Energy Law Studies

Online ISSN: 2538-3140

Volume: 11, Issue:1

Homepage: https://jrels.ut.ac.ir

Spring & Summer 2025

Technological Crimes, Actions in the Realm of Digital Platforms; From Criminalization to Response in International Law

Peyman Namamian

Associate Professor of Criminal Law and Criminology, Faculty of Administrative Sciences and Economics, Arak University, Arak, Iran. Email: p-namamian@araku.ac.ir

Article Info

Article type:
Research Article

Manuscript received:
6 May 2025
final revision received:
24 June 2025
accepted:
28 August 2025
published online:
10 September 2025

Keywords:
Digital Security, Information and Communication Technology, Digital Technology, International Criminal Court, Technological Law, Technological Crimes

Abstract

With the advancement of technology and the increasing complexity of technological crimes, the criminalization of these offenses at the global level is essential. The development of new laws to identify, punish, and prevent these crimes, particularly in the areas of national security and human rights, is imperative. Addressing these crimes faces challenges, and strengthening international cooperation, as well as sharing information and technologies between countries, is crucial. In 2021, the United Nations General Assembly held meetings to prevent the threats posed by technological crimes and to enhance international cooperation in combating them. These meetings led to the drafting and adoption of the "United Nations Convention Against Cybercrime (2024)," which emphasizes the need for Response regarding technological threats and the development of international cooperation, particularly in identifying and prosecuting offenders. Given the transnational nature of these crimes, the International Criminal Court has jurisdiction over them. Additionally, during 2010 and 2011, UN expert meetings led to the drafting of a statute for the International Criminal Court to address these crimes. Designing a comprehensive framework for the criminalization, punishment, and Response of technological crimes for global implementation is vital. Due to the transnational nature of these crimes, a legal framework at the international level to combat them is essential. Moreover, existing laws are inadequate to address the challenges posed by technological advancements, thus requiring their revision and updating. This paper, therefore, emphasizes the importance of strengthening international cooperation and understanding the nature of technological crimes.

Cite this article: Namamian, Peyman (2025)" Technological Crimes, Actions in the Realm of Digital Platforms; From Criminalization to Response in International Law" Energy Law Studies, 11 (1): 167- 195. DOI:https://doi.com/10.22059/JRELS.2025.391901.583

Publisher: University of Tehran Press.

Introduction

In the current era, alongside the rapid expansion of modern technologies, technology-related crimes have also significantly increased, characterized by features such as the anonymity of perpetrators, high speed of execution, and the ability to transcend geographical borders. These crimes, especially in countries with weak information technology infrastructures, pose transnational and global threats. Therefore, effective countermeasures require the formulation of comprehensive laws, harmonized criminalization, and strengthened international cooperation. Technology-related crimes encompass a broad spectrum of criminal behaviors, including unauthorized access to computer systems, information theft, internet fraud, misuse of social networks, and violations of intellectual property rights. The technical complexity of these crimes, the lack of physical evidence, and their cross-border nature have made the identification and prosecution of offenders particularly challenging. Moreover, insufficient specialized knowledge among judges, the potential manipulation of digital evidence, and criminals' use of emerging technologies have reduced the effectiveness of criminal justice measures. Thus, the existence of dedicated laws, clear jurisdictional provisions, adaptation of legal procedures to the digital environment, and enhanced cooperation among states are indispensable.
At the international level, the United Nations has taken steps since the 1990s to combat technology-related crimes, including holding global summits on the information society in Geneva (2003) and Tunis (2005), and adopting relevant policy documents. Despite these efforts, until 2024, no binding international treaty specifically addressing cybercrime had been adopted. However, in December 2024, all UN member states ratified the *Comprehensive Convention on Cybercrime*, a treaty comprising 68 articles aimed at promoting global cooperation, facilitating the exchange of digital evidence, protecting victims, and ensuring respect for human rights. Besides the UN, organizations such as the International Telecommunication Union (ITU), Interpol, and the Group of Eight (G8) have also played effective roles by drafting specialized regulations, training relevant personnel, and establishing technical committees. These developments reflect the global community's movement toward establishing a coherent and effective legal framework for good governance in cyberspace.

Methodology

This study examines relevant legal texts and specialized literature through descriptive and analytical methods. By conducting detailed and systematic analyses of existing documents, it aims to achieve a comprehensive and deeper understanding of the nature of the agreements under investigation. The theoretical framework of the article is based on the principles of international criminal law, with a particular emphasis on transparency and the prevention of conflicts of interest.

Conclusion

The findings indicate that technology-related crimes, with their complex, transnational, and evolving nature, represent some of the most significant modern security threats. Given their cross-border nature, which weakens traditional sovereignty boundaries, effective responses require adopting coherent international legal strategies. Accordingly, it is recommended to prioritize the drafting of a binding international legal instrument focused on establishing a special criminal tribunal for technology-related crimes. Such a body could, based on recognized international norms, hold perpetrators of widespread cyberattacks and digital rights violations criminally accountable. Achieving this goal requires multilateral cooperation among states, harmonization of domestic laws with international standards, and the application of universal jurisdiction principles. Furthermore, institutions such as the International Telecommunication Union, Interpol, and the Council of Europe can play effective roles in coordination, policy formulation, and experience exchange. Ultimately, achieving good governance in the digital realm necessitates comprehensive regulatory frameworks, capacity building, intergovernmental information sharing, and the promotion of a cybersecurity culture to effectively counter emerging technological threats.

مطالعات حقوق انرژی

شاپا الکترونیکی: ۳۱۴۰-۲۵۳۸
دوره ۱۱، شماره ۱
بهار و تابستان ۱۴۰۴

Homepage: https://jrels.ut.ac.ir

جرایم فناورانه، کُنشی در گسترهٔ سکوهای دیجیتالی؛ از جرم‌انگاری تا پاسخ‌گذاری در حقوق بین‌المللی

پیمان نمامیان

دانشیار گروه حقوق کیفری و جرم‌شناسی، دانشکدهٔ علوم اداری و اقتصاد، دانشگاه اراک، اراک، ایران. رایانامه: p-namamian@araku.ac.ir

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۴/۲/۱۷
تاریخ بازنگری:
۱۴۰۴/۴/۴
تاریخ پذیرش:
۱۴۰۴/۶/۷
تاریخ انتشار:
۱۴۰۴/۶/۲۰

کلید واژه‌ها:
امنیت دیجیتالی، جرایم فناورانه، حقوق فناورانه، دیوان کیفری بین‌المللی، فناوری اطلاعات و ارتباطات، فناوری دیجیتالی.

چکیده

با پیشرفت فناوری و افزایش پیچیدگی جرایم فناورانه، جرم‌انگاری این دسته از جرایم در سطح جهانی ضرورتی انکارناپذیر است. تدوین قوانین جدید برای شناسایی، مجازات و پیشگیری از آن‌ها، به‌ویژه درزمینهٔ امنیت ملی و حقوق بشر، الزامی است. پاسخ‌گذاری به این جرایم با چالش‌های متعددی روبه‌روست و تقویت همکاری‌های بین‌المللی و اشتراک‌گذاری اطلاعات و فناوری میان کشورها، امری حیاتی است. در سال ۲۰۲۱، مجمع عمومی سازمان‌ملل نشست‌هایی برای پیشگیری از تهدیدهای ناشی از جرایم فناورانه و تقویت همکاری‌های بین‌المللی در مقابله با آن‌ها برگزار کرد. این نشست‌ها به تدوین و تصویب «کنوانسیون سازمان‌ملل‌متحد علیه جرایم سایبری، (۲۰۲۴)» انجامید که بر لزوم پاسخ‌گذاری به تهدیدهای فناورانه و توسعهٔ همکاری‌های بین‌المللی، به‌ویژه در شناسایی و تعقیب مرتکبان، تأکید دارد. باتوجه به ماهیت فرامرزی این جرایم، دیوان کیفری بین‌المللی صلاحیت رسیدگی به آن‌ها را دارد. افزون‌براین، در سال‌های ۲۰۱۰ و ۲۰۱۱، نشست‌های کارشناسی سازمان‌ملل‌متحد به تهیهٔ پیش‌نویس اساسنامهٔ دیوان کیفری بین‌المللی برای رسیدگی به این جرایم انجامید. طراحی چهارچوب جامع برای جرم‌انگاری، مجازات و پاسخ‌گذاری به جرایم فناورانه به‌منظور اجرایی‌شدن جهانی، امری انکارناپذیر است. به‌هر روی، باتوجه به ماهیت فرامرزی جرایم فناورانه، ایجاد چهارچوبی حقوقی در سطح بین‌المللی برای مقابلهٔ مؤثر با آن‌ها ضروری است. درعین‌حال، قوانین کنونی توانایی پاسخ‌گذاری به چالش‌های ناشی از پیشرفت فناوری را ندارند و ازاین‌رو، اصلاح و روزآمدی آن‌ها لازم است. بنابراین، مقالهٔ پیش‌رو بر اهمیت تقویت همکاری‌های بین‌المللی و شناسایی ماهیت جرایم فناورانه، تأکید دارد.

استناد: نمامیان، پیمان (۱۴۰۴). «جرایم فناورانه، کُنشی در گسترهٔ سکوهای دیجیتالی؛از جرم‌انگاری تا پاسخ‌گذاری در حقوق بین‌المللی»، *مطالعات حقوق انرژی*،۱۱ (۱)،۱۹۵ – ۱۶۷.

http//doi.org/10.22059/JRELS.2025.391901.583

ناشر: مؤسسه انتشارات دانشگاه تهران.

مقدمه

در دهۀ گذشته، جهان شاهد افزایش قابل‌توجه مقررات حاکم بر اینترنت و سکوهای دیجیتالی بوده است. با گسترش سریع اینترنت در آغاز قرن بیست‌ویکم، قانون‌گذاران در سراسر جهان ملزم شدند سکوهای دیجیتالی را با قوانین و مقررات ملی خاص تطبیق دهند، تا شکاف قانونی موجود که با مقررات فعلی قابل رفع نبود، جبران شود. بدیهی است که با ظهور اینترنت، بخش زیادی از نگرانی‌های امنیتی بین‌المللی بر این فضا متمرکز شده است (Khokhlov & Korotayev, 2022: 389).

جرایم فناورانه در فضای دیجیتال به‌دلیل ویژگی‌هایی، ازجمله دسترسی آسان، ناشناسی و سرعت بالا، امکان ارتکاب جرم بدون محدودیت جغرافیایی را فراهم می‌کنند. این تهدیدها به دلیل ضعف‌های فناورانۀ یک کشور ممکن است به تهدیداتی جهانی بدل شوند. برای مقابله با آن‌ها، ضرورت دارد که جرم‌انگاری هماهنگ در سطح ملی و بین‌المللی انجام و همکاری‌های جهانی تقویت شود؛ زیرا چنانکه گفته شد، فضای مجازی جهانی به بستری مناسب برای ارتکاب جرایم فناورانه بدل شده است.

جرایم فناورانه به‌عنوان تهدیدی فراملی که از مرزها و قلمروهای حاکمیتی دولت‌ها عبور می‌کند، بحرانی‌ترین چالش‌ها را در جامعۀ اطلاعاتی ایجاد می‌کند؛ ازجمله امنیت داده‌های دیجیتالی، حفاظت از سامانه‌های اطلاعاتی و پیشگیری از بهره‌گیری مخرب و غیرقانونی از فناوری‌های ارتباطات و اطلاعات توسط مجرمان فناورانه، گروه‌های تروریستی یا بازیگران دولتی (Awwad Alkharman & Hassan, 2023: 17-18). با افزایش جرایم فناورانه، کاربران عمده اینترنت، به‌ویژه سازمان‌ها، اهمیت حفاظت از فضای اینترنت را دریافته‌اند. به‌طور گسترده، امنیت فناورانه[1] مورد توجه و بررسی قرار گرفته و درنتیجه، سازمان‌ها اقدام به توسعۀ نرم‌افزارهایی کرده‌اند که به‌سادگی قادر به شناسایی بدافزارها و ویروس‌ها هستند؛ چه هدف از آن سرقت داده‌های سازمان باشد یا نباشد.[2]

---

۱. «امنیت فناورانه» برای تأمین امنیت اطلاعات دیجیتال و سامانه‌های اطلاعاتی در جامعۀ اطلاعاتی طراحی و اجرا می‌شود. این مفهوم شامل اقدامات اجتماعی، قانونی، نظارتی و فناوری است که به‌منظور تضمین یکپارچگی، محرمانگی، دسترسی و امنیت اطلاعات دیجیتال، به ایجاد اعتماد و امنیت در فضای دیجیتال کمک می‌کند.

۲. برای‌مثال، چین برای حفاظت از اسرار دولتی خود، از فناوری رمزنگاری به‌منظور ذخیرۀ امن داده‌های حساس استفاده می‌کند. براین‌اساس، «قانون رمزنگاری جمهوری خلق چین» که در چهاردهمین جلسۀ کمیتۀ دائمی سیزدهمین کنگرۀ ملی جمهوری خلق چین با ۴۴ ماده در تاریخ ۲۶ اکتبر ۲۰۱۹ به تصویب رسید، بدین‌وسیله اعلام شد و از اول ژانویۀ ۲۰۲۰ لازم‌الاجرا گردید. این قانون، ضمن الزام به ذخیره و انتقال کلیۀ اسرار دولتی با استفاده از رمزگذاری مشترک اصلی، به‌منظور توسعه و استفاده از رمزگذاری تجاری مجاز و تنظیم شده است.

باوجوداین، نگارنده در این پژوهش بر آن است تا با تکیه بر اهدافی همچون بررسی ساختار شناختی جرایم فناورانه، مطالعهٔ فرایند و سیر تکامل تحولات حاکم بر آن و البته امکان‌سنجی پاسخگویی به این جرایم، به این پرسش پاسخ دهد: «باتوجه به تحولات مستمر و گسترش فزایندهٔ جرایم فناورانه در عصر دیجیتال، چگونه می‌توان با بهره‌گیری از ظرفیت‌های موجود در نظام حقوق بین‌الملل، نسبت به پیشگیری و مقابلهٔ مؤثر با این جرایم اقدام و سازوکارهای کارآمدی در این راستا طراحی و اجرا کرد؟».

این پژوهش با استفاده از روش توصیفی–تحلیلی و تأکید بر منابع کتابخانه‌ای و اسنادی تدوین شده است تا اهداف پژوهش تحقق یابد و پاسخ مناسبی به پرسش یادشده داده شود.

۱. تعریف و شناخت مفهومی

شناسایی و تعقیب جرایم فناورانه در دنیای دیجیتال، به دلیل سرعت بالای تحولات فناوری و عقب‌ماندگی قوانین، با چالش‌های زیادی روبه‌روست. این جرایم اغلب ردپایی آشکار ندارند و از مرزهای جغرافیایی فراتر می‌روند. عواملی مانند ناآگاهی مقامات قضایی، دست‌کاری شواهد دیجیتال و بهره‌گیری مرتکبان از فنون پیشرفته، فرایند شناسایی و پیگیری این جرایم را پیچیده‌تر می‌سازد.

بنابراین، تثبیت مفهوم جرایم فناورانه در قالب یک تعریف واحد، امری بسیار پیچیده است. یکی از صاحب‌نظران در این زمینه، ضمن اشاره به پیشرفت‌های فناورانه و دشواری ارائهٔ یک تعریف دقیق برای جرایم فناورانه، یادآور می‌شود که یک تعریف جامع باید شامل دانش یا بهره‌گیری از ابزارهای رایانه‌ای در ارتکاب جرم باشد. در دهمین کنگرهٔ سازمان‌ملل‌متحد دربارهٔ جرم و برخورد با مجرمان، جرایم فناورانه از دو منظر تعریف شد؛ تعریف نخست یا محدود، جرایم فناورانه را شامل هرگونه رفتار غیرقانونی دانسته که با استفاده از عملیات الکترونیکی با هدف قرار دادن امنیت یک سامانهٔ رایانه‌ای و داده‌های پردازش‌شده توسط آن انجام می‌شود (Ramos, 2014: 1). تعریف دوم یا تعریف گسترده، جرایم فناورانه را به‌عنوان هر رفتار غیرقانونی می‌داند که در چهارچوب روابط یا از طریق به‌کارگیری یک سامانه یا شبکهٔ رایانه‌ای ارتکاب می‌یابد.[1]

در سطح جهانی، جرایم فناورانه دامنهٔ گسترده‌ای دارند و شامل اقدامات مالی، فعالیت‌های مرتبط با محتوای رایانه‌ای و همچنین اقدامات علیه محرمانگی، یکپارچگی و دسترسی به سامانه‌های رایانه‌ای می‌شوند. مفهوم جرایم فناورانه اصولاً اعمالی را دربرمی‌گیرد که از پیش

1. United Nations Office on Drugs and Crime (UNODC). Comprehensive Study on Cybercrime. Draft prepared for the second meeting of the open-ended intergovernmental expert group on cybercrime by the UNODC.

جرم محسوب می‌شوند، اما با استفاده از رایانه یا وسایل الکترونیکی، یا با هدف بهره‌گیری رایانه برای ارتکاب جرم انجام می‌گیرند. نمونه‌های جرایم فناورانه گسترده و متنوع‌اند. این جرایم شامل تروریسم فناورانه، کلاهبرداری فناورانه، جعل رایانه‌ای، دسترسی غیرقانونی به رایانه، رهگیری غیرقانونی داده‌ها یا ترافیک شبکه و غیره می‌شوند. از تعاریف پیش‌گفته می‌توان نتیجه گرفت که رایانه‌ها، شبکه‌ها و داده‌ها، ازجمله اهداف اصلی این جرایم هستند (Shaweorcid & McAndrew, 2023: 552-553).

در تلاش برای تعریف جرایم فناورانه، ضروری است که گستره و مفهوم این جرایم به‌طور موشکافانه مورد بررسی قرار گیرد. درک این تفاوت، از ماهیت جرم ناشی می‌شود. جرم می‌تواند به‌عنوان عملی غیرقانونی تعریف شود که به شخص یا دارایی دیگری آسیب می‌رساند یا در آن مداخله می‌کند. گفتنی است که جرایم فناورانه، اعمالی هستند که با استفاده از رایانه علیه دولت انجام می‌شوند؛ درحالی‌که تخلفات فناورانه، رفتارهای مدنی نادرستی هستند که با استفاده از رایانه یا ابزارهای الکترونیکی (یا با هدف قرار دادن رایانه) انجام و باعث آسیب شخصی به فرد یا گروهی از افراد می‌شوند (Aaron, 2019: 6).

به‌هر روی، می‌توان گفت شماری از اندیشمندان، «جرم فناورانه» را به‌عنوان جرمی تعریف می‌کنند که در آن از فناوری‌های رایانه‌ای برای ارتکاب رفتارهای مجرمانه استفاده می‌شود. این مفهوم طیف گسترده‌ای از فعالیت‌های غیرقانونی را دربرمی‌گیرد؛ از کلاهبرداری گرفته تا حمله به سامانه‌های دولتی (Kovacich & Jones, 2006: 99).

جرایم فناورانه به‌دلیل برخورداری از ویژگی‌های پیچیده و پیشرفته، خطرات و تهدیدهای متعددی را برای کاربران، سازمان‌ها و دولت‌ها به‌وجود می‌آورند. مصادیق این جرایم شامل جرایم سایبری مانند هک، سرقت اطلاعات و دسترسی غیرمجاز به سامانه‌ها و داده‌های حساس؛ جرایم مالی دیجیتال همچون فریب‌های برخط، کلاهبرداری اینترنتی و سوءاستفاده از سکوهای مالی برای ارتکاب جرم؛ جرایم در شبکه‌های اجتماعی از قبیل افترا، نشر اطلاعات نادرست، آزار و تهدید کاربران از طریق این سکوها؛ و جرایم مرتبط با مالکیت معنوی نظیر نقض حقوق کپی‌رایت، سرقت نرم‌افزار و توزیع محتوای غیرمجاز به‌صورت دیجیتال است. این تنوع در مصادیق نشان می‌دهد که هریک از انواع جرایم فناورانه مستلزم رویکردی اختصاصی و توجه ویژه به ابعاد امنیتی خاص خود هستند.

۲. سیر تحولات و تکامل

ردیابی نخستین جرم ارتکابی در فضای مجازی ممکن نیست، اما شناسایی اولین حملهٔ بزرگ در این فضا، یا نخستین تهاجم گسترده‌ای که با بهره‌گیری از رایانه و اینترنت موجودیت جهان را

تحت‌تأثیر قرار داده است، امری ناممکن به نظر نمی‌رسد (Crootof, 2018: 588). بنابراین، پیشینهٔ جرایم فناورانه را می‌توان در دههٔ ۱۹۷۰ جست‌وجو کرد؛ زمانی که مجرمان از طریق خطوط تلفن مرتکب جنایاتی به نام Phreaking[1] شدند (Raven, 2002: 1). این اقدام مبتنی‌بر استفاده از صداهای خاصی بود که امکان برقراری تماس‌های تلفنی رایگان را فراهم می‌کرد. *جان درپیر*[2]، با نام مستعار *کاپیتان کرانچ*[3] و مهندس پیشین نیروی‌هوایی ایالات‌متحده، هنگام کار در *سیلیکون‌ولی*[4] در سال ۱۹۷۱ دریافت که سوت‌های تبلیغاتی اهدایی در جعبه‌های معروف به Cap'n Crunch Cereal، همان بسامدهای صوتی را تولید می‌کنند که در سامانه‌های سوئیچینگ تلفن به‌کار می‌روند. او سپس دستورالعمل‌هایی دربارهٔ چگونگی استفاده از این سوت‌ها برای برقراری تماس‌های راه دور رایگان منتشر کرد (Crootof, 2018: 591).

در سال ۱۹۸۱، *ایان مورفی*[5]، ملقب به *کاپیتان زاپ*[6]، نخستین فردی بود که به‌عنوان مرتکب جرایم فناورانه محاکمه و مجازات شد. وی با هک کردن شبکهٔ تلفن همراه شرکت تلفن و تلگراف امریکا، ساعت داخلی آن‌ها را تغییر داد (Mifitzgerald, 2004: 1). افزون‌براین، در سال ۱۹۸۹ اولین بانک ملی شیکاگو[7]، قربانی یک سرقت رایانه‌ای هفتاد میلیون دلاری شد. این رخداد که بازتاب گسترده‌ای در سطح جهانی داشت، سرانجام در سال ۱۹۹۰ به تصویب «قانون سوءاستفاده از رایانه» در بریتانیا انجامید؛ قانونی که برای نخستین‌بار دسترسی غیرمجاز به سامانه‌های رایانه‌ای را جرم‌انگاری کرد (Groot, 2020: 1).

جرایم فناورانه در گذر زمان دچار تحول چشمگیری شده‌اند و امروزه طیف گسترده‌ای از رفتارهای مجرمانه را دربرمی‌گیرند؛ ازجمله حملات سرویس، انتشار بدافزارها، تخریب سامانه‌های رایانه‌ای، سرقت و نقض حقوق مالکیت معنوی، جاسوسی اقتصادی و نفوذ غیرمجاز به شبکه‌ها. با پیشرفت فناوری، فرصت ارتکاب این جرایم افزایش یافته است. در اوایل دههٔ ۱۹۸۰، همزمان با گسترش فناوری‌های رایانه‌ای، سازمان‌های مجری قانون با چالشی جدی درزمینهٔ کمبود قوانین کیفری برای مقابله با این جرایم روبه‌رو شدند. در آغاز شکل‌گیری جرایم فناورانه، بیشتر این جرایم از سوی کارکنان فردی و حملات فیزیکی به سامانه‌ها ارتکاب می‌یافت. از دههٔ ۱۹۹۰ به

---

۱. Phreaking در دههٔ ۱۹۶۰ آغاز شد؛ زمانی‌که کشف شد سوت‌های خاصی می‌توانند گام ۲۶۰۰ هرتز مورد استفاده در سامانه‌های سیگنالینگ تلفن در ایالات‌متحده را تکرار کنند؛

- "Phreaking, Telecom Security, History & Techniques, Britannica". www.britannica.com.

2. John Draper
3. Captain Crunch
4. Silicon Valley
5. Ian Murphy
6. Captain Zap
7. National Bank of Chicago

بعد، اینترنت به عامل اصلی افزایش جرایم رایانه‌ای تبدیل شد و مجرمان از روش‌های غیرمجاز برای دسترسی به سامانه‌ها استفاده کردند. در این دوره، کلاهبرداری‌های مرتبط با کارت‌های اعتباری به‌صورت چشمگیری افزایش یافت و سرقت هویت نیز در آغاز قرن بیست‌ویکم به یکی از شایع‌ترین انواع جرایم فناورانه بدل شد. در سال ۲۰۰۸، کلاهبرداری دیجیتال به سریع‌ترین شکل رشد در میان جرایم فناورانه تبدیل شد. همچنین، جرایم مرتبط با تلفن‌های همراه در سال‌های اخیر رو به افزایش بوده و نشان‌دهندهٔ ظهور نوع جدیدی از فعالیت‌های مجرمانه است. این جرایم را می‌توان به چهار دستهٔ اصلی تقسیم کرد:

۱. رایانه به‌مثابه هدف جرم؛

۲. رایانه به‌عنوان موضوع جرم، یعنی رایانه محیط وقوع جرم است؛

۳. رایانه به‌عنوان ابزار ارتکاب جرم؛

۴. استفاده از نمادهای رایانه‌ای برای انجام فعالیت‌های غیرقانونی (Casey, 2011: 43-44).

جرایم فناورانه در طول زمان در قالب سه نسل متفاوت تکامل یافته‌اند. نسل اول که در دهه‌های ۱۹۶۰ تا ۱۹۸۰ میلادی شکل گرفت، عمدتاً محدود به «جرایم رایانه‌ای» بود و تمرکز آن بر خود سامانه‌های رایانه‌ای قرار داشت[1]. نسل دوم، در دهه‌های ۱۹۸۰ تا ۱۹۹۰ تحت عنوان «جرایم علیه داده‌ها» شناخته شد و محوریت آن بر داده‌ها و اطلاعات موجود در سامانه‌ها بود[2]. نسل سوم، معروف به «جرایم مجازی»، با تلفیق فناوری رایانه و مخابرات همراه شد و ویژگی شاخص آن استفاده از شبیه‌سازی و مجازی‌سازی است[3]؛ در این نسل، رایانه به‌عنوان ابزار ارتکاب جرم به‌کار گرفته می‌شود و جرایم عمدتاً در فضای الکترونیکی و اطلاعاتی رخ می‌دهند.

در چهار دههٔ نخست شکل‌گیری فناوری‌های رایانه‌ای، جرایم مرتبط با آن محدود بودند، اما با گسترش فضای مجازی، پنج دستهٔ اصلی جرایم فناورانه پدید آمده که هریک شامل چندین عنوان متفاوت است. ظهور اینترنت چالش‌های امنیتی گسترده‌ای برای دولت‌ها به‌همراه داشته و ضعف فناوری در یک کشور می‌تواند تهدیدهایی جدی برای دیگر کشورها ایجاد کند؛ به‌ویژه هنگامی که زیرساخت‌های اینترنتی به‌صورت نادرست برای اقدامات مخرب و جنگ‌های مجازی مورد استفاده قرار گیرند (Reveron & Savage, 2023: 237-239).

1.https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=10075&context=dissertations

2. https://www.scribd.com/document/810589436/A-Brief-History-of-Cyberspace

3. https://www.igi-global.com/chapter/unmasking-virtual-crimes/375598

۳. از جرایم سنتی تا جرایم فناورانه؛ معیارها و مؤلفه‌ها

گرایش غالب پژوهشگران و نویسندگان این است که جرایم فناورانه را به‌عنوان نهادی مجزا از جرایم سنتی بررسی کنند؛ هرچند این جرایم معمولاً توسط همان دسته از مجرمان و به دلایلی مشابه ارتکاب می‌یابند. باوجوداین، جرایم فناورانه از نظر شیوه‌های ارتکاب کاملاً مشابه جرایم سنتی نیستند. دو تفاوت قابل‌توجه در این زمینه وجود دارد: اول، شناسایی و تشخیص وقوع جرم در فضای فناورانه دشوارتر است و دوم، ردیابی و تعیین مقصر به‌طور منظم با پیچیدگی و چالش‌های بیشتری همراه است (Ayswariya, G. K & Aswathy, 2017: 131-132).

یکی از تفاوت‌های مهم میان جرایم فناورانه و جرایم سنتی، اثبات جرم است. در جرایم سنتی، کلاهبرداران معمولاً از طریق آثار فیزیکی مانند اثر انگشت یا سایر شواهد ملموس، ردپایی از جنایت برجای می‌گذارند. بااین‌حال، مرتکبان جرایم فناورانه به اینترنت به‌عنوان ابزار اصلی ارتکاب جرم وابسته هستند و برخلاف جرایم سنتی، ردپای فیزیکی مانند اثر انگشت یا سایر تأییدات ملموس از خود باقی نمی‌گذارند تا بتوان از آن‌ها به‌عنوان مدرک استفاده کرد. درنتیجه، پلیس علمی در تأیید و اثبات چنین جرایمی که می‌تواند به محکومیت مرتکبان بینجامد، معمولاً با مشکلات فراوانی روبه‌رو هستند؛ زیرا مجرمان می‌توانند هویت خود را بدون هیچ مانعی تغییر دهند.

دومین تفاوت که از تفاوت نخست برمی‌خیزد، این است که مرتکبان جرایم فناورانه اغلب از نام‌های مجعول بهره می‌برند و از مناطق دوردست اقدام می‌کنند؛ بنابراین شناسایی هویت واقعی مرتکبان و ایمن‌سازی آن‌ها در اغلب موارد زمان بیشتری می‌طلبد (Krannenbarg, 2018: 1).

جرایم فناورانه از جرایم سنتی متمایز هستند؛ زیرا مرتکبان آن می‌توانند در مقیاسی وسیع‌تر عمل کنند[1]؛ برای‌مثال، یک سارق سنتی ممکن است تنها بتواند در هفته به یک یا دو بانک دستبرد بزند؛ درحالی‌که مرتکب جرم فناورانه می‌تواند همزمان صدها وب‌سایت را هدف قرار دهد[2]. این ویژگی، نشان‌دهندهٔ افزایش خطر و ماهیت غیرقابل کنترل جرایم فناورانه است[3]. افزون‌براین، این نوع جرایم پیش از تدوین سیاست‌ها و مقررات مربوطه به‌سرعت گسترش می‌یابند و حتی پس از وضع قوانین، شناسایی و تعقیب مرتکبان برای اجرای کامل مقررات با مشکلات جدی روبه‌روست.

1. Protection Group International. (2018). What is the Difference between Cybercrime and Traditional Crime? PGI 2018 <https://www.pgitl.com/blog/what-is-the-difference-between-cyber-crime-and-traditional-crime/>
2. International Telecommunication Union (ITU). (2011). ICT Facts and Figures. ITU, 2011 https://www.itu.int/ITU-D/ict/facts/2011/material/ICTFactsFigures2011.pdf&ved
3. 0Orji, U.J. (2012). Cybersecurity Law and Regulation. 1 Wolf Legal Publishers.

بنابراین، اذعان می‌شود که جرایم سنتی و فناورانه تفاوت‌های اساسی و بنیادینی با یکدیگر دارند. جرایم سنتی معمولاً در مقیاس محدود و فیزیکی رخ می‌دهند؛ درحالی‌که جرایم فناورانه قادرند در زمانی کوتاه و به‌طور گسترده و حتی جهانی گسترش یابند. در جرایم سنتی، دسترسی به محل وقوع جرم مستلزم حضور فیزیکی است؛ اما در جرایم فناورانه، مرتکب می‌تواند از هر نقطه‌ای از جهان به سامانه‌ها دسترسی پیدا کند. این نوع جرایم نیازمند فناوری‌های پیشرفته و پیچیده هستند و مقابله با آن‌ها مستلزم همکاری بین‌المللی، تدوین قوانین نوین و هماهنگی میان ساختارهای حاکمیتی است. ازاین‌رو، تهدیدات ناشی از جرایم فناورانه به‌مراتب وسیع‌تر و پیچیده‌تر از جرایم سنتی است.

۴. پاسخ‌گذاری‌های کیفری در قلمرو حقوق بین‌الملل؛ ضرورت تدوین چهارچوب‌های قانونی و تقویت همکاری‌های بین‌المللی برای مقابله با جرایم فناورانه

وجود چهارچوب قانونی برای مقابله با جرایم فناورانه امری ضروری است تا امکان پیشگیری و پاسخ‌گذاری مؤثر فراهم شود. چنین چهارچوبی معمولاً شامل جرم‌انگاری، همکاری بین‌المللی، تعیین صلاحیت قضایی و اختیارات رویه‌ای است. در سطح ملی، تمرکز بر جرم‌انگاری جرایم فناورانه، موضوع‌های مرتبط با شواهد الکترونیکی، تعیین صلاحیت دادگاه‌ها و تضمین همکاری جهانی است. در سطح بین‌المللی نیز، تلاش‌های گسترده‌ای برای ایجاد یک چهارچوب قانونی هماهنگ انجام شده که در دهۀ گذشته موفقیت‌هایی را به‌همراه داشته است.

تجزیه‌وتحلیل اسناد حقوقی چندجانبۀ بین‌المللی نشان می‌دهد که این اسناد، با وجود اندکی تفاوت، دارای مقرراتی مشترک هستند[1]. این اسناد تأثیر شگرفی بر شکل‌گیری مقررات ملی داشته‌اند؛ زیرا بسیاری از کشورها از آن‌ها به‌عنوان مقررات نمونه استفاده می‌کنند. ازاین‌رو، پاسخ‌گذاری نهادهای بین‌المللی به جرایم فناورانه و همچنین چهارچوب قانونی تعیین‌شده توسط آن‌ها، معیار سنجش قوانین ملی در این زمینه هستند.

1. United Nations Office On Drugs and Crime (UNODC). (2013). Comprehensive Study on Cybercrime. p..xix]
https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

۴. ۱. تقویت همکاری‌های فراملی در پرتو ظرفیت‌های حقوقی سازمان‌ملل‌متحد و نهادهای بین‌المللی

در گذشته، واکنش‌های بین‌المللی به جرایم فناورانه مشابه سایر پدیده‌های مجرمانه بود، اما ویژگی‌های خاص این جرایم، ازجمله ابعاد فراملی و چالش‌های قضایی، ماهیتی بی‌سابقه به آن‌ها بخشیده است. باوجود تلاش‌های سازمان‌ملل‌متحد برای مقابله با این چالش‌ها، تاکنون موفق به ایجاد یک توافق‌نامهٔ الزام‌آور بین‌المللی در این زمینه نشده است؛ هرچند اقدامات متعددی برای مقابله با جرایم فناورانه از سوی این نهاد انجام گرفته است. بنابراین، ممکن است چنین برداشت شود که سازمان‌ملل‌متحد اولین اقدام رسمی خود دربارهٔ جرایم فناورانه را در سپتامبر ۱۹۹۰ انجام داد؛ زمانی‌که مجمع عمومی این سازمان، پس از هشتمین کنگرهٔ پیشگیری از جرم و رفتار با مجرمان، قطعنامهٔ ۱۲۱/۴۵ را تصویب کرد. براساس این قطعنامه، سازمان‌ملل‌متحد در سال ۱۹۹۴، کتابچهٔ راهنمای پیشگیری و کنترل جرایم رایانه‌ای را منتشر کرد[1]. همچنین، در سال ۲۰۰۰، موضوع جرایم رایانه‌ای در دهمین کنگرهٔ سازمان‌ملل‌متحد درزمینهٔ پیشگیری از جرم و رفتار با مجرمان که در وین برگزار شد، مورد بحث و بررسی قرار گرفت.[2]

در سال ۲۰۰۱، سازمان‌ملل‌متحد با تصویب قطعنامه‌هایی درزمینهٔ مقابله با سوءاستفادهٔ مجرمانه از فناوری‌های اطلاعاتی، از کشورهای عضو دعوت کرد تا «در صورت لزوم، از دستاوردهای کمیسیون پیشگیری از جرم و عدالت کیفری و همچنین سایر سازمان‌های بین‌المللی و منطقه‌ای، در توسعهٔ چهارچوب‌های قانونی، سیاستی و اجرایی ملی برای مقابله با سوءاستفادهٔ مجرمانه از فناوری اطلاعات بهره گیرند».[3]

در ۲۱ دسامبر ۲۰۰۱، مجمع‌عمومی سازمان‌ملل‌متحد با تصویب قطعنامهٔ شمارهٔ ۱۸۳/۵۶، برگزاری اجلاس جهانی در مورد جامعهٔ اطلاعاتی را تأیید کرد که براساس آن نخستین اجلاس سران در سال ۲۰۰۳ در ژنو برگزار شد[4]. در این اجلاس، بیانیه‌ای با محوریت ایجاد اعتماد و

1. United Nations. UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5)
http://www.uncjin.org/Documents/EighthCongress.html
2. United Nations Crime and Justice Information Network (UNCJIN). (2000). Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. A/CONF.185/15, No. 165,
http://www.uncjin.org/Documents/congr10/15e.pdf
3. Combating Criminal Misuse No 1, UN Doc A/RES/55/63; Combating Criminal Misuse No 2, UN Doc A/RES/56/121, para. 1
4. World Summit on the Information Society, GA Res 56/183, UN GAOR, 56th sess, 90th plenmtg, Agenda Item 95(c), UN Doc A/RES/56/183 (31 January 2002, adopted 21 December 2001).

امنیت در بهره‌گیری از فناوری‌های اطلاعات و ارتباطات صادر شد؛ این بیانیه بر ضرورت پیشگیری، شناسایی و واکنش مؤثر در برابر جرایم فناورانه و سوءاستفاده از فناوری اطلاعات و ارتباطات تأکید داشت[۱]. همچنین، در سال ۲۰۰۲ مجمع‌عمومی سازمان‌ملل‌متحد قطعنامهٔ شمارهٔ ۶۳/۵۵ را تصویب کرد که بر بررسی رویکردهای موجود در سازمان‌های بین‌المللی و منطقه‌ای برای مقابله با جرایم فناورانه و نیز ترویج گفت‌وگو میان دولت و بخش خصوصی درزمینهٔ ارتقای ایمنی و اعتماد در فضای مجازی تأکید داشت[۲]. در همان سال، «پروتکل اختیاری کنوانسیون حقوق کودک در مورد فروش کودکان، فحشا و هرزه‌نگاری کودکان» نیز به تصویب رسید[۳]. پس از یازدهمین کنگرهٔ سازمان‌ملل‌متحد درزمینهٔ پیشگیری از جرم و عدالت کیفری که در سال ۲۰۰۵ در بانکوک برگزار شد، مجمع‌عمومی سازمان‌ملل بیانیه‌ای صادر کرد که در آن بر ضرورت تقویت و گسترش همکاری‌ها برای پیشگیری و مقابله با جرایم فناورانه تأکید شده بود[۴]. در همان سال، دومین اجلاس جهانی نیز برگزار شد که نتیجهٔ آن تصویبِ دستور کار *تونس* برای جامعهٔ اطلاعاتی بود. این سند، دولت‌ها را به تدوین مقررات لازم برای تحقیق و تعقیب جرایم فناورانه فراخواند.[۵]

در سال ۲۰۰۵، سازمان‌ملل‌متحد کتابچه‌ای با عنوان «ناامنی اطلاعات؛ راهنمای بقا در سرزمین‌های ناشناختهٔ تهدیدهای سایبری و امنیت سایبری»[۶] منتشر کرد. این اثر، بر ضرورت

1. International Telecommunication Union (ITU). (2003). World Summit on the Information Society, Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium. (Document No WSIS-03/GENEVA/DOC/4-E, 12 December 2003), p. 40; International Telecommunication Union. (2003). World Summit on the Information Society, 'Plan of Action' (Document No WSIS-03/GENEVA/DOC/5-E, 12 December 2003).
2. A/RES/56/121.
http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf
3. United Nations, Treaty Series, Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography; 18 January 2002, No. 2753, vol. 2171, p. 227;
https://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=iv-11-c&chapter=4&clang=_en
4. Follow-up to the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/RES/60/177 (20 March 2006).
5. International Telecommunication Union, World Summit on the Information Society, 'Tunis Agenda for the Information Society', WSIS-05/TUNIS/DOC/6(Rev. 1)-E, (18 November 2005) 40.
6. United Nations, Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber Threats and Cyber Security (Ict Task Force Series), July 1, 2005, https://unesdoc.unesco.org/ark:/48223/pf0000143889

پیشگیری و پاسخ‌گذاری به حملات سایبری و امنیت اطلاعات تأکید داشت و تمرکز آن بر حفاظت و امنیت فضای مجازی بود.

در ۲۱ دسامبر ۲۰۱۰، مجمع‌عمومی سازمان‌ملل قطعنامهٔ شمارهٔ ۲۱۱/۶۴ را به‌عنوان بخشی از ابتکار جهانی در جهت ایجاد فرهنگ امنیت در فضای مجازی به تصویب رساند.[1] این قطعنامه به دو قطعنامهٔ اصلی دربارهٔ جرایم فناورانه (قطعنامه‌های شمارهٔ ۶۳/۵۵ و ۱۲۱/۵۶) و همچنین دو قطعنامهٔ محوری در مورد امنیت فضای مجازی (قطعنامه‌های شمارهٔ ۲۳۹/۵۷ و ۱۹۹/۵۸) اشاره دارد.

بااین‌حال، ضرورت تدوین یک کنوانسیون جهانی برای مقابله با جرایم سایبری نخستین‌بار در سال ۲۰۱۰، در جریان دوازدهمین کنگرهٔ سازمان‌ملل‌متحد دربارهٔ پیشگیری از جرم و عدالت کیفری که در سالوادور برزیل برگزار شد، مطرح گردید[2]. در پی این طرح، سازمان‌ملل انجام یک مطالعهٔ جامع را در دستور کار قرار داد که هدف آن بررسی چالش‌های ناشی از جرایم فناورانه و نحوهٔ پاسخ‌دهی کشورهای عضو، جامعهٔ بین‌المللی و بخش خصوصی به این پدیده بود. این مطالعه در چهارچوب کمیسیون پیشگیری از جرم و عدالت کیفری و در بازهٔ زمانی ۲۰۱۱ تا ۲۰۱۳ انجام گرفت و محورهای آن شامل تبادل اطلاعات در مورد قوانین ملی، شناسایی بهترین شیوه‌ها، ارائهٔ کمک‌های فنی و تقویت همکاری‌های بین‌المللی بود. هدف نهایی از این اقدام، ارزیابی گزینه‌های تقویت سازوکارهای موجود و پیشنهاد پاسخ‌های حقوقی نوین ملی و بین‌المللی یا سایر پاسخ‌های مربوط برای مقابله با جرایم فناورانه بود.

موضوع تدوین کنوانسیون جهانی جرایم سایبری در کمیسیون پیشگیری از جرم و عدالت کیفری در آوریل ۲۰۱۳[3] مورد بررسی قرار گرفت. در ادامهٔ این روند، مجمع‌عمومی سازمان‌ملل‌متحد به‌موجب قطعنامهٔ شمارهٔ ۷۱/۱۸۷ که در ۱۷ دسامبر ۲۰۱۸ تصویب شد، دستور کار جدیدی با عنوان «مقابله با استفاده از فناوری اطلاعات و ارتباطات برای اهداف مجرمانه»[4] را که از سوی فدراسیون روسیه پیشنهاد شده بود، پذیرفت[5]. همچنین در سال ۲۰۲۱، مجمع‌عمومی

1. A/RES/64/211 (17 March 2010)

2. Rep. of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, UN Doc A/CONF.213/18 at 56–7 [202]– [204] (18 May 2010)

3. Commission on Crime Prevention and Criminal Justice, Strengthening International Cooperation to Combat Cybercrime, UN ESCOR, 22nd sess, Agenda Item 7, UN Doc d E/CN.15/2013/L.14 (2 April 2013) para 3.

۴. این عبارت، دامنه‌ای به‌مراتب گسترده‌تر از مفهوم متعارف «جرم فناورانه» ترسیم می‌کند و با هیچ‌یک از تعاریف پیشین هم‌خوانی ندارد. قرار بود نشست کمیتهٔ موقت با جلسه‌ای سه‌روزه در آگوست ۲۰۲۰ برگزار شود تا دربارهٔ طرح کلی و روش‌های فعالیت‌های بعدی توافق شود.

5. Countering the use of information and communications technologies for criminal purposes, A/RES/73/187 (14 January 2019)

سازمان‌ملل قطعنامهٔ شمارهٔ ۲۹۱/۷۵ را تصویب کرد که بر حفاظت از اهداف آسیب‌پذیر در برابر تهدیدهای سایبری تأکید داشت.[۱]

به‌هرحال، کنوانسیون سازمان‌ملل‌متحد درزمینهٔ جرایم سایبری، پس از پنج سال مذاکرات فشرده، در تاریخ ۲۴ دسامبر ۲۰۲۴ با اجماع تمامی ۱۹۳ عضو مجمع‌عمومی سازمان‌ملل به تصویب رسید. هدف اصلی این کنوانسیون، تقویت همکاری‌های بین‌المللی در مقابله با جرایم ارتکابی از طریق فناوری‌های اطلاعات و ارتباطات و تسهیل تبادل شواهد الکترونیکی مرتبط با جرایم مهم است. این سند حقوقی شامل ۶۸ ماده و یادداشت‌های تفسیری مربوط به مواد ۲، ۱۷، ۲۳ و ۳۵ بوده و به‌منظور اجرای قطعنامه‌های شمارهٔ (۲۰۱۹)۲۴۷/۷۴[۲] و (۲۰۲۱)۲۸۲/۷۵[۳] مجمع‌عمومی سازمان‌ملل‌متحد در تاریخ ۲۶ مه ۲۰۲۱ به تصویب رسید[۴]. کنوانسیون مزبور، به‌عنوان معاهدهٔ الزام‌آور بین‌المللی شناخته می‌شود که قرار است از سال ۲۰۲۵ میلادی برای امضا در شهر *هانوی*[۵] گشوده شود و نود روز پس از تصویب آن توسط دست‌کم چهل دولت عضو، لازم‌الاجرا گردد[۶]. محورهای اصلی آن شامل ارتقای همکاری‌های بین‌المللی در مقابله با جرایمی مانند دسترسی غیرمجاز به داده‌ها، کلاهبرداری‌های رایانه‌ای و تهدید علیه زیرساخت‌های حیاتی، تبادل اطلاعات میان دولت‌ها، حمایت از بزه‌دیدگان و رعایت اصول حقوق بشر در فضای دیجیتال است (De Silva De Alwis, 2025: 29-32).

1. United Nations. (2021, June 30). *Resolution 75/291: The United Nations Global Counter-Terrorism Strategy: Seventh review*. Seventy-fifth session. https://docs.un.org/en/A/RES/75/291
2. https://docs.un.org/en/A/RES/74/247
3. https://docs.un.org/en/A/RES/75/282
4. United Nations General Assembly. (2024, December 24). Resolution adopted by the General Assembly on the report of the Third Committee (A/79/460, para. 15): 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. https://docs.un.org/en/A/RES/79/243
5. Hanoi

۶. این کنوانسیون که نخستین سند جهانی در حوزهٔ عدالت کیفری طی بیش از دو دههٔ اخیر محسوب می‌شود، نقطه‌عطفی در اقدامات جامعهٔ بین‌المللی برای مقابلهٔ مؤثر با جرایم سایبری و گسترش همکاری‌های چندجانبه در این زمینه تلقی می‌گردد. شهر هانوی، پایتخت جمهوری سوسیالیستی ویتنام، در سال ۲۰۲۵ میزبان مراسم امضای این سند بین‌المللی بود. این کنوانسیون، چهارچوبی حقوقی برای تقویت همکاری‌های قضایی و پلیسی میان دولت‌ها، توسعهٔ ظرفیت‌های فنی و نهادی و ارتقای امنیت فضای دیجیتال فراهم می‌سازد؛ به‌گونه‌ای که مرتکبان جرایم سایبری در قبال رفتارهای خود پاسخگو باشند:

- United Nations Office on Drugs and Crime. (2025, February 19). The Road to Hanoi: Opening for signature of the UN Convention against Cybercrime. Conference Room 8, UNHQ. https://unodaweb-meetings.unoda.org/public/2025-02/Concept%20note%20The%20Road%20to%20HN%20-%20OEWG.pdf

اتحادیهٔ بین‌المللی مخابرات که در سال ۱۸۶۵ در *ژنو* تأسیس شد، در دو مرحله در سال‌های ۲۰۰۳ در ژنو و ۲۰۰۵ در تونس، برنامه‌هایی تحت عنوان «بیانیهٔ اصول و اقدام ژنو»[۱] و «تعهد و دستور کار تونس»[۲] برای جامعهٔ اطلاعاتی برگزار کرد. در برنامهٔ اقدام ژنو از دولت‌ها خواسته شد تا با همکاری بخش خصوصی اقداماتی را در راستای پیشگیری، شناسایی و پاسخ‌گذاری به جرایم فناورانه و استفاده غیرقانونی از فناوری اطلاعات و ارتباطات اتخاذ کنند. این اقدامات شامل موارد زیر بود:

الف- تدوین دستورالعمل‌هایی برای حمایت از تلاش‌های جاری درزمینهٔ مقابله با جرایم فناورانه؛

ب- ترویج همکاری و کمک متقابل؛

ج- تقویت حمایت نهادی در سطح بین‌المللی برای پیشگیری، کشف و بازیابی از حوادث سایبری؛

د- تشویق به آموزش و افزایش آگاهی.[۳]

در دستور کار تونس برای جامعهٔ اطلاعاتی، نیاز به همکاری بین‌المللی در مقابله با جرایم فناورانه مورد تأکید قرار گرفت و به رویکردهای حقوقی موجود، ازجمله کنوانسیون شورای اروپا راجع‌به جرایم سایبری و قطعنامه‌های مجمع‌عمومی سازمان‌ملل‌متحد اشاره شد[۴]. این دستور کار بر اهمیت تعقیب جرایم فناورانه در حوزه‌های مختلف قضایی تأکید کرد.[۵]

---

1. WSIS Geneva Plan of Action, WSIS-03/GENEVA/DOC/5-E, (12 December 2003), available from https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0005!!MSW-E.doc

2. Tunis Commitment, WSIS-05/TUNIS/DOC/7 –E (18 November 2005), available from https://www.itu.int/wsis/docs2/tunis/off/7.doc; Tunis Agenda For The Information Society, Document: WSIS-05/TUNIS/DOC/6(Rev.1)-E (18 November 2005) available from https://www.itu.int/wsis/docs2/tunis/off/6rev1.doc

3. International Telecommunication Union (ITU). (2014). Understanding Cybercrime: Phenomena, Challenges and Legal Response, p.125, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/cybercrime2014.pdf

4. see: http://www.itu.int/wsis/c5/, and also the meeting report of the second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: http://www.itu.int/osg/csd/cybersecurity/pgc/2007/ events/docs/meetingreport.pdf and the meeting report of the third Facilitation Meeting for WSIS Action Line C5, 2008, available from http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_ Report_June_2008.pdf.

5. Rep. of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, Held in San Jose, from 25 to 27 May 2009, UN Doc A/CONF.213/RPM.1/1 (26 May 2009) 10 [41].

به‌منظور سنجش و توسعهٔ اقدامات و راهبردها باتوجه به اهداف دستور کار جهانی امنیت مجازی، دبیرکل اتحادیهٔ بین‌المللی مخابرات گروهی از کارشناسان را برای بررسی اقدامات حقوقی اتخاذشده درزمینهٔ جرایم فناورانه تشکیل داد. این بررسی شامل رویکردهای گوناگون منطقه‌ای و بین‌المللی نسبت به جرایم فناورانه، تجزیه‌وتحلیل مقررات کیفری، اسناد رویه‌ای و مقررات مربوط به مسئولیت ارائه‌دهندگان خدمات اینترنتی بود. افزون‌براین، اتحادیهٔ بین‌المللی مخابرات چندین کنفرانس منطقه‌ای برگزار کرده است تا به‌طور ویژه به موضوع جرایم فناورانه پرداخته شود.[1]

درراستای بهبود اجرای توصیه‌های سران کشورهای گروه هشت در سال ۱۹۹۶، این گروه پنج گروه فرعی ایجاد کرد. یکی از این گروه‌ها «کمیتهٔ فرعی جرایم فناورانهٔ پیشرفته»[2] است که در سال ۱۹۹۷ تشکیل شد و به بررسی جرایم اینترنتی می‌پردازد. در جریان نشست وزیران

1. 23-25 November 2009 (Santo Domingo, Dominican Republic): http://www.itu.int/ITUD/cyb/events/2009/santo-domingo; 23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cyber security Forum for Asia-Pacific; 4-5 June 2009 (Tunis, Tunisia): 2009 ITU Regional Cyber security Forum for Africa and Arab States; 18-22 May 2009 (Geneva, Switzerland): WSIS Forum of Events 2009, including Action Line C5 dedicated to building confidence and security in the use of ICTs, and activities for child online protection; 7-9 September 2009 and 6-7 April 2009 (Geneva, Switzerland): ITU-D Rapporteur's Group Meeting on Question 22/1 on Securing Information and Communication Networks; 7-9 October 2008 (Sofia, Bulgaria): ITU Regional Cyber security Forum for Europe and the Commonwealth of Independent States (CIS); 25-28 August 2008 (Lusaka, Zambia): ITU Regional Cyber security Forum for Eastern and Western Africa; 15-18 July 2008 (Brisbane, Australia): ITU Regional Cyber security Forum for Asia Pacific and Seminar on the Economics of Cyber security; 18-21 February 2008 (Doha, Qatar): ITU Regional Workshop on Frameworks for Cyber security and Critical Information Infrastructure Protection (CIIP) and Cyber security Forensics Workshop; 27-29 November 2007 (Praia, Cape Verde): ITU West Africa Workshop on Policy and Regulatory Frameworks for Cyber security and CIIP, 29-31 October 2007 (Damascus, Syria): ITU Regional Workshop on E-Signatures and Identity Management; 16-18 October 2007 (Buenos Aires, Argentina): ITU Regional Workshop on Frameworks for Cyber security and Critical Information Infrastructure Protection (CIIP); 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cyber security and Critical Information Infrastructure Protection (CIIP); 2831 August 2007 (Hanoi, Vietnam): ITU Regional Workshop on Frameworks for Cyber security and Critical Information Infrastructure Protection (CIIP).

2. Subcommittee on High-tech Crimes

دادگستری و امور داخلی گروه هشت در واشنگتن، اصول ده‌گانه و برنامهٔ اقدام ۱۰ ماده‌ای برای مقابله با جرایم فناورانهٔ پیشرفته به تصویب رسید[۱] که شامل موارد زیر است:

الف- برای کسانی که از فناوری اطلاعات سوءاستفاده می‌کنند، نباید پناهگاه امنی وجود داشته باشد؛

ب- تحقیق و تعقیب جرایم بین‌المللی فناورانهٔ پیشرفته باید بین همهٔ کشورهای ذی‌ربط هماهنگ شود، صرف‌نظر از اینکه آسیب در کدام قلمرو رخ داده است؛

ج- برای رسیدگی به جرایم فناورانهٔ پیشرفته، کارکنان مجری قانون باید آموزش دیده و مجهز شوند.

در سال ۱۹۹۹، گروه هشت در کنفرانس وزیران مبارزه با جرایم سازمان‌یافتهٔ فراملی در مسکو، برنامه‌های ویژه‌ای را برای مقابله با جرایم فناورانهٔ پیشرفته طراحی کرد[۲]. افزون‌براین، گروه هشت در کنفرانسی که در سال ۲۰۰۰ در پاریس برگزار شد، به‌صورت ویژه به موضوع جرایم فناورانه پرداخت و خواستار اقدام برای پیشگیری از ایجاد یا تخریب پناهگاه‌های دیجیتالی غیرقانونی شد[۳]. این کارگاه بر اجرای تعهدات مربوط به نگهداری و حفاظت از داده‌ها به‌عنوان سازوکار جایگزین تأکید داشت.[۴]

جرایم فناورانه بار دیگر در نشست سال ۲۰۰۹ وزیران دادگستری و امور داخلی در رُم ایتالیا مورد بحث قرار گرفت. اعلامیهٔ نهایی این نشست خواستار اجرای دستورالعملی برای بستنِ وب‌گاه‌هایی شد که توسط سازمان‌های بین‌المللی برای بهره‌برداری از هرزه‌نگاری کودکان منتشر و روزآمد می‌شدند.[۵] در سال ۲۰۱۰ نیز، «بیانیهٔ موسکوکا» درخصوص نگرانی‌ها دربارهٔ تهدید

1. Regarding the G8 activities in the fight against cybercrime, see also: United Nations Conference on Trade and Development, Information Economy Rep. 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, p.233, available from http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf

2. Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organized Crime, Moscow, (19-20 October 1999).

3. G8 Officials and the Private Sector Meet to Discuss Combating Computer Crime G8 Government/Private Sector High-level Meeting on High-tech Crime (May 24th 2001) (Press Release) available from
https://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-3.html

4. Rep. for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety and Security in Cyberspace, Tokyo, (May 2001).

5. Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, p. 7, available from
http://www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

فزایندهٔ جرایم فناورانه درزمینهٔ جرایم ترویستی صادر شد و خواستار تشدید مبارزه با این جرایم گردید.[۱]

اینترپل با تحقیق درزمینهٔ جرایم نوظهور، بررسی آخرین فنون آموزشی و توسعهٔ ابزارهای پلیسی نوین، رهبری رویکرد بین‌المللی علیه جرایم فناورانه را برعهده دارد. همچنین، این سازمان نقاط مرجع ملی برای جرایم مرتبط با رایانه را ایجاد کرده است که اساساً سامانه‌ای برای هشدار اولیه میان واحدهای تحقیقات جرایم فناوری اطلاعات فراهم می‌کند تا مسیرهای امن و مناسب اینترپل برای استفاده توسط واحدهای تخصصی تحقیقات جرایم فناوری اطلاعات و تبادل اطلاعات در کوتاه‌ترین زمان ممکن ارائه شود. باتوجه به ماهیت فراملی و بین‌المللی جرایم فناورانه، همکاری اینترپل، به‌ویژه در روند حل این جرایم، ضروری است. برای اهداف این همکاری، همهٔ کشورهای عضو اینترپل میزبان یک دفتر مرکزی ملی اینترپل هستند که مجریان حقوق داخلی آن‌ها را با سایر کشورها و نیز دبیرخانهٔ عمومی اینترپل مرتبط می‌کند.[۲]

از دیگر نوآوری‌های ایجادشده توسط سازمان بین‌المللی پلیس جنایی (اینترپل)، راه‌اندازی «مجتمع جهانی برای نوآوری»[۳] در سال ۲۰۱۴ است. این مجتمع یک سازمان هماهنگ‌کنندهٔ جهانی است که در سنگاپور واقع شده و هدف اصلی آن کمک به کشف و پیشگیری از جرایم فناورانه با تمرکز بر تحقیق و توسعه است (Gabey, 2013: 1). همچنین، برای مقابله با افزایش تهدیدهای ناشی از ارتکاب جرایم فناورانه در جنوب شرق آسیا، اینترپل در ژوئیهٔ ۲۰۱۸ «میز قابلیت مجازی آسه‌آن»[۴] را تأسیس کرد. بااین‌حال، در سال ۲۰۲۰، نام این میز به «میز عملیات جرایم سایبری آسه‌آن»[۵] تغییر یافت تا عملکرد و ارتباط عملیاتی آن به‌صورت مطلوب‌تری منعکس شود[۶]. در همین راستا، اینترپل طیف گسترده‌ای از دوره‌های آموزشی ارائه می‌دهد که با

1. G8 Summit 2010.Muskoka Declaration, available from http://www.g7.utoronto.ca/summit/2010muskoka/communique.html.

۲. گفتنی است که مرکز تلفیق مجازی به‌منظور هماهنگی و تسهیل تحقیقات و عملیات فراملی در حوزهٔ جرایم فناورانه ایجاد شده است و فعالیت‌هایی مانند به‌اشتراک‌گذاری اطلاعات و ارائهٔ راهنمایی در تحقیقات این جرایم را دربرمی‌گیرد. این مرکز، فضای امنی برای مجریان قانون و صنعت فراهم می‌کند تا اطلاعات مجازی را برای مقابله با جرایم فناورانه به‌اشتراک بگذارند. همچنین، اینترپل از تشکیل گروه‌های کاری منطقه‌ای برای تبادل تجربیات و توسعهٔ بهترین شیوه‌ها حمایت می‌کند. افزون‌براین، جرایم مالی و فناورانهٔ پیشرفته در کنار سایر جرایم، ازجمله تروریسم و قاچاق انسان، به‌عنوان اولویت‌های اصلی فعالیت‌های این سازمان تعیین شده‌اند.

3. Global Complex for Innovation (IGCI)
4. ASEAN Cyber Capability Desk
5. ASEAN Cybercrime Operations Desk
6. Interpol, Supporting collective actions against Cybercrime in Southeast Asiahttps: //www.interpol.int/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-OperationsDesk

هدف پاسخگویی به نیازهای شرکت‌کنندگان، موضوع‌هایی مانند روندهای نوظهور در جرایم فناورانه، فنون تحقیق و پزشکی قانونی دیجیتالی را پوشش می‌دهد.

۴. ۲. ارتقای امنیت فناورانه در چهارچوب اسناد و معاهده‌های بین‌المللی

در چهارچوب کنوانسیون‌های بین‌المللی، تهدیدهای ناشی از جرایم فناورانه مورد توجه قرار گرفته است. کنوانسیون‌های بین‌المللی، ازجمله «کنوانسیون سرکوب بمب‌گذاری‌های تروریستی (۱۹۹۷)»[۱] و «پیش‌نویس کنوانسیون جامع مقابله با تروریسم بین‌المللی (۲۰۰۰)»[۲] به‌طور ضمنی تهدیدهای فناورانه را درنظر گرفته‌اند؛ هرچند نیاز به اصلاحات و تفسیرهای جدید برای پوشش بهتر این تهدیدها احساس می‌شود.

درحال‌حاضر تنها سند بین‌المللی الزام‌آور دربارهٔ جرایم فناورانه، «کنوانسیون بوداپست در مورد جرایم سایبری (۲۰۰۱)»[۳] است[۴]. این کنوانسیون به‌عنوان سندی تعیین‌کننده در مورد بهترین رویهٔ بین‌المللی، از شناسایی و پذیرش گسترده‌ای برخوردار است[۵]. افزون‌براین، کنوانسیون دولت‌های عضو را ملزم می‌کند تا ضمن جرم‌انگاری مجموعه‌ای از جرایم فناورانه و اعطای اختیارات رویه‌ای به مقامات قضایی کیفری، تأمین مدارک الکترونیکی هر جرمی را تضمین کنند و در همکاری‌های بین‌المللی شرکت مؤثر داشته باشند. ازاین‌رو، در سپتامبر ۲۰۱۷، مذاکرات برای دومین پروتکل الحاقی به‌منظور افزایش همکاری بین‌المللی و دسترسی به شواهد در فضای

1. United Nations. (1997, December 15). *International Convention for the Suppression of Terrorist Bombings*. https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-9&chapter=18&clang=_en

2. United Nations. (2000, August 28). *Draft comprehensive convention on international terrorism* (A/C.6/55/1). General Assembly, Fifty-fifth session, Sixth Committee. https://digitallibrary.un.org/record/422477?v=pdf

3. The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols, https://www.coe.int/en/web/cybercrime/the-budapest-convention

4. European Treaty Series - No. 185. Convention on Cybercrime, Council of Europe, Details of Treaty No.185 available from http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

5. Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, European Treaty Series - No. 189, available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800 8160f

مجازی آغاز شد[۱]. این اقدام می‌تواند پاسخی به انتقادها نسبت به سازوکارهای کنوانسیون باشد که انتظار می‌رفت شرایط دسترسی به شواهد بین‌المللی از سال ۲۰۲۱ فراهم شود.[۲]

ضرورت وجود «قانون نمونهٔ مشترک‌المنافع در مورد جرایم رایانه‌ای و مرتبط با رایانه»، نخستین‌بار در جلسهٔ سوم تا هفتم می ۱۹۹۹ وزیران مشترک‌المنافع در بندر اسپانیا، ترینیداد و توباگو مطرح شد. هدف از آن، حمایت از کشورهای مشترک‌المنافع در پدیدآوردن یک سند حقوقی به‌منظور ایجاد چهارچوبی برای جرم‌انگاری و تعقیب جرایم رایانه‌ای بود. ازاین‌رو، وزیران به دبیرخانه دستور دادند گروهی از کارشناسان برای بررسی محتوای چنین قانون نمونه‌ای تشکیل شود. دبیرخانه، ضمن ایجاد این گروه کارشناسی، در ژوئیهٔ ۲۰۰۰ دستور تهیهٔ پیش‌نویس دستورالعمل قانون یادشده را صادر کرد[۳]. به‌علاوه، جلسات متعددی در مارس و نوامبر سال ۲۰۰۲ برگزار شد که بالاخره به تهیهٔ پیش‌نویس نهایی انجامید. سپس این پیش‌نویس توسط وزیران قانون کشورهای مشترک‌المنافع تصویب شد و برای بهره‌برداری توسط سایر کشورهای عضو توصیه گردید (Alex, 2014: 1).

«پیش‌نویس کنوانسیون بین‌المللی برای تقویت حفاظت در قبال جرایم سایبری و تروریسم» در پی نشستی که در ششم و هفتم دسامبر ۱۹۹۹ در دانشگاه استنفورد برگزار شد، تهیه گردید[۴]. این پیش‌نویس با هدف تشویق به شناسایی جهانیِ جرایم اساسی در فضای مجازی و ایجاد توافق جهانی برای همکاری در تحقیق، استرداد و تعقیب مرتکبان جرایم فناورانه طراحی شده است. مواد ۶ و ۱۱ پیش‌نویس استنفورد، مساعدت‌های حقوقی متقابل و اجرای قانون را برای تقویت همکاری دولت‌های عضو در تحقیقات فراهم می‌کند. براین‌اساس، دولت‌های عضو ملزم به تبادل اطلاعات، کمک در گردآوری و حفظ شواهد، دستگیری مرتکبان احتمالی جرایم

1. Council of Europe, Acceding to the Budapest Convention on Cybercrime: Benefits, Version 15 May 2017 available from https://rm.coe.int/cyber-buda-benefits-v6/168072bddc

۲. هرچند اصطلاح «جرم فناورانه» به‌معنای جرمی است که در اینترنت یا از طریق آن رخ می‌دهد، اما چهارچوب عملی کنوانسیون فراتر از این محدودیت است و شامل جرایمی می‌شود که با استفاده از رایانه انجام می‌شوند یا به‌طورکلی رایانه‌ها در آن‌ها دخالت دارند.

3. The Commonwealth Model Law on Computer and Computer Related Crime, Commonwealth Secretariat, LMM (02)17, Model Law on Computer and Computer Related Crime, pp.1 & 3, available:
http://www.veritaszim.net/sites/veritas_d/files/Commonwealth%20Model%20Law%20on%20Computer% 20and%20Computer%20Related%20Crime.pdf

4. Draft International Convention to Enhance Protection from Cyber Crime and Terrorism,
https://web.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf

فناورانه، تعقیب یا استرداد آن‌ها و اجرای استانداردهای بین‌المللی توافق‌شده در حوزهٔ اجرای قانون و امنیت هستند.[۱]

ماهیت «پیش‌نویس قانون صلح و امنیت در فضای سایبری» (موسوم به پروتکل جهانی راجع‌به امنیت فضای مجازی و جرایم فناورانه) این است که جرایم علیه صلح و امنیت در فضای دیجیتال از طریق یک کنوانسیون یا پروتکل، به‌عنوان جرایم تحت شمول حقوق بین‌الملل معرفی شوند. این امر نیازمند اقدامات امنیتی دیجیتال و توسعهٔ راهبردهایی است برای ایجاد یک پروتکل جهانی درزمینهٔ امنیت و جرایم فناورانه؛ به‌گونه‌ای که با قوانین ملی و منطقه‌ای موجود هماهنگ و قابل‌اجرا باشد (Stein & Solange, 2009: 1). البته مقابله با بهره‌گیری از فناوری‌های جدید و نوظهور برای اهداف تروریستی به‌عنوان رویکردی قابل‌تأمل و مورد اهتمام، در نشست ویژه کمیتهٔ مبارزه با تروریسم شورای امنیت سازمان‌ملل‌متحد[۲] که در ۲۸ و ۲۹ اکتبر ۲۰۲۲ در دهلی‌نو برگزار شد، مورد بحث و بررسی قرار گرفت.[۳]

«قانون امنیت سایبری اتحادیهٔ اروپا (۲۰۱۹)»[۴] و «مقررات عمومی حفاظت از داده‌ها (۲۰۱۸)»[۵] نیز تأکید فراوانی بر امنیت فناورانه دارند. این مقررات، به‌ویژه در شرایط تهدیدهای فناورانه، اهمیت ویژه‌ای یافته‌اند. رفتارهای مخرب در فضای مجازی از سوی بازیگران دولتی و غیردولتی از نظر مقیاس، شدت، پیچیدگی و تأثیرگذاری رو به افزایش است. دراین‌زمینه، اتحادیهٔ اروپا در نشست شورای خود در ۱۸ نوامبر ۲۰۲۴، بیانیه‌ای موسوم به «بیانیهٔ اتحادیهٔ اروپا و

---

۱. مادهٔ ۷ پیش‌نویس استنفورد، تعهدی برای تعقیب یا استرداد پیش‌بینی می‌کند که برعهدهٔ همهٔ دولت‌هایی است که یک مجرم احتمالی در قلمرو آن‌ها حضور دارد.

۲. شورای امنیت سازمان‌ملل‌متحد در سال ۲۰۱۷ با قطعنامهٔ شمارهٔ ۲۳۴۱ از دولت‌ها خواست که حملات سایبری را به‌عنوان جرایم جدی شناسایی کنند:

- United Nations. (2017, February 13). *Resolution 2341 (2017)*: Adopted by the Security Council at its 7882nd meeting. https://docs.un.org/S/RES/2341(2017)

در قطعنامهٔ شمارهٔ ۲۳۹۶ نیز بر تقویت همکاری‌های بین‌المللی برای مقابله با تهدیدات سایبری تأکید شد:

- United Nations. (2017, December 21). *Resolution 2396 (2017)*: Adopted by the Security Council at its 8148th meeting. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2396.pdf

3. The Delhi Declaration, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_specialmeeting_ outcome_document.pdf.

4. EU Cybersecurity Act, Regulation (EU) 2019/881, 2019 O.J. (L 151) 15, http://data.europa.eu/eli/reg/2019/881/oj.

5. General Data Protection Regulation (GDPR), https://gdpr-info.eu/

کشورهای عضو آن در مورد درک مشترک از کاربرد حقوق بین‌الملل در فضای مجازی» را تصویب کرد.[۱]

«کنوانسیون سازمان‌ملل‌متحد علیه جرایم سایبری (۲۰۲۴)»[۲] به‌منظور تقویت همکاری‌های بین‌المللی در قبال تهدیدهای فناورانه، تصویب شد. این کنوانسیون باوجود چالش‌هایی همچون نگرانی‌های حقوق بشری، کشورهای امضاکننده را به همکاری در گردآوری شواهد الکترونیکی و مقابله با تهدیدهای فناورانه ملزم می‌کند.

۴. ۳. ضرورت تشکیل دیوان کیفری بین‌المللی برای رسیدگی به جرایم فناورانه

هیچ‌یک از چالش‌های جهانی کنونی، ازجمله تغییرات اقلیمی و جرایم فناورانه، نمی‌تواند به‌تنهایی توسط یک کشور یا بازیگر قدرتمند حل شود. این پدیده‌های پیچیده نیازمند چهارچوبی برای همکاری مؤثر بین‌المللی هستند و در این چهارچوب، حقوق بین‌الملل الگویی برای جامعهٔ بین‌المللی فراهم می‌کند (Henkin, 1978: 93). به‌منظور تحقق یک رویکرد جهانی واقعی برای حاکمیت امنیت دیجیتالی که ناهنجاری‌ها و اقدامات غیرقانونی در جامعهٔ اطلاعاتی جهانی را کاهش می‌دهد، نمی‌توان بیش از حد بر ضرورت ایجاد یک چهارچوب حقوقی بین‌المللی در حوزهٔ امنیت دیجیتالی تأکید کرد (Hadji-Janev & Aleksoski, 2021: 117-119). ایجاد دیوان بین‌المللی برای رسیدگی به جرایم فناورانه امری ضروری است تا افراد مسئول نقض حقوق بین‌الملل در این حوزه، براساس موازین حقوق بین‌الملل و اساسنامهٔ رُم، تحت پیگرد قرار گیرند (Fidler, 2016: 14).

باتوجه به موانع موجود در رسیدگی به جرایم فناورانه، لازم است مقررات بین‌المللی قابل‌اجرا در سطح جهانی تعیین و اجرا شوند. این مقررات می‌توانند مبنای تعاملات بین‌المللی میان دولت‌ها و نهادهای بین‌المللی قرار گیرند. ازاین‌رو، با اعمال صلاحیت جهانی، انتظار می‌رود دولت‌ها از طریق معاهدات دو یا چندجانبه، همکاری‌هایی برای رسیدگی به جرایم فناورانهٔ فرامرزی ایجاد کنند (Rachmawati Madjid, 2021: 395-396). دیوان کیفری بین‌المللی طبق اساسنامهٔ رُم می‌تواند نقش مؤثری در مقابله با جرایم فناورانه که علیه زیرساخت‌های اطلاعاتی حیاتی انجام می‌شود، ایفا کند. براساس مادهٔ ۹۳ اساسنامه، دیوان می‌تواند به درخواست دولت‌های

1. Council of the European Union, Declaration by the European Union and its Member States on a Common Understanding of the Application of International Law to Cyberspace, Brussels, 18 November 2024, https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf

2. Explanation of Position of the United States on the Adoption of the Resolution on the UN Convention Against Cybercrime in UNGA's Third Committee – United States Mission to the United Nations

عضو در تحقیقات و محاکمهٔ جرایم مرتبط کمک کند. جرایم فناورانه به‌عنوان «جرم جدی» شناخته شده و اساسنامهٔ رُم می‌تواند فرایند دادرسی جهانی را تقویت کند. این اساسنامه، همچنین می‌تواند چهارچوبی قضایی برای مقابله با این جرایم در سطح جهانی و بدون مصونیت از مجازات فراهم آورد (Andini, 2021: 338).

وجود یک دیوان کیفری بین‌المللی در نظام حقوقی بین‌المللی، «حلقهٔ مفقوده» است؛ زیرا بسیاری از جرایم فناورانه بدون رسیدگی و بی‌کیفر می‌مانند. تأسیس چنین دیوانی موجب اجرای جهانی اصل مسئولیت کیفری فردی خواهد شد. این اقدام به‌طور طبیعی از ضرورت وجود حقوق بین‌المللی ویژه برای جرایم فناورانه ناشی می‌شود که پس از آن، صلاحیت دیوان برای رسیدگی به این جرایم در چهارچوب حقوق بین‌المللی ممکن می‌شود.

برای تحقق این هدف، مقررات الحاقی باید در فهرست جرایم تحت صلاحیت دیوان کیفری بین‌المللی قرار گیرند. همچنین، راه‌حل جایگزین می‌تواند تأسیس یک دیوان کیفری بین‌المللی ویژه برای رسیدگی به جرایم فناورانه به‌عنوان زیرمجموعه‌ای از دیوان بین‌المللی کیفری باشد. بدیهی‌ترین جایگزین، تأسیس این دیوان براساس تصمیم شورای امنیت سازمان‌ملل‌متحد است (Orji, 2012: 13). به‌هرحال، تحقیقات و تعقیب حقوق بین‌المللی برای رسیدگی مستقل و کارآمد دربارهٔ جدی‌ترین جرایم جهانی خاص، یعنی جرایم فناورانه، به دیوان کیفری بین‌المللی نیاز دارد (Khaeriah kadir & Judhariksawan, 2019: 152).

بااین‌همه، اتحادیهٔ بین‌المللی مخابرات در می ۲۰۰۷، دستور کار جهانی جرایم سایبری[1] را راه‌اندازی کرد تا چهارچوبی فراهم آورد که پاسخ بین‌المللی به چالش‌های رو به افزایش امنیت سایبری در آن هماهنگ شود. به‌منظور کمک به اتحادیهٔ بین‌المللی مخابرات در توسعهٔ پیشنهاد راهبردی، در اکتبر ۲۰۰۷ گروهی جهانی از کارشناسان فنی و خبره تشکیل شد. این کارشناسان، متشکل از تقریباً یکصدنفر از سراسر جهان، در سال ۲۰۰۸ گزارش‌هایی همراه با توصیه‌هایی درخصوص امنیت دیجیتال و مقررات جرایم فناورانه ارائه کردند. کارگروه اصلی نیز در سال ۲۰۱۰ به‌منظور ارائهٔ توصیه‌هایی برای پاسخ‌های حقوقی بین‌المللی جدید به جرایم فناورانه تشکیل شد. در همین حال، سازمان‌ملل‌متحد مطالعهٔ جامعی دربارهٔ وضعیت جرایم فناورانه آغاز کرد که با هدف بررسی گزینه‌های تقویت وضعیت موجود و پیشنهاد پاسخ‌های حقوقی جدید ملی و بین‌المللی انجام گرفت. اولین نشست این گروه کارشناسی از ۱۷ تا ۲۱ ژانویهٔ ۲۰۱۱ در وین برگزار شد.

ایالات‌متحده و اتحادیهٔ اروپا نیز در اجلاس سران اتحادیهٔ اروپا و ایالات‌متحده‌امریکا طی نوامبر ۲۰۱۰، گروه کاری ویژه‌ای درزمینهٔ امنیت فضای مجازی و جرایم فناورانه تشکیل دادند.

1. Global Cybercrime Agenda (GCA)

ازجملهٔ این تلاش‌ها، پیشبرد کنوانسیون شورای اروپا درزمینهٔ جرایم سایبری، برنامهٔ گسترش الحاق تمامی کشورهای عضو اتحادیهٔ اروپا و همکاری برای کمک به کشورهای خارج از منطقه برای رعایت استانداردهای آن بود. ازاین‌رو، دیوان کیفری بین‌المللی که قابلیت تأسیس آن فراهم خواهد شد، درخصوص تعقیب و محاکمهٔ جرایم فناورانه، باید صلاحیت رسیدگی به موضوع‌های زیر را دارا باشد:

الف- نقض یک معاهدهٔ جهانی یا مجموعه‌ای از معاهدات در مورد جرایم فناورانه؛

ب- حملات گسترده و هماهنگ جهانی فناورانه علیه زیرساخت‌های ارتباطی و اطلاعاتی حیاتی.

تشکیل دیوان کیفری بین‌المللی برای رسیدگی به جرایم فناورانه، به‌ویژه جرایم سایبری و فناوری‌های نوین، به‌دلیل گسترش تهدیدات دیجیتال و سرعت بالای تحولات فناورانه، به موضوعی حیاتی و ضروری تبدیل شده است. قوانین موجود در بسیاری از کشورها قادر به هماهنگی با این تغییرات سریع نیستند و تفاوت‌های حقوقی و سیاسی موجود، مانع ایجاد همکاری‌های مؤثر بین‌المللی می‌شود. ازاین‌رو، تشکیل دیوانی برای رسیدگی به چنین جرایمی، می‌تواند نقش مؤثری در حل مشکلات پیش‌رو ایفا کند؛ به‌ویژه در شرایطی که جرایم فناورانه مرزهای ملی را درمی‌نوردند و به‌صورت فرامرزی گسترش می‌یابند.

این دیوان می‌تواند معیارهایی جهانی برای جرم‌انگاری، مجازات و رسیدگی به این جرایم وضع کند و کشورها را به تطبیق قوانین خود با این معیارها تشویق کند. باوجوداین، نگرانی‌هایی درخصوص نقض حاکمیت ملی و استقلال قضایی کشورهای مختلف وجود دارد که باید با دقت و شفافیت آن‌ها را مدیریت کرد. موفقیت چنین نهادی مستلزم تعیین دقیق صلاحیت‌ها و ایجاد توافقات بین‌المللی برای تسهیل همکاری و اجرای احکام است. سرانجام، ایجاد این دیوان نیازمند دقت، هماهنگی و همکاری‌های مؤثر در سطح بین‌المللی است تا از بروز چالش‌های نوین و نقض حقوق حاکمیتی کشورها پیشگیری کند. براین‌اساس، می‌توان پیشنهاد داد که مصادیق جرایم ارتکابی به‌عنوان جرم مستقل بین‌المللی در اساسنامهٔ دیوان درج شود. این جرم شامل حملات فناورانهٔ سازمان‌یافته با اهدافی چون ایجاد رعب، تضعیف حکومت‌ها و آسیب به زیرساخت‌هاست؛ هرچند شناسایی این جرم می‌تواند بازدارندگی را تقویت کند و همکاری‌های بین‌المللی را ارتقا بخشد.

افزون‌براین، براساس مادهٔ نخست پیش‌نویس معاهدهٔ سازمان‌ملل‌متحد، دیوان کیفری بین‌المللی صلاحیت رسیدگی به جدی‌ترین حملات و جرایم فناورانه با ابعاد و نگرانی‌های جهانی را خواهد داشت و افراد مسئول این جرایم را تحت پیگرد قرار می‌دهد. در این فرایند، نقش قضات در حمایت از حاکمیت حقوق بین‌الملل و حقوق بشر در فضای دیجیتال باید مطابق با اصول

اعلامیهٔ جهانی حقوق بشر و میثاق‌های بین‌المللی حقوق مدنی، سیاسی، اقتصادی، اجتماعی و فرهنگی باشد و حقوق بشر برای همهٔ افراد تضمین شود.[۱]

نتیجه

مبارزه با جرایم فناورانه نیازمند همکاری جهانی است و نمی‌توان آن را محدود به یک ملت یا منطقه کرد. چالش‌های موجود نشان می‌دهد که برای مقابله با این جرایم باید سیاست‌ها، راهبردها و چهارچوب‌های حقوقی مناسب در سطح جهانی ایجاد شود. مقابله با جرایم فناورانه باید با وضع مقررات جامع و ویژه آغاز شود که موازین مربوطه، قوانین و دستورالعمل‌ها را برای افزایش امنیت فضای دیجیتال مشخص کند. گزارش‌های دفتر مواد مخدر و جرم سازمان‌ملل نشان می‌دهند که این موازین معیارهایی برای رفتار کاربران فناوری اطلاعات تعیین می‌کنند.

باوجوداین، ناهماهنگی‌های موجود در حقوق بین‌المللی موجب تضعیف امنیت دیجیتال شده و نیاز به یک معاهدهٔ جهانی دراین‌زمینه بیش‌ازپیش احساس می‌شود. بااین‌حال، می‌توان با اجرای سازوکارهای عملیاتی زیر با جرایم فناورانه مقابله کرد:

الف- افزایش آگاهی عمومی از امنیت فناورانه و همچنین خطرها و تعهدات مرتبط با اینترنت و رسانه‌های اجتماعی از طریق رویکرد چندسازمانی؛

ب- افزایش همکاری با دیگر سازمان‌های مجری قانون و ذی‌نفعان برای مقابله با جرایم فناورانه؛

ج- تقویت هماهنگی و به‌اشتراک‌گذاری تخصص در رسیدگی به جرایم فناورانه؛

د- اقدامات پیشگیرانه برای تحقیق و گردآوری اطلاعات با هدف مقابله با جرایم فناورانه.

بیانیهٔ نبود تعارض منافع

نویسندگان اعلام می‌دارند که تعارض منافع وجود ندارد و تمام مسائل اخلاق در پژوهش را شامل پرهیز از دزدی ادبی، انتشار و یا ارسال بیش از یک بار مقاله، تکرار پژوهش دیگران، داده‌سازی یا جعل داده‌ها، منبع‌سازی و جعل منابع، رضایت ناآگاهانه سوژه یا پژوهش‌شونده، سوء رفتار و غیره، به‌طور کامل رعایت کرده‌اند.

1. See www.ohchr.org

قدردانی

نگارندگان، از داوران گرامی برای مطالعه مقالهٔ حاضر و ارائهٔ نظرات ساختاری، علمی و ارزشمند و همچنین از دست‌اندرکاران محترم مجله، صمیمانه سپاسگزاری می‌کنند.

References

Aaron, A. (2019). *A legal Analysis of Cybercrime and Cyber Torts: Lessons for Nigeria*. [LL. B Thesis, University of Lagos].

Ayswariya, G. K & Aswathy, R. (2017). "A Comparative Study on the Difference Between Conventional Crime and Cybercrime". *International Journal of Pure and Applied Mathematics*, 119(17), PP. 69-75. https://acadpubl.eu/hub/2018-119-17/2/120.pdf (Accessed 14 December 2024).

Andini, O. P. (2021). "Cyber Terrorism Criminal Acts in the Perspective of Transnational Organized Crime". *Unnes Law J*ournal, 7(2), PP. 333-346. https://journal.unnes.ac.id/sju/ulj/article/view/38804

Alex, G. (2014). "Coming Soon: Another Country to Ratify the Budapest Convention". *CFR blog*. https://www.cfr.org/blog/coming-soon-another-country-ratify-budapest-convention (Accessed 21 December 2024).

Alkharman, Jamal Awwad & Isyaku Hassan (2023). "Cyberterrorism and Self-Defense in the Framework of International Law". *Journal of Law and Sustainable Development*, 11(8), PP. 1-21. DOI: https://doi.org/10.55908/sdgs.v11i8.1430

De Silva De Alwis, R. (2025). Gendering the new international convention on cybercrimes and new norms on artificial intelligence and emerging technologies. Washington Journal of Law, Technology & Arts, 20(2), PP. 1-41. http://dx.doi.org/10.2139/ssrn.4945578

Eoghan Casey (2011). *Digital Evidence and Computer Crime* (3rd Ed.). Elsevier Inc publisher, PP. 1-304.

Crootof, R. (2018). "International Cyber Torts: Expanding State Accountability in Cyberspace". *Cornell Law Review*, 103(1), PP. 565-644. https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=4753&context=clr(Accessed 5 January 2025).

Fidler, D. P. (2016). "Cyberspace, Terrorism and International Law". *Journal of Conflict and Security Law*, 21(3), PP. 1-26. https://doi.org/10.1093/jcsl/krw013

Gabey. G. (2013). "INTERPOL Global Complex for Innovation: Interpol lays out response blueprint for global cybercrime war". *Digital News Asia*.https://www.digitalnewsasia.com/security/interpol-lays-outresponse-blueprint-for-global-cybercrime-war (Accessed 14 January 2025).

Khokhlov, N., & Korotayev, A. (2022). "Internet, Political Regime and Terrorism: A Quantitative Analysis". *CrossCultural Research*, 56(4), PP. 385–418. DOI: 10.1177/10693971221085343

Krannenbarg, M.W. (2018). "Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison". *Journal of Developmental and Life-Course Criminology*, 4(3), PP. 343-364. DOI: 10.1007/s40865-018-0087-8.

Khaeriah kadir, Nadiah & Judhariksawan, Maskun. (2019). "Terrorism and Cyber space; A Phenomenon of Cyber-Terrorism as Transnational Crimes". *Fiat Justicia Journal*,13(4), PP. 147-162. DOI: 10.25041/fiatjustisia.v13no4.1735

Mifitzgerald. (2004). "Nine Famous Hacks". *Extreme Tech*. https://www.extremetech.com/extreme/55530nine-famous-hacks (Accessed 18 November 2024).

L. Kovacich & Andy Jones (2006). "Investigating High-Technology". in: *Crimes High-Technology Crime Investigator's Handbook Gerald, (Second Edition) Establishing and Managing a High-Technology Crime Prevention Program*, pp. 99-113. https://www.sciencedirect.com/science/article/abs/pii/B9780750679299500506(Accessed 16 November 2024).

Juliana De Groot. (2020). "A History of RAnsomeware Attacks: The Biggest and Worst Ransomware Attacks of All Times". *Digital Guardian's Blog*. https://digitalguardian.com/blog/historyransomware-attacks-biggest-and-worst-ransomware-attacks-all-time (Accessed 8 November 2024).

Shaweorcid, Robb, Ian R. McAndrew. (2023). "Cybersecurity and Domestic Terrorism: Purpose and Future". *Journal of Software Engineering and Applications*, 16(10), PP. 548-560. DOI: 10.4236/jsea.2023.1610028

Hadji-Janev, M., & Aleksoski, S. (2021). "Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace". *Mediterranean Journal of Social Sciences*, 4(14), PP. 115-126. https://connections-qj.org/article/use-force-self-defense-against-cyber-attacks-and-shockwaves-legal-community-one-more-reason (Accessed 27 February 2025).

Rachmawati Madjid, Yasniar. (2021). "Cyberterrorism Challenges: The Need for Global Mutual Legal Assistance for Universal Criminal Jurisdiction". *Yustisia Jurnal Hukum*,10(3), PP. 388-414. DOI: https://doi.org/10.20961/yustisia.v10i3.54953

Reveron, Derek S. & John E. Savage. (2023). I*nternational Law and Norms in Cyberspace, in: Security in the Cyber Age an Introduction to Policy and Technology*. Cambridge University Press.

Stein, S. & Solange, G. (2009). *A Global Protocol on Cybersecurity and Cybercrime*. (Oslo: E-dit).

Henkin, L. (1978). *How Nations Behave*. Columbia University Press, 2nd edn.

Orji, U.J. (2012). *Cybersecurity Law and Regulation*. 1 Wolf Legal Publishers.

Ramos, A. (2014). "United Nations' Definition of Cybercrime". *Innovative Dynamic Networks*. https://idnwi.com/united-nations-definition-cybercrime/ (Accessed 8 (Accessed 12 October 2024).

Raven. (2002). "The History of Hacking and Phreaking". *HelpnetSecurity*. www.helpnetsecruity.com/2002/04/04/the-history-of-hacking-and-phreaking/ (Accessed 8 November 2024).