Received: 12 /04/2026
Review: 17/05/2026
Accepted: 08 /06/2026
DOI: 10.22054/jocl.2025.8563. 49714

Journal of Cyber Law
No(3),Vol(1), 22-41.
ISSN: 0972-6934
www.jocl.ir

Criminal Prevention of Online Terrorism Against Public Health Rights in the UK Legal System

Peyman Namamian [1*]

1*- Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran

ABSTRACT

In the English legal system, online criminal counter-terrorism emerges as a fundamental legal and policy issue in light of emerging threats to public health rights. This research examines how cyberattacks against healthcare infrastructure, as well as the organized dissemination of misinformation during health crises, cause individual-level anxiety, distrust in scientific treatments, and undermine citizens' psychological security. At the institutional level, it assesses the effectiveness and challenges of implementing regulations such as the "Terrorism Act 2000," the "Computer Misuse Act 1990," and the "Online Safety Act 2023" in preventing, identifying, and containing these threats, while also maintaining a balance between public security and fundamental rights, including privacy and freedom of information. At the international level, it addresses the necessity of continuous review of legal frameworks, strengthening regulatory coordination, and expanding transnational cooperation to counter terrorists' exploitation of digital technologies and effectively protect public health. Accordingly, this study, employing a descriptive-analytical method, identifies existing challenges and gaps in online criminal counter-terrorism and elucidates the necessary legal and institutional solutions to enhance effective oversight, reduce psychological and social consequences, and safeguard public health rights.

Keywords:
Online Terrorism, Violation of Public Health Rights, Legal Protections, Psychological Harm, Online Surveillance, Legal System of the United Kingdom.

Article Type:Research Article

How to Cite: Namamian,P . (2026). Criminal Prevention of Online Terrorism Against Public Health Rights in the UK Legal System. *Journal of Cyber Law (JOCL)*, 3(1), 22-41. doi: 10.22054/jocl.2025.8563.49714

)Corresponding Author: p-namamian@araku.ac.ir

نشریه حقوق سایبری
شماره (۱) ۴۱-۲۲
دوره ۱۴۰۵

تاریخ دریافت: ۱۴۰۵/۰۱/۲۳
تاریخ اصلاح: ۱۴۰۵/۰۲/۲۷
تاریخ پذیرش: ۱۴۰۵/۰۳/۱۸

پیشگیری کیفری از تروریسم برخط علیه حقوق سلامت عمومی در نظام حقوقی انگلستان

پیمان نمامیان [1*]

۱- دانشیار حقوق کیفری و جرم شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران

چکیده

در نظام حقوقی انگلستان، پیشگیری کیفری از تروریسم برخط در پرتو تهدیدهای نوظهور علیه حقوق سلامت عمومی به‌عنوان یک مسأله بنیادین حقوقی و سیاست‌گذاری مطرح است. این پژوهش بررسی می‌کند که چگونه حملات سایبری علیه زیرساخت‌های مراقبت‌های بهداشتی و نیز اشاعه سازمان‌یافته اطلاعات نادرست در بحران‌های بهداشتی، در سطح فردی موجب اضطراب، بی‌اعتمادی به درمان‌های علمی و تضعیف امنیت روانی شهروندان می‌شود؛ در سطح نهادی، کارآمدی و چالش‌های اجرای مقرراتی نظیر «قانون تروریسم ۲۰۰۰»، «قانون سوءاستفاده از رایانه ۱۹۹۰» و «قانون ایمنی برخط ۲۰۲۳» در پیشگیری، شناسایی و مهار این تهدیدات و نیز حفظ توازن میان امنیت عمومی و حقوق بنیادین از جمله حریم خصوصی و آزادی اطلاعات ارزیابی می‌گردد؛ و در سطح بین‌المللی، ضرورت بازنگری مستمر در چارچوب‌های قانونی، تقویت هماهنگی مقرراتی و گسترش همکاری‌های فراملی برای مقابله با بهره‌برداری تروریست‌ها از فناوری‌های دیجیتال و حفاظت مؤثر از سلامت عمومی مورد توجه قرار می‌گیرد. بر این اساس، پژوهش حاضر با بهره‌گیری از روش توصیفی ـ تحلیلی، ضمن شناسایی چالش‌ها و شکاف‌های موجود در پیشگیری کیفری از تروریسم برخط، راهکارهای حقوقی و نهادی لازم برای ارتقای نظارت مؤثر، کاهش پیامدهای روانی و اجتماعی و صیانت از حقوق سلامت عمومی را تبیین می‌کند.

کلیدواژه‌ها:

تروریسم برخط، نقض حقوق سلامت عمومی، حمایت‌های حقوقی، آسیب‌های روانی، نظارت برخط، نظام حقوقی انگلستان.

نوع مقاله: پژوهشی

نحوه استناد:

نمامیان،پیمان . (۱۴۰۵). پیشگیری کیفری از تروریسم برخط علیه حقوق سلامت عمومی در نظام حقوقی انگلستان. حقوق سایبری، ۳(۱)، ۲۲-۴۱.

[1*] ایمیل نویسنده مسئول: p-namamian@araku.ac.ir

۱. مقدمه

در ۲۶ ژانویه ۲۰۲۴، سازمان بهداشت جهانی طی گزارشی پیرامون واکنش به «بزهکاری برخط»[1] و ضرورت اتخاذ سیاست‌های مراقبتی در نظام‌های بهداشتی، به وجود خطرات نوظهور امنیت سلامت ناشی از تروریسم سایبری علیه زیرساخت‌های مراقبت بهداشتی و گسترش اطلاعات نادرست اذعان کرد.[2] این گزارش با تمرکز بر نقش اطلاعات نادرست در دوره‌های همه‌گیری و چگونگی بهره‌برداری از سازوکارهای شناختی مخاطبان، به تحلیل ابعاد مختلف این تهدیدات پرداخته است.[3] به‌علاوه، شناسایی عوامل محرک بی‌اعتمادی در جوامع می‌تواند نقش مؤثری در بهبود راهبردهای مقابله با اطلاعات نادرست ایفا نماید.[4] بنابراین، ارتکاب فعالیت‌های مجرمانه‌ای نظیر «تروریسم برخط»[5] به‌مثابه بزهکاری برخط تهدیدات جدی برای حقوق سلامت عمومی به‌همراه دارند. این تهدیدات شامل حملات سایبری به زیرساخت‌های بهداشتی[6]، انتشار اطلاعات نادرست در بحران‌های بهداشتی که موجب ایجاد ترس و اضطراب عمومی می‌شود، و انتشار دستورالعمل‌های ساخت مواد سمی یا بیولوژیک است(Pavlova, 2020: 398). سرعت بالای انتشار اطلاعات نادرست در فضای برخط و ضرورت حفظ تعادل میان نظارت امنیتی و رعایت حقوق فردی، از چالش‌های اساسی در مقابله با این تهدیدات به‌شمار می‌روند.[7] این دسته از فعالیت‌های برخط، تهدیداتی جدی برای سلامت عمومی و صحت اطلاعات بهداشتی ایجاد کرده است و نیاز به واکنش‌های قانونی مؤثر دارد. از اینرو، آماج‌های موجود به زیرساخت‌های مراقبت بهداشتی می تواند خدمات درمانی را مختل کرده و جان بیماران را تهدید کند. در ضمن، انتشار اطلاعات نادرست در بحران‌های بهداشتی موجب ایجاد ترس، اضطراب عمومی و کاهش اعتماد به واکسن‌ها و درمان‌های علمی می‌شود(Denniss, & Lindberg, 2025: 6-8). با این همه، پیشگیری کیفری از

---

[1] Online Crime

[2] سازمان بهداشت جهانی با همکاری اینترپل و سایر نهادهای بین‌المللی (نظیر *دفتر مبارزه با مواد مخدر و جرم سازمان ملل متحد، دفتر مبارزه با تروریسم سازمان ملل متحد، مرکز محاسبات بین‌المللی سازمان ملل متحد، مؤسسه تحقیقات جرم و عدالت بین منطقه‌ای سازمان ملل متحد و مؤسسه صلح سایبری*)، دو گزارش را در تاریخ ۲۶ ژانویه ۲۰۲۴ منتشر کرده است که به بررسی خطرات سایبری و اطلاعات نادرست در حوزه بهداشت می‌پردازند. گزارش نخست، تأثیر حملات سایبری بر زیرساخت‌های مراقبت بهداشتی در دوران همه‌گیری کووید-۱۹ را مورد بررسی قرار می‌دهد؛ حملاتی که منجر به اختلال در ارائه خدمات بهداشتی و پرداخت باج‌های سنگین توسط مراکز بهداشتی شد. گزارش دوم، به چالش‌های مقابله با اطلاعات نادرست در شرایط اضطراری بهداشتی، هم‌چون بحران کووید-۱۹، می‌پردازد و بر این نکته تأکید دارد که اطلاعات نادرست، برخلاف اخبار غلط، به‌طور عمده با هدف ایجاد تفرقه و بی‌اعتمادی در میان نهادهای مختلف منتشر می‌شود؛

- World Health Organization. (2024, February 6). *WHO reports outline responses to cyber-attacks on health care and the rise of disinformation in public health emergencies*. WHO. https://www.who.int/news/item/06-02-2024-who-reports-outline-responses-to-cyber-attacks-on-health-care-and-the-rise-of-disinformation-in-public-health-emergencies

[3] https://iris.who.int/bitstream/handle/10665/375831/WER9904-25-37.pdf?sequence=1&isAllowed=y

[4] https://iris.who.int/bitstream/handle/10665/375832/WER9904-38-48.pdf

[5] Online Terrorism

[6] زیرساخت‌های مراقبت بهداشتی در انگلستان شامل خدمات و منابع حیاتی برای ارتقای سلامت عمومی است، از جمله «خدمات بهداشت ملی»، مؤسسات بهداشتی، برنامه‌های پیشگیرانه و دسترسی به آب شرب سالم و سیستم‌های فاضلاب. ارائه این خدمات تحت چارچوب قانونی خاصی، از جمله «قانون بهداشت و مراقبت اجتماعی، مصوب ۲۰۱۲»، و تحت نظارت سازمان‌هایی مانند «کمیسیون کیفیت مراقبت» قرار دارد. دسترسی به خدمات بهداشتی به عنوان یک حق اساسی برای شهروندان شناخته می‌شود و نظارت بر نیروی انسانی متخصص و تدوین سیاست‌های بهداشتی از طریق مجموعه‌ای از قوانین و مقررات انجام می‌گیرد؛

- British Medical Association. (2024, June 28). *Building the future: Healthcare infrastructure reports*. https://www.bma.org.uk/advice-and-support/nhs-delivery-and-workforce/the-future/building-the-future-healthcare-infrastructure-reports

[7] https://www.pewresearch.org/internet/2017/10/19/the-future-of-truth-and-misinformation-online/

تروریسم برخط، باید توازنی میان امنیت عمومی و حفاظت از حقوق فردی برقرار کند. نظارت بی‌مورد و محدودیت‌های نامتناسب می‌تواند حقوق بشر و حریم خصوصی را نقض کند.

در نظام حقوقی انگلستان، حقوق دسترسی به خدمات بهداشتی، تحت «مقررات خدمات سلامت ملی و بهداشت عمومی، مصوب ۲۰۱۳»[1] قرار می گیرد و شامل اقدامات پیشگیرانه و حفاظتی برای محافظت از سلامت جامعه است. انگلستان به‌منظور شناسایی و تعقیب تروریسم برخط، تلاش می کند از طریق مقررات کیفری اقدام نماید، در حالی که به حفظ حریم خصوصی و پیشگیری از نقض حقوق بشر اهمیت می‌دهد(Chang, 2018: 143). در این چارچوب، همکاری‌های بین‌المللی و بهره گیری از ابزارهای قانونی برای پیشگیری و بازدارندگی از تهدیدات آینده در اولویت قرار دارد(کریمی و نیک‌روش، ۱۴۰۳: ۷۶-۷۴). هدف اصلی این رویکرد، حفاظت از سلامت عمومی و حقوق افراد در قبال آثار منفی تروریسم برخط است. بنابراین، نقض حقوق سلامت عمومی به‌واسطه تروریسم برخط که می‌تواند مشتمل بر دسترسی ناکافی به خدمات بهداشتی یا انتشار اطلاعات نادرست در بحران‌های بهداشتی باشد، تحت مقررات گوناگونی نظیر «قانون بهداشت عمومی (کنترل بیماری)، مصوب ۱۹۸۴»[2] قرار می گیرند. پیشگیری کیفری از این تهدیدات، که منجر به نقض حقوق سلامت عمومی خواهد شد، به معنای پاسخگو بودن فرد یا سازمان در قبال تروریسم برخط در چارچوب نظام حقوقی انگلستان است. پیشگیری کیفری شامل مجازات‌ها و اقدامات قانونی برای مقابله با تروریسم برخط و مستلزم اجرای مقرراتی نظیر «قانون عدالت کیفری، مصوب ۱۹۸۸»[3] و «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰»[4]، است. بنابراین، باید اذعان داشت در انگلستان پیشگیری کیفری از تروریسم برخط به‌منظور حفظ سلامت عمومی و حقوق فردی امری ضروری است. حملات سایبری به زیرساخت‌های مراقبت بهداشتی می‌تواند منجر به اختلال در خدمات درمانی و تهدیدی جدی برای سلامت عمومی گردد. علاوه بر این، در شرایط بحران‌های بهداشتی، انتشار اطلاعات نادرست می‌تواند موجب ایجاد اضطراب عمومی و تضعیف اعتماد به نظام‌های بهداشتی شود. که بر این اساس، پیشگیری کیفری در راستای مقابله با این تهدیدات و پیشگیری از تشدید بحران‌ها ضرورتی انکارناپذیر است.

این پژوهش با رویکردی مسأله‌محور و در چارچوبی چندسطحی، با بهره‌گیری از روش توصیفی–تحلیلی، به بررسی کارآمدی پیشگیری کیفری در نظام حقوقی انگلستان در مواجهه با تروریسم برخط و پیامدهای آن بر حقوق سلامت عمومی می‌پردازد. در این راستا، آثار تروریسم برخط بر سلامت روانی، احساس امنیت اجتماعی و حق شهروندان در برخورداری از محیط اطلاعاتی سالم و ایمن مورد توجه قرار می گیرد؛ البته، کارآمدی سازوکارهای حقوقی و اجرایی و نیز چالش‌های ناشی از اجرای مقرراتی نظیر قانون تروریسم[5](مصوب ۲۰۰۰) و قانون ایمنی برخط[6](مصوب ۲۰۲۳) در فرآیند پیشگیری، شناسایی و مقابله با این تهدیدات در راستای حمایت از سلامت عمومی تحلیل می‌شود؛ در قلمرو بین‌المللی، ضرورت بازنگری در سیاست‌های حقوقی، تقویت همکاری‌های فراملی و هماهنگی میان دولت‌ها و نهادهای

---

[1] The National Health Service and Public Health (Functions and Miscellaneous Provisions) Regulations 2013, UK Statutory Instruments 2013 No. 261. (2013). Retrieved from https://www.legislation.gov.uk/uksi/2013/261

[2] Public Health (Control of Disease) Act 1984, UK Public General Acts 1984 c. 22. Retrieved from https://www.legislation.gov.uk/ukpga/1984/22

[3] Criminal Justice Act 1988, UK Public General Acts 1988 c. 33. Retrieved from https://www.legislation.gov.uk/ukpga/1988/33/contents

[4] Computer Misuse Act 1990, UK Public General Acts 1990 c. 18. Retrieved from https://www.legislation.gov.uk/ukpga/1990/18/contents

[5] Terrorism Act 2000, https://www.legislation.gov.uk/ukpga/2000/11/contents

[6] Online Safety Act 2023, https://www.legislation.gov.uk/ukpga/2023/50

ذی‌ربط برای مقابله مؤثر با تروریسم برخط و کاهش پیامدهای روانی و اجتماعی ناشی از آن مورد بررسی قرار می‌گیرد. بر این اساس، پژوهش حاضر می‌کوشد به این مسأله پاسخ دهد که پیشگیری کیفری از تروریسم برخط چگونه می‌تواند در حمایت از حقوق سلامت عمومی مؤثر واقع شود و اجرای مقررات مرتبط در این حوزه با چه چالش‌های حقوقی، نهادی و بین‌المللی مواجه است.

۱. پیشینه و تحولات حقوقی

با گسترش اینترنت و فناوری‌های دیجیتال، تروریست‌ها به‌سرعت از این بستر برای تبلیغ اندیشه‌ها، جذب نیرو و برنامه‌ریزی حملات بهره‌برداری کردند(نمامیان، ۱۴۰۴: ۸). در پی این تحولات، انگلستان با توجه به تغییرات سریع در فناوری‌های نوین، ضرورت طراحی پیشگیری کیفری نوین از تروریسم برخط را شناسایی کرد. این رویکرد در همان آغاز تحولات با تصویب «قانون تروریسم، مصوب ۲۰۰۰» به‌طور رسمی اتخاذ شد. توجه به تروریسم برخط از اوایل دهه ۲۰۰۰، مقامات انگلستان را به چالش کشید و مسائل نوینی در زمینه تروریسم و حقوق عمومی مطرح کرد. تهدیدات ناشی از چنین فعالیت‌هایی می‌توانند زیرساخت‌های مراقبت بهداشتی و خدمات عمومی را هدف قرار دهند و تأثیرات جدی بر سلامت عمومی وارد کنند. به‌این‌ترتیب، قانون تروریسم مصوب ۲۰۰۰، با تمرکز بر استفاده از اینترنت برای ترویج خشونت و انتشار پیام‌های تروریستی، پیشگیری کیفری از این تهدیدات فراهم کرد. افزون بر این، قانون‌گذار انگلستان در پیشگیری کیفری از نگرانی‌های فزاینده ناشی از تهدیدات و تروریسم برخط مبادرت به تصویب مقرراتی نظیر «قانون ضدتروریسم، جنایت و امنیت، مصوب ۲۰۰۱»[1] و «قانون تروریسم، مصوب ۲۰۰۶»[2] نمود که هرگونه فعالیت تروریستی برخط را به‌طور دقیق‌تری تعریف کرده و به مقامات این امکان را می‌دادند که با استفاده از ابزارهای فناوری، این نوع از فعالیت‌های مجرمانه را شناسایی و با آن مقابله کنند. این در حالی بود که «کلایو واکر» در مقاله‌ای با عنوان «تروریسم سایبری؛ اصول حقوقی و قوانین در انگلستان» در سال ۲۰۰۶ به بررسی اصول حقوقی و چالش‌های تروریسم سایبری در انگلستان می‌پردازد؛ مقاله مزبور به ابهام موجود در تعریف تروریسم برخط در نظام حقوقی انگلستان و ضرورت ایجاد چارچوب‌های قانونی نوین در قبال تهدیدات ناشی از آن اشاره دارد. علاوه بر این، مقررات موجود نظیر «قانون تروریسم، مصوب ۲۰۰۰» و «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰» نیازمند بازنگری و تطبیق با تحولات فزاینده فناوری هستند. در ضمن، مقاله به چالش‌های حفظ تعادل میان امنیت عمومی و حقوق بشر، به ویژه حریم خصوصی، و اهمیت همکاری‌های بین‌المللی در مقابله با تروریسم برخط تأکید دارد. بر این اساس، اصلاحات قانونی و تدوین چارچوب‌های جدید برای مقابله با تهدیدات ناشی از این دسته از فعالیت‌های مجرمانه برخط مورد تأکید قرار گرفت(Walker, 2006: 637-341).

با گسترش تروریسم برخط و نگرانی‌های فزاینده راجع‌به تهدیدات ناشی از آن، انگلستان راهبردهایی را پیرامون پیشگیری کیفری از این تهدیدات اتخاذ نمود؛ بر این اساس، طی سال ۲۰۱۱ انگلستان راهبرد «امنیت سایبری بریتانیا؛ حفاظت و ارتقای بریتانیا در دنیای دیجیتال» را با هدف حفاظت از این کشور در قبال تهدیدات برخط و ترویج رشد

[1] UK Government. (2001). *Anti-terrorism, Crime and Security Act 2001* (UK Public General Acts 2001 c. 24). https://www.legislation.gov.uk/ukpga/2001/24/contents

[2] UK Government. (2006). *Terrorism Act 2006* (UK Public General Acts 2006 c. 11). https://www.legislation.gov.uk/ukpga/2006/11/contents

دیجیتال تدوین و طراحی نمود.[۱] هدف‌های اساسی این راهبرد شامل «حفاظت از زیرساخت‌های حیاتی و منافع ملی در قبال تهدیدات سایبری»، «تقویت همکاری‌ها برای مقابله با تهدیدات جهانی و به اشتراک‌گذاری اطلاعات»، «تضمین امنیت خدمات برخط و زیرساخت‌ها به‌منظور حمایت از اقتصاد و ارتقای اعتماد به فناوری»، «توسعه مهارت‌های امنیت سایبری در سطوح عمومی و تخصصی»، «ترویج نوآوری‌های سایبری و سرمایه‌گذاری در فناوری‌های پیشرفته»، و «اصلاح قوانین به‌منظور مقابله با تهدیدات نوین و تقویت حمایت‌های حقوقی»، بود. هدف نهایی این راهبرد، حفاظت از انگلستان در قبال تهدیدات دیجیتال و ارتقای آن به‌عنوان یک پیشرو در عرصه سایبری جهانی است. در سال ۲۰۱۵، دولت انگلستان با توجه به تهدیدات فزاینده سایبری، طرح مبارزه با تروریسم برخط را با صدور سندی تحت عنوان «سیاست دولت ۲۰۱۰ تا ۲۰۱۵: امنیت سایبری»[۲] مبادرت به تمرکز در قبال تهدیدات ناشی از تروریسم برخط علیه سامانه‌های حیاتی، از جمله بهداشت عمومی و شبکه‌های بیمارستانی نمود.[۳] با افزایش استفاده تروریست‌ها از فضای دیجیتال، همچنان چالش‌هایی برای روزآمدی قوانین و تطبیق آن‌ها با تهدیدات جدید وجود داشت (Walton & Johnstone, 2024: 431-433).

با این همه، مقرراتی نظیر «قانون اختیارات تحقیق، مصوب ۲۰۰۰»[۴] و «قانون اختیارات تحقیق، مصوب ۲۰۱۶»[۵] به مقامات انگلستان این امکان را می‌دهد تا نظارت دقیق‌تری بر تروریسم برخط اِعمال کنند. در دوران همه‌گیری کووید-۱۹، افرادی نظیر «پاتریک روآن»[۶] به‌دلیل تشویق به خشونت علیه مقامات بهداشتی از طریق سکوهایی مانند تلگرام، به پنج سال حبس محکوم شد.[۷] این اقدام نشان‌دهنده جدیت انگلستان در قبال چنین تهدیداتی است. به‌عنوان نمونه می‌توان به حمله باج‌افزار «واناکرای»[۸] در ماه مه ۲۰۱۷ به سازمان «خدمات بهداشت ملی»[۹] که درانگلستان خسارات قابل توجهی وارد کرد، اشاره داشت.[۱۰] این باج‌افزار با سوءاستفاده از آسیب‌پذیری‌های موجود در سیستم‌عامل ویندوز، به‌ویژه در سامانه‌هایی که به‌روزرسانی‌های امنیتی لازم را دریافت نکرده بودند، موجب اختلالات گسترده در خدمات بهداشتی و

---

[1] Cabinet Office. (2011, November). *The UK cyber security strategy: Protecting and promoting the UK in a digital world*. https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf

[2] UK Government. (2015, May 8). *2010 to 2015 government policy: Cyber security*. https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security

[۳] وفق این سند، دولت انگلستان در دوره ۲۰۱۰ تا ۲۰۱۵ بر دو محور اصلی امنیت سایبری تمرکز داشت: حفاظت از زیرساخت‌های حیاتی و تقویت همکاری‌ها در سطح ملی و بین‌المللی. اقدامات اصلی شامل «تأسیس سازمان امنیت سایبری ملی»، «همکاری با بخش خصوصی و بین‌المللی، احترام به حقوق بشر و حریم خصوصی»، «تصویب قوانین امنیت سایبری و حریم خصوصی اینترنتی»، و «برنامه‌های آموزشی برای ارتقای آگاهی عمومی»، بود. این سیاست‌ها بر تقویت امنیت سایبری، همکاری‌های داخلی و بین‌المللی، و تطابق با حقوق بشر تأکید داشت تا از تهدیدات سایبری و آسیب‌پذیری‌ها پیشگیری کند(Wołyniec, 2018: 146-147).

[4] UK Government. (2000). *Regulation of Investigatory Powers Act 2000* (UK Public General Acts 2000 c. 23). https://www.legislation.gov.uk/ukpga/2000/23/contents

[5] UK Government. (2016). *Investigatory Powers Act 2016* (UK Public General Acts 2016 c. 25). https://www.legislation.gov.uk/ukpga/2016/25/contents

[6] Patrick Rowan

[7] https://www.millerchevalier.com/sites/default/files/2023-11/GIR_Sanctions_4th-Edition.pdf

[8] WannaCry, https://techcrunch.com/2019/05/12/wannacry-two-years-on/

[9] National Health Service (NHS) in England, https://www.gov.uk/government/organisations/nhs-england

[10] National Audit Office. (2017, October 27). *Investigation into the WannaCry cyber attack and the NHS*. https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

درمانی شد.[۱] اثرات این حمله شامل تعطیلی برخی بیمارستان‌ها، تاخیر در انجام درمان‌ها و ایجاد اضطراب در بیماران بود. این رویداد توجه بیشتری به اهمیت امنیت سایبری در حوزه بهداشت عمومی جلب کرد و منجر به اتخاذ تدابیر و اقدامات لازم برای تقویت زیرساخت‌های امنیتی در این بخش شد(Ghafur, et al, 2019: 4-5)؛ بر این اساس، آماج‌های مزبور حاکی از توانایی تروریست‌ها در ایجاد مخاطره و آسیب به شبکه‌های دیجیتال برای نقض سلامت عمومی هستند(Evan, et al., 2017: 5-6). در ضمن، طی سال ۲۰۲۰، انگلستان با صدور سندی موسوم به «سفیدنامه آسیب‌های برخط»[۲] به دنبال افزایش پاسخ و مسئولیت سکوهای برخط در پیشگیری از انتشار محتوای تروریستی و آسیب‌رسان به سلامت عمومی بود. این اقدام همچنین چالش‌های ناشی از مقابله با تروریسم برخط و ارتباط آن با نقض حقوق سلامت عمومی را مورد توجه قرار داد(ر.ک: شایق، علیرضا و ناجی‌زواره، ۱۳۹۵: ۹۹-۹۸).

در ژوئن ۲۰۲۴، هکرها به مرکز پاتولوژی در انگلیس حمله کردند و چهارصد گیگابایت اطلاعات بیماران را منتشر کردند.[۳] گروه «کیلیم»[۴] که تهدید کرده بود در صورت عدم پرداخت باج، اطلاعات بیماران را افشا می‌کند، نام، تاریخ تولد، شناسه بهداشتی و اسناد مالی و حقوقی را فاش کرد. این حمله موجب تأخیر در دوهزار قرار ملاقات پزشکی و یک‌هزار و یکصد عمل جراحی شد.[۵]

افزون بر این، می‌توان به حمله «اکسل روداکوبانا»[۶] در «» انگلستان در استودیوی «هارت اسپیس»[۷] طی سال ۲۰۲۴ اشاره نمود.[۸] پس از این حمله تروریستی، انگلستان اقدامات قانونی قابل توجهی را آغاز کرد؛ نخست‌وزیر «کایر رادنی استارمر»[۹] اعلام کرد که مقررات مبارزه با تروریسم اصلاح خواهد شد تا اقدامات خشونت‌آمیز غیرعقیدتی را نیز پوشش دهد.[۱۰] درضمن، دولت انگلستان «دیوید جفری اندرسون»[۱۱] را برای رهبری بررسی مجدد برنامه پیشگیری از افراط‌گرایی منصوب کرد[۱۲]؛ البته مقامات دولتی انگلستان بر لزوم تقویت نظارت و پیشگیری در راستای مقابله با تهدیدات غیرعقیدتی تأکید کردند.[۱۳] در این راستا و مطابق شرایط بحرانی حاکم در سکوهای برخط، «رابین کوپلند» و «ناتان تابک» در سال

---

[1] https://www.extnoc.com/learn/general/wannacry-ransomware

[2] UK Government. (2020, December 15). *Consultation outcome: Online harms white paper*. https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper

[3] https://www.theguardian.com/society/article/2024/jun/24/nhs-england-confirms-theft-of-patient-records-data-from-its-provider

[4] Qilin

[5] https://conosco.com/in-the-news/nhs-cyber-attacks-june-2024

[6] Axel Rudakubana's

[7] Hart Space

[۸] در ۲۹ ژوئیه ۲۰۲۴، یک حمله با چاقو در استودیوی «هارت اسپیس» در «ساوت‌پورت»(Southport)، «مرسی‌ساید»(Merseyside)، انگلستان رخ داد که سه دختر را به قتل رساند و ده نفر دیگر را زخمی کرد. اکسل روداکوبانا، مهاجم ۱۷ ساله، پس از حمله دستگیر شد و به قتل و اقدام به قتل متهم شد. وی همچنین تحت اتهامات تروریستی به دلیل داشتن «ریسین»(Ricin) و مطالعه «کتابچه راهنمای القاعده» قرار گرفت. پس از اعترافات او، مشخص شد که سابقه رفتار خشونت‌آمیز داشته و چندین بار به برنامه پیشگیری از افراط‌گرایی ارجاع شده بود؛

- https://www.theguardian.com/uk-news/2025/jan/21/expert-warn-of-dangers-of-violent-content-being-readily-available-online?utm_source=chatgpt.com

[9] Keir Rodney Starmer

[10] https://www.theguardian.com/uk-news/2025/jan/21/keir-starmer-vows-change-terror-laws-deal-lone-wolf-killers-southport

[11] David Jeffrey Anderson

[12] https://www.gov.uk/government/news/open-competitions-launched-for-independent-prevent-commissioner-and-commissioner-for-countering-extremism

[13] https://www.gov.uk/government/publications/independent-review-of-prevents-report-and-government-response/independent-review-of-prevent-one-year-on-progress-report-accessible

۲۰۲۴ با انتشار نتایج و یافته‌های علمی خود در چارچوب مقاله‌ای تحت عنوان «سایبر-حس‌گر: گسترش چارچوب بهداشت عمومی سایبری» به بررسی تأثیرات فضای برخط بر سلامت عمومی و معرفی مفهوم «سایبر-حس‌گر» پرداختند؛ این مفهوم ضمن اشاره به تأثیرات حسی و رفتاری انسان‌ها در فضای دیجیتال، تأکید دارد که چارچوب بهداشت عمومی برخط باید روزآمدسازی شود تا تهدیدات جدیدی مانند مشکلات روانی و اطلاعات نادرست را پوشش دهد. به‌علاوه، تهدیدات برخط نظیرهک‌های بهداشتی و دسترسی غیرمجاز به داده‌ها نیازمند قوانین دقیق‌تر و همکاری‌های بین‌المللی هستند. البته، اصلاح قوانین برای مقابله مؤثر با این تهدیدات و حفظ حقوق بشر در فضای دیجیتال ضروری است(Coupland, & Taback, 2024: 1-3).

نظام حقوقی انگلستان در مواجهه با تروریسم برخط، با وجود تدوین اسنادِ موضوعه نظیر قوانین سال‌های ۲۰۰۰، ۲۰۰۶ و ۲۰۱۶، در مقام اجرا با ناکارآمدی‌های ساختاری مواجه بوده است. تحلیل انتقادی یافته‌ها نشان می‌دهد که بحران اصلی، نه صرفاً «فقدان نص قانونی»، بلکه «تورم تقنینیِ مبهم» و «ضعف در ضمانت‌اجرای عملی» است؛ به‌گونه‌ای که تعارض ذاتی میان «صیانت از امنیت ملی» و «صیانت از حریم خصوصی»، بن‌بست‌های جدی در نظارت ایجاد کرده است. فقدان تعریفی جامع از «تروریسم برخط» و ناتوانی در همگام‌سازی قواعد با تحولات فناوری، امنیت زیرساخت‌های حیاتی (همچون نظام سلامت) را به‌شدت آسیب‌پذیر ساخته است. البته ناکارآمدی در پیشگیری، ریشه در تعامل پیچیده میان ابهامِ ماهوی قانون، ضعف در نظارتِ فنی و تضادِ حقوق بشری دارد که نیازمند بازنگری بنیادین است.

۲. تروریسم برخط و سلامت عمومی

تروریسم برخط که شامل ترویج تروریسم، نشر پیام‌های نفرت‌انگیز، جذب نیرو و تهدیدات برخط هستند، تهدیدات جدی برای سلامت عمومی به‌شمار می‌آیند. این فعالیت‌ها می‌توانند باعث اضطراب، اختلالات اجتماعی و آسیب به اعتماد عمومی به سامانه‌های مراقبت بهداشتی و درمانی شوند(Mughal, et al., 2023: 73-75). در نظام حقوقی انگلستان، مقرراتی نظیر «قانون ضدتروریسم، جنایت و امنیت، مصوب ۲۰۰۱» و «قانون تروریسم، مصوب ۲۰۰۶» این اقدامات را جرم‌انگاری کرده‌اند و «قانون حفاظت از داده‌ها، مصوب ۲۰۱۸»[1] نیز به حفاظت از داده‌های برخط پرداخته است. چالش‌ها در این زمینه شامل تعارض میان آزادی بیان و مبارزه با تروریسم و همچنین دشواری اجرای مقررات در سطح بین‌المللی است.

وفق مقرراتی نظیر «قانون ضدتروریسم، جنایت و امنیت، مصوب ۲۰۰۱» و «قانون تروریسم، مصوب ۲۰۰۶»، تروریسم به اقداماتی اطلاق می‌شود که با استفاده از خشونت و ترساندن عمومی، به‌منظور تأثیرگذاری بر سیاست‌های دولتی صورت می‌گیرد. تهدیدات بهداشتی به‌طور خاص در این چارچوب قرار می‌گیرند و می‌توانند به‌عنوان ابزاری برای تحقق اهداف تروریستی در نظر گرفته شوند. این قوانین انتشار محتوای تروریستی و تبلیغ خشونت برخط را جرم‌انگاری کرده‌اند. در سطح بین‌المللی، کنوانسیون‌هایی نظیر تصویب «کنوانسیون بوداپست در مورد جرایم سایبری، مصوب ۲۰۰۱»[2] و

---

[1] UK Public General Acts. (2018). *Data Protection Act 2018*, c. 12. Retrieved from https://www.legislation.gov.uk/ukpga/2018/12/contents

[2] https://dig.watch/updates/comparative-analysis-the-budapest-convention-vs-the-un-convention-against-cybercrime

«کنوانسیون سازمان ملل متحد علیه جرایم سایبری، مصوب ۲۰۲۴»[1]، ضمن اطلاق تروریسم برخط به‌عنوان تهدیدی جهانی، کشورهای عضو را ملزم به اقدام برای مقابله با آن می‌کنند(وزیردفتر، ۱۴۰۳: ۸۱-۷۹). این فعالیت‌ها می‌توانند به‌طور غیرمستقیم سلامت عمومی را از طریق ایجاد اضطراب روانی و اختلالات اجتماعی تهدید کنند.

تروریسم برخط می‌توانند حریم خصوصی افراد را نقض کرده و موجب تهدید سلامت عمومی شوند. این تهدیدات شامل انتشار اطلاعات شخصی، جذب افراد به گروه‌های تروریستی و تحدید دسترسی به اطلاعات است که ممکن است منجر به اضطراب اجتماعی و کاهش اعتماد عمومی به ساختار نظام بهداشت و درمان شود (Sekalala, Dagron, Forman, & Meier, 2020: 14-17). در حقوق انگلستان، «قانون ضدتروریسم، جنایت و امنیت، مصوب ۲۰۰۱» و «قانون حفاظت از داده‌ها، مصوب ۲۰۱۸» به مقابله با این تهدیدات پرداخته‌اند، اما اجرای مؤثر آن‌ها نیازمند توازنی میان مقابله با تروریسم و حفظ حقوق فردی مانند حریم خصوصی و آزادی اطلاعات است(شکری، ۱۳۹۹: ۴۱-۳۹)؛ اگرچه غایت این امر باید حفظ سلامت عمومی و پیشگیری از آثار منفی آن بر جامعه باشد.

تهدیدات برخط همچون انتشار اطلاعات نادرست پزشکی، تهدیدات بیولوژیک و شیمیایی، و حملات سایبری به زیرساخت‌های مراقبت بهداشتی می‌توانند سلامت فردی و جمعی را تهدید کنند و واکنش‌های عمومی را مختل نمایند. اطلاعات نادرست پزشکی به‌ویژه در بحران‌های بهداشتی می‌تواند موجب گمراهی عمومی و تصمیمات اشتباه درباره بیماری‌ها، درمان‌ها و واکسن‌ها شود که به رفتارهای خطرناک منجر می‌گردد. در راستای مقابله با این تهدیدات، «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰»[2]، «قانون ضدتروریسم، جنایت و امنیت، مصوب ۲۰۰۱» و «قانون ارتباطات، مصوب ۲۰۰۳»[3] در انگلستان دارای کاربردهای قابل ملاحظه‌است. البته تهدیدات به استفاده از سلاح‌های بیولوژیک، شیمیایی یا رادیولوژیک از طریق اینترنت می‌تواند سلامت عمومی را به‌طور جدی تهدید کند. این تهدیدات شامل انتشار اطلاعات نادرست، دستورالعمل‌ها یا تشویق به حملات بیولوژیک و شیمیایی است که می‌تواند منجر به پانیک اجتماعی و اختلال در واکنش‌های بهداشتی شود که در چارچوب نظام تقنینی انگلستان وفق مقرراتی هم‌چون «قانون بهداشت عمومی (کنترل بیماری)، مصوب ۱۹۸۴»، «قانون سلاح‌های شیمیایی، مصوب ۱۹۹۶»[4]، «قانون ضدتروریسم، جنایت و امنیت، مصوب ۲۰۰۱» و «قانون عدالت کیفری و مهاجرت، مصوب ۲۰۰۸»[5] امکان پیشگیری را دارند.

استفاده از اینترنت برای تشویق به تروریسم علیه مراکز بهداشت و درمان یا کارکنان حوزه سلامت تهدیدی جدی برای سلامت عمومی است. این اقدامات می‌توانند شامل حملات فیزیکی یا سایبری به بیمارستان‌ها و کادر پزشکی باشند و موجب اختلال در خدمات درمانی و تهدید امنیت عمومی شوند(Ulmer, et al., 2022: 27-31). بر این اساس، مطابق مقررات حاکم در نظام حقوقی انگلستان مانند «قانون ضدتروریسم، جنایت و امنیت، مصوب ۲۰۰۱» و «قانون ارتباطات، مصوب ۲۰۰۳» برای مقابله با این تهدیدات کاربرد دارند. افزون بر این، حملات سایبری به شبکه‌های بهداشت

[1] Explanation of Position of the United States on the Adoption of the Resolution on the UN Convention Against Cybercrime in UNGA's Third Committee – United States Mission to the United Nations, https://www.unodc.org/unodc/cybercrime/convention/home.html
[2] Computer Misuse Act 1990, https://www.legislation.gov.uk/ukpga/1990/18/contents
[3] Communications Act 2003, https://www.legislation.gov.uk/ukpga/2003/21/contents
[4] UK Public General Acts. (1996). *Chemical Weapons Act 1996, c. 6*. Retrieved from https://www.legislation.gov.uk/ukpga/1996/6/contents
[5] UK Public General Acts. (2008). *Criminal Justice and Immigration Act 2008, c. 4*. Retrieved from https://www.legislation.gov.uk/ukpga/2008/4/contents

و درمان با هدف سرقت داده‌های پزشکی یا ایجاد اختلال در خدمات درمانی تهدیدی جدی برای سلامت عمومی است(Seh, et al., 2020: 133-136). این حملات می‌توانند منجر به افشای اطلاعات حساس و آسیب به اعتماد عمومی به سیستم بهداشت شوند(Li, et al., 2025: 34-35). در نظام حقوقی انگلستان، وفق محتوای مقرر در «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰» برای مقابله با دسترسی غیرمجاز و سرقت داده‌ها و «قانون ضدتروریسم، جنایت و امنیت، مصوب ۲۰۰۱» برای حملات سایبری با هدف تهدید امنیت عمومی قابلیت اجرا دارند. از این‌رو، پیشگیری کیفری باید به‌گونه‌ای تنظیم شود که ضمن پیشگیری از اختلال در خدمات بهداشتی، حقوق فردی از جمله حفاظت از داده‌ها نیز به‌طور کامل رعایت گردد(محمدنسل، محمدنسل و گلدوزیان، ۱۳۹۹: ۹۸-۹۶).

با این همه، تروریسم برخط، مانند ترویج تروریسم و تهدیدات برخط، تهدیدات جدی برای سلامت عمومی ایجاد می‌کنند، از جمله اضطراب و اختلالات اجتماعی(Durodié & Wainwright, 2018: 64-65). از این‌رو، در انگلستان، «قانون ضدتروریسم، جنایت و امنیت مصوب ۲۰۰۱» و «قانون تروریسم مصوب ۲۰۰۶»، این‌گونه فعالیت‌ها را جرم‌انگاری کرده‌اند، در حالی که «قانون حفاظت از داده‌ها مصوب ۲۰۱۸»، تضمین‌کننده حفاظت از داده‌های شخصی است. چالش‌های اصلی شامل تعارض بین آزادی بیان و مبارزه با تروریسم و مشکلات اجرایی موازین بین‌المللی است. این تهدیدات می‌توانند شامل انتشار اطلاعات نادرست پزشکی، تهدیدات بیولوژیک و حملات سایبری به زیرساخت‌های مراقبت بهداشتی باشند. برای مقابله با این تهدیدات، اجرای «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰ و «قانون تروریسم، مصوب ۲۰۰۰»[1] ضروری است. علاوه بر این، همکاری‌های بین‌المللی و نظارت دقیق بر محتوای برخط از اهمیت حیاتی برخوردار است.

مقررات حاکم در انگلستان در زمینه مهار تروریسم برخط مؤثر بر سلامت عمومی، هرچند واجد کارکرد بازدارنده‌اند، از حیث انسجام و کارایی کامل تلقی نمی‌شوند. پیش‌بینی عناوین مجرمانه‌ای نظیر تشویق و تحریک، تهدید، دسترسی غیرمجاز و افشای داده‌ها، امکان مداخله پیشگیرانه و حمایت از زیرساخت‌های درمانی و اعتماد عمومی را فراهم ساخته است؛ با این وجود، تشتت مقررات میان حوزه‌های تروریسم، جرایم رایانه‌ای، ارتباطات، بهداشت و حفاظت از داده‌ها، هماهنگی اجرایی و تفسیر منسجم را با دشواری مواجه می‌سازد. از حیث ماهوی، فقدان ضابطه‌ای صریح برای تمایز میان هشدار مشروع، نقد علمی یا اطلاعات نادرست با محتوای تروریستی، زمینه بروز تعارض با آزادی بیان و حق دسترسی به اطلاعات سلامت را فراهم می‌آورد. افزون بر این، اتکای سازوکار اجرا به همکاری‌های فرامرزی، تعامل با سکوهای دیجیتال و تحصیل ادله الکترونیکی، در مواجهه با حملات سریع سایبری کارآمدی لازم را تضمین نمی‌کند. نهایتاً، تعارض بالقوه میان پایش گسترده داده‌ها و اصل تناسب، حریم خصوصی بیماران را در معرض مخاطره قرار داده و مشروعیت مداخله کیفری را نیز محل تردید می‌سازد.

۳. توازن میان امنیت عمومی و حقوق فردی

[1] UK Public General Acts. (2000). *Terrorism Act 2000, c. 11*. Retrieved from https://www.legislation.gov.uk/ukpga/2000/11/contents

همان‌گونه که پیشتر ملاحظه شد، در انگلستان، پیشگیری کیفری از تروریسم برخط تحت مجموعه‌ای از مقررات، از جمله «قانون حقوق بشر، مصوب ۱۹۹۸»[1]، «قانون تروریسم، مصوب ۲۰۰۰» و «قانون اختیارات تحقیق، مصوب ۲۰۱۶» قرار دارد. هدف این مقررات، مقابله با تروریسم و در عین حال حفاظت از حقوق فردی است.[2] یکی از چالش‌های اساسی در این زمینه، برقراری تعادل میان تأمین امنیت عمومی و حفظ حقوق فردی، به‌ویژه آزادی بیان و حریم خصوصی می‌باشد(Burke, 2021: 246). اقدامات پیشگیرانه نظیر نظارت برخط، اگرچه ممکن است در این فرایند مؤثر باشند، اما می‌توانند منجر به نقض حقوق فردی شوند. از اینرو، نظام قضائی انگلستان باید تدابیر متوازنی اتخاذ نماید تا هم از امنیت عمومی محافظت کند و هم حقوق فردی را محترم بشمارد. وانگهی، تروریسم برخط علیه سامانه‌های بهداشتی در انگلستان تحت «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰» قرار دارد که دسترسی غیرمجاز به سامانه‌ها و تخریب داده‌ها را جرم‌انگاری می‌کند. این حملات تهدیداتی جدی برای امنیت داده‌های پزشکی و سلامت عمومی ایجاد می‌کند(Chan, et al., 2016: 629). چالش اصلی در این حوزه، تعادل میان حفظ امنیت عمومی و رعایت حقوق فردی، به‌ویژه حریم خصوصی بیماران، است. علاوه بر این، مشکلاتی در شناسایی مجرمان و جمع‌آوری شواهد معتبر وجود دارد که اجرای اقدامات کیفری را پیچیده می‌سازد. در این راستا، نظام حقوقی انگلستان می‌بایست رویکردی متوازن اتخاذ نماید که از یک‌سو سلامت عمومی را تأمین کند و از سوی دیگر حقوق فردی و حریم خصوصی افراد را محترم شمارد.[3]

در قبال تروریسم برخط و نقض حقوق سلامت عمومی، «قانون حقوق بشر، مصوب ۱۹۹۸» نقش اساسی ایفا می‌کند. این قانون بر حفظ حقوق اساسی افراد تأکید دارد و به‌ویژه بر حق حریم خصوصی، آزادی بیان و محاکمه منصفانه تأکید می‌نماید(Draghici, 2011: 689-692). مطابق با ماده ۸ این قانون، نظارت و جمع‌آوری داده‌های شخصی باید به‌گونه‌ای باشد که متناسب و محدود باشد تا حقوق حریم خصوصی افراد نقض نگردد. همچنین، وفق ماده ۱۰، اقدامات پیشگیرانه در قبال تروریسم برخط ممکن است تهدیدی برای آزادی بیان به‌شمار آید. در عین حال، بر اساس مفاد ماده ۶، در تعقیب کیفری تروریسم برخط، رعایت حقوق دفاعی و تضمین دسترسی به محاکمه منصفانه از جمله اصول ضروری است. این قانون سعی دارد تعادلی میان تأمین امنیت عمومی و حفظ حقوق فردی، از جمله حریم خصوصی، آزادی بیان و حق محاکمه منصفانه برقرار سازد(بهرام‌نیا و ناصح‌زاده، ۱۴۰۳: ۸۶-۸۵).

به‌طور خاص، «قانون تروریسم، مصوب ۲۰۰۰» به تروریسم برخط پرداخته است. این قانون، تروریسم برخط نظیر انتشار پیام‌های خشونت‌آمیز یا تشویق به تروریسم از طریق فضای دیجیتال، را جرم‌انگاری می‌کند (Banaji & Bhat, 2022: 79-82). بند نخست از ماده ۵۸ این قانون به جرایم سایبری، مانند دعوت به خشونت از طریق اینترنت، پرداخته شده و نقش مهمی در پیشگیری کیفری از تهدیدات سایبری ایفا می‌کند. به‌علاوه، مواد ۱۹ و ۲۱ دولت انگلستان را مجاز به نظارت بر فعالیت‌های برخط می‌کنند، اما این نظارت باید محدود و متناسب با حقوق حریم خصوصی باشد.[4] در ضمن،

---

[1] UK Public General Acts. (1998). *Human Rights Act 1998*, c. 42. https://www.legislation.gov.uk/ukpga/1998/42/contents

[2] https://justice.org.uk/counter-terrorism-human-rights/

[3] https://www.hhrjournal.org/2013/09/06/litigation-as-a-strategy-to-hold-governments-accountable-for-implementing-the-right-to-health/

[4] See: UK Public General Acts. (2024, December 12). *Operation of police powers under the Terrorism Act 2000 and subsequent legislation: Arrests, outcomes, and stop and search, Great Britain, quarterly update to September 2024*. https://www.gov.uk/government/statistics/operation-of-police-powers-under-tact-2000-to-

این قانون ابزارهای نظارتی و کیفری لازم را برای مقابله فراهم کرده است، اما در این فرآیند باید حقوق فردی، نظیر حریم خصوصی و آزادی بیان، به‌طور مؤثر محافظت شود.[۱]

نظام حقوقی انگلستان ابزارهای نوآورانه‌ای برای مقابله با تروریسم برخط و حفاظت از سلامت عمومی در چارچوب «قانون ضدتروریسم و امنیت، مصوب ۲۰۱۵»[۲] فراهم کرده است. انتشار محتوای تروریستی، از جمله پیام‌های رادیکال و تشویق به خشونت از طریق اینترنت، جرم محسوب می‌شود و تهدیدی جدی برای سلامت روانی و عمومی جامعه است. این قانون به دولت مجوز می‌دهد تا بر فعالیت‌های برخط نظارت کند و محتوای تروریستی را شناسایی و مسدود نماید؛ با این حال، نظارت باید به‌طور متناسب انجام شود و از نقض حریم خصوصی افراد پیشگیری کند(Macdonald, et al., 2019: 185-186). علاوه بر این، قانون مذکور بر کاهش آثار منفی این‌گونه فعالیت‌ها، از جمله تهدیدات روانی و اضطراب در جامعه، تأکید دارد و از طریق اقدامات پیشگیرانه، از آسیب به سلامت عمومی پیشگیری می‌کند.

«قانون حفاظت از داده‌ها، مصوب ۲۰۱۸»، نقش حیاتی در حفاظت از اطلاعات پزشکی و سلامت عمومی در قبال تروریسم برخط ایفا می‌کند. این قانون، داده‌های پزشکی را به‌عنوان داده‌های حساس شناسایی کرده و از افشای غیرمجاز آن‌ها پیشگیری می‌نماید.[۳] وفق این قانون، سازمان‌ها و نهادهای مرتبط موظف به اتخاذ تدابیر امنیتی مناسب هستند و در صورت نقض مسئولیت های خود، تحت پیگرد قانونی قرار خواهند گرفت. پردازش اطلاعات پزشکی باید وفق موافقت‌نامه‌های شفاف و مستند صورت پذیرد و سوءاستفاده از داده‌ها برای اهداف تروریستی منجر به مجازات‌های کیفری خواهد شد. افراد حق دارند به اطلاعات خود دسترسی داشته باشند و در صورت نقض امنیت، باید به‌طور سریع و شفاف مطلع شوند(Piasecki & Chen, 2022: 119-121). به‌علاوه، نظام نظارتی دقیقی برای پیگیری نقض‌های امنیتی و حفاظت از سلامت عمومی وفق این قانون در این زمینه وجود دارد. به‌طور کلی، این قانون به مقابله با تهدیدات برخط و حفظ سلامت عمومی در قبال خطرات احتمالی کمک می‌کند(Brouwer, 2021: 387). این قانون نظارت‌های دقیقی برای شناسایی و پیشگیری از نقض امنیت داده‌ها فراهم کرده تا تهدیدات سلامت عمومی کاهش یابد و افراد در صورت وقوع نقض امنیتی، به‌طور شفاف مطلع شوند.

---

september-2024/operation-of-police-powers-under-the-terrorism-act-2000-and-subsequent-legislation-arrests-outcomes-and-stop-and-search-great-britain-quarterly-u

[۱] در چارچوب قوانین عمومی دولت انگلستان، گزارش «اقدامات تروریسم در سال ۲۰۲۳: گزارش بازبینی مستقل قانون تروریسم (*قابل دسترسی*)»، طی ۱۵ جولای ۲۰۲۵ منتشر شد. این گزارش بر ضرورت حفظ تعادل میان امنیت عمومی و حقوق فردی در چارچوب مقررات تروریسم انگلستان تأکید دارد. تحلیل ارائه‌شده در این گزارش شامل پنج نکته اساسی است؛ نظارت مستمر بر انطباق مقررات تروریسم با اصول حقوق بشر، تضمین رعایت حقوق فردی از جمله حق دادرسی منصفانه، حفظ تعادل میان امنیت و حقوق فردی، ایجاد نهاد نظارتی مستقل به‌منظور پیشگیری از سوءاستفاده، و پیشنهاد اصلاحات در نظارت بر استفاده از قدرت‌های امنیتی و داده‌های دیجیتال. هدف نهایی این گزارش، تضمین رعایت حقوق بشر و تأمین توازن میان امنیت و آزادی‌های فردی در فرآیند مقابله با تروریسم است؛

- Independent Reviewer of Terrorism Legislation. (2025, July 15). *The Terrorism Acts in 2023: Report of the Independent Reviewer of Terrorism Legislation (accessible)*. UK Public General Acts. https://www.gov.uk/government/publications/the-terrorism-acts-in-2023/the-terrorism-acts-in-2023-report-of-the-independent-reviewer-of-terrorism-legislation-accessible

[2] UK Public General Acts. (2015). *Counter-Terrorism and Security Act 2015*, c. 6. https://www.legislation.gov.uk/ukpga/2015/6/contents

[3] https://www.virtual-college.co.uk/resources/the-data-protection-act-2018

نظام حقوقی انگلستان با هدف مقابله با تروریسم برخط و پیشگیری از بحران‌های اجتماعی و کاهش اعتماد عمومی، مبادرت به تصویب «قانون مبارزه با تروریسم و امنیت مرزی، مصوب ۲۰۱۹»[۱]، کرد که ابزارهای حقوقی لازم را برای مقابله با تروریسم برخط و تأمین سلامت عمومی فراهم نموده است.[۲] این قانون، انتشار محتوای تروریستی برخط را به‌عنوان رفتار جنایی تحت شناسایی قرار داده و دولت را مجاز به نظارت بر فعالیت‌های برخط می‌سازد، مشروط بر اینکه اصول حقوق بشر و حریم خصوصی افراد، محترم شمرده شود(Graziani, 2021: 234-235). «قانون ایمنی برخط، مصوب ۲۰۲۳»[۳] با هدف مقابله با تروریسم برخط و حفاظت از سلامت عمومی، سکوهای برخط را ملزم به شناسایی و حذف محتوای غیرقانونی، از جمله محتوای مرتبط با تروریسم، می‌نماید.[۴] در صورت عدم رعایت این الزامات، سکوها ممکن است با جریمه های مالی سنگین یا انسداد مواجه گردند. این قانون همچنین بر اهمیت حفظ حقوق کاربران راجع‌به آزادی بیان و حریم خصوصی تأکید کرده و در صورت تخلف، امکان اِعمال تعقیب کیفری و مجازات‌های قانونی پیش‌بینی شده است.[۵]

با این همه، می‌توان اذعان داشت در انگلستان، مجموعه‌ای از مقررات از جمله «قانون حقوق بشر، مصوب ۱۹۹۸»، «قانون تروریسم، مصوب ۲۰۰۰» و «قانون اختیارات تحقیق، مصوب ۲۰۱۶» به منظور مقابله با تروریسم برخط و حفظ امنیت عمومی وضع گردیده‌اند. این قوانین به‌ویژه بر لزوم حفظ تعادل میان تأمین امنیت و رعایت حقوق فردی، از جمله حریم خصوصی و آزادی بیان، تأکید دارند. نظارت بر فعالیت‌های برخط باید به‌گونه‌ای انجام شود که حقوق مذکور به‌طور مؤثر محافظت گردد. علاوه بر این، قوانینی مانند «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰» به‌ویژه در مورد حملات سایبری به زیرساخت‌های مراقبت بهداشتی، اقداماتی را برای پیشگیری از افشای غیرمجاز داده‌های پزشکی پیش‌بینی می‌کنند. «قانون حفاظت از داده‌ها، مصوب ۲۰۱۸» نیز به‌طور خاص در راستای حفاظت از داده‌های پزشکی و اطلاعات حساس افراد عمل کرده و افشای غیرمجاز این داده‌ها را ممنوع می‌کند. در ضمن، «قانون ضدتروریسم و امنیت، مصوب ۲۰۱۵» و «قانون ایمنی برخط، مصوب ۲۰۲۳» بر شناسایی و حذف محتوای تروریستی از کوهای برخط تأکید دارند، مشروط بر اینکه این اقدامات به‌طور متناسب با حقوق فردی و آزادی‌های اساسی انجام گیرد.

---

[1] UK Government. (2019). *Counter-Terrorism and Border Security Act 2019, Section 8: Sentencing* (UK Public General Acts 2019 c. 3, Part 1, Chapter 2). https://www.legislation.gov.uk/ukpga/2019/3/section/8

[۲] در چارچوب بخش هجدهم سند سیاست «بررسی پس از قانون‌گذاری قانون ضد تروریسم و امنیت مرزی ۲۰۱۹ (قابل دسترسی)، منتشر شده در ۲۲ ژانویه ۲۰۲۵»، تحت عنوان «بازداشت مظنونین تروریستی: درمان در بیمارستان»، اشاره به بازداشت افراد مظنون به تروریسم که نیاز به درمان پزشکی دارند، شده است. این بخش تأکید می‌کند که حقوق متهمان در خصوص دریافت درمان پزشکی باید رعایت شود. چالش‌های حقوق بشری مرتبط با این ماده شامل رعایت اصول انسان‌دوستانه و حقوق فردی در شرایط بازداشت می‌باشد. به‌علاوه، وفق ساختار مقرر در بخش بیستم با عنوان «افراد آسیب‌پذیر در برابر جذب به تروریسم»، شناسایی افرادی که در معرض خطر جذب به تروریسم قرار دارند، مورد توجه قرار گرفته و هدف آن پیشگیری از تروریسم از طریق مداخله پیشگیرانه است. مقامات مجاز به انجام اقدامات ویژه برای حمایت از این افراد هستند. چالش‌های حقوق بشری این بخش نیز شامل مداخله در آزادی فردی و تعارض با حقوق خصوصی می‌باشد. به‌طور کلی، بخش‌های مذکور به پیشگیری از تروریسم و حقوق قانونی افراد مظنون توجه دارند، اما با چالش‌هایی در زمینه حقوق فردی مواجه هستند که نیازمند نظارت مستمر می‌باشند؛

- Government of the United Kingdom. (2025, January 22). *Post-legislative scrutiny of the Counter-Terrorism and Border Security Act 2019 (accessible)*. https://www.gov.uk/government/publications/counter-terrorism-and-border-security-act-2019-post-legislative-scrutiny/post-legislative-scrutiny-of-the-counter-terrorism-and-border-security-act-2019-accessible

[3] Online Safety Act 2023, https://www.legislation.gov.uk/ukpga/2023/50

[4] https://www.brookings.edu/articles/dual-use-regulation-managing-hate-and-terrorism-online-before-and-after-section-230-reform/

[5] https://consoc.org.uk/the-online-safety-act-privacy-threats-and-free-speech-risks/

مقررات ناظر بر مقابله با تروریسم برخط، علی‌رغم تلاش برای جامعیت، در مقام اجرا با چالش‌های عمده‌ای مواجه‌اند. تحلیل انتقادی یافته‌های پژوهشی حاکی از آن است که ریشه اصلی مشکلات، نه در فقدان قوانین، بلکه در ضعف سازوکارهای اجرایی و تضاد ماهوی میان الزامات امنیتی و حقوق بنیادین بشر استوار است. چارچوب‌های حقوقی، از جمله «قانون حقوق بشر ۱۹۹۸»، «قانون تروریسم ۲۰۰۰» و «قانون اختیارات تحقیق ۲۰۱۶»، بر لزوم ایجاد توازنی دقیق میان تأمین امنیت ملی و صیانت از آزادی‌های فردی، به‌ویژه آزادی بیان و حریم خصوصی، تأکید دارند. معهذا، رویکردهای پیشگیرانه نظیر نظارت فراگیر بر فضای آنلاین، علی‌رغم پتانسیل اثربخشی، غالباً به نقض حقوق مذکور منجر شده و نظام قضائی را در یافتن راهکارهای متعادل و متناسب با چالش روبرو می‌سازد. از اینرو، پیچیدگی‌های اجرایی ناشی از دشواری در شناسایی مرتکبین و تحصیل ادله متقن، فرآیند دادرسی کیفری را مختل می‌سازد. در مواجهه با حملات سایبری به زیرساخت‌های حیاتی حوزه سلامت، «قانون سوءاستفاده از رایانه ۱۹۹۰» و «قانون حفاظت از داده‌ها ۲۰۱۸» با جرم‌انگاری دسترسی‌های غیرمجاز و وضع الزامات برای حفاظت از داده‌های حساس، چارچوبی تقنینی را بنا نهاده‌اند؛ با این حال، اعمال نظارت‌های دقیق و پیاده‌سازی مؤثر مفاد این قوانین همچنان در هاله‌ای از ابهام قرار دارد. تصویب قوانین اخیر، همچون «قانون ایمنی برخط ۲۰۲۳»، که سکوهای آنلاین را مکلف به شناسایی و حذف محتوای تروریستی می‌نماید، تلاشی برای رفع کاستی‌های اجرایی محسوب می‌شود؛ اما ابهامات پیرامون تناسب این الزامات با حقوق کاربران و مصونیت آزادی بیان همچنان برجاست. علاوه بر این، ناکارآمدی نظام نظارتی و ابهام در تعاریف تروریسم برخط، در کنار تنش دائمی میان الزامات امنیتی و حقوق بشر، موانع کلیدی در این عرصه به شمار می‌روند. وانگهی، مقررات انگلستان در مقابله با تروریسم برخط، گرچه تا حدی کارآمد ظاهر شده‌اند، اما با چالش‌های جدی در مرحله اجرا، ضعف در سازوکارهای نظارتی، و تعارضات ذاتی میان منافع امنیتی و حقوق اساسی شهروندان دست و پنجه نرم می‌کنند، امری که مستلزم بازنگری بنیادین و اصلاح مستمر رویکردهای اجرایی است.

٤. نظارت و پیشگیری کیفری از آسیب‌های برخط

نظارت برخط در حقوق انگلستان، ابزاری پیشگیرانه برای مهار تروریسم سایبری و صیانت از سلامت عمومی است. انتشار محتوای افراطی در فضای مجازی، افزون بر تهدید امنیت اجتماعی، آثار روانی گسترده‌ای بر شهروندان برجای می‌گذارد. «قانون تروریسم ۲۰۰۰»، «قانون ضدتروریسم و امنیت ۲۰۱۵» و «قانون ایمنی برخط ۲۰۲۳»، مبنای رصد، حذف محتوا و مسئولیت سکوها را فراهم می‌کنند. بااین‌حال، بر پایه «قانون حقوق بشر ۱۹۹۸»، هرگونه مداخله باید ضروری، متناسب و محدود باشد. حمایت درمانی و روانی از بزه‌دیدگان نیز مکمل سیاست‌های کیفری است.

٤-١. حفظ سلامت عمومی با نظارت برخط

نظارت برخط ابزاری حیاتی برای مقابله با تروریسم برخط و آثار آن بر سلامت عمومی به شمار می‌آید.[1] این دسته از فعالیت‌ها می‌توانند به‌طور جدی امنیت روانی و اجتماعی جامعه را تهدید کنند؛ از اینرو، تقویت نظارت برخط به‌منظور

[1] لازم به‌ذکر است، تدابیر نظارتی به مجموعه‌ای از اقدامات پایشی و مراقبتی اطلاق می‌شود که به‌منظور تأمین امنیت در فضاهای برخط به‌کار گرفته می‌شوند. این اقدامات به طور کلی به دو دسته تقسیم می‌گردند؛ «تدابیر نظارتی فعال» و «تدابیر نظارتی منفعل». در تدابیر نظارتی فعال، مأموران کشف جرم با انجام سلسله اقداماتی در قالب عملیات‌های پلیسی که به‌طور معمول تحت عنوان «دام گستری» (ر.ک: سروری، ۱۴۰۱: ۹۲-۸۸) شناخته می‌شوند، به پیشگیری از وقوع جرم و کشف آن اقدام می‌نمایند. از سوی دیگر، در تدابیر نظارتی منفعل، مأموران و مسئولان پیشگیری از جرم از طریق اقدامات پایشی و نظارتی در

شناسایی و مقابله با این تهدیدات ضرورتی انکارناپذیر است. مقرراتی نظیر همچون «قانون تروریسم، مصوب ۲۰۰۰» و «قانون ضدتروریسم و امنیت، مصوب ۲۰۱۵»، به دولت انگلستان این امکان را می‌دهند تا تروریسم برخط را رصد کند؛ اگرچه ممکن است این امکان از سوی دولت منجر به نقض حقوق فردی، از جمله حریم خصوصی و آزادی بیان، شود(Zedner, 2021: 62-63). افزون بر این، وفق «قانون حقوق بشر، مصوب ۱۹۹۸»، نظارت باید متناسب و محدود به موارد ضروری باشد. علاوه بر این، همان‌گونه که ملاحظه شد، مقرراتی هم‌چون «قانون ایمنی برخط، مصوب ۲۰۲۳» سکوها را ملزم به شناسایی و حذف محتوای تروریستی می‌کنند. یکی از چالش‌های اساسی در این زمینه، شناسایی مجرمان و جمع‌آوری شواهد دیجیتال در جرایم پیچیده است. با این وجود، تقویت نظارت برخط می‌تواند به کاهش تهدیدات برخط و آثار منفی آن بر سلامت عمومی کمک کند(Edelstein, 2018: 1325-1326). در ضمن، نظارت برخط باید به حداقل ضروریات محدود شود تا از نقض حقوق فردی پیشگیری شود و توازن مناسبی میان امنیت عمومی و حقوق فردی برقرار گردد.

علی‌هذا، نظارت مستمر نهادهای امنیتی، از جمله «مرکز ملی امنیت سایبری»[1]، «مرکز ارتباطات دولتی»[2] و «پلیس ملی»[3]، بر تروریسم برخط و سلامت عمومی با استناد به مقرراتی نظیر «قانون تروریسم، مصوب ۲۰۰۰»، «قانون ضدتروریسم و امنیت، مصوب ۲۰۱۵» و «قانون ایمنی برخط، مصوب ۲۰۲۳»، امکان مقابله به‌طور مؤثر را فراهم می‌سازد. با این حال، نظارت برخط ممکن است منجر به نقض حقوق فردی شود(دانکین، ۱۳۹۸: ۸۰-۷۹)؛ از اینرو، مطابق با اصول مندرج در «قانون حقوق بشر، مصوب ۱۹۹۸»، نظارت باید به‌طور متناسب و ضروری اعمال گردد تا توازن مطلوبی میان امنیت عمومی و حقوق فردی برقرار شود. وانگهی، مسئولیت نظارت بر محتوای تروریستی منتشرشده در سکوهای برخط باید بر عهده خود سکوها باشد. طبق «قانون ایمنی برخط، مصوب ۲۰۲۳»، سکوها موظف به شناسایی و حذف محتوای غیرقانونی هستند. در صورتی که سکوها در این زمینه کوتاهی کنند، باید مسئولیت کیفری برای آن‌ها در نظر گرفته شود تا از نقض حقوق سلامت عمومی پیشگیری گردد.

نظام حقوقی انگلستان در مواجهه با تروریسم سایبری، با وجود برخورداری از چارچوب‌های تقنینی منسجم، در مقام اجرا با گسست‌های بنیادین مواجه است. معضل غایی نه در نقیصه قانونی، بلکه در فرآیندهای نظارتی غیرشفاف و ضعف مفرط در ضمانت‌اجراهای عملی نهفته است که برقراری توازن میان الزامات امنیتی و صیانت از حقوق بنیادین بشر را مختل ساخته است. برون‌سپاریِ پالایش محتوا به سکوهای دیجیتال، افزون بر تعارض با اصل آزادی بیان، به دلیل پیچیدگی‌های فنی، در مواجهه با تهدیدات نوین ناکارآمد بوده و فقدان ضوابط مضیق برای تبیین «ضرورت»، زمینه‌ساز نقض حریم خصوصی و تسلط خودسرانه اجرایی شده است.

پی کشف و شناسایی به‌موقع جرایم هستند. مهم‌ترین این اقدامات شامل گشت‌های پلیسی در فضاهای برخط مانند چت‌روم‌ها و شبکه‌های اجتماعی، نظارت‌های متصدیان بانک‌ها برای پیشگیری از پول‌شویی دیجیتالی، و مراقبت‌های متصدیان کافی‌نت‌ها و مراکز عمومی است(آگنج، شیخ‌الاسلامی و ولی‌پوری، ۱۴۰۲: ۱۹۱).

[1] https://www.ncsc.gov.uk/
[2] https://www.hmgcc.gov.uk/
[3] https://www.police.uk/

٤-۲. پیشگیری از آسیب‌های برخط

ضرورت پیشگیری کیفری از تروریسم برخط، به‌منظور حفظ حقوق بزه‌دیدگان و پیشگیری از آسیب‌های مرتبط با فضای برخط، امری حائز اهمیت است. بزه‌دیدگان تروریسم برخط باید از حمایت‌های حقوقی و درمانی برخوردار باشند(Zarmsky, 2024: 172-173). «قانون تروریسم، مصوب ۲۰۰۰» و «قانون ایمنی برخط، مصوب ۲۰۲۳» علاوه بر مقابله با تروریسم، حمایت از بزه‌دیدگان را نیز مدنظر قرار داده‌اند. این حمایت‌ها مشتمل بر خدمات درمانی، مشاوره‌ای، جبران خسارات و حمایت‌های قانونی است. اقدامات کیفری باید به کاهش آسیب‌های اجتماعی و روانی بزه‌دیدگان کمک کند و در چارچوب حقوق بشر، حقوق سلامت عمومی را حفظ نماید(Lancry, 2023: 69). در ضمن، با توجه به تنوع و شیوع فزاینده انواع بزه‌دیدگی‌های کودکان در فضای مجازی، ضرورت مطالعات عمیق و تخصصی به‌ویژه در حوزه حمایت از کودکان آسیب‌دیده در محیط‌های برخط بیش از پیش احساس می‌شود. یکی از اولویت‌های اصلی در این زمینه، تأمین حمایت‌های لازم برای کودکان و نوجوانان در مقابله با بزهکاران و پیشگیری از تعرضات و اعمال خشونت‌آمیز است(حسینی‌اکبرنژاد و جواهری‌آراسته، ۱۳۹۹: ۱۲۳-۱۲۲). حفاظت از حقوق کودکان و نوجوانان در فضای دیجیتال و مقابله با شیوه‌های مختلف سوءاستفاده و استثمار از این گروه آسیب‌پذیر، به مسأله‌ای اساسی برای بسیاری از دولت‌ها و نهادهای بین‌المللی تبدیل گردیده است(موسوی، روحانی‌مقدم و آقایی‌بجستانی، ۱۴۰۱: ۱۲۹؛ ر.ک: فرهادی‌آلاشتی، ۱۴۰۱: ۲۸۴-۲۸۱).

مقابله با پیامدهای روانی این پدیده بر سلامت عمومی اهمیت ویژه‌ای دارد. در این راستا، دولت باید برنامه‌های آگاهی‌رسانی و ارائه خدمات مشاوره روانی را برای کاهش آثار مخرب چنین فعالیت‌هایی اجرا کند. پیشگیری کیفری در این حوزه نباید صرفاً به مجازات مرتکبان محدود شود، بلکه لازم است تدابیر حمایتی برای جامعه و بزه‌دیدگان را نیز در بر گیرد.[1] بر اساس «قانون تروریسم ۲۰۰۰» و «قانون ایمنی برخط ۲۰۲۳»، دولت انگلستان موظف است اقدامات پیشگیرانه و حمایتی لازم را برای کاهش پیامدهای روانی و اجتماعی ناشی از تروریسم برخط اتخاذ کند (Prentice, & Taylor, 2018: 466). این اقدامات می‌تواند شامل ارائه خدمات مشاوره و درمان روانی، حمایت‌های اجتماعی و برنامه‌های آگاهی‌بخشی عمومی درباره مخاطرات فعالیت‌های تروریستی در فضای برخط باشد.

پیشگیری کیفری از تروریسم برخط باید به‌طور دوره‌ای ارزیابی شود تا تأثیر آن در کاهش فعالیت‌ها و حفاظت از حقوق سلامت عمومی مشخص گردد.[2] ارزیابی‌ها باید شامل بازخورد از نهادهای گوناگون در حوزه‌هایی هم‌چون بهداشت، پلیس و جامعه باشد. هدف از پیشگیری کیفری، نه‌تنها مجازات مجرمان، بلکه کاهش آسیب‌های اجتماعی و روانی ناشی از تروریسم برخط است.[3] ارزیابی مداوم اقدامات کیفری می‌تواند ضمن کمک به تطابق مطلوب سیاست‌ها با نیازهای جامعه، بلکه حفاظت از سلامت عمومی را تضمین نماید(Shortland, Neil D., et al, 2021: 329). فرایند مزبور به دولت انگلستان این امکان را می‌دهد که در صورت لزوم، اصلاحات لازم را در مقررات و اقدامات کیفری برای مقابله مؤثرتر با تروریسم برخط صورت پذیرد. با این حال، پیشگیری کیفری باید تهدیدات و آثار منفی آن بر سلامت روانی و

---

[1] See: Institute of Medicine (US) Committee on Responding to the Psychological Consequences of Terrorism. (2003). *Preparing for the psychological consequences of terrorism: A public health strategy* (A. S. Butler, A. M. Panzer, & L. R. Goldfrank, Eds.). National Academies Press.

[2] https://www.ncbi.nlm.nih.gov/books/NBK221639/

[3] https://www1.essex.ac.uk/hrc/documents/54198-criminalization-of-healthcare-web.pdf

اجتماعی جامعه را در قبال تروریسم برخط کاهش دهد. این نوع از پیشگیری باید به‌طور دوره‌ای ارزیابی شوند تا تأثیر آن‌ها در کاهش تهدیدات و پیشگیری از آسیب‌ها مشخص گردد. این ارزیابی باید شامل همکاری نهادهای امنیتی، قضائی و بهداشتی باشد. در نهایت، هدف حفظ حقوق سلامت عمومی و پیشگیری از نقض آن‌ها است (Bada, & Nurse, 2019-2020: 14-16).

چارچوب‌های تقنینی موجود در حوزه پیشگیری کیفری از تروریسم سایبری، علی‌رغم رویکرد حمایتی نسبت به بزه‌دیدگان، در مقام انطباق با واقعیت‌های اجرایی دچار گسست‌های عملیاتی هستند. یافته‌های تحلیلی نشان می‌دهد که چالش بنیادین نه فقدان هنجارهای قانونی، بلکه قصور در ارائه حمایت‌های تخصصی و فقدان سازوکارهای نظارتیِ پایشگر برای ارزیابی مستمر است. این شکاف‌های ساختاری، افزون بر ناکامی در تقلیل پیامدهای آسیب‌زای روانی-اجتماعی، منجر به تعارض میان رویکردهای امنیتی و موازین حقوق بشری شده و کارآمدیِ پیشگیرانه را در راستای صیانت از سلامت عمومی تضعیف نموده است.

نتیجه‌گیری

مقررات انگلستان در مقابله با تروریسم برخط، علی‌رغم تصویب قوانینی چون «قانون تروریسم، مصوب ۲۰۰۰»، «قانون ضدتروریسم، جنایت و امنیت، مصوب ۲۰۰۱»، و «قانون تروریسم، مصوب ۲۰۰۶»، با چالش‌های عملی جدی مواجه بوده‌اند. رویکرد پیشگیرانه کیفری که با هدف مقابله با استفاده تروریست‌ها از اینترنت برای تبلیغ، جذب نیرو و برنامه‌ریزی حملات طراحی شده، در سازگاری با سرعت تحولات فناورانه و گستردگی فضای دیجیتال، دچار ضعف‌هایی است. مهم‌ترین یافته پژوهش این است که چالش اصلی، به‌طور صرف شکاف قانونی نیست، بلکه ترکیبی از ابهام در تعریف تروریسم برخط، ضعف در اجرای مؤثر قوانین، تعارض میان الزامات امنیتی و حقوق بشر (به‌ویژه حریم خصوصی و آزادی بیان)، و «ناکافی بودن سازوکارهای نظارتی» است.

سیاست‌گذاری ناظر به قانون‌گذاری در انگلستان، با وجود فراهم کردن امکان مداخله در قبال تهدیدهای سازمان‌یافته و فناورانه، مشروعیت این مداخلات را منوط به رعایت اصول ضرورت، تناسب، شفافیت و نظارت قضایی می‌داند. با این حال، کاربرد گسترده ابزارهایی نظیر هوش مصنوعی و تحلیل داده‌ها، بدون تضمین‌های کافی حقوق بشری، می‌تواند منجر به نقض حریم خصوصی و محدود شدن آزادی بیان گردد. حوادثی همچون حمله باج‌افزار «واناکرای» در سال ۲۰۱۷ و افشای اطلاعات بیماران در سال ۲۰۲۴، ناکارآمدی در حفاظت از زیرساخت‌های حیاتی و داده‌های حساس را آشکار ساخته و ضرورت بازنگری در قوانین را بیش از پیش برجسته کرده است. این وقایع نشان می‌دهند که دستیابی به تعادل میان امنیت ملی و حقوق فردی، و همچنین همگام‌سازی مقررات با فناوری‌های نوین از جمله رمزنگاری پیشرفته، نیازمند اصلاحات مستمر است.

برای ارتقای پیشگیری کیفری در قبال تهدیدات برخط مرتبط با تروریسم و سلامت عمومی، رویکردی منسجم، متناسب و مبتنی بر حقوق بشر ضروری است. این رویکرد باید مشتمل بر توسعه نظام‌های هوشمند رصد محتوا با رعایت اصول آزادی بیان و حریم خصوصی، ایجاد سازوکارهای همکاری میان نهادهای قضایی، پلیس سایبری و مراجع بهداشتی، و جرم‌انگاری هدفمند انتشار اطلاعات نادرست پزشکی باشد. به‌علاوه، تقویت همکاری‌های بین‌المللی در چارچوب کنوانسیون‌های مرتبط، از ارکان اساسی مقابله با شبکه‌های فراملی ترویج تروریسم برخط و تهدیدات علیه سلامت

عمومی محسوب می‌شود. در نهایت، بازنگری مستمر در قوانین و مقررات، همراه با افزایش همکاری‌های بین‌المللی، برای مقابله مؤثر با این تهدیدات، امری حیاتی است.

منابع

۱. منابع فارسی

آگنج، مهرورز، شیخ‌الاسلامی، عباس و ولی‌پوری، معصومه. (۱۴۰۲). سیاست جنایی ایران و انگلیس در پیشگیری از وقوع جرایم سایبری. فقه جزای تطبیقی، ۳(۳)، ۱۸۵-۱۹۴.

بهرام‌نیا، نیما و ناصح‌زاده، سارا. (۱۴۰۳). بررسی تاثیر آگاهی قانونی نسبت به جرایم سایبری و پیشگیری از وقوع جرم. حقوق سایبری، ۱(۴)، ۷۴-۱۰۳.

سروری، علی‌محمد. (۱۴۰۱). بررسی تطبیقی دام‌گستری در حقوق افغانستان و انگلستان. یافته‌های جزا و جرم‌شناسی، ۲(۳)، ۸۵-۱۰۴.

شایق، علیرضا و ناجی‌زواره، مرتضی. (۱۳۹۵). مطالعه تطبیقی تحصیل دلیل کیفری در فضای سایبری در حقوق ایران، انگلستان و فرانسه با تأکید بر وظایف و اختیارات پلیس. پژوهش‌های حقوقی انتظامی، ۱(۲)، ۹۳-۱۱۶.

شکری، رضا. (۱۳۹۹). حریم خصوصی ارتباطات در فضای الکترونیکی از منظر حقوق کیفری ایران و انگلستان. حقوق و فناوری اطلاعات، ۱(۱)، ۶۵-۳۲.

دانکین، سوزان. (۱۳۹۸). پیشگیری از تروریسم و کنترل ریسک: بررسی تطبیقی دستورات نظارتی در انگلستان و استرالیا. ترجمه پیمان دولت‌خواه‌پاشاکی، تهران: خرسندی، چاپ اول.

فرهادی‌آلاشتی، زهرا. (۱۴۰۲). برساخت قضایی کنترل جرائم سایبری کودکان و نوجوانان: به‌سوی ارائهٔ نظریه‌ای داده‌بنیاد. مطالعات حقوق کیفری و جرم‌شناسی، ۵۲(۲)، ۳۰۰-۲۷۹.

حسینی‌اکبرنژاد، هاله و جواهری‌آراسته، محسن. (۱۳۹۹). حمایت کیفری از کودکان درمقابل سوءاستفاده در فضای مجازی در قوانین ایران و انگلیس و اسناد بین‌المللی. پژوهش‌های حقوقی، ۱۹(۴۴)، ۱۰۷-۱۳۲.

کریمی، نسترن و نیک‌روش، سامان. (۱۴۰۳). جرایم سایبری سازمان‌یافته و فیشینگ: رویکردهای حقوقی در سطح بین‌المللی. حقوق سایبری، ۱(۲)، ۸۳-۶۶.

محمدنسل، زهرا، محمدنسل، غلامرضا و گلدوزیان، ایرج. (۱۳۹۹). مطالعه تطبیقی دسترسی غیرمجاز به داده ها و سامانه های رایانه ای در قوانین کیفری ایران و انگلستان و فرانسه. پژوهش‌های اطلاعاتی و جنایی، ۱۵(۳)، ۸۱-۱۰۶.

موسوی، سیدجمال، روحانی‌مقدم، محمد و آقایی‌بجستانی، مریم. (۱۴۰۱). حمایت از اطفال بزه‌دیده فضای سایبری با تأکید بر نحوه جبران خسارت. فقه جزای تطبیقی، ۲(۲)، ۱۲۷-۱۳۷.

نمامیان، پیمان. (۱۴۰۴). ملاحظات حقوق بشری سازمان‌ها و نهادهای جهانی برای مقابله با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی. حقوق سایبری، ۲(۳)، ۱-۱۹.

وزیردفتر، امید. (۱۴۰۳). سایبر تروریسم و خلأهای حقوق کیفری بین‌المللی: نیاز به تدوین کنوانسیون جهانی جرایم سایبری. حقوق سایبری، ۱(۳)، ۸۳-۷۲.

۲. منابع انگلیسی

Bada, Maria., & Nurse, Jason R. C. (2019/20). The social and psychological impact of cyber-attacks. In Benson, M., & McAlaney, J. (Eds.), Emerging cyber threats and cognitive vulnerabilities (pp. 1–21). Academic Press.

Banaji, Shakuntala., & Bhat, Ramnath. (2022). Social media and hate. Routledge.

Brouwer, Evelien. (2021). Private life and data protection in the area of freedom, security and justice. In Sara Iglesias Sánchez & Maribel González Pascual (Eds.), Fundamental rights in the EU area of freedom, security and justice (pp. 373–393). Cambridge University Press.

Burke, P. (2021). National counter-terrorism responses: United Kingdom. In P. Burke (Ed.), et al., Global jihadist terrorism: Terrorist groups, zones of armed conflict and national counter-terrorism strategies (pp. 233-252). Edward Elgar Publishing.

Chan, Tom., et al. (2016). The UK National Data Guardian for health and care's review of data security, consent and opt-outs: Leadership in balancing public health with rights to privacy? BMJ Health and Care Informatics, 23(3), 627–632.

Chang, Brian. (2018). From internet referral units to international agreements: Censorship of the internet by the UK and EU. Columbia Human Rights Law Review, 49(2), 114-212.

Coupland, Robin., & Taback, Nathan. (2024). Cyber-sensorium: An extension of the cyber public health framework. Computers and Society, Cornell University. https://arxiv.org/abs/2406.05929?utm_source=chatgpt.com

Draghici, Carmen. (2011). The human-rights compliance of UK anti-terrorism legislation in the light of domestic and international case law. In G. Guarino & I. D'Anna (Eds.), International institutions and cooperation: Terrorism, migrations, asylum (pp. 673–714). Satura Editrice.

Denniss, Emily., & Lindberg, Rebecca. (2025). Social media and the spread of misinformation: Infectious and a threat to public health. Health Promotion International, 40(2), 1-10.

Durodié, Bill., & Wainwright, David. (2018). Terrorism and post-traumatic stress disorder: A historical review. The Lancet Psychiatry, 6(1), 61–71.

Edelstein, Michael., et al. (2018). Strengthening global public health surveillance through data and benefit sharing. Emerging Infectious Diseases, 24(7), 1324–1330.

Evan, T., et al. (2017). Cyber terrorism: Assessment of the threat to insurance. Cambridge Risk Framework Series. Centre for Risk Studies, University of Cambridge.

Ghafur, S., et al. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. npj Digital Medicine, 2(1), 1-7.

Graziani, Chiara. (2021). Removing terrorist content online: The intersection between the international, regional, and domestic level. In Arianna Vedaschi & Kim Lane Scheppele (Eds.), 9/11 and the rise of global anti-terrorism law: How the UN Security Council rules the world (pp. 222–241). Cambridge University Press.

Lancry, Teresa., et al. (2023). Cyber victimisation, restorative justice and victim-offender panels. Asian Journal of Criminology, 18(1), 61–74.

Li, Susan., et al. (2025). Cyber-attacks on hospital systems: A narrative review. The American Journal of Geriatric Psychiatry: Open Science, Education, and Practice, 7, 30–39.

Macdonald, Stuart., et al. (2019). Regulating terrorist content on social media: Automation and the rule of law. International Journal of Law in Context, 15(2), 183–197.

Mughal, Rabya., et al. (2023). Public mental health approaches to online radicalisation: An empty systematic review. International Journal of Environmental Research and Public Health, 20(16), 65-86.

Pavlova, Pavlina. (2020). Human-rights based approach to cybersecurity: Addressing the security risks of targeted groups. Peace Human Rights Governance, 4(3), 391-418.

Piasecki, Stanislaw., & Chen, Jiahong. (2022). Complying with the GDPR when vulnerable people use smart devices. International Data Privacy Law, 12(2), 113–131.

Prentice, Shery., & Taylor, Paul J. (2018). Psychological and behavioral examinations of online terrorism. In Violent extremism (pp. 450–470). IGI Global.

Seh, Adil Hussain., et al. (2020). Healthcare data breaches: Insights and implications. Healthcare (Basel), 8(2), 128-141.

Shortland, Neil D., et al. (2021). A public health ethics model of countering violent extremism. Terrorism and Political Violence, 33(2), 324–337.

Walker, Clive. (2006). Cyber-terrorism: Legal principle and law in the United Kingdom. Dickinson Law Review, 110(3), 625-665.

Walton, Oliver., & Johnstone, Andrew. (2024). The fragmentation of the security-development nexus: The UK government's approach to security and development 2015-2022. Peacebuilding, 12(3), 429–444.

Wołyniec, Jakub. (2018). The UK government's response to cyber threats. Teka Komisji Politologii i Stosunków Międzynarodowych, 13(2), 143–154.

Ulmer, Nitzan., et al. (2022). Terrorist attacks against hospitals: World-wide trends and attack types. Prehospital and Disaster Medicine, 37(1), 25–32.

Zarmsky, Sarah. (2024). Is international criminal law ready to accommodate online harm? Challenges and opportunities. Journal of International Criminal Justice, 22(1), 169–184.

Zedner, Lucia. (2021). Countering terrorism or criminalizing curiosity? The troubled history of UK responses to right-wing and other extremism. Common Law World Review, 50(1), 57-75.