JOURNAL OF CYBER LAW
نشریه حقوق سایبری

Received: 16 /11/2025
Review: 21/11/2025
Accepted: 03 /12/2025
DOI: 10.22054/jocl.2025.8563. 29553

Journal of Cyber Law
No(3),Vol(2), 1-19.
ISSN: 0972-6934
www.jocl.ir

Human Rights Considerations of Global Organizations and Institutions in Countering Terrorist Activities Carried out on Digital Platforms

Peyman Namamian [1*]

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

ABSTRACT

In recent years, the development of digital technologies and the expansion of communication networks have introduced a new threat to international security under the term "digital terrorism." This threat includes the production and dissemination of extremist content, organizing violent operations, targeting critical infrastructures, and manipulating information. The transnational and complex nature of this phenomenon has limited the ability of individual countries to address it independently, highlighting the need for international cooperation and the role of global organizations, particularly the United Nations. Through the development of global frameworks and standards, the UN seeks to enhance the security of digital platforms while ensuring human rights and fundamental freedoms. Striking a balance between security and individual freedoms is crucial, as excessive restrictions on freedoms could pave the way for "digital authoritarianism." Adherence to the principles of necessity, proportionality, and non-discrimination, along with the protection of freedom of expression, privacy, and free access to information, not only preserves individual rights but also increases the effectiveness of security policies. Cooperation between governments and regional organizations such as the European Union strengthens the fight against digital threats, but the lack of a common definition and differences in data access pose challenges to global coordination. The UN, drawing on international documents and collaborating with agencies such as Interpol and Europol, ensures digital security, applying transparency, a clear legal framework, and judicial oversight as key principles.

Keywords:
Digital Terrorism, International Cybersecurity, Human Rights and Fundamental Freedoms, Digital Security Policies, Digital Authoritarianism.

Article type:Research Article

How to Cite: Namamian,P. (2025). Human Rights Considerations of Global Organizations and Institutions in Countering Terrorist Activities Carried out on Digital Platforms. *Journal of Cyber Law (JOCL)*, 2(3),1-19. doi: 10.22054/jocl.2025.8563.29553

Journal of Cyber Lawin Development and Evolution is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.

© Authors

* Corresponding Author:p_namamian1512@yahoo.com

JOURNAL OF CYBER LAW
نشریه حقوق سایبری

نشریه حقوق سایبری
شماره (۳) ۱۹-۱
دوره ۱۴۰۴

تاریخ دریافت: ۱۴۰۴/۰۸/۲۵
تاریخ اصلاح: ۱۴۰۴/۰۸/۳۰
تاریخ پذیرش: ۱۴۰۴/۰۹/۱۲

ملاحظات حقوق بشری سازمان‌ها و نهادهای جهانی برای مقابله با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی

پیمان نمامیان [1*]

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

چکیده

در سال‌های اخیر، توسعه فناوری‌های دیجیتال و گسترش شبکه‌های ارتباطی، تهدید تازه‌ای تحت عنوان «تروریسم دیجیتال» را به عرصه امنیت بین‌المللی وارد کرده است. این تهدید شامل تولید و انتشار محتوای افراطی، سازماندهی عملیات خشونت‌آمیز، هدف قرار دادن زیرساخت‌های حیاتی و دستکاری اطلاعات می‌شود. ماهیت فرامرزی و پیچیده این پدیده، توانایی مقابله مستقل هر کشور را محدود ساخته و ضرورت همکاری بین‌المللی و نقش سازمان‌های جهانی، به‌ویژه سازمان ملل متحد، را برجسته کرده است. سازمان ملل با تدوین چارچوب‌ها و استانداردهای جهانی، تلاش می‌کند امنیت سکوهای دیجیتالی را تقویت و حقوق بشر و آزادی‌های بنیادین را تضمین کند. برقراری توازن میان امنیت و آزادی‌های فردی اهمیت ویژه‌ای دارد، زیرا محدودسازی بی‌رویه آزادی‌ها می‌تواند زمینه «اقتدارگرایی دیجیتالی» را فراهم آورد. رعایت اصول ضرورت، تناسب و عدم تبعیض، همراه با حفاظت از آزادی بیان، حریم خصوصی و دسترسی آزاد به اطلاعات، هم حقوق فردی را حفظ کرده و هم کارآمدی سیاست‌های امنیتی را افزایش می‌دهد. همکاری میان دولت‌ها و سازمان‌های منطقه‌ای مانند اتحادیه اروپا مقابله با تهدیدات دیجیتال را تقویت می‌کند، اما فقدان تعریف مشترک و افتراق در دسترسی به داده‌ها هماهنگی جهانی را با چالش مواجه می‌سازد. سازمان ملل متحد با استناد به اسناد بین‌المللی و همکاری با نهادهایی مانند اینترپل و یوروپل، امنیت دیجیتال را تضمین و شفافیت، چارچوب قانونی مشخص و نظارت قضایی را به‌عنوان اصول اساسی اعمال می‌کند.

کلیدواژه‌ها:

تروریسم دیجیتال، امنیت دیجیتالی بین‌المللی، حقوق بشر و آزادی‌های بنیادین، سیاست‌های امنیت دیجیتال، اقتدارگرایی دیجیتالی.

نوع **مقاله** : **پژوهشی**

نحوه استناد:

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

نشریه حقوق سایبری در توسعه و تکامل تحت مجوز کریتیو کامنز انتساب – غیرتجاری ۴,۰ بین‌المللی منتشر شده است.

©نویسندگان

* ایمیل نویسنده مسئول: p_namamian1512@yahoo.com

۱. مقدمه

در عصر گسترش فناوری‌های دیجیتال و شبکه‌های ارتباطی، امنیت بین‌المللی با تهدیدهای جدیدی مواجه شده که برجسته‌ترین آن «تروریسم دیجیتال» یا فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی است. این پدیده شامل فعالیت‌هایی مانند انتشار محتوای افراطی، سازمان‌دهی حملات خشونت‌آمیز، حمله به زیرساخت‌های حیاتی و دستکاری داده‌ها می‌شود(ر.ک: میردامادی‌اصل، ۱۴۰۴: ۸۹-۸۸). ماهیت فرامرزی و پیچیده این تهدید، مقابله یک‌جانبه دولت‌ها را دشوار کرده و ضرورت همکاری بین‌المللی، به‌ویژه نقش سازمان ملل متحد در تدوین چارچوب‌ها و استانداردهای جهانی، را افزایش داده است. سازمان ملل متحد با هدف هم تضمین امنیت دیجیتال و هم حفاظت از حقوق بشر، اقدامات متعددی از جمله تدوین راهبردها، قطعنامه‌های شورای امنیت و استانداردهای جهانی را پیش برده است.

این پدیده نخستین بار توسط بری کالین در دهه ۱۹۸۰ معرفی شد و به حملات دیجیتال برنامه‌ریزی شده‌ای اشاره دارد که با انگیزه‌های سیاسی علیه اطلاعات، سامانه‌ها و داده‌های حساس انجام می‌شود(Pollitt, 1997: 285). این حملات می‌توانند تأثیرات گسترده‌ای بر زیرساخت‌های حیاتی مانند برق، آب و اقتصاد کشورها داشته باشند. تروریسم دیجیتالی به‌طور کلی شامل فعالیت‌هایی مانند هک کردن، آلوده‌سازی سامانه‌های رایانه‌ای و تحدید دسترسی به منابع دیجیتال با هدف آسیب رساندن به امنیت کشور و تهدید روابط بین‌المللی است. فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی به حملات عمدی با انگیزه‌های سیاسی اطلاق می‌شود که از ابزارهای الکترونیکی برای تأثیرگذاری بر تصمیمات دولتی و افکار عمومی استفاده می‌کند. این نوع بزهکاری با هدف ایجاد ترس و تأثیرگذاری روانی از طریق رسانه‌های دیجیتال و سلاح‌های الکترونیکی در فضای مجازی صورت می‌گیرد. دو دسته‌بندی اصلی برای این بزهکاری وجود دارد: اول، بر اساس آثار آن که حملات دیجیتالی باید مخرب و ترس‌آفرین باشند؛ دوم، بر اساس هدف که در آن حملات برای وادار کردن دولت‌ها به تغییر تصمیمات سیاسی یا آسیب رساندن به زیرساخت‌های اقتصادی انجام می‌شود(Jian & Sanjay, 2012: 108).

این نوع فعالیت‌ها با استفاده از ابزارهای دیجیتال، رسانه‌های اجتماعی و فناوری‌های نوین برای ایجاد ترس، نفرت و اختلال در تصمیمات سیاسی و اجتماعی طراحی می‌شوند. به‌ویژه در عرصه حقوق بین‌الملل، مسأله استفاده تروریست‌ها از اینترنت برای تبلیغات، جذب نیرو و تأمین مالی مورد توجه قرار گرفته است. لازم به‌ذکر است «گروه ویژه اقدام مالی» در پاسخ به تهدیدات تروریستی در سکوهای دیجیتالی و ارزهای مجازی سه توصیه اصلی دارد؛ نخست، رعایت حقوق بشر و پیشگیری از نظارت‌های بی‌مورد بر کاربران. دوم، تقویت نظارت بر سکوهای دیجیتال و الزام صرافی‌ها به رعایت قوانین ضدپول‌شویی. سوم، افزایش شفافیت تراکنش‌ها از طریق شناسایی هویت کاربران. این در حالی است که گروه ویژه، بر اهمیت همکاری‌های بین‌المللی و آموزش نهادهای نظارتی برای پیشگیری از سوءاستفاده از سکوهای دیجیتالی تأکید می‌کند(Packin & Volovelsky, 2024: 83-89). با این حال، فقدان چارچوب قانونی قوی و اجماع جهانی در حمایت از مقابله با این جرایم باعث شده است که دولت‌ها نتوانند به‌طور مؤثر در قبال این تهدیدات واکنش نشان دهند. از سوی دیگر، استفاده از رسانه‌های اجتماعی برای ارتکاب فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی، در چارچوب حقوق بین‌الملل کیفری به‌عنوان یک جرم جنگی مستقل محسوب نمی‌شود، اما هنوز به‌عنوان یک تهدید اساسی نیازمند توجه ویژه است. در نهایت، این بزهکاری‌ها بدون اصلاحیه‌های قانونی لازم در دیوان کیفری بین‌المللی، از طریق محاکم ملی تعقیب خواهند شد(Syihabudin, 2022: 108).

مقابله با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی با چالش‌های متعدد در ابعاد مختلف مواجه است. از جنبه حاکمیتی، دولت‌ها با مشکلاتی همچون محدودیت‌های جغرافیایی در فضای دیجیتال و تهدیدات فرامرزی مواجه‌اند که این موضوع می‌تواند موجب تنش‌ها و تضادهایی میان حاکمیت‌های ملی و نظارت‌های بین‌المللی گردد. از نظر حقوقی، عدم وجود چارچوب‌های یکپارچه و هماهنگ برای تعریف و مقابله با چنین فعالیت‌هایی، مانع از اتخاذ اقدامات مؤثر در سطح جهانی می‌شود. در بُعد اجتماعی، فضای دیجیتال به ابزاری برای جذب افراد به گروه‌های تروریستی تبدیل شده است که می‌تواند موجب رادیکالیزه شدن افراد، به‌ویژه جوانان و آسیب‌پذیران، گردد. علاوه بر این، نابرابری‌های دیجیتال در دسترسی به فناوری در برخی مناطق، توانایی مقابله مؤثر با تهدیدات تروریستی را محدود می‌سازد. از منظر روانی، انتشار محتوای تروریستی و خشونت‌آمیز در فضای دیجیتال می‌تواند بر روحیه جامعه تأثیرات منفی به‌جا بگذارد و موجب افزایش اضطراب و ترس در افراد گردد. همچنین، تهدیدات دیجیتالی از سوی گروه‌های تروریستی که از شبکه‌های رمزنگاری‌شده استفاده می‌کنند، چالش‌های امنیتی جدیدی به‌وجود می‌آورد. در ضمن، ملاحظات حقوق بشری در مقابله با فعالیت‌های تروریستی در سکوهای دیجیتالی نیازمند توازن دقیق میان حفظ امنیت و رعایت حقوق فردی است تا از نقض اصول حقوق بشر پیشگیری شود. این توازن باید در چارچوب اصول حقوق بشری و استانداردهای بین‌المللی برای مقابله با این پدیده لحاظ گردد.

در سطح جهانی، تلاش‌های حقوقی و منطقه‌ای برای تقویت هماهنگی در مقابله با تهدیدات دیجیتال در حال شکل‌گیری است، اما نبود تعریف یکسان از فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی و اختلافات میان دولت‌ها و شرکت‌های فناوری در خصوص دسترسی به داده‌ها، مانع از همگرایی کامل می‌شود. مقابله مؤثر نیازمند همکاری بین‌المللی، شفافیت در مقررات، احترام به آزادی‌های فردی و استفاده از نوآوری‌های حقوقی و فناوری است تا اعتماد عمومی به اقدامات امنیتی تقویت شود.

پژوهش حاضر درصدد پاسخ به این پرسش است که چگونه چارچوب‌ها و رویه‌های بین‌المللی حقوق بشری در سازمان‌ها و نهادهای جهانی می‌توانند امنیت دیجیتال را در مقابله با جرائم و تهدیدات دیجیتالی تأمین کرده و همزمان حقوق بشر و آزادی‌های اساسی را تضمین کنند. به این منظور، با بهره‌گیری از روش تحلیل اسنادی و محتوایی، اسناد، کنوانسیون‌ها و قطعنامه‌های سازمان ملل متحد و سایر نهادهای بین‌المللی مرتبط مورد بررسی قرار گرفته‌اند. در چارچوب تحلیل حقوقی، سیاست‌ها و استانداردهای سازمان‌های جهانی و منطقه‌ای، از جمله اتحادیه اروپا، در مواجهه با تهدیدات دیجیتال و رعایت حقوق بشر مقایسه شده است. رویکرد تحلیلی-توصیفی این پژوهش، تضادهای احتمالی میان امنیت دیجیتال و آزادی‌های فردی را شناسایی کرده و خطرات اقتدارگرایی دیجیتال را مورد ارزیابی قرار می‌دهد. یافته‌های این پژوهش حاکی از آن است که چارچوب‌های بین‌المللی، با رعایت اصول ضرورت، تناسب و عدم تبعیض، امکان مقابله مؤثر با تهدیدات دیجیتالی را فراهم می‌آورند؛ با این حال، محدودیت‌های ناشی از همکاری بین‌المللی و هماهنگی سیاست‌ها همچنان چالش‌هایی بر جای می‌گذارند.

۱. چالش‌های فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی و نقش سازمان ملل متحد و نهادهای وابسته در قبال تهدیدات دیجیتالی جهانی

با رشد فناوری‌های دیجیتال، تهدیدات نوینی در سکوهای برخط ظهور کرده‌اند که هم امنیت جهانی و هم حریم خصوصی افراد را به چالش می‌کشند. این تهدیدات شامل انتشار محتوای افراطی، حملات سایبری و نفوذ به داده‌های

حساس هستند و اغلب ابعادی فرامرزی دارند. فعالیت‌های تروریستی در سکوهای دیجیتالی با اهدافی مانند ترویج خشونت، هماهنگی حملات و آسیب به زیرساخت‌ها انجام می‌شوند. مقابله با این تهدیدات به دلیل ناشناسی هویت‌ها و پیچیدگی موازین بین‌المللی دشوار بوده و نیازمند اقداماتی است که هم امنیت و هم حقوق بشر را حفظ کند.

به‌عنوان نمونه، در سال‌های اخیر، مراجع حقوق بشری بین‌المللی راجع‌به نظارت دیجیتال و شواهد ضدتروریستی آرای قابل توجهی صادر کرده‌اند. در پرونده «یوکسل یالچینکایا» علیه ترکیه طی سال ۲۰۲۳، دیوان اروپایی حقوق بشر استفاده از پیام‌رسان «بای‌لاک» به‌عنوان مدرک برای محکومیت عضویت در گروه‌های تروریستی را نقض حق دادرسی عادلانه و آزادی تجمع دانست و خواستار اصلاح شیوه‌های جمع‌آوری و تحلیل شواهد دیجیتال در ترکیه شد (European Court of Human Rights, 2023). در سطح جهانی، گزارشگران ویژه سازمان ملل متحد به مسائل نظارت الکترونیکی، استفاده از پهپادها در عملیات ضدتروریستی و سایر مسائل حقوق بشری پرداخته‌اند(www.ohchr.org/en/special-procedures/sr-terrorism). علاوه بر این، در اتحادیه اروپا، دستورالعمل ۵۴۱/۲۰۱۷ و نقدهای جامعه مدنی بر نگرانی‌ها در خصوص نقض حقوق بشر در اقدامات ضدتروریستی تأکید دارند(www.opensocietyfoundations.org).

مقابله مؤثر با این تهدیدات تنها در چارچوب قوانین ملی ممکن نیست، به همین دلیل سازمان ملل متحد نقش مهمی در تدوین استراتژی‌های بین‌المللی ایفا می‌کند. همکاری‌های جهانی از طریق نهادهایی مانند اتحادیه اروپا و کنوانسیون بوداپست نیز برای تضمین امنیت دیجیتال و حفظ حقوق بشر ضروری است. مسئولیت نظارت بر محتوای تروریستی به‌طور عمده بر عهده شرکت‌های فناوری است که به دلیل حجم بالای داده‌ها، قادر به مدیریت دقیق آن‌ها نیستند.

۱-۱. نقش سازمان ملل متحد در توازن‌بخشی میان امنیت دیجیتالی و حقوق بشر

رشد سریع فناوری‌های ارتباطی و گسترش فضای دیجیتال، تهدیدات جدیدی مانند فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی را به وجود آورده است. این تهدید با استفاده از شبکه‌های اجتماعی و فناوری‌های نوظهور، امنیت داخلی و بین‌المللی را به چالش کشیده و شناسایی آن را دشوار کرده است. مقابله مؤثر نیازمند همکاری بین‌المللی، چارچوب‌های حقوقی شفاف و رعایت اصول حقوق بشر است(جابری و همکاران، ۱۴۰۱: ۱۰۲). در سطح فراملی، دولت‌ها، سازمان‌های منطقه‌ای و نهادهای بین‌المللی کوشیده‌اند سازوکارهایی ایجاد کنند که ضمن تقویت توان مقابله با تهدیدات دیجیتال، آزادی‌های اساسی افراد نیز محفوظ بماند. مقررات‌گذاری‌های اتحادیه اروپا و ایجاد چارچوب‌های الزام‌آور برای شرکت‌های فناوری، نمونه‌ای از تلاش‌های هماهنگ برای تنظیم فضای دیجیتال است. البته گسترش فضای مجازی تبادل سریع و کم‌هزینه اطلاعات را ممکن کرده است، اما با خطرات پیچیده‌ای مانند فعالیت‌های تروریستی دیجیتال همراه است که می‌تواند به زیرساخت‌های حیاتی کشورها آسیب بزند. دولت‌ها موظف به حفظ حقوق بشر و امنیت فردی هستند، اما باید در عین اعمال محدودیت‌ها از نقض حقوق خصوصی افراد جلوگیری کنند(قاسمی، و همکاران، ۱۳۹۴: ۲۳۷). بنابراین، اسنادی مانند «کنوانسیون بوداپست» همکاری میان دولت‌ها را در تعقیب و رسیدگی به چنین فعالیت‌هایی تسهیل کرده است، اما فقدان یک تعریف حقوقی جامع از این نوع فعالیت‌ها همچنان چالشی بزرگ است. این شکاف مفهومی باعث می‌شود دولت‌ها برداشت‌های متفاوتی از مصادیق تروریسم دیجیتالی داشته باشند، که هماهنگی جهانی را دشوار می‌کند. علاوه بر این، اختلافات میان دولت‌ها و شرکت‌های فناوری در خصوص دسترسی به داده‌ها، پالایش محتوا و تعهدات سکوها، پیچیدگی‌ها را تشدید می‌کند.

سازوکارهای ضدتروریسم سازمان ملل، مانند قطعنامه‌ها و تحریم‌ها، با چالش‌هایی از جمله ضعف هماهنگی بین‌المللی و سوءاستفاده‌های سیاسی مواجه‌اند. اجرای ناقص این اقدامات می‌تواند به آسیب به مردم عادی و نقض حقوق بشر منجر شود. در عصر دیجیتال، تعادل میان امنیت و حقوق بشر ضروری است تا حریم خصوصی و آزادی بیان حفظ گردد و تهدیدات جهانی کاهش یابد. از اینرو، سازمان ملل متحد در واکنش به این چالش‌ها اسناد، راهبردها و قطعنامه‌هایی منتشر کرده است که به‌طور هم‌زمان بر ضرورت مقابله با تهدیدات دیجیتال و رعایت استانداردهای حقوق بشر تأکید دارند. قطعنامه‌های ۲۳۵۴ و ۲۳۹۶ سال ۲۰۱۷ شورای امنیت بر لزوم همکاری کشورهای عضو در شناسایی و پیشگیری از تهدیدات دیجیتالی و اتخاذ اقدامات مشترک تأکید دارند. در این چارچوب، سازمان ملل متحد رعایت اصول حقوق بشر، از جمله آزادی بیان، حریم خصوصی و حق دسترسی به اطلاعات را در تمامی اقدامات ضدتروریستی ضروری می‌داند(McKeever, 2021: 451). علاوه بر این، سازمان ملل متحد بر تقویت همکاری‌های قضایی و اطلاعاتی میان کشورها و تدوین استانداردهای جهانی برای مقابله با تهدیدات دیجیتالی تأکید می‌کند(www.unjiu.org). این استانداردها باید بر مبنای اصول حقوق بشری مانند تناسب، ضرورت و عدم تبعیض تنظیم شوند. افزون بر این، مشارکت نهادهای غیردولتی و سازمان‌های حقوق بشری در نظارت بر این اقدامات و تضمین شفافیت و پاسخگویی امری ضروری است(https://unicri.org). در چارچوب رویکرد حاکم در سازمان ملل متحد، امنیت دیجیتال بدون پای‌بندی به آزادی‌های اساسی، صرفاً به ایجاد فضای بی‌اعتمادی و تضعیف مشروعیت اقدامات ضدتروریسم می‌انجامد. به همین دلیل، اقدامات گسترده نظارتی بدون وجود ضرورت واقعی، بدون نظارت قضایی یا فاقد شفافیت کافی، ناقض حقوق بنیادین به‌ویژه حق حریم خصوصی تلقی می‌شود.

یکی از مهم‌ترین محورهای کار سازمان ملل، تدوین اصول و معیارهایی است که سازوکارهای ضدفعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی باید مبتنی بر آنها باشد. از جمله این اصول می‌توان به ضرورت وجود دلیل موجه و مستند برای هر اقدام امنیتی، شفافیت در سازوکارهای نظارت و جمع‌آوری داده، اتکا به چارچوب‌های قانونی روشن، پرهیز از تبعیض در اجرای قوانین، و ایجاد امکان نظارت قضایی و پارلمانی بر اقدامات دولت‌ها اشاره کرد(گیوکی، ۱۴۰۰: ۲۲۹). این معیارها ریشه در اسناد الهام‌بخش حقوق بشری، از جمله میثاق حقوق مدنی و سیاسی دارند(Özler, 2018: 397) و دولت‌ها ملزم به رعایت آن هستند(Celorio, 2024: 1). البته ورود فناوری‌های نوین مانند هوش مصنوعی و تحلیل داده‌های کلان ابعاد جدیدی از امنیت و آزادی دیجیتال را به وجود آورده است. این فناوری‌ها می‌توانند به تشخیص تهدیدات کمک کنند، اما بدون قوانین شفاف، ممکن است به نظارت فراگیر تبدیل شوند. سازمان ملل بر رعایت اصول ضرورت، تناسب و مشروعیت در استفاده از این فناوری‌ها تأکید دارد(Radanliev, 2025: 43).

افزون بر این، یکی از مهم‌ترین نگرانی‌های نهادهای حقوق بشری، گسترش نظارت‌های بی‌ضابطه بر کاربران با توجیه مقابله با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی است. افزایش جمع‌آوری داده‌ها، استفاده از ابزارهای تحلیل رفتاری و کنترل گسترده ارتباطات می‌تواند به محدود شدن آزادی بیان، تشدید خودسانسوری و کاهش اعتماد عمومی نسبت به دولت‌ها منجر شود. بر همین اساس، گزارشگران ویژه سازمان ملل متحد تأکید می‌کنند که گردآوری داده‌ها باید محدود به موارد ضروری، متناسب با تهدید و مطابق مقررات قانونی باشد. از اینرو، برای مواجهه مؤثر با این تهدیدات، سازمان ملل متحد راهبردی چندلایه را دنبال می‌کند: ارتقای ظرفیت دولت‌ها، به‌ویژه کشورهای در حال

توسعه؛ تقویت همکاری‌های فرامرزی؛ تدوین اسناد الزام‌آور و غیرالزام‌آور درباره جرایم دیجیتالی؛ ایجاد شبکه‌های هماهنگ تبادل اطلاعات؛ و توسعه سامانه‌های نظارتی برای اطمینان از رعایت حقوق بشر در اقدامات ضدتروریسم. تصویب «کنوانسیون بین‌المللی مقابله با جرایم سایبری (۲۰۲۴)» یکی از گام‌های مهم در ایجاد یک رژیم حقوقی جامع برای مقابله با سوءاستفاده از فضای دیجیتال است که هم‌زمان توجه ویژه‌ای به حفاظت از حقوق بشر دارد.

با این همه، کنوانسیون‌های پالرمو(۱۹۹۹)، بوداپست (۲۰۰۱) و البته کنوانسیون سازمان ملل متحد علیه جرایم سایبری (۲۰۲۴) با تأکید بر راهبرد مجمع عمومی سازمان ملل متحد برای تقویت همکاری بین‌المللی در مبارزه با جرایم ارتکابی از طریق فناوری‌های اطلاعات و ارتباطات و تسهیل اشتراک‌گذاری شواهد الکترونیکی جرایم جدی(https://docs.un.org/en/A/RES/79/243) با ۶۸ ماده و (یادداشت‌های تفسیری راجع‌به مواد ۲، ۱۷، ۲۳ و ۳۵ کنوانسیون سازمان ملل متحد علیه جرایم سایبری برای تقویت همکاری بین‌المللی برای مبارزه با برخی جرایم ارتکابی از طریق سامانه‌های فناوری اطلاعات و ارتباطات و برای به اشتراک گذاشتن شواهد الکترونیکی جرایم جدی) وفق قطعنامه‌های (۲۰۱۹)۲۴۷/۷۴ و (۲۰۲۱)۲۸۲/۷۵ مجمع عمومی، مبادرت به بررسی تهدیدات دیجیتالی و همکاری‌های بین‌المللی برای مقابله با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی نمودند(https://docs.un.org/en/A/RES/77/298).

ماهیت پیچیده و مرزگریز فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی ایجاب می‌کند که دولت‌ها، سازمان‌های بین‌المللی، شرکت‌های فناوری و جامعه مدنی در تعامل مستمر و بر اساس اصول مشترک عمل کنند. وفق یافته‌های پژوهشی، مقررات دیجیتالی در صورتی که منطبق با موازین و معیارهای حقوق بشر و با نگاهی نو بر اساس نیازهای جدید فضای نوپدید دیجیتالی، بازنگری یا تدوین شده باشند می‌توانند در صیانت از حقوق شهروندی و به خصوص حق بر توسعه از نسل سوم حقوق بشر نقش موثر و قابل ملاحظه‌ای داشته باشند(رئیسی، ۱۴۰۲: ۲۵). بنابراین، سازمان ملل متحد تأکید دارد که تعادل میان امنیت و آزادی‌های بنیادین باید محور اصلی سیاست‌های مرتبط با فضای دیجیتال باشد. تحقق امنیت پایدار مستلزم شفافیت، پاسخگویی، رعایت کرامت انسانی و ایجاد اعتماد عمومی است؛ اموری که بدون آنها هرگونه اقدام ضدتروریستی می‌تواند خود به منبعی برای نقض حقوق بشر تبدیل شود.

با توسعه فناوری‌های دیجیتال، تهدیدات جدیدی مانند تروریسم برخط و حملات دیجیتالی ظهور کرده که می‌تواند امنیت ملی و حریم خصوصی افراد را به خطر اندازد. این تهدیدات شامل انتشار محتوای افراطی، حملات به زیرساخت‌های حیاتی و دسترسی غیرمجاز به اطلاعات حساس است. برای مقابله با این چالش‌ها، ضروری است که حقوق بشر و اصول حاکمیت قانون به‌طور کامل رعایت شوند، زیرا اقدامات غیرقانونی می‌تواند به نقض آزادی‌های فردی منجر شود. سازمان ملل متحد با تأکید بر اهمیت حقوق بشر و شفافیت در نظارت قضائی، سعی در تقویت همکاری‌های جهانی برای مقابله با تهدیدات دیجیتالی دارد. یکی از مسائل کلیدی در این زمینه، فقدان یک تعریف واحد از فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی و اختلافات میان دولت‌ها و شرکت‌های فناوری است. برای مبارزه مؤثر با این تهدیدات، استفاده از فناوری‌های نوین مانند هوش مصنوعی باید در چارچوب‌های قانونی شفاف و با رعایت حقوق فردی انجام شود(کاظم‌نژاد و توکلی‌فر، ۱۴۰۳: ۶۶-۶۴).

۱-۲. همکاری اینترپل و یوروپل در ایجاد امنیت دیجیتال با توازن میان مقابله با تهدیدات دیجیتالی و رعایت حقوق بشر

افزایش فعالیت‌های تروریستی در سکوهای دیجیتالی و سوءاستفاده از داده‌های شخصی، نیاز به ایجاد سازوکارهای همکاری حقوقی و عملیاتی مؤثر و مبتنی بر اصول حقوقی روشن را ضروری کرده است. «اینترپل» و «یوروپل» نقش کلیدی در هماهنگی اقدامات، تقویت زیرساخت‌های فنی و تضمین رعایت حقوق بشر دارند. این همکاری‌ها عمدتاً شامل تبادل اطلاعات، تحلیل تهدیدات و تعامل با شرکت‌های فناوری است. با این حال، اثربخشی آن‌ها تنها در صورت رعایت کامل حقوق بشر تضمین می‌شود. همچنین، سازوکارهای ضدتروریسم بین‌المللی، به‌ویژه تحریم‌ها، گاه پیامدهای منفی برای جمعیت‌های غیرنظامی دارند و ممکن است منجر به نقض حقوق بشر شوند.

اینترپل، به‌عنوان نهادی با صلاحیت جهانی در هماهنگی پلیسی، همواره با ضرورت ایجاد توازن میان اقتضائات امنیتی و حقوق فردی مواجه است. این سازمان دستورالعمل‌ها و قواعدی تدوین کرده است که رعایت اصول حقوق بشری را در فرآیندهای جمع‌آوری، پردازش و تبادل داده الزام‌آور می‌داند. از منظر اینترپل، اقدامات امنیتی باید مستند، شفاف و محدود به مواردی باشند که ضرورت آنها اثبات شده است. بر همین اساس، اینترپل می‌کوشد سازوکارهایی طراحی کند که هم امکان ردیابی تهدیدات پیچیده دیجیتالی را فراهم سازد و هم از مداخله غیرضرور در حریم خصوصی و آزادی‌های بنیادین پیشگیری شود(رجبی‌تاج‌امیر، ۱۴۰۱: ۱۶). شبکه‌های همکاری چندجانبه‌ای که این سازمان میان دولت‌های عضو ایجاد کرده، بستری برای جریان قانونی اطلاعات و انتقال تجربیات فراهم می‌کند و تقویت ظرفیت جمعی در قبال فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی را امکان‌پذیر می‌سازد. این رویکرد به کشورهای عضو اجازه می‌دهد راهبردی هماهنگ و متکی بر اصول حقوق بشری در مواجهه با تهدیدات فراملی اتخاذ کنند(Calcara, 2021: 126). اقدامات باید در چارچوب قوانین بین‌المللی طراحی و اجرا شوند تا از نقض حقوق افراد پیشگیری شود. افزون بر این، اینترپل برای مقابله مؤثر با تهدیدات دیجیتال، به تقویت همکاری‌های بین‌المللی و به اشتراک‌گذاری تجربیات و منابع کشورهای عضو نیاز دارد(https://documents.unoda.org).

در سیاست‌های امنیتی اینترپل، بر این نکته تأکید می‌شود که امنیت دیجیتال نباید از بُعد انسانی آن جدا شود. یعنی اقدامات نظارتی و امنیتی تنها زمانی مشروعیت دارند که با رعایت آزادی‌ها و حقوق بنیادین همراه باشند. ازاین‌رو، عملیات نظیر پایش فعالیت‌های برخط، تحلیل داده‌های کلان یا بهره‌گیری از ابزارهای رفتاری، باید در چارچوب قوانین مشخص و با ارزیابی‌های مستمر در زمینه ضرورت و تناسب انجام گیرد. اینترپل از دولت‌های عضو می‌خواهد که در اجرای تدابیر مقابله با تروریسم، از چارچوب‌های حقوقی معتبر عدول نکنند؛ موضوعی که علاوه بر پیشگیری از سوءاستفاده احتمالی از اختیارات امنیتی، به افزایش اعتماد عمومی نسبت به اقدامات پیشگیرانه نیز کمک می‌کند. یکی از چالش‌های اصلی، حفظ امنیت دیجیتالی بدون نقض حقوق فردی است(Calcara, 2019: 92). البته اینترپل بر لزوم شفافیت در اقدامات امنیتی تأکید دارد؛ به‌ویژه در جمع‌آوری داده‌های شخصی و نظارت بر فعالیت‌های دیجیتالی، که باید بر اساس قوانین و استانداردهای بین‌المللی صورت گیرد. اینترپل با طراحی و اجرای رویه‌های منظم و شفاف، کوشیده است تعادلی میان تضمین امنیت دیجیتالی و رعایت حقوق فردی برقرار کند. یکی از مهم‌ترین چالش‌های این سازمان، پایش فعالیت‌های برخط و جمع‌آوری داده‌هاست؛ کاری که باید همسو با موازین قانونی و اخلاقی انجام شود تا از تجاوز به حریم خصوصی شهروندان پیشگیری شود(مستوفیان، ۱۴۰۴: ۲۹). اینترپل همچنین بر اهمیت شفافیت و

مستندسازی در روند جمع‌آوری اطلاعات تأکید دارد و تلاش می‌کند تمامی اقداماتش در چارچوب اصول حقوق بشر صورت پذیرد(Calleja, 2025: 189).

اینترپل با تقویت شبکه‌های همکاری بین‌المللی و تسهیل تبادل اطلاعات، به کشورهای عضو کمک می‌کند تا تهدیدات دیجیتال را شناسایی و مدیریت کنند(Calcara, 2020: 12). هم‌زمان، با تأکید بر شفافیت و مستندسازی اقدامات امنیتی، این سازمان تلاش می‌کند از هرگونه نقض حقوق بشر پیشگیری نماید. مقابله مؤثر با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی نیازمند همکاری جهانی و اتخاذ رویکردی متوازن میان امنیت دیجیتالی و حفاظت از حقوق فردی است که اینترپل در تحقق آن نقش حیاتی ایفا می‌کند(Gottlieb, 2011: 141).

در سطح منطقه‌ای، یوروپل به‌عنوان نهاد اطلاعاتی و عملیاتی اتحادیه اروپا در بستر حقوقی متفاوتی فعالیت می‌کند اما با چالش‌هایی مشابه مواجه است(https://www.uaces.org). این آژانس براساس کنوانسیون اروپایی حقوق بشر و دیگر اسناد الزام‌آور اتحادیه اروپا، مکلف است اطمینان حاصل کند که تمامی عملیات خود مطابق اصول قانونی‌بودن، ضرورت، شفافیت و تناسب باشد. با توجه به اتکای گسترده یوروپل بر فناوری‌های تحلیل داده، سامانه‌های پیش‌بینی تهدید و ابزارهای نظارت دیجیتال، ایجاد هماهنگی میان کارآمدی عملیاتی و رعایت حقوق اساسی شهروندان، به عرصه‌ای حساس و پیچیده تبدیل شده است. علاوه بر این، یوروپل با همکاری‌های بین‌المللی گسترده و تبادل اطلاعات با کشورهای عضو اتحادیه اروپا و نهادهای حقوق بشری، به تقویت نظارت و اجرای حقوق بشر در فرآیندهای امنیتی پرداخته است(Ligeti & Giuffrida, 2023: 372). از آنجا که تهدیدات دیجیتال به‌طور فزاینده‌ای فرامرزی هستند، پیروی از اصول حقوق بشری در تعاملات جهانی و همکاری‌های بین‌المللی برای حفاظت از حقوق فردی و آزادی‌های اساسی امری ضروری است.

یوروپل در توسعه توان فنی خود ملزم است ترتیباتی ایجاد کند که نه تنها اثربخشی مقابله با تهدیدات را افزایش دهد، بلکه مانع نقض حریم خصوصی و محدودسازی آزادی بیان شود. لازم به‌ذکر است، در نظام حقوق بشر اروپایی، آزادی بیان به عنوان یکی از حقوق بنیادین شناخته می‌شود و به افراد امکان می‌دهد نظرات و عقاید خود را آزادانه مطرح کنند(Coche, 2018: 11). با این حال، این آزادی نباید به گونه‌ای اعمال شود که حقوق دیگران، از جمله حقوق مذهبی، را نقض کند. به عبارت دیگر، چارچوب حقوقی اروپایی، آزادی بیان را نه تنها به عنوان رکن اساسی یک جامعه دمکراتیک، بلکه به عنوان شرط ضروری برای پیشرفت فردی و خودشکوفایی افراد می‌داند(رهامی و همکاران، ۱۴۰۳: ۲۴۷).

در حوزه مقابله با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی، یوروپل از فناوری‌هایی بهره می‌گیرد که تحلیل الگوهای رفتاری، شناسایی تهدیدات نوپدید و ردیابی شبکه‌های مجرمانه را تسهیل می‌کند. اما به‌کارگیری این ابزارها بدون سازوکارهای نظارتی مناسب می‌تواند به تحدید آزادی‌های عمومی بیانجامد(امامی، ۱۴۰۲: ۱۳۵-۱۳۴). از همین‌رو، یوروپل با ایجاد نظام‌های شفافیت و کنترل داخلی از سوءاستفاده از داده‌ها جلوگیری کرده و همکاری مستمر با نهادهای حقوق بشری اتحادیه اروپا را برای رعایت الزامات حقوق بشر انجام می‌دهد. این آژانس بر تقویت همکاری‌های فرامرزی تأکید دارد و با همکاری بین‌المللی، تبادل داده‌ها و هماهنگی عملیاتی را تسهیل می‌کند(https://www.europol.europa.eu). یوروپل بر اصول محدودیت پردازش داده‌ها، ضرورت، تناسب و

احترام به حریم خصوصی تأکید دارد. همکاری‌های یوروپل و اینترپل در امنیت دیجیتال نمونه‌ای از حکمرانی چندجانبه است که امنیت و حقوق بشر را متوازن می‌سازد.

با توجه به گسترش تهدیدات دیجیتال و افزایش فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی، نیاز به همکاری‌های بین‌المللی در راستای تقویت امنیت سایبری امری اجتناب‌ناپذیر است. نهادهایی همچون اینترپل و یوروپل موظفند ضمن اتخاذ اقدامات امنیتی در این زمینه، حقوق بشر و آزادی‌های فردی را به‌عنوان اصول بنیادین در فرآیندهای خود رعایت کنند. این نهادها از طریق تبادل اطلاعات و شناسایی تهدیدات برخط، نقش اساسی در حفظ امنیت جهانی ایفا می‌کنند. رعایت اصول حقوق بشری در سیاست‌های امنیتی دیجیتال از اهمیت ویژه‌ای برخوردار است. تمامی اقدامات امنیتی باید در چارچوب موازین بین‌المللی و با احترام به حقوق فردی صورت گیرد. این اصول شامل حفاظت از داده‌های شخصی، تضمین حق دفاع در قبال اتهامات نادرست و شفافیت در فرآیندهای نظارتی است. نظارت بر فعالیت‌های برخط باید با دقت، شفافیت و متناسب با ماهیت تهدیدات انجام پذیرد. در ضمن، همکاری‌های مؤثر تنها زمانی تحقق می‌یابد که این اقدامات با رعایت اصول حقوق بشر و تحت نظارت دقیق و شفاف به‌طور جامع اجرایی شوند، تا از هرگونه سوءاستفاده و نقض حقوق فردی پیشگیری گردد.

۱-۳. ظرفیت‌سنجی شورای امنیت و مجمع عمومی در قبال تروریسم دیجیتال با حفظ توازن میان امنیت و حقوق بشر

شورای امنیت سازمان ملل متحد و کمیته مبارزه با تروریسم از مهم‌ترین ارکان بین‌المللی در مقابله با تهدیدات نوظهور، به‌ویژه فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی، به شمار می‌روند. شورای امنیت با مأموریت حفظ صلح و امنیت بین‌المللی، از طریق تصویب قطعنامه‌ها، اعمال تحریم‌ها و در شرایط استثنایی استفاده از نیروی نظامی، کشورهای عضو را به همکاری در مقابله با تهدیدات ملزم می‌سازد. کمیته مبارزه با تروریسم به‌عنوان بازوی اجرایی و نظارتی شورای امنیت، با تسهیل هماهنگی بین کشورها، تبادل اطلاعات و ارتقای ظرفیت‌های عملیاتی، توان مقابله با تهدیدات دیجیتال را تقویت می‌کند(https://www.accessnow.org). این دو نهاد همزمان بر حفظ توازن میان امنیت و حقوق بشر تأکید دارند؛ محدودیت‌های اعمال‌شده بر آزادی بیان، تهدید حریم خصوصی و احتمال تعارض اقدامات امنیتی با استانداردهای حقوق بشری، از مهم‌ترین چالش‌های پیش‌رو هستند(Galloro & Guida, 2024: 9).

قطعنامه‌های اصلی شورای امنیت، از جمله قطعنامه‌های ۱۳۷۳ و ۲۱۷۸، کشورهای عضو را ملزم به تقویت ظرفیت‌های قانونی، اجرایی و فناوری خود کرده و همزمان حفاظت از حقوق فردی را مورد توجه قرار می‌دهند. کمیته مبارزه با تروریسم نیز سازوکارهایی برای نظارت مستمر بر اقدامات ضدتروریستی، ارزیابی آثار حقوق بشری و تضمین انطباق اقدامات با استانداردهای بین‌المللی ایجاد کرده است. فعالیت‌های عملیاتی این کمیته شامل پایش اقدامات دیجیتال، اجرای فیلترینگ هدفمند و ارتقای توانمندی‌های کشورهای عضو است، مشروط بر آنکه اصول حقوق بشر و آزادی‌های فردی رعایت شود. در این راستا، همکاری‌های بین‌المللی برای تقویت ظرفیت‌های کشورهای عضو در مقابله با تهدیدات دیجیتال و حفظ اصول حقوق بشر بسیار ضروری است. در نهایت، شورای امنیت باید به‌طور مؤثر با تهدیدات دیجیتالی مقابله کند، بدون اینکه حقوق بشر قربانی اقدامات امنیتی شود(Ezra, 2022: 131).

قطعنامه‌های ضدتروریسم شورای امنیت سازمان ملل با هدف مقابله با تهدیدات تروریستی در سطح جهانی تصویب شده‌اند، اما در عمل با چالش‌هایی مواجه‌اند. اصلی‌ترین عوامل ناکارآمدی این سیاست‌ها شامل عدم هماهنگی میان

کشورهای مختلف، تضاد منافع سیاسی و نقص در پیگیری و نظارت بر اجرای این تصمیمات است. همچنین، با ظهور تهدیدات جدید مانند فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی، نیاز به رویکردهایی نوین و سازگار با فضای دیجیتال احساس می‌شود که در چارچوب کنونی موجود نیست. از سوی دیگر، در برخی موارد، تحریم‌ها و قطعنامه‌ها به جای مبارزه با تروریسم، به ابزاری برای منافع سیاسی تبدیل شده‌اند. برای مقابله مؤثر با تروریسم، ضروری است که سیاست‌ها بازبینی شده و همکاری‌های بین‌المللی تقویت شود. همکاری‌های بین‌المللی نقش تعیین‌کننده‌ای در موفقیت اقدامات شورای امنیت و کمیته دارد. تبادل اطلاعات، هماهنگی عملیاتی و تقویت توانمندی کشورهای عضو، به‌ویژه در کشورهای در حال توسعه، از ابزارهای کلیدی مقابله با تهدیدات دیجیتال محسوب می‌شوند. در مقابل، اختلاف دیدگاه میان اعضا، محدودیت‌های مالی و زیرساختی و عدم هماهنگی در اجرای تدابیر، از موانع عمده به شمار می‌روند. رعایت کامل استانداردهای حقوق بشری و پیشگیری از نقض حقوق فردی، از وظایف حیاتی این نهادهاست (Voloshchuk, el al, 2021: 74).

مجمع عمومی سازمان ملل نیز با نقش سیاست‌گذاری و هماهنگی، به ایجاد توازن میان امنیت و حقوق بشر کمک می‌کند(https://acuns.org). این نهاد با فراهم آوردن بستر گفت‌وگو، تصویب قطعنامه‌ها و رهنمودهای عمومی و هماهنگی با سایر ارکان، چارچوب قانونی و نظارتی مقابله با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی را تقویت می‌کند(https://docs.un.org/en/A/RES/78/210). راهبردهای مجمع شامل ارتقای قطعنامه‌ها، تدوین مقررات منطبق با حقوق بشر، توسعه همکاری‌های بین‌المللی و تسهیل تبادل اطلاعات میان کشورهای عضو است. ایجاد سازوکارهای شفاف نظارتی، اقدامات اصلاحی و برنامه‌های آموزشی تخصصی برای کشورهای عضو، از دیگر اقدامات راهبردی آن محسوب می‌شوند(Iftikhar, 2024: 71). از اینرو، مقابله با چنین فعالی‌هایی نیازمند رویکردی چندجانبه، هماهنگ و مبتنی بر حقوق بشر است. شورای امنیت، کمیته مبارزه با تروریسم و مجمع عمومی با همکاری‌های میان‌نهادی، امنیت جهانی را تضمین و حقوق بشر را حفظ می‌کنند.

شورای امنیت سازمان ملل از ابزارهای متنوعی مانند تصویب قطعنامه‌ها، اعمال تحریم‌ها و در موارد ضروری استفاده از نیروی نظامی برای تشویق کشورهای عضو به همکاری در مقابله با تهدیدات تروریستی جهانی بهره می‌برد. در حوزه تهدیدات دیجیتال، قطعنامه‌های ۱۳۷۳ و ۲۱۷۸ بر لزوم تقویت ظرفیت‌های قانونی کشورها و رعایت اصول حقوق بشری در اقدامات ضدتروریستی تأکید دارند. کمیته مبارزه با تروریسم به‌عنوان نهاد اجرایی شورای امنیت، با تسهیل تبادل اطلاعات و نظارت بر اجرای اقدامات، تضمین می‌کند که فعالیت‌ها مطابق استانداردهای بین‌المللی حقوق بشر انجام شود. مجمع عمومی سازمان ملل نیز نقش کلیدی در تدوین سیاست‌های جهانی، ایجاد چارچوب‌های قانونی و تسهیل همکاری میان کشورهای عضو دارد و بر ضرورت حفظ تعادل میان امنیت و حقوق فردی تأکید می‌کند. این نهاد از طریق تصویب مقررات بین‌المللی، هماهنگی و تبادل اطلاعات را تقویت می‌کند تا اقدامات ضدتروریستی مؤثر و هماهنگ باشند. به‌طور کلی، شورای امنیت و کمیته مبارزه با تروریسم بر جنبه‌های اجرایی و نظارتی تمرکز دارند، در حالی که مجمع عمومی مسئول تدوین سیاست‌ها و هم‌افزایی بین‌المللی است. همکاری میان این نهادها برای اجرای مؤثر اقدامات و حفاظت کامل از حقوق بشر و آزادی‌های فردی ضروری است.

۲. توازن امنیت دیجیتالی و آزادی بیان در چارچوب‌های حقوقی بین‌المللی

در عصر حاضر، پیشرفت‌های فناوری‌های دیجیتال به‌طور گسترده‌ای در زندگی فردی، اجتماعی و اقتصادی انسان‌ها نفوذ کرده و ضمن ایجاد فرصت‌های متعدد، تهدیدات نوینی نیز به همراه آورده است. یکی از مهم‌ترین این تهدیدات، فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی است که با بهره‌گیری از ابزارهای برخط، شبکه‌های اجتماعی و سامانه‌های اطلاعاتی، فعالیت‌های خشونت‌آمیز خود را برنامه‌ریزی، سازماندهی و گسترش می‌دهد. این نوع تهدید نه تنها سلامت و امنیت جامعه جهانی را به خطر می‌اندازد، بلکه چالش‌های جدی حقوق بشری، از جمله حفاظت از حریم خصوصی و آزادی‌های فردی، را نیز به وجود می‌آورد(https://www.gp-digital.org). فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی به عنوان یک خطر بالقوه تمامی کشورهای جهان را تهدید می‌کند و با ویژگی‌هایی که دارد ناقض جدی صلح، امنیت بین‌المللی و حقوق بشر است(میربد و همکاران، ۱۴۰۱: ۵۴۶)؛ از اینرو، نظارت دیجیتال و ردیابی برخط به‌ویژه در مقابله با تهدیدات دیجیتال مانند تروریسم می‌تواند حقوق فردی را به‌خطر اندازد. بنابراین، مقابله با این دسته از فعالیت‌های تروریستی مستلزم تدوین سیاست‌ها و چارچوب‌هایی است که همزمان امنیت و حقوق بنیادین انسان‌ها را تضمین کنند.

تدوین چارچوب‌های حقوقی بین‌المللی، از ارکان اصلی پاسخ به تهدیدات دیجیتال است. این چارچوب‌ها باید به گونه‌ای طراحی شوند که هم امنیت دیجیتال را تضمین کنند و هم از آزادی‌های بنیادین، حقوق فردی، آزادی بیان و حریم خصوصی حفاظت نمایند. توسعه چنین مقرراتی نیازمند همکاری نزدیک میان کشورها، تبادل اطلاعات و تدوین استانداردهای مشترک در حوزه حفاظت از داده‌ها و فناوری‌های نوین است(Sendjaja, 2024: 1012). همچنین، این مقررات باید انعطاف‌پذیر و قابلیت به‌روزرسانی داشته باشند تا با تحولات سریع فناوری و ظهور تهدیدات جدید هماهنگ باشند و پاسخگویی مؤثر را تضمین کنند. علاوه بر تدوین قوانین، ایجاد سازوکارهای نظارتی مستقل برای ارزیابی و کنترل عملکرد اقدامات امنیتی ضروری است(Allahrakha, 2023: 88). نظارت شفاف و مستمر می‌تواند از اعمال محدودیت‌های غیرضروری بر حقوق فردی پیشگیری کند و تضمین نماید که سیاست‌های مقابله با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی مطابق با استانداردهای بین‌المللی و اصول حقوق بشر اجرا می‌شوند(Cristiano, 2020: 12-14). بدون چنین سازوکارهایی، حتی قوانین مدون نیز ممکن است در عمل به نقض حقوق بنیادین منجر شوند.

سازوکار رسیدگی به فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی، به همکاری‌های بین‌المللی و هماهنگی‌های حقوقی گسترده نیاز دارد. در فرآیند رسیدگی فردی، مواردی همچون استرداد مجرمان، تبادل اطلاعات و نظارت بر محتوای دیجیتال مطرح است که در آن حقوق بشر و حریم خصوصی باید حفظ شود. در سطح دولتی، نهادهای بین‌المللی همچون سازمان ملل و اتحادیه اروپا برای ایجاد چارچوب‌های قضائی و هماهنگ‌سازی اقدامات همکاری می‌کنند. کنوانسیون‌های بوداپست و پالرمو زمینه‌ساز این همکاری‌ها هستند و کنوانسیون سازمان ملل متحد علیه جرایم سایبری (۲۰۲۴) می‌تواند با استانداردسازی قوانین، پاسخگویی به تهدیدات سایبری پیچیده‌تر را تسهیل کند.

آگاهی‌بخشی و آموزش نقش حیاتی در مدیریت متوازن امنیت و حقوق بشر دارند. ارتقای دانش در حوزه‌های امنیت دیجیتالی و حقوق بشر، به نهادها و سازمان‌ها کمک می‌کند تا اقدامات خود را با رعایت حقوق فردی طراحی کنند(Popa Tache, 2024: 7). تبادل تجربیات بین‌المللی و هماهنگی قوانین، همکاری‌های جهانی در مقابله با تهدیدات دیجیتالی را تقویت می‌کند(Rahman & Das, 2024: 993). همچنین، ایجاد سازوکارهای بین‌المللی و

تقویت زیرساخت‌ها(Emmanuel, el al, 2025: 221)، برای تأمین امنیت جهانی و حفظ حقوق فردی ضروری است. به‌طور کلی، دستیابی به توازن میان امنیت جهانی و حقوق بشر در عصر دیجیتال نیازمند رویکردی چندجانبه است که شامل تدوین مقررات بین‌المللی، همکاری‌های جهانی، ایجاد نهادهای نظارتی مستقل و تقویت آموزش و آگاهی‌بخشی در حوزه امنیت دیجیتال و حقوق بشر باشد(Alubaidi, 2023: 34). این رویکرد هم امنیت جامعه جهانی را تأمین می‌کند و هم از آزادی‌ها و حقوق فردی محافظت می‌نماید. با این حال، هرگونه نظارت باید مبتنی بر قانون و متناسب با اهداف مشروع باشد. اهمیت این موضوع زمانی بیشتر می‌شود که خطر نقض حقوق بشر در زمینه اشتراک‌گذاری داده‌ها و نظارت گسترده وجود دارد، و ضرورت ایجاد سازوکارهای نظارتی کارآمد و مناسب را آشکار می‌سازد(https://docs.un.org/en/A/78/269).

مدیریت مؤثر تهدیدات دیجیتال بدون رعایت حقوق بشر، نه تنها ناکارآمد است، بلکه مشروعیت اقدامات امنیتی را تضعیف و موجب نارضایتی و بی‌اعتمادی عمومی می‌شود. از اینرو، ایجاد نهادهای نظارتی مستقل برای ارزیابی عملکرد دولت‌ها و سازمان‌های بین‌المللی در مقابله با تهدیدات دیجیتال اهمیت ویژه‌ای دارد(مرادی و همکاران، ۱۴۰۱: ۴۲). این نهادها باید به‌طور مستقل فرآیندهای مقابله با تهدیدات دیجیتال را رصد و ارزیابی کنند و از هرگونه سوءاستفاده احتمالی پیشگیری نمایند(Safitra, el al, 2023: 16). بنابراین، در تدوین اسناد بین‌المللی ضروری است به تفاوت‌های نظام‌های حقوقی کشورها احترام گذاشته شود و رویکردی جامع و قابل قبول برای تمامی اعضا اتخاذ گردد. بسیاری از توافقات و همکاری‌های بین‌المللی پیشین در حوزه مبارزه با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی فاقد سازوکارهای نظارتی مستقل و شفاف بوده‌اند، امری که نگرانی‌هایی درباره نقض حقوق بشر و عدم شفافیت در اجرای اقدامات ایجاد کرده است(Clough, 2014: 706). بر این اساس، اسناد بین‌المللی جدید باید شامل مکانیسم‌های نظارتی مؤثر برای حفاظت از حقوق بشر و تضمین جبران خسارت در صورت نقض حقوق افراد باشند.

سیاست‌گذاران، سازمان‌های بین‌المللی و جوامع مدنی باید با همکاری یکدیگر چارچوب‌هایی طراحی کنند که امنیت دیجیتال، حریم خصوصی، آزادی بیان و حقوق داده‌ها را به‌طور همزمان تأمین کنند. این رویکرد مستلزم نوآوری در حوزه‌های حقوقی و فناوری، پایبندی به اصول حقوق بشر و تلاش مستمر برای مدیریت تهدیدات دیجیتال به شیوه‌ای مؤثر و منصفانه است. از اینرو، مقابله با این تهدیدات نیازمند نظارت و ردیابی دیجیتال است، اما این اقدامات باید به‌گونه‌ای انجام گیرد که حقوق فردی و آزادی‌های عمومی محفوظ بماند. علاوه بر این، ایجاد همکاری‌های بین‌المللی، تدوین چارچوب‌های قانونی مناسب و تقویت نهادهای نظارتی مستقل برای مقابله مؤثر با این تهدیدات، اهمیت ویژه‌ای دارد تا بتوان توازن مناسبی میان امنیت جهانی و حفظ حقوق بشر برقرار کرد.

۳. ضرورت تدوین چارچوب‌های بین‌المللی الزام‌آور برای امنیت و رعایت حقوق بشر

فعالیت‌های تروریستی در سکوهای دیجیتالی تهدیدی نوظهور برای امنیت ملی و بین‌المللی ایجاد کرده‌اند. گروه‌های تروریستی با استفاده از فناوری‌های ارتباطی، توانایی سازمان‌دهی، تأمین مالی و اجرای حملات دیجیتال را دارند. مقابله با این تهدید نیازمند همکاری بین‌المللی و طراحی اقدامات امنیتی مبتنی بر رعایت حقوق بشر است تا آزادی‌های اساسی، کرامت انسانی و حاکمیت ملی حفظ شود. ماهیت فرامرزی تهدیدات دیجیتال ضرورت ایجاد چارچوب‌های حقوقی بین‌المللی الزام‌آور را روشن می‌کند. تهدیدات ناشی از این فعالیت‌ها مرزهای جغرافیایی را نادیده می‌گیرند و فقدان قوانین شفاف و تبادل اطلاعات ایمن می‌تواند به نقض حقوق بشر منتهی شود(https://www.clingendael.org).

این چارچوب‌ها باید امنیت، هماهنگی میان کشورها، و رعایت حقوق بشر را تضمین کرده و شامل ضوابط قانونی، سازوکارهای نظارتی مستقل و جبران خسارت در صورت نقض حقوق بنیادین باشند. بدون چنین سازوکارهایی، همکاری‌ها آسیب‌پذیر و خطر سوءاستفاده افزایش می‌یابد.

نهادهای بین‌المللی مانند یوروپل، اینترپل، کمیته مبارزه با تروریسم شورای امنیت و دفتر مقابله با مواد مخدر و جرم سازمان ملل نقش محوری در تدوین استانداردهای مشترک، آموزش‌های تخصصی و توسعه فناوری‌های پیشرفته برای مقابله با تهدیدات دیجیتال دارند(https://www.undp.org). این سازمان‌ها می‌توانند با تقویت نظارت مستقل، شفاف‌سازی فرآیند تبادل اطلاعات و ظرفیت‌سازی در کشورهای کمتر توسعه‌یافته، اثربخشی همکاری جهانی را افزایش دهند(Frosio & Geiger, 2023: 59). موفقیت این اقدامات مستلزم وجود چارچوب حقوقی منسجم و همسو با اصول حقوق بشر است تا اقدامات مقابله‌ای مشروع و متناسب با تهدیدها باشد.

از دیدگاه حقوق بشری، اقدامات مقابله‌ای باید مطابق با قانون، متناسب و بدون تبعیض باشند. مداخلات در حریم خصوصی، دسترسی به اطلاعات شخصی و اقدامات قضائی تنها در چارچوب قوانین داخلی و تعهدات بین‌المللی مجاز است. میثاق بین‌المللی حقوق مدنی و سیاسی، حقوق حریم خصوصی، آزادی بیان و دادرسی عادلانه را تضمین کرده و محدودیت‌های دیجیتال باید با رعایت این اصول اعمال شوند. اقدامات امنیتی باید بر اساس ضرورت و تناسب طراحی شوند تا تعادل میان امنیت و آزادی حفظ گردد. این میثاق از حریم خصوصی دفاع کرده و تأکید دارد که دخالت‌های غیرمجاز در زندگی خصوصی، خانواده یا مکاتبات شخصی باید مطابق با قانون و اهداف مشروع باشد. همچنین، ماده ۱۹ این میثاق به آزادی بیان می‌پردازد، اما آزادی بیان مشروط به محدودیت‌هایی است که در مواقع ضروری و برای حفظ امنیت ملی یا نظم عمومی اعمال می‌شود. در فضای دیجیتال، نظارت‌های گسترده تحت عنوان مبارزه با تروریسم، در صورتی که قوانین محدودکننده رعایت نشوند، می‌توانند تهدیدی برای حقوق فردی باشند(Farber, 2025: 11-12). در ضمن، مبارزه با تهدیدات تروریستی باید در چارچوب اصول حقوق بشری و احترام به حقوق فردی انجام شود.

تعارض میان حاکمیت ملی و ضرورت اقدامات فراملی در مبارزه با تروریسم دیجیتال چالشی جهانی است. کشورها حق کنترل فضای دیجیتال خود را دارند، اما تهدیدات تروریستی برخط که مرز نمی‌شناسند، نیازمند پاسخ‌های هماهنگ بین‌المللی است. این تضاد زمانی پیچیده‌تر می‌شود که قوانین ملی با اصول حقوق بشری مانند آزادی بیان و حریم خصوصی تداخل پیدا می‌کند. سازمان‌های بین‌المللی در تلاشند تا استانداردهای مشترک برای مقابله با این تهدیدات ایجاد کنند. حل این تعارض نیازمند همکاری جهانی و نظارت مؤثر بر سکوهای دیجیتال است(https://unicri.org). بنابراین، تدوین قواعد بین‌المللی برای مقابله با این دسته از فعالیت‌های تروریستی باید با احترام به حاکمیت ملی و صلاحیت سرزمینی کشورها همراه باشد. طبق منشور ملل متحد، مداخلات غیرمجاز باید پیشگیری شود، بنابراین همکاری‌های بین‌المللی باید امنیت را تأمین کرده و در عین حال حقوق حاکمیت ملی را رعایت کنند. این قواعد باید امکان تبادل امن داده‌ها، ایجاد پروتکل‌های امنیتی مشترک، و ظرفیت‌سازی در حوزه آموزش و فناوری را فراهم سازند.

تروریسم به‌عنوان تهدیدی برای حقوق بشر، آزادی‌ها و حق حیات، علاوه بر فجایع انسانی، به بی‌ثباتی دولت‌ها و تهدید صلح و توسعه منجر می‌شود. اسناد بین‌المللی تأکید دارند که حقوق بشر باید در تمامی اقدامات ضدتروریستی مدنظر قرار گیرد تا از نقض این حقوق پیشگیری شود(عباسی و همکاران، ۱۴۰۳: ۲۴۷). از اینرو، یکی از چالش‌های اساسی، برقراری توازن میان امنیت و حقوق بشر است. نظارت دیجیتال اگرچه ابزار موثری برای مقابله با تهدیدات است، ممکن

است حقوقی همچون حریم خصوصی، آزادی بیان و تجمع را محدود کند(https://necessaryandproportionate.org). محدودیت‌ها باید با رعایت اصول تناسب، ضرورت و نظارت قضایی اعمال شوند. برای اثربخشی همکاری‌های بین‌المللی، ایجاد سازوکارهای قانونی الزام‌آور و نهادهای نظارتی مستقل ضروری است تا از حقوق بشر حفاظت و اقدامات امنیتی شفاف شود.

هم‌افزایی بین‌المللی در قبال فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی به معنای تقویت هماهنگی میان دولت‌ها، سازمان‌های بین‌المللی، نهادهای نظارتی و فعالان بخش فناوری است. این همکاری‌ها باید شامل تبادل اطلاعات، اقدامات مشترک، تدوین استانداردهای بین‌المللی و ظرفیت‌سازی باشد و همواره با رعایت حقوق بشر و حاکمیت ملی همراه باشد. فقدان چارچوب‌های الزام‌آور جهانی، تفاوت نظام‌های حقوقی و شکاف‌های فناورانه ضرورت ایجاد ساختارهای بین‌المللی مستحکم با ضمانت اجرایی را نشان می‌دهد. مقابله مشروع با این نوع فعالیت‌ها تنها از طریق ترکیب همکاری بین‌المللی، چارچوب‌های قانونی الزام‌آور، نظارت مستقل و رعایت دقیق حقوق بشر امکان‌پذیر است. نهادهای بین‌المللی مانند یوروپل، اینترپل و کمیته مبارزه با تروریسم شورای امنیت باید در تدوین استانداردهای جهانی و تقویت زیرساخت‌های همکاری نقش محوری ایفا کنند. طراحی اقدامات باید تعادلی میان امنیت جهانی، آزادی‌های فردی، کرامت انسانی و حاکمیت ملی برقرار کند تا مشروعیت اقدامات ضدتروریستی و اعتماد متقابل میان کشورها حفظ شود. همچنین، نظارت بر فعالیت‌های برخط باید مطابق اصول حقوقی و رعایت حقوق بنیادین باشد تا از نقض حقوق بشر و آسیب‌پذیری کشورها پیشگیری شود و مقابله مؤثر با تهدیدات دیجیتالی تضمین گردد.

نتیجه‌گیری

سکوهای دیجیتال به دلیل ویژگی‌های فرامرزی خود، به چالشی مهم در نظارت بر فعالیت‌های تروریستی در فضای مجازی تبدیل شده‌اند. این واقعیت ضرورت تدوین مقررات جهانی هماهنگ را برجسته می‌سازد. این مقررات باید به‌گونه‌ای طراحی شوند که ضمن پاسخ‌گویی به چالش‌های امنیتی کشورهای مختلف، تهدیدات تروریستی را کاهش دهند. یکی از چالش‌های اصلی در این زمینه، حفظ تعادل میان امنیت ملی و حقوق فردی است؛ چرا که اقدامات امنیتی ممکن است به نقض حقوق بشر و آزادی‌های اساسی منجر شوند. به همین دلیل، رویکردهای نظارتی باید با دقت، شفافیت، و احترام به اصول حقوق بشر طراحی شوند.

در راستای مقابله با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی، توجه به حقوق بشر و تضمین جبران خسارت به قربانیان از اهمیت اساسی برخوردار است. نظارت مستقل و شفاف بر فرآیندهای ضدتروریستی، نه تنها به جلوگیری از سوءاستفاده‌ها کمک می‌کند، بلکه از نقض حقوق بشر و آزادی‌های فردی نیز پیشگیری خواهد کرد. همچنین، استفاده از فناوری‌های نوین مانند هوش مصنوعی و تحلیل داده‌ها می‌تواند در شناسایی تهدیدات و حذف محتوای تروریستی مؤثر واقع شود. این امر به‌ویژه در شرایطی که تروریست‌ها از فناوری‌های رمزگذاری برای مخفی‌سازی هویت خود استفاده می‌کنند، اهمیت پیدا می‌کند. بنابراین، همکاری‌های بین‌المللی در حوزه امنیت سایبری به‌ویژه در چارچوب «کنوانسیون بین‌المللی مقابله با جرایم سایبری (۲۰۲۴)» ضروری است. اشتراک‌گذاری اطلاعات و نظارت بر ترافیک اینترنتی می‌تواند در شناسایی و مقابله سریع‌تر با حملات تروریستی مؤثر باشد. با این حال، این همکاری‌ها باید مطابق با چارچوب‌های قانونی بین‌المللی باشد تا از بروز تعارضات حقوقی و سیاسی پیشگیری شود. در ضمن، برای مقابله مؤثر با

تروریسم دیجیتال، تدوین قوانین جامع و همکاری‌های بین‌المللی الزامی است. این قوانین باید از یک‌سو به حفاظت از امنیت دیجیتالی پرداخته و از سوی دیگر، حقوق بشر و آزادی‌های فردی را در فضای دیجیتال تضمین کنند.

برای مقابله مؤثر با فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی، نیاز به رویکردی جامع و چندجانبه وجود دارد. از نظر فنی، شرکت‌های فناوری باید شفافیت بیشتری در عملکرد الگوریتم‌های خود ایجاد کنند و از فناوری‌های هوش مصنوعی به‌منظور شناسایی و حذف محتوای تروریستی به‌گونه‌ای استفاده کنند که حریم خصوصی کاربران به خطر نیفتد. در حوزه حقوقی، تدوین قوانین بین‌المللی واضح و دقیق برای تعریف و مقابله با این پدیده بر اساس اصول حقوق بشر و آزادی‌های فردی ضروری است. همچنین، همکاری‌های حقوقی میان کشورها باید به‌منظور هم‌راستاسازی مقررات و تسهیل تبادل اطلاعات، تقویت شود. در زمینه امنیت، تقویت همکاری‌های بین‌المللی در قبال تهدیدات دیجیتالی و ایجاد مراکز تخصصی برای مبارزه با چنین امری از اهمیت ویژه‌ای برخوردار است. در نهایت، لازم است یک تعریف جهانی مشترک از فعالیت‌های تروریستی ارتکابی در سکوهای دیجیتالی پذیرفته شده و نظارت بر اقدامات ضدتروریستی با تأکید بر حفظ حقوق بشر و آزادی‌ها به‌صورت مؤثرتر صورت گیرد.

منابع

۱.منابع فارسی

کتاب‌ها

امامی، عادل. (۱۴۰۲). *تدابیر پلیس اروپا در پیکار با جرایم سایبری*. انتشارات آیین دادرسی، چاپ اول.

مقاله‌ها

امامی، عادل. (۱۴۰۲). *تدابیر پلیس اروپا در پیکار با جرایم سایبری*. انتشارات آیین دادرسی، چاپ اول.

جابری، مهران.، شهبازی، آرامش.، و جلالی، غلامرضا. (۱۴۰۱). بررسی چالش‌های حقوق بین‌المللی در مواجهه با حملات سایبری و ارائه راهکارهای مناسب جهت برون‌رفت از چالش‌های مذکور. *شهر ایمن، ۵(۲)، ۹۵-۱۲۸*.

قاسمی، غلامعلی.، و باقرزاده، سجاد. (۱۳۹۴). جایگاه حقوق بشر در مبارزه با سایبرتروریسم. *مجله حقوقی بین‌المللی، ۳۲(۵۲)، ۲۲۷-۲۵۴*.

رهامی، روح‌اله.، و محسنی جیهانی، فاطمه. (۱۴۰۳). تقابل آزادی بیان و توهین‌های مذهبی در نظام اروپایی حقوق بشر. *حقوق بشر*، ۱۹(۱)، ۲۲۹-۲۵۰.

رئیسی، لیلا. (۱۴۰۲). صیانت از حقوق شهروندی در فضای سایبر در پرتوی نسل سوم حقوق بشر (با تاکید بر کشور ایران). *مطالعات بین‌المللی، ۲۰(۳)، ۲۵-۶۲*.

رجبی‌تاج‌امیر، ابراهیم. (۱۴۰۱). ضرورت اتخاذ سیاست جنایی هماهنگ بین‌المللی پلیس در مقابله با جرایم سایبری. *تحقیقات حقوقی بین‌الملل، ۱۵(۵۵)، ۱-۲۳*.

عباسی، لیدا.، غضنفری، هنگامه.، و آزادبخت، فرید. (۱۴۰۳). استانداردهای حقوق بشر در چارچوب هنجاری مبارزه با تروریسم. *مطالعات بین‌المللی*، ۲۱(۳)، ۲۴۱-۲۵۶.

کاظم‌نژاد، شروین.، توکلی‌فر. (۱۴۰۳). حاکمیت داده و حق مالکیت بر داده‌های تولیدشده توسط هوش مصنوعی؛ چالش‌های حقوقی و الزامات سایبری. *حقوق سایبری*، ۱(۳)، ۶۱-۷۱.

گیوکی، آذر.، کفایی فر، محمدعلی.، و رضایی، محمدتقی. (۱۴۰۰). حملات سایبری و لزوم رعایت اصول اساسی حقوق بشر دوستانه در آنها. *تحقیقات حقوقی بین‌المللی، ۱۴(۵۱)، ۲۲۷-۳۰۵*.

مرادی، صادق.، شکرچی زاده، محسن.، نقش، امیررضا.، و مسعود، غلامحسین. (۱۴۰۱). تهدیدات و جرایم سایبری علیه امنیت و چالش‌های پیش‌رو. *فقه جزای تطبیقی، ۲(۱)، ۳۷-۵۰*.

مستوفیان، فخرالزمان. (۱۴۰۴). جایگاه اخلاق دیجیتال در توسعه نظام‌مند حقوق سایبری برای نسل چهارم فناوری‌ها. *حقوق سایبری*، ۲(۲)، ۲۹-۴۳.

میردامادی‌اصل، کامران. (۱۴۰۴). حقوق سایبری و چالش‌های تنظیم‌گری حملات سایبری ترکیبی علیه زیرساخت‌های حیاتی. *حقوق سایبری*، ۲(۱)، ۸۲-۹۴.

میربد، لیلا.، سلیمی، صادق.، نیاورانی، صابر.، و زمانی، سیدقاسم. (۱۴۰۱). ابعاد تعهد دولت‌ها به همکاری در وضع قواعد در واکنش به تروریسم سایبری. *حقوق پزشکی، ۱۶(۵)، ۵۲۶-۵۵۴.*

۲.منابع انگلیسی

Journal Articles

Alubaidi, A. (2023). Challenges to implementing the international digital law to protect digital rights. Journal of Law and Sustainable Development, 11(5), 1-41.

McKeever, D. (2021). Revisiting Security Council action on terrorism: New threats; (a lot of) new law; same old problems? Leiden Journal of International Law, 34(2), 441-470.

Özler, Ş. İ. (2018). The Universal Declaration of Human Rights at seventy: Progress and challenges. Ethics & International Affairs, 32(4), 395-406.

Celorio, R. (2024). The cyber world and human rights: Perspectives on international accountability strengthening human rights law in the digital domain. Stimson. (September 13) https://www.stimson.org/2024/the-cyber-world-and-human-rights-perspectives-on-international-accountability/

Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. Journal of Cyber Security Technology, 9(1), 28-78.

Calcara, G. (2021). Balancing international police cooperation: INTERPOL and the undesirable trade-off between rights of individuals and global security. Liverpool Law Review, 42(3), 111–142.

Calcara, G. (2019). INTERPOL's rules on the processing of data. Oxford International Organizations (OXIO), 441, 89-106.

Calleja, C. J. (2025). Assessing interference: Disrupting computer-enabled crime under Articles 8 and 10 of the European Convention on Human Rights. In W. Stol, L. Wacher Lentz, M. Naarttijärvi, I. M. Sunde, A. Jackson, L. Strikwerda, & J. Jansen (Eds.), Legal and ethical issues in digital policing: Policing in the digital society network yearbook (pp. 177-202), Boom.

Coche, E. (2018). Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online. Internet Policy Review, 7(4), 1–17.

Calcara, G. (2020). A transnational police network co-operating up to the limits of the law: Examination of the origin of INTERPOL. Transnational Legal Theory, 1–28.

Gottlieb, Y. (2011). Article 3 of Interpol's Constitution: Balancing international police cooperation with the prohibition on engaging in political, military, religious, or racial activities. Florida Journal of International Law, 23(4), 124-146.

Farber, S. (2025). The evolving nexus of cybercrime and terrorism: A systematic review of convergence and policy implications. Security Journal, 38(29), 1-23.

Ligeti, K., & Giuffrida, F. (2023). Europol. In K. Ambos & P. Rackow (Eds.), The Cambridge Companion to European Criminal Law (pp. 361–386). Cambridge University Press.

Galloro, L., & Guida, M. (2024). The limits of UN Security Council action in imposing economic sanctions under UN Charter and international law: The subtle balance between international security and human rights compliance. Charles University in Prague Faculty of Law Research Paper, 2024/III/4, 1–20.

Ezra, G. (2022). The UN Security Council and the saga of "global legislation." International Law Studies, 99(2), 93–141.

Voloshchuk, O., Kolesnyk, V., Shevchuk, A., Yushchyk, O., & Krainii, P. (2021). Human rights protection in the context of combating terrorism: Problems of finding the optimal balance. Amazonia Investiga, 10(45), 73–81.

Iftikhar, S. (2024). Cyberterrorism as a global threat: A review on repercussions and countermeasures. PeerJ Computer Science, 10, e1772.

Sendjaja, T., Irwandi, Prastiawan, E., & Suryani, Y. (2024). Cybersecurity in the digital age: Developing robust strategies to protect against evolving global digital threats and cyber attacks. International Journal of Science and Society, 6(1), 1008–1019.

Allahrakha, N. (2023). Balancing cyber-security and privacy: Legal and ethical considerations in the digital age. Legal Issues in the Digital Age, 4(2), 78–121.

Cristiano, F., Broeders, D., & Weggemans, D. (Eds.). (2020). Countering cyber terrorism in a time of 'war on words': Kryptonite for the protection of digital rights? The Hague Program for Cyber Norms, 12–14.

Popa Tache, C. E. (2024). The new international triangle: Human rights-digitalization-security. International Investment Law Journal, 4(1), 1–14.

Packin, N. G., & Volovelsky, U. (2024). Digital assets, anti-money laundering, and counter financing of terrorism: An analysis of evolving regulations and enforcement in the era of NFTs. The Cambridge Handbook of Law and Policy for NFTs, 78-102. Cambridge University Press.

Rahman, M. M., & Das, T. K. (2024). Countering cyberattacks: Gaps in international law and prospects for overcoming them. Journal of Digital Technologies and Law, 2(4), 973–1002.

Emmanuel, O. G., Adeyemo, B. W., & Wilson, S. (2025). Balancing surveillance and privacy: Legal frameworks governing technology in the digital age. Rivers State University Journal of Public Law, 13(1), 212–226.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(4), 1-32.

Clough, J. (2014). A world of difference: The Budapest Convention on Cybercrime and the challenges of harmonisation. Monash University Law Review, 40(3), 698–736.

Frosio, G., & Geiger, C. (2023). Taking fundamental rights seriously in the Digital Services Act's platform liability regime. European Law Journal, 29(1-2), 31–77.

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

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

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

Conference Papers (Proceedings)

Access Now. (2024, June). Wavering resolutions: The UN Security Council on digital rights: Digital, cyber, and human rights in the language of UN Security Council resolutions between 2001–2023. https://www.accessnow.org/wp-content/uploads/2024/07/UN-Security-Council-in-the-digital-age-technical-report.pdf

European Court of Human Rights. (2023, September 26). Yüksel Yalçınkaya v. Türkiye [GC], 15669/20. Judgment. https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22002-14187%22]}

https://www.ohchr.org/en/special-procedures/sr-terrorism

https://www.opensocietyfoundations.org/uploads/6bc0fc07-e5b7-4719-bc57-343dbd83f4bc/joint-civil-society-report-on-the-fundamental-rights-impact-of-the-eu-directive-on-combatting-terrorism-20211130.pdf?utm_source=chatgpt.com

https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_english.pdf

https://unicri.org/sites/default/files/2024-02/02_Principles_Resp_AI_Innovation_Feb24.pdf

United Nations. (2024, December 31). Resolution A/RES/79/243: United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes [Resolution]. General Assembly, Seventy-ninth session, Agenda item 108. https://docs.un.org/en/A/RES/79/243

United Nations. (2023, July 3). Resolution A/RES/77/298: The United Nations Global Counter-Terrorism Strategy: Eighth Review [Resolution]. General Assembly, Seventy-seventh session, Agenda item 121. https://docs.un.org/en/A/RES/77/298

https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf

https://www.uaces.org/sites/default/files/2024-07/Jaseff%20Raziel%20Yauri%20Miranda%20-%20paper.pdf
https://www.europol.europa.eu/about-europol/data-protection-transparency/relations-partners
https://acuns.org/wp-content/uploads/2022/07/2002_John_Holmes_Lecture_Sills.pdf
United Nations. (2023, December 22). A/RES/78/210: Terrorism and human rights (Seventy-eighth session, Agenda item 71(b)). General Assembly. https://docs.un.org/en/A/RES/78/210
https://www.gp-digital.org/wp-content/uploads/2016/05/Travel-Guide-to-the-Digital-World_Cybersecurity-Policy-for-HRD.pdf
United Nations. (2023, August 2). Terrorism and human rights: Report of the Secretary-General (A/78/269). General Assembly. https://docs.un.org/en/A/78/269
https://www.clingendael.org/sites/default/files/pdfs/The%20relationship%20between%20external%20and%20internal%20security.pdf
https://www.undp.org/sites/g/files/zskgke326/files/2023-10/undp-protecting-human-rights-in-constitutions.pdf
https://necessaryandproportionate.org/files/iachr-en-august2016.pdf