Journal of
International Criminal Law
www.iclj.ir

Volume 4, Issue 3, 2026

The Role of the United Nations in Regulating International Standards to Combat Cybercrime

Ahmad Ranjbar Tovakoli[1], Babak Pourghahramani[2*], Mehrdad Teymouri[3]

1. Department of Criminal Law and Criminology, Ka.C., Islamic Azad University, Karaj, Iran.
2. Department of Criminal Law and Criminology, Mar.C., Islamic Azad University, Maragheh, Iran. (Corresponding Author).
3. Department of Criminal Law and Criminology, Ta.C., Islamic Azad University, Tabriz, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: ***1-12***

Corresponding Author's Info:
ORCID: *0009-0006-6252-5971*
TELL: *+041-37454506*
Email: *Pourghahramani@iau.ac.ir*

Article History:
Received: *07 Feb 2026*
Revised: *24 Feb 2026*
Accepted: *07 Apr 2026*
Published online: *23 Sep 2026*

Keywords:
Cybercrime, International Criminal Law, United Nations, International Standards.

ABSTRACT

In light of the unprecedented expansion of modern communication and information technologies, cybercrime has become one of the most complex and transnational challenges facing international criminal law. This research aims to explain and analyze the role of the United Nations in developing international standards to combat cybercrime by examining a collection of binding and non-binding documents, General Assembly resolutions, and specifically the Convention on Combating Cybercrime (Resolution A/RES/74/247). The research method is based on library study and comparative analysis of international documents, conventions, and regulations. The research findings indicate that the United Nations' role has thus far remained primarily at the level of developing guiding documents and recommendations, and the aforementioned Convention also faces shortcomings in the areas of criminalization of offenses, precise determination of jurisdiction, and provision of effective implementation mechanisms. The most significant achievement of the United Nations in the process of standardizing cybercrime can be seen in the adoption and signing of the "United Nations Convention on Combating Cybercrime" (Hanoi Treaty). This important international instrument is designed around three fundamental axes: first, the unification of rules and ending the phenomenon of "escape from the law"; second, creating a fundamental transformation in judicial cooperation with an emphasis on speed instead of time-consuming bureaucracies; and third, reducing the technological gap and realizing justice for developing countries. This article endeavors, while analyzing the UN's role in regulating international standards to combat cybercrime through the examination of existing documents, to also critique and evaluate the aforementioned global treaty.

How to Cite This Article: Ranjbar Tovakoli, A; Pourghahramani, B. & Teymouri, M. (2026). "The Role of the United Nations in Regulating International Standards to Combat Cybercrime". *Journal of International Criminal Law*, 4(3): 1-12.

فصلنامه حقوق جزای بین‌الملل

www.iclj.ir

انجمن علمی فقه جزای تطبیقی ایران

دوره چهارم، شماره سوم، پائیز ۱۴۰۵

نقش سازمان ملل متحد در تنظیم استانداردهای بین‌المللی برای مقابله با جرائم سایبری

احمد رنجبر توکلی[۱]، بابک پورقهرمانی[۲*]، مهرداد تیموری[۳]

۱. گروه حقوق کیفری و جرم‌شناسی، واحد کرج، دانشگاه آزاد اسلامی، کرج، ایران.
۲. گروه حقوق کیفری و جرم‌شناسی، واحد مراغه، دانشگاه آزاد اسلامی، مراغه، ایران. (نویسنده مسؤول)
۳. گروه حقوق کیفری و جرم‌شناسی، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱۲-۱

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۹-۰۰۰۶-۶۲۵۲-۵۹۷۱

تلفن: ۳۷۴۵۴۵۰۶-۰۴۱+

ایمیل: Pourghahramani@iau.ac.ir

سابقه مقاله:

تاریخ دریافت: ۱۴۰۴/۱۱/۱۸

تاریخ ویرایش: ۱۴۰۴/۱۲/۰۵

تاریخ پذیرش: ۱۴۰۵/۰۱/۱۸

تاریخ انتشار: ۱۴۰۵/۰۷/۰۱

واژگان کلیدی:

جرائم سایبری، حقوق بین‌الملل کیفری، سازمان ملل متحد، استانداردهای بین‌المللی.

چکیده

در پرتو گسترش بی‌سابقه فناوری‌های نوین ارتباطی و اطلاعاتی، جرائم سایبری به یکی از پیچیده‌ترین و فراملی‌ترین چالش‌های حقوق بین‌الملل کیفری تبدیل شده است. این پژوهش با هدف تبیین و واکاوی نقش سازمان ملل متحد در تدوین استانداردهای بین‌المللی مقابله با جرائم سایبری، به بررسی مجموعه‌ای از اسناد الزام‌آور و غیر الزام‌آور، قطعنامه‌های مجمع عمومی و به‌طور ویژه کنوانسیون مقابله با جرائم سایبری (قطعنامه A/RES/74/247) پرداخته است. روش تحقیق مبتنی‌بر مطالعه کتابخانه‌ای و تحلیل تطبیقی اسناد، کنوانسیون‌ها و مقررات بین‌المللی است. یافته‌های پژوهش نشان می‌دهد که نقش‌آفرینی سازمان ملل متحد تاکنون عمدتا در سطح تدوین اسناد راهنما و توصیه‌نامه‌های باقی‌مانده و کنوانسیون یادشده نیز با نارسایی‌هایی در زمینه جرم‌انگاری جرائم، تعیین دقیق صلاحیت قضایی و پیش‌بینی سازوکارهای اجرایی مؤثر مواجه است. مهم‌ترین دستاورد سازمان ملل متحد در فرایند استانداردسازی جرائم سایبری را می‌توان در تصویب و امضای «کنوانسیون مبارزه با جرائم سایبری سازمان ملل متحد» (پیمان هانوی) دانست. این سند مهم بین‌المللی در سه محور اساسی طراحی شده است: نخست، یکپارچه‌سازی قواعد و پایان دادن به پدیده «فرار از قانون»؛ دوم، ایجاد تحول بنیادین در همکاری‌های قضایی با تأکید بر سرعت به‌جای بوروکراسی‌های زمان‌بر؛ و سوم، کاهش شکاف فناوری و تحقق عدالت برای کشورهای در حال توسعه. این مقاله می‌کوشد ضمن تحلیل نقش سازمان ملل در تنظیم استانداردهای بین‌المللی مقابله با جرائم سایبری از طریق بررسی اسناد موجود، به نقد و ارزیابی معاهده جهانی مذکور نیز بپردازد.

مقدمه

تحولات پرشتاب در عرصه فناوری‌های دیجیتال، ابعاد نوینی از بروز جرائم در فضای سایبری را آشکار ساخته است. این دگرگونی‌ها، قواعد سنتی حقوق بین‌الملل کیفری را با چالش‌هایی بی‌سابقه مواجه کرده و مفاهیمی چون صلاحیت قضایی، جرم‌انگاری و همکاری‌های بین‌المللی را نیازمند بازتعریف نموده است (Clough, 2014: 118). برخلاف جرائم سنتی که عموما در محدوده جغرافیایی مشخصی تحقق می‌یافتند، جرائم سایبری ماهیتی فراملی و فاقد قلمرو سرزمینی دقیق دارند و همین امر ظرفیت مداخله نهادهای کلاسیک بین‌المللی را محدود ساخته است (Tropina, 2020: 45). نقش سازمان ملل متحد به‌عنوان مهم‌ترین بازیگر عرصه تنظیم استانداردهای بین‌المللی، اهمیتی مضاعف یافته است. این سازمان با بهره‌گیری از نهادهای تخصصی خود و فرآیندهای چندجانبه تلاش کرده است چارچوب‌های حقوقی هماهنگ و قابل‌پذیرش برای دولت‌های عضو تدوین نماید. تحولات مفهوم مرز در فضای سیاسی مجازی نشان می‌دهد که مرزها دیگر صرفا خطوط جغرافیایی نیستند، بلکه بیشتر به‌صورت سازه‌های اجتماعی و سیاسی عمل می‌کنند. پژوهش نشان می‌دهد که در بستر شبکه‌های اجتماعی و فضای مجازی، مرزهای سنتی قدرت و کنترل تغییر یافته و دولت‌ها با چالش‌های نوینی در حفاظت از حاکمیت و امنیت مواجه‌اند (افضلی و همکاران، ۱۳۹۲: ۴۵). تصویب قطعنامه‌هایی همچون A/RES/55/63 (2000) و اقدامات دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد (UNODC) نشان می‌دهد که این سازمان از دو دهه پیش در صدد ایجاد مبنای حقوقی مشترکی در حوزه جرائم سایبری بوده است (Sumadinata, 2023: 134).

با این حال، ماهیت غیر الزام‌آور اغلب اسناد و فقدان اجماع میان کشورهای عضو بر سر مفاهیم کلیدی، موجب شده است روند استانداردسازی با کاستی‌های جدی مواجه گردد (Buçaj & Idrizaj, 2025: 90–91). سؤال اصلی پژوهش حاضر این است که: **«سازمان ملل متحد چه نقش و تأثیری در تنظیم استانداردهای بین‌المللی برای مقابله با جرائم سایبری داشته و تا چه حد این استانداردها توانسته‌اند پاسخگوی تهدیدات فراملی جرائم سایبری باشند؟»**

خلأهای موجود در اسناد بین‌المللی و عدم توافق بر سر معاهده‌ای جامع، ضرورت پژوهش حاضر را دوچندان می‌کند.

۱- تحلیل ساختار نهادی و کارکردی سازمان ملل در تنظیم استانداردهای بین‌المللی سایبری

ساختار نهادی سازمان ملل متحد در مواجهه با پدیده نوظهور و پیچیده‌ای مانند جرائم سایبری، در مراحل نخست بر پایه نهادهای سنتی این سازمان شکل گرفت، از جمله شورای اقتصادی و اجتماعی (ECOSOC) (Tropina, 2020: 45)، کمیسیون پیشگیری از جرم و عدالت کیفری (CCPCJ) (Clough, 2014: 120) و دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد (UNODC). با این حال، گستره فرامرزی، ماهیت فنی و تغییرپذیری مستمر فضای سایبری، ناکارآمدی سازوکارهای سنتی را به‌طور آشکار نمایان ساخت. جرائم سایبری با ویژگی‌های خاص خود، از جمله سرعت انتشار و قابلیت فرامرزی، مستلزم بازنگری در آیین دادرسی کیفری سنتی هستند. پژوهش انجام‌شده نشان می‌دهد که قوانین موجود در ایران قادر نیستند به‌صورت کامل با پیچیدگی‌های این دسته از جرائم مقابله کنند و پیشنهاد می‌شود چارچوب قانونی جدیدی متناسب با ماهیت جرائم سایبری تدوین شود (جلالی و فراهانی، ۱۳۸۹: ۱۲۰).

به همین سبب، سازمان ملل متحد به‌تدریج به‌سوی ایجاد ساختارهای ویژه‌محور حرکت کرد که نمونه شاخص آن تشکیل **«کمیته ویژه مذاکراتی برای تدوین کنوانسیون بین‌المللی مقابله با جرائم سایبری»** ذیل قطعنامه A/RES/74/247 در سال ۲۰۱۹ بود (Buçaj & Thaqi, 2025: 92). این کمیته با رویکردی بین دولتی و با مشارکت تمامی اعضا، مأموریت طراحی معاهده‌ای جامع در سطح جهانی را بر عهده دارد. با این وجود، ماهیت مذاکرات‌محور و وابستگی تصمیم‌گیری به اجماع اعضا، به مصالحه‌های حقوقی گسترده منجر شده و کارایی هنجاری سند را محدود ساخته است.

جرائم سایبری، با توجه به شتاب فزاینده تحولات فناورانه و گسترش تعاملات بین‌المللی، نیازمند توجه ویژه در حوزه

پیشگیری و آموزش هستند. بررسی تجارب بین‌المللی نشان می‌دهد که همکاری میان کشورها و ایجاد سازوکارهای حقوقی هماهنگ برای مقابله با جرائم سایبری ضرورتی اجتناب‌ناپذیر است و بدون وجود چارچوب قانونی جهانی، کنترل این جرائم با دشواری‌های جدی مواجه خواهد شد (انجلیز، ۱۳۸۳: ۷۵). از منظر کارکردی، سازمان ملل متحد به‌جای تمرکز صرف بر جرم‌انگاری جرائم رایانه‌ای، کوشیده است ابعاد همکاری بین‌المللی، صلاحیت قضایی، انتقال داده‌ها و حمایت از حریم خصوصی را نیز در ساختار معاهده لحاظ کند. برای مثال، مواد ۶ تا ۱۶ معاهده، جرائم سایبری نظیر دسترسی غیرمجاز، مداخله در داده‌ها و سامانه‌ها و استفاده از ابزارهای مخرب دیجیتال را در بر می‌گیرد. با این حال، عدم شفافیت در تعاریف، به‌ویژه در مقررات مربوط به محتوای غیرقانونی، تهدیدی جدی برای آزادی بیان و حق دسترسی به اطلاعات ایجاد کرده است. همچنین ماده ۲۳ در حوزه صلاحیت قضایی، فاقد قواعد روشن اولویت‌بندی میان صلاحیت‌های متعارض کشورهاست که این امر احتمال بروز تعارض صلاحیتی و بی‌اثر شدن تعقیب‌های کیفری در سطح بین‌المللی را افزایش می‌دهد.

در حوزه همکاری بین‌المللی، سازمان ملل متحد تلاش کرده است قالب‌هایی برای استرداد مجرمان، انتقال پرونده‌ها و ارائه ادله الکترونیکی طراحی کند که عمدتا بر الگوی **«کنوانسیون بوداپست»** مصوب شورای اروپا استوار است (Clough, 2014: 122–123). با این حال، فقدان الزام‌آوری حقوقی و نبود سازوکار داوری فوری، موجب کاهش اثرگذاری عملی این مقررات شده است.

یکی دیگر از کارکردهای اساسی، ایجاد توازن میان امنیت سایبری و صیانت از حقوق بشر است. ماده ۴۰ کنوانسیون جرائم سایبری بر عدم نقض حقوق بشر شناسایی‌شده در اسناد بین‌المللی، از جمله میثاق بین‌المللی حقوق مدنی و سیاسی، تأکید می‌کند (Tropina, 2020: 46). با این وجود، در فقدان نهاد مستقل نظارتی، این نگرانی وجود دارد که دولت‌ها از ابزارهای مقابله با جرائم سایبری برای محدودسازی ناموجه حقوق دیجیتال شهروندان بهره‌برداری کنند.

از منظر اصول حقوقی، یکی از نارسایی‌های ساختار کارکردی سازمان ملل متحد، عدم انطباق کافی مفاد معاهده با اصول بنیادین حقوق کیفری، از جمله اصل قانونی بودن جرم و مجازات (Nullum Crimen Sine Lege) و اصل تناسب در پاسخ کیفری است (Sumadinata, 2023: 136). به‌عنوان نمونه، تعریف ارائه‌شده در ماده ۸ دربارهٔ جرائم مرتبط با سیستم‌های رایانه‌ای، فاقد معیارهای عینی و قابل پیش‌بینی برای شهروندان است و در نظام‌های کیفری با رویکرد حداقلی، از پشتوانه مشروعیت حقوقی کافی برخوردار نیست. چنین ابهام‌هایی زمینه‌ساز تفسیرهای فراقانونی و اعمال خودسرانه ضمانت‌اجراهای کیفری می‌شود.

فقدان تعامل مؤثر میان ساختار نهادی سازمان ملل متحد و سایر نهادهای فنی و تخصصی جهانی، از جمله اتحادیه بین‌المللی مخابرات و مجمع جهانی اقتصاد دیجیتال، سبب شده است طراحی هنجارهای سایبری از جامع‌نگری فنی و هم‌افزایی نهادی لازم برخوردار نباشد (Naseeb & Khan, 2024: 104). در صورت تشکیل کمیسیون‌های مشترک میان حقوقدانان، متخصصان امنیت سایبری و نمایندگان بخش خصوصی، کارکرد و اثربخشی معاهدات بین‌المللی به‌طور قابل‌توجهی ارتقا خواهد یافت.

در نهایت، ظرفیت ساختاری سازمان ملل متحد در سطح اجرایی نیز محدود است. برخلاف برخی معاهدات موفق بین‌المللی مانند کنوانسیون مبارزه با فساد، کنوانسیون جرائم سایبری فاقد سازوکارهای نظارت، گزارش‌دهی ادواری و ارزیابی مستقل اجرای مفاد سند توسط کشورهای عضو است و در غیاب این سازوکارها، میزان انطباق اقدامات کشورها با مفاد معاهده محدود باقی می‌ماند (Luo, 2022: 60).

با توجه به ساختار و کارکرد سازمان ملل متحد، می‌توان نتیجه گرفت که سازوکارهای نهادی موجود، به‌ویژه نهادهای سنتی، برای مقابله با پیچیدگی‌های جرائم سایبری کفایت لازم را ندارند. وابستگی تصمیم‌گیری‌ها به اجماع اعضا و ماهیت مذاکرات‌محور کمیته ویژه، سرعت و اثربخشی معاهدات را کاهش داده و کارایی هنجاری آن‌ها را محدود می‌سازد. افزون‌بر این، عدم شفافیت در تعاریف جرائم سایبری و فقدان

قواعد روشن برای تعیین صلاحیت قضایی، بستر تفسیرهای فراقانونی و اعمال خودسرانه ضمانت‌اجراهای کیفری را فراهم می‌آورد. فقدان هماهنگی با نهادهای فنی و تخصصی جهانی نیز شکافی میان تنظیم‌گری حقوقی و واقعیت‌های فناورانه ایجاد کرده که در عمل از اثربخشی معاهدات بین‌المللی می‌کاهد. از سوی دیگر، ظرفیت اجرایی سازمان ملل متحد در سطح بین‌المللی محدود بوده و نبود سازوکارهای نظارت، گزارش‌دهی ادواری و ارزیابی مستقل، مانع انطباق دولت‌ها با مفاد معاهده می‌شود. این وضعیت نشان می‌دهد که تحقق اهداف واقعی تنظیم استانداردهای جهانی مستلزم توسعه کمیسیون‌های تخصصی مشترک با مشارکت حقوقدانان، متخصصان امنیت سایبری و نمایندگان بخش خصوصی و همچنین طراحی سازوکارهای نظارتی و ارزیابی مستمر است؛ امری که می‌تواند به ایجاد چارچوب حقوقی جامع و الزام‌آور در مقابله مؤثر با جرائم سایبری منجر شود. نقش‌های نهادی و کارکردی ارکان مختلف سازمان ملل متحد از اهمیت ویژه‌ای برخوردار است که به شرح ذیل تشریح می‌شوند.

الف- مجمع عمومی (رکن هنجارگذار و قانون‌نویسی)

نقش نهادی (منشوری): تصویب معاهدات بین‌المللی و توسعه حقوق بین‌الملل.

کارکرد در استانداردسازی سایبری: مرکز ثقل قانون‌نویسی.

تدوین مستقیم: در دسامبر ۲۰۲۴، کنوانسیون ملل متحد علیه جرائم سایبری را تصویب کرد. این سند حاصل فعالیت یک کمیته ویژه (Ad Hoc Committee) بود که مجمع عمومی در سال ۲۰۱۹ ایجاد نمود.

بستر مذاکره: مجمع عمومی میزبان کارگروه باز (Open-Ended Working Group) در حوزه امنیت فناوری اطلاعات است که چارچوب رفتار مسئولانه دولت‌ها را توسعه می‌دهد.

نتیجه: بدون اقدام مجمع عمومی، اساسا هیچ استاندارد الزام‌آور جهانی در این حوزه شکل نمی‌گرفت.

ب- شورای امنیت (رکن امنیتی – صلح و منازعه)

نقش نهادی (منشوری): مسئولیت اصلی حفظ صلح و امنیت بین‌المللی.

کارکرد در استانداردسازی سایبری: ایجاد پیوند میان جرم و تهدید علیه صلح.

سیاست‌گذاری امنیتی: شورای امنیت به‌طور مستقیم جرم‌انگاری نمی‌کند، اما با تصویب قطعنامه‌های متعدد برای مقابله با تروریسم سایبری و تأمین مالی آن، چارچوب‌های امنیتی مرتبط را تقویت کرده است.

یکپارچه‌سازی: دبیرکل از شورا خواسته است تهدیدات سایبری را در عملیات‌های حفظ صلح و حفاظت از غیرنظامیان ادغام کند که این امر به استانداردسازی رویه‌های حفاظتی در میدان منجر می‌شود.

نقش مکمل: شورای امنیت با شناسایی تهدیدات سایبری به‌عنوان مصادیق تهدید علیه صلح، بستر اجرایی کنوانسیون جرائم سایبری را فراهم می‌کند.

ج- دبیرخانه و دبیرکل (رکن اجرایی و هماهنگی)

نقش نهادی: مدیریت اجرایی، میانجیگری و نمایندگی سازمان.

کارکرد در استانداردسازی سایبری: پشتیبانی، امضا و ظرفیت‌سازی.

امضای معاهده: دبیرکل سازمان ملل متحد (آنتونیو گوترش) مستقیما در مراسم امضای کنوانسیون در هانوی در اکتبر ۲۰۲۵ شرکت کرد و آن را ابزاری برای دفاع جمعی معرفی نمود.

حمایت فنی: دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد (UNODC) به نمایندگی از دبیرخانه، مسئول هماهنگی فنی، آموزش و اجرای کنوانسیون در کشورهای در حال توسعه است.

چارچوب کلان: ابتکار **«دستور کار جدید برای صلح»** دبیرکل، حاکمیت قانون در فضای دیجیتال را به‌عنوان یک استاندارد الزام‌آور مطرح کرده است.

د- شورای اقتصادی و اجتماعی (رکن هماهنگی سیاستی)

نقش نهادی: هماهنگی نهادهای تخصصی و توسعه‌ای.

کارکرد در استانداردسازی سایبری: غیرمستقیم و زیرساختی.

بر اساس اسناد موجود، شواهدی دال بر نقش مستقیم شورای اقتصادی و اجتماعی در جرم‌انگاری یا استانداردسازی جرائم سایبری مشاهده نمی‌شود، هرچند نهادهای وابسته به آن، از جمله اتحادیه بین‌المللی مخابرات (ITU)، به‌طور تاریخی در

تدوین استانداردهای امنیت شبکه نقش داشته‌اند، اما این اسناد مستقیما به کنوانسیون جدید منتهی نشده‌اند.

و- سایر ارکان (دیوان و قیمومیت)

دیوان بین‌المللی دادگستری (ICJ): تاکنون رأی مشورتی یا الزام‌آوری در خصوص جرائم سایبری صادر نکرده است، اما در آینده می‌تواند در تفسیر تعهدات دولت‌ها ذیل کنوانسیون جدید نقش‌آفرین باشد.

شورای قیمومیت: در این حوزه فاقد هرگونه نقش مؤثر است.

۱-۱- ظرفیت‌های حقوقی و نقش راهنمای اسناد سازمان ملل در استانداردسازی بین‌المللی جرائم سایبری

در فرآیند استانداردسازی بین‌المللی جرائم سایبری، اسناد صادره از سوی سازمان ملل متحد، هرچند از منظر حقوقی الزام‌آور به شمار نمی‌آیند، نقش مهم و تعیین‌کننده‌ای در شکل‌دهی قواعد عرفی، یکپارچه‌سازی تفسیرهای هنجاری و تسهیل دستیابی به اجماع سیاسی میان دولت‌ها ایفا می‌کنند. این اسناد با اتکا به مشروعیت نهادی سازمان ملل متحد و بهره‌گیری از مفاهیم متمایز حقوق بین‌الملل، به منبعی از اقتدار معنوی و ابزاری برای تحقق همگرایی تدریجی نظام‌های حقوقی ملی تبدیل شده‌اند. به‌ویژه در حوزه جرائم سایبری که شتاب تحولات فناورانه با کندی فرایندهای معاهداتی در تعارض قرار دارد، این اسناد به‌عنوان ابزارهایی انعطاف‌پذیر، هدایت نظام‌های کیفری به‌سوی اصول مشترک و قواعد عرفی نوظهور را امکان‌پذیر می‌سازند (Tropina, 2020: 15).

تحلیل محتوایی اسناد راهنمایی و توصیه‌نامه‌های سازمان ملل متحد، از جمله **«راهنمای ۲۰۱۵ سازمان ملل برای همکاری‌های بین‌المللی در مقابله با جرائم سایبری»**، نشان می‌دهد که ارائه تعاریف عملیاتی از مفاهیم کلیدی مانند **«دسترسی غیرمجاز»**، **«دست‌کاری داده‌ها»** و **«محتوای غیرقانونی»**، زمینه‌های لازم برای شکل‌گیری هنجارهای بین‌المللی را فراهم کرده است. هرچند این تعاریف در اسناد الزام‌آور، از جمله کنوانسیون جرائم سایبری، به‌طور مستقیم اقتباس نشده‌اند، اما از طریق اثرگذاری بر رویه‌ی کشورهای عضو، موجبات همگرایی تدریجی مفاهیم کیفری را فراهم می‌آورند (Buçaj & Idrizaj, 2025: 42). تحولات حقوق بین‌الملل دریایی از دوره گروسیوس تا کنفرانس‌های ژنو نیز نشان می‌دهد که قواعد حقوقی حاکم بر دریاها همواره متناسب با توسعه تجارت بین‌المللی و نیازهای امنیتی دستخوش تغییر بوده‌اند. کنفرانس‌های ژنو نقطه عطفی در تعیین حقوق حاکمیتی دولت‌ها بر دریاها و منابع دریایی محسوب می‌شوند و سازوکارهای حقوقی جدیدی را برای حل‌وفصل اختلافات بین‌المللی ارائه کرده‌اند (متین دفتری، ۱۳۸۷: ۱۵۰).

یکی از ویژگی‌های مهم این اسناد، تسهیل مشارکت دولت‌ها با مواضع متفاوت است. برخلاف معاهدات الزام‌آور که مستلزم پذیرش صریح دولت‌ها هستند، اسناد راهنمای سازمان ملل متحد به دلیل فقدان الزام حقوقی، امکان ایجاد چارچوبی از توافق حداقلی و حل اختلافات فنی، از جمله انتقال فرامرزی داده‌ها و اشتراک‌گذاری ادله دیجیتال را فراهم می‌کنند (Tennis, 2020: 37).

از منظر ساختار حقوق بین‌الملل، این اسناد نه‌تنها به‌عنوان مرحله‌ای گذار به‌سوی قواعد الزام‌آور ایفای نقش می‌کنند، بلکه در فرایند شکل‌گیری حقوق عرفی بین‌المللی نیز تأثیرگذار هستند. استناد مکرر به این اسناد در رویه‌های قضایی، آراء دیوان‌ها و اسناد سیاستی دولت‌ها، زمینه شکل‌گیری عقیده حقوقی نسبت به جرم‌انگاری و همکاری‌های بین‌المللی در مقابله با جرائم سایبری را فراهم می‌سازد. قطعنامه‌های مجمع عمومی سازمان ملل متحد، هرچند در ظاهر ماهیتی توصیه‌ای دارند، اما با گذشت زمان واجد کارکرد تفسیری نسبت به اصول منشور ملل متحد و سایر اسناد الزام‌آور می‌شوند. به‌عنوان نمونه، قطعنامه A/RES/57/239 (2002) نقش مؤثری در ایجاد زبان مشترک در خصوص تهدیدات سایبری و همکاری‌های امنیتی ایفا کرد و در سال‌های بعد، مبنای شکل‌گیری گروه کارشناسان دولتی و گروه کاری آزاد قرار گرفت (Naseeb & Khan, 2024: 11).

اسناد راهنمای سازمان ملل متحد همچنین در شکل‌دهی به استانداردهای رفتاری مسئولانه دولت‌ها در فضای سایبری نقشی بنیادین دارند. گزارش‌های نهایی گروه کارشناسان دولتی (GGE)، به‌ویژه گزارش سال ۲۰۱۵، با تأکید بر اصول عدم مداخله، حسن‌نیت و احترام به حاکمیت سایبری، مجموعه‌ای از

هنجارها را به استانداردهای رفتاری دولت‌ها تبدیل کرده‌اند. این استانداردها با تکرار در اسناد منطقه‌ای و دوجانبه، به‌تدریج ماهیتی فراتر از نرم‌قانون پیدا کرده‌اند (Buçaj & Thaqi, 2025: 29).

اسناد راهنمای سازمان ملل متحد با فراهم‌سازی بستری مشترک برای تعاریف کلیدی و اصول رفتاری، نقش مهمی در کاهش واگرایی میان نظام‌های حقوقی و هماهنگ‌سازی اقدامات بین‌المللی ایفا می‌کنند. این اسناد به دولت‌هایی با چارچوب‌های حقوقی متفاوت امکان می‌دهند، بدون خدشه به حاکمیت خود، بر سر اصول کلان هنجاری به اجماعی نسبی دست یابند. افزون‌بر این، به‌عنوان ابزارهایی انعطاف‌پذیر، توان پاسخگویی به تحولات سریع فضای سایبری را دارند و زمینه‌ساز تدوین معاهدات الزام‌آور محسوب می‌شوند.

تحلیل نهایی نشان می‌دهد که مشروعیت و میزان اثرگذاری اسناد راهنمای سازمان ملل متحد وابسته به مشارکت گسترده دولت‌های کلیدی، تحقق اجماع نسبی و بهره‌گیری راهبردی از قدرت نرم این سازمان است. اسنادی که با مشارکت طیف متنوعی از کشورها و در چارچوب نهادی معتبر تدوین شده‌اند، از ظرفیت اثرگذاری بیشتری برخوردارند و می‌توانند به‌عنوان مکمل، تقویت‌کننده و حتی پیش‌برنده حقوق بین‌الملل کیفری در حوزه جرائم سایبری ایفای نقش کنند.

۲-۱- نقش نهادهای سازمان ملل در توسعه و استقرار قواعد نرم حقوق بین‌الملل سایبری

در بستر پویا و پیچیدهٔ حقوق بین‌الملل سایبری، توسعه قواعد نرم (Soft Law) به‌عنوان ابزاری اساسی در گذار از پراکندگی هنجاری به‌سوی هماهنگی تدریجی تلقی می‌شود. قواعد نرم، هرچند فاقد الزام‌آوری صریح قواعد سخت حقوقی هستند، در عمل نقشی مؤثر در شکل‌دهی به هنجارهای رفتاری دولت‌ها و نهادهای فراملی ایفا می‌کنند. نهادهای مختلف وابسته به سازمان ملل متحد، از جمله شورای حقوق بشر، دفتر مقابله با مواد مخدر و جرم و گروه‌های کاری مجمع عمومی، در بسط و گسترش این قواعد، به‌ویژه در حوزه‌هایی که اغلب فاقد اجماع الزام‌آور حقوقی‌اند، سهم قابل‌توجهی داشته‌اند. کار ویژه این نهادها صرفا به تولید بیانیه‌ها و گزارش‌ها محدود نمی‌شود، بلکه شامل ایجاد بسترهایی برای اجماع‌سازی هنجاری، الگوبرداری نهادی و شکل‌دهی به رویه‌های ارجاعی است که آثار آن را می‌توان در تحول تدریجی رژیم‌های حقوقی مرتبط با جرائم سایبری مشاهده کرد (Tropina, 2020: 45).

شورای اقتصادی و اجتماعی سازمان ملل متحد از طریق نهادهای فرعی خود، به‌ویژه کمیسیون پیشگیری از جرم و عدالت کیفری، در تدوین و تقویت چارچوب‌های هنجاری مرتبط با جرائم سایبری نقشی پیشران ایفا کرده است. این نهاد با تصویب قطعنامه‌ها و تشکیل گروه‌های کارشناسی، بستر تولید قواعد شبه‌حقوقی را فراهم آورده است. برای نمونه، سند "Guidelines on the Role of Prosecutors" در تفسیر نحوهٔ مواجهه نظام‌های کیفری با جرائم رایانه‌ای، علی‌رغم فقدان الزام‌آوری حقوقی، در نظام‌های مختلف مورد استناد قرار گرفته و به‌عنوان الگویی برای رفتارهای نهادی معرفی شده است. این رویه‌سازی، بیانگر کارآمدی قواعد نرم در پر کردن خلأهای ناشی از فقدان تقنین جهانی منسجم در این حوزه است (Buçaj & Idrizaj, 2025: 33).

دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد از دیگر نهادهایی است که از طریق انتشار گزارش‌های فنی، ارائه مدل‌های قانون‌نویسی و برگزاری کنفرانس‌های تخصصی، در مسیر هنجارسازی غیر الزام‌آور مشارکت فعالی دارد. گزارش موسوم به "Comprehensive Study on Cybercrime" که در سال ۲۰۱۳ منتشر شد و همچنان در اسناد بعدی مورد ارجاع قرار می‌گیرد، نقشی محوری در ایجاد مبنای مفهومی مشترک میان دولت‌ها ایفا کرده است. این گزارش با تحلیل تفاوت‌های میان‌نظامی در مواجهه با جرائم سایبری، پیشنهادهایی برای همگرایی تدریجی ارائه داده که عمدتا توسط کشورهای در حال توسعه در فرایند مدل‌سازی حقوق داخلی مورد استفاده قرار گرفته‌اند (Sumadinata, 2023: 78).

یکی از جلوه‌های بارز قواعد نرم را می‌توان در سازوکار گروه کاری ویژه مجمع عمومی برای تدوین کنوانسیون جامع مبارزه با جرائم سایبری مشاهده کرد. این گروه که ذیل قطعنامه A/RES/74/247 تشکیل شد، بدون آنکه به تولید الزام

حقوقی مستقیم منتهی شود، از طریق ارائه اسناد، تبادل دیدگاه‌ها و طراحی اصطلاح‌شناسی مشترک، نقشی مؤثر در شکل‌دهی به زبان مشترک در حقوق سایبری بین‌الملل ایفا کرده است. مفاهیمی نظیر "Malicious Code, Cross-Border Data Access" و "Critical Infrastructure" که پیش‌تر در سطح بین‌المللی فاقد تعریف روشن بودند، از طریق فعالیت این گروه کاری وارد گفتمان حقوقی نهادینه شدند (Naseeb & Khan, 2024: 56).

در این میان، شورای حقوق بشر سازمان ملل متحد نیز از منظر حمایت از حقوق بنیادین در فضای دیجیتال، نقشی مکمل در توسعه قواعد نرم ایفا کرده است. گزارشگر ویژه آزادی بیان، به‌ویژه در گزارش A/HRC/29/32، موضوعاتی چون نظارت دولتی، حریم خصوصی و امنیت دیجیتال را وارد گفتمان بین‌المللی کرده است. این مداخلات، به‌ویژه در راستای تفسیر ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی (ICCPR) در بستر فضای سایبری، در ارتقاء هنجارهای غیر الزام‌آور نقش مؤثری داشته‌اند (Clough, 2014: 112).

مبنای حقوقی قواعد نرم در نظام حقوق بین‌الملل را می‌توان در نظریه‌های عرف‌سازی تدریجی و شکل‌گیری رویه بین‌الدولی جست‌وجو کرد. مطابق ماده ۳۸ اساسنامه دیوان بین‌المللی دادگستری، هرچند قواعد نرم در زمرهٔ منابع اصلی حقوق بین‌الملل ذکر نشده‌اند، اما می‌توان از رویه دولت‌ها و اصول کلی حقوقی به‌عنوان سازوکارهایی برای ارتقاء آنها به سطح قواعد الزام‌آور بهره گرفت. به‌ویژه در مواردی که قواعد نرم به‌طور مکرر در اسناد سازمان ملل تکرار شده و از سوی دولت‌ها در سیاست‌گذاری‌ها و اسناد داخلی اقتباس می‌شوند، قابلیت تبدیل به عرف بین‌المللی را پیدا می‌کنند (Pocar, 2004: 89).

نهادهای سازمان ملل متحد با اتکا به ظرفیت فروم‌های چندجانبه و شبکه گسترده کارشناسی، در ایجاد زمینه‌ای برای تلاقی منافع، استانداردسازی تدریجی و پذیرش جهانی قواعد غیر الزام‌آور نقش پیشرو داشته‌اند. این فرایند که در ادبیات حقوق بین‌الملل با عنوان "Diffusion of Norms" شناخته می‌شود، نقطه عزیمت حقوق بین‌الملل سایبری به‌سوی تقنین سخت تلقی می‌گردد. تأثیر گزارش‌های برنامه توسعه ملل متحد در طراحی سیاست‌های سایبری کشورهای جنوب جهانی، مؤید نقش هنجارساز این اسناد است (Buçaj & Thaqi, 2025: 47).

نقش برنامه‌های توسعه ظرفیت سازمان ملل متحد، از جمله "Cybercrime Repository" تحت نظارت UNODC، در تدوین استانداردهای رویه‌ای و مدل‌سازی نهادهای قضایی و پلیسی نیز قابل توجه است. این برنامه‌ها با معرفی رویه‌های مطلوب برای همکاری بین‌المللی در تحقیقات سایبری، علی‌رغم فقدان الزام صریح، بسترهایی را فراهم کرده‌اند که در نهایت زمینه‌ساز تصویب کنوانسیون‌های منطقه‌ای، از جمله کنوانسیون مالابو در اتحادیه آفریقا، شده‌اند (Luo, 2022: 65).

در نهایت، تعامل میان نهادهایی نظیر ITU، UNIDIR و UNCTAD در حوزه‌های تلاقی امنیت، تجارت و توسعه، بیانگر افق‌گشایی در فرایند قاعده‌سازی غیر الزام‌آور در فضای سایبری است. از این منظر، قواعد نرم تولیدشده توسط نهادهای ملل متحد نه به‌عنوان جایگزین قواعد الزام‌آور، بلکه به‌مثابه‌ی پیش‌زمینه‌هایی پویا برای تکوین تدریجی رژیم‌های حقوقی الزام‌آور بین‌المللی قابل تحلیل هستند. قواعد نرم صادره از سوی نهادهای سازمان ملل متحد، علی‌رغم فقدان الزام‌آوری مستقیم، نقشی اساسی در شکل‌دهی به فهم مشترک و هماهنگی رفتاری میان دولت‌ها ایفا می‌کنند. این قواعد با ایجاد اصطلاح‌شناسی مشترک، تعریف مفاهیم کلیدی و ارائه رویه‌های الگو، زمینه‌ای فراهم می‌آورند که نظام‌های حقوقی مختلف بتوانند ضمن حفظ چارچوب‌های بومی خود به اصول هنجاری جهانی نزدیک شوند.

از سوی دیگر، میزان اثرگذاری این قواعد نرم تا حد زیادی به مشارکت فعال دولت‌های کلیدی، تکرار و استناد مستمر به اسناد و شبکه‌سازی نهادی وابسته است. در فقدان این مؤلفه‌ها، قواعد نرم ممکن است صرفا جنبه‌ای نمادین پیدا کنند و نتوانند تحولی عملی در رژیم‌های حقوقی ایجاد نمایند. ازاین‌رو، قواعد نرم نه جایگزین معاهدات الزام‌آور، بلکه مکمل و پیش‌برندهٔ

توسعه حقوق بین‌الملل کیفری در حوزهٔ جرائم سایبری محسوب می‌شوند.

۳-۱- چالش‌های موجود در اسناد بین‌المللی در قبال تعریف و دایره شمول جرائم سایبری در حقوق بین‌الملل معاصر

تعارضات بین‌المللی در تعریف و تعیین دایرهٔ شمول جرائم سایبری، یکی از مهم‌ترین چالش‌های حقوق بین‌الملل معاصر به شمار می‌آید که در سطح اسناد تنظیمی سازمان ملل متحد و سایر کنوانسیون‌های چندجانبه به‌صورت پیچیده و چندلایه بروز یافته است. منشأ اصلی این تعارضات را می‌توان در فقدان زبان حقوقی مشترک برای توصیف، طبقه‌بندی و جرم‌انگاری رفتارهای مجرمانه در فضای سایبری جست‌وجو کرد. از یک‌سو، برخی کشورها از جمله ایالات‌متحده آمریکا و اعضای شورای اروپا با تدوین کنوانسیون بوداپست در سال ۲۰۰۱ تحت عنوان **«کنوانسیون جرائم سایبری»**، درصدد استانداردسازی بین‌المللی تعاریف این جرائم برآمدند؛ اما از سوی دیگر، کشورهای در حال توسعه و برخی دولت‌ها با نظام‌های حقوقی متفاوت، این تعاریف را نه‌تنها ناکافی، بلکه در پاره‌ای موارد ناقض حاکمیت دیجیتال خود تلقی کردند (Clough, 2014: 112).

کنوانسیون بوداپست که به‌عنوان نخستین معاهده بین‌المللی در حوزه جرائم سایبری توسط شورای اروپا تدوین شده و عضویت در آن برای کشورهای غیراروپایی نیز آزاد است، در مواد ۲ تا ۶ به تعریف جرائمی نظیر دسترسی غیرمجاز، رهگیری غیرقانونی، مداخله در داده‌ها، مداخله در سیستم‌ها و سوءاستفاده از ابزارها پرداخته است. هرچند این تعاریف در قلمرو کشورهای عضو لازم‌الاجرا هستند، اما فقدان شمول جهانی کنوانسیون و عدم الحاق قدرت‌های مهمی چون روسیه، چین و هند، موجب محدودیت جدی در کارکرد این سند به‌عنوان مرجع بین‌المللی شده است. این خلأ سبب گردیده که تعریف جرائم سایبری عمدتا تابع نظام‌های حقوق داخلی باقی بماند و اسناد سازمان ملل از وحدت مفهومی لازم در این زمینه برخوردار نباشند (Tennis, 2020: 58).

اسناد غیر الزام‌آور سازمان ملل متحد، از جمله قطعنامه ۵۵/۶۳ مجمع عمومی تحت عنوان **«مبارزه با استفاده از فناوری‌های اطلاعاتی و ارتباطاتی برای اهداف جنایی»**، نیز نتوانسته‌اند چارچوبی الزام‌آور و واجد ضمانت اجرا برای تعریف جرائم سایبری ارائه دهند. این اسناد عمدتا به طرح توصیه‌هایی کلی دربارهٔ همکاری‌های بین‌المللی، تبادل اطلاعات و ظرفیت‌سازی پرداخته‌اند و فاقد تعریف جامع یا حتی حداقلی از جرائم سایبری هستند. به همین دلیل، کارگروه‌های بین‌دولتی تحت نظارت دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد، به‌ویژه در نشست‌های سال‌های ۲۰۱۹ و ۲۰۲۱، با چالش‌های اساسی در تعیین قلمرو موضوعی کنوانسیون جهانی مقابله با جرائم سایبری مواجه شده‌اند (Buçaj & Idrizaj, 2025: 41).

یکی از ریشه‌های اساسی این تعارضات، تفاوت بنیادین میان نظام‌های حقوقی مبتنی‌بر رویکرد لیبرال غربی و نظام‌های اقتدارگرا در تعریف آزادی بیان و امنیت ملی در فضای مجازی است. برای مثال، برخی دولت‌ها مانند چین و روسیه، دامنه‌ی جرائم سایبری را به‌گونه‌ای گسترده تعریف کرده و رفتارهایی نظیر انتشار اطلاعات **«مخرب»** یا تضعیف اقتدار ملی در فضای دیجیتال را نیز در زمره این جرائم قرار داده‌اند. این در حالی است که در رویکرد کشورهای عضو اتحادیه اروپا، چنین شمولی ناقض حقوق بنیادین تضمین‌شده در اسناد بین‌المللی، از جمله ماده ۱۹ میثاق بین‌المللی حقوق مدنی و سیاسی، تلقی می‌شود (Sumadinata, 2023: 64).

تعارضات مفهومی همچنین در خصوص رفتارهایی نظیر جاسوسی سایبری، جنگ سایبری و جرائم سازمان‌یافته سایبری تشدید شده است. تاکنون هیچ‌یک از اسناد سازمان ملل متحد به‌صورت صریح این مقولات را در زمرهٔ جرائم سایبری تعریف نکرده‌اند. در کنوانسیون بین‌المللی مقابله با استفاده مجرمانه از فناوری اطلاعات، مقررات روشنی درباره جرائم منتسب به دولت–ملت‌ها پیش‌بینی نشده و این امر موجب اعتراض کشورهایی شده است که خود را قربانی حملات سایبری دولتی می‌دانند و خواستار جرم‌انگاری این رفتارها در سطح بین‌المللی هستند (Luo, 2022: 73).

نبود اجماع درباره تعاریف رفتاری نظیر نفوذ به داده‌ها، سرقت هویت دیجیتال، پول‌شویی سایبری یا حملات DDOS به‌عنوان جرائم بین‌المللی، فرایند همگرایی نظام‌های حقوقی را

با مانع جدی مواجه کرده است. برخی کشورها حمله به سامانه‌های بانک‌های مرکزی یا سیستم‌های انتخاباتی را تهدیدی علیه امنیت ملی و مصداق جرائم فراملی تلقی می‌کنند، درحالی‌که برخی دیگر این اقدامات را در زمرهٔ جرائم مالی یا حتی سیاسی دانسته و فاقد وصف کیفری بین‌المللی می‌شمارند (Buçaj & Thaqi, 2025: 49).

عدم وحدت نظری در تبیین مفهوم **«جرم سایبری»** نیز به پیچیدگی تنظیم تعاریف حقوقی دامن زده است. برخی نظریه‌پردازان، از جمله Tropina، جرم سایبری را صرفا رفتاری می‌دانند که در بستر فضای دیجیتال و با استفاده از زیرساخت‌های فناوری اطلاعات و ارتباطات ارتکاب می‌یابد؛ در مقابل، صاحب‌نظرانی مانند Pocar معتقدند صرف ارتباط با فضای سایبری کافی نیست و فعل مجرمانه باید واجد عنصر بین‌المللی، اثرگذاری بر امنیت جهانی یا اخلال در نظم بین‌المللی باشد تا قابلیت جرم‌انگاری در سطح بین‌المللی را پیدا کند.

تلاش‌های کشورهای عضو گروه ویژه G7، به‌ویژه در اسناد اجلاس ۲۰۲۱ بریتانیا، برای ارائه فهرستی از جرائم سایبری قابل شناسایی در سطح جهانی، با مخالفت کشورهای خارج از این گروه مواجه شد. منتقدان بر این باورند که این فهرست‌ها بازتاب‌دهنده اولویت‌های امنیتی خاص دولت‌های غربی است و نمی‌تواند مبنایی جامع و بی‌طرف برای تدوین یک کنوانسیون بین‌المللی تلقی شود (Nduka & Basdeo, 2022: 39).

در نهایت، فقدان هماهنگی مفهومی در تعاریف جرائم سایبری نه‌تنها انسجام حقوق بین‌الملل کیفری را با تهدید مواجه می‌سازد، بلکه زمینه سوءاستفاده دولت‌ها از خلأهای تعریفی برای سرکوب مخالفان یا پوشش فعالیت‌های اطلاعاتی خود تحت عنوان **«مقابله با جرائم سایبری»** را نیز فراهم می‌آورد. ازاین‌رو، دستیابی به تعریفی جهانی، دقیق و عاری از بار ایدئولوژیک از جرائم سایبری در اسناد تنظیمی سازمان ملل متحد، ضرورتی اجتناب‌ناپذیر برای تحقق نظم حقوقی مؤثر در عصر دیجیتال به شمار می‌رود.

تعارضات موجود در تعاریف جرائم سایبری، ریشه در تفاوت‌های بنیادین میان نظام‌های حقوقی و فقدان زبان مشترک حقوقی دارد. در غیاب چنین زبان مشترکی، هر دولت بر اساس اولویت‌ها و ملاحظات سیاسی و امنیتی خود، تعریفی متفاوت از جرائم سایبری ارائه می‌دهد و این امر به پراکندگی حقوقی و نبود چارچوبی منسجم در سطح بین‌المللی منجر شده است.

همچنین، حتی تلاش‌ها برای تدوین فهرست‌های جرائم سایبری یا اسناد الزام‌آور، در صورت فقدان مشارکت و اجماع جهانی، قادر به رفع این تعارضات نخواهند بود. بر این اساس، ایجاد یک مرجع تفسیر حقوقی مشترک و الزام‌آور با قابلیت حل اختلاف و هماهنگ‌سازی رویه‌ها، ضرورتی اساسی تلقی می‌شود تا وحدت مفهومی و همگرایی عملی میان نظام‌های حقوقی تقویت شده و امکان سوءاستفاده دولت‌ها از خلأهای تعریفی به حداقل برسد.

۲- تحلیل انتقادی معاهده جهانی جرائم سایبری با تمرکز بر نقش هماهنگ‌کننده سازمان ملل

معاهده جهانی جرائم سایبری که در مجامع بین‌المللی، به‌ویژه در چارچوب سازمان ملل متحد، مطرح شده است، کوششی آشکار در جهت ایجاد یک نظام حقوقی فراگیر و هماهنگ برای مواجهه با تهدیدهای سایبری محسوب می‌شود. با این وجود، این معاهده نه‌تنها از حیث ساختار حقوقی، بلکه از منظر نقش سازمان ملل متحد به‌عنوان هماهنگ‌کننده اصلی این فرآیند، با چالش‌های بنیادینی روبه‌رو است؛ چالش‌هایی که تحلیل انتقادی آنها مستلزم بررسی هم‌زمان ابعاد حقوقی، نهادی و سیاسی می‌باشد. سازمان ملل در مقام نهاد هماهنگ‌کننده، باید از توانایی لازم برای مدیریت تعارض منافع میان دولت‌ها، مواجهه با تنوع و تکثر در تفسیر مفاهیم حقوقی و تضمین اجرای عادلانه و منصفانه مقررات در قالب یک نظام چندجانبه برخوردار باشد؛ نظامی که بر اصول برابری دولت‌ها، حاکمیت قانون و احترام به حقوق بشر در فضای مجازی استوار است (Tennis, 2020: 45). اهمیت این بخش در برجسته ساختن نقشی فراتر از صرف تدوین مقررات برای سازمان ملل نهفته است، زیرا پیچیدگی ذاتی فضای سایبری و اختلاف دیدگاه‌های موجود میان دولت‌ها نشان می‌دهد که موفقیت این معاهده،

بیش از هر چیز، مستلزم هماهنگی دقیق و مؤثر میان دولت‌هاست.

در همین راستا، کنوانسیون با استناد به ماده ۶ ناظر بر احترام به حقوق بشر و سایر تضمین‌های پیش‌بینی‌شده، دولت‌ها را ملزم می‌سازد که اختیارات و قدرت‌های خود را در حوزه مقابله با جرائم سایبری به‌گونه‌ای متناسب و در چارچوب تشریفات قضایی اعمال کنند، به‌نحوی که اعمال این صلاحیت‌ها منجر به نقض حقوق بنیادین افراد در فضای مجازی نگردد.

۲-۱- چالش‌های حقوقی کنوانسیون مقابله با جرائم سایبری و تعارض با قوانین داخلی

از جمله مهم‌ترین چالش‌های حقوقی کنوانسیون مقابله با جرائم سایبری می‌توان به خطر تفاسیر موسع یا مضیق مقررات توسط دولت‌ها، تعارض احتمالی با تعاریف گسترده‌تر یا متفاوت موجود در قوانین داخلی برخی کشورها و فقدان تعریف جامع و واحد از مفهوم **«جرائم سایبری»** اشاره کرد؛ امری که موجب تمرکز کنوانسیون بر برخی مصادیق خاص جرائم سایبری و در نتیجه ایجاد صلاحیت‌های متقابل و بعضا متعارض می‌گردد. افزون‌بر این، خطر سوءاستفاده از سازوکارهای پیش‌بینی‌شده در کنوانسیون برای تعقیب فراملی فعالان مدنی و سیاسی، یکی دیگر از نگرانی‌های اساسی در این حوزه به‌شمار می‌رود. همچنین، نیاز به هماهنگی گسترده با قوانین داخلی کشورها در زمینه استرداد مجرمان و ارائه معاضدت‌های قضایی، در کنار تحمیل بار عملیاتی سنگین بر نظام‌های قضایی ملی، از دیگر چالش‌های اجرایی این معاهده محسوب می‌شود.

معاهده، علی‌رغم تلاش برای ارائه تعریفی جامع از جرائم سایبری، با مسئله هم‌پوشانی قواعد کیفری داخلی دولت‌ها و احتمال بروز تعارض میان آن‌ها مواجه است. به‌عنوان نمونه، ماده ۴ معاهده که به جرم‌انگاری دسترسی غیرمجاز به سامانه‌های اطلاعاتی می‌پردازد، از حیث کلی با مفاد ماده ۲ کنوانسیون بوداپست ۲۰۰۱ هم‌خوانی دارد؛ با این حال، ابهام موجود در تعریف **«دسترسی غیرمجاز»** می‌تواند زمینه‌ساز تعارض در تفسیر و اجرا در نظام‌های حقوقی مختلف گردد. افزون‌بر این، موادی که به همکاری قضایی بین‌المللی اختصاص یافته‌اند، از جمله ماده ۲۳، الزامات پیچیده‌ای را ایجاد می‌کنند که به‌دلیل ملاحظات حاکمیتی دولت‌ها و فقدان اعتماد متقابل، در عمل به‌صورت ناقص اجرا می‌شوند (Clough, 2014: 112). این اختلافات تفسیری و هم‌پوشانی‌های قانونی، ضرورت طراحی سازوکارهای مؤثر حل‌وفصل اختلافات و ایجاد هماهنگی حقوقی بین‌المللی را بیش‌ازپیش برجسته می‌سازد.

۲-۲- نقش سازمان ملل به‌عنوان هماهنگ‌کننده در کنوانسیون مقابله با جرائم سایبری

نقش سازمان ملل متحد به‌عنوان هماهنگ‌کننده در فرآیند تدوین و تصویب کنوانسیون مقابله با جرائم سایبری، موسوم به کنوانسیون هانوی را می‌توان در قالب سه مرحله متمایز **«تسهیل‌گری»**، **«اجماع‌سازی»** و **«پشتیبانی»** مورد تحلیل قرار داد. این نقش، هرچند با چالش‌ها و انتقادهای حقوقی و سیاسی همراه بوده است، در نهایت به تصویب نخستین معاهده الزام‌آور جهانی در حوزه جرائم سایبری انجامیده که می‌توان آن را نقطه عطفی در تاریخ همکاری‌های بین‌المللی در این زمینه دانست.

سازمان ملل متحد در ایفای این نقش باید در چارچوب سازوکارهای حاکم بر معاهدات بین‌المللی و اصول مقرر در کنوانسیون وین درباره حقوق معاهدات ۱۹۶۹ عمل کند. ماده ۲۶ این کنوانسیون بر اصل اجرای تعهدات بین‌المللی با حسن نیت تأکید دارد و ماده ۲۷ نیز تصریح می‌کند که دولت‌ها نمی‌توانند به قوانین داخلی خود به‌عنوان توجیهی برای عدم اجرای تعهدات بین‌المللی استناد کنند (Buçaj & Thaqi, 2025: 89). بر این اساس، نقش سازمان ملل فراتر از صرف تدوین مقررات حقوقی است و این نهاد باید به‌عنوان هماهنگ‌کننده اجرای منصفانه تعهدات و حل تعارضات میان قوانین داخلی دولت‌ها و الزامات بین‌المللی کنوانسیون عمل کند.

علاوه‌بر این، کنوانسیون باید در حوزهٔ توانمندسازی کشورهای در حال توسعه نیز نقشی فعال ایفا نماید. یکی از ارکان کلیدی این سند، حمایت از کشورهایی است که با **«شکاف توانایی دیجیتال»** مواجه‌اند. بر اساس ماده ۶۰ کنوانسیون و نیز بیانیه‌های دبیرکل سازمان ملل متحد، این سازمان موظف است از طریق دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد (UNODC)، کمک‌های فنی، برنامه‌های آموزشی و انتقال

فناوری را در اختیار کشورهای در حال توسعه قرار دهد تا این کشورها نیز بتوانند به‌طور مؤثر در مقابله با جرائم سایبری مشارکت کنند.

۳-۲- تعارض رویکردها به حاکمیت دیجیتال در کنوانسیون مقابله با جرائم سایبری

تعارض رویکردها نسبت به مفهوم حاکمیت دیجیتال در کنوانسیون مقابله با جرائم سایبری، از جمله کنوانسیون هانوی، یکی از مهم‌ترین ابعاد ژئوپلیتیکی این معاهده به شمار می‌آید. این تعارضات نه‌تنها در فرآیند مذاکرات و تدوین کنوانسیون، بلکه در متن نهایی و چالش‌های اجرایی آن نیز بازتاب یافته است. تحلیل این اختلافات را می‌توان در قالب سه رویکرد اصلی بررسی کرد: رویکرد غربی که بر حاکمیت محدود دولت‌ها و جریان آزاد داده‌ها تأکید دارد؛ رویکرد چین و روسیه که قائل به حاکمیت مطلق دیجیتال و کنترل گسترده دولتی بر فضای مجازی هستند؛ و در نهایت، رویکرد میانه کشورهای جنوب جهانی که بیشتر بر امنیت زنجیرهٔ تأمین، حفاظت از زیرساخت‌های حیاتی و محلی‌سازی داده‌ها تمرکز دارد.

در این چارچوب، برداشت‌ها از مفهوم **«حاکمیت دیجیتال»** به‌شدت متنوع است، به‌گونه‌ای که برخی دولت‌ها بر اعمال کنترل گسترده و ملاحظات امنیت حاکمیتی تأکید می‌ورزند، درحالی‌که گروهی دیگر آزادی اینترنت و محدودسازی مداخلات دولتی را اصل بنیادین می‌دانند. این دوگانگی رویکردی، به‌ویژه در بخش‌های مربوط به تبادل اطلاعات، استرداد متهمان و همکاری‌های قضایی بین‌المللی، به ایجاد خلأهایی در ضمانت اجرا و تضعیف اثربخشی کنوانسیون منجر شده است (Buçaj & Idrizaj, 2025: 134). در این شرایط، سازمان ملل متحد ناگزیر است چارچوبی انعطاف‌پذیر اما در عین حال منسجم، برای ایجاد توازن میان این دیدگاه‌های متعارض ارائه کند.

۴-۲- جرائم فناوری‌های نوظهور در کنوانسیون مقابله با جرائم سایبری

مطالعه کنوانسیون بین‌المللی مقابله با جرائم سایبری سازمان ملل متحد، موسوم به کنوانسیون هانوی، نشان می‌دهد که این سند در مواجهه با جرائم ناشی از فناوری‌های نوظهور، رویکردی نسبتا محافظه‌کارانه و بعضا ناهمگون اتخاذ کرده است. اگرچه کنوانسیون در برخی موارد گام‌هایی در جهت به‌روزرسانی مفاهیم حقوقی برداشته، اما در قبال چالش‌های پیچیده ناشی از فناوری‌هایی نظیر هوش مصنوعی، بلاک‌چین و اینترنت اشیاء، یا سکوت اختیار کرده یا به ارجاعات کلی بسنده نموده است.

ماده ۱۰ معاهده تلاش دارد برخی رفتارهای مرتبط با فناوری‌های نوظهور، از جمله هوش مصنوعی و اینترنت اشیاء را تحت پوشش قرار دهد؛ با این حال، فقدان اجماع جهانی درباره ماهیت، آثار و مخاطرات این فناوری‌ها، زمینه‌ساز بروز اختلاف در تفسیر و اجرای این مقررات شده است. از این‌رو، انتظار می‌رود سازمان ملل متحد از طریق ایجاد کارگروه‌های تخصصی و تقویت همکاری‌های بین‌بخشی، به تدوین استانداردهای علمی و حقوقی روشن و قابل‌اتکا در حوزه فناوری‌های نوظهور مبادرت ورزد.

افزون‌بر این، معاهده از فقدان یک سازوکار مؤثر برای پایش اجرای تعهدات و نبود نهاد داوری یا نظارتی مشخص رنج می‌برد. هرچند ماده ۲۷ بر همکاری‌های آموزشی و تبادل اطلاعات تأکید دارد، اما در غیاب ساختارهای الزام‌آور، این مقررات بیشتر جنبه توصیه‌ای پیدا می‌کنند و از کارایی لازم برخوردار نیستند (Naseeb & Khan, 2024: 66).

در مجموع، معاهدهٔ پیشنهادی، هرچند گامی ضروری در جهت شکل‌دهی به نظم حقوقی سایبری در سطح بین‌المللی محسوب می‌شود، اما بدون اصلاحات اساسی در حوزه تعریف جرائم، تقویت مکانیزم‌های اجرایی، تضمین مؤثر حقوق بشر و مدیریت تعارضات ژئوپلیتیکی، قادر به تحقق کامل اهداف خود نخواهد بود. در این میان، سازمان ملل متحد باید نقش هماهنگ‌کننده خود را از طریق ارتقاء شفافیت مذاکرات، تحکیم همکاری‌های چندجانبه و تضمین مشارکت مؤثر تمامی ذی‌نفعان ایفا کند تا این معاهده به چارچوبی حقوقی جامع، منسجم و فراگیر تبدیل شود. حضور فعال، مستمر و راهبردی سازمان ملل، شرطی اساسی برای موفقیت معاهده است و بدون آن، این سند نخواهد توانست جایگاه حقوقی جهانی لازم را به دست آورد.

نتیجه‌گیری

تحلیل روندهای تقنینی در سطح بین‌المللی نشان می‌دهد که مواجهه جامعه جهانی با پدیده جرائم سایبری همچنان از فقدان انسجام ساختاری و محتوایی رنج می‌برد. اگرچه نهادهای مختلف زیرمجموعه سازمان ملل متحد، از جمله دفتر مقابله با مواد مخدر و جرم سازمان ملل متحد (UNODC) و مجمع عمومی سازمان ملل متحد (UNGA)، در این حوزه اقدامات و ابتکارهایی را دنبال کرده‌اند، اما استانداردهای الزام‌آور همراه با ضمانت اجرای مؤثر برای مقابله با طیف پیچیده و رو به گسترش جرائم سایبری در چارچوب حقوق بین‌الملل کیفری هنوز به‌صورت نهادینه تثبیت نشده‌اند. تصویب قطعنامه A/RES/74/247 در سال ۲۰۱۹ و تشکیل کمیته ویژه برای تدوین معاهده جهانی جرائم سایبری را می‌توان گامی ساختاری و نهادی در این مسیر تلقی کرد؛ با این حال، اختلافات عمیق و پایدار میان بلوک‌های ژئوپولیتیکی مختلف در خصوص تعاریف بنیادین، نظام صلاحیت کیفری و سازوکارهای همکاری فراملی، مانع از دستیابی به پیشرفت‌های ماهوی و کارآمد در فرآیند تدوین این معاهده شده است.

کنوانسیون جهانی ارائه‌شده در سال ۲۰۲۳ در مواد ۶ تا ۱۰ تلاش کرده است با جرم‌انگاری مصادیق متداولی نظیر دسترسی غیرمجاز به سامانه‌های اطلاعاتی، اختلال در داده‌ها و سوءاستفاده از ابزارهای سایبری، نوعی یکپارچگی مفهومی در حوزه جرائم سایبری ایجاد کند؛ با این حال، اتخاذ رویکردی موسع و فاقد مرزبندی مفهومی دقیق، بستر لازم را برای شکل‌گیری تفسیرهای متعارض در اجرای حقوق کیفری فراملی فراهم می‌آورد. در همین چارچوب، ماده ۱۳ که به سوءاستفاده از ابزارهای رمزنگاری اختصاص یافته است، به دلیل فقدان معیارهای عینی و مشخص برای تفکیک میان استفاده مشروع و رفتار مجرمانه از فناوری‌های نوین، نه‌تنها با اصل قانونی بودن جرم و مجازات در تعارض قرار می‌گیرد، بلکه می‌تواند زمینه‌ساز سوءاستفاده‌های سیاسی در فرآیند تعقیب کیفری نیز باشد.

نظام صلاحیتی پیش‌بینی‌شده در ماده ۲۳ معاهده، هرچند اصل وجود صلاحیت‌های همپوشان میان دولت‌ها را به رسمیت می‌شناسد، اما به‌طور هم‌زمان فاقد هرگونه سازوکار مشخص برای حل تعارض یا اولویت‌بندی اعمال صلاحیت‌هاست. این خلأ نهادی می‌تواند به بروز رقابت‌های قضایی، صدور آرای متعارض و در نهایت بی‌ثباتی رویه‌های قضایی در سطح بین‌المللی منجر شود. افزون بر این، عدم پیش‌بینی سازوکار داوری یا امکان ارجاع اختلافات تفسیری به دیوان بین‌المللی دادگستری، چشم‌انداز اجرای منسجم و هماهنگ مقررات کنوانسیون را بیش‌ازپیش تضعیف می‌کند.

از منظر حقوق بشر، تعارض میان مفاد معاهده و تعهدات بین‌المللی دولت‌ها در حوزه حقوق دیجیتال همچنان به‌صورت حل‌نشده باقی مانده است. در مواد مرتبط با نظارت، جمع‌آوری ادله دیجیتال و تبادل اطلاعات، ضوابط الزام‌آور و روشنی برای تضمین حفاظت از حریم خصوصی و آزادی بیان پیش‌بینی نشده است؛ امری که می‌تواند به مشروعیت‌بخشی به چارچوب‌های نظارتی تهاجمی از سوی دولت‌ها بینجامد و توازن حساس میان الزامات امنیتی و حقوق و آزادی‌های بنیادین را بر هم زند.

در مجموع، مدل تعامل سازمان ملل متحد که عمدتا بر رضایتمندی و اجماع دولت‌ها استوار است، در شرایطی که اختلافات بنیادین حقوقی، فناورانه و سیاسی میان بازیگران بین‌المللی وجود دارد، کارآمدی لازم را از خود نشان نمی‌دهد. تا زمانی‌که تعاریف کیفری شفاف، نظام صلاحیتی منسجم، سازوکار حل اختلاف مشخص و ملاحظات حقوق بشری به‌طور نهادی در متن معاهده نهادینه نشوند، استانداردهای پیشنهادی نه‌تنها قابلیت تبدیل‌شدن به حقوق سخت (Hard Law) را نخواهند داشت، بلکه می‌توانند به عاملی برای تشدید بی‌اعتمادی میان دولت‌ها بدل شوند. از این‌رو، سازمان ملل متحد باید فراتر از صرف تدوین متون حقوقی، به طراحی و تبیین سازوکارهای تنفیذ، نظارت و تفسیر مقررات بپردازد و نقش خود را در شکل‌دهی به نظم کیفری جهانی در عصر سایبری، به‌صورت نظام‌مند، پایدار و مؤثر ایفا نماید.

ملاحظات اخلاقی: موارد مربوط به اخلاق در پژوهش و نیز امانت‌داری در استناد به متون و ارجاعات به مقاله تماما رعایت گردید.

تعارض منافع: در تدوین این مقاله، هیچ‌گونه تعارض منافعی وجود نداشته است.

سهم نویسندگان: نگارش این مقاله به‌صورت مشترک توسط نویسندگان انجام شده است.

تشکر و قدردانی: از تمام کسانی که نویسندگان را در تهیه این مقاله یاری رسانده‌اند، سپاسگزاریم.

منابع و مآخذ

الف. منابع فارسی

– افضلی، رسول؛ قالیباف، محمدباقر؛ احمدی فیروزجائی، میثم (۱۳۹۲). «تبیین تحولات مفهوم مرز در فضای سیاسی مجازی». *پژوهش‌های جغرافیای انسانی*، ۴۵(۱).

– جلالی فراهانی، امیرحسین (۱۳۸۹). *درآمدی بر آیین دادرسی کیفری جرائم سایبری*. تهران: خرسندی.

– دی‌آنجلیز، جینا (۱۳۸۳). *جرائم سایبر*. ترجمه سعید حافظی و عبدالصمد خرم‌آبادی، تهران: دبیرخانه شورای عالی اطلاع‌رسانی.

– متین دفتری، احمد (۱۳۸۷). *سیر تحول حقوق بین‌الملل دریایی از گرو سیوس تا کنفرانس‌های ژنو*. تهران: گنج دانش.

ب. منابع انگلیسی

- Buçaj, E & Idrizaj, K (2025). "The Need for Cybercrime Regulation on a Global Scale by International Law and Cyber Convention". *Multidisciplinary Reviews*, 8(1): 2025024.

- Buçaj, E & Thaqi, A (2025). "Global Regulation of Cybercrime through International Law and Cyber Conventions". *Kriminologie – Das Online-Journal | Criminology – The Online Journal*, 7: 155–170.

- 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.

- Luo, D (2022). "Progress, Prospects, and Outlook of Global Convention on Combating Cybercrime from the Perspective of International Law". *International Journal of Cyber Criminology*, 16(2): 175–191.

- Naseeb, S & Khan, W. N (2024). "Mitigating Cybercrime Through International Law: The role of Global Cybersecurity Agreements". *Mayo Communication Journal*, 1(1): 31–40.

- Nduka, R. E., & Basdeo, V. (2022). "The need for Harmonised and Specialised Global Legislation to Address the Growing Spectre of Cybercrime". *Southern African Public Law*, 36(2): 22–31.

Pocar, F. (2004). "New Challenges for International Rules against Cyber-Crime". *European Journal on Criminal Policy and Research*, 10: 27–37.

Sumadinata, W. S. (2023). "Cybercrime and Global Security Threats: A Challenge in International Law". *Russian Law Journal*, 11(3): 438–444.

Tennis, M. M. (2020). "A United Nations Convention on Cybercrime". *Capital University Law Review*, 48: 189.

Tropina, T. (2020). Cybercrime: Setting International Standards. In *Routledge Handbook of International Cybersecurity* (pp. 148–160). Routledge.