Ilam University

Comparative Studies on Islamic Countries Law

Print ISSN: 2980-8006 Online ISSN: 2980-8014

Homepage: https://lcs.ilam.ac.ir

Iranian Association of Constitutional Law

Confronting Terrorist Criminals in the Digital Space; A Glance at the Legislative Experience in Islamic Countries

Peyman Namamian[1], Fatemeh Ameri Siahoui[2]

1. Associate Prof. of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran. E-mail: p_namamian1512@yahoo.com

2. Assistant Prof., Dep. of Law and Social Sciences, Payame Noor University, Tehran, Iran.

Article Info

Article type:
Research Article

Article history:
Received 3 Aug 2024
Received in revised form 6 Sep 2024
Accepted 19 Sep 2024
Available online 30 Sep 2024

Keywords:
Digital Space,
Terrorist Crimes,
Terrorist Crimes in the Digital Space,
Islamic Countries' Rights.

ABSTRACT

With the increasing use of information and communication technology in various areas of contemporary life, widespread access to the Internet and the use of social media, individuals and organizations are faced with constant threats and challenges arising from the adverse consequences of terrorist crimes in the digital space. Terrorist crimes in the digital space are today referred to as crimes that are not limited to time, place and region and cause damage. Today, this category of electronic crimes is one of the main challenges for law enforcement. Information technology is faced with a wave of laws that protect the interests of people who use web technology. These laws are derived from common laws and regulations in general crimes. With the growth of digital technologies, the way in which this type of crime is committed in the digital space has expanded in a terrifying and extreme way, and while creating insecurity in this space for users, it has also provided the opportunity for terrorist crimes to be committed. As digital infrastructure becomes more critical and barriers to entry for malicious actors decrease, terrorist crimes in the digital space have become a growing concern. Detecting, responding to, and preventing this crime pose unique challenges for law enforcement and governments, requiring a multifaceted approach. Accordingly, this article seeks to identify this criminal phenomenon within the realm of prevailing policy in the legislative policy of Islamic countries, and to examine the possibility of confronting it in such a situation.

Cite this article: Namamian, Peyman., Ameri Siahoui, Fatemeh. (2024). Confronting Terrorist Criminals in the Digital Space; A Glance at the Legislative Experience in Islamic Countries. *Comparative Studies on Islamic Countries Law*, 2 (3), 19- 28. http//doi.org/ 10.22034/lcs.2024.2037407.1050

DOI: http//doi.org/10.22034/lcs.2024.2037407.1050

Publisher: Ilam University.

Comparative Studies on Islamic Countries Law

Print ISSN: 2980-8006 Online ISSN: 2980-8014

Homepage: https://lcs.ilam.ac.ir

Ilam University

Iranian Association of Constitutional Law

رویارویی با بزهکارهای تروریستی در فضای دیجیتالی؛ نگاهی به تجربه قانون‌گذاری در کشورهای اسلامی

پیمان نمامیان[1] | فاطمه عامری سیاهویی[2]

۱. دانشیار حقوق کیفری و جرم شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران. رایانامه: p_namamian1512@yahoo.com

۲. استادیار گروه حقوق و علوم اجتماعی، دانشگاه پیام نور، تهران، ایران.

اطلاعات مقاله

نوع مقاله:
مقاله پژوهشی

تاریخ دریافت: ۱۴۰۳/۰۵/۱۳
تاریخ بازنگری: ۱۴۰۳/۰۶/۱۶
تاریخ پذیرش: ۱۴۰۳/۰۶/۲۹
تاریخ انتشار: ۱۴۰۳/۰۷/۰۹

کلیدواژه‌ها:
فضای دیجیتالی،
بزهکاری‌های تروریستی،
بزهکاری‌های تروریستی در فضای دیجیتالی،
حقوق کشورهای اسلامی.

چکیده

با افزایش استفاده از فناوری اطلاعات و ارتباطات در عرصه‌های مختلف زندگی معاصر، دسترسی گسترده به اینترنت و استفاده از رسانه‌های اجتماعی، افراد و سازمان‌ها با تهدیدها و چالش‌های دائمی ناشی از پیامدهای ناهنجار بزهکاری‌های تروریستی در فضای دیجیتالی مواجه هستند. بزهکاری‌های تروریستی در فضای دیجیتالی امروزه به‌مثابه بزهکاری‌هایی اطلاق می‌شوند که محدود به زمان، مکان و منطقه نیست و موجب آسیب می‌شود. امروزه این دسته از بزهکاری‌های الکترونیکی یکی از چالش‌های اصلی برای اجرای قانون است. فناوری اطلاعات با موجی از قوانینی مواجه است که از منافع افرادی که از فناوری وب استفاده می‌کنند محافظت می‌کند. این قوانین برگرفته از قوانین و قوانین رایج در بزهکاری‌های عمومی است. با رشد فناوری‌های دیجیتالی، نحوه ارتکاب این نوع از بزهکاری‌ها در فضای دیجیتالی به نحو دهشتناک و افراطی گسترش یافته و ضمن ایجاد ناامنی در این فضا را برای کاربران رغم زده است، موجبات ارتکاب بزهکاری‌های تروریستی را نیز فراهم آورده است. با بحرانی شدن زیرساخت‌های دیجیتال و کاهش موانع ورود برای عوامل مخرب، بزهکاری‌های تروریستی در فضای دیجیتالی به یک نگرانی فزاینده تبدیل شده است. کشف، واکنش و پیشگیری از این جنایت چالش‌های منحصربه‌فردی را برای مجریان قانون و دولت‌ها ایجاد می‌کند که نیازمند رویکردی چندوجهی است. بر این اساس، این مقاله درصدد است تا ضمن شناسایی این پدیده مجرمانه در قلمرو سیاست حاکم در سیاست قانون‌گذاری کشورهای اسلامی، امکان مقابله با آن را در چنین وضعیتی مورد مداقه قرار دهد.

استناد: نمامیان، پیمان؛ عامری سیاهویی، فاطمه (۱۴۰۳). رویارویی با بزهکارهای تروریستی در فضای دیجیتالی؛ نگاهی به تجربه قانون‌گذاری در کشورهای اسلامی. *مطالعات تطبیقی حقوق کشورهای اسلامی*، ۲ (۳)، ۲۸-۱۹.
http//doi.org/10.22034/lcs.2024.2037407.1050

ناشر: دانشگاه ایلام.

مقدمه

در قرن جدید، پیچیدگی محض و تعداد حوادث ارتکابی در فضای دیجیتالی گزارش‌شده، نقص‌های عمده‌ای را در زیرساخت امنیت دیجیتالی سکوها و حتی ساختار امنیت دیجیتالی کشورها ایجاد کرده است. در دنیای پست‌مدرن امروزی با جدیدترین و برترین فناوری‌های اینترنتی موجود در بازار، اگر برقراری ارتباط با دیگران در گوشه دیگر دنیا برای همه آسان و قابل‌دسترس شده باشد، باعث ایجاد بزهکاری‌های دیجیتالی ازجمله بزهکاری تروریستی در فضای دیجیتالی نیز شده است که نه‌تنها تهدیدهای جدی برای کل جهان ایجاد کرده است، بلکه این سؤال را نیز مطرح کرده است که «آیا تروریست‌های دیجیتالی با دستکاری فضای دیجیتالی می‌توانند به زیرساخت فیزیکی هدف خود آسیب بزنند یا از بین ببرند؟» به دلیل سهولت دسترسی به همه و آسیب‌های شدید واردشده در مقایسه با بزهکاری تروریستی سنتی، امروزه تروریست‌ها به بزهکاری‌های تروریستی در فضای دیجیتالی نیز متکی هستند.

بازیگران تروریستی که در درگیری‌های مسلحانه فعالیت می‌کنند، رسانه‌های اجتماعی را با استفاده از این پلتفرم‌ها برای تهدید و انتشار تصاویر وحشیانه به‌منظور طعن، وحشت و ارعاب غیرنظامیان به سلاح تبدیل کرده‌اند. این اعمال یا تهدید به خشونت، ترور است، جنایت جنگی ممنوع که در آن اعمال یا تهدید به خشونت با هدف اصلی گسترش وحشت در میان مردم غیرنظامی صورت می‌گیرد. اسلحه‌سازی محتوای ترور از طریق رسانه‌های اجتماعی یک جنایت تروریستی دیجیتال است.

بزهکاری‌های تروریستی دیجیتالی شامل استفاده از اینترنت و سایر اشکال فناوری اطلاعات و ارتباطات برای تهدید یا ایجاد آسیب بدنی برای به دست آوردن قدرت سیاسی یا عقیدتی از طریق تهدید یا ارعاب است. سرقت داده‌ها، دستکاری داده‌ها و اختلال در خدمات ضروری، همه انواع این نوع از بزهکاری‌های تروریستی دیجیتالی هستند. بزهکاری‌های تروریستی در فضای دیجیتالی، جنایتی است که به خاطر خطراتش شناخته می‌شود و تأثیرات آن بر جامعه و زندگی مردم در طول تاریخ ظاهر شده است، زیرا جان میلیون‌ها انسان بی‌گناه را گرفت، جوامع را ویران کرد و این جنایت مرزی نمی‌شناسد. در عرصه‌های مختلف دنیا مرتکبین بزهکاری‌های مختلف از فناوری روز ابزارهای جدیدی برای ارتکاب بزهکاری‌های خود گرفته‌اند، به‌طوری‌که بسیاری از بزهکاری‌ها از طریق اینترنت یا وسایل الکترونیکی مرتکب می‌شوند؛ آنچه بزهکاری‌های تروریستی در فضای دیجیتالی نامیده می‌شود، ظهور کرده است.

یک بزهکاری تروریستی به معنای سنتی، اما عمدتاً از طریق ابزارهای فناورانه انجام می‌شود، جایی که مرتکب این جرم از اینترنت و ابزارهای فناوری مدرن برای ارتکاب جرم خود یا مشارکت یا تحریک آن، خواه به‌عنوان ابزار جرم یا ابزاری که ارتکاب جرم را تسهیل می‌کند، پنهان‌سازی آن را تسهیل می‌کند یا عناصر ارتباطی و برنامه‌ریزی بین مرتکبین و سایر احتمالات را برآورده می‌کند و از طریق ابزارهای ارتباطی الکترونیکی به بزهکاری‌های تروریستی در فضای دیجیتالی کمک می‌کند و به آن دامن می‌زند به دلیل سهولت استفاده از این سلاح، علی‌رغم آسیب و تأثیرگذاری فراوان، از فناوری‌های مدرن برای اجرای بزهکاری‌های تروریستی خود استفاده کنند (Roy, ۲۰۲۲: ۹۵).

رسانه اجتماعی موجود در فضای مجازی ویژگی‌های مفیدی برای انتشار محتوا، دسترسی آزاد به کاربران، توانایی بازآفرینی و انتقال فوری اطلاعات دارد، اما همین مزیت‌ها موجب شده است تا این‌گونه رسانه‌ها ابزار سودمندی برای تروریست‌ها باشند (Weimann, ۲۰۱۴: ۱).

به هر روی، مسئله این مقاله با محوریت پیدایش نوع جدیدی از بزهکاری‌های تروریستی به‌عنوان به بزهکاری‌های تروریستی در فضای دیجیتالی است که از طریق بهره‌گیری از اینترنت و کاربردهای گوناگون آن صورت

می‌پذیرد، مورد مطالعه قرار می‌گیرد. ازاین‌رو این مقاله با استفاده روش تحلیلی توصیفی در پاسخ به این پرسش که «آیا قلمرو قانون‌گذاری کشورهای اسلامی امکان پاسخ به بزهکاری‌های تروریستی در فضای دیجیتالی را دارد؟» تقریر یافته است.

۱. مفاهیم و تعاریف در بوته تحولات

استفاده روزافزون از فناوری‌های دیجیتال مخاطره‌هایی را برای سیستم‌های حیاتی به دلیل بهره‌برداری توسط تروریست‌ها ایجاد می‌کند. امنیت فضای دیجیتال مستلزم اقدامات پیشگیرانه و واکنشی است که برای محافظت از نرم‌افزار و دستگاه‌های الکترونیکی در قبال هرگونه تهدید طراحی شده است. بااین‌حال، افزایش موارد تهدیدهای دیجیتالی توسط تروریست‌ها صورت می‌پذیرد که ایدئولوژی‌ها یا نارضایتی‌های خاصی دارند (Shaweorcid, McAndrew, ۲۰۲۳: ۵۵۲).

یکی از محققان ارشد «بری کالین»، در مؤسسه امنیت و اطلاعات در کالیفرنیا، برای اولین مرتبه طی دهه ۱۹۸۰ اصطلاح «تروریسم سایبری» و یا به تعبیری «بزهکاری تروریستی در فضای دیجیتالی» را ابداع کرد. وی از این اصطلاح به‌عنوان پیوند فضای دیجیتالی و جرم تروریستی یاد کرد و اظهار داشت: «بزهکاری تروریستی در فضای دیجیتالی حمله از پیش برنامه‌ریزی شده و با انگیزه سیاسی علیه اطلاعات، سیستم‌های رایانه‌ای، برنامه‌های رایانه‌ای و داده‌هایی است که منجر به خشونت علیه اهداف غیرنظامی توسط گروه‌های زیر ملی یا عوامل مخفی می‌شود» (Pollitt, ۱۹۹۷: ۲۸۵). در ضمن، حملات با انگیزه سیاسی که باعث آسیب جدی می‌شوند، مانند مشکلات شدید اقتصادی یا از دست دادن مداوم برق یا آب، ممکن است به‌عنوان بزهکاری تروریستی در فضای دیجیتالی نیز شناخته شوند (Syihabudin, ۲۰۲۲: ۱۰۸).[۱]

بر این اساس، اصطلاح «تروریسم دیجیتالی» از دو کلمه تشکیل شده است، یک کلمه به معنای اینترنت و کلمه دیگر به معنای تروریسم که از نظر اهداف با تروریسم به معنای سنتی آن تفاوتی ندارد، بلکه از طریق ابزار مورداستفاده متفاوت است. اجرای پروژه بزهکاری‌های تروریستی در فضای دیجیتالی منوط به استفاده از توانمندی‌های علمی و فنی و بهره‌برداری از وسایل ارتباطی و شبکه‌ها، اطلاعات به‌منظور ارعاب و ارعاب دیگران، آسیب رساندن به آن‌ها و تهدید آن‌ها است. استفاده از فناوری مدرن برای ارعاب دیگران و حمله به سیستم‌های اطلاعاتی درزمینهٔ انگیزه‌های سیاسی، مذهبی یا قومی.

به‌طورکلی، جرائم تروریستی دیجیتالی به‌مثابه رفتارهایی برای هک، انسداد و آلودگی رایانه به‌منظور محدودیت افراد دارای مجوز قانونی برای دسترسی به منابع رایانه‌ای و کسب و تحصیل غیرمجاز به هرگونه اطلاعاتی است که به‌منظور امنیت کشور، اطلاعات محدود شده یا روابط خارجی است (Raj & Yadav, ۲۰۲۲: ۱۳۷– ۱۳۸).

بزهکاری‌های تروریستی در فضای دیجیتالی را می‌توان این‌گونه تعریف کرد: فعالیت یا حمله عمدی با انگیزه‌های سیاسی که به دنبال تأثیرگذاری بر تصمیمات دولتی و افکار عمومی جهانی است و از فضا،

۱- تاکنون هیچ تعریف واحدی از بزهکاری‌های تروریستی در فضای دیجیتالی وجود ندارد که مورد پذیرش همگان باشد. تعاریفی وجود دارد که بر مقاصد بزهکاران تروریستی در فضای دیجیتالی تمرکز دارد و برخی دیگر بر روی دستکاری فناوری اطلاعات توسط آن‌ها تمرکز دارد. همچنین تعداد کمی از کارشناسان امنیتی وجود دارند که آن را برحسب اثر یکپارچه هر حمله تعریف می‌کنند، در حالی که یک نتیجه مخرب و مخرب، مقدار زیادی ترس می‌تواند مشابه یک حمله تروریستی سنتی ایجاد شود. تحت چنین حملاتی، که می‌تواند منجر به جراحت، سقوط هواپیمای مرگ، قطع برق طولانی مدت، از دست دادن عمده اقتصاد یا آلودگی آب شود، به‌عنوان بزهکاری‌های تروریستی در فضای دیجیتالی تعریف می‌شود.

همان‌طور که می‌خواهد، در فرآیند انجام جرم تروریستی و به‌عنوان یک ابزار الکترونیکی کمکی استفاده می‌کند. رسانه به‌عنوان عاملی برای ایجاد تأثیر اخلاقی و روانی از طریق تحریک به نفرت پراکنی این اثر به‌صورت دیجیتالی از طریق استفاده از سازوکارهای جدید سلاح‌های الکترونیکی در نبردهایی است که در فضای مجازی رخ می‌دهد؛ بنابراین، دو راه برای توضیح کلی بزهکاری‌های تروریستی در فضای دیجیتالی وجود دارد که بدین شرح است؛ نخست، مبتنی بر اثرات؛ این نوع بزهکاری تروریستی در فضای دیجیتالی مادامی محقق می‌شود که نتیجه حملات رایانه‌ای در مقایسه با بزهکاری تروریستی سنتی مخرب باشد و ترس شدید ایجاد کند. دوم، مبتنی بر هدف؛ این نوع بزهکاری تروریستی در فضای دیجیتالی زمانی صورت می‌پذیرد که حملات با انگیزه سیاسی یا غیرقانونی برای وادار کردن دولت موجود برای دستیابی به یک هدف سیاسی یا ایجاد آسیب بزرگ به زیرساخت‌های اقتصادی ارتکاب یابد (Jian & Sanjay, ۲۰۱۲: ۱۰۸).

دولت‌ها مدت‌هاست که نگران استفاده تروریست‌ها از اینترنت برای انجام جرائم تروریستی دیجیتال، گسترش تبلیغات، استخدام و افراط‌گرایی افراد و جمع‌آوری سرمایه هستند. حقوق بین‌الملل برای حمایت از پاسخ به جرائم تروریستی دیجیتال موقعیت مناسبی ندارد، اما فقدان چنین حملاتی تا به امروز انگیزه دولت‌ها را برای توسعه حقوق بین‌المللی در برابر این تهدید تضعیف می‌کند. در مورد استفاده تروریست‌ها از اینترنت و رسانه‌های اجتماعی برای تبلیغات، رادیکال سازی، جذب نیرو و جمع‌آوری کمک مالی، بحران ناشی از فعالیت‌های برخط، اجماع کافی برای حمایت از نقش برجسته حقوق بین‌المللی در قبال جرائم تروریستی دیجیتال ایجاد نکرده است (Fidler, ۲۰۱۶: ۴۷۵).

به‌هرروی، بزهکاری‌های جنگی تروریستی در مورد بزهکاری‌های تروریستی در فضای دیجیتالی که از طریق پلتفرم‌های رسانه‌های اجتماعی انجام می‌شوند، اجرا می‌شود[۱]؛ این بزهکاری‌های تروریستی در فضای دیجیتالی را در چارچوب رویه قضایی موجود در مورد ترور در محاکم کیفری بین‌المللی موقت و مختلط قرار می‌دهد. بزهکاری‌های تروریستی در قلمرو حقوق بین‌المللی کیفری به‌مثابه بزهکاری‌های جنگی مستقل به شمار می‌آید، اما کلیه محکومیت‌های قبلی برای بزهکاری تروریستی در چارچوب یک رفتار جنایی اساسی رخ داده است. ازاین‌رو، بزهکاری‌های تروریستی در فضای دیجیتالی متفاوت است؛ یعنی، رفتار اساسی بهره‌گیری از رسانه‌های اجتماعی، لزوماً جرم جنگی خارج از جرم تروریستی به شمار نمی‌آید (Corliss, ۲۰۲۳: ۹۸).

بر این اساس می‌توان اذعان داشت با توجه به فقدان اصلاحیه‌ای در اساسنامه رُم که امکان تعقیب بزهکاری‌های جنگی تروریستی در دیوان کیفری بین‌المللی را فراهم می‌کند، هرگونه تعقیب بعدی برای بزهکاری‌های تروریستی در فضای دیجیتالی از سوی این نهادهای بین‌المللی و محاکم کیفری سرزمینی صورت خواهد پذیرفت (Taylor, Fritsch, Liederbach, ۲۰۱۹: ۲۷۱- ۲۷۴).

۱- مادامی که بزهکاری‌های تروریستی در فضای دیجیتالی در چارچوب مخاصمات مسلحانه ارتکاب یابد، بزهکاری‌های جنگی تروریستی را تشکیل می‌دهد. استفاده از بزهکاری‌های تروریستی در فضای دیجیتالی متناسب با تعریف مشخص شده از این رفتارها جرم یا تهدید است که هدف اصلی آن گسترش وحشت در بین غیرنظامیان است. در بسیاری از موارد، غیرنظامیان مورد هدف مستقیم ارتکاب بزهکاری‌های تروریستی هستند. غیرنظامیان به‌عنوان اهداف حمله، به‌طور مستقیم توسط اعضای بازیگران تروریستی غیردولتی مورد خشونت قرار می‌گیرند که این دسته از رفتارهای ارتکابی خشونت‌آمیز در فیلم‌ها یا عکس‌ها ثبت و در فضای مجازی انتشار می‌یابند. در چنین مواردی، غیرنظامیان، بزه‌دیدگان مستقیم خشونت هستند، عملی که ممکن است مستقلاً به‌مثابه یک جرم تروریستی اطلاق گردد (Corliss, ۲۰۲۳: ۹۹).

۲. قلمرو قانون‌گذاری کشورهای اسلامی؛ از رویکردها تا سیاست‌گذاری‌ها

با توجه به پیچیدگی روزافزون تهدیدهای دیجیتالی و امکان ارتکاب بزه‌کاری‌های تروریستی در چنین فضا و قلمرویی اتخاذ سیاست‌گذاری و تقریر مقررهایی برای پاسخ متناسب با آن ضمن حفاظت از اطلاعات، امکان مقابله همه‌جانبه و اثربخش را میسر خواهد کرد. ازاین‌رو، در پاسخ به این تهدیدها و چالش‌ها، دولت و سازمان‌های مجری قانون در کشورهای مختلف جهان به‌ویژه کشورهای اسلامی مقرراتی را برای مقابله با بزهکاری‌های تروریستی در فضای دیجیتالی وضع کرده‌اند که وفق این امر می‌توان اذعان داشت شناسایی قلمرو سیاست قانون‌گذاری کشورهای اسلامی و تبیین و سنجش موازین قانونی آن‌ها امکان رفع شکاف‌های موجود و دسترسی به مطلوب را فراهم خواهد ساخت.

به‌هرروی، با توجه به تهدیدهای مختلف مربوط به جرائم دیجیتالی به دلیل رشد سریع فناوری اطلاعات، مالزی در وضع قوانین و مقررات در حوزه دیجیتالی برای حفاظت و حفاظت از حاکمیت و هماهنگی کشور مستثنا نیست؛ ازجمله اقدامات مربوطه ایجاد شده در این زمینه مشتمل بر «قانون جرائم رایانه‌ای، مصوب ۱۹۹۷»[۱]، «قانون ارتباطات و چندرسانه‌ای، مصوب ۱۹۹۸»[۲]، «قانون امضای دیجیتال، مصوب ۱۹۹۸»[۳]، «قانون تجارت الکترونیک، ۲۰۰۶»،[۴] «قانون حفاظت از داده‌های شخصی، مصوب ۲۰۱۰»[۵]، «قانون ضد اخبار جعلی ۲۰۱۸»[۶] و «قانون امنیت سایبری، مصوب ۲۰۲۴» وضع شد. البته با توجه به افزایش تهدید در جرائم دیجیتالی و لزوم رسیدگی مؤثر به پرونده‌های جرائم دیجیتالی و با رویکردهای تروریستی و سازمان‌یافته، دولت مالزی در راستای راهبرد قضایی حاکم در قلمرو حاکمیتی، تشکیل «دادگاه ویژه دیجیتالی»[۷] را اعلام کرد.[۸] اولین دادگاه دیجیتالی ویژه، مستقر در مجتمع دادگاه کوالالامپور در اول سپتامبر سال ۲۰۱۶ به بهره‌برداری رسید.[۹] هدف از تشکیل این دادگاه ارائه ابزارهای مکفی و اثرگذار برای نظام قضایی جهت رسیدگی به جرائم دیجیتالی نظیر هک، کلاه‌برداری برخط، سرقت اطلاعات برخط و غیره است.[۱۰] این در حالی است

1- Computer Crimes Act 1997; Date of Royal Assent 18 June 1997 Date of publication in the Gazette 30 June 1997 PREVIOUS REPRINT, http://www.commonlii.org/my/legis/consol_act/cca1997185/

2- Communications and Multimedia Act 1998; date of Royal assent 3 september 1998 date of publication in the Gazette 5 october 1998,https://www.vertic.org/media/National%20Legislation/Malaysia/MY_Communications_and_Multimedia_Act.pdf

3- Digital Signature Act 1997; Date of Royal Assent 18 June 1997 Date of publication in the Gazette 30 June 1997 PREVIOUS REPRINT

4- Electronic Commerce Act 2006; Date of Royal Assent 30 August 2006, Date of publication in the Gazette 31 August 2006, Date of coming into operation 19 October 2006 [P.U. (B) 280/2006], http://www.commonlii.org/my/legis/consol_act/eca2006182/

5- Personal Data Protection Act 2010; https://www.pdp.gov.my/jpdpv2/laws-of-malaysia-pdpa/personal-data-protection-act-2010/?lang=en

6- Anti-Fake News Act 2018; The Act was passed by the Malaysian Parliament on April 4 and received Royal Assent on April 9, https://www.loc.gov/item/global-legal-monitor/2018-04-19/malaysia-anti-fake-news-act-comes-into-force/

7- Malaysian Special Cyber Court; https://lpplaw.my/insights/e-articles/special-cyber-court-and-e-court/

۸- لازم به‌ذکر است دسترسی به اطلاعات مربوط به پرونده‌های جرائم دیجیتالی در مالزی برای عموم مردم بسیار دشوار است؛ زیرا این پرونده‌ها به‌طور عمده در دادگاه‌های پایین‌تر مورد رسیدگی قرار می‌گیرند و در رسانه‌های قانونی گزارش نمی‌شوند؛

-https://www.researchgate.net/publication/335867251_CYBERCRIME_CASES_IN_A_DECADE_The_Malaysian_Experience

۹- اولین دادگاه دیجیتالی مالزی نشانه تعمیق اقتصاد دیجیتال است. ازاین‌رو، مفهوم دادگاه دیجیتالی، مفهوم جدیدی نیست؛ چرا که جرائم دیجیتالی تا مادامی که اینترنت وجود داشته است، وجود دارند. امری که به‌طور فزاینده‌ای در کل جهان در حال فراگیری است؛

-https://www.digitalnewsasia.com/digital-economy/malaysia%E2%80%99s-first-cyber-court-signals-deepening-digital-economy

۱۰- در حالی که دادگاه ویژه دیجیتالی مادام یک مفهوم بسیار جدید است، مالزی دادگاه الکترونیکی را معرفی کرده‌اند؛ اساساً، این دادگاه از فناوری حمایتی برای تسهیل امور روزمره دادگاه استفاده می‌کند وهدف این نظام تسریع کارآمد در دفع موارد با استفاده از فناوری است. در واقع، هدف سیستم دادگاه الکترونیکی به‌عنوان

کـه در ۱۲ اکتبـر ۲۰۲۰، دولـت مالـزی «راهبـرد امنیـت سـایبری مالـزی ۲۰۲۴-۲۰۲۰»[1] را تدویـن و تصویـب کـرد. اهـداف اساسـی در پنـج رکـن راهبـردی طبقه‌بنـدی شـده اسـت کـه بـر کلیـه ابعـاد برنامه‌ریـزی و اجـرای امنیـت دیجیتالـی در مالـزی تـا سـال ۲۰۲۴ حاکـم خواهنـد بـود.[2] در ضمـن در چارچـوب رویکـرد اجرایـی، راهبـرد امنیـت سـایبری مالـزی شـامل ۱۲ راهبـرد، ۳۵ طـرح اقـدام و ۱۱۳ برنامـه اسـت کـه شـامل ابتـکارات گوناگـون بـرای حفاظـت از فضـای سـایبری کشـور اسـت. وزارت ارتباطـات و چندرسـانه‌ای[3] و آژانـس امنیـت سـایبری ملـی[4] وظیفـه تدویـن، اجـرا، نظـارت و هماهنگـی برنامـه اقـدام میان‌مـدت را بـر عهـده دارنـد. مالـزی یکـی از اولیـن کشـورهای آسـیای جنـوب شـرقی بـود کـه سیاسـت امنیـت سـایبری ملـی[5] را اتخـاذ کـرد. سیاسـت امنیـت سـایبری ملـی کـه در سـال ۲۰۰۶ تدویـن شـد، تأسـیس آژانـس دولتـی مربوطـه را ایجـاد کـرد و پایـه محکمـی بـرای راهبـرد امنیـت سـایبری مالـزی ۲۰۲۴-۲۰۲۰ فراهـم کـرد (Redzuan Mohamad, et al, ۲۰۲۴).[6]

رویکـرد حاکـم در سیاسـت قانون‌گـذار در کشـور مصـر در تصمیـم شـماره ۲ قانـون مبـارزه بـا تروریسـم در مـاده ۲، اقـدام تروریسـتی را چنیـن تعریـف کـرده اسـت: عمـل تروریسـتی بـه معنـای هرگونـه اسـتفاده از زور، خشـونت، تهدیـد یـا ارعـاب در داخـل یـا خـارج از کشـور به‌منظـور برهـم زدن نظـم عمومـی اسـت. یـا بـه خطـر انداختـن امنیـت جامعـه، مصالحـه یـا ملـت آن یـا آسـیب رسـاندن بـه افـراد یـا ایجـاد رعـب و وحشـت در میـان آن‌هـا و همچنیـن هـر رفتـاری کـه بـه قصـد دسـتیابی بـه یکـی از اهـداف منـدرج در بنـد اول ایـن مـاده انجـام شـود. بـرای آن یـا تحریـک آن درصورتی‌کـه بـه ارتباطـات، سیسـتم‌های اطلاعاتـی، سیسـتم‌های مالـی یـا بانکـی یـا اقتصـاد آسـیب برسـاند. البتـه قانون‌گـذار تعریـف اقـدام تروریسـتی را بـه گونـه‌ای گسـترش داد کـه شـامل همـه رفتارهایـی می‌شـود کـه شـامل اسـتفاده از زور، خشـونت، تهدیـد یـا ارعـاب بـرای دسـتیابی بـه اهـداف تروریسـتی و همچنیـن تحریـک و مشـارکت در اعمالـی می‌شـود کـه بـه ارتباطـات یـا سیسـتم‌های اطلاعاتـی آسـیب می‌رسـاند. قانون‌گـذار مصـری همچنیـن هـدف اسـتفاده از ابزارهـای تروریسـتی را بـا قـرار دادن اصطلاحـات گسـترده‌ای ماننـد آسـیب رسـاندن بـه وحـدت ملـی، صلـح اجتماعـی، امنیـت ملـی یـا آسـیب رسـاندن بـه محیط‌زیسـت و غیـره گسـترش داد. البتـه در اوت ۲۰۱۸، قانـون شـماره ۱۷۵ تحـت عنـوان، «قانـون مبـارزه بـا بزهکاری‌هـای سـایبری و فنـاوری اطلاعـات در مصـر»[7] تصویـب شـد. ایـن قانـون، انتشـار آنلایـن اطلاعـات در مـورد جنبـش ارتـش و پلیـس را ممنوع کـرده و هـک کردن سیسـتم‌های اطلاعاتـی را جـرم انـگاری می‌کنـد. ایـن قانـون مجازات‌هایـی را بـرای دسترسـی غیرمجـاز، نقـض حریـم خصوصـی داده‌هـا و سـایر اشـکال تخلـف دیجیتالـی مشـخص می‌کنـد. قانـون ۲۰۲۰/۱۵۱ در مـورد حفاظـت از داده‌هـای شـخصی[8]، حفاظـت از اطلاعـات شـخصی افـراد، تعییـن اسـتاندارد جدیـدی بـرای حفاظـت از داده‌هـا و تأثیـر قابل‌توجهـی بـر امنیـت دیجیتالـی در مصـر

یـک کل، اسـتفاده از فنـاوری بـرای رسـیدگی بـه مسـائل و پرونده‌هایـی اسـت که سـال‌ها نظـام قضایـی را درگیر خود کـرده اسـت. لازم به‌ذکر آیت کـه این نـوع از دادگاه در ژانویه سـال ۲۰۱۶ تأسـیس شـد؛ https://lpplaw.my/insights/e-articles/special-cyber-court-and-e-court/

1- Malaysia Cyber Security Strategy (MCSS); https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurity Strategy2020-2024.pdf

2- https://www.coe.int/en/web/octopus/-/malaysia

3- Communications and Multimedia Ministry (KKMM)

4- National Cyber Security Agency (NACSA)

5- National Cyber Security Policy (NCSP)

6- https://www.coe.int/en/web/octopus/-/malaysia

7- Law No. 175 of 2018 on Anti-Cyber and Information Technology Crimes, Egypt, https://www.wipo.int/wipolex/en/legislation/details/19959

8- Law No. 151 of 2020 Promulgating the Personal Data Protection Law

است. ماده نخست این قانون در مورد حفاظت از داده‌های شخصی که به‌صورت الکترونیکی، جزئی یا کلی، توسط هر دارنده، کنترل‌کننده یا پردازشگر در رابطه با اشخاص حقیقی پردازش می‌شود، اعمال می‌شود.[۱]

سیاست قانون‌گذار در کشور عمان با فرمان شماره (۷۲) سال ۲۰۰۱ قانون مجازات عمان را اصلاح کرده است[۲] و بر اساس این اصلاحیه، مجموعه‌ای از اقداماتی که رایانه در معرض آن قرار می‌گیرد، ازجمله ورود غیرقانونی به سیستم‌های رایانه‌ای، جرم انگاری شده است.[۳] عمان کنوانسیون عربی برای مبارزه با تروریسم ازجمله مقابله با بزهکاری‌های تروریستی در فضای دیجیتالی را با فرمان شماره ۵۵/۹۹ در سال ۱۹۹۹ تصویب کرد. به‌علاوه، «قانون بزهکاری‌های سایبری عمان» با فرمان سلطنتی به شماره ۲۰۱۱/۱۲ صادر شده است.[۴] تدوین این قانون عصر جدیدی را برای عمان آغاز می‌کند؛ جایی که یک جامعه واقعاً فعال الکترونیکی در تحقق جامعه دیجیتالی عمان تکامل می‌یابد. این یک نقطه عطف بزرگ در اجرای راهبرد ملی فناوری اطلاعات توسط سازمان فناوری اطلاعات عمان است.[۵] لازم به ذکر است این قانون جرم دیجیتال را در یک تعریف صریح به‌عنوان استفاده علمی از محاسبات و الکترونیک و ارتباطات برای پردازش و توزیع داده‌ها و اطلاعات در تمام اشکال مختلف آن تعریف می‌کند. قانون‌گذار عمان با به‌روزرسانی قوانین و قوانینی که با انواع بزهکاری‌ها و به‌ویژه بزهکاری‌های الکترونیکی و اطلاعاتی مبارزه می‌کند، توانسته است با توسعه تمدن و چالش‌های جدید مقابله کند (Salim Alshibli, ۲۰۲۱: ۸۹).

در چارچوب مقررات امارات متحده عربی بزهکاری‌های دیجیتالی شامل استفاده از رایانه به‌عنوان ابزاری برای اهداف غیرقانونی، نظیر ارتکاب کلاه‌برداری، قاچاق هرزه‌نگاری کودکان و مالکیت معنوی، سرقت هویت، یا نقض حریم خصوصی و غیره است. البته توزیع ویروس‌ها، دانلود غیرقانونی فایل‌ها، فیشینگ و سرقت شخصی نیز در شمارش این بزهکاری‌ها قرار دارند. قانون فدرال (۲) امارات در سال ۲۰۰۶ در خصوص مبارزه با بزهکاری‌های فناوری اطلاعات که چارچوب قانونی مبارزه با بزهکاری‌های دسترسی غیرقانونی به سیستم اطلاعاتی است، صادر شد. هم‌چنین طبق ماده ۲ فرمان فدرال ایالتی فدرال قانون شماره ۱ ۲۰۰۴ در مورد مبارزه با بزهکاری‌های تروریستی، عمل تروریستی در اجرای مفاد این فرمان عبارت است از هر فعل یا ترک فعلی که تروریست در اجرای یک پروژه مجرمانه فردی یا جمعی به آن متوسل شود (Alyammahi, Bin Mohd Noor, ۲۰۲۳: ۱۱۴- ۱۱۶). قانون اخیر به افزایش بزهکاری‌های الکترونیکی می‌پردازد که شامل بزهکاری‌هایی مانند کلاه‌برداری از کارت اعتباری، بزهکاری‌های اینترنتی، بزهکاری تروریستی در فضای دیجیتالی، ایجاد و یا توزیع ویروس‌ها، هک، تداخل در سیستم، دسترسی غیرقانونی و رهگیری و غیره می‌شود. همچنین هدف آن تشویق همکاری بین کشورهای عربی در مبارزه با

1- https://www.acc.com/sites/default/files/program-materials/upload/Data%20Protection%20Law%20-%20Egypt%20-%20EN%20-%20MBH.PDF

۲- در ماده ۱۳۲ قانون مجازات عمان آمده است: «اقدامی تروریستی است که با استفاده از مواد سمی یا اپیدمی، مواد منفجره یا هر وسیله‌ای که باعث ایجاد خطر عمومی شود، درصورتی‌که خرابکاری در یک مکان عمومی یا خصوصی رخ دهد، حالت وحشت ایجاد کند مؤسسه، کشتی، هواپیما، حمل و نقل یا حمل و نقل، در این صورت مجازات را تشدید می‌کند.»

3- The Penal Law Promulgated by Royal Decree 7/2018, https://oman.om/docs/default-source/default-document-library/omani-penal-law.pdf?sfvrsn=64250c36_2

4- Royal Decree No 12/2011 Issuing the Cyber Crime Law, https://www.mtcit.gov.om/ITAPortal/Data/English/DocLibrary/FID20114117574666/Royal%20Decree%20No%20122011%20-%20Issuing%20the%20Cyber%20Crime%20Law.pdf

5- https://www.mtcit.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=54

بزهکاری‌های دیجیتالی است. این موافقت‌نامه همچنین بر اهمیت اجرای قانون حق چاپ تصریح می‌کند. برای متخلفان از شرایط و مقررات قرارداد جریمه در نظر گرفته می‌شود.[1]

نتیجه‌گیری

با ظهور اینترنت بخش قابل‌توجهی از دغدغه‌های امنیت بین‌المللی معطوف این فضا شده است. فضایی که با ساختار فنی پیچیده خود چالش‌های مهمی را برای دولت‌ها که از سوی شرکت‌های فناوری به‌عنوان بازیگران فعال به گوشه‌ای رانده شده‌اند، فراهم آورده است. ازاین‌رو، هدف اساسی بزهکاری تروریستی در فضای دیجیتالی به‌احتمال‌زیاد همان بزهکاری تروریستی سنتی است، یعنی «ایجاد رعب و وحشت» در میان مردم و برای اجبار رژیم موجود. بزهکاری تروریستی در فضای دیجیتالی شامل اعمال سیاسی، مذهبی، مالی، عقیدتی و موارد مشابه است. اکنون به ابزارهای مدرن شبکه منتقل شده و تهدیدهای جدی برای زیرساخت‌های عمومی و خصوصی ایجاد می‌کند.

در دنیای امروز، بزهکاری تروریستی در فضای دیجیتالی به یک چالش بین‌المللی تبدیل شده است و بسیاری از سازمان‌های بین‌المللی با تشریک‌مساعی سعی بر آن دارند تا با آن مبارزه کنند. به دلیل وابستگی به زیرساخت‌های فیزیکی توسط اکثر کشورها به‌ویژه کشورهای اسلامی مایل نیستند اطلاعات امنیت دیجیتالی خود را با سایر ایالت‌ها به اشتراک بگذارند. چارچوب‌های قانونی در دسترس است، اما هنوز هم خلأهایی در سیستم امنیت دیجیتالی به‌طورکلی وجود دارد. اسناد، معاهده‌ها، موافقت‌نامه‌های زیادی علیه ناامنی دیجیتالی در چارچوب قلمرو قانون‌گذاری کشورهای اسلامی وجود دارد؛ بنابراین، یکی از بزرگ‌ترین خطراتی که این فضا برای کشورهای اسلامی ایجاد نموده آن است که ضعف فناورانه حتی یک کشور می‌تواند بستری برای تهدیدهای جدی علیه تمامی کشورها فراهم آورد. بزهکاری تروریستی در فضای دیجیتالی ضمن اینکه امنیت افراد را با مخاطره مواجه می‌سازد، امکان ورود خدشه به امنیت فضای دیجیتالی را از طریق نقض حقوق بشر و آزادی‌های اساسی را نیز فراهم می‌آورد؛ بنابراین، اتخاذ سازوکارهایی برای ارتقای امنیت دیجیتالی باید در امکان در دسترس بودن، یکپارچگی و محرمانه بودن اطلاعات را تقویت کند.

اگرچه در چارچوب سیاست قانون‌گذاری کشورهای اسلامی سنت‌های مشترک و ارزش‌های اسلامی، حقوقی، فرهنگی و اجتماعی قابل ملاحظه است، اما شباهت‌ها و تفاوت‌هایی در مقررات مبارزه با بزهکاری‌های تروریستی در فضای دیجیتالی آن‌ها وجود دارد. علاوه بر این، در حوزه رسیدگی به این نوع از بزهکاری‌ها نیز متنوع است؛ بنابراین، کلیه کشورهای اسلامی ضرورت دارد تا شکاف‌های فناوری مربوط به بزهکاری تروریستی در فضای دیجیتالی و امنیت دیجیتالی را کاهش دهند. جستجوی اشتراک اطلاعات متقابل بین کشورهای اسلامی برای راه‌حل امنیت اطلاعات نیز ضروری است. همچنین باید توجه داشت که مقرراتی موجود برای بزهکاری تروریستی فیزیکی نمی‌تواند برای محیط فناوری اطلاعات مورد استفاده قرار گیرد؛ بنابراین، نیاز مبرمی به ایجاد چارچوب قانونی برای اجرای فعالیت‌های بزهکاری تروریستی در فضای دیجیتالی وجود دارد.

1- https://www.sabaip.com/saudi-arabia-arab-cybercrime-agreement-approved/

منابع

موسوی، سیدجمال، محمد روحانی‌مقدم و مریم آقائی بجستانی (۱۴۰۱)، تدابیر پیشگیری از جرائم سایبری با تأکید بر اقدامات پلیسی با رویکردی فقهی، مطالعات فقه و حقوق اسلامی، شماره ۲۶.

Alyammahi, Mohamed S., Sulaiman Shakib Bin Mohd Noor (2023), "Cybercrimes in the United Arab Emirates: Characteristics and Countermeasures", International Journal of Academic Research in Public Policy and GOvernance, 9(1): 108- 122.

Corliss, Cody (2023), "Digital Terror Crimes", Columbia Journal of Transnational Law, 62(13): 58112-.

Fidler, David P (2016), "Cyber Space, Terrorism and International Law Get Access Arrow", Journal of Conflict and Security Law, 21(3): 475- 493.

Jian, Hua & Bapna Sanjay (2012), "How Can we Deter Cyber Terrorism?", Information Security Journal, 21(2):102- 116.

Pollitt, Mark M (1997), "Cyber-terrorism: Fact or Fancy?", Proceedings of the 20th National Information Systems Security Conference, p. 285–289

Shaweorcid, Robb, Ian R. McAndrew (2023), "Cybersecurity and Domestic Terrorism: Purpose and Future", Journal of Software Engineering and Applications, 16(10): 548- 560.

Raj, P., & Yadav S. (2022), "Cyber Terrorism: A Threat to Cyber World. Emerging Trends in Technology & its Impact on Law", 1.

Redzuan Mohamad, Ahmad, et al. (2024), The Efficacy of the Malaysian Government's Response towards Cybercrime, Open Journal of Political Science, 14, 166- 176.

Roy, Sourodip (2022), "Cybercrime and islamic law: Revisiting the advantageous and hiatus horizon(s)", Annals of Justice and Humanity, 1(2): 93- 99

Taylor, Robert E, Eric J. Fritsch, John Liederbach (2019), Digital Crime and Digital Terrorism, Publisher Pearson, 3rd Edition.

Salim Alshibli, Abdullah Ali (2021), "Electronic Crime in the Sultanate of Oman Challenges and Legal Solutions", Journal of Economic, Administrative and Legal Sciences, 2(3): 83- 98.

Syihabudin (2022), "Cybercrimes and Use of Digital Technologies: An Islamic Law Perspective in an Emerging Economy", International Journal of Cyber Criminology, 16(2): 104–118.

Weimann, Gabriel (2014), "New Terrorism and New Media", Wilson Center Commons Lab, 1, available at http://www.wilsoncenter.org/publication/new-terrorism-and-new-media.