فهرست مطالب

مقدمه

تحولات و پیشرفت شگرف تکنولوژی و فناوری اطلاعات و ارتباطات، مولد تغییرات عمده‌ای در زیر ساخت‌های مهم و حیاتی کشور بوده و بسیاری از مفاهیم سنتی حقوق کیفری را با چالش مواجه ساخته است. در این میان حملات تروریستی سایبری گونه‌ای نوین از جرائم سایبری هستند که استعداد ایجاد تغییرات بنیادین در ساختارهای امنیتی را در سطوح مختلف ملی و بین المللی دارند. تروریسم سایبری یکی از مهمترین جرائم ارتکابی در بستر فضای سایبر، است.این پدیدهٔ مجرمانه از تلاقی اعمال تروریستی و فضای سایبر پا به عرصهٔ وجود نهاده است و از طریق دسترسی به اطلاعات حفاظت شده صورت می‌پذیرد. درحال حاضریکی از دغدغه‌های نظام قانونگذاری در هر کشوری، جرم انگاری کارآمد و مؤثر این پدیدهٔ مجرمانه است چراکه تروریسم از رویکردهای سنتی خود رنگ باخته و به سوی فناوریهای نوین روی آورده است. تروریسم سایبری، با وجود نو ظهور بودن به مراتب خطرناک تر از تروریسم کلاسیک و سنتی است وتهدیدات آن برای امنیت ملی دولت‌ها و کشورها به خطری بالقوه تبدیل شده است. تروریسم در فضای سایبر طیفی از حملات و تهدیدات غیرقانونی توسط تروریست‌ها علیه رایانه، شبکه‌ها و اطلاعات ذخیره شده برای مرعوب ساختن یا مجبور کردن یک حکومت یا افراد یک کشور جهت پیشبرد اهداف اجتماعی و سیاسی است. حمایتِ دولتی که زمانی یک از مؤلفه‌های اصلی تروریسم بود، ممکن است از این پس برای تروریست‌ها چندان حیاتی نباشد، زیرا فناوری اطلاعات و فضای سایبر با فراهم آوردن ظرفیت‌های جدید و مؤثرتر برای تروریست‌ها و هم چنین آزادی عمل آن‌ها برای انجام حملات سازمان یافته تروریستی در عمل بسیاری از مزایای حمایت دولت‌ها را منسوخ کرده است درعصر حاضر ارتباط میان تروریست‌ها از طریق شبکه‌های بین المللی و تبادل افکار و اعمال مجرمانه در سطح بسیار پیچیده است که از ویژگی‌های این نوع ارتباط عدم توانایی پلیس در کنترل

وشنود این ارتباطات می‌باشد از این رو،پیشگیری کارآمد از آن تنها با مشارکت کشورها و مداخله سازمان‌های بین المللی قابل تصور است.در پژوهش حاضر نگارندگان بر آن شدند تا ضمن بررسی تفاوت بنیادین میان تروریسم کلاسیک و تروریسم سایبری، به این سوال پاسخ دهند که تفاوت‌های موجود میان این دو پدیده نظام‌های حقوقی افتراقی را میطلبند یا صرفًا روش و ابزار و شیوه ارتکاب جرم متفاوت است و درنهایت با روش توصیفی- تحلیلی به شیوهٔ استقرایی- قیاسی ، به اثبات این فرضیه می‌پردازد که، میان دوپدیده تروریسم سایبری و تروریسم کلاسیک تفاوت‌های بنیادین حقوقی به نحوی که متضمن دو نظام حقوقی افتراقی باشند وجود ندارد و تنها شیوه‌های ارتکاب جرم و روش‌های اثباتی آن‌ها متفاوت بوده و نیازمند آن است تا قوانین جامعی در خصوص تروریسم سایبری مدون گردد. نوشتار حاضر بدنبال بازخوانی تروریسم با رویکرد ارتکاب در فضای سایبر و استفاده ازسامانه‌های رایانه‌ای و مخابراتی، به تبیین جایگاه تروریسم سایبری در نظام حقوقی ایران و آئین اثبات دلیل در این گونه از جرائم تروریستی پرداخته و ضمن بررسی چالش‌های اجرائی تروریسم سایبری به ارائه راهکارهای مطلوب حقوقی و کیفری در جهت مقابله با گسترش تروریسم در فضای سایبر و همچنین پیشگیری از این پدیدهٔ مجرمانه در عرصهٔ داخلی و بین المللی، جهت تحقق عدالت کیفری می‌پردازد.

بخش اول: مفاهیم و کلیات تحقیق

۱- ادبیات نظری تحقیق

۱-۱- تروریسم

وقتی سخن از واژه «ترور» و «تروریسم» به میان می‌آید، شامل تمامی اعمال خشونت‌آمیزی می‌شود که معمولاً منافع حیاتی یک کشور را هدف قرار می‌دهد و آنچه در این‌گونه اعمال مجرمانه موضوعیت پیدا می‌کند ایجاد ترس و وحشت است. (قدیم زاده، ۱۳۹۵، ۲۴۹) در ماده یک لایحه مبارزه با تروریسم پیش‌بینی شده است که «ارتکاب یا تهدید به ارتکاب جرائم و اقدامات خشونت آمیز از طریق به وحشت‌افکندن مردم جهت تأثیرگذاری بر خط و مشی، تصمیمات و اقدامات دولت جمهوری اسلامی ایران، سایر کشورها و سازمان‌های بین الدولی، جرم تروریستی محسوب می‌شود.» علاوه بر تعریف مذکور، تعریف ساده‌ای که می‌توان از تروریسم ارائه داد عبارتست از: «ارتکاب اعمال خشونت آمیز یا تهدید به استفاده از خشونت علیه اشخاص یا اموال برای ایجاد رعب و وحشت عمومی.» (حکیمی‌ها، ۱۳۸۴، ۶-۵)

۱-۲- تروریسم سایبری

امروزه از تلاقی اعمال تروریستی و فضای سایبرگونه‌ای نوپا از اعمال تروریستی تحت عنوان تروریسم سایبری پا به عرصه وجود نهاده‌است،که از طریق دسترسی به اطلاعات حفاظت شده صورت می‌پذیرد. (هرمزی، ۱۳۹۷، ۲) ارتباط میان تروریست‌ها از طریق شبکه‌های بین‌المللی و تبادل افکار و اعمال مجرمانه در سطح بسیار پیچیده صورت می‌پذیرد و از ویژگی‌های این نوع ارتباطات

عدم توانایی پلیس در کنترل و شنود آن‌هاست. با توجه به تعاریف مختلفی که معاهدات و حقوقدانان ارائه نموده‌اند می‌توان گفت تروریسم سایبری عبارت است از: «طیفی از حملات و تهدیدات غیرقانونی توسط تروریست‌ها علیه رایانه، شبکه‌ها و اطلاعات ذخیره شده برای مرعوب ساختن یا مجبور کردن یک حکومت یا افراد یک کشور جهت پیشبرد اهداف اجتماعی و سیاسی.» (عاملی، ۱۳۹۰، ۵۳۰؛ چاووشی، ۱۳۸۸، ۵۶)

۳-۱- فضای سایبر

«محیطی است مجازی و غیر ملموس که در فضای شبکه‌های بین‌المللی وجود دارد. در این محیط تمام اطلاعات مربوط به روابط افراد، ملت‌ها، فرهنگ‌ها، کشورها، به صورت ملموس و فیزیکی در یک فضای مجازی و به صورت دیجیتالی وجود داشته و قابل استفاده و در دسترس استفاده کنندگان و کاربران می‌باشد؛ کاربرانی که از طریق کامپیوتر، اجزای آن و شبکه‌های بین‌المللی بهم مرتبط اند.» (هرمزی، ۱۳۹۷، ۹) از محیط سایبر به محیط فناوری اطلاعات یا محیط اطلاعات و ارتباطات نیز یاد شده‌است از این رو به جرم‌های محیط سایبر، جرم‌های علیه فناوری اطلاعات نیز گفته می‌شود. (زندی، ۱۳۸۹، ۴۰)

٤-۱- ادله اثبات دعوی

دلیل هر آنچه است که با رعایت حقوق متهم و بدون الزام دادرس به عناوین خاص مانند اقرار و شهادت و... به کشف حقیقت و اقناع وجدانی دادرس می‌انجامد و اثبات از نظر حقوقی عبارت است از: اقامه دلیل نزد قاضی به طریقی که قانون آن را معین نموده‌است. (عباسی کلیمانی، ۱۳۹۴، ۲۵-۲۴) در نهایت می‌توان گفت ادله اثبات دعوی یعنی آنچه از مقررات نوشته یا عرفی که در مقام اثبات امری از امور در مراجع قضایی بکار رود خواه آن امور از دعاوی باشند خواه نه، مانند شهادت، امارات، قسم، سند و اقرار. چون غالباً این امور برای اثبات دعاوی بکار می‌آیند، آنها را از باب تغلیب ادله اثبات دعوی گفته اند. (جعفری لنگرودی، ۱۳۴۶، ۲۴)

۵-۱- رفتار مجرمانه

عنصر مادی جرم گاه رفتاری است که در وضعی خاص از انسان بروز می‌کند و گاه به ندرت حالتی است که بر او مستولی می‌گردد. رفتار انسان ظهور خارجی اراده او است یعنی نیرویی که در صدد