شناسهٔ دیجیتال (DOI): 10.22106/pr.2025.207818.1063
مقالهٔ پژوهشی، دورهٔ ۲، شمارهٔ ۱، بهار و تابستان ۱۴۰۴، صفحات ۲۹ تا ۵۳
تاریخ دریافت: ۱۴۰۴/۰۳/۰۴ - تاریخ پذیرش: ۱۴۰۴/۰۶/۱۵

واکاوی تطبیقی نظام حقوق دیجیتال انگلستان و فرانسه در پاسخ‌گذاری کیفری به نقض حقوق عامه از طریق فعالیت‌های تروریستی برخط

پیمان نمامیان *

چکیده

پاسخ‌گذاری کیفری به نقض حقوق عامه در فعالیت‌های تروریستی برخط، به‌ویژه در نظام حقوق دیجیتال انگلستان و فرانسه، یکی از چالش‌های پیچیده در دنیای دیجیتال و فضای مجازی است. با گسترش استفاده از سکوهای برخط برای ارتکاب فعالیت‌های تروریستی، مانند تبلیغ خشونت، جذب نیرو و تأمین مالی غیرقانونی، حقوق عامه ازجمله امنیت فردی، نظم اجتماعی و اعتماد عمومی با تهدید روبه‌رو می‌شود. دراین‌راستا، نظام حقوق دیجیتال انگلستان و فرانسه با وضع مقررات کیفری خاص به مقابله با نقض حقوق عمومی در فضای دیجیتال پرداخته‌اند. انگلستان با رویکردی منعطف و به‌ویژه در قبال فعالیت‌های تروریستی برخط از مقرراتی استفاده می‌کند، در حالی که فرانسه با تصویب مقررات ویژه‌ای برای مقابله با این فعالیت‌ها، اقدامات جدی‌تری برای حذف محتوای غیرقانونی اتخاذ کرده است. این مطالعه به تحلیل و مقایسه نظام حقوق دیجیتال انگلستان و فرانسه در زمینه مقابله با نقض حقوق عامه ناشی از فعالیت‌های تروریستی برخط پرداخته و چالش‌ها و محدودیت‌های این مقررات را بررسی می‌کند. برای تأمین امنیت عمومی و حفاظت از حقوق عامه، ضروری است که قوانین ضدتروریستی در انگلستان و فرانسه بازنگری شوند. مرزهای فعالیت‌های تروریستی و آزادی بیان باید به‌طور دقیق و روشن تعیین گردد تا از سوءاستفاده پیشگیری شود. نهادهای نظارتی باید مستقل و حامی حقوق فردی باشند. به‌علاوه، همکاری‌های بین‌المللی، تدوین استانداردهای مشترک و بهره‌برداری از فناوری‌های نوین با رعایت حقوق بشر در مبارزه با فعالیت‌های تروریستی برخط امری ضروری است. اصلاحات در قوانین و فرایندها برای ایجاد توازن میان امنیت و حقوق عامه الزامی است.

واژگان کلیدی: امنیت عمومی و حقوق فردی، حقوق دیجیتال انگلستان و فرانسه، محتوای و فعالیت‌های تروریستی برخط، نقض حقوق عامه.

---

* . دانشیار گروه حقوق، دانشکده علوم اداری و اقتصاد دانشگاه اراک، اراک، ایران P_namamian1512@yahoo.com

مقدمه

امروزه فضای مجازی باتوجه به ویژگی‌های خاص خود، به محیطی مناسب برای بروز انواع ناهنجاری‌های اجتماعی تبدیل شده است. تروریسم با ورود به این بستر، از امکانات فناورانه و قدرت رسانه‌ای آن بهره‌برداری کرده و دراین‌راستا، با هدف بسط و گسترش جهان‌بینی فکری و سیاست‌های خود، از اهرم خشونت استفاده کرده و به ایجاد رسانه‌های مجازی اختصاصی اقدام نموده است (Ahmadi Moghadam & Gholami Doun, 2017). این در حالی است که حقوق عامه، حقوق و آزادی‌های اساسی شهروندان نظیر آزادی فردی، امنیت و دسترسی به اطلاعات است که برای حفظ رفاه و مقابله با سلطه نهادهای قدرت طراحی شده‌اند(Caruso, 2025: 118). در فضای مجازی، این حقوق با تهدیداتی مانند نقض حریم خصوصی، نفرت‌پراکنی و فعالیت‌های تروریستی برخط[آنلاین] مواجه‌اند.[1] فعالیت‌های تروریستی در این فضا، ازجمله انتشار محتوای خشونت‌آمیز و فراخوان به افراط‌گرایی، تهدیدی جدی برای نظم اجتماعی و امنیت عمومی محسوب می‌شوند.[2] در واکنش به این چالش‌ها، نظام حقوق دیجیتال[3] انگلستان و فرانسه اقدامات کیفری ویژه‌ای برای مقابله با نقض حقوق عامه در بستر دیجیتال اتخاذ کرده‌اند(Beitragsaufruf, 2022: 1).

انگلستان و فرانسه به‌منظور مقابله با نقض حقوق عمومی و تهدیدات تروریستی در فضای دیجیتال، چارچوب‌های قانونی جامعی را وضع کرده‌اند. در انگلستان، قوانینی ازجمله «قانون حفاظت از داده‌ها، مصوب ۲۰۱۸»[4]، «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰»[5] و «قانون تروریسم، مصوب ۲۰۰۶»[6]، زمینه‌های قانونی لازم برای حفاظت از داده‌های شخصی و مقابله با انتشار محتوای تروریستی را فراهم

1. https://www.brookings.edu/articles/dual-use-regulation-managing-hate-and-terrorism - online-before-and-after-section-230-reform/
2. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism /files / countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf
۳. حقوق دیجیتال (Digital Rights) به مجموعه‌ای از اصول و حقوق عامه در محیط برخط اشاره دارد که شامل محافظت از حریم خصوصی، آزادی بیان، دسترسی به اطلاعات، حفظ امنیت داده‌ها، کنترل بر اطلاعات شخصی، امنیت دیجیتالی و برخورداری از فرصت‌های برابر برای استفاده از اینترنت می‌شود. این حقوق به افراد اجازه می‌دهد که در فضای مجازی احساس امنیت، آزادی و برابری داشته باشند؛
- https://digital-strategy.ec.europa.eu/en/policies/digital-principles
باتوجه به گسترش روزافزون استفاده از اینترنت، تضمین این حقوق برای پیشگیری از نقض‌ها و ایجاد یک فضای امن و عادلانه برای تمام کاربران ضروری به‌نظر می‌رسد (Lucchi, 2011: 8-9).
4. Data Protection Act 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents
5. Computer Misuse Act 1990, https://www.legislation.gov.uk/ukpga/1990/18/contents
6. Terrorism Act 2006, https://www.legislation.gov.uk/ukpga/2006/11/contents

می‌سازند.[۱] در فرانسه نیز، مقرراتی نظیر «قانون راجع‌به اعتماد به نفس در اقتصاد دیجیتال، مصوب ۲۰۰۴»[۲]، «قانون مقابله با نفرت‌پراکنی برخط، مصوب ۲۰۲۰»[۳] و «قانون مبارزه با تبلیغات تروریستی برخط، مصوب ۲۰۲۲»[۴]، سکوهای دیجیتال را ملزم می‌سازد تا محتوای غیرقانونی، ازجمله محتوای تروریستی را ظرف بیست و چهار ساعت از زمان شناسایی یا اعلام رسمی، حذف نمایند. براین‌اساس، چارچوب مقررات انگلستان و فرانسه بر مسئولیت قانونی ارائه‌دهندگان خدمات اینترنتی و ضرورت برقراری توازن میان امنیت عمومی و صیانت از حقوق عامه تأکید دارند.

چالش‌ها و محدودیت‌های حقوقی در پاسخ‌گذاری کیفری به نقض حقوق عامه در فضای مجازی، به‌ویژه در مواجهه با فعالیت‌های تروریستی، در انگلستان و فرانسه، به‌سبب تحولات سریع فناوری و جهانی‌بودن فضای دیجیتال، پیچیدگی‌های خاصی دارد. ازاین‌رو، در انگلستان، مقررات مصوب برای تعیین مسئولیت سکوها مُکفی به‌نظر می‌رسند، در حالی که وفق مقررات فرانسه، نظیر قانون مقابله با نفرت‌پراکنی برخط، سکوها را ملزم به حذف محتوای غیرقانونی ظرف بیست و چهار ساعت پس از

---

۱. لازم به‌ذکر است دولت انگلستان «راهبرد امنیت ملی ۲۰۲۵ بریتانیا؛ امنیت برای مردم بریتانیا در دنیای خطرناک» (National Security Strategy 2025; Security for the British People in a Dangerous World) را با رویکردی فعالانه به بازتعریف امنیت ملی، ضمن مبادرت به شناسایی تهدیدات جهانی، توجه ویژه‌ای به تهدیدات داخلی شامل مسائل اقتصادی، فناوری، اقلیمی و انسجام اجتماعی معطوف داشت. این سند به‌طورخاص بر این نکته تأکید می‌کند که بریتانیا با تقویت امنیت داخلی، تقویت اتحادهای راهبردی و توسعه توانمندی‌های فناورانه مستقل، قصد دارد جایگاه خود را به‌عنوان یک قدرت جهانی بازپس‌گیرد؛

- https://www.gov.uk/government/publications/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world/national-security-strategy-2025-security-for-the-british-people-in-a-dangerous-world-html

در ضمن، تأکید می‌گردد «راهبرد مبارزه با تروریسم بریتانیا (Counter-terrorism strategy "CONTEST", 2023)»، به‌عنوان راهبرد ملی سال ۲۰۲۳ در قبال تهدیدات تروریستی، از سال ۲۰۰۶ به‌طور مداوم روزآمدسازی شده است. هدف کلان راهبرد، حفاظت از امنیت مردم و جامعه بریتانیا در قبال تهدیدات تروریستی است و مشتمل بر بخش‌هایی نظیر پیشگیری، آماده‌سازی و پاسخ به بحران‌های تروریستی است. این راهبرد بر رویکردهای پیشگیرانه، تقویت همکاری‌های بین‌المللی و مقابله با تهدیدات ناشی از فعالیت‌های تروریستی برخط تأکید دارد.

- https://www.gov.uk/government/publications/counter-terrorism-strategy-contest-2023/counter-terrorism-strategy-contest-2023-accessible

2. Law No. 2004-575 of June 21, 2004, on Confidence in the Digital Economy, France, https://www.wipo.int/wipolex/en/legislation/details/12761
3. France's Online Hate Law, Signed Law No. 2023-566, https:// digitalpolicyalert.org /event/13124-signed-law-no-2023-566-aimed-at-establishing-a-digital-majority-and-combating-online-hate-establishing-age-verification-requirement
4. Loi contre la propagande terroriste, https://www.assemblee-nationale.fr /13/projets/pl4497-ei.asp

گزارش، می‌کنند(Moslemzadeh Tehrani, et al., 2013: 209). علاوه‌براین، قوانین ضد نفرت‌پراکنی در انگلستان و فرانسه ممکن است منجر به حذف یا ویرایش محتوای غیرضروری یا محدودیت آزادی بیان شوند. در ضمن، با چالش‌هایی در راستای حفظ حریم خصوصی در قبال نیازهای امنیتی و دسترسی به داده‌ها مواجه هستند. این چالش‌ها به‌ویژه در زمینه فعالیت‌های تروریستی برخط که نیازمند شناسایی و حذف سریع محتوای مجرمانه هستند، پیچیدگی بیشتری پیدا می‌کنند.[1] اجرای مؤثر مقررات در سطح جهانی نیز برای انگلستان و فرانسه دشوار است؛ به‌ویژه باتوجه به وجود سکوهای جهانی که خارج از مرزهای ملی قرار دارند. ازاین‌رو، تطبیق مقررات با تحولات سریع فناوری، نظیر هوش مصنوعی و بلاک‌چین، برای انگلستان و فرانسه چالشی اساسی به‌شمار می‌رود. به‌علاوه، نظارت و پیگیری تخلفات در فضای مجازی نیازمند تخصیص منابع کافی است که به چالشی مهم تبدیل شده است. بنابراین، این چالش‌ها ایجاب می‌کند که مقررات به‌طور مستمر به‌روز رسانی شده و با تحولات دیجیتالی و جهانی همگام گردند.[2] در پاسخ به چنین شرایطی، انگلستان و فرانسه به‌طور جدی از حقوق فردی در قبال تهدیدات فضای مجازی، به‌ویژه درخصوص فعالیت‌های تروریستی برخط، محافظت می‌کنند. برای مقابله مؤثر با نقض حقوق عمومی در فضای مجازی در این زمینه، پیشنهادهایی هم‌چون تقویت مقررات سایبری، ایجاد نهادهای نظارتی مستقل، آموزش عمومی، و همکاری بین‌المللی قابل اجراست که امکان حفاظت از حقوق افراد، مقابله با تهدیدات تروریستی و کاهش مشکلات اجتماعی در فضای دیجیتال را فراهم می‌سازد.

به‌هرروی، این پژوهش به واکاوی و تطبیق پاسخ‌گذاری کیفری به نقض حقوق عامه در فعالیت‌های تروریستی برخط در انگلستان و فرانسه، با استفاده از روش توصیفی‌تحلیلی، می‌پردازد. اهداف پژوهش، مداقه در مقررات و سازوکارهای کیفری نظام حقوق دیجیتال انگلستان و فرانسه برای مقابله با تهدیدات تروریستی برخط، شناسایی چالش‌ها و محدودیت‌های موجود در پاسخ‌گذاری به این تهدیدات و مقایسه رویکردهای حقوقی آن‌ها است. به‌علاوه، این پژوهش به سنجش آثار حقوقی مقرر در این قوانین بر حقوق فردی و امنیت عمومی پرداخته و پیشنهادهایی برای تقویت پاسخ‌گذاری کیفری، حفاظت از حقوق فردی در فضای دیجیتال و بهبود هماهنگی بین‌المللی در قبال فعالیت‌های تروریستی برخط ارائه می‌دهد. درنهایت، این پژوهش به پرسش کلیدی «باتوجه به چالش‌ها و محدودیت‌های پاسخ‌گذاری کیفری در

1. https://www.esteri.it/wp-content/uploads/2021/12/UNIBO_Applicazione-dei-principi-della-Carta-delle-Nazioni-Unite-nello-spazio-cibernetico.pdf
2. https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---france.pdf

نظام حقوق دیجیتال انگلستان و فرانسه در مواجهه با فعالیت‌های تروریستی برخط، چگونه می‌توان ضمن پاسخ به تهدیدات، با نقض حقوق عامه در سکوهای مجازی مقابله کرد؟» پاسخ خواهد داد.

۱. پیشینه و تحولات تاریخی تقنینی

با گسترش روزافزون اینترنت در دهه‌های اخیر، گروه‌های تروریستی از بستر فضای مجازی برای تبلیغ اندیشه‌های افراطی، جذب نیرو، آموزش و برنامه‌ریزی عملیات‌های تروریستی بهره‌برداری کرده‌اند(Zeiger & Gyte, 2021: 376)؛ پدیده‌ای که به نقض‌های جدی در حقوق عامه، ازجمله امنیت عمومی، حقوق عامه و حریم خصوصی انجامیده است. ازاین‌رو، در اواخر قرن بیستم و هم‌زمان با توسعه فناوری‌های ارتباطی، بازیگران غیردولتی نظیر القاعده و متعاقب آن گروه تروریستی داعش[1]، با بهره‌گیری از فناوری‌های برخط، مبادرت به انتشار پیام‌های رادیکال، ایجاد شبکه‌های ارتباطی غیررسمی، و بسیج نیروهای افراطی نمودند(Ralstin, 2024: 18-19). با تبدیل اینترنت به ابزاری کارآمد برای رادیکال‌سازی در فرایند این تحولات، جهان شاهد آغاز مرحله‌ای نوین در نقض حقوق عمومی در حوزه‌های امنیت، انسجام اجتماعی و حفظ حریم خصوصی بود.

نخستین نمود آشکار نقض حقوق عامه در بستر فضای مجازی، در حوادث ۱۱ سپتامبر ۲۰۰۱ متجلی شد. از آن پس، اینترنت به‌عنوان بستری مؤثر برای نشر آموزش‌های تروریستی، تبلیغات اندیشه‌ها و انتشار محتوای خشونت‌آمیز تبدیل شد. با ظهور و گسترش شبکه‌های اجتماعی در دهه ۲۰۰۰، این روند شتاب بیشتری یافت (ظهیری، ۱۳۹۷: ۴۲۲) و بازیگران غیردولتی نظیر القاعده و متعاقب آن گروه تروریستی داعش از این سکوها برای گسترش دامنه تبلیغات، جذب نیرو و هدایت افکار عمومی بهره‌گیری کردند؛[2] وضعیتی که مراجع امنیتی و قانونگذار ملی و بین‌المللی را با چالش‌های نوینی مواجه ساخت(Schmitt, 2014: 279-281).

در پاسخ به این تهدیدات، برخی از کشورهای اروپایی همچون انگلستان و فرانسه با اصلاح و تقویت مقررات کیفری، سیاست‌های مقابله‌ای خود را در زمینه ارتکاب فعالیت‌های تروریستی برخط به‌طور قابل‌توجهی توسعه داده‌اند.[3] انگلستان از طریق تصویب مقررات جامع ضدتروریستی و تمرکز بر

---

۱. ظهور گروه تروریستی داعش را می‌توان نقطه عطفی در عصر فعالیت‌های تروریستی برخط انگاشت. این گروه تروریستی با بهره‌گیری گسترده از سکوهایی نظیر توییتر، فیسبوک و تلگرام، موفق به انتشار وسیع پیام‌های تبلیغاتی، تحریک جوانان و جذب نیرو از سراسر جهان شد؛ وضعیتی که نقض فاحش امنیت عمومی و حریم خصوصی را به‌همراه داشت(Chaliand & Blin, 2016: 154-155).

2. https://unrcca.unmissions.org/sites/default/files/old_dnn/The%20Impact %20of %20External%20factors%20on%20Security%20and%20Development%20in%20Central%20Asia_ENG.pdf

3. https://assets.publishing.service.gov.uk/media/5b23df8f40f0b634d557b020/140618_CCS207_CCS0218929798-1_CONTEST_3.0_WEB.pdf;

مسئولیت‌پذیری سکوها،[1] و فرانسه با رویکردی سخت‌گیرانه‌تر و تمرکز بر حذف فوری محتوای غیرقانونی،[2] تلاش داشته‌اند با تهدیدات ناشی از فعالیت‌های تروریستی برخط مقابله کنند. همکاری میان دولت‌ها و سکوهای دیجیتال برای شناسایی، پالایش و انسداد محتوای افراطی، ازجمله اقدامات محوری در این حوزه بوده است.[3] بنابراین، رویکرد مزبور با چالش‌های حقوقی و اخلاقی مهمی مواجه‌اند. ازجمله این چالش‌ها می‌توان به عدم توافق راجع‌به تعریف جامع و شفاف از «فعالیت‌های تروریستی برخط»، تمایز مبهم میان آزادی بیان و ترویج خشونت، تهدید فزاینده حریم خصوصی ناشی از نظارت‌های گسترده و دشواری در برقراری توازن میان امنیت ملی و حقوق بنیادین بشر اشاره کرد.

پس از وقوع حملات گسترده‌ای نظیر تیراندازی به «مجله طنز شارلی ابدو»[4] پاریس در هفتم ژانویه سال ۲۰۱۵ و انفجار ۲۲ مِی سال ۲۰۱۷ پس از اجرای کنسرت در خارج از سالن «منچستر آرنا» در منچستر بریتانیا، موجب شد تا کشورهای اروپایی و البته ایالات متحده آمریکا نسبت به تصویب مقررات سخت‌گیرانه‌تری در حوزه مبارزه با فعالیت‌های تروریستی برخط اقدام‌های جدی‌تری داشته باشند. درهرحال، اتخاذ سیاست‌های کیفری در قبال فعالیت‌های تروریستی برخط به یکی از چالش‌برانگیزترین موضوعات در تقاطع امنیت ملی، مقابله با افراط‌گرایی و رعایت حقوق بشر تبدیل شد و منجر به تلاش از سوی برخی کشورهای اروپایی نظیر انگلستان و فرانسه برای تقویت چارچوب‌های حقوقی و ایجاد سازوکارهای نظارتی مؤثر، جهت مقابله‌ای متوازن و مشروع با تهدیدات ناشی از فعالیت‌های تروریستی برخط گردید.

۲. نقض حقوق عامه در سکوهای مجازی؛ اقسام و مفهوم‌شناختی

اقسام نقض حقوق عامه در سکوهای مجازی در چارچوب نظام حقوق دیجیتال انگلستان و فرانسه برای پاسخ کیفری به فعالیت‌های تروریستی برخط شامل آزار و اذیت برخط، انتشار اطلاعات کذب، کلاهبرداری برخط، محتوای مخرب و تفرقه‌انگیز، و نقض حریم خصوصی و امنیت اطلاعات است. این نقض‌ها تهدیدات جدی برای امنیت اجتماعی و حقوق فردی در دنیای دیجیتال محسوب می‌شوند و پاسخ‌های قانونی متناسب در این زمینه ضروری است.

---

https://www.asser.nl/about-the-asser-institute/news/new-publication-countering-cyber-terrorism-in-a-time-of-war-on-words-the-case-of-france/

1. https://techagainstterrorism.org/news/2020/10/22/online-regulation-series-the-united - kingdom
2. https://onu.delegfrance.org/Together-against-terrorist-use-of-internet
3. https://www.gov.uk/government/publications/uk-france-joint-leaders-declaration/uk-france -joint-leaders-declaration
4. Attentat contre Charlie Hebdo

رفتارهای مضر در فضای دیجیتال که هدف آن‌ها آسیب‌رساندن به فرد یا گروه خاص از طریق توهین‌ها، تهدیدات و حملات سایبری است، «**آزار و اذیت برخط**» گفته می‌شود (Slaughter & Newman, 2022: 14). در انگلستان و فرانسه، این نوع آزار، قابل تعقیب قانونی است.[1] در این کشورها، مقررات خاصی برای جرم‌انگاری توهین‌ها، تهدیدات و حملات سایبری وجود دارد که بر مسئولیت سکوهای برخط برای نظارت و حذف محتواهای مضر تأکید می‌کند(Ayepeku, et al., 2024: 7-8). این آزارها می‌توانند آسیب‌های روانی و جسمی زیادی به افراد وارد کنند و برای حمایت از بزه‌دیدگان، نظام‌های حقوقی کشورها اقداماتی را اتخاذ کرده‌اند. در ضمن، به انتشار محتوای نادرست و گمراه‌کننده‌ای که با هدف فریب، تحریک احساسات یا تغییر نگرش‌ها منتشر می‌گردد، جرم «**انتشار اطلاعات کذب** یا اخبار جعلی» اطلاق می‌شود که امکان کاهش اعتماد عمومی به رسانه‌ها و نهادهای دولتی، مختل‌کردن فرایندهای دموکراتیک، و تحریک تنش‌های اجتماعی را فراهم می‌کند.[2] در انگلستان و فرانسه، مقررات و تدابیر نظارتی برای مقابله با اخبار جعلی ضروری است؛ زیرا این نوع محتوا تهدیدی جدی برای انسجام اجتماعی و اعتماد عمومی به‌حساب می‌آید(Coe, 2023: 236).

ارتکاب رفتارهای فریب‌کارانه با هدف دستیابی غیرقانونی به اطلاعات شخصی یا مالی کاربران در بستر اینترنت کلاهبرداری برخط[3] است که از طریق روش‌هایی همچون فیشینگ، خریدهای اینترنتی جعلی، یا دسترسی غیرمجاز به حساب‌های بانکی صورت می‌پذیرد.[4] نظام حقوق دیجیتال انگلستان و فرانسه، مقرراتی گوناگونی در حوزه جرایم رایانه‌ای و حمایت از مصرف‌کنندگان به تصویب رسیده است که بر ارتقای آگاهی عمومی و اتخاذ تدابیر قانونی و فنی جهت پیشگیری و مقابله با این تهدیدات تأکید دارند(Cross, 2019: 123-125). به‌علاوه، برانگیختن تنش، اختلاف و تفرقه میان گروه‌های اجتماعی، مذهبی یا قومی منتشر نظیر پیام‌های حاوی مضامین نژادپرستانه، تبعیض‌آمیز یا تحریک‌آمیز، به‌عنوان نشر محتوای مخرب و تفرقه‌انگیز به‌شمار می‌آید که منجر به نفرت‌پراکنی، تبعیض و حتی خشونت می‌شوند(Banchio, 2024: 29-31). مقررات انگلستان و فرانسه با تمرکز بر سکوهای دیجیتال، اقدامات گسترده‌ای را برای رصد، محدودیت و حذف این نوع محتواها پیش‌بینی کرده‌اند تا از تشدید شکاف‌های اجتماعی، فرهنگی و سیاسی پیشگیری کنند(Sander, 2021: 172-174). البته هرگونه دسترسی یا

1. https://www.universitiesuk.ac.uk/sites/default/files/field/downloads/2021-07/ tackling - online-harassment.pdf
2. Department for Digital, Culture, Media and Sport. (2019). *Online Harms White Paper: Full Government Response to the Consultation* (CP 57). London: HM Government.
3. Online fraud
4. https://www.bajajfinserv.in/insurance/online-fraud-and-types-of-online-fraud

بهره‌برداری غیرمجاز از داده‌های شخصی افراد مشتمل بر شامل هک حساب‌های کاربری، سرقت داده‌ها، شنود غیرمجاز، یا افشای و فروش اطلاعات حساس، موجب خواهد شد تا حریم خصوصی و امنیت اطلاعات نقض شود.[۱] در انگلستان،[۲] «قانون حفاظت از داده‌ها، مصوب ۲۰۱۸»[۳] و در فرانسه،[۴] «قانون حفاظت از داده‌ها، مصوب ۱۹۸۷؛ اصلاحی ۲۰۰۴»[۵] به‌عنوان مبنای حقوقی اصلی، وظایف اشخاص و نهادها را در زمینه گردآوری، پردازش و نگهداری داده‌ها مشخص کرده و سازوکارهای حمایتی مؤثری برای حفظ حریم خصوصی افراد پیش‌بینی کرده‌اند.

بااین‌همه، اذعان می‌گردد یکی از چالش‌های اساسی در حوزه حقوق فناوری اطلاعات در انگلستان و فرانسه، مقابله با نقض حقوق عامه در فرایند ارتکاب فعالیت‌های تروریستی برخط است. این کشورها با تصویب مقرراتی همانند «قانون ایمنی برخط، مصوب ۲۰۲۳»[۶] در انگلستان و تدوین مقرراتی سخت‌گیرانه پس از حملات تروریستی در فرانسه، سکوهای دیجیتال را ملزم به شناسایی و حذف سریع محتوای تروریستی و غیرقانونی کرده‌اند(Tsesis, 2017: 623). بااین‌حال، ضرورت رعایت توازن میان الزامات امنیتی و تضمین حقوق بنیادینی نظیر آزادی بیان و حق بر حریم خصوصی همواره مورد تأکید قرار گرفته است.[۷] بنابراین، تدابیر نظارتی باید شفاف، متناسب و براساس اصول حاکم بر حقوق بشر طراحی شوند تا از هرگونه سوءاستفاده و نقض آزادی‌های مدنی پیشگیری به عمل آید.

۳. چالش‌های نقض حقوق عامه و رویکردهای حقوقی پاسخ به تهدیدهای ناشی از فعالیت‌های تروریستی برخط

در دنیای دیجیتال امروز، سکوهای مجازی به یکی از ابزارهای حیاتی برای ارتباطات و نشر اطلاعات

1. https://www.gdprsummary.com/personal-data-breach-guide/
2. https://www.dlapiperdataprotection.com/?c=GB
3. Data Protection Act 2018; https://www.legislation.gov.uk /ukpga/ 2018/ 12/contents/enacted
4. https://www.dlapiperdataprotection.com/index.html?t=law&c=FR
5. La Loi Informatique et Libertés, créée en 1978 et modifiée en 2004, https://donnees-rgpd.fr/loi-informatique-libertes/
6. Online Safety Act 2023, https://www.legislation.gov.uk/ukpga/2023/50

۷. تطبیق حق آزادی بیان با ممنوعیت و مقابله با استفاده از فضای مجازی برای اهداف تروریستی، چالشی نوین در حقوق بین‌الملل است(Kazerooni, 2016: 167) که نیازمند تعادل میان حفاظت از حقوق فردی و تأمین امنیت عمومی می‌باشد. از یک‌سو، حق آزادی بیان به‌عنوان یکی از اصول بنیادین حقوق بشر در اسناد بین‌المللی به‌ویژه میثاق بین‌المللی حقوق مدنی و سیاسی تضمین شده است، و هرگونه محدودیت بر این حق باید مطابق با استانداردهای بین‌المللی اعمال گردد. از دیگر سو، بهره‌گیری از فضای مجازی برای ترویج فعالیت‌های تروریستی تهدیدی جدی برای امنیت ملی و بین‌المللی است که دولت‌ها موظف به مقابله با آن می‌باشند. در این راستا، سیاست‌های حقوقی باید ضمن رعایت حقوق بشر، از امنیت عمومی نیز حمایت کنند و این دو اصل را به‌طور هم‌زمان تأمین نمایند.

تبدیل شده‌اند. بااین‌حال، این سکوها هم‌زمان بـه ابـزاری بـرای فعالیت‌هـای تروریسـتی تبـدیل شـده‌اند. تروریست‌ها از سکوهای مجازی برای انتشار اطلاعات، تبلیغات، جـذب نیروهـای جدیـد، سـازماندهی عملیات‌ها، تأمین مالی غیرقانونی و انجام عملیات روانی استفاده می‌کنند. ایـن اقـدامات بـه‌طور مسـتقیم تهدیـدی بـرای حقـوق عامـه، ازجملـه امنیـت عمـومی، اعتمـاد اجتمـاعی و حقـوق عامـه بـه شـمار می‌روند(White, 2020: 31-33).

فعالیت‌های تروریستی علیه حقوق عامـه در سـکوهای مجـازی می‌تواننـد شـامل انتشـار ویـدیوهای تهدیدآمیز، فراخوان‌ها به خشونت، آموزش‌های اینترنتـی، تـأمین مـالی از طریـق روش‌هـای غیرقـانونی و عملیات روانی برای برهم‌زدن نظم عمومی باشند.[1] ایـن اقـدامات نـه‌تنها بـا اصـول حقـوقی نظیـر امنیـت عمومی و حقوق عامه در تضاد هستند، بلکه تهدیداتی جدی برای حقوق اجتماعی و امنیت ملی کشـورها به‌وجود می‌آورند.

انگلستان در راستای مقابله با تهدیدات فضای دیجیتال، مقررات متعددی نظیر «قـانون سوءاسـتفاده از رایانه، مصوب ۱۹۹۰»، «قانون تروریسم، مصوب ۲۰۰۰»[2] و «قانون ایمنـی بـرخط، مصـوب ۲۰۲۳» را برای نظارت بر فعالیت‌های سایبری و تروریستی برخط تصویب کرده اسـت؛ ایـن مقـررات در انگلسـتان نه‌تنها به‌منظور تأمین امنیت عمومی، بلکه برای حفظ حقوق فردی و مقابله با تهدیداتی هستند کـه ممکـن است منجر به نقض امنیت ملی و اجتماعی شوند. در ضمن، فرانسه نیز در واکنش به تهدیـدات مشـابه در فضای مجازی، مقرراتی را مشتمل بر «قانون اعتماد در اقتصاد دیجیتال، مصوب ۲۰۰۴»[3]، «قانون مبـارزه با محتوای نفرت‌انگیز در اینترنت، مصوب ۲۰۲۰»[4] و «قانون مجازات، اصلاحی ۲۰۲۵»،[5] برای نظارت بر فعالیت‌های تروریستی برخط تصویب کرده است.

انگلستان و فرانسه با تصویب مقررات متنوع، ضـمن کنتـرل تهدیـدات، بـا جرم‌انگـاری بهره‌گیـری از سکوهای مجازی برای تبلیغات تروریستی و الزام سـکوها بـه حـذف سـریع محتـوای غیرقـانونی، مقابلـه کردند(Macdonald, et al., 2019: 187-188). البته باید توجه داشت که این مقررات بایـد بـه‌طور دقیـق و

1. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/transparency -reporting-on-terrorist-and-violent-extremist-content-online_3f72a170/901cb8cf-en.pdf
2. Terrorism Act 2000, https://www.legislation.gov.uk/ukpga/2000/11/contents
3. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (1), https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164
4. LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (1), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970
5. Code pénal, Dernière mise à jour des données de ce code: 11 juillet 2025 (Version en vigueur au 31 juillet 2025), https://www.legifrance.gouv.fr/codes /texte_lc /LEGITEXT000006070719/

بدون نقض حقوق عامه اجرا شوند تا تعادلی مناسب میان امنیت و حقوق فردی برقرار شود. بنابراین، انگلستان و فرانسه با تصویب مقررات گوناگون، در تلاشند تا از این سکوها به‌عنوان ابزارهای نظارتی و امنیتی برای مقابله با فعالیت‌های تروریستی برخط بهره‌برداری کنند. در این راستا، هماهنگی مقررات و نظارت دقیق بر محتوای برخط ضروری است تا ضمن پیشگیری از نقض حقوق بشر، نسبت به حفظ امنیت عمومی مبادرت شود.[1]

۴. پاسخ‌گذاری‌های کیفری به نقض حقوق عامه از طریق فعالیت‌های تروریستی برخط

سکوهای مجازی در دنیای معاصر به ابزاری مؤثر در ارتکاب و ترویج فعالیت‌های تروریستی تبدیل شده‌اند و ازاین‌حیث، تهدیدی جدی برای امنیت ملی و حقوق عامه محسوب می‌شوند. در واکنش به این وضعیت، انگلستان و فرانسه با تصویب قوانین خاص، تلاش کرده‌اند از طریق الزام سکوهای دیجیتال به شناسایی، حذف محتوای تروریستی و اعمال نظارت مؤثر، با این پدیده مقابله کنند. بااین‌حال، چالش اساسی در این مسیر، حفظ توازن میان تأمین امنیت عمومی و صیانت از حقوق و آزادی‌های بنیادین افراد است؛ امری که باید در چهارچوب اصول حقوق بشر و الزامات دادرسی منصفانه مورد توجه قرار گیرد.

در این راستا، بررسی تطبیقی رویکردهای کیفری دو نظام حقوق دیجیتال انگلستان و فرانسه در مواجهه با نقض حقوق عامه ناشی از فعالیت‌های تروریستی برخط، می‌تواند به تبیین نقاط قوت، چالش‌ها و الزامات حقوقی مؤثر در تقنین و اجرای این سیاست‌ها کمک نماید.

۴-۱. نظام حقوقی انگلستان

با گسترش فضای دیجیتال و تهدیدات تروریستی برخط، نظام‌های حقوقی به بازنگری در سازوکارهای کیفری خود پرداخته‌اند. انگلستان، به‌عنوان پیشگام در مقابله با فعالیت‌های تروریستی برخط، مجموعه‌ای از قوانین کیفری سنتی و نوین را وضع کرده است. فعالیت‌های تروریستی برخط تهدیداتی فیزیکی، فرهنگی، روانی و سیاسی ایجاد می‌کند که نیاز به پاسخ‌گذاری کیفری مؤثر از سوی نظام حقوقی دارد. این پاسخ‌گذاری باید ضمن حفظ امنیت عمومی و حقوق فردی، از تهدید آزادی‌های بنیادین پیشگیری کند. بنابراین، انگلستان مجموعه‌ای از مقررات برای مقابله با فعالیت‌های تروریستی برخط و نقض حقوق عامه تدوین کرده است که توازن میان امنیت و حقوق فردی را هدف قرار می‌دهند(Wei, 2024: 7-8).

بنابراین، نظام حقوقی انگلستان مجموعه‌ای از مقررات را به‌منظور مقابله با فعالیت‌های تروریستی برخط و نقض حقوق عامه تدوین کرده است. این مقررات در واکنش به چالش‌های نوظهور و با هدف

1. https://www.interieur.gouv.fr/actualites/actualites-du-ministere/rapport-annuel-sur-cybercriminalite-2024

تقویت امنیت عمومی و حفظ حقوق فردی، و نیز برقراری توازن میان این دو، وضع شده‌اند.[1] ازاین‌رو، این مقررات به‌اختصار بررسی می‌شوند:

الف- «قانون تشویق به نفرت، مصوب ۱۹۸۶»[2]؛ این قانون در ابتدا برای مقابله با نفرت‌پراکنی در اماکن عمومی طراحی شد، اما با توسعه فضای دیجیتال، به انتشار محتوای نفرت‌انگیز در بسترهای مجازی نیز گسترش یافته است. قانون مزبور، با جرم‌انگاری تحریک به نفرت نژادی، قومی، دینی یا جنسیتی، در پی حفظ کرامت انسانی و پیشگیری از خشونت است.

ب- «قانون انتشار مطالب تهدیدآمیز، مصوب ۱۹۸۸»؛[3] این قانون بر ممنوعیت ارسال پیام‌های تهدیدآمیز یا توهین‌آمیز از طریق پست، تلفن یا ارتباطات دیجیتال تمرکز دارد. با گسترش شبکه‌های اجتماعی، اهمیت اجرای این قانون دوچندان شده است. قانون مصوب، اگرچه ابزاری مؤثر برای مقابله با تهدیدات روانی و آزارهای دیجیتال است، اما ضرورت بازتعریف و شفاف‌سازی در حوزه‌های نوپدید رسانه‌ای انکارناپذیر است.

ج- «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰»؛ این قانون، به‌عنوان نخستین گام برای مقابله با جرائم سایبری، دسترسی غیرمجاز به سامانه‌ها، خرابکاری دیجیتال و بدافزارها را جرم‌انگاری کرده است؛ اگرچه این قانون نقش زیربنایی در مبارزه با جرائم سایبری ایفا می‌کند، اما در مقابله با فعالیت‌های تروریستی سازمان‌یافته در بستر دیجیتال کفایت ندارد و نیازمند بازنگری منظم است.[4]

د- «قانون حفاظت در قبال آزار و اذیت»؛[5] این قانون، آزارهای مکرر و تهدیدآمیز را ازجمله در فضای برخط مشمول جرم‌انگاری قرار داده است. قانون مزبور، ابزار مناسبی برای حمایت از افراد در برابر تهدیدات مستمر است، اما در حوزه فعالیت‌های تروریستی برخط نیازمند تکمیل با سازوکارهای امنیتی گسترده‌تر می‌باشد.

هـ- «قانون تروریسم، مصوب ۲۰۰۰»[6]؛ این قانون، بنیان حقوقی پاسخ به فعالیت‌های تروریستی در انگلستان را فراهم کرده و مصادیقی چون عضویت در گروه‌های تروریستی، حمایت یا ترویج فعالیت‌های تروریستی را جرم اطلاق می‌کند. اصلاحیه «قانون تروریسم ۲۰۰۰ (سازمان‌های ممنوعه)، (اصلاح) دستور ۲۰۱۱»[7] نیز تأکید ویژه‌ای بر ترویج فعالیت‌های تروریستی برخط دارد. با وجود اهمیت پیشگیرانه، این قانون به دلیل دامنه وسیع و فقدان تعریف دقیق مفاهیمی چون «تحریک» یا «تحسین تروریسم»، ممکن است ناقض اصل قانونی‌بودن جرائم و مجازات‌ها تلقی شود.

1. https://www.brookings.edu/articles/dual-use-regulation-managing-hate-and-terrorism-online-before-and-after-section-230-reform/
2. Public Order Act 1986, https://www.legislation.gov.uk/ukpga/1986/64
3. Malicious Communications Act 1988, https://www.legislation .gov.uk/ ukpga/1988 /27/section/1
4. https://www.legislation.gov.uk/ukpga/1990/18/contents
5. Protection from Harassment Act 1997, https://www.legislation .gov .uk/ ukpga /1997/40/contents
6. Terrorism Act 2000, https://www.legislation.gov.uk/ukpga/2000/11
7. The Terrorism Act 2000 (Proscribed Organisations) (Amendment) Order 2011, https://www.legislation.gov.uk/ukdsi/2011/9780111505700

ر- «قانون ارتباطات، مصوب ۲۰۰۳»[1]؛ ارسال پیام‌های آزاردهنده یا تهدیدآمیز از طریق اینترنت، تحت ماده ۱۲۷ جرم‌انگاری شده است. این قانون، در مقابله با خشونت‌های کلامی و تهدیدات سایبری مفید است، اما با چالش اثبات سوءنیت در فضای مجازی مواجه است.

ز- «**قانون اختیارات تحقیق، مصوب ۲۰۱۶**»؛[2] این قانون به دولت اجازه می‌دهد نظارت گسترده‌ای بر ارتباطات دیجیتال داشته باشد، که شامل جمع‌آوری فراگیر اطلاعات و فعالیت‌های برخط می‌شود. با وجود هدف امنیتی، این قانون با انتقاداتی شدید از سوی مدافعان حقوق بشر و آزادی‌های مدنی مواجه شده و خطر تضعیف حریم خصوصی را افزایش داده است.

ژ- «قانون حفاظت از داده‌ها، مصوب ۲۰۱۸»؛[3] این قانون در راستای مقررات عمومی حفاظت از داده اتحادیه اروپا[4] طراحی شده و اصولی نظیر رضایت، شفافیت و حق فراموشی را تقویت می‌کند. وجود این قانون تضمینی برای محدودیت نظارت افراطی در مقررات ضدتروریستی بوده و نقش مهمی در توازن امنیت و حریم خصوصی دارد.

ح- «قانون ایمنی برخط، مصوب ۲۰۲۳»؛ **این قانون با تمرکز بر محافظت از کودکان در فضای دیجیتال، مسئولیت‌هایی را برای سکوها تعیین کرده و آن‌ها را به حذف محتوای مضر ملزم می‌سازد. در عین حمایت از کودکان، نگرانی‌هایی از بابت تأثیر بر آزادی بیان و مسئولیت حقوقی بیش از حد برای سکوها مطرح است.**

نظام حقوق کیفری انگلستان در قبال نقض حقوق عامه به‌واسطه فعالیت‌های تروریستی برخط، از ترکیب مقررات سنتی و نوین استفاده می‌کند. این رویکرد نه‌تنها به جرم‌انگاری فعالیت‌های تروریستی برخط، بلکه به گسترش صلاحیت‌های نظارتی دولت، مسئولیت سکوها و حفاظت از حقوق شهروندان نیز توجه دارد. مقرراتی همچون «قانون تروریسم، مصوب ۲۰۰۰» و اصلاحات آن، معیارهای فعالیت‌های تروریستی برخط نظیر حمایت و تحریک به فعالیت‌های تروریستی برخط تعیین می‌کنند. بااین‌حال، ابهام در مفاهیمی مانند «تحریک» می‌تواند با اصول حقوق کیفری و آزادی بیان در تضاد باشد.[5]

---

1. Communications Act 2003, https://www.legislation.gov.uk/ukpga/2003/21/contents
2. Investigatory Powers Act 2016, https://www.legislation.gov.uk/ukpga/2016/25
3. Data Protection Act 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents

٤. مقررات عمومی حفاظت از داده‌ها(**General Data Protection Regulation "GDPR"**) که از سوی اتحادیه اروپا مصوب شده است، معیارهای سخت‌گیرانه‌ای را برای حفاظت از داده‌های شخصی در سراسر اروپا تعیین کرده است؛
- General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016 O.J. (Apr. 27, 2016).
این مقررات که در ۲۵ مه ۲۰۱۸ به تصویب رسید، با هدف حفاظت از حریم خصوصی افراد در قبال تهدیدهای دیجیتالی ایجاد شده است؛
- https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/.

5. Jonathan Hall K.C. (2025, July 15). The Terrorism Acts in 2023: Report of the Independent Reviewer of Terrorism Legislation (accessible). UK Government.

در زمینه نظارت، «قانون اختیارات تحقیق، مصوب ۲۰۱۶» اختیارات گسترده‌ای به دولت می‌دهد که موجب نگرانی‌هایی درخصوص حریم خصوصی و فقدان نظارت قضائی مستقل شده است. در مقابل، «قانون حفاظت از داده‌ها، مصوب ۲۰۱۸» تلاش کرده تا توازن میان امنیت و حریم خصوصی را برقرار کند. افزون‌براین، «قانون ایمنی برخط، مصوب ۲۰۲۳» سکوها را ملزم به حذف محتوای مضر می‌کند و در صورت عدم رعایت این تکالیف، مسئولیت کیفری و مدنی به همراه دارد؛ هرچند نگرانی‌هایی درخصوص آزادی بیان و مسئولیت‌های نامتناسب مطرح است(Siagian, et al., 2023: 518). البته در پاسخ به این انتقادها، «قانون حفاظت از داده‌ها، مصوب ۲۰۱۸»، که منطبق با «**مقررات عمومی حفاظت از داده اتحادیه اروپا**، مصوب ۲۰۱۶» تدوین شده، با تأکید بر اصولی نظیر رضایت، محدودیت در پردازش، و حق حذف داده‌ها («حق فراموشی»)، در صدد توازن‌بخشی میان الزامات امنیتی و حمایت از حریم خصوصی برآمده است(Farrand, 2024: 253).

بااین‌حال، افزون بر مقررات خاص در قبال فعالیت‌های تروریستی برخط، مجموعه‌ای از مقررات مکمل همچون «قانون تشویق به نفرت، مصوب ۱۹۸۶»، «قانون انتشار مطالب تهدیدآمیز، مصوب ۱۹۸۸»، «قانون سوءاستفاده از رایانه، مصوب ۱۹۹۰» و «قانون ارتباطات، مصوب ۲۰۰۳» نیز در واکنش به ابعاد مختلف فعالیت‌های تروریستی برخط نظیر نفرت‌پراکنی، تهدیدهای روانی و خرابکاری سایبری به‌کار گرفته شده‌اند؛ گرچه این مقررات در ابتدا با اهدافی خارج از حوزه فعالیت‌های تروریستی برخط تصویب شده‌اند، اما در واکنش به تحولات امنیتی، تفسیر موسع یافته و نقشی مکمل برای مقررات خاص ایفا می‌کنند.

به‌هر روی، پاسخ کیفری انگلستان به فعالیت‌های تروریستی برخط در حمایت از حقوق عامه، رویکردی چندلایه با تأکید بر جرم‌انگاری، نظارت دولت، مسئولیت سکوها و حمایت از حقوق کاربران است، اما همچنان چالش‌هایی چون ابهام مفاهیم کیفری و تهدید آزادی بیان باقی است.[1] ازاین‌رو، برای حفظ مشروعیت حقوقی این نظام، بازنگری در مفاهیم و نظارت مستقل قضائی، ضرورتی انکارناپذیر است.

۴-۲. نظام حقوقی فرانسه

نظام حقوقی فرانسه در قبال تهدیدات ناشی از فعالیت‌های تروریستی برخط، مجموعه‌ای از مقررات قانونی را تصویب کرده است که شامل نظارت دیجیتال، دادرسی ویژه و همکاری‌های بین‌المللی

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

1. https://techagainstterrorism.org/news/2020/10/22/online-regulation-series-the-united-kingdom

می‌شود.[۱] این مقررات به نهادهای امنیتی امکان تعقیب مرتکبان و حفظ توازن میان امنیت عمومی و حقوق فردی را فراهم می‌آورد. باتوجه به گسترش تهدیدات نوین، این مقررات به‌طور مستمر روزآمد شده‌اند تا با چالش‌های نوین سازگاری داشته باشند؛ ازاین‌رو، این مقررات به‌اختصار بررسی می‌شوند:

الف- «قانون کیفری فرانسه، مصوب ۱۸۱۰»[۲]؛ این قانون با وجود قدمت، همچنان اصول بنیادین حقوقی مانند اصل قانونی‌بودن جرم و مجازات و فرض بی‌گناهی را حفظ کرده است. اگرچه این قانون به‌طور مستقیم به فعالیت‌های تروریستی برخط نمی‌پردازد، اما مبانی آن وفق چارچوب حقوقی مقرراتی نظیر «قانون مبارزه با تروریسم، مصوب ۲۰۱۵ [قانون شماره ۲۰۱۵-۹۱۲ مورخ ۲۴ ژوئیه ۲۰۱۵ راجع‌به اطلاعات]»[۳] و «قانون امنیت داخلی، مصوب ۲۰۱۵»[۴]، اِعمال شده است.

ب- «قانون اِعمال آزادی رسانه‌ها، مصوب ۲۰۰۴»[۵]؛ **این قانون برای تنظیم فضای دیجیتال و تقویت اعتماد در اقتصاد برخط تدوین شده است. این قانون، ارائه‌دهندگان خدمات اینترنتی را مسئول انتشار محتوای غیرقانونی، به‌ویژه محتوای تروریستی می‌کند. به‌علاوه، حقوق کاربران را در زمینه حفاظت از داده‌ها و شفافیت فعالیت‌های برخط تضمین می‌کند.**

ج- **«پیشگیری از تروریسم و مبارزه با نقض آزادی‌های فردی، مصوب ۲۰۱۱»**؛[۶] **این قانون به مقامات اجازه می‌دهد بدون دستور قضائی، نظارت بر فعالیت‌های برخط و** ارتباطات **مظنونان تروریستی را انجام دهند و ترویج و آموزش اقدامات تروریستی در فضای دیجیتال را جرم‌انگاری می‌کند.**

د- **«قانون ضدتروریسم، مصوب ۲۰۱۴»**؛[۷] قانون ضدتروریسم ۲۰۱۴ فرانسه به‌منظور تقویت اقدامات مقابله با فعالیت‌های تروریستی و ارتقای امنیت عمومی تصویب گردیده است. این قانون به مقامات ذی‌صلاح امکان دسترسی به محتوای برخط، تسهیل همکاری‌های بین‌المللی درخصوص مبارزه با فعالیت‌های تروریستی و تجویز بازرسی‌های امنیتی بدون نیاز به حکم

1. https://www.sgdsn.gouv.fr/files/files/ Publications / 20181004 – plan - d- action – contre -le-terrorisme-anglais.pdf
2. Code Pénal de 1810, https://www.legifrance.gouv.fr/codes/texte_ lc / LEGITEXT 000006071029/1810-02-27
3. Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899
4. Loi n° 2015-912 du 24 juillet 2015 relative à la sécurité intérieure, https://www.legifrance.gouv.fr /loda/id/JORFTEXT000030931899
5. Loi sur la Confiance dans l'Économie Numérique – LCEN, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164
6. Loi n° 2011-392 du 14 avril 2011 relative à la prévention du terrorisme et à la lutte contre les atteintes aux libertés individuelles, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000023860729/
7. Loi du 13 novembre 2014 relative à la lutte contre le terrorisme, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000029754374

قضائی را می‌دهد. علاوه‌براین، تدابیر حمایتی برای بزه‌دیدگان حملات تروریستی پیش‌بینی شده و مجازات‌های سخت‌گیرانه‌تری برای ارتکاب جرایم مرتبط با فعالیت‌های تروریستی، نظیر پیوستن به گروه‌های تروریستی، تعیین گردیده است.

هـ- «قانون مبارزه با تروریسم، مصوب ۲۰۱۵»؛ این قانون پس از حملات تروریستی پاریس تصویب شد تا ابزارهای قانونی برای مقابله با تهدیدات تروریستی تقویت شود. این قانون ابزارهای قانونی نوینی برای مقابله با تهدیدات تروریستی نظیر نظارت بیشتر بر ارتباطات دیجیتال و فعالیت‌های برخط و جرم‌انگاری تبلیغ فعالیت‌های تروریستی در فضای دیجیتال مقرر نمود.

ر- «قانون امنیت داخلی، مصوب ۲۰۱۵»؛ پس از وقوع حملات گسترده‌ای نظیر تیراندازی به «مجله طنز شارلی ابدو» در ژانویه ۲۰۱۵، این قانون اختیارات وسیعی به مقامات امنیتی برای نظارت اطلاعاتی، رصد ارتباطات الکترونیکی و استفاده از الگوریتم‌ها برای شناسایی تهدیدات داده است.

ز- «**قانون حفاظت از داده‌های شخصی، مصوب ۲۰۱۸**»؛[1] **این قانون برای هم‌راستایی با مقررات عمومی حفاظت از داده‌های اتحادیه اروپا تدوین شده و هدف آن تقویت حفاظت از داده‌های شخصی و افزایش شفافیت در استفاده از این داده‌ها است. البته بر شفافیت در استفاده از داده‌های شخصی و حقوق دسترسی و اصلاح داده‌ها تأکید دارد.**

ژ- « قانون راجع‌به مبارزه با دستکاری اطلاعات، مصوب ۲۰۱۸»؛[2] **این قانون به‌ویژه برای مقابله با اخبار نادرست و حفظ امنیت عمومی در دوره‌های انتخاباتی طراحی شده است و به مقامات اجازه می‌دهد تا در قبال محتوای مضر، اقدامات قانونی نظیر** حذف محتوا، شفاف‌سازی منابع اطلاعاتی، و مقابله با استفاده از ربات‌ها **انجام دهند.**

ح- «قانون مبارزه با محتوای نفرت‌انگیز در اینترنت، مصوب ۲۰۲۰»؛ **این قانون به‌منظور حذف سریع محتوای نفرت‌انگیز و توهین‌آمیز از فضای دیجیتال تصویب شده است و** سکوهای **برخط را ملزم به حذف محتوای مضر ظرف ۲۴ ساعت می‌کند.** باوجود اهداف امنیتی، قانون با انتقاداتی درباره تهدید به آزادی بیان و حذف یا ویرایش محتوا مواجه شده است.

ج- «**قانون تقویت احترام به جمهوری، مصوب ۲۰۲۱**»؛[3] که به‌طور غیررسمی به‌نام «قانون ضدجدایی‌طلبی» شناخته می‌شود، با هدف مقابله با جدایی‌طلبی و به‌ویژه به‌منظور مقابله با

1. Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037085952
2. LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information (1), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/
3. LOI n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République, https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000042635616/

فعالیت‌های تروریستی و تقویت اصول جمهوری‌خواهی در فرانسه تصویب شده است. این قانون نظارت بر مدارس و مساجد را افزایش داده و به مقامات اجازه می‌دهد محتوای تروریستی برخط را شناسایی و حذف کنند.

چ- «قانون مبارزه با قلدری در مدرسه، مصوب ۲۰۲۲»؛[1] این قانون در راستای پیشگیری از آزار و اذیت برخط و در مقابله با قلدری سایبری در فضای برخط به‌ویژه در شبه‌های اجتماعی مصوب شد و آزار سایبری گروهی و سازمان‌یافته را جرم‌انگاری می‌کند. به‌علاوه، از گروه‌های آسیب‌پذیر نظیر کودکان و افراد دارای معلولیت حمایت می‌کند.

ط- «**قانون مبارزه با تبلیغات تروریستی برخط، مصوب ۲۰۲۲**»؛[2] این قانون در فرانسه به تصویب رسید تا با مقررات اروپایی راجع‌به حذف سریع محتوای تروریستی از اینترنت هم‌پوشانی داشته باشد. قانون، **سکوها و شبکه‌های اجتماعی را موظف به حذف محتوای تروریستی ظرف یک ساعت پس از شناسایی یا گزارش می‌کند.**[3]

ظ- «**قانون** ایمن‌سازی و تنظیم فضای دیجیتال، مصوب ۲۰۲۴»؛[4] این قانون با هدف ارتقای امنیت فضای دیجیتال و مقابله با محتوای تروریستی، چارچوبی حقوقی برای حذف سریع محتوای غیرقانونی، تبیین مسئولیت ارائه‌دهندگان خدمات دیجیتال و صیانت از حقوق بنیادین شهروندان ایجاد می‌نماید. به‌علاوه، بر ضرورت ایجاد توازن میان الزامات امنیتی و حقوق اساسی، تضمین شفافیت فرایندها، تقویت نظارت مؤثر و فراهم‌سازی امکان دسترسی واقعی به مراجع قضائی تأکید دارد.

بااین‌همه، نظام کیفری فرانسه در مواجهه با فعالیت‌های تروریستی برخط، مجموعه‌ای از مقررات خاص را برای حفظ امنیت عمومی، نظم دیجیتال و حقوق بنیادین شهروندان وضع کرده است؛ ازاین‌رو، هرچند «قانون کیفری فرانسه، مصوب ۱۸۱۰» در دوران پیشادیجیتال تدوین شده، اما اصول بنیادین دادرسی کیفری ازجمله اصل قانونی‌بودن جرم و مجازات، اصل برائت، و الزام به دادرسی منصفانه را تبیین

1. LOI n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire (1), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045287658
2. LOI n° 2022-1159 du 16 août 2022 portant diverses dispositions d'adaptation au droit de l'Union européenne ..., https://www.legifrance.gouv.fr/ jorf/id/ JORFTEXT000046186784
۳. این چارچوب قانونی، از تلاش‌های فرانسه برای پیروی از مقررات اروپایی راجع‌به محتوای تروریستی برخط (EU 2021/784)است که سکوهای دیجیتال را ملزم می‌کند تا برای حذف این نوع محتوا سریع عمل کنند؛
- https://www.assemblee-nationale.fr/dyn/16/textes/l16t0007_texte-adopte-seance#
4. LOI n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (1), https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368

نموده که همچنان مبنای تفسیر و اجرای مقررات کیفری نوین در حوزه مقابلـه بـا فعالیت‌هـای تروریسـتی برخط محسوب می‌شود(Cross, 2017: 632). در ضمن، باتوجه به عدم کفایت مقررات سنتی در مواجهـه با چالش‌هـای نـوین فضـای سـایبری، در دهـه‌های اخیـر، مجموعـه‌ای از مقـررات خـاص بـه تصـویب رسیده‌اند. ازجمله، «**قانون ضدتروریسم، مصـوب ۲۰۱۴**»، «قانون مبارزه بـا تروریسـم، مصـوب **۲۰۱۵**» و قانون امنیت داخلی، مصوب **۲۰۱۵**»، و «**قانون مبـارزه بـا تبلیغـات تروریسـتی بـرخط، مصـوب ۲۰۲۲**» کـه همگی به صراحت مصادیق فعالیت‌های تروریستی برخط را جرم‌انگاری کرده‌اند. این مصادیق مشتمل بـر تبلیغ، آموزش، تحریک به ارتکاب عملیات تروریستی، عضویت در گروه‌های تروریستی برخط، و انتشـار محتوای تروریسـتی اسـت. ویژگـی بـارز مقـررات مزبـور، گسـترش دامنـه جرم‌انگـاری بـا بهره‌گیـری از ظرفیت‌های فناوری‌های نوین اطلاعاتی است که امکان اقـدامات پیش‌دسـتانه را بـرای مراجـع قضـائی و امنیتی فراهم می‌سازد(Todorovic, et al., 2021: 607-608).

به‌علاوه نظام حقوقی فرانسه در چارچوب پاسـخ بـه نقـض حقـوق عامـه در فعالیت‌هـای تروریسـتی برخط، نظارت‌های گسترده بدون مجوز قضـائی را نیـز پیش‌بینـی کـرده کـه بـا انتقـادات حقـوقی بـه‌ویژه درخصوص نقض حریم خصوصی و آزادی بیان همراه بوده است. افزون براین، سکوها به‌موجب مقرراتـی نظیر «**قانون** ایمن‌سازی و تنظیم فضای دیجیتـال، مصـوب **۲۰۲۴**»، مکلـف بـه حـذف سـریع محتـوای تروریستی شده‌اند و در صورت قصور، ممکن است با مسئولیت کیفری غیرمستقیم مواجه شوند. به‌علاوه، مقررات مرتبط با حفاظت از داده‌ها و شفافیت فرایندهای نظارتی تصویب شده‌اند تـا اقـدامات امنیتـی بـا اصول حقوق بشری هم‌سو باشد. سیاست‌های مکمل «**قانون تقویت احترام به جمهـوری، مصـوب ۲۰۲۱**» و «قانون مبارزه با قلدری در مدرسه، مصـوب **۲۰۲۲**، بُعـد پیشـگیرانه و حمـایتی پاسـخ کیفـری فرانسـه را تقویت کرده‌اند. با وجود این تلاش‌ها، نگرانی‌هایی جدی درباره نقض آزادی‌های عمومی، حذف محتوای گسترده و عدم نظارت قضائی مؤثر همچنان باقی است و تداوم مشروعیت حقوقی این سیاست‌ها، نیازمنـد نظارت مستقل و تضمین‌های قضائی شفاف است.[1]

به‌طورکلی، تحولات نوین در فعالیت‌های تروریستی، مسائل حقـوقی پیچیـده‌ای در حوزه‌هـایی نظیـر حقوق بشر و صلاحیت قضائی به وجود آورده است.(Seidnaseri, et al., 2024: 15) بنابراین، پاسخ‌گذاری کیفری فرانسه در قبال نقض حقوق عامـه در بسـتر فعالیت‌هـای تروریسـتی بـرخط، مبتنـی بـر ترکیبـی از جرم‌انگاری صریح رفتارهای تروریستی بـرخط، توسـعه صـلاحیت‌های نظـارتی نهادهـای امنیتـی، الـزام سکوها به مداخله فوری در حذف محتوای غیرقانونی و حمایت نهادی و تقنینی از حقـوق کـاربران اسـت. بااین‌وجود تلاش‌ها، چالش‌هایی نظیر تهدید به حریم خصوصی، حذف محتوای گسترده، و اعمال تـدابیر

1 https://knightcolumbia.org/content/the-long-online-shadow-of-the-material-support-law

کیفری بدون نظارت قضائی مؤثر همچنان پابرجاست.[1] تحقق توازن میان امنیت دیجیتالی و حقوق بنیادین، مستلزم تضمین‌های حقوقی و نظارت مستقل از سوی نهادهای قضائی و حقوق بشری است تا پاسخ کیفری فرانسه از مشروعیت و کارآمدی لازم در قبال فعالیت‌های تروریستی برخط برخوردار باشد.

۴-۳. سنجش تطبیقی پاسخ‌گذاری کیفری؛ رویکردی نو به چالش‌ها و توازن میان امنیت و حقوق بشر

همان‌گونه که پیشتر ملاحظه گردید، انگلستان و فرانسه مجموعه‌ای از مقررات را در قبال فعالیت‌های تروریستی برخط برای حمایت از حقوق عامه در بستر دیجیتال (به‌عنوان ابزار اصلی ارتکاب جرم) برای جرم‌انگاری فعالیت‌های تروریستی برخط و تقویت نظارت امنیتی اختصاص وضع کردند؛[2] ازاین‌رو، یکی از چالش‌های اساسی در انگلستان و فرانسه، حفظ تعادل میان تأمین امنیت عمومی و حفاظت از حقوق فردی است. در انگلستان، مقرراتی مانند «قانون اختیارات تحقیق، مصوب ۲۰۱۶» به دولت اجازه می‌دهد تا نظارت‌های گسترده‌ای بر ارتباطات دیجیتال اعمال کند که این امر با نگرانی‌هایی در خصوص نقض حریم خصوصی مواجه است. در فرانسه نیز قوانینی مانند «قانون ضدتروریسم، مصوب ۲۰۱۴» و «قانون امنیت داخلی، مصوب ۲۰۱۵»که به مقامات اجازه نظارت بدون مجوز قضائی می‌دهند، با انتقادات مشابهی روبه‌رو هستند. در هر دو کشور، نگرانی‌های جدی درباره تهدید به حریم خصوصی و حقوق عامه، به‌ویژه در مواجهه با نظارت‌های بی‌ضابطه وجود دارد.[3]

راجع‌به مسئولیت سکوهای دیجیتال در انگلستان و فرانسه در فرایند مقابله با محتوای تروریستی و مضرِ برخط، متمرکز است. در انگلستان، «قانون ایمنی برخط، مصوب ۲۰۲۳» سکوها را ملزم به حذف محتوای مضر می‌کند و برای عدم رعایت این وظیفه، مسئولیت کیفری و مدنی تعیین می‌شود. در فرانسه، «قانون مبارزه با تبلیغات تروریستی برخط، مصوب ۲۰۲۲» سکوها را موظف به حذف محتوای تروریستی ظرف یک ساعت می‌کند. ازاین‌رو، هر دو کشور با نگرانی‌هایی درباره فشار بر سکوها و تهدید به آزادی بیان مواجه هستند که ممکن است منجر به حذف محتوای مشروع شود.

در تدوین مقررات جدید، انگلستان و فرانسه تلاش کرده‌اند تا حقوق بشر و دادرسی منصفانه را حفظ کنند، اما نگرانی‌هایی درباره تعادل میان امنیت و حقوق فردی وجود دارد. در انگلستان، انتقاداتی نسبت به

1. https://jsis.washington.edu/news/french-content-moderation-and-platform-liability-policies/
2. https://www.brookings.edu/articles/dual-use-regulation-managing-hate-and-terrorism-online-before-and-after-section-230-reform/; https://techagainstterrorism.org/news/2020/10/20/the-online-regulation-series-france
3. https://files.justice.org.uk/wp-content/uploads/2023/08/31123029/JUSTICE-The-State-Were-In-Addressing-Threats-Challenges-to-the-Rule-of-Law-September-2023.pdf

گستردگی مقررات مانند «قانون تروریسم، مصوب ۲۰۰۰» و عدم تعریف دقیق مفاهیم همچون «تحریک به تروریسم» مطرح است که ممکن است با اصل قانونی‌بودن جرائم و مجازات‌ها در تضاد باشد. در فرانسه، تصویب قوانین جدید که نظارت‌های بدون مجوز قضائی و حذف سریع محتوای تروریستی را ممکن می‌سازد، ممکن است به تهدید حقوق فردی و آزادی بیان منجر شود.

به‌طورکلی، اگرچه مقررات مصوب در انگلستان و فرانسه درخصوص تهدیدات تروریستی برخط متمرکز هستند، اما در رویکردهای قانونی و نظارتی وجوه افتراقی قابل ملاحظه است؛ براین‌اساس، انگلستان بر حفظ تعادل میان امنیت و حقوق فردی تأکید دارد، در حالی که فرانسه بیشتر به نظارت گسترده و حذف سریع محتوا متمایل است. بااین‌حال، انگلستان و فرانسه با چالش‌هایی نظیر تهدید حقوق عامه، حریم خصوصی و نظارت‌های بی‌ضابطه مواجه‌اند که نیازمند بازنگری از منظر حقوق بشر و دادرسی منصفانه است (Stoykova, 2023: 17-18).

۵. چالش‌ها و پیچیدگی‌های حقوقی در قبال تهدیدات تروریستی برخط؛ توازن میان امنیت و حقوق فردی

چالش‌ها و پیچیدگی‌های حقوقی در مقابله با تهدیدات تروریستی برخط در انگلستان و فرانسه نشان‌دهنده تضاد میان نیاز به حفظ امنیت عمومی و حفظ حقوق فردی است(Beitragsaufruf, 2022: 1). در هر دو کشور، قوانین ضدتروریستی اختیارات گسترده‌ای به مقامات امنیتی می‌دهند تا فعالیت‌های برخط مشکوک را تعقیب کنند، که این شامل نظارت بر ارتباطات الکترونیکی و استفاده از داده‌های اینترنتی برای شناسایی فعالیت‌های تروریستی می‌شود. بااین‌حال، این اقدامات نگرانی‌هایی در خصوص نقض حریم خصوصی و حقوق عامه ایجاد می‌کنند.

در انگلستان، «قانون تروریسم، مصوب ۲۰۰۰» و اصلاحات بعدی آن، به مقامات اجازه می‌دهند که به سرعت واکنش نشان دهند، اما نظارت بی‌رویه ممکن است منجر به سوءاستفاده از داده‌ها و تهدید به نقض حقوق بشر شود. در فرانسه، قوانین مشابه، نظیر «**قانون تقویت احترام به جمهوری، مصوب ۲۰۲۱**»، به مقامات این امکان را می‌دهند که بدون نیاز به مجوز قضائی، ارتباطات برخط را ردیابی کنند، اما این اقدامات ممکن است تهدیداتی برای آزادی بیان و حریم خصوصی ایجاد کنند.

از دیگر چالش‌ها، می‌توان به مشکلات مربوط به تعریف دقیق فعالیت‌های تروریستی برخط، تمایز میان آزادی بیان و ترویج خشونت، و ضرورت همکاری‌های بین‌المللی برای مقابله مؤثر با تهدیدات تروریستی اشاره کرد. به‌طورکلی، تعادل میان حفظ امنیت و رعایت حقوق فردی، به‌ویژه در زمینه حریم خصوصی و آزادی‌های اساسی، یکی از مهم‌ترین چالش‌های حقوقی در این زمینه است.

تهدیدات تروریستی برخط با عبور از مرزهای ملی، شناسایی صلاحیت قضائی را با پیچیدگی‌هایی مواجه

می‌سازد و همکاری‌های بین‌المللی را در زمینه تبادل اطلاعات و جمع‌آوری ادله دیجیتال، به‌ویژه در حوزه حریم خصوصی، با موانع حقوقی روبه‌رو می‌کند. اگرچه قوانین ضدتروریستی در انگلستان و فرانسه امکان تعقیب و نظارت فرامرزی را فراهم می‌آورند، اما در مواردی با الزامات اسناد بین‌المللی حقوق بشر در تعارض قرار می‌گیرند. ازاین‌رو، اصلاح و روزآمدی چارچوب‌های حقوقی بین‌المللی، همراه با تقویت همکاری‌های فراملی بر مبنای اصول حقوق بشر، امری ضروری است(Cross, 2017: 621).

از سوی دیگر، تعریف و شمول فعالیت‌های تروریستی برخط یکی از چالش‌های اساسی در تدوین و اجرای قوانین مرتبط محسوب می‌شود. در انگلستان و فرانسه، باتوجه به گستردگی قوانین ضدتروریستی، مرز میان افکار افراطی، آزادی بیان و فعالیت‌های تروریستی به‌وضوح مشخص نیست؛ موضوعی که می‌تواند منجر به محدودیت‌های غیرمعقول در آزادی بیان شود(Binder & Kenyon, 2022: 6). شمول این جرایم در نظام حقوق دیجیتال انگلستان و فرانسه، که به نهادهای امنیتی امکان نظارت گسترده در فضای مجازی را می‌دهد، خطر تهدید آزادی‌های مدنی و حقوق فردی، به‌ویژه حریم خصوصی را افزایش می‌دهد. تنوع در تعاریف و اختلافات میان قوانین داخلی و استانداردهای بین‌المللی حقوق بشر نیز اجرای مؤثر این قوانین را دشوارتر می‌سازد(Sun, 2023: 496).

حفظ تعادل میان امنیت ملی و حقوق عامه ازجمله چالش‌های محوری در این حوزه است. اختیارات گسترده نظارتی در نظام حقوق دیجیتال انگلستان و فرانسه، گرچه به‌منظور مقابله با تهدیدات تروریستی اعطا شده‌اند، در مواردی با اصول بنیادین حقوق بشر، ازجمله حق آزادی بیان و حق بر حریم خصوصی، در تعارض قرار می‌گیرند. افزون‌برآن، همکاری‌های بین‌المللی برای مقابله با این تهدیدات نیز با چالش‌هایی مانند تفاوت در رژیم‌های حقوقی ملی، به‌ویژه در حوزه حفاظت از داده‌ها، روبه‌رو است. درنتیجه، بازنگری در قوانین ملی و بین‌المللی و ارتقای سازوکارهای هماهنگی میان کشورها، ضرورتی اجتناب‌ناپذیر تلقی می‌شود(Wei, 2024: 9).

دسترسی به شواهد دیجیتال نیز با موانع حقوقی متعدد همراه است. در بسیاری از موارد، جمع‌آوری اطلاعات بدون اخذ مجوز قضائی، ناقض حریم خصوصی افراد تلقی می‌گردد و مشروعیت ادله را با تردید مواجه می‌سازد.[1] این وضعیت، لزوم تدوین قواعد شفاف، منطبق با استانداردهای بین‌المللی حقوق بشر و با تأکید بر همکاری‌های قضائی فراملی را آشکار می‌سازد.[2] افزون‌براین، محدودیت‌های فناوری نیز مانع جدی در کارآمدی سیاست‌های مقابله با فعالیت‌های تروریستی برخط است. رمزنگاری اطلاعات، عدم دسترسی

1. https://www.unesco.org/en/preventing-violent-extremism
2. https://conflictoflaws.net/2024/transforming-legal-borders-international - judicial - cooperation-and-technology-in-private-international-law-part-ii/

بـه داده‌هـای ذخیره‌شـده در خـارج از قلمـرو سـرزمینی، و کاسـتی‌های الگوریتم‌هـای شناسـایی محتـوای تروریستی، موجب کـاهش اثربخشـی ابزارهـای نظـارتی شـده‌اند. ازایـن‌رو، توسـعه فناوری‌هـای دقیـق‌تر و بـازنگری در چارچوب‌هـای قـانونی بـرای تضـمین حقـوق کـاربران در برابـر مـداخلات فناورانـه ضـروری است(Luk, 2024: 152).

درنهایت، آموزش و ارتقای آگاهی عمومی نقش محوری در پیشگیری از گسترش افراط‌گرایـی بـرخط دارد. در انگلستان و فرانسه، آموزش سواد رسانه‌ای و نحوه شناسایی محتوای افراطـی ازجملـه راهکارهـای مکمل قوانین کیفری به‌شمار می‌رود. این آموزش‌ها باید بـه گونـه‌ای طراحـی شـوند کـه ضـمن مقابلـه بـا افراط‌گرایـی، آزادی بیـان را نیـز محتـرم بشـمارند. اطلاع‌رسـانی شـفاف در مـورد حقـوق شـهروندان و سازوکارهای نظارتی می‌تواند اعتماد عمومی را افزایش دهـد. بـااین‌حـال، برخـی برنامـه‌های آموزشـی بـا سوءبرداشت‌ها و مقاومت اجتماعی مواجه‌انـد. موفقیـت در ایـن حـوزه مسـتلزم همکـاری میـان دولـت، نهادهای آموزشی، رسانه‌ها و شرکت‌های فناوری، در چارچوب اصول حقوق بشری و با رویکردی شـفاف و مشارکتی است (Svennevig, et al., 2021: 96-97) .

نتیجه‌گیری

یافته‌های پژوهشی در تحلیل تطبیقی پاسخ کیفری به فعالیت‌های تروریستی برخط در انگلستان و فرانسـه نشان می‌دهد که ایجاد تعادل میان حفظ امنیت ملی و رعایت حقوق عمومی، چالشـی عمـده اسـت. قـوانین ضدتروریستی هر دو کشور به نهادهای امنیتی اختیارات وسیعی برای نظارت دیجیتال اعطا کرده‌انـد، امـا ایـن اقدامات با نگرانی‌هایی درباره نقض آزادی بیان و حریم خصوصی همراه بوده است. تعیین مرز دقیق بین بیـان افراطی و اقدامات تروریستی در فضای برخط امری پیچیده است و ممکن اسـت بـه اعمـال محـدودیت‌های غیرضروری بر آزادی بیان منجر شود. تفاوت‌های موجود در قوانین ملی پیرامون حـریم خصوصـی و نظـارت دیجیتال، همکاری‌های بین‌المللی و دسترسی به شواهد دیجیتال را با موانع جدی مواجه کرده است. بنـابراین، اصلاح و بازنگری قوانین ضدتروریستی و ایجاد شفافیت بیشتر در فرایندهای اجرایی ضـروری اسـت تـا ایـن قوانین بتوانند ضمن مقابله مؤثر با افراط‌گرایی برخط، از نقـض حقـوق بشـر و آزادی‌هـای بنیـادی پیشـگیری کنند. این اصلاحات باید مطابق با استانداردهای بین‌المللـی حقـوق بشـر انجـام شـود و هـدف آن مـدیریت متناسب تهدیدات تروریستی در فضای دیجیتـال باشـد. بـه‌علاوه، تقویـت همکـاری‌هـای فراملـی و تـدوین استانداردهای مشترک در زمینه نظـارت دیجیتـال و حفاظـت از داده‌هـای شخصـی از الزامـات اصـلی بـرای افزایش اثربخشی در مقابله با فعالیت‌های تروریستی برخط است.

در همین راستا، انگلستان با اتکاء به مقرراتی نظیـر «قـانون تروریسـم، مصـوب ۲۰۰۰» و فرانسـه بـا بهره‌گیری از «قانون ضدجدایی‌طلبی، مصوب ۲۰۲۱»، چارچوب‌هایی قانونی برای مقابله بـا فعالیت‌هـای

تروریستی برخط ایجاد کرده‌اند که به مقامات صلاحیت‌های گسترده‌ای برای نظارت بر ارتباطات دیجیتال اعطا می‌کند. هر دو کشور از فناوری‌های نوین نظیر هوش مصنوعی و ابزارهای تحلیل داده به‌منظور شناسایی محتوای تروریستی استفاده می‌کنند. بااین‌وجود، تأمین هم‌زمان امنیت ملی و تضمین حقوق فردی همچنان از چالش‌های جدی این نظام‌های حقوقی است و نیاز به هماهنگی‌های بیشتر در سطح بین‌المللی برای حفظ تعادل میان امنیت و آزادی‌های بنیادین به‌شدت احساس می‌شود.

به‌هرروی، برای بهبود پاسخ‌گذاری به نقض حقوق عامه از طریق فعالیت‌های تروریستی برخط و حفظ حقوق بشر در چارچوب نظام حقوق دیجیتالی انگلستان و فرانسه، پیشنهادهای زیر قابل ملاحظه است:

الف- ضروری است که قوانین ضدتروریستی بازنگری شوند تا علاوه بر نظارت کارآمد بر فعالیت‌های تروریستی، از تهدید آزادی بیان و حریم خصوصی افراد پیشگیری شود. به‌علاوه، باید تمایز واضحی بین آزادی بیان افراطی و اقدامات تروریستی ایجاد گردد؛

ب- نهادهای نظارتی باید کاملاً مستقل از نهادهای امنیتی عمل کنند تا در صورت نیاز، اقدامات مقابله با تروریسم را بررسی کرده و از نقض حقوق فردی پیشگیری کنند؛

ج- تدوین استانداردهای بین‌المللی برای نظارت بر ارتباطات دیجیتال و حفاظت از داده‌های شخصی می‌تواند به تسهیل همکاری‌های جهانی و مقابله مؤثر با تروریسم دیجیتال کمک کند؛

د- استفاده از فناوری‌های پیشرفته، نظیر هوش مصنوعی، برای شناسایی محتوای تروریستی باید مطابق با اصول حقوق بشر و قوانین شفاف و مسئولانه انجام شود؛

هـ- همکاری‌های بین‌المللی در نظارت بر فعالیت‌های تروریستی و دسترسی به شواهد دیجیتال باید تقویت شده و استانداردهای مشترک در این حوزه تدوین و به‌طور مؤثر اجرا گردد؛

ر- آموزش و توانمندسازی مقامات قضائی و انتظامی: مقامات قضائی و انتظامی باید به‌طور مداوم در زمینه اصول نظارت دیجیتال و حقوق بشر آموزش ببینند و با تحولات جدید در فناوری و شیوه‌های مقابله با جرایم آشنا شوند؛

ز- تعریف دقیق‌تر مفاهیم نقض حقوق عمومی در فضای دیجیتال: مفاهیم مربوط به فعالیت‌های تروریستی برخط و نقض حقوق عمومی باید به‌طور دقیق و شفاف‌تری تعریف شوند تا از سوءاستفاده‌های احتمالی در اجرای قانون برخط گردد.

بااین‌همه، برای دستیابی به توازن مناسب میان تأمین امنیت ملی و حفظ حقوق فردی، نیاز به اصلاحات بنیادین در قوانین و فرایندهای اجرایی است تا از یک‌سو تهدیدات تروریستی برخط تحت کنترل قرار گیرد و از سوی دیگر، حقوق بشر به‌طور مؤثر حفظ گردد.

منابع

منابع فارسی

- احمدی‌مقدم، جواد، غلامی‌دون، حسین. (۱۳۹۶). تروریسم سایبری: ماهیت، روش‌ها و تدابیر مقابله. کنفرانس بین‌المللی ابعاد حقوقی-جرم‌شناختی تروریسم. چاپ اول، تهران: دانشگاه علامه طباطبایی.
- کازرونی، سیدمصطفی. (۱۳۹۵). چالش تطبیق حق آزادی بیان با ممنوعیت استفاده از فضای سایبر توسط تروریسم. مطالعات بین‌المللی، ۱۲(۴)، ۱۶۷-۱۹۸.
- سیدناصری، محمدمهدی، میربد، لیلا. (۱۴۰۳). تروریسم و افراط‌گرایی سایبری-تکنولوژیک: چالش‌های حقوقی و امنیتی برای نظام حقوقی بین‌المللی. رویکردهای حقوق سیاسی ، ۲(۱)، ۱۵-۲۷. https://doi.org/10.22084/qjpla.2025.30336.1008
- ظهیری، صمد. (۱۳۹۷). جامعه شبکه‌ای و تروریسم مجازی. سیاست، ۴۸(۲)، ۴۱۳-۴۳۱.

منابع انگلیسی

- Ahmadi Moghadam, Javad, Gholami Doun, Hossein. (2017). Cyber Terrorism: Nature, Methods, and Countermeasures. International Conference on the Legal-Criminological Dimensions of Terrorism. First Edition, Tehran: Allameh Tabatabai University (In Persian).
- Ayepeku, Olukayode Felix, Olabode, Omosola, Ayeni, James K. (2024). The criminalization of the internet and cybercrime in general: A comprehensive study. Scientific and Practical Cyber Security Journal, 7(3), 1-10.
- Banchio, Pablo Rafael. (2024). Legal framework to combat disinformation and hate speech on digital platforms (pp. 1-37). SSRN. https://ssrn.com/abstract=4879162. http://dx.doi.org/10.2139/ssrn.4879162
- Beitragsaufruf. (2022). Digital justice and criminal proceedings in France and the United Kingdom: The impact of new technologies on fundamental rights in light of domestic and European laws. Calenda. (January 19). https://calenda.org/956558?formatage=print&lang=de. DOI: https://doi.org/10.58079/182n
- Binder, Jens F., Kenyon, Jonathan J. (2022). Terrorism and the internet: How dangerous is online radicalization? Frontiers in Psychology, 6(3), 1-10. DOI: https://doi.org/10.3389/fpsyg.2022.997390
- Blin, Arnaud, Chaliand, Gérard. (2016). The history of terrorism: From antiquity to ISIS (1st ed.). University of California Press.
- Caruso, Corrado. (2025). Towards the institutions of freedom: The European public discourse in the digital era. German Law Journal, 26(1), 114–137. DOI: https://doi.org/10.1017/glj.2024.68
- Chaliand, Gérard, Blin, Arnaud. (2016). The history of terrorism: From antiquity to ISIS (1st ed.). University of California Press.
- Coe, Peter. (2023). Tackling online false information in the United Kingdom: The Online Safety Act 2023 and its disconnection from free speech law and theory. Journal of Media Law, 15(2), 213-242. DOI: https://doi.org/10.1080/17577632.2024.2316360

- Cross, Cassandra. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. Journal of Criminological Research, Policy and Practice, 5(4), 120–131. DOI: https://doi.org/10.1108/JCRPP-01-2019-0008
- Cross, Jennifer. (2017). Cybersecurity and the rights of the internet user in France. Georgia Journal of International & Comparative Law, 45(2), 609–643.
- Farrand, Benjamin. (2024). How do we understand online harms? The impact of conceptual divides on regulatory divergence between the Online Safety Act and Digital Services Act. Journal of Media Law, 16(2), 240-262. DOI: https://doi.org/10.1080/17577632.2024.2357463
- Kazerooni, Seyed Mostafa. (2016). The Challenge of Reconciling the Right to Freedom of Expression with the Prohibition of Terrorism's Use of Cyberspace. International Studies, 12(4), 167-198 (In Persian).
- Lucchi, N. (2011). Access to network services and protection of constitutional rights: Recognizing the essential role of internet access for the freedom of expression. Cardozo Journal of International and Comparative Law, 19(3), 1-35.
- Luk, Ann. (2024). The relationship between law and technology: Comparing legal responses to creators' rights under copyright law through safe harbour for online intermediaries and generative AI technology. Law, Innovation and Technology, 16(1), 148-169. DOI: https://doi.org/10.1080/17579961.2024.2313800
- Macdonald, Stuart, Correia, Sara Giro, Watkin, Amy-Louise. (2019). Regulating terrorist content on social media: Automation and the rule of law. International Journal of Law in Context, 15(2), 183–197. DOI: https://doi.org/10.1017/S1744552319000119
- Moslemzadeh Tehrani, Pardis, Abdul Manaph, Nazura Taji, Hossein. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. Computer Law & Security Review, 29(3), 207–215. DOI: https://doi.org/10.1016/j.clsr.2013.03.011
- Ralstin, Grace. (2024). The rise of ISIS: A growing threat to the world. Pepperdine Policy Review, 16(8), 1–30.
- Sander, Barrie. (2021). Democratic disruption in the age of social media: Between marketized and structural conceptions of human rights law. European Journal of International Law, 32(1), 159–193. DOI: https://doi.org/10.1093/ejil/chab022
- Schmitt, Michael N. (2014). The law of cyber warfare: Quo vadis? Stanford Law & Policy Review, 25(4), 269-299. DOI: https://ssrn.com/abstract=2320755
- Siagian, Riduan, Siahaan, Leonard, Ichwan, Hamzah. (2023). Human rights in the digital era: Online privacy, freedom of speech, and personal data protection. Journal of Digital Learning and Distance Education, 2(4), 513-523. DOI: https://doi.org/10.56778/jdlde.v2i4.149
- Seidnaseri, Mohammad Mahdi, Mirbad, Leila. (2024). Cyber-Technological Terrorism and Extremism: Legal and Security Challenges for the International Legal System. Journal of Political Legal Approaches, 2(1), 15-27 (In Persian). DOI: https://doi.org/10.22084/qjpla.2025.30336.1008
- Slaughter, Autumn, Newman, Elana. (2022). New frontiers: Moving beyond cyberbullying to define online harassment. Journal of Online Trust and Safety, 1(2), 1-25. DOI: https://doi.org/10.54501/jots.v1i2.5
- Stoykova, R. (2023). The right to a fair trial as a conceptual framework for digital

evidence rules in criminal investigations. Computer Law & Security Review, 49(4), 1-28. DOI: https://doi.org/10.1016/j.clsr.2023.105801

- Sun, Qixuan. (2023). The enforcement of international human rights law: Challenges and solutions. Journal of Education Humanities and Social Sciences, 8(3), 491-498. DOI: https://doi.org/10.54097/ehss.v8i.4295
- Svennevig, Hans, Jerome, Lee, Elwick, Alex. (2021). Countering violent extremism in education: A human rights analysis. Human Rights Education Review, 4(1), 91-110. DOI: https://doi.org/10.7577/hrer.3980
- Tsesis, Alexander. (2017). Social media accountability for terrorist propaganda. Fordham Law Review, 86(2), 605–631. DOI: https://ssrn.com/abstract=3047868
- Todorovic, Branislav., Trifunovic, Darko. (2021). Prevention of (ab-)use of the internet for terrorist plotting and related purposes. In A. P. Schmid (Ed.), Handbook of terrorism prevention and preparedness (pp. 594–618). The International Centre for Counter-Terrorism Press.
- Wei, Xingxing. (2024). Rule of law or not? A critical evaluation of legal responses to cyberterrorism in the UK. Computer Law & Security Review, 53(3), 1-11. DOI: https://doi.org/10.1016/j.clsr.2024.105951
- White, Jessica. (2020). Terrorism and the mass media (RUSI Occasional Paper). Royal United Services Institute for Defence and Security Studies.
- Zahiri, Samad. (2018). The Networked Society and Virtual Terrorism. Politics, 48(2), 413-431 (In Persian).
- Zeiger, Sara, Gyte, Joseph. (2021). Prevention of radicalization on social media and the Internet. In A. P. Schmid (Ed.), Handbook of terrorism prevention and preparedness (pp. 358–395). The International Centre for Counter-Terrorism Press.