سال ۱۲، شماره ۱۳

۳۴- موسوی، محمدرضا و حیدری، خدیجه (۱۳۹۲)، "تأثیر تهدیدات امنیتی تروریسم سایبری بر

امنیت ملی جمهوری اسلامی ایران و راهکارهای مقابله با آن"، شماره ۱۴، دوره چهارم، مجله مطالعات بین

المللی پلیس

۳۵- نمایان، پیمان (۱۳۹۲)، "مواجهه با تروریسم سایبری در حقوق بین الملل کیفری"، سال بیستم،

شماره ۱، فصلنامه حقوق ارتباطی.

ج) منابع لاتین

Books

36-Andrew Lewis. J. (2010), The Cyber War Has Not Begun, Center for Strategic and International Studies, 1-4. Available at: http://csis.org/files/publication/100311_TheCyberWarHasNotBegun.

37- Clarke. R., V. (2013), Situational Crime Prevention Successful Case Studies, Second Edition, London: Harrow and Heston Pub.

38- Gonzalez , Elise (2013), The nexus between human trafficking and terrorism, orgenaized crime, combating human trafficking by creating a cooperative law enforcement system, student scholarship pub.

Articles

39- Cherrif Bassioni (2015), " International Terrorism " , transnational journal of China.

40-Cox, S.J. (2016), "Confronting Threat Through Unconventional Means: Offensive Information Warfare as a Covert Alterntive to Preemptive War " , Houston Law Review, vol 42, numb (3).



پروہشگاہ علوم انسانی و مطالعات فرہنگی
پرتال جامع علوم انسانی