Journal of
Comparative Criminal Jurisprudence
www.jccj.ir

Volume 4, Issue 2, 2024

Digital Terrorist Crimes and Considerations in the Legal Capacities of Islamic Countries

Peyman Namamian*[1], Farid Farahmand[2]

1. Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran. (Corresponding Author)
2. Assistant Professor, Department of Law and Social Sciences, Payame Noor University, Tehran, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: ***145-156***

Corresponding Author's Info
ORCID: *0000-0001-7681-7293*
TELL: *+988632620000*
Email: *p_namamian1512@yahoo.com*

Article history:
Received: *22 Feb 2024*
Revised: *03 May 2024*
Accepted: *08 Jun 2024*
Published online: *21 Jun 2024*

Keywords:
Digital Space, Terrorist Crimes, Digital Terrorist Crimes, Criminal Law of Islamic Countries.

ABSTRACT

Committing digital terrorist crimes involves using the Internet and other forms of information and communication technology to threaten or cause physical harm to gain political or ideological power through threats or intimidation. Data theft and manipulation, and disruption of essential services, are examples of this category of crimes. Therefore, today, technologies enable the increase of crimes, especially digital terrorist crimes, in order to violate the security of users and make the cyberspace face increasing insecurity and challenges. As digital infrastructure becomes more critical and barriers to entry for malicious actors decrease, digital terrorist crimes have become a growing concern. Detecting, responding to, and preventing this crime presents unique challenges for law enforcement and governments that require a multifaceted approach. Based on this, some Islamic countries have started to approve regulations in their territorial legal and sovereign territory to deal with digital crimes. It is emphasized that the regulations approved by the Islamic countries have made it possible to prevent and deal with such crimes to a considerable extent, but this does not mean that the said regulations provide the maximum possibility of dealing with the complex methods and patterns of digital terrorist crimes for the Islamic countries. Will do Therefore, it is necessary to form a global and regional consensus in this regard in order to provide the ground for confronting and suppressing it.

How to Cite This Article: Namamian, P & Farahmand, F (2024). "Digital Terrorist Crimes and Considerations in the Legal Capacities of Islamic Countries". *Journal of Comparative Criminal Jurisprudence*, 4(2): 145-156.

فصلنامه فقه جزای تطبیقی
www.jccj.ir
انجمن علمی فقه جزای تطبیقی ایران
فصلنامه فقه جزای تطبیقی

دوره چهارم، شماره دوم، تابستان ۱۴۰۳

جرایم تروریستی دیجیتالی و ملاحظاتی در ظرفیت‌های حقوقی کشورهای اسلامی

پیمان نمامیان*[۱]، فرید فرهمند[۲]

۱. دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران. (نویسنده مسؤول)

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

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱۴۵-۱۵۶

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۰-۰۰۰۱-۷۶۸۱-۷۲۹۳

تلفن: ۰۰۰۰ ۳۲۶۲ ۹۸۸۶+

ایمیل: p_namamian1512@yahoo.com

سابقه مقاله:

تاریخ دریافت: ۱۴۰۲/۱۲/۰۳

تاریخ ویرایش: ۱۴۰۳/۰۲/۱۴

تاریخ پذیرش: ۱۴۰۳/۰۳/۱۸

تاریخ انتشار: ۱۴۰۳/۰۴/۰۱

واژگان کلیدی:

فضای دیجیتال، جرایم تروریستی، جرایم تروریستی دیجیتالی، حقوق کشورهای اسلامی.

چکیده

ارتکاب جرایم تروریستی دیجیتالی مشتمل بر بهره‌گیری از اینترنت و سایر اشکال فناوری اطلاعات و ارتباطات برای تهدید یا ایجاد آسیب بدنی برای به‌دست‌آوردن قدرت سیاسی یا عقیدتی از طریق تهدید یا ارعاب است. سرقت و دستکاری داده‌ها و اختلال در خدمات ضروری، به‌عنوان نمونه‌هایی از این دسته جرایم هستند. بنابراین امروزه فناوری‌ها امکان افزایش جرایم به‌ویژه جرایم تروریستی دیجیتالی را فراهم می‌نماید تا ضمن نقض امنیت کاربران، فضای مجازی را با ناامنی و چالش‌های روزافزونی مواجه سازد. با بحرانی‌شدن زیرساخت‌های دیجیتالی و کاهش موانع ورود برای عوامل مخرب، جرایم تروریستی 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، برخی از کشورهای اسلامی نسبت به مقابله با جرایم دیجیتالی مبادرت به تصویب مقرراتی در قلمرو قانونی و حاکمیتی سرزمینی خود نموده‌اند. تأکید می‌گردد که مقررات مصوب از سوی کشورهای اسلامی تا حدود قابل ملاحظه‌ای امکان پیشگیری و مقابله با چنین جرایمی را فراهم آورده است، اما این بدان معنا نیست که مقررات مزبور امکان مقابله حداکثری را با روش‌ها و فنون پیچیده جرایم تروریستی دیجیتالی را برای کشورهای اسلامی ایجاد خواهد کرد. ازاین‌رو، ضرورت دارد تا اجماعی جهانی و منطقه‌ای در این رابطه شکل گیرد تا زمینه مقابله و سرکوب آن فراهم شود.

مقدمه

فناوری اطلاعات را یکی از نتایج این دگرگونی فرهنگی و پیشرفت علمی در حوزه شبکه‌ها و رایانه‌ها می‌دانند که جهان را فراگرفت تا آن را بدون مرز و نامحدود کند. جهان پس از راهپیمایی فناوری اطلاعات در تمام معابر خود به مکانی عظیم و متنوع تبدیل شد که به تولید و توسعه بسیاری از رفتارهای مجرمانه کمک کرد که زندگی افراد و جامعه را به‌شدت تحت تأثیر قرار داد. بازیگران تروریستی که در درگیری‌های مسلحانه فعالیت می‌کنند، رسانه‌های اجتماعی را با استفاده از این سکوهای دیجیتالی برای تهدید و انتشار تصاویر وحشیانه به‌منظور طعن، وحشت و ارعاب غیرنظامیان به سلاح تبدیل کرده‌اند.

فناوری‌های دیجیتالی در حال حاضر حیات بشری را به‌شدت تغییر داده است. تقریباً هر حوزه از روابط اجتماعی در حال حاضر هم در سطح ملی و هم در سطح بین‌المللی در حال دیجیتالی‌شدن است. زیرساخت‌های ارتباطی اطلاعات و همچنین دستگاه‌های دیجیتال در حال حاضر به بخشی جدایی‌ناپذیر از واقعیت امروز تبدیل شده‌اند. دیجیتالی‌شدن تأثیر بسیار زیادی بر توسعه و رعایت حقوق بشر و همچنین بر وضعیت خود فرد دارد. با رشد فناوری‌های دیجیتالی، جرایم تروریستی در فضای مجازی هم گسترش یافت و فرصت‌های زیادی را برای مرتکبان جرایم تروریستی فراهم کرد تا اقدام‌هایی را جهت ورود آسیب جدی به زیرساخت‌ها و بسترهای اجتماعی، سیاسی و حتی امنیتی فراهم نماید.[۱] بنابراین جرایم دیجیتالی یک جرم طی دهه‌های اخیر است که چالش‌های نوینی را به‌ویژه برای جامعه جهانی ایجاد کرده است. ازاین‌رو، جرایم دیجیتالی هیچ مرز جغرافیایی ندارد و کل جهان تحت تأثیر قرار خواهد گرفت. این در حالی است که با رشد فناوری‌های دیجیتالی، نحوه ارتکاب این نوع از جرایم در فضای دیجیتالی به‌نحو دهشتناک و افراطی گسترش یافته و موجبات ارتکاب جرایم تروریستی را نیز فراهم آورده است.

بنابراین جرایم تروریستی دیجیتالی به‌دلیل اتکای فزاینده به فناوری اطلاعات در بسیاری از جنبه‌های جامعه و احتمال ایجاد اختلال یا آسیب قابل توجه ناشی از حمله‌های دیجیتالی با رویکرد تروریستی، یک نگرانی رو به رشد است. تأثیر قابل توجهی در سطح جهانی داشت و همچنان ابعاد مختلف ثبات یک کشور را تهدید می‌کند. یکی از بزرگ‌ترین اثرات این نوع از جرایم، انسداد زیرساخت‌های حیاتی نظیر شبکه‌های حمل و نقل، شبکه‌های برق و بانکی است.

در ضمن، تروریست‌ها به‌طور روزافزون از فضای مجازی به‌عنوان ابزاری برای جذب نیرو و شناساندن خود به مردم استفاده می‌کنند.[۲] رسانه اجتماعی یک نوآوری جدید است که به افراد اجازه می‌دهد اطلاعات، ایده‌ها، پیام‌های شخصی و محتویات دیگر (مانند فیلم) را در سراسر دنیا با یکدیگر به اشتراک بگذارند.[۳]

به هر روی، در این پژوهش سعی بر آن است تا به پرسش‌هایی نظیر «مفهوم جرایم تروریستی دیجیتالی چیست؟» و «کشورهای اسلامی دارای چه ظرفیت حقوقی و قانون‌گذاری در قبال جرایم تروریستی دیجیتالی هستند؟» به‌گونه‌ای مستدل و بر پایه مقررات کیفری کشورهای اسلامی و البته با استفاده روش تحلیلی توصیفی پاسخ داده شوند.

۱- مفهوم‌شناختی

استفاده روزافزون از فناوری‌های دیجیتال مخاطره‌هایی را برای سیستم‌های حیاتی به‌دلیل بهره‌برداری توسط تروریست‌ها ایجاد می‌کند. امنیت فضای دیجیتال مستلزم اقدامات

۱- فناوری‌های دیجیتال ابزار جدیدی برای دفاع و اجرای حقوق بشر فراهم می‌کنند. استفاده از فناوری‌های نوین اطلاعات و ارتباطات، حتی توسط افراد و نهادهای غیردولتی ممکن است تهدیدی برای صلح و امنیت بین‌المللی باشد.

۲- علاقه فزاینده‌ای در میان گروه‌های افراطی و سازمان‌های تروریستی به استفاده از فضای دیجیتالی وجود دارد، درنتیجه جرایم تروریستی دیجیتالی به یک تهدید بالقوه در سراسر جهان تبدیل شده است (Lee *et al*, 2021: 337-338)؛ این نوع جرم، شکل خاصی از جرایم تروریستی است که برای دستیابی به اهداف عقیدتی، اجتماعی و سیاسی خاصی از طریق ایجاد سردرگمی و ترس در میان جمعیت هدف طراحی شده است (Golose, 2022: 112-113). در هر حال، ترس از جرایم تروریستی دیجیتالی به‌طور مداوم در حال افزایش است و گروه‌های تروریستی قصد دارند اطلاعات جدیدی را استخراج کنند و از آن به نفع خود از طریق فناوری‌های دیجیتال نظیر رسانه‌های اجتماعی برای انتشار پیام‌های رادیکال در بین اقشار گوناگون مردم استفاده کنند (Kapu, 2021: 49-51).

3- Social Media, Merriam-Webster. https://www.merriam-webster.com/dictionary/social/20media.

پیشگیرانه است که برای محافظت از نرم‌افزار و دستگاه‌های الکترونیکی در قبال هرگونه تهدید طراحی شده است (Shaweorcid & McAndrew, 2023: 548). ازاین‌رو، ورود این فناوری به روش‌های ارتکاب جرایم نیز امکان‌پذیر شده و یکی از مهم‌ترین آن‌ها جرایم نوین نظیر جرایم تروریستی دیجیتالی است، البته گروه‌های تروریستی اکنون از فرصت‌های ارائه‌شده توسط اینترنت و فضای مجازی بهره می‌برند و از منابع برخط برای فرماندهی، کنترل و برقراری ارتباط با شبکه‌های خود استفاده می‌کنند و روایت‌های خود را به‌گونه‌ای شکل می‌دهند که نگرانی‌های عمومی را ابراز و نیروهای جدید را جذب می‌کنند (Yüksel, 2020: 1089).

بنابراین جرایم دیجیتالی از نظر ماهیت پیچیده بوده و مشتمل رشته‌های بسیاری از جمله جرم‌شناسی، علوم رایانه، روان‌شناسی، جامعه‌شناسی، اقتصاد، جغرافیا، علوم سیاسی و حقوق هستند (Dupont & Holt, 2022: 25). بنابراین جرایم دیجیتال جرایمی است که مولود جامعه فناور و نوین بوده و به همین دلیل، ابهامات زیادی در باب ماهیت و پیشینه این‌گونه جرایم از یک‌سو و ویژگی‌های این جرایم و مرتکبان آن‌ها از سوی دیگر وجود دارد. با عنایت به این ابهامات و نیز تفاوت‌های موجود بین جرایم دیجیتال و سایر جرایم، پیشگیری و مقابله با جرایم دیجیتال اقدامات تهاجمی خاصی را می‌طلبد (موسوی و همکاران، ۱۴۰۱: ۳۲۳).

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 مورد استفاده متفاوت است. اجرای پروژه جرایم تروریستی دیجیتالی منوط به استفاده از توانمندی‌های علمی و فنی و بهره‌برداری از وسایل ارتباطی و شبکه‌ها، اطلاعات به‌منظور ارعاب دیگران، آسیب‌رساندن و تهدید آن‌ها است (السند، ۲۰۰۴: ۹).

«رشد فزاینده فناوری اطلاعات و ارتباطات نظیر اینترنت عرصه شکل‌گیری مجموعه‌ای از ارتباطات میان گروه‌های اجتماعی متفاوت از فاصله‌های بسیار دور در دنیای واقعی است که فرصت‌ها و تهدیدهای نوینی را فراروی جامعه بین‌المللی قرار داده است؛ به‌طور نمونه جرایم تروریستی، ازجمله تهدیدهای نوینی است که فضای مجازی و دیجیتالی موجبات آن را فراهم ساخته است» (یزدان‌پناه‌درو و جعفری، ۱۳۹۷: ۲۲۱).

از منظر روان‌شناختی، واژه «تروریسم دیجیتال» ترس از اعمال خشونت‌آمیز را با ترس از فناوری ترکیب می‌کند. دلیل آن این است که یک تهدید ناشناخته از نظر روانی قدرتمندتر از یک تهدید شناخته‌شده مانند یک بمب تروریستی تلقی می‌شود. به‌علاوه، از طریق جرایم تروریستی دیجیتالی علیه دولت‌ها، سرورهای خصوصی، شبکه‌ها یا سایر دستگاه‌های الکترونیکی، هکرها می‌توانند با استفاده از ویروس‌ها، کرم‌ها ضمن ایجاد آسیب به سیستم‌ها، وب‌سایت‌ها را مخدوش کنند.[۱] ازاین‌رو، می‌توان مصداق‌هایی از جرایم تروریستی دیجیتالی را ذکر کرد:

۱- شبکه‌های تروریستی جهانی که سایت‌های اصلی را با ایجاد مزاحمت‌های عمومی یا توقف ترافیک اینترنتی مختل می‌کنند؛

۲- دسترسی تروریست‌های دیجیتالی بین‌المللی و سپس غیرفعال‌کردن یا اصلاح سیگنال‌های فناوری نظامی؛

۳- تروریست‌های دیجیتالی که سیستم‌های زیرساختی حیاتی مانند تصفیه‌خانه آب یا شبکه برق را هدف قرار می‌دهند؛

۴- جاسوسی دیجیتالی که توسط دولت‌ها یا سازمان‌های خصوصی برای جاسوسی از ارتباطات اطلاعاتی انجام می‌شود (Buresh, 2020: 20).

برخی جرایم تروریستی دیجیتالی را این‌گونه تعریف کرده‌اند «تهاجم و تهدید فیزیکی یا اخلاقی توسط افراد، گروه‌ها یا کشورها علیه ذهن، مذهب، ناموس یا دارایی افراد بدون حق

---

[۱]- در این ارتباط می‌توان به هک جایگاه‌های سوخت در ایران و اختلال در پمپ بنزین‌های اقصی‌نقاط کشور ایران در ۲۷ آذرماه ۱۴۰۲ اشاره داشت که این امر به‌گفته مسؤولین امر که توسط خبرگزاری‌های داخلی انعکاس یافت، توسط یک گروه هکری صهیونیستی به نام «گنجشک درنده» بوده که مسؤولیت هک سیستم سوخت‌رسانی ایران را برعهده گرفته است. این در حالی است که پیش‌تر هکرها در چهارم آبان ۱۴۰۰، اطلاعات کارت سوخت شخصی را هدف قرار دادند؛ https://www.farsnews.ir/news/14020927000595/D8.

با استفاده از وسایل الکترونیکی و اطلاعاتی به اشکال مختلف تجاوز و فساد» (عبدالفتاح مطر، ۲۰۰۵: ۲).

با این حال، هیچ تعریف قابل قبولی از جرایم دیجیتالی وجود ندارد. یک رویکرد رایج این است که آن را در دو دسته تعریف کنیم: «جرایم وابسته به فناوری دیجیتالی[۱]» و «جرایم مبتنی‌بر فضای دیجیتالی[۲]». ازاین‌رو، جرایم وابسته به فناوری دیجیتالی به جرایمی اطلاق می‌شوند که تنها با استفاده از فناوری اطلاعات و ارتباطات قابل ارتکاب هستند که در این زمینه می‌توان به هک‌کردن یک سازمان یا دستگاه فرد، رمزگذاری داده‌ها و درخواست پرداخت برای رمزگشایی به‌عنوان نمونه اشاره داشت. در مقابل، جرایم مبتنی‌بر فضای دیجیتالی جرایمی هستند که با استفاده از فناوری اطلاعات و ارتباطات، سرعت، مقیاس و دامنه تغییر یافته‌اند که در این رابطه می‌توان به نمونه‌هایی همچون کلاه‌برداری‌های بانکی برخط، سرقت هویت یا کلاه‌برداری اشاره کرد.[۳]

درواقع، جرایم تروریستی دیجیتالی از ارسال تصاویر برای تبدیل غیرنظامیان دیگر، به اهداف حمله، استفاده می‌کنند؛ این بدان معناست که انتشار تصاویر وحشیانه برای جمعیت غیرنظامی از طریق رسانه‌های اجتماعی با هدف گسترش وحشت در بین مردم غیرنظامی انجام می‌شود.[۴] ازاین‌رو، این‌گونه رفتارها که منجر به ایجاد محتوا با استفاده از وحشیانه می‌شوند، حتی بدون تبدیل آن‌ها به یک جرم تروریستی دیجیتالی از طریق فرآیندهای بعدی، به خودی خود به‌مثابه یک جرم دهشتناک در تراز جهانی قلمداد می‌شود[۵] (Corliss, 2023: 99).

بر این اساس می‌توان اذعان داشت باتوجه به فقدان اصلاحیه‌ای در اساسنامه رُم که امکان تعقیب جرایم جنگی تروریستی در دیوان کیفری بین‌المللی را فراهم می‌کند، هرگونه تعقیب بعدی برای جرایم تروریستی دیجیتالی از سوی این نهادهای بین‌المللی و محاکم کیفری سرزمینی صورت خواهد پذیرفت (Taylor *et al*, 2019: 271-274).

در هر حال، تأکید می‌شود ارتباط بین اینترنت و جرایم تروریستی پس از حوادث ۱۱ سپتامبر ۲۰۰۱ پدیدار شد و رویارویی با جرایم تروریستی و تروریست‌ها از رویارویی فیزیکی به رویارویی دیجیتالی منتقل شد.[۶]

۲- تهدیدها و رویکردها

گسترش فزاینده فناوری اطلاعات و ارتباطات منجر به تحول و دگرگونی جوامع در ابعاد مختلف سیاسی، امنیتی، اقتصادی و اجتماعی شده است. در چنین فضایی که با عنوان فضای مجازی توصیف می‌شود، تهدیدهای نوینی نظیر جنگ مجازی، جنگ اطلاعاتی، جرایم دیجیتال، پدیده هکرها و سرقت اطلاعات محرمانه نهادهای امنیتی و اطلاعاتی، ظهور کرده‌اند تا امنیت ملی کشورها را با چالش جدی مواجه سازند.

دیجیتالی‌شدن، سرمایه‌داری نظارتی و افزایش عملیات مخرب دیجیتال، همگی اعمال حقوق بین‌المللی موجود در فضای دیجیتال را به چالش کشیده‌اند. در حال حاضر هیچ ابزار هنجاری خاصی وجود ندارد که به‌طور جامع حقوق بشر قابل اجرا در عصر دیجیتال را تعیین کند. در مقابل، پیشرفت‌های فناوری اطلاعات و ارتباطات برای رژیم‌های مختلف بین‌المللی و محلی موجود که به‌دنبال حمایت از حقوق بشر هستند، پیامدهایی دارد. توسعه فناوری‌های دیجیتال کلیه ابعاد حیات بشر و حقوق بین‌المللی نظیر گستره، مسائل، ابزار و روش‌های تحریم‌های بین‌المللی و یک‌جانبه را تغییر داده و همچنان در حال تغییر است.

در این راستا، چالش‌های جدیدی برای حقوق فردی و انسجام اجتماعی پدیدار شده است. قانون به‌عنوان ابزاری برای

---

[1]- Crimes Related to Digital Technology
[2]- Crimes Based on Digital Space
[3]- https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter

[۴]- 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, 2014: 1).

[۵]- لازم به‌ذکر است، مسؤولیت ارتکاب جرایم تروریستی دیجیتالی شامل رهبری بازیگران غیردولتی تروریستی تحت یک شکل گسترده از مسؤولیت شرکت جنایی مشترک است که در محاکم مختلط و موقت بین‌المللی مورد بهره‌گیری قرار می‌گیرد.

[۶]- با این حال، ارتکاب جرایم تروریستی دیجیتالی ممکن است از راه‌هایی غیر از رایانه‌ها مانند تلفن همراه، دستگاه‌های بلک‌بری، تبلت‌ها و آی‌پدها ارتکاب یابد.

تضمین حقوق، توزیع تعهدات و فراهم‌کردن جوامع باثبات، باید مطابق با فناوری تغییر کند. پس از اختراع اینترنت، روندهای جدیدتر مانند دیجیتالی‌شدن، سرمایه‌داری نظارتی و افزایش عملیات مخرب دیجیتال، همگی اعمال حقوق بین‌المللی موجود در فضای دیجیتال را به چالش کشیده‌اند.

نگرانی فزاینده‌ای در مورد سوءاستفاده تروریست‌ها از فناوری‌های اطلاعات و ارتباطات به‌ویژه اینترنت و فناوری‌های دیجیتال جدید برای ارتکاب، تحریک، عضوگیری، تأمین مالی یا برنامه‌ریزی جرایم تروریستی وجود دارد. ازاین‌رو، سازمان ملل متحد به خطرات استفاده تروریستی از اینترنت پی برده است. در دهه ۱۹۹۰ سازمان از دولت‌های عضو خواست خطر استفاده تروریستی از سیستم‌ها و شبکه‌های الکترونیکی یا مخابراتی با سیم جهت انجام اعمال جنایتکارانه را متذکر شوند و سازوکاری برای پیشگیری از چنین جرم و جنایتی و برای ترویج همکاری به تناسب حال پیدا کنند.[۱] پس از آن شورای امنیت از دولت‌های عضو خواست با تبادل اطلاعات مربوط به استفاده گروه‌های تروریستی از فناوری ارتباطات و مخابراتی همکاری بین‌المللی را افزایش دهند.[۲] دستیابی به این همکاری به‌طور عملی دشوارتر از آن بود که تصور می‌شد (Archick, 2016: 8-9). با این حال سازمان در سال ۲۰۰۵ مشکل خاص تروریست‌هایی که به‌ویژه در عصر رسانه‌های پرطرفدار شبکه‌سازی اجتماعی همچون فیس‌بوک، تلگرام، توییتر، یوتوب، فلیکر و سکوهای وبلاگ‌سازی از اینترنت سوءاستفاده می‌شد و افرادی که خواسته یا ناخواسته مقدار بی‌سابقه‌ای از اطلاعات حساس را از طریق اینترنت انتشار دادند را اعلام کرد.

دولت‌های عضو سازمان ملل متحد وفق قطعنامه ۲۳۴۱ شورای امنیت مصوب سال ۲۰۱۷ و راهبرد جهانی مبارزه با تروریسم سازمان ملل متحد، بر اهمیت همکاری چندجانبه سازمان‌های بین‌المللی، منطقه‌ای و زیرمنطقه‌ای، بخش خصوصی و جامعه مدنی در قبال تهدیدهای ناشی از جرایم تروریستی در فضای دیجیتال، تأکید کردند، البته از دفتر مبارزه با تروریسم و سایر نهادهای مرتبط با پیمان هماهنگی جهانی مبارزه با تروریسم درخواست شد تا به‌طور مشترک از اقدام‌ها و رویکردهای نوآورانه برای ایجاد ظرفیت دولت‌های عضو، درصورت درخواست آن‌ها، برای مقابله این چالش‌ها حمایت کنند.[۳]

کمیته مبارزه با تروریسم شورای اروپا[۴] نشستی دیجیتالی با عنوان «مقابله با ارتباطات تروریستی: تبلیغات تروریستی، تحریک عمومی، استخدام و رادیکالیزه‌کردن[۵]» در محل شورای اروپا در سی‌ویکم ژانویه تا یکم فوریه ۲۰۲۳ برگزار کرد. این همایش بر سازوکارهای عملیاتی نظارت و مقابله با فعالیت‌های گروه‌های تروریستی به‌صورت برخط و غیربرخط، به‌ویژه تلاش‌های گروه‌های تروریستی برای عضوگیری و جلب حمایت در میان حوزه‌های مورد نظرشان و نیز آن‌هایی که با هدف ارائه ابزار و دانش لازم برای انجام فعالیت‌ها انجام می‌شوند، متمرکز بود.[۶]

با این همه، حقوق بین‌المللی در مورد فضای دیجیتال به سختی برای بازیگران دولتی مؤثر است و نیاز به درخواست‌های گسترده‌تری برای تدوین هنجارهای اینترنتی جهانی مبتنی‌بر قاعده، آزادی‌محور و فراگیر در آینده دارد. از آنجایی که جرایم دیجیتالی یک تهدید بزرگ برای همه کشورهای جهان است، باید اقدامات خاصی در سطح بین‌المللی برای پیشگیری از جرایم دیجیتالی انجام شود. باید عدالت کامل برای بزه‌دیدگان جرایم دیجیتالی با رویکرد تروریستی از طریق جبران خسارت و برخورد قاطع با متخلفان برقرار شود تا نمونه‌ای باشد تا بتواند مجرمان جرایم دیجیتالی را پیش‌بینی کند.

۳- رویکردها و سیاست‌گذاری‌های قانونی

یکی از چالش‌هایی که جامعه بشری را به‌گونه‌ای جدی با آثار ناشی بهره‌گیری غیرمجاز از آن در فضای مجازی و دیجیتالی مواجه ساخته، وجود جرایم تروریستی دیجیتالی است که

[1]- G.A. Res. 51 /210.
[2]- 6. S.C. Res. 1373, para. 3, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

[3]- https://www.un.org/counterterrorism/cybersecurity.
[4]- Council of Europe Committee on Counter-Terrorism (CDCT).
[5]- Digital Conference on "Countering Terrorist Communications: Terrorist Propaganda, Public Provocation, Recruitment and Radicalisation", 31 January to 1 February 2023.
[6]- https://www.coe.int/en/web/counter-terrorism/-/digital-conference-on-countering-terrorist-communications-terrorist-propaganda-public-provocation-recruitment-and-radicalisation.

فرصت‌های زیادی را برای مرتکبان آن فراهم آورده تا با ارتکاب آن، موقعیت و بستری را برای ورود آسیب جدی به زیرساخت‌ها و بسترهای اجتماعی، سیاسی و حتی امنیتی فراهم نماید. وفق این امر، جامعه جهانی و نیز برخی از کشورها به‌ویژه کشورهای اسلامی در این رابطه مبادرت به طراحی، تبیین و حتی تدوین و تصویب مقرراتی در پیشگیری و مقابله با جرایم تروریستی دیجیتالی در قلمرو حاکمیتی خود نموده‌اند که در ذیل سعی بر آن می‌شود تا ضمن مداقه در سیاست‌گذاری قانونی کشورهای اسلامی، ظرفیت حقوقی آن‌ها در قبال این دسته از جرایم فناورانه مورد سنجش قرار گیرد.

۳-۱- جمهوری عربی مصر

باتوجه به پیچیدگی روزافزون تهدیدهای دیجیتالی در سطح جهانی و ازجمله مصر، رعایت این مقررات مرتبط با این نوع از تهدیدها بسیار مهم است. شرکت‌های امنیت دیجیتالی در مصر نقشی اساسی در حصول اطمینان از اینکه کسب‌وکارها به‌نحو مطلوبی محافظت می‌شوند و با مقررات موجود مطابقت دارند، ایفا می‌کنند.[۱]

قانون‌گذار مصر براساس تصمیم شماره ۲ قانون مبارزه با تروریسم و در چهارچوب مفاد ماده ۲، اقدام تروریستی را چنین تعریف کرده است: «**اقدام تروریستی به معنای هرگونه استفاده از زور، خشونت، تهدید یا ارعاب در داخل یا خارج از کشور به‌منظور برهم‌زدن نظم عمومی است یا به خطرانداختن امنیت جامعه، ملت یا آسیب‌رساندن به افراد یا ایجاد رعب و وحشت در میان آن‌ها و همچنین هر رفتاری که به قصد دستیابی به یکی از اهداف مندرج در بند اول این ماده ارتکاب یابد؛ برای آنکه به ارتباطات، سیستم‌های اطلاعاتی، مالی یا بانکی یا اقتصادی، آسیب ایجاد نماید.**»

قانون‌گذار مصر تعریف اقدام تروریستی را به‌گونه‌ای گسترش داده است که رفتارهایی نظیر زور، خشونت، تهدید یا ارعاب برای دستیابی به اهداف تروریستی و همچنین تحریک و مشارکت شامل شده و موجبات ورود آسیب را به ارتباطات یا سیستم‌های اطلاعاتی ایجاد می‌کند. قانون‌گذار مصری همچنین هدف استفاده از ابزارهای تروریستی را با قراردادن اصطلاحات گسترده‌ای نظیر آسیب‌رساندن به وحدت ملی، صلح اجتماعی، امنیت ملی یا آسیب‌رساندن به محیط زیست و ... گسترش داد.

در اوت ۲۰۱۸، عبدالفتاح السیسی، رییس‌جمهور مصر قانون شماره ۱۷۵ سال ۲۰۱۸، «قانون مبارزه با جرایم سایبری و فناوری اطلاعات در مصر[۲]» را تصویب کرد. این قانون مشتمل بر چهار بخش، شامل بخش اول احکام کلی، بخش دوم احکام و آیین دادرسی، بخش سوم جرایم و مجازات‌ها و بخش انتهایی احکام پایانی است. درخصوص بخش جرایم و مجازات‌های قانونی باید اذعان داشت که شامل ۹ فصل است که به جرایم مختلف رخداده در فضای مجازی اینترنت می‌پردازد. هر فصل به موضوعات و جرایم مختلفی می‌پردازد، ازجمله موضوعاتی مانند نقض شبکه‌ها، سیستم‌ها و فناوری‌های اطلاعاتی، جرایم ارتکابی از طریق سیستم و فناوری‌های اطلاعاتی، کلاه‌برداری و تخلف در کارت‌های بانکی و روش‌های پرداخت الکترونیکی، جرایم مربوط به حساب‌ها و ایمیل‌های جعلی، جرایم مرتبط با آن. حریم خصوصی زندگی خصوصی و محتوای غیرقانونی، جرایم ارتکابی توسط مدیر وب‌گاه، ارائه‌دهنده خدمات، مسؤولیت کیفری مرتبط، عوامل تشدیدکننده جرایم، مسؤولیت کیفری شخصی قضایی، مجازات‌های فرعی و عوامل تخفیف‌دهنده.[۳]

قانون مزبور انتشار برخط اطلاعات در مورد نیروی ارتش و پلیس را ممنوع کرده و هک‌کردن سیستم‌های اطلاعاتی مربوطه را جرم‌انگاری می‌کند. در ضمن، این قانون ستون فقرات قانون جرایم سایبری در مصر را تشکیل می‌دهد. این قانون مجازات‌هایی را برای دسترسی غیرمجاز، نقض حریم خصوصی داده‌ها و سایر اشکال تخلف دیجیتالی مشخص می‌کند. هدف قانون ۲۰۲۰/۱۵۱ در مورد حفاظت از داده‌های شخصی[۴]، حفاظت از اطلاعات شخصی افراد، تعیین استاندارد

[1]- https://www.eg.andersen.com/cybersecurity-in-egypt/.

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

[3]- https://www.hg.org/legal-articles/anti-cyber-and-information-technology-crimes-law-in-egypt-48872.

[4]- Law No. 151 of 2020 Promulgating the Personal Data Protection Law.

جدیدی برای حفاظت از داده‌ها و تأثیر قابل توجهی بر امنیت دیجیتالی در مصر است.[۱] 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.[۲]

لازم به‌ذکر است ماده ۲ قانون اخیرالذکر شرکت‌های مخابراتی را ملزم می‌کند که داده‌های کاربران را به مدت ۱۸۰ روز نگهداری و ذخیره کنند تا به مقامات در شناسایی کاربران، فراداده‌ها و آدرس‌های آی‌پی رایانه کمک کنند. ماده ۴ این قانون، وزارتخانه‌های امور خارجه و همکاری‌های بین‌المللی را موظف می‌کند تا برای مسدودکردن برخی وب‌گاه‌ها در کشورهای خارجی، تا حد امکان با دولت‌های خارجی به توافق‌های دوجانبه در زمینه فناوری اینترنت و جرایم دیجیتالی و حتی با رویکردهای تروریستی دست یابند. ماده ۷ به مقامات تحقیق این اختیار را می‌دهد که هر وب‌سایتی را هر زمان که فکر کنند محتوای وب‌گاه‌ها ایده‌های افراطی را تبلیغ نموده و امنیت ملی را نقض می‌کند یا به اقتصاد مصر آسیب می‌رساند، مسدود کند.[۳]

۳-۲- سلطان‌نشین عمان

قانون‌گذار عمان با فرمان شماره ۷۲ سال ۲۰۰۱ قانون مجازات عمان را اصلاح کرده است و براساس این اصلاحیه، مجموعه‌ای از اقداماتی که رایانه در معرض آن قرار می‌گیرد، ازجمله ورود غیرقانونی به سیستم‌های رایانه‌ای، جرم‌انگاری شده است و داده‌های محتوای آن نیز همان‌گونه که در ماده ۲۷۶ مکرراً در مورد نتیجه داده‌های متعلق به دیگران مجازات شده است، مجازات می‌شود. این در حالی است که باتوجه به تحولات تقنینی صورت‌گرفته در سلطان‌نشین عمان، در سال ۲۰۱۸ قانون مجازات دستخوش تغییر و تحولات قابل ملاحظه‌ای شد.[۴] در ماده ۱۳۲ قانون مجازات عمان آمده است: «**اقدامی تروریستی است که با استفاده از مواد سمی، مواد منفجره یا هر وسیله‌ای که منجر به ایجاد خطر عمومی شود، اطلاق می‌گردد. مادام که خرابکاری در یک مکان عمومی یا خصوصی رخ دهد و حالت وحشت ایجاد کند، موجب تشدید مجازات است.**»

سلطان‌نشین عمان کنوانسیون عربی برای مبارزه با تروریسم ازجمله مقابله با جرایم تروریستی دیجیتالی را با فرمان شماره ۵۵/۹۹ در سال ۱۹۹۹ تصویب کرد. به‌علاوه، «قانون جرایم سایبری سلطان‌نشین عمان» با فرمان سلطنتی به‌شماره ۲۰۱۱/۱۲ صادر شده است.[۵] تدوین این قانون عصر جدیدی را برای عمان آغاز می‌کند؛ جایی که یک جامعه واقعاً فعال الکترونیکی در تحقق جامعه دیجیتالی سلطان‌نشین تکامل می‌یابد. این یک نقطه عطف بزرگ در اجرای راهبرد ملی فناوری اطلاعات توسط سازمان فناوری اطلاعات عمان است.[۶]

لازم به‌ذکر است این قانون جرم دیجیتال را در یک تعریف صریح به‌عنوان استفاده عملی از محاسبات و الکترونیک و ارتباطات برای پردازش و توزیع داده‌ها و اطلاعات در کلیه اشکال آن تعریف می‌کند و جرایم دیجیتالی را جرایمی تعریف می‌کند که در قانون امنیت سایبری که توسط فرمان سلطنتی برای این کشور ابلاغ شده است، البته باید اذعان شود قانون‌گذار عمان با روزآمدسازی مقررات که با انواع جرایم و به‌ویژه جرایم دیجیتالی و اطلاعاتی مبارزه می‌کند، توانسته است با توسعه تمدن و چالش‌های نوین مقابله کند (Salim Alshibli, 2021: 89).

---

[۱]- قانون مبارزه با جرایم سایبری و فناوری اطلاعات مصر برای ایمن‌سازی فضاهای دیجیتالی طراحی شده است، اما پیامدهای مستقیمی برای حاکمیت شرکتی نیز دارد. اکنون شرکت‌ها ملزم به اتخاذ پروتکل‌های سختگیرانه مدیریت داده و امنیت دیجیتالی برای پیشگیری از مجازات هستند. از سوی دیگر، قانون شرکت‌های مصر (شماره ۱۵۹ در سال ۱۹۸۱) و قانون سرمایه‌گذاری (شماره ۷۲ سال ۲۰۱۷) چهارچوب قانونی را برای عملیات تجاری، ازجمله ابعاد راجع به مدیریت داده‌ها، مالکیت معنوی و رفتار برخط تعیین می‌کند.

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

[3]- https://www.loc.gov/item/global-legal-monitor/2018-10-05/egypt-president-ratifies-anti-cybercrime-law/.

[4]- 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.

[5]- 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.

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

۳-۳- پادشاهی اردن

قانون اردن تعریف روشن و جامعی از جرایم دیجیتال در قانون اردن اعمال نکرده است، بلکه تنها به اشکال جرایم دیجیتالی مشمول قانون جرایم الکترونیکی اردن برای سال ۲۰۱۵ اشاره می‌کند؛ جایی که قانون اردن برخی از جنبه‌های تجاوز به ایمنی را پوشش می‌دهد.[۱] این قانون همچنین به برخی از موارد تخلف از کارت‌های اعتباری و جرایم تهمت، افترا و اهانت به‌همراه برخی از امور مربوط به مراحل تحقیقات کیفری اشاره کرده است. قانون اردن تنها از طریق ماده ۱۲ به جرایم دیجیتالی می‌پردازد که به ضرر یکی از منافع خارجی پادشاهی انجام می‌شود، جایی که قانون مجازات را بدون مشخص‌کردن چهارچوب‌های مرزهای جغرافیایی بیان می‌کند.

افزون بر این، ماده ۶ این قانون مقرر می‌دارد که: «**مجازات را برای هر کسی که داده‌ها یا اطلاعات مربوط به کارت‌های اعتباری، تراکنش‌های مالی یا بانکداری الکترونیکی را به‌طور غیرقانونی به‌دست آورده یا از آن‌ها استفاده کند، تعیین کرده است**» (Romman, 2017: 14-16).

با این همه، قانون‌گذار اردن با تصویب مقرره‌های فوق‌الذکر درصدد مقابله با جرایم دیجیتالی و به‌ویژه جرایم تروریستی در فضای دیجیتالی بوده است.

۳-۴- امارات متحده عربی

امارات متحده عربی در خط مقدم اتخاذ اقدامات قاطع و پیشگیرانه برای مهار شیوع جرایم دیجیتالی به‌ویژه با رویکردهای تروریستی در منطقه بوده است. راهبرد و موفقیت در مبارزه با جرایم دیجیتالی در منطقه در گرو تصویب مقررات جامع و کارآمد با مجازات‌های سخت‌گیرانه است. ازاین‌رو، در چهارچوب مقررات امارات متحده عربی جرایم 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 ... است، البته توزیع ویروس‌ها، دانلود غیرقانونی فایل‌ها، فیشینگ و سرقت شخصی نیز در شمار این جرایم قرار دارند.[۲]

بر این اساس، قانون فدرال (۲) امارات متحده عربی در سال ۲۰۰۶ درخصوص مبارزه با جرایم فناوری اطلاعات که چهارچوب قانونی مبارزه با جرایم دسترسی غیرقانونی به سیستم اطلاعاتی است، صادر شد.

همچنین طبق ماده ۲ فرمان فدرال ایالتی فدرال قانون شماره ۱ ۲۰۰۴ در مورد مبارزه با جرایم 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, 2023: 114-116). با هدف ایجاد رعب و وحشت در بین مردم، ارعاب آن‌ها، یا برهم‌زدن نظم عمومی، به خطرانداختن ایمنی جامعه، آسیب‌رساندن به محیط زیست یا تأسیسات عمومی یا خصوصی یا قراردادن یک منبع طبیعی در معرض خطر.

۳-۵- عربستان سعودی

ساختار مبارزه با جرایم اطلاعاتی در عربستان سعودی ایجاد شد که هدف آن کنترل تراکنش‌های الکترونیکی و جرم‌انگاری تجاوز یا حمله الکترونیکی است. از طریق وسایل الکترونیکی، دسترسی غیرمجاز عمدی به سیستم‌های

---

[۱]- این موارد شامل محرمانه‌بودن و در دسترس‌بودن داده‌ها و اطلاعات الکترونیکی و سیستم‌های رایانه‌ای، علاوه‌بر برخی از انواع جرایم محتوایی مربوط به هرزه‌نگاری و فحشا است.

[۲]- جرایم دیجیتال در قلمرو مقررات امارات متحده عربی به پنج دسته طبقه‌بندی کرد؛ ۱- جرایم اقتصادی: جرایم اقتصادی دیجیتال اغلب جرایم بسیار سازمان‌یافته‌ای هستند که از پیشرفته‌ترین فناوری‌ها و ابزارها برای ارتکاب چنین جنایاتی، اغلب از طریق هک، استفاده می‌کنند. ۲- جرایم تروریستی: حمله دیجیتال اصطلاحی به‌عنوان یک جرم تروریستی است که علیه منافع یک کشور، به‌ویژه زیرساخت‌ها، اقتصاد، منابع و ... آن کشور هدف قرار گیرد. ۳- کنش‌گرایی: «ویکی لیکس» نمونه درستی برای نمایش یک جرم دیجیتال فعال است که در آن هک‌کردن در راستای پیشبرد یک برنامه ایده‌آلیستی انجام می‌شود. ۴- جاسوسی: این می‌تواند شامل جاسوسی شرکتی و سیاسی باشد. در جایی که مجرم تلاش می‌کند تا اطلاعات محرمانه، اسرار تجاری محافظت شده و سایر حقوق مالکیت معنوی را برای به‌دست‌آوردن مزیت تجاری یا سیاسی به دست آورد. ۵- جنگ دیجیتال: جنگ دیجیتال شامل اقدام یک سازمان خصوصی یا بین‌المللی است که تلاش می‌کند با هدف قراردادن شبکه اطلاعاتی یا سیستم رایانه‌ای به کشور دیگری به‌طور فعال آسیب برساند یا به آن حمله کند (Elhais, 2021: 1).

رایانه‌ای را جرم می‌داند و تجاوز به حقوق دیگران است. ازاین‌رو، پادشاهی عربستان سعودی توجه زیادی به مبارزه با جرایم دیجیتالی البته با رویکردهای تروریستی داشته است، زیرا «کنوانسیون عربی برای مبارزه با جرایم فناوری اطلاعات[۱]» در سال ۲۰۱۲ را تصویب کرد[۲] که مفاد آن گروهی از جرایم تروریستی دیجیتالی نظیر گسترش افکار تروریستی، تأمین مالی گروه‌های تروریستی و تسهیل را از بین می‌برد (Mohamed & Elamin, 2013: 17).

قانون اخیر به افزایش جرایم الکترونیکی می‌پردازد که شامل جرایمی مانند کلاه‌برداری از کارت اعتباری، جرایم اینترنتی، جرایم تروریستی دیجیتالی، ایجاد و/یا توزیع ویروس‌ها، هک، تداخل در سیستم، دسترسی غیرقانونی و رهگیری و ... می‌شود. همچنین هدف آن تشویق همکاری بین کشورهای عربی در مبارزه با جرایم دیجیتالی با رویکرد تروریستی است.[۳]

نتیجه‌گیری

جرایم دیجیتالی با جرایم سنتی متفاوت می‌باشد؛ فراتر از مرزهای زمانی و مکانی هر کشوری، قانون‌گذاران را بر آن می‌دارد تا مقررات نظارتی را برای تعیین قوانین به‌منظور برخورد با این جرایم و پیامدهای آن در نظر بگیرند. ازاین‌رو، جرایم تروریستی دیجیتالی به یک تهدید تبدیل شده و کل جهان را در معرض تهدید تروریستی از طریق اینترنت قرار داده است و این امر موجب شده تا فناوری مدرن به‌تنهایی قادر به محافظت از مردم در برابر جرایم تروریستی دیجیتالی نباشد.

جرایم تروریستی دیجیتالی یکی از انواع جرایم اطلاعاتی در نظر گرفته می‌شود، زیرا به‌شکل میدان یا دامنه‌ای است که یک عمل تروریستی در آن انجام می‌شود یا ابزاری است که می‌توان از آن برای انجام یک جرم تروریستی استفاده کرد. یکی از علل بروز جرایم تروریستی دیجیتالی، ظهور فناوری دیجیتالی است که به‌دلیل دشواری نظارت بر اینترنت یا پاسخگویی به آنچه منتشر می‌شود، وقوع جرم مزبور را موجب می‌گردد.

جرم تروریستی دیجیتالی به‌مثابه یک جرم عمدی است؛ بنابراین نمی‌توان تصور کرد که به اشتباه رخ داده باشد. بنابراین تروریست‌ها از ابزارهای دیجیتالی نظیر اینترنت، دستگاه‌های هوشمند و ... به‌منظور ترویج باورهای خود، ارسال پیام‌های تهدیدآمیز، برنامه‌ریزی، تأمین مالی، جمع‌آوری اطلاعات و هک حساب‌ها استفاده می‌کنند که برای مواجهه با این وضعیت باید برنامه‌ها و سیستم‌های لازم برای حفاظت از فضای مجازی و تشخیص زودهنگام در زمان ارتکاب جرایم تروریستی دیجیتالی فراهم شود.

البته آموزش کلیه اقشار جامعه از طریق رسانه‌های همگانی در مورد جدی‌بودن این دسته از جرایم در فضای دیجیتال از مسائل ضروری است که باید از سوی نهادهای مسؤول مانند دانشگاه‌ها و مراکز آموزشی و نیز رسانه‌ها به مخاطبان انعکاس یابد، به‌علاوه، توسعه لازم برای نظارت، ایجاد و تنظیم تارنماها، به‌ویژه تارنماهایی که برای انتشار اطلاعات و ایده‌های سمی و مخرب مورد استفاده قرار می‌گیرند و در خدمت اهداف تروریستی هستند، صورت پذیرد.

آموزش دادرسان، مقامات تحقیق و پلیس در زمینه برخورد با رایانه و اینترنت از مهم‌ترین راهبردهایی است که باید از سوی دولت‌ها برای ایجاد حکمرانی دیجیتالی صورت گیرد، البته ضرورت همکاری و هماهنگی بین کشورها در زمینه مقابله با این جرایم و تدوین مقررات حقوقی برای کنترل، بازرسی و نظارت بر مبادلات دیجیتالی، امری انکارناپذیر به‌شمار می‌آید.

ملاحظات اخلاقی: در این پژوهش تمامی ملاحظات اخلاقی رعایت گردیده است.

تعارض منافع: نگارش این مقاله، فاقد هرگونه تعارض منافعی بوده است.

---

[1]- Arab Convention on Combating Information Technology Offences, https://www.asianlaws.org

[۲]– هدف این معاهده بهبود همکاری بین کشورهای عربی در زمینه مبارزه با جرایم فناوری اطلاعات برای حفاظت از امنیت و منافع کشورهای عربی و امنیت جوامع و افراد آن‌هاست. این معاهده جرایم مربوط به فناوری اطلاعات، مقررات رویه‌ای و سازوکارهای همکاری حقوقی و قضایی بین دولت‌های عضو را تشریح می‌کند. در ضمن از دیگر اهداف آن، تقویت و تقویت همکاری بین کشورهای عربی در زمینه مبارزه با جرایم فناوری اطلاعات به‌منظور دفع تهدیدات این‌گونه جنایات به‌منظور حفظ امنیت و منافع کشورهای عربی و امنیت جوامع آن‌هاست.

[3]- https://www.sabaip.com/saudi-arabia-arab-cybercrime-greement-approved/.

سهم نویسندگان: نگارش مقاله مشترکاً توسط نویسندگان انجام گرفته است.

تشکر و قدردانی: لازم است از تمام کسانی که در تدوین این مقاله ما را یاری رسانده‌اند، قدردانی نماییم.

تأمین اعتبار پژوهش: این پژوهش بدون تأمین مالی انجام گرفته است.

منابع و مآخذ

الف. منابع فارسی و عربی

– السند، عبدالرحمن (۲۰۰۴). *الأحکام الفقهیه للتعاملات الإلکترونیه*. ریاض: دار الوراق للنشر و التوزیع.

– عبدالفتاح مطر، عصام (۲۰۰۵). *الجرمیه الإرهابیه*. الإسکندریه: دار الجامعه الجدیده للنشر.

– موسوی، سیدجمال؛ روحانی‌مقدم، محمد و آقائی بجستانی، مریم (۱۴۰۱). «تدابیر پیشگیری از جرایم سایبری با تأکید بر اقدامات پلیسی با رویکردی فقهی». *مطالعات فقه و حقوق اسلامی*، ۱۴(۲۶): ۳۲۳–۳۵۸.

– یزدان‌پناه‌درو، کیومرث و جعفری، مهتاب (۱۳۹۷). «تحلیل ژئوپلیتیک اثرگذاری اینترنت در افزایش فعالیت تروریسم: با تأکید بر داعش». *پژوهش‌های راهبردی سیاست*، ۷(۲۶): ۲۲۱–۲۴۴.

ب. منابع انگلیسی

- Alyammahi, MS & Shakib Bin Mohd Noor, S (2023). “Cybercrimes in the United Arab Emirates: Characteristics and Countermeasures”. *International Journal of Academic Research in Public Policy and Governance*, 9(1): 108-122.

- Archick, K (2016). *U.S.-E.U. Cooperation Against Terrorism*. Congressional Research Service, p.1-35.

- Buresh, DL (2020). “Does Digital Terrorism Really Exist?”. *Journal of Advanced Forensic Sciences*, 1(1): 18-29.

- Corliss, C (2023). “Digital Terror Crimes”. *Columbia Journal of Transnational Law*, 62(13): 58-112.

- Dupont, B & Holt, T (2022). “The Human Factor of Cybercrime”. *Soc Sci Comput Rev*, 40(4): 860-864.

- Elhais, H (2021). *New Updates on How UAE Combats Cybercrime: Punishments and Penalties*. https://www.linkedin.com/pulse/new-updates-how-uae-combats-cybercrime-punishments-penalties-elhais.

- Golose, RP (2022). “A Comparative Analysis of the Factors Predicting Fears of Terrorism and Cyberterrorism in a Developing Nation Context”. *Journal of Ethnic and Cultural Studies*, 9(4): 106-119.

- Kapu, S (2021). “Triangle of Cyber, Terrorism and Radicalization”. *Cyberpolitik Journal*, 6(11): 48-58.

- Lee, CS; Choi, KS; Shandler, R & Kayser, C. (2021). “Mapping Global Cyberterror Networks: An Empirical Study of Al-Qaeda and ISIS Cyberterrorism Events”. *Journal of Contemporary Criminal Justice*, 37(3): 333-355.

- Mohamed, B & Elamin, B (2013). “Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future”. *Journal of Information & Knowledge Management*, 3(12): 14-18.

- Romman, A (2017). “A Comparative Study between the Jordanian and Omani Digital Crimes Law”. *Journal of Information Security*, 8: 8-22.

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

- Shaweorcid, R & McAndrew, IR (2023). “Cybersecurity and Domestic Terrorism: Purpose and Future”. *Journal of Software Engineering and Applications*, 16(10): 548-560.

- Taylor, RE; Fritsch, EJ & Liederbach, J (2019). *Digital Crime and Digital Terrorism*. 3rd ed, London: Pearson Publications.

- Weimann, G (2014). *New Terrorism and New Media*. Washington, DC: Woodrow Wilson Center Press.

- Yüksel, C (2020). “Combating Terrorist Use of the Internet and Social Media: Recommended Solutions within the Scope of International Law”. *Public and Private International Law Bulletin*, 40(2): 1089-1112.