



Shiraz University
RiCeST
ISC

ISSN: 2008-7926

Journal of

Legal Studies

Vol. 18, Issue 3, Autumn 2026

JLS

Journal of Legal Studies

Journal Homepage: <https://jls.shirazu.ac.ir/>
doi: <https://10.22099/JLS.2025.53777.5354>



Research Article

Responding to The Fundamental Human Rights Challenges Arising from The Dissemination of Terrorist Content Online in Light of the Counter-Terrorism Legal Regime of the EU

Peyman Namamian^{1*}, Ayatollah Jalili²

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

2. Assistant Professor, Department of Public Law, Faculty of Law, University of Qom, Qom, Iran

Article history:

Received: 24-07-2025

Accepted: 02-11-2025

Abstract

Introduction

In the digital age, terrorists have moved to the online space, and this shift has created new threats that necessitate the development of appropriate legal frameworks. One of the main challenges in this regard is the conflict between safeguarding freedom of speech and combating terrorist content. On the one hand, freedom of expression must be guaranteed, while on the other hand, this freedom may become a tool for promoting violence. On April 29, 2021, the European Union adopted Regulation 784/2021 to address the spread of terrorist content online. This regulation specifically focuses on preventing the abuse of online hosting services for disseminating terrorist content and serves as a complement to the EU's 2017 Directive on

Please cite this article as:

Namamian, P., Jalili, A (2026). Responding to The Fundamental Human Rights Challenges Arising from The Dissemination of Terrorist Content Online in Light of the Counter-Terrorism Legal Regime of the EU. *Journal of Legal Studies*, 18(3), 513-548. doi: <https://10.22099/JLS.2025.53777.5354>

* Corresponding author:

E-mail address: p-namamian@araku.ac.ir



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

countering terrorism, aiming to protect public security and prevent online harm. However, this regulation faces human rights challenges, especially in preserving fundamental individual rights and preventing violations of freedom of speech. Human rights activists have raised concerns regarding the impact of this regulation on fundamental rights. Consequently, the challenges in this area can be divided into two categories: 1) challenges related to human rights and the protection of freedom of expression, and 2) technical and operational challenges in monitoring and removing terrorist content.

Method

The article uses a descriptive-analytical approach to examine the challenges posed by EU Regulation 784/2021 in combating online terrorism. The findings indicate that although this regulation is a significant step in the fight against terrorism, it is essential to strike a proper balance between public security and fundamental individual rights to prevent violations of personal rights. Additionally, the article analyzes the nature and legal structure of crime, emphasizing the importance of maintaining this balance in the regulatory process.

Results and Discussion

In the digital space, issues related to content regulation, especially in the areas of "misinformation" and "terrorist content", have created complex legal and conceptual challenges. One of the most important challenges is the precise definition of "terrorist crimes", which remains a subject of dispute at the international level. These ambiguities have prevented terrorist concepts from effectively addressing new threats, such as digital terrorism. Digital terrorism not only poses a threat to national security but can also lead to violations of human rights and individual freedoms.

EU Regulation 784/2021, aimed at combating online terrorist content, identifies five main categories of such content: incitement to commit terrorist offenses, dissemination of terrorist information, participation in terrorist groups, instructions for making explosives, and threatening behavior. These regulations seek to transfer terrorist content from the physical space to the digital one, but there are still challenges in aligning terrorist concepts with the realities of the virtual space.

One of the complex issues is striking a balance between freedom of expression and national security. International conventions, such as the International Covenant on Civil and Political Rights, set limitations on state interference in freedom of speech. However, in the digital space, which operates globally and is complex, assessing these limitations is difficult, especially when the detection and management of terrorist content are not

easily achievable. This balance can lead to violations of human rights and digital freedoms, particularly when decisions are made without transparency and are cross-border in nature.

Regulation 784/2021 grants national authorities the power to issue orders for the removal of online terrorist content, but this process faces challenges. One of the challenges is the uncertainty in defining terrorist content and its consequences for freedom of expression. Concerns grow when non-transparent, cross-border decisions are made, as this could lead to violations of human rights and digital freedoms.

Regulations and laws must be updated in line with digital developments and new technologies. This process must be designed in such a way that it prevents the spread of terrorist content while ensuring that fundamental rights are not violated. Human rights approaches in countering digital terrorism should be designed to protect national security while respecting individual freedoms and human rights.

Conclusion

In recent decades, with the expansion of anti-terrorism regulations, crimes related to terrorism and the criminalization of radical speech have increased. The European Union has adopted regulations to address online terrorist content, but due to ambiguities in definitions and implementation approaches, these efforts have not been fully effective in preventing the spread of such content. The EU must adopt new regulations that increase legal transparency while simultaneously preserving freedom of expression. Effective solutions in this area include the use of advanced technologies such as artificial intelligence for the rapid identification of terrorist content, providing precise definitions of terrorist content, and strengthening cooperation between security authorities, IT experts, and judicial officials. Additionally, ensuring the protection of human rights and collaborating with human rights organizations to prevent violations of individual freedoms is of particular importance.

Keywords: Digital space, terrorist crimes, online terrorist content, human rights, EU Regulation 784/2021.

Ethical Considerations

Not applicable

Funding

Not applicable

Conflict of interest

The authors declare no conflict of interest



مقاله پژوهشی

پاسخ به چالش‌های اساسی حقوق بشر ناشی از انتشار محتوای تروریستی برخط در پرتو رژیم حقوقی ضد تروریستی اتحادیه اروپا

پیمان نامامیان^{۱*}، آیت‌اله جلیلی^۲

۱. دانشیار حقوق کیفری و جرم‌شناسی، دانشکده علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران

۲. استادیار گروه حقوق عمومی، دانشکده حقوق، دانشگاه قم، قم، ایران

تاریخ پذیرش: ۱۴۰۴/۰۸/۱۱

تاریخ دریافت: ۱۴۰۴/۰۵/۰۲

اطلاعات مقاله

چکیده

با گسترش فضای دیجیتال و نقش فزاینده اینترنت در تسهیل ارتباطات و انتقال محتوا، گروه‌های تروریستی نیز از این فضا برای تبلیغ، جذب نیرو و سازماندهی فعالیت‌های خود بهره‌برداری می‌کنند. در پاسخ به این تهدید فزاینده، اتحادیه اروپا مقررات ۲۰۲۱/۷۸۴ را تصویب کرد که هدف آن مقابله مؤثر با انتشار محتوای تروریستی برخط است. مقررات ۲۰۲۱/۷۸۴ اتحادیه اروپا برای مقابله با انتشار محتوای تروریستی برخط تصویب شد و ارائه‌دهندگان خدمات میزبانی را ملزم می‌سازد تا محتوای تروریستی را در مدت زمان کوتاه (یک ساعت) از دسترس خارج کنند. این مقررات به‌طور بی‌سابقه‌ای

استناد به این مقاله:

نامامیان، پیمان و جلیلی، آیت‌اله (۱۴۰۵). پاسخ به چالش‌های اساسی حقوق بشر ناشی از انتشار محتوای تروریستی برخط در پرتو رژیم حقوقی ضد تروریستی اتحادیه اروپا. *مجله مطالعات حقوقی*. ۱۸. (۳). ۵۴۸-۵۱۳.

E-mail address: p-namamian@araku.ac.ir

* نویسنده مسئول:

Copyright: C 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

یک رژیم حقوقی فراملی برای کنترل فضای دیجیتال ایجاد می‌کند. با این حال، چالش‌هایی قابل ملاحظه است؛ سرعت بالای انتشار محتوای تروریستی و خطر حذف نادرست محتوای غیرتروریستی که می‌تواند بر آزادی بیان تأثیر بگذارد. برای جلوگیری از این مشکلات، سازوکارهایی همچون حق اعتراض و نظارت قضایی بر حذف محتوا در نظر گرفته شده است. این مقررات گامی مهم در مبارزه با تروریسم دیجیتال است، اما باید از محدودسازی نادرست آزادی‌های فردی جلوگیری کرد و تعادل مناسبی میان امنیت و حقوق بنیادین حفظ شود. این مقاله با معرفی تلاش‌های اخیر اتحادیه اروپا برای مقابله با انتشار محتوای تروریستی برخط وفق مقررات ۲۰۲۱/۷۸۴، سعی بر آن دارد تا چالش‌های اساسی حقوق بشر را با پاسخ به این پرسش که رژیم حقوقی ضدتروریستی اتحادیه اروپا تا چه حد امکان مقابله با انتشار محتوای تروریستی برخط را برای حفاظت از موازین حقوق بشری دارد؟ با روش پژوهش توصیفی تحلیلی مورد سنجش قرار دهد.

واژگان کلیدی: فضای دیجیتال، جرایم تروریستی، محتوای تروریستی برخط، حقوق بشر، مقررات ۲۰۲۱/۷۸۴ اتحادیه اروپا.

سرآغاز

توسعه فناوری‌های نوین در زمینه حقوق بشر، دو جنبه متناقض دارد؛ از یک‌سو، این فناوری‌ها می‌توانند به مستند سازی نقض حقوق بشر، تسهیل دسترسی به اطلاعات و تقویت پاسخگویی کمک کنند؛ اما از سوی دیگر، همین فناوری‌ها می‌توانند به ابزاری برای نقض حقوق بشر تبدیل شوند؛ نظیر نظارت گسترده، تهدید حریم خصوصی و استفاده از آن‌ها در سرکوب سیاسی یا نقض آزادی‌های فردی. از این‌رو، برای حفاظت از حقوق بشر، باید تعادلی میان استفاده مثبت از فناوری‌ها و مقابله با سوءاستفاده‌های آن برقرار کرد. این امر نیازمند تدوین استانداردهای حقوقی و مقررات دقیق برای حفظ حریم خصوصی و آزادی‌های فردی است.

در عصر دیجیتال، تروریست‌ها عملیات خود را به فضای برخط منتقل کرده‌اند که موجب افزایش محتوای تروریستی دیجیتال شده است. این امر، تهدیدهای نوینی ایجاد کرده که نیازمند چارچوب‌های قانونی جدید است. یکی از چالش‌های مهم، تعارض میان حق آزادی بیان و مقابله با محتوای تروریستی است. از یک‌سو، باید آزادی بیان حفظ شود و از سوی دیگر، این آزادی ممکن است برای ترویج افکار خشونت‌آمیز استفاده شود. نهادهای مجری قانون نیز قلمرو نظارتی خود را به دنیای دیجیتال گسترش داده‌اند که ممکن است با نقض حقوق بشر و آزادی‌های فردی همراه باشد. چالش اصلی در این حوزه حفظ تعادل میان امنیت و حقوق بشر است که نیازمند شفافیت و نظارت‌های مستقل است (Clifford, 2021: 16).

در ۲۹ آوریل ۲۰۲۱، اتحادیه اروپا مقررات ۲۰۲۱/۷۸۴ را در مورد رسیدگی به انتشار محتوای تروریستی برخط به‌عنوان یکی از مصادیق «آسیب‌های برخط» تصویب کرد.^۱ آسیب‌های برخط مشتمل بر اقسامی از اعمال یا رفتارهایی است که از طریق

1. Defined in: Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing the Dissemination of Terrorist Content

ابزارهای برخط ارتکاب می‌یابند و قلدری برخط، آزار و اذیت اینترنتی تا سوءاستفاده جنسی برخط و به اشتراک‌گذاری محتوای خشونت‌آمیز یا افراطی از مصادیق آن‌ها هستند. در چارچوب حقوق بین‌المللی، ضرورت مقابله با این دسته از آسیب‌ها از طریق قطعنامه ۷۶/۲۲۷ مصوب ۲۴ دسامبر ۲۰۲۱ مجمع عمومی سازمان ملل متحد به رسمیت شناخته شده است. حال، هیچ اقدام رسمی وفق اسناد حقوق بین‌المللی در قبال آسیب‌های برخط اتخاذ نشده است (Zarmsky, 2024: 172-173).

به هر روی، هدف مقررات ۲۰۲۱/۷۸۴ «تعیین مقررات یکسان برای رسیدگی به سوءاستفاده از خدمات میزبانی برای انتشار محتوای تروریستی برخط به عموم مردم است». این مقررات از طریق تمرکز بر عناصر مجازی به‌جای عناصر ملموس مقابله با جرائم تروریستی، مکمل رژیم حقوقی تنظیم شده وفق «دستورالعمل اتحادیه اروپا راجع به مقابله با تروریسم» در سال ۲۰۱۷ است.^۱ در ضمن، اتحادیه اروپا موازین «مقابله با انتشار محتوای تروریستی برخط»^۲ را در نتیجه قطعنامه ۱۷ آوریل ۲۰۱۹ تصویب کرد که هدف آن پیشگیری از «سوءاستفاده از خدمات میزبانی برای اهداف تروریستی و کمک به امنیت عمومی در اروپا است». سند مزبور به‌طور خاص نسبت به آنچه می‌تواند توسط «سرویس‌های میزبانی» (سکوها‌های رسانه‌های اجتماعی) در تنظیم محتوا و حذف انجام شود، تمرکز دارد. برخی از بخش‌های بحث‌برانگیزتر طرح، نظیر الزام حذف محتوای تروریستی ظرف یک ساعت پس از ارسال، کاهش یافته بود تا به شرکت‌های بخش خصوصی، زمان بیشتری برای تکمیل این کار داده شود.

Online (O.J. L 172, 17 March 2021, p. 79) [hereinafter 'Regulation (EU) 2021/784'], Article 2 (1).

1. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on Combating Terrorism and Replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (O.J. L 88, 31 March 2017, p. 6) [hereinafter 'Directive (EU) 2017/541'].

2. https://www.europarl.europa.eu/doceo/document/TA-8-2019-0421_EN.pdf?redirect.

در جریان مذاکرات مقررات اتحادیه اروپا در خصوص رسیدگی به انتشار محتوای تروریستی برخط، فعالان حوزه دیجیتال و حقوق بشر، نگرانی‌هایی را در پیرامون حفظ حقوق اساسی بشر مطرح کردند؛ این بازیگران، تا حدی در تأثیرگذاری بر ابعاد متن نهایی مقررات موفق بودند و این پرسش را مطرح کردند که «چگونه چنین گروه‌هایی توانسته‌اند بر سیاست سنتی ضد تروریستی امنیتی شده تأثیر بگذارند؟» این موضوع از دریچه سیاسی سازی نشان می‌دهد، به‌رغم ادامه گفتمان‌های امنیتی سازی، برخی از ابعاد مقررات مقابله با جرائم تروریستی اتحادیه اروپا قابل اعتراض است (Ahmed, 2023: 1).

چالش‌هایی که در این رابطه قابل استنتاج خواهد بود، در دو زمینه است؛ از یک‌سو، به‌گونه‌ای عمدتاً غیرمستقیم، انتشار محتوای واقعی تروریستی برخط، بهره‌مندی افراد از حقوق بشر، به‌ویژه حق زندگی و حق آزادی و امنیت شخصی را با مخاطره‌هایی مواجه خواهد کرد (Macklin, 2019: 18). از سوی دیگر، هرگونه تحمیل نادرست دستور حذف راجع به اقدام‌های گفتاری تروریستی فرضی، آثار مجدانه‌ای بر آزادی بیان و آزادی دریافت و انتشار اطلاعات و ایده‌ها که وفق ماده ۱۰ کنوانسیون اروپایی حقوق بشر، ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی و ماده ۱۱ منشور حقوق اساسی اتحادیه اروپا است، خواهد داشت (Pirkova et al., 2021: 97-98). به دیگر تعبیر، می‌توان چالش‌ها را در دو سطح مطرح کرد؛ الف. چالش‌ها در حفاظت و تضمین رعایت حقوق بشر؛ نظارت بر محتوای برخط و حذف سریع آن ممکن است منجر به نقض آزادی بیان و حقوق کاربران شود. اتحادیه اروپا باید در طراحی مقررات خود به‌گونه‌ای عمل کند که از آزادی‌های فردی محافظت کند و در عین حال امنیت عمومی را تأمین کند. ب. چالش‌های فنی و عملیاتی؛ الگوریتم‌ها و سامانه‌های خودکار ممکن

است قادر به شناسایی تمام انواع محتوای تروریستی نباشند و این می‌تواند باعث بروز مشکلات در نظارت و مدیریت صحیح محتوای برخط شود.^۱

این مقاله با روش توصیفی - تحلیلی، در چارچوب مقررات ۲۰۲۱/۷۸۴ اتحادیه اروپا و اهداف آن، به بررسی و تحلیل جرم از حیث ماهیت و ساخت حقوقی آن می‌پردازد. در این فرآیند، با تحلیل مقررات مذکور و مقایسه آن‌ها با اصول حقوق بشر، به ارزیابی ظرفیت این مقررات برای اجرای دستور حذف محتوای تروریستی برخط در رژیم حقوقی اتحادیه اروپا پرداخته می‌شود. مقاله به این پرسش پاسخ می‌دهد که «مقررات ۲۰۲۱/۷۸۴ اتحادیه اروپا چگونه با انتشار محتوای تروریستی برخط مقابله می‌کند؟» و تلاش دارد تا ابعاد مختلف این مقررات و تناسب آن با حقوق اساسی و آزادی‌های فردی را مورد بررسی قرار دهد. در این راستا، مفاهیم اصلی مرتبط با مقررات ۲۰۲۱/۷۸۴ نظیر «محتوای تروریستی»، «دستور حذف» و «حقوق بشر» به تفصیل بررسی می‌شود و چالش‌ها و فرصت‌های این مقررات در مقابله با انتشار محتوای تروریستی در فضای دیجیتال تحلیل می‌شود. در ضمن، مقاله به ارزیابی عملی این مقررات و تأثیرات آن بر آزادی بیان، امنیت عمومی و نحوه برخورد با محتوای برخط خواهد پرداخت.

۱. توصیف جرم؛ چالش‌های حقوقی و مفهومی در تعریف و مقابله با محتوای

تروریستی برخط

در مقایسه با سایر اصطلاحات انتزاعی مورد استفاده در هنگام بحث راجع به تنظیم محتوا در فضای دیجیتال، نظیر «اطلاعات نادرست» و مفهوم «محتوای تروریستی» اصولاً به دلیل تأثیر متقابل آن با تعاریف قانونی جرائم تروریستی، این امکان فراهم

1. European Commission. (2020). Regulation on terrorist content online (EU) 2021/123. <https://ec.europa.eu>

می‌شود تا چالش‌هایی ایجاد گردند. حال، تعاریف حقوقی جرائم تروریستی از نظر سیاسی و حقوقی در سطح بین‌المللی بحث‌برانگیز باقی می‌ماند؛ زیرا این جرائم هنوز یک «مفهوم اساساً مورد مناقشه» است که جامعه بین‌المللی در تلاش برای دستیابی به توافق در خصوص آن است. به همین دلیل، اسناد حقوقی بین‌المللی راجع به مقابله با جرائم تروریستی همچنان در معرض تعاریف سیاست زده و غیرحقوقی قرار می‌گیرند که امکان انعکاس جلوه‌های جرائم تروریستی معاصر، نظیر انتشار محتوای تروریستی در فضای دیجیتال را به‌طور کافی ندارند.^۱

مقررات اتحادیه اروپا ۲۰۲۱/۷۸۴ محتوای تروریستی برخط را با قرار دادن آن در پنج دسته، مورد تعریف قرار می‌دهد؛ هر پنج محور حول مجموعه‌ای از جرائم تروریستی که در دستورالعمل اتحادیه اروپا درباره مقابله با آن مفهوم‌سازی شده است، تکامل می‌یابند که به‌طور مجموع تعریف قانونی اتحادیه اروپا از جرائم تروریستی را تشکیل می‌دهند: الف. مطالبی که جرائم تروریستی را تحریک می‌کند (نظیر تحریک غیرمستقیم به واسطه تمجید از اقدام‌های تروریستی)؛ ب. اطلاعاتی که به انتشار و انعکاس جرائم تروریستی کمک کند؛ ج. مسائلی که خواستار مشارکت در فعالیت‌های یک گروه تروریستی است؛ د. موادی که دستورالعمل‌هایی راجع به استفاده از مواد منفجره، سلاح‌ها و مواد ارائه می‌دهد؛ هـ. رفتارهای تهدیدآمیز به مثابه جرائم تروریستی اطلاق شود.

مقررات اتحادیه اروپا به‌طور معمول، بر جرائم تروریستی فیزیکی مانند حمله به افراد یا تخریب اموال عمومی متمرکز است، بر اساس تصمیم چارچوب ۲۰۰۲. مقررات ۲۰۲۱/۷۸۴ این رویکرد را به فضای دیجیتال منتقل کرده و بر محتوای تروریستی برخط تأکید دارد. این مقررات اگرچه جرائم جدیدی ایجاد نمی‌کند، اما مفاهیم تروریسم را از

1. For example, UN Security Council Resolution 1373, U.N.Doc. S/RES/1373 (Sep. 28, 2001); UN Security Council Resolution 2178, U.N.Doc. S/RES/2178 (Sep. 24, 2014); and UN Security Council Resolution 2396, U.N.Doc. S/RES/2396 (Dec. 21, 2017).

فضای فیزیکی به مجازی منتقل می‌سازد. با این حال، چالش اصلی در تطبیق دقیق «محتوای تروریستی برخط» با مفاهیم فیزیکی است. در فضای دیجیتال، تأثیرات تروریستی به‌طور غیرمستقیم و جهانی بروز پیدا می‌کند که نیاز به دقت بیشتر در تعریف و شناسایی محتوای تروریستی دارد.

از آنجایی که مقررات به‌شدت بر تعریف جرم تروریستی وفق ماده ۳ دستورالعمل مقابله با تروریسم تکیه دارد، برخی از ایرادات اساسی این سند قانونی را نیز مدنظر قرار داده است.^۱ مقدمه دستورالعمل حاوی یک بند استثنا است که تصریح می‌کند این دستورالعمل «فعالیت‌های نیروهای مسلح در طول مخاصمات مسلحانه را کنترل نمی‌کند». اسناد حقوقی بین‌المللی راجع به مقابله با جرائم تروریستی به‌طور فزاینده‌ای برای تعریف دقیق جرم تروریستی می‌توانند به‌طور قانونی به‌عنوان جرائم تروریستی طبقه‌بندی شوند (Bartels). از آنجا که تعریف دستورالعمل از این جرائم، تا حد زیادی تعیین می‌کند که محتوای برخط چه محتوای تروریستی را تشکیل می‌دهد، بند حذف دستورالعمل نیز تعریف محتوای تروریستی را پیش‌بینی کرده و می‌تواند منجر به نتایج مشکوک و نامتقارن شود.

جرم تروریستی در چارچوب مقررات اتحادیه اروپا، افزون بر عدم قطعیت راجع به کاربرد آن برای اعمالی که در چارچوب یک مخاصمه مسلحانه ارتکاب می‌یابد، دارای نقص‌های ذاتی دیگری است که بر تلاش‌ها برای مقابله با محتوای تروریستی در فضای دیجیتال تأثیر می‌گذارد؛ با توجه به یافته‌های موجود، آنچه واضح است اهداف و عناصر ذهنی تعریف چالش‌هایی را برای حاکمیت قانون ایجاد می‌کنند؛ زیرا عبارات گسترده آن‌ها نمی‌تواند اطمینان حقوقی و قابل پیش‌بینی را برای افراد فراهم کند و منجر به تنش با اصل قانونی بودن می‌شود (Reinisch, 2004: 102). البته گستردگی دامنه تعریف اتحادیه اروپا، اعمالی را به همراه می‌آورد که به‌هیچ‌وجه نمی‌توان آن‌ها را در اصطلاح

1. Directive (EU) 2017/541, Recital 37, Preamble.

رایج تروریستی در محدوده آن و مفهوم محتوای تروریستی توصیف کرد. به عنوان نمونه، تعریف اتحادیه اروپا از جرم تروریستی، در خصوص اعمالی استعمال می‌شود که عبارت «باعث تخریب گسترده یک دارایی خصوصی شده که احتمالاً منجر به زیان اقتصادی بزرگ می‌شود» و با هدف «بی‌ثباتی جدی ساختارهای اساسی سیاسی، قانون اساسی، اقتصادی یا اجتماعی یک کشور» کاربرد پیدا کند.

وفق تعریف اتحادیه اروپا از جرم تروریستی مقرر در مقررات ۲۰۱۷ و تصمیم چارچوب ۲۰۰۲ برای هماهنگی مقررات کیفری اروپا در حوزه مقابله با تروریسم طراحی شده است؛ حتی اگر این مسئله که «تا چه حد در انجام این امر موفق بوده است» قابل بحث باشد، تأثیر عمیق آن بر نظام‌های حقوق کیفری داخلی غیر قابل انکار است. ملاحظات مشابهی راجع به دستورهای حذف برای حذف محتوایی وجود دارند که از یک فرد یا گروهی از افراد، برای شرکت در فعالیت‌های یک گروه تروریستی دعوت می‌کند (Decoeur, 2017: 306-309). وفق مقررات مقابله با جرائم تروریستی اتحادیه اروپا، مفهوم «گروه تروریستی» باید به صورت موردی و با مشخص کردن سوءنیت تروریستی گروه مورد سنجش قرار گیرد. البته به جای اشاره به گروه‌های تروریستی یا سازمان‌های تروریستی که به طور کامل فهرست شده‌اند، هر گروه آزاد حداقل از سه عضو می‌تواند به مثابه یک گروه تروریستی قابل اطلاق باشد. با توجه به ابهام میزان مشارکت و ساختار یک گروه تروریستی، نمی‌توان رد کرد که مفهوم بی‌پایان گروه تروریستی، می‌تواند منجر به استقرار وضعیت دهشتناک در چارچوب یک ساختار نظیر کشور و اثرگذاری آن در نقض امنیت ملی شود.

۲. چالش‌های برقراری توازن میان آزادی بیان و امنیت ملی در مقررات ۲۰۲۱/۷۸۴

اتحادیه اروپا

ملاحظات امنیت ملی، به عنوان بخشی از الزام هرگونه مداخله در آزادی بیان که در یک جامعه دموکراتیک ضروری است، نسبت به برخی دلایل بالقوه مشروع دیگر برای محدود کردن گفتار و سایر شیوه‌های بیان، کمتر برجسته شده است (Skjoldager, 2020: 129-131). تغییر شرایط اجتماعی، فناوریانه و بین‌المللی مستلزم درک دقیقی از آزادی بیان در اینترنت و در ارتباط با امنیت ملی است. در مفهوم هنجاری، اطلاعات نادرست برخلاف استفاده از رویکردهای فناوری نوین، نظیر الگوهای زبان بزرگ و هوش مصنوعی مولد، نمی‌تواند کاملاً کنترل نشده باقی بماند. از نظر اخلاق کاربردی، ارزش‌های بیشتری را می‌توان در معرض استدلال و ارزیابی قرار داد. با توجه به تحلیل دادگاه اروپایی حقوق بشر، تمرکز خاص‌تری بر اطلاعات نادرست ممکن است مرتبط باشد و سایر محدودیت‌های مرتبط بدون تکیه بر استدلال امنیت ملی، قابل بررسی باشد (Martin Tomažič, 2024: 7-8). در عین حال، تجزیه و تحلیل محتوا را می‌توان وفق تصمیم‌های دیوان حقوق بشر اروپا و بحث‌های علمی مرتبط صورت داد تا احراز شود که چه ارزش‌هایی همراه با آزادی بیان و امنیت ملی، به عنوان مفاهیم متنی ترسیم می‌شوند.

معیارهای معاصر حاکم بر آزادی بیان در اروپا توسط کنوانسیون اروپایی حقوق بشر، شکل گرفته است که در ۴ نوامبر ۱۹۵۰ امضا شد. این کنوانسیون، در درجه اول به دنبال رسیدگی به جنایات جنگ جهانی دوم بود؛ به این ترتیب، کنوانسیون بخشی از دستور کار گسترده‌تر حقوق بشر بود که شامل اعلامیه جهانی حقوق بشر نیز می‌شد. این کنوانسیون طیف وسیعی از حقوق بشر را برای شهروندان کشورهای عضو شورای اروپا که به‌طور تقریبی همه کشورهای اروپایی را شامل می‌شد، تضمین می‌کرد.^۱ این

1. http://www.echr.coe.int/Documents/Convention_ENG.pdf.

کنوانسیون، دیوان حقوق بشر اروپا را به‌عنوان مرجعی قضایی برای افراد، برای طرح دعوی حقوق اساسی بشر علیه دولت‌های اروپایی ایجاد کرد. احکام حاکی از نقض، برای کشورهای مربوطه الزام‌آور است و آن‌ها موظف به اجرای آن هستند. حال، کنوانسیون تشخیص داد که آزادی بیان یک حق مطلق نیست.

ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی، به‌صراحت از حق آزادی بیان حمایت می‌کند و محدودیت‌هایی که دولت‌ها می‌توانند بر آن اعمال کنند را به‌طور جدی محدود می‌سازد. با این حال، در بند ۳ این ماده، حفظ «امنیت ملی» یا «نظم عمومی» به‌عنوان اهداف موجه برای اعمال محدودیت‌ها پذیرفته شده، ولی این محدودیت‌ها باید با اصول قانونی و ضرورت‌هایی خاص تطابق داشته باشد. بسیاری از کشورها از این مقررات کلی در حقوق بین‌المللی بهره برده‌اند تا در قوانین مقابله با تروریسم، اقداماتی را که مربوط به انتشار عقایدی که ممکن است تروریسم را تحریک، تأیید یا تشویق کند، جرم‌انگاری کنند. تعیین مرز بین اظهارات افراطی، چالش‌برانگیز یا توهین‌آمیز که به‌طور مشروع تحت حمایت حقوق بشر قرار دارند و عباراتی که ممکن است به آسیب یا تهدیدات غیر قابل قبول منجر شوند، در بسیاری از موارد پیچیده است. اشتباه در ارزیابی این مرزها می‌تواند تأثیر منفی بر آزادی تبادل افکار و مباحثه در مورد موضوعات مختلف داشته باشد.

چارچوب ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی و ماده ۱۰ منشور حقوق اساسی اتحادیه اروپا دارای نکاتی است که در این ارتباط دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد تأکید دارد در عمل، ایجاد توازن مناسب بین حفظ حق آزادی بیان و اجرای مقررات کیفری با هدف تحریک جرائم تروریستی همچنان چالشی برای دولت‌ها است. افزون بر این، دبیر کل سازمان ملل متحد با بیان این موضوع موافقت کرد «اتخاذ هرگونه تعریف بیش‌ازحد مبهم یا گسترده از واژه تروریسم در مقررات داخلی می‌تواند منجر به جرم‌انگاری رفتاری شود که به‌عنوان تروریسم به شمار نیاید.»

گزارشگران سازمان ملل متحد در مورد آزادی بیان تأکید کرده‌اند، مفاهیم «افراط‌گرایی خشونت‌آمیز» و «افراط‌گرایی» نباید به مثابه مبنایی برای محدودیت آزادی بیان مورد استفاده قرار گیرند، مگر اینکه به وضوح تعریف شده باشند و به طور مشخص برای حمایت از حقوق دیگران، امنیت ملی یا نظم عمومی ضروری و متناسب است.^۱ گزارشگر ویژه، نژادپرستی و بیگانه‌هراسی را به جای تروریسم، «جدی‌ترین تهدید برای دموکراسی» می‌داند (Hashemi, 2021: 151). البته گزارشگر ویژه در زمینه ارتقا و حمایت از حقوق و آزادی‌های اساسی بشر در مقابله با جرائم تروریستی بر لزوم محدودیت جرم‌انگاری عبارات به مواردی که در آن‌ها وجود دارد، تأکید کرده است (Perrigo, 2020: 1).

از منظر حقوق بشر، کاربران سکوهایی برخط به طور کلی در هنگام ارسال محتوا به صورت برخط از آزادی بیان محافظت می‌شوند. حال، چنین محتوایی نیز تابع یک سری مقررات تعدیل خصوصی، الزامات جامعه یا شرایط خدمات است که توسط خود سکوها تعریف شده‌اند. این امر، به ویژه در مورد محتوای تروریستی برخط مرتبط است؛ زیرا به موازات مقررات ضد تروریستی ملی و موازین بین‌المللی، سکوها سیاست‌های خاص خود را در این زمینه حساس تنظیم کرده‌اند.

مقامات ملی وفق مقررات ۲۰۲۱/۷۸۴ اتحادیه اروپا، این امکان را دارند تا دستور حذف صادر کنند تا ارائه دهندگان خدمات میزبانی را ملزم به حذف محتوای تروریستی یا غیرفعال کردن دسترسی به محتوای تروریستی در کلیه کشورهای عضو کند. ماده ۵ شامل مجموعه‌ای از سازوکارهای پیشگیرانه است که به طور قطع، نقش واسطه‌ها را در این زمینه به ویژه مسئولیت نظارت بر محتوای آن‌ها تغییر می‌دهد؛ زیرا آن‌ها تکلیف را دارند تا سازوکارهای خاصی را برای محافظت از خدمات خود، در برابر انتشار محتوای تروریستی به مردم اتخاذ کنند. نهادهای دولتی، هم‌چنین این اختیار را خواهند داشت که

1. <http://www.oas.org/en/iachr/expression/showarticle.asp?artID=650&IID=1>.

چنین سازوکارهایی را با اهداف آیین‌نامه بررسی و درخواست کنند؛ اگرچه مقررات اجازه تحمیل الزام استفاده از ابزارهای خودکار را نمی‌دهد، ماهیت خاص تعهدها و مسئولیت‌های وفق مقررات ممکن است به‌طور عملی، تعیین کننده استفاده فعال از این نوع فنون تعدیل باشد (York, 2018: 1).

با این مقررات، اتحادیه اروپا به‌طور فزاینده‌ای به واگذاری مسئولیت‌های اجرای قانون به شرکت‌های خصوصی نزدیک می‌شود که در این روند کاربران اینترنت و ارائه دهندگان خدمات میزبانی از حمایت‌های قانونی و رویه‌ای که پیشتر برای این‌گونه تصمیم‌ها وجود داشت، محروم می‌شوند. سکوه‌ای دیجیتال ممکن است به تدریج در موقعیتی قرار گیرند که مجبور شوند تصمیمات گسترده‌ای اتخاذ کنند. باید توجه داشت که چنین سیاست‌هایی از یک سو می‌توانند به نقض آزادی بیان منجر شوند، زیرا ممکن است محتوای غیر تروریستی نیز حذف شود و از سوی دیگر، با خصوصی‌سازی سکوها ممکن است تهدیدات امنیتی ملی کشورها افزایش یابد. هر رویکردی که به ریشه‌های عمیق افراط‌گرایی و رفتار تروریستی توجه نکند و آن‌ها را تحت نظارت دقیق قرار ندهد، نمی‌تواند موفق باشد. برای محافظت مؤثر از سکوها در برابر تهدیدات تروریستی، لازم است که سیاست‌ها و اقدامات مناسب و دقیق تعریف شوند.

۳. از «توازن میان مقابله با محتوای تروریستی برخط» تا «حفظ آزادی بیان»

این تصور که شکاف در قانون وجود دارد، درواقع به علت اهمیت فضای دیجیتالی در جهان امروز است که می‌تواند شکاف بسیار مهمی باشد. بر اساس این رویکرد، موازین حقوق بشر برای پرداختن به چالش‌های نوین ناکافی تلقی می‌شوند؛ صرفاً به این دلیل که صراحتاً برای جهانی که ویژگی آن دیجیتالی سازی، رشد تصاعدی داده‌ها و جریان‌های ارتباطی، نسبی سازی مرزهای بین‌المللی بین دولت‌های مستقل و ظهور برخی بازیگران خصوصی فوق‌العاده قدرتمند که بر قلمرو دیجیتال تسلط دارند. در ضمن، قابل درک است رویکرد دیگری در بحث‌های معاصر پدیدار شده و مفروض

است، چالش‌های حقوق بشر در فضای دیجیتال به بهترین وجه از طریق تصویب مقررات جدید قابلیت حل و فصل دارند (Brkan, 2020: 701-702).

فرآیند سیاسی تدوین دستورالعمل‌ها، اعلامیه‌ها یا موازین جدید اخلاقی است که می‌تواند مورد توجه قرار گیرد؛ به دنبال رسیدگی به چالش‌های حقوقی نوپدید، نظیر برخی مسائل راجع به «اخلاق» یا «حقوق انسانی»، با رد رویکردهای اخیر، باید اذعان داشت با ساختار موجود در چارچوب موازین حقوق بشر امکان پرداختن به چالش‌های عمده حوزه دیجیتال از طریق رویکرد سومی برقرار شود که ماهیت تفسیری دارد؛ جدی گرفتن مفاهیم، اصول و اندیشه‌های حقوقی زیربنای موازین موجود و سایر منابع قانونی حاکم در حقوق بشر، پرداختن به چالش‌های حقوق بشری را که در فضای دیجیتالی پدید می‌آیند، ممکن می‌سازد. همین رویکرد در مواضع اغلب متحول‌کننده‌ای که کمیته حقوق بشر ملل متحد برای رسیدگی به چالش‌های نوین و پیچیده نظیر کودتای نظامی در اروگوئه^۱ منعکس می‌شود.

با توجه به تحولات حوزه دیجیتال، چالش‌های جدیدی در زمینه حقوق بشر به وجود آمده‌اند که از آن‌ها نمی‌توان به‌طور کامل به‌عنوان خلاءهای قانونی یاد کرد. رویکرد «بازگشت به اصول» که بر تکیه بر اصول موازین حقوق بشر تأکید دارد، به‌ویژه در مواجهه با محتوای تروریستی برخاسته، می‌تواند فرایند رسیدگی به این چالش‌ها را تسهیل کند. ایجاد سازوکاری مبتنی بر حقوق بشر برای مقابله با تهدیدات ناشی از فعالیت‌های گروه‌ها یا افراد تروریستی، حتی آن‌هایی که منابع مالی، فناوری یا لجستیکی قابل توجهی ندارند، ضروری است. این سازوکار باید ارتباط میان تبلیغات تروریستی و هدف یا مشارکت در تحریک دیگران به خشونت و تروریسم را در نظر گیرد.

1. H.R. Committee, Lopez Burgos v Uruguay, Communication No. 52/1979, 29 July 1981 (CCPR/C/13/D/52/1979). H.R. Committee, Leopoldo Buffo Carballal v Uruguay, Communication No. 33/1978, 27 March 1981 (CCPR/C/12/D/33/1978).

موازن حقوق بشر، بر پایه آزادی بنا شده است و بر این اساس، آزادی فردی به عنوان یک هدف اساسی شناخته می‌شود؛ بنابراین، هرگونه مداخله دولت‌ها در این حوزه، باید توجیه قوی داشته باشد و از لحاظ قانونی، مبنای مناسبی را برای آن در نظر گرفت. همچنین، مداخله دولت‌ها باید تناسب لازم را با منافع حاصل از آن و کاهش آسیب‌های ناشی از نقض حقوق بشر داشته باشد. با این حال، زمانی که حمایت از حقوق بشر ایجاب کند که افراد تحت محدودیت‌هایی قرار گیرند تا از آسیب رساندن به دیگران پیشگیری شود، رسانه‌ها و فضای دیجیتال به طور خاص، باید در چارچوب مقررات حقوق کیفری داخلی و بر اساس کیفرهای متناسب با آن مورد توجه قرار گیرند.

در زمینه مقابله با محتوای تروریستی برخط، موازن حقوق بشر باید به طور واضح تعیین کنند که چه زمانی محتوای برخط مشمول تحریم قرار گیرد. در این زمینه، تشخیص تأثیرات نامطلوب این اقدامات بر آزادی بیان و دیگر حقوق بنیادین باید صورت گیرد، به ویژه زمانی که اعمال کیفرها می‌تواند آسیب‌های جدی به حقوق بشر وارد کند؛ بنابراین، باید محتوای تروریستی در فضای دیجیتال تنها از منظر اصول حقوق کیفری تحلیل شود، به ویژه زمانی که این محتوا موجب تحریک به خشونت می‌شود. این تحلیل باید بر اساس تعاریف قانونی شناخته شده از خشونت تروریستی باشد تا از ارزیابی‌های سیاسی و بی‌طرفانه پیشگیری شود.

جرائم تروریستی که در بسیاری از کشورها همچنان به عنوان مفهومی مورد مناقشه باقی مانده‌اند، ممکن است در برخی موارد نیاز به اقدام فوری داشته باشند. به ویژه در شرایطی که حمله تروریستی در حال انجام است، دولت‌ها باید توانایی اقدام سریع برای پیشگیری از پخش زنده آن را داشته باشند.^۱ این اقدامات باید به گونه‌ای باشند که مانع

۱. توانمندی دولت‌ها در به کارگیری فناوری‌های سایبری، موجب شده است که آن‌ها قادر باشند از این فناوری‌ها، برای وارد آوردن خسارات به رقبای خود استفاده کنند. به طور میانگین، روزانه میلیون‌ها حمله سایبری در نقاط مختلف جهان صورت می‌گیرد که این حملات اغلب علیه تأسیسات نظامی، سامانه‌های مالی، زیرساخت‌های هسته‌ای (نماین، ۱۴۰۴) و دیگر زیرساخت‌های حیاتی (نماین، ۱۴۰۳) کشورهای مختلف انجام می‌شود. در

از تشکیل یک محاکمه کیفری مناسب به عنوان اقدام اولیه نشوند. با این حال، صدور دستور حذف محتوای تروریستی باید با دقت و پس از ارزیابی کامل انجام شود. این دستور تنها زمانی باید صادر شود که محتوای دیجیتال از مرزهایی عبور کرده باشد که امکان پیگرد قانونی را فراهم می‌کند. در این صورت، مقام دولتی که دستور حذف را صادر می‌کند، باید آماده باشد تا در صورت لزوم، فرد یا گروه مسئول را به دلیل تحریک به خشونت و تروریسم تحت پیگرد قانونی قرار دهد.

برای مجموعه مقررات در طراحی چارچوبی مؤثر و به‌طور اصولی مجاز برای پرداختن به محتوای تروریستی برخاط با آن مواجه است، ساختار تقنینی حقوق بشر نقش اساسی در پرداختن به چالش‌های متعددی دارد. بر این اساس، باید سازوکارهای نوآورانه‌ای یافت تا مبتنی بر مفاهیم، اصول و اندیشه‌های اساسی موازین حقوق بشر باشد. مرحله نخست، رد انحرافات از حقوق بشر بدون وضعیت اضطراری رسمی اعلام شده در ساختار حقوق و جامعه بین‌المللی است؛ از آنجایی که هیچ‌کس خلاً قانونی در حوزه دیجیتال وجود ندارد، کسانی که ادعا می‌شود از اینترنت برای توزیع تبلیغات تروریستی بهره‌گیری می‌کنند، بدون هیچ‌گونه حمایت قانونی «دشمن نوع بشر»^۱ نیستند (Milanovic, 2015: 118-119). مرحله دوم، مادام مقام صلاحیت‌دار تعیین‌شده دستورات حذف فرامرزی صادر کند که آزادی بیان را نقض می‌کند، باید مورد بازخواست قرار گیرد؛ به همین ترتیب، باید عملکرد محافظتی در رابطه با ارائه دهندگان خدمات میزبانی و ارائه دهندگان محتوا بر اساس قلمرو خود و اعمال آزادی بیان آن‌ها به رسمیت قرار گیرند. محاکم در هر دو کشور سرزمینی و فرا سرزمینی و

حال حاضر، قوانین مشخص و جامعی برای حوزه سایبری وجود ندارد و کشورهای دارای توانمندی‌های بالا در این زمینه، از این خلاً قانونی بهره‌برداری کرده و حملاتی را علیه رقبای خود ترتیب می‌دهند (فرشا سعید و همکاران، ۱۴۰۰: ۲۰۵).

هم‌چنین نهادهای بین‌المللی حقوق بشر، باید برای شناسایی، توقف و تحریم نقض حقوق بشر از آمادگی لازم برخوردار باشند.

ظهور پدیده‌های جدید در قلمرو دیجیتال، کنار گذاشتن اندیشه‌های حقوق بشری تثبیت شده، سنجش محدودیت‌های مجاز را توجیه نمی‌کند. این امر در تعیین اینکه چه امری نقض حقوق بشر است و چه امری نیست، حائز اهمیت است. محدودیت‌ها باید مبنای قانونی مناسبی داشته باشند که الزامات قابل پیش‌بینی و سازوکارها را برآورده کند. محدودیت‌ها باید برای رساندن منفعت اثبات شده به یک نیاز فوری اجتماعی، یک هدف مشروع، ضروری باشند. هرگونه محدودیتی که بر برخورداری از حقوق بشر اعمال می‌شود، باید به هسته اصلی آن احترام بگذارد و نباید سایر حقوق بشر را نقض کند. تأثیر نامطلوب بر حقوق بشر باید متناسب با منافع واقعی به‌دست‌آمده در جهت یک هدف مشروع رقابتی باقی بماند.

۴. از ساختار رژیم حقوقی تا سنجش رویکردی در اتحادیه اروپا

به‌منظور رسیدگی به چالش‌های ناشی از حضور محتوای تروریستی در قلمرو فضای دیجیتال، اتحادیه اروپا یک رژیم حقوقی بین‌المللی بی‌سابقه جهانی از دستورات حذف دولتی برای حذف چنین محتوایی ایجاد کرده است که بر اساس آن، دستور صادر شده توسط «مرجع ذی‌صلاح» تعیین شده یک دولت، اثر فرا سرزمینی مستقیم در کشورهای خارجی دارد. تصویب مقررات ۲۰۲۱/۷۸۴ توسط اتحادیه اروپا و کشورهای عضو آن که هدف آن «شناسایی و اطمینان از حذف سریع محتوای تروریستی توسط ارائه دهندگان خدمات میزبان» است، باید در پرتو نگرانی‌های فزاینده در سراسر جهان در مورد گسترش محتوای تروریستی برخط در حوزه دیجیتال صورت پذیرد.^۱ این بخشی از تلاش‌های بین‌المللی گسترده برای مقابله با چنین محتواهایی در اروپا است.

1. Regulation (EU) 2021/784, Article 1 (1) (b) (i).

آنچه مقررات ۷۸۴ اتحادیه اروپا را از سایر مقررات که هدف آن‌ها مقابله با محتوای تروریستی برخط است جدا می‌کند، ماهیت ذاتاً فراملیتی رژیم حقوقی است که در ارتباط با تأثیر فرا سرزمینی تصمیم‌های غیر شفاف اتخاذ شده توسط مقامات ذی صلاح است. پرسشی که در این زمینه قابل نظر خواهد بود این که «آیا دستورهای حذف خاص با تداخل ناشی از آن با حقوق بشر ارائه دهندگان محتوا متناسب است یا خیر؟» این امر به علت گستره فوق‌العاده این مقررات تشدید می‌شود که برای هر ارائه دهنده خدمات میزبانی «ارائه خدمات در اتحادیه، صرف‌نظر از محل استقرار اصلی‌شان تا جایی که اطلاعات را در اختیار عموم قرار می‌دهند» اعمال می‌شود.^۱ این مقررات به جای محدود شدن به اتحادیه اروپا، در سطح جهانی اهمیت دارد و به‌طور گسترده‌ای، بررسی دقیق پیامدهای نامطلوب حقوق بشری آن را توجیه می‌کند.

ماهیت فراملی رژیم حقوقی، همان‌طور که در ماده ۳ (۱) مقررات بیان شده، تصریح می‌کند که «مقام صلاحیت‌دار هر کشور عضو این اختیار را دارد که حکم حذف صادر کند که ارائه دهندگان خدمات میزبانی را ملزم به حذف محتوای تروریستی یا غیرفعال کردن دسترسی به محتوای تروریستی در تمام کشورهای عضو کنند.» مادامی که حکم حذف توسط یک مقام ملی خاص صادر شد، «ارائه دهندگان خدمات میزبانی باید محتوای تروریستی را حذف کنند یا دسترسی به محتوای تروریستی را در تمام کشورهای عضو در اسرع وقت و در هر صورت ظرف یک ساعت پس از دریافت حکم حذف، غیرفعال کنند.»^۲

برای پیشگیری از آثار مالی نامطلوب ناشی از عدم انطباق با مقررات اتحادیه اروپا، ارائه دهندگان خدمات میزبانی بزرگ‌تر، به‌ویژه شرکت‌های بزرگ در لوای پرکاربردترین رسانه‌های اجتماعی نظیر توییتر، متا و گوگل که شامل یوتیوب می‌شود، تعدادی از دستورات حذف، رویه‌ها و پروتکل‌هایی را ایجاد کرده‌اند که شامل استفاده

1. Regulation (EU) 2021/784, Article 1 (2).

2. Regulation (EU) 2021/784, Article 3 (3).

از ابزارهای تصمیم‌گیری خودکار برای اجرای دستورات حذف، وفق الگوریتم‌ها است. حتی در غیر این موارد، ارائه دهندگان خدمات میزبانی محتمل است تلاش‌های خود را بر روی انطباق سطحی با مقررات متمرکز کرده و متناسب با مقرراتی که با تأمین مالی تروریسم و پول‌شویی مقابله می‌کند (ر.ک: سبحانی، ۱۴۰۴: ۱۶۱-۱۶۰)، اقدام کنند. این مقررات پیش‌بینی نمی‌کند که ارائه دهندگان خدمات میزبانی باید نسبت به تناسب و ضرورت احکام حذف بررسی کنند. عدم انطباق با دستورات حذف تنها در موارد «فورس ماژور»، «عدم امکان عملی غیر قابل انتساب به ارائه دهنده خدمات میزبانی»، «خطاهای آشکار» یا «اطلاعات ناکافی برای اجرای سفارش» مجاز است. مقامات ملی تعیین شده شامل خدمات امنیتی (استونی، لتونی)، پلیس (دانمارک، آلمان، ایرلند، اسلواکی، سوئد)، وزارت کشور (بلغارستان، کرواسی، اسپانیا)، خدمات دادستانی عمومی (بلژیک) و دادگاه‌ها (دانمارک) هستند (Gherbaoui, 2023: 8-9).

این واقعیت که مقررات یکسان مقررات توسط چنین مجموعه متنوعی از مقامات ملی اعمال و تفسیر می‌شود، خطر اجرای پراکنده مقررات را در سراسر قاره اروپا افزایش می‌دهد. حذف بسیاری از کشورهای عضو برای تعیین یک مرجع ذی‌صلاح، برای حمایت از آزادی بیان محروم می‌کند؛ زیرا هیچ همتای محلی وجود نخواهد داشت که به‌عنوان ناظر در رابطه با تعیین شده توسط کشورهای خارجی عمل کند.

در حالی که وظیفه اصلی مقامات ملی، حذف محتوا از طریق صدور دستور حذف است، رویکرد مقرر در ماده ۴(۳) به‌طور خاص به مرجع ذی‌صلاح تعیین شده بر اساس ماده ۱۲ (۱-ب) در کشورهای عضو این اختیار را می‌دهد که «حکم حذف را به‌طور دقیق بررسی کند تا مشخص شود که آیا این حکم به‌طور جدی یا آشکار حقوق و آزادی‌های اساسی تضمین شده توسط منشور را نقض می‌کند یا خیر». این فرآیند، قدرت بررسی دقیق دستورات صادر شده از سوی مقامات ملی کشورهای دیگر را می‌توان به‌عنوان عملکرد محافظتی برای مقامات ذی‌صلاح در نظر گرفت.

اگرچه موارد نادری وجود دارد که در آن‌ها موضوعات سیاسی یا بحث‌برانگیز سیاست‌های ملی مطرح می‌شود، مقامات ملی تعیین شده به‌طور معمول در فضای دیجیتال، برای شناسایی محتوای تروریستی گشت زنی می‌کنند. در بسیاری از کشورهای عضو اتحادیه اروپا، انگیزه‌های بسیار کمی برای اعتراض به حذف محتوای علامت‌گذاری شده به‌عنوان محتوای تروریستی وجود دارد. با این حال، مقامات ملی، از جمله سرویس‌های امنیتی و پلیس، معمولاً تخصص قانونی لازم برای ارزیابی این‌که آیا یک دستور حذف خاص حقوق و آزادی‌های اساسی را نقض می‌کند یا نه را ندارند. چنین ارزیابی‌ای نیازمند بررسی تناسب دقیق است که باید بر اساس رویه‌های قضایی موجود و دانش حقوقی عمیق صورت گیرد.

افزون بر تأثیر حقوق بشر ناشی از احکام حذف واقعی که محتوای خاص را هدف قرار می‌دهد، تلاش‌های اتحادیه اروپا برای رسیدگی به محتوای تروریستی در فضای دیجیتال خطر واقعی تبدیل‌شدن به نوعی تعدیل محتوای عمومی را به دنبال دارد. این مقررات از ارائه دهندگان خدمات میزبانی که اعلام می‌شود «در معرض محتوای تروریستی» هستند، می‌خواهد سازوکارهایی را اتخاذ کنند که فراتر از پرداختن به موقعیت‌های خاص است. ماده ۵ این مقررات، ضمن تجویز اعمال «سازوکارهای خاص»، از اتخاذ شرایط و ضوابط در مورد «سوءاستفاده از خدمات آن برای انتشار عمومی محتوای تروریستی» تا ایجاد سازوکارهایی که کاربران می‌توانند محتوای تروریستی ادعایی را پرچم‌گذاری و گزارش کنند، مدنظر قرار می‌دهد.^۱ به‌منظور پیروی از سازوکارهایی که با هدف پیشگیری از محتوای تروریستی در آینده به شیوه‌ای کلی انجام می‌شود، ارائه دهندگان خدمات میزبانی «در معرض محتوای تروریستی» احتمالاً سیاست‌های خطر‌گریزی را اتخاذ می‌کنند که ممکن است از طریق بهره‌گیری از ابزارهای خودکار بدون نظارت انسانی اعمال شوند؛ اگرچه این مقررات تصریح می‌کند که چنین

1. Regulation (EU) 2021/784, Article 5 (1) and (2).

سازوکارهایی باید «با هدف پیشگیری از حذف مطالبی که محتوای تروریستی نیستند» اجرا شوند، اما به سهولت می‌توان ملاحظه کرد که چگونه سازوکارهای خاص می‌تواند منجر به تعدیل پیشگیرانه عمومی تر محتوای قانونی شود (Conway, 2023: 1).

برای افزایش کارایی و به حداقل رساندن خطرات، ارائه دهندگان خدمات میزبانی که در اتحادیه اروپا فعالیت می‌کنند، ممکن است سیاست‌هایی را طراحی کنند که به‌منظور انطباق با مقررات اتحادیه، به‌ویژه «سازوکارهای خاص»، گسترش یابند. با توجه به اینکه مرزهای ملی در فضای دیجیتال به‌طور فزاینده‌ای بی‌ربط می‌شوند، مقررات اروپایی می‌توانند به‌سرعت به حداقل موازین جهانی برای تنظیم محتوای تروریستی تبدیل شوند. مقررات و سیاست‌های ضد تروریستی اتحادیه اروپا، با وجود طراحی ضعیف در برخی موارد، به‌وضوح ظرفیت این را دارند که به‌عنوان الگویی برای اقدامات سرکوبگرانه در کشورهای مستبد یا نیمه استبدادی عمل کنند.

اتحادیه اروپا در سال‌های اخیر، مجموعه‌ای از اقدامات را برای مقابله با انتشار محتوای تروریستی برخط اتخاذ کرده است. این اقدامات، از آن جهت اهمیت دارند که تروریسم و افراط‌گرایی در فضای مجازی به‌سرعت گسترش یافته و تهدیدات جدی برای امنیت و تمامیت اجتماعی به وجود آورده‌اند. با این حال، اتحادیه اروپا با تدوین قوانین جامع و همکاری‌های بین‌المللی به مقابله با انتشار این نوع محتوا پرداخته است. این اقدامات نه‌تنها بر تأمین امنیت تأکید دارند، بلکه حفظ حقوق بشر و آزادی‌های فردی نیز در آن‌ها در نظر گرفته شده است. در همین راستا، کشورهای غیر عضو اتحادیه اروپا و نهادهای بین‌المللی با این اتحادیه همکاری می‌کنند. این همکاری‌ها شامل تبادل اطلاعات، ایجاد استانداردهای مشترک و تنظیم ساختارهای قانونی برای مبارزه با تروریسم در فضای دیجیتال است.

اتحادیه اروپا همچنین، به پیشگیری از افراط‌گرایی و تروریسم در فضای دیجیتال توجه ویژه‌ای دارد. برنامه‌های آموزشی برای آگاه‌سازی کاربران از تهدیدهای برخط و نحوه شناسایی و گزارش محتوای تروریستی، ازجمله اقداماتی است که در این راستا

اجرا می‌شود؛ اگرچه اتحادیه اروپا به‌شدت در قبال محتوای تروریستی برخط فعال است، اصول حقوق بشر و آزادی بیان نیز در این اتحادیه از اهمیت قابل‌ملاحظه‌ای برخوردارند؛ بنابراین، تمامی اقدامات باید به‌گونه‌ای طراحی شوند که توازن مناسبی بین امنیت و حقوق فردی برقرار کنند. این به این معناست که محدودیت‌های اعمال شده نباید به‌طور غیر ضروری آزادی‌های فردی و حق بیان را محدود سازند.

۵. رویکرد تهاجمی در اتحادیه اروپا و امکان‌سنجی توازن میان امنیت ملی و آزادی بیان

وفق ماده ۱۹ اعلامیه جهانی حقوق بشر، هر فرد حق آزادی عقیده و بیان دارد. این حق شامل، آزادی داشتن عقاید بدون مداخله و همچنین دریافت، جستجو و انتشار اطلاعات و عقاید از طریق هر رسانه‌ای است، بدون توجه به مرزهای جغرافیایی. عصر دیجیتال نهایتاً وعده آخرین کلمات این ماده را به واقعیت تبدیل کرده است. پیش از این، غالب مردم در یک کشور تنها از آزادی عقیده و آزادی دریافت اطلاعات در فضای فیزیکی که در آن زندگی می‌کردند، بهره‌مند بودند؛ اما انتشار اطلاعات عمدتاً در اختیار کسانی بود که دارای رسانه‌های جمعی بودند که اغلب به ایجاد کارتل‌ها، انحصارها یا کنترل‌های دولتی منجر می‌شد. مرزهای ملی به‌عنوان موانع مؤثری برای جریان آزاد اطلاعات و دیدگاه‌ها عمل می‌کردند و این جریان، اغلب به دست عده‌ای خاص محدود می‌شد. دیجیتالی شدن اطلاعات و گسترش اینترنت به شکلی بی‌سابقه، آنچه را که در اعلامیه جهانی حقوق بشر وعده داده شده بود، به تحقق رسانده است.

عصر اطلاعات دیجیتال، تا حد زیادی مرزهای بین دولتها را از محو کرد و دیجیتالی شدن جامعه این احتمال را افزایش داده است که محتوای تروریستی برخط در سکوه‌های دیجیتالی منتشر شود و این امر می‌تواند، منجر به ارتکاب جرائم تروریستی جدید یا آسیب‌های دیگر به جامعه، گسترده‌تر شود. رویه قضایی حاکم در ماده ۱۰ کنوانسیون اروپایی حقوق بشر و ماده ۱۱ منشور حقوق اساسی اتحادیه اروپا، نشان می‌دهد که موازن حقوق بشر حاوی یک فرض قوی در راستای احترام به آزادی بیان

است که همان‌طور که دیوان حقوق بشر اروپا، در قضیه «ریچارد هندسی ساید»^۱ علیه بریتانیا حکمی صادر کرد: «نه‌تنها برای «اطلاعات» یا «آیده‌هایی» که به نحو مطلوب دریافت می‌شوند یا به‌عنوان غیر توهین‌آمیز یا بی‌تفاوت تلقی می‌شوند، اعمال می‌شود؛ بلکه برای آن‌هایی که دولت یا هر بخش از جمعیت را توهین، شوکه یا مزاحم می‌کنند نیز کاربرد دارد. این چنین است خواسته‌های کثرت‌گرایی، مدارا و وسعت اندیشی که بدون آن «جامعه دموکراتیک» وجود ندارد».^۲

دیوان حقوق بشر اروپا در برخی از کاوش‌های خود در زمینه آزادی بیان، شاید بسیار سهل، تشخیص داده است که راه‌های مشخصی برای شناسایی با یک سازمان تروریستی، نظیر تمجید از یک سازمان تروریستی، می‌تواند تحریک خشونت تلقی شود و از این‌رو محدودیت آزادی بیان را توجیه می‌کند. محدودیت‌های آزادی بیان را می‌توان به‌منظور تضمین «حفاظت از امنیت ملی یا نظم عمومی» توجیه کرد، اما پس از آن باید ضروری و متناسب با این هدف باشد. البته یکی از صاحب‌نظران با این استدلال نتیجه‌گیری می‌کند که دشواری اتخاذ یک رویکرد مبتنی بر حقوق برای توازن بین الزامات اخیر و مقابله با جرائم تروریستی، نه‌تنها به علت چالش‌های منحصربه‌فرد ارائه شده توسط اینترنت برای حفاظت و اعمال حقوق اساسی بشر است، بلکه به دلیل فقدان مستمر این موازین است.^۳ شاید بارزترین نمونه از رویکرد نسبتاً سهل‌انگیز دیوان در تجلیل از تروریسم در تصمیم، در خصوص قضیه «ژان مارک روئیلان» علیه

1. The Richard Handyside v United Kingdom (5493/72) Case, 7 December 1976, <https://hudoc.echr.coe.int/eng?i=001-57499>

2. Eur. Ct. H.R. (Plenary), Handyside v. The United Kingdom, 7 December 1976 (Appl. No. 5493/72), 49.

3. Jonathan Hall, The Terrorism Acts in 2021: Report of the Independent Reviewer of Terrorism Legislation on the Operation of the Terrorism Acts 2000 and 2006, and the Terrorism Prevention and Investigation Measures Act 2011, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachm ent_data/file/1140911/E02876111_Terrorism_Acts_in_2021_Accessible.pdf.

فرانسه باشد.^۱ این پرونده، مربوط به محکومیت کیفری برای تجلیل از تروریسم (عذرخواهی) یک شهروند فرانسوی است که خود، به دلیل اقدام‌های تروریستی به حبس ابد محکوم شده بود؛ زیرا عاملان جرائم تروریستی وحشیانه پاریس در نوامبر ۲۰۱۵ را از طریق یک کانال رادیویی «شجاع» خوانده بود.^۲

دولت‌ها می‌توانند به ماده ۱۷ کنوانسیون حقوق بشر اروپایی استناد کنند که استفاده از مفاد این کنوانسیون را برای اهدافی که منجر به نقض حقوق بشر می‌شود، ازجمله برای توجیه جرم‌انگاری گفتار تروریستی، ممنوع می‌کند. پیشرفت‌های فناوری، ارائه دهندگان خدمات میزبانی را در موقعیتی پیچیده قرار داده است. آن‌ها در موقعیت ایدئالی برای تسهیل دریافت و انتشار اطلاعات و دیدگاه‌ها بدون توجه به مرزها قرار دارند، اما در عین حال مسئولیت نظارت بر محتوای اطلاعات و دیدگاه‌هایی که برای انتشار مناسب نیستند را بر عهده دارند. این مسئولیت به‌طور اجتناب‌ناپذیر، مستلزم اتخاذ تصمیم‌هایی است که به‌طور اساسی، به سیاست‌های عمومی مربوط می‌شوند که برای بازیگران خصوصی که توسط اتحادیه اروپا مأمور به گشت زنی در فضای دیجیتال شده‌اند، مناسب نبوده و فاقد مشروعیت دموکراتیک هستند.

۶. کاربرد هوش مصنوعی در شناسایی و حذف محتوای تروریستی

سامانه‌های هوش مصنوعی، به‌طور فزاینده‌ای در مدیریت انبوه داده‌ها و محتوای منتشرشده در محیط‌های مجازی، نقشی تعیین‌کننده و حائز اهمیت یافته‌اند. پارلمان اروپا و شورای اتحادیه اروپا بر ضرورت تقویت دسترسی به محتوای قابل اعتماد تأکید می‌کنند. ریشه اصلی این مسئله، اطلاعات نادرست در الگوی اقتصادی وب مبتنی بر درآمدهای تبلیغاتی نهفته است و اصلاح این فرآیند می‌تواند از شدت مشکل، به‌طور

1. Jean-Marc Rouillan v. France - 28000/19 case, 23/06/2022, <https://hudoc.echr.coe.int/eng?i=002-13708>

2. Eur. Ct. H.R. (5th Section), Rouillan v. France, 23 June 2022 (Appl. No. 28000/19).

چشمگیری پیش‌گیری کند و دیگر اینکه، سامانه‌های هوش مصنوعی ابزار مناسبی برای تعدیل یا حتی شناسایی محتوای اطلاعات نادرست نیستند، اما می‌توانند در مقابله با دست‌کاری ساختاری زیست‌بوم دیجیتال نقشی مؤثرتر ایفا کنند (Bontridder, 2021: 32-1).

برخی معتقدند، در ناهنجاری‌هایی که به صورت مجزا در نظر گرفته می‌شود، این احتمال وجود دارد که نشان‌دهنده آمادگی‌های تروریستی باشد، در حالی که معمولاً این‌گونه نیست. سامانه‌های خبره مبتنی بر هوش مصنوعی، به تحلیل سیگنال‌های ناشناخته برای شناسایی آمادگی‌های احتمالی فعالیت‌های تروریستی می‌پردازند. این سیگنال‌ها از داده‌هایی مانند الگوهای خرید، روابط مالی و بین فردی، استفاده از اینترنت و پیشینه شخصی استخراج می‌شوند؛ البته ذکر این نکته نیز لازم است که همان‌طور که بیان شد، لزوماً هر سیگنال به‌تنهایی نشان‌دهنده فعالیت تروریستی نیست. معماری سامانه، شامل مراحل جمع‌آوری و پردازش داده، تولید گزارش، دریافت بازخورد و توسعه تدریجی است و محدودیت‌های آن را نیز مورد توجه قرار می‌دهد (Koltko, 2004: 1). با این حال، به‌کارگیری فناوری‌های هوش مصنوعی در زمینه حذف محتوای تروریستی، با چالش‌های قابل توجهی در حوزه حقوق بشر و آزادی‌های بنیادین همراه است. هم‌چنین، ذکر این نکته ضروری است که هوش مصنوعی، در حال تغییر جهان است و وعده آن برای بهبود زندگی، بسیار زیاد است. با این حال، دارای معایبی نیز هست که وعده‌های قابل توجه آن را تضعیف می‌کند. سامانه‌های مبتنی بر هوش مصنوعی، بر حق حریم خصوصی تأثیر می‌گذارند، زیرا آن‌ها به جمع‌آوری و استفاده از مقادیر زیادی از داده‌ها برای پیش‌بینی‌هایی وابسته هستند که در موارد متعدد، به تداوم الگوهای اجتماعی موجود از تعصب و تبعیض کمک کرده‌اند (Raso, et al, 2018: 6).

«در سپتامبر ۲۰۱۸، کمیسیون اروپا پیشنهاد خود را برای تدوین آیین‌نامه‌ای در مورد پیشگیری از انتشار محتوای تروریستی برخط منتشر کرد. ازجمله موارد مهم آن: ۱) قوانینی در مورد وظایف مراقبتی، که باید توسط ارائه‌دهندگان خدمات میزبانی برای

پیشگیری از انتشار محتوای تروریستی و تضمین حذف سریع آن اعمال شود؛ و ۲) مجموعه‌ای از اقدامات که باید توسط کشورهای عضو برای شناسایی محتوای تروریستی، برای امکان حذف سریع آن توسط ارائه دهندگان خدمات میزبانی و تسهیل همکاری بین ذینفعان اعمال شود. به‌طور خاص، این پیشنهاد چندین روش برای پیشگیری از انتشار محتوای تروریستی به صورت برخط، به‌عنوان مثال، ارجاع محتوا، دستور حذف و اقدامات پیشگیرانه را شرح می‌دهد. نکته مهم این است که این پیشنهاد همچنین شامل تعدادی از اقدامات حفاظتی است که سعی در پیشگیری از مداخله نامتناسب در حقوق اساسی، به‌ویژه حق آزادی بیان و دسترسی به اطلاعات دارد» (Kuczerawy, 2018:1).

همچنین، انتشار گزارش‌های سالانه عملکرد سکوها و انجام ممیزی‌های مستقل، می‌تواند نظارت عمومی و حقوقی را تقویت کرده و از اقدامات غیر شفاف و خودسرانه پیشگیری کند؛ بنابراین، هوش مصنوعی ابزاری کارآمد اما دوپهلوی، در مدیریت محتوای تروریستی است: از یک‌سو، امکان شناسایی و مهار سریع محتوا و کاهش تهدیدات امنیتی را فراهم می‌کند و از سوی دیگر، در صورت فقدان شفافیت، پاسخگویی و رعایت موازین حقوق بشری، خطر نقض گسترده آزادی‌های بنیادین را در پی خواهد داشت. بر این اساس، رویکرد پایدار مستلزم پیوند نوآوری فنی با ضمانت‌های حقوقی مستحکم و استقرار نهادهای نظارتی مستقل است تا هم‌زمان هر دو هدف صیانت از امنیت عمومی و پاسداشت حقوق بشر تحقق یابد.

در هر حال، مقررات ۲۰۲۱/۷۸۴ اتحادیه اروپا با هدف تقویت مقابله با محتوای تروریستی برخط تصویب شد و به ارائه دهندگان خدمات میزبانی برخط دستور می‌دهد که ظرف یک ساعت پس از دریافت دستور حذف از مقامات ملی، محتوای تروریستی را از سکوها خود حذف کنند. این مقررات، به‌ویژه برای مقابله با تهدیدات تروریستی در فضای دیجیتال طراحی شده‌اند. با این حال، نگرانی‌هایی در زمینه حقوق بشر، به‌ویژه آزادی بیان و حریم خصوصی، به‌ویژه در ارتباط با استفاده از الگوریتم‌ها و

هوش مصنوعی برای حذف خودکار محتوای تروریستی، وجود دارد؛ زیرا این فرآیند ممکن است به حذف محتوای مشروع منجر شود؛ بنابراین، هوش مصنوعی می‌تواند در شناسایی و حذف محتوای تروریستی به‌طور مؤثر عمل کند، اما چالش‌هایی نظیر دقت اندک، تشخیص نادرست محتوای ابراز عقیده و وابستگی به داده‌های آموزشی ناقص می‌تواند منجر به ایجاد اشتباهات در شناسایی محتوای تروریستی شود. علاوه بر این، مقررات ۲۰۲۱/۷۸۴ ممکن است چالش‌هایی در راستای حقوق بشر ایجاد کند، از جمله محدودیت‌های آزادی بیان و دسترسی به اطلاعات و نگرانی‌هایی در مورد حریم خصوصی و شفافیت؛ بنابراین، پاسخ به چالش‌های حقوق بشری ناشی از انتشار محتوای تروریستی، باید متعادل و مبتنی بر اصول حقوق بشری باشد. فرآیندهای شفاف و قابل نظارت باید برای پیشگیری از سوءاستفاده و نقض حقوق فردی ایجاد شود. همچنین، استفاده از هوش مصنوعی باید با ملاحظات دقیق حقوق بشر همراه باشد تا هم از امنیت حفاظت شود و هم آزادی‌های اساسی حفظ شود.

فرجام سخن

در دهه‌های اخیر، با توسعه مقررات ضد تروریستی، جرائم مرتبط با تروریسم گسترش یافته و جرم‌انگاری گفتار رادیکال به‌عنوان «تحریک»، «توجیه» یا «عذرخواهی» خشونت تروریستی در دستور کار قرار گرفته است. هدف این جرائم، مقابله با سخنانی است که حمایت یا تأیید خشونت تروریستی را به همراه دارند. پس از حوادث ۱۱ سپتامبر ۲۰۰۱، شکاف‌های موجود در رژیم جهانی مقابله با تروریسم، توجه قانون‌گذاران را به‌سوی مفاهیم مبهمی مانند «تجلیل از تروریسم» و انتشار محتوای تروریستی برخط جلب کرد.

اتحادیه اروپا برای مقابله با جرائم تروریستی در سکوه‌های دیجیتال مقرراتی تصویب کرد، اما این مقررات نتوانست مقابله حداکثری با انتشار محتوای تروریستی برخط را فراهم کند. پس از حوادث ۱۱ سپتامبر ۲۰۰۱، اتحادیه اروپا به دنبال تنظیم مقررات

جامع‌تری بود تا از نقض صلح و تهدیدات حقوق بشر پیشگیری کند. با این حال، مقررات ۲۰۲۱/۷۸۴ ممکن است بیشتر یک موضع‌گیری سیاسی و نمادین باشد؛ زیرا هنوز ابهاماتی در تعاریف و رویکردهای کشورهای عضو اتحادیه اروپا در خصوص مقابله با محتوای تروریستی برخط وجود دارد. اینترنت به‌عنوان فضایی آزاد، چالش‌های نوینی در زمینه سخنرانی‌های بحث‌برانگیز ایجاد کرده است.

اتحادیه اروپا باید مقررات جدیدی تصویب کند تا شفافیت در چارچوب‌های حقوقی و اطمینان حقوقی را تقویت کند. اتحادیه اروپا با شفاف‌سازی معیارهای مقابله با انتشار محتوای تروریستی برخط، می‌تواند آزادی بیان را در محدوده خود حفظ کند و این اقدام می‌تواند الگویی برای کشورهای عضو باشد. اتحادیه اروپا باید، عناصر مبهم مقررات را با تمرکز بر تحریک خشونت و گفتار عمومی بررسی کند و با اختصاص منابع به مجریان قانون، اجرای مؤثرتری برای کاهش خشونت و افراط‌گرایی انجام دهد. به هر روی، پاسخ به چالش‌های حقوق بشر ناشی از انتشار محتوای تروریستی برخط، به‌ویژه در چارچوب مقررات ۲۰۲۱/۷۸۴ اتحادیه اروپا، نیازمند ترکیبی از راهکارها اعم از امنیتی، حقوقی و فنی است. از این‌رو، راهکارهای مزبور مشتمل بر موارد ذیل است:

الف. برای مقابله مؤثر با محتوای تروریستی، ضروری است که ارائه دهندگان خدمات میزبانی سامانه‌های شناسایی سریع محتوای تروریستی را به کار گیرند. بهره‌گیری از فناوری‌های پیشرفته، مانند هوش مصنوعی و یادگیری ماشین می‌تواند به تشخیص الگوهای مرتبط با تروریسم و کاهش زمان واکنش در برابر تهدیدات کمک کند. علاوه بر این، روزآمدی مداوم تدابیر امنیت دیجیتال برای پیشگیری از سوءاستفاده‌ها و تهدیدات سایبری امری ضروری است. همکاری نزدیک میان نهادهای امنیتی، کارشناسان فناوری اطلاعات و مقامات قضائی در راستای مقابله با محتوای تروریستی در فضای برخط نیز از اهمیت بالایی برخوردار است.

ب. یکی از مهم‌ترین چالش‌ها در اجرای مقررات، تعریف دقیق و واضح محتوای تروریستی است تا از سوءاستفاده‌ها و سانسور محتوای غیر تروریستی پیشگیری شود. مبارزه با محتوای تروریستی، باید به گونه‌ای انجام شود که اصول حقوق بشر حفظ شود و توازن مناسبی میان امنیت عمومی و حقوق فردی برقرار شود. در این راستا، فرآیندهای قضائی منصفانه باید تضمین کننده حقوق متهمان باشند و همچنین راهکارهایی مستقل برای اعتراض به حذف نادرست محتوا باید فراهم شود. علاوه بر این، همکاری‌های حقوقی میان کشورهای اتحادیه اروپا و کشورهای غیر عضو برای مقابله با محتوای تروریستی از اهمیت ویژه‌ای برخوردار است.

ج. به کارگیری فناوری‌های خودکار، مانند پردازش زبان طبیعی و تشخیص تصویر می‌تواند سرعت شناسایی محتوای تروریستی را افزایش دهد. این فناوری‌ها، باید به طور مستمر به روزرسانی شوند تا کارایی آن‌ها حفظ شود. ایجاد مراکز مشترک دولتی و خصوصی برای نظارت بر محتوا و همکاری با کشورهای اتحادیه اروپا و سازمان‌های بین‌المللی، برای تسهیل این فرآیند ضروری به نظر می‌رسد. در کنار این اقدامات، آموزش مستمر کاربران و کارکنان سکوها دیجیتال و شفافیت در فرآیند حذف محتوا می‌تواند به تقویت اعتماد عمومی منجر شود. سامانه‌های قابل نظارت نیز می‌توانند موجب اطمینان بیشتر کاربران شوند.

د. همکاری با نهادهای حقوق بشری و جامعه مدنی کمک می‌کند تا اقدامات ضد تروریستی در فضای دیجیتال مطابق با حقوق بشر پیش برود و از نقض آزادی‌های فردی پیشگیری شود. همچنین، سکوها و ارائه دهندگان خدمات، باید به نوآوری در فناوری‌های ضد تروریستی برای شناسایی و حذف مؤثر محتوای تروریستی تشویق شوند.

در هر حال، ترکیب این راهکارها در چارچوب مقررات ۲۰۲۱/۷۸۴ اتحادیه اروپا می‌تواند به مقابله مؤثر با محتوای تروریستی برخاسته کند، در حالی که از حقوق بشر و امنیت عمومی نیز محافظت خواهد شد.

تعارض منافع: این مقاله مشمول هیچ گونه تعارض منافع نیست.

اصول اخلاقی: نویسندگان مقاله، تمام مسائل اخلاق در پژوهش را که شامل پرهیز از سرقت ادبی، انتشار و یا ارسال بیش از یک بار مقاله، تکرار پژوهش‌های دیگران، داده‌سازی یا جعل داده‌ها، منبع‌سازی و جعل منابع، رضایت ناآگاهانه سوژه یا پژوهش‌شوندگان است، رعایت کرده‌اند. تالیف این مقاله به هوش مصنوعی داده نشده است.

منابع

- فرشا سعید، پرویز؛ جلالی، محمود؛ گودرزی، مهناز. (۱۴۰۰). ضرورت تدوین کنوانسیون بین‌المللی حملات سایبری. *مطالعات حقوقی*، ۱۳(۱)، ۲۰۵-۲۳۰.
- سبحانی، حسین. (۱۴۰۴). رویکرد ریسک پایه ناظر بر عواید مجرمانه در پرتو مطالعه تطبیقی و استاندارد های FATF. *مطالعات حقوقی*، ۱۷(۱)، ۱۵۷-۲۰۰.
- نماین، پیمان. (۱۴۰۳). الزامات حقوقی جهانی حفاظت از امنیت زیرساخت‌های حیاتی کشورها در قبال جرائم تروریستی فناورانه. *دولت و حقوق*، ۵(۴)، ۴۶-۲۵.
- نماین، پیمان. (۱۴۰۴). رویکردهای حقوقی ناظر بر پیشگیری از جرائم تروریستی دیجیتالی علیه تأسیسات هسته‌ای. *پژوهش‌های جرم‌شناسی کاربردی*، ۳(۷)، ۱۵-۳۴.
- هاشمی، کامران. (۱۴۰۰). دین، نژاد و مبارزه حقوق بشر برای حمایت از افراد آسیب‌پذیر. *حقوق بشر*، ۱۶(۲): ۱۵۱-۱۷۲.

References

- Ahmed, R. (2023). Negotiating Fundamental Rights: Civil Society and the EU Regulation on Addressing the Dissemination of Terrorist Content Online. *Studies in Conflict & Terrorism*, 19 Jun, <https://www.tandfonline.com/doi/full/10.1080/1057610X.2023.2222890?src=recsys>
- Bartels R. (2018). When Do Terrorist Organizations Qualify as “Parties to an Armed Conflict” under International Humanitarian Law? *The Military Law and the Law of War Review* 56(2): 451-464.
- Bontridder, N., & Poulet, Y. (2021). The role of artificial intelligence in disinformation. *Data & Policy*, 3: e32.
- Brkan, M., M. Claes, and C. Rauchegger. (2020). European fundamental rights and digitalization. *Maastricht Journal of European and Comparative Law* 27(6): 695-714.

- Clifford, B. (2021). *Moderating Extremism: The State of Online Terrorist Content Removal Policy in the United States*. The George Washington University Program on Extremism.
- Conway, M. & Stuart, M. (2023). Introduction to Special Issue: The Practicalities and Complexities of (Regulating) Online Terrorist Content Moderation. *Studies in Conflict & Terrorism*, (19 Jun), <https://www.tandfonline.com/doi/figure/10.1080/1057610X.2023.2222887?scroll=top&needAccess=true>
- Decoeur, H. (2017). The Criminalization of Armed Jihad under French Law: Guilt by Association in the Age of Enemy Criminal Law. *European Journal of Crime, Criminal Law and Criminal Justice* 25(4): 304-323.
- Farshasaiid, P.; Jalali, M.; Goudarzi, M.. (2021). The Necessity of Drafting a Convention on Cyberattacks. *Journal of Legal Studies*, 13(1), 205-230. [In Persian]
- Gherbaoui, T., and M., Scheinin. (2023). A Dual Challenge to Human Rights Law: Online Terrorist Content and Governmental Orders to Remove it. *European Journal of Human Rights*, 2(1): 1-22.
- Macklin, G. (2019). The Christchurch Attacks: Livestream Terror in the Viral Video Age, *CTC Sentinel* 12(6): 7-24.
- Kuczerawy, A. (2018). *The proposed regulation on preventing the dissemination of terrorist content online: Safeguards and risks for freedom of expression* (For Center for Democracy and Technology). Center for Democracy and Technology. <https://ssrn.com/abstract=3296864>
- Milanovic, M. (2015). Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. *Harvard International Law Journal* 56(1): 115-127.
- Namanian, P. (2025). Global Legal Requirements for Protecting the Security of Critical Infrastructures of Countries Against Technological Terrorist Crimes. *Government and Law*, 5(4), 46-25. [In Persian]
- Namanian, P. (2025). Legal Approaches to Preventing Digital Terrorist Crimes Against Nuclear Facilities. *Applied Criminology Research*, 3(7), 15-34. [In Persian]
- Koltko-Rivera, M. E. (2004). Detection of Terrorist Preparations by an Artificial Intelligence Expert System Employing Fuzzy Signal Detection Theory, <https://www.sto.nato.int/document/paper-2-detection-of-terrorist-preparations-by-an-artificial-intelligence-expert-system-employing-fuzzy-signal-detection-theory/>
- Pirkova, E., et al. (2021). *Spotlight on Artificial Intelligence and Freedom of Expression: A Policy Manual* (Office of the Representative on Freedom of the Media. Organization for Security and Co-operation in Europe.

- Perrigo, B. (2020). These Tech Companies Managed to Eradicate ISIS Content. But They're Also Erasing Crucial Evidence of War Crimes, *Time*, (11 April), <https://time.com/5798001/facebook-youtube-algorithms-extremism/?xid=tcoshare>
- Hashemi, K. (2021). Religion, Race, and Human Rights Struggle for the Protection of Vulnerable People. *Journal of Human Rights* 16(2): 151-172. [In Persian]
- Tomažič, L. (2024). Freedom of Expression on the Internet and National Security in Europe: Liberty and Basic Goods. *NASK*, 3(1): 1-16.
- York, J. C., Karen, G. (2018) Offline/Online Project Highlights How the Oppression Marginalized Communities Face in the Real World Follows Them Online. *Electronic Frontier Foundation*, (6 March), <https://www.eff.org/deeplinks/2018/03/offlineonline-project-highlights-how-oppression-marginalized-communities-face-real>
- Raso, F., et al. (2018). *Artificial intelligence & human rights: Opportunities & risks* (Berkman Klein Center Research Publication No. 6). Berkman Klein Center for Internet & Society. <https://ssrn.com/abstract=3259344>
- Reinisch, A. (2004). The Action of the European Union to Combat International Terrorism. in A. Bianchi (ed.), *Enforcing International Law Norms Against Terrorism*, London, Hart Publishing.
- Skjoldager E. (2020). Lasse and Christian Bjørnskov. "Does Freedom of Expression Cause Less Terrorism?". *Political Studies* 70(1): 1-19.
- Sobhani, H. (2025). Risk-based Approach to Criminal Proceeds in Light of Comparative Study and FATF Standards. *Legal Studies*, 17(1), 157-200. [In Persian]
- Zarmsky, S. (2024). Is International Criminal Law Ready to Accommodate Online Harm? Challenges and Opportunities. *Journal of International Criminal Justice* 22(1): 172-173.

