Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

فصلنامه علمی فقه و حقوق نوین

Print ISSN: 2717- 1469
Online ISSN: 2717 – 1477

ISC.SID.NOORMAGZ.MAGIRAN
GOOGLESCHOLAR.ENSANI
www.jaml .ir

سال ۱۴۰۴، سال ششم، شماره ۲۵،
صفحات۱۸-۱

همکاری های بین المللی در مقابله با جرم سایبری با تاکید بر کنوانسیون بوداپست

فرزانه اسدی خلیق گروه حقوق، جزا و جرم شناسی، دانشگاه آزاد اسلامی،واحد تبریز، ایران

نازنین حسن پور گروه حقوق، جزا و جرم شناسی، دانشگاه آزاد اسلامی،واحد تبریز، ایران

چکیده

در عصر دیجیتال، جرایم سایبری به یکی از چالش‌های جدی امنیت ملی و بین‌المللی تبدیل شده‌اند. ماهیت فراملی این جرایم، ضرورت همکاری‌های بین‌المللی گسترده را برای مقابله مؤثر با آنها ایجاب می‌کند. کنوانسیون بوداپست سال ۲۰۰۱ به عنوان نخستین معاهده بین‌المللی جامع در زمینه مبارزه با جرایم سایبری، چارچوبی حقوقی برای هماهنگی قوانین داخلی، تقویت همکاری‌های قضایی و تسهیل تحقیقات فرامرزی فراهم آورده است.این پژوهش با هدف تحلیل مکانیسم‌های همکاری بین‌المللی در مقابله با جرایم سایبری، کارآمدی کنوانسیون بوداپست را در مواجهه با جرایم سنتی و نوظهور سایبری مورد ارزیابی قرار می‌دهد. جرایم موضوع این کنوانسیون شامل دسترسی غیرمجاز به سیستم‌های کامپیوتری، جعل و کلاهبرداری رایانه‌ای، محتوای غیرقانونی و نقض حقوق مالکیت معنوی است. با این حال، تحولات تکنولوژیک منجر به ظهور جرایم جدیدی همچون باج‌افزارها، حملات بات‌نت، جرایم مرتبط با هوش مصنوعی، سوءاستفاده از رمزارزها برای پولشویی، حملات به زیرساخت‌های حیاتی، دیپ‌فیک‌های مجرمانه و بهره‌برداری از اینترنت اشیاء شده است که چالش‌های نوینی را برای نظام حقوقی بین‌المللی ایجاد کرده‌اند. پژوهش حاضر به بررسی ظرفیت‌ها و محدودیت‌های کنوانسیون بوداپست در پاسخگویی به این جرایم نوظهور می‌پردازد و نقش پروتکل‌های الحاقی و اصلاحات پیشنهادی را تحلیل می‌کند. همچنین، موانع همکاری بین‌المللی از جمله تفاوت‌های نظام‌های حقوقی، حفظ حاکمیت ملی، چالش‌های حفظ حریم خصوصی و عدم عضویت برخی کشورهای کلیدی مورد بحث قرار می‌گیرد. یافته‌های این تحقیق می‌تواند به تدوین سیاست‌های جنایی ملی و بین‌المللی مؤثرتر و ارتقای مکانیسم‌های همکاری قضایی در فضای سایبری کمک نماید.

این پژوهش با رویکرد توصیفی-تحلیلی و با استفاده از روش اسنادی-کتابخانه‌ای انجام می‌شود.

واژگان کلیدی: جرم سایبری؛ کنوانسیون؛ بوداپست؛ حقوق جزا؛ بین الملل

طبقه‌بندی JEL: فقه – حقوق – جزا و جرم شناسی – حقوق بین الملل – حقوق خصوصی

Journal of
Modern Jurisprudence and Law
Homepage: http://www.jaml.ir

International Cooperation in Combating Cybercrime with Emphasis on the Budapest Convention

Scientific Journal of Modern Jurisprudence and Law

Print ISSN: 2717- 1469
Online ISSN: 2717 - 1477

Profile in ISC,SID, Noormags, Magiran, Ensani, GoogleScholar
www.jaml .ir

Year 2025و Sixth year ,Issue 25

Pages 1-18

Farzaneh Asadi Khaliq Department of Law, Criminal Law and Criminology, Islamic Azad University, Tabriz Branch, Iran

Nazanin Hassanpour Department of Law, Criminal Law and Criminology, Islamic Azad University, Tabriz Branch, Iran

Abstract

In the digital age, cybercrimes have become one of the serious challenges to national and international security. The transnational nature of these crimes necessitates extensive international cooperation to effectively combat them. The 2001 Budapest Convention, as the first comprehensive international treaty to combat cybercrimes, has provided a legal framework for harmonizing domestic laws, strengthening judicial cooperation, and facilitating cross-border investigations. This study aims to analyze the mechanisms of international cooperation in combating cybercrimes and evaluates the effectiveness of the Budapest Convention in dealing with traditional and emerging cybercrimes. The crimes covered by this convention include unauthorized access to computer systems, computer fraud and forgery, illegal content, and infringement of intellectual property rights. However, technological developments have led to the emergence of new crimes such as ransomware, botnet attacks, AI-related crimes, misuse of cryptocurrencies for money laundering, attacks on critical infrastructure, criminal deepfakes, and exploitation of the Internet of Things, which have created new challenges for the international legal system.The present study examines the capacities and limitations of the Budapest Convention in responding to these emerging crimes and analyzes the role of additional protocols and proposed amendments. Also, obstacles to international cooperation, including differences in legal systems, maintaining national sovereignty, privacy protection challenges, and the non-membership of some key countries, are discussed. The findings of this study can help formulate more effective national and international criminal policies and promote judicial cooperation mechanisms in cyberspace.

This study is conducted with a descriptive-analytical approach and using a documentary-library method.

Keywords: Cybercrime; Convention; Budapest; Criminal Law; International

JEL Classification: Jurisprudence - Law - Criminal and Criminology - International Law - Private Law

مقدمه

گسترش فناوری اطلاعات و ارتباطات و تحول دیجیتال جوامع، فرصت‌های بی‌سابقه‌ای را برای توسعه اقتصادی، اجتماعی و فرهنگی فراهم آورده است. با این حال، این تحولات به موازات مزایای خود، چالش‌های امنیتی و حقوقی جدیدی را نیز به همراه داشته‌اند. فضای سایبری به عرصه‌ای برای ارتکاب جرایم نوین تبدیل شده که ماهیت فرامرزی، سرعت اجرا، ناشناس‌بودن مرتکبان و دشواری شناسایی و تعقیب آنها، مقابله با این جرایم را برای نظام‌های عدالت کیفری ملی با چالش‌های جدی مواجه ساخته است. جرایم سایبری نه تنها امنیت افراد، بلکه امنیت ملی، اقتصادی و زیرساخت‌های حیاتی کشورها را تهدید می‌کنند و خسارات میلیاردی را به اقتصاد جهانی تحمیل می‌نمایند. در این راستا، ضرورت همکاری‌های بین‌المللی برای مقابله مؤثر با این پدیده، بیش از پیش احساس می‌شود.کنوانسیون بوداپست راجع به جرایم سایبری، مصوب ۲۳ نوامبر ۲۰۰۱ میلادی، نخستین سند بین‌المللی جامع و الزام‌آور در حوزه مبارزه با جرایم رایانه‌ای است که توسط شورای اروپا تدوین و در سال ۲۰۰۴ لازم‌الاجرا گردید. این کنوانسیون با هدف ایجاد هماهنگی در قوانین کیفری داخلی کشورها، تسهیل همکاری‌های قضایی فرامرزی، و تأمین ابزارهای حقوقی لازم برای جمع‌آوری و تبادل شواهد دیجیتال، چارچوبی نوآورانه برای مقابله با جرایم سایبری ارائه نموده است. تاکنون بیش از ۷۰ کشور از قاره‌های مختلف به این کنوانسیون ملحق شده‌اند و آن را به مهم‌ترین ابزار حقوقی بین‌المللی در این حوزه تبدیل کرده‌اند. با وجود این، تحولات سریع تکنولوژیک و ظهور جرایم نوظهور سایبری، کارآمدی این کنوانسیون را با چالش‌هایی مواجه ساخته است.

هدف از این پژوهش، تحلیل حقوقی مکانیسم‌های همکاری بین‌المللی مندرج در کنوانسیون بوداپست و ارزیابی ظرفیت این سند در پاسخگویی به جرایم سایبری سنتی و نوظهور است. با توجه به اینکه جرایم مبتنی بر فناوری‌های نوین همچون هوش مصنوعی، رمزارزها، و اینترنت اشیاء در زمان تدوین کنوانسیون پیش‌بینی نشده بودند، بررسی شکاف‌های موجود در نظام حقوقی بین‌المللی و ارائه راهکارهای حقوقی برای تقویت همکاری‌های بین‌المللی ضروری می‌نماید. این تحقیق در پی پاسخ به این پرسش اساسی است که آیا کنوانسیون بوداپست و پروتکل‌های الحاقی آن، ابزارهای کافی برای مقابله با جرایم سایبری قرن بیست و یکم فراهم می‌آورند و چه اصلاحات و تکمیل‌هایی برای ارتقای کارآمدی نظام همکاری بین‌المللی مورد نیاز است.

۱-کلیات

۱-۱-تعریف و ویژگی‌های فضای سایبر

کلمه سایبر از لحاظ ریشه‌ای به معنی سکاندار است و از نظر مفهومی دلالت بر خودکار شدن کنترل مصنوعی و رایانه‌ای شدن دارد. برخی فضای سایبر را فضای خیالی و برخی دیگر فضای سایبر دور از واقعیت را می پندارند اما بعضی دیگر بر این باور هستند که فضای سایبر واقعی و حاضر است و آن را با ذخیره و انتقال الکترونیکی اطلاعات برابر گرفته‌اند نقطه

بعضی نیز آن را با ارتباطات در شبکه‌های رایانه‌ای یکسان پنداشته‌اند.[۱]

همچنین ، مهمترین عنصر در نگرشی که محیط مجازی را یک جهان به موازات جهان واقعی می‌داند گستره بی‌منتهای فضای مجازی باشد ، گستره‌ای که دائماً در حال قبض و بسط است و شاید کم از گستره جهان واقعی نداشته باشد. در کنار این موضوع برخی ویژگی‌های فضای مجازی که از آن به عنوان فرا متغیر[۲] یاد می‌شود شامل سرعت بالا ، فرامکانی بودن ، انتشار یافتگی و تکثر پذیری ، تعاملی بودن و تشدید واقعیت مویدی بر جهان دگر بودن فضای مجازی است.[۳]

۱-۲-تعریف جرایم سایبری

جرایم سایبری شامل جرایمی است که توسط اشخاص در محیط سایبر ارتکاب می‌یابند. جرایمی همچون کلاهبرداری رایانه‌ای ، جعل رایانه‌ای ، جاسوسی رایانه‌ای ، تخریب و اخلالگری(سابوتاژ) رایانه‌ای ، دستتیابی و شنود غیر مجاز رایانه‌ای از جمله جرایم سایبری هستند. چنین به نظر می‌رسد ویژگی خاص فضای سایبر سبب شده تا همان گونه که افراد مرتکب جرایم سایبری می‌شوند دولت‌ها نیز بتوانند مرتکب جرایم سایبری شوند. در حقیقت در این فضا بعضی دولت‌ها علاوه بر جنگ ، به جرم و تروریسم دست می‌زنند در صورتی که افراد علاوه بر جرم و تروریسم به جنگ نیز دست می‌زنند. سازمان همکاری و توسعه اقتصادی ، جرایم سایبری را سوء استفاده از رایانه شامل هر نوع رفتار غیرقانونی ، غیر اخلاقی یا غیر مجاز که مربوط به پردازش اتوماتیک و انتقال داده‌ها می‌باشد تعریف می‌نماید.[۴]

۱-۳- انواع جرایم سایبری

کنگره دهم سازمان ملل متحد این جرایم را در دسته زیر تفکیک کرده است:

الف. جرم های ارتکابی علیه فناوری‌ها و کاربران آنها ، دستیابی غیر مجاز به رایانه یا سیستم‌های رایانه‌ای ، استفاده غیر مجاز از سیستم‌های رایانه‌ای ، خواندن ، کپی کردن یا کپی گرفتن داده بدون اجازه ، ایجاد یا تمهید برنامه‌های مهاجم ، تخریب داده‌ها و سیستم‌های رایانه‌ای مورد استفاده عموم خرابکاری رایانه‌ای.

ب. جرم های سنتی ارتکابی با استفاده از رایانه یا فناوری‌های ارتباطی ، جرم‌های مربوط به محتوای مجرمانه ، کودک ربایی اینترنتی به جهت سوء استفاده جنسی ، کلاهبرداری ، جاسوسی صنعتی یا تجاری ، جرم‌های مربوط به مالکیت فکری ، قاچاق ، پولشویی

---

[۱] -عاملی، سعیدرضا(۱۳۹۶)، فلسفه فضای مجازی، تهران: انتشارات امیرکبیر،ص۹۲

[۲] - فرا متغیرها ، عواملی هستند که همه چیز را تحت تاثیر قرار می‌دهند و در یک رابطه متقابل ، تاثیر و تاثر پذیری پیچیده‌ای بر یکدیگر نیز دارند.

[۳] - انصاری ، باقر؛ انصاری ، اسماعیل(۱۳۹۱) ، حقوق اطلاعات از منظر تحلیل اقتصادی ، مجله مطالعات حقوق تطبیقی ، دوره ۳ ، شماره ۲ ،ص ۸

[۴] -خداقلی ، زهرا(۱۳۸۴) ، جرایم کامپیوتری ، چاپ اول ، انتشارات آریان ،ص ۲۹

پ. استفاده از فناوری برای حمایت از دیگر فعالیت‌های مجرمانه.[1]

۱-۴- تاریخچه جرایم سایبری

جرایم سایبری از زمان پیدایش تاکنون با سه نسل یا تیپ روبرو گشته است. دهه‌های ۶۰ و ۷۰ و اوایل ۸۰ زمان حاکمیت نسل اول تحت عنوان جرایم رایانه‌ای است. در این زمان در مورد جرایم ، محوریت بحث با رایانه بود .به همین جهت تعداد توصیف‌های مجرمانه بسیار کم بود. به تدریج در دهه ۸۰ تا اوایل دهه ۹۰ نسل دوم ایجاد گردید که بحث محتوا مورد استفاده قرار گرفت یعنی به موضوع جرایم داده و اطلاعات توجه شد. به همین جهت نسل دوم تحت عنوان جرایم علیه داده‌ها مطرح گردید. پس از ۴ یا ۵ سال ، حاکمیت نسل سوم که از آن به جرایم سایبری یاد می‌شود به وجود آمد که ویژگی این نسل تجمیع رایانه با مودم و مخابرات با حالات شبیه‌سازی و مجازی‌سازی است. در این نسل تاکید بر رایانه نیست بلکه رایانه خود وسیله ارتکاب جرم است.جرایم نسل سوم در بستر شاهراه‌های الکترونیکی ارتباطی و اطلاعاتی به وقوع می‌پیوندند. اگر در ۴ دهه حاکمیت جرایم رایانه ، شاهد جرایم انگشت شمار بودیم اما در فضای سایبر ۵ دسته اصلی جرم وجود دارد که هر کدام بالغ بر چندین عنوان مطرح هستند و شاید تعداد مصادیق عمد و غیر عمد آن بالغ بر ۲۰۰ عنوان مجرمانه شود. نخستین جرم سایبری در ایران به سال ۱۳۸۱ و ناظر به عمل دانشجویان برای اسکن اسکناس و پرینت رنگی از آن عطف شده اما گزارش‌های غیر رسمی حاکی از این است که در دهه ۶۰ تغییر نمرات درسی و تغییر بعضی از اسامی پذیرفته شده در کنکور ۶۴ اتفاق افتاد.[2]

۱-۵-ماهیت کنوانسیون بوداپست

کنوانسیون بوداپست، یکی از اسناد بین‌المللی است که در سال ۲۰۰۱ به امضای ۲۶ کشور از اعضای شورای اروپا و چهار دولت غیرعضو (ژاپن، ایالات متحده، کانادا و آفریقای جنوبی) رسیده است. کنوانسیون در ۴۸ ماده و چهار فصل تصویب شد. فصل اول؛ به بیان اصطلاحات ، و فصل دوم؛ به بیان تدابیری که باید در حقوق ماهوی و شکلی داخلی اتخاذ شوند، پرداخته است. در فصل سوم؛ به همکاریهای بین‌المللی، و در نهایت در فصل چهارم؛ به مقررات پایانی، اشاره شده است. کمیسیون، در بخش موضوعات حقوق ماهوی، مقررات جرم انگاری را با سایر مقررات مربوط به حوزه جرایم رایانه‌ای یا مرتبط با رایانه و سپس مسئولیت و ضمانت اجراهای تبعی را بحث نموده و جرایمی که در کنوانسیون تعریف شده‌اند را برشمرده است. بقیه جرایم نیز عبارتند از: دسترسی غیرقانونی (غیرمجاز)، شنود غیرقانونی (غیرمجاز)، مختل کردن داده‌ها، مختل کردن سیستمها، جعل مرتبط با رایانه، کلاهبرداری مرتبط با رایانه، جرایم مرتبط با هرزه‌نگاری کودکان و جرایم مرتبط با حق نشر و حقوق همجوار.[3]

---

[1] -لک، بهزاد(۱۳۹۱)، شناسایی و پیشگیری از کمین سایبری در فضای مجازی، مجله کارآگاه، دوره دوم، سال پنجم، شماره۱۸،ص۹۵

[2] - شیرزاد ، کامران(۱۳۸۸) ، جرایم رایانه‌ای ، چاپ اول ، تهران: نشر بهینه فراگیر ،ص ۲۳

[3] -جلالی فراهانی، امیرحسین(۱۳۸۹)، کنوانسیون جرایم سایبر و پروتکل الحاقی آن با همراه گزارش توجیهی، چاپ اول، معاونت حقوق و توسعه قوه قضاییه،ص۱۵

۱-۶- اهداف اصلی کنوانسیون

اهداف اصلی کنوانسیون عبارتند از: ۱- هماهنگ کردن عناصر تشکیل دهنده جرم در حقوق جزای ماهوی داخلی و مقررات راجع به آن در حوزه جرایم سایبر ۲- اعطای اختیارات لازم در آیین دادرسی کیفری داخلی برای تحقیق و تعقیب اینگونه جرایم و همچنین سایر جرایمی که به وسیله سیستم‌های رایانه‌ای ارتکاب می‌یابند یا ادله الکترونیکی مرتبط با جرایم ۳-پایه ریزی رژیم سریع و کارآمد همکاری بین‌المللی.[۱]

در مجموع مقصود کنوانسیون، ارتقای ابزارهای پیشگیری و متوقف کردن جرایم رایانه‌ای یا مرتبط با رایانه است که با وضع معیارهای حداقلی مشترک برای آنها محقق میشود. این نوع هماهنگ سازی، مبارزه با چنین جرایمی را در دو سطح ملی و بین‌المللی آسان میکند. همگرایی قوانین داخلی میتواند از سوءاستفاده‌های ناشی از انتقال ارتکاب یک فعل به کشور عضوی که معیار پیشین پایینتری دارد، پیشگیری کند. در نتیجه، تجارب مشترک مفید به دست آمده از رسیدگی عملی به پرونده‌ها نیز می‌تواند بطور گسترده مبادله شود. برای مثال، همکاری بین‌المللی (به ویژه برای استرداد و معاضدت قضایی دوجانبه) در خصوص مقررات راجع به بحث تعقیب و تحقیق، باعث تسهیل در مقابله‌ی همه جانبه با جرم موردنظر می‌شود.[۲]

۱-۷-دستاوردهای کنوانسیون

کنوانسیون، برای دولتهای عضو شورای اروپا و سایر دولتهای امضاءکننده این کنوانسیون، با این دیدگاه که هدف شورای اروپا دستیابی به اتحاد بزرگتر اعضایش است، با ارج نهادن به ارزش تقویت همکاری با سایر کشورهایی که به این کنوانسیون ملحق می‌شوند، سیاست جنایی مشترکی را به عنوان یک اولویت در حمایت از جامعه در برابر جرایم سایبر، با اقداماتی از قبیل تصویب قوانین مناسب و گسترش همکاری‌های بین‌المللی پایه‌ریزی نموده است.[۳]

در ادامه‌ی این سیاست، به حمایت از منافع مشروع استفاده و توسعه فناوری اطلاعات و حمایت از داده‌های شخصی و حمایت از حقوق بشر و آزادی‌های اساسی ۱۹۵۰ و میثاق بین‌المللی سازمان ملل راجع به حقوق مدنی و سیاسی ۱۹۶۶و همچنین سایر معاهدات قابل اجرای بین‌المللی حقوق بشری که بار دیگر بر حق هر کس در داشتن عقیده بدون دخالت دیگران و حق آزادی ابراز عقیده که شامل حق آزادی جستجو، دریافت و نشر اطلاعات و هر نوع عقیده، بدون ملاحظه مرزها، و حقوق راجع به احترام حریم خصوصی می‌شود، پرداخته است. سپس با امعان نظر به کنوانسیون سازمان ملل راجع به حقوق کودک ۱۹۸۹و کنوانسیون سازمان بین‌المللی کار راجع به بدترین اشکال کار کودکان ۱۹۹۹و با مدنظر قرار دادن

---

۱ - Gallagher, Borchgraze, Cillusso, William H. Webster, Frank J. Cilluffo, Berkowitz, S. Lan ; Cybercrime, Cyber terrorism, Cyber warfare , Averting an Electronic waterloo, Center for Strategic & International Studies,1998, P.5.

۲ - Davis, Benjamin.R; Ending the Cyber Jihad: Combating terrorists explation of the internet with the rule of low and improved tools for cyber governance, common low conspectus, volume 15, 2006-2007, P.122.

۳ - Pollitt, Mark.M; Cyberterrorism: Fact or Fancy, Proceedings of the 20th National Information Systems Security Conference, October 1997, pp. 285–289

کنوانسیون‌های کنونی شورای اروپا در زمینه همکاری کیفری، در کنار معاهده‌های مشابه میان دولتهای عضو شورای اروپا و سایر دولتها و تأکید بر این موضوع که کنوانسیون حاضر به عنوان مکمل آن کنوانسیون‌ها و در راستای مؤثرتر کردن تحقیق‌ها و آیین دادرسی کیفری راجع به جرایم مرتبط با سیستم‌ها و داده‌های رایانه‌ای و امکانپذیر کردن جمع آوری ادله الکترونیکی جرایم ارتکابی است.[۱]

همچنین، در قطعنامه شماره ۳ که در بیست و سومین گردهمایی وزرای دادگستری اروپا به تصویب رسیدو با توجه به برنامه اقدام سران دولتهای شورای اروپا که به مناسبت دومین اجلاس خود در استراسبورگ ۱۰ و ۱۱ اکتبر ۱۹۹۷ برای یافتن راه حل‌های مشترک جهت پایه‌ریزی فناوری‌های اطلاعات نوین بر اساس معیارها و ارزشهای شورای اروپا به تصویب رساندند، با آنچه که در کنوانسیون در مورد جرم انگاری رفتارها و ضمانت اجراها و مسئولیت‌های تبعی بیان شده، موافقت شده است مسئله‌ای که در جرایم معنونه در کنوانسیون مطرح شده، این است که رفتارهای مجرمانه بایدبدون حق باشد لذا با این شرط، کنوانسیون اعمالی را که با مجوز قانونی صورت می‌گیرد، از شمول جرم انگاری‌ها خارج کرده است و علاوه بر آن ، جرایم مندرج در کنوانسیون باید از روی عمد ارتکاب یابند تا مسئولیت کیفری قابل اعمال باشد.[۲]

ایضاً اینکه، مسئله دیگری که در سیاست جنایی کنوانسیون جرایم سایبر، قابل بحث است بازدارندگی از جرایم سایبری در آینده از طریق تعیین مجازات‌ها می‌باشد.(ماده۱۳ کنوانسیون) و تعیین ضمانت اجراهای کیفری را به صلاحدید نظام حقوق داخلی کشور واگذار کرده است این مسئله اجرای کنوانسیون را سست می‌کند چرا که جنبه بازدارندگی مجازاتها یک امر نسبی بر اساس ضمانت اجراهایی که کشورها تعیین کرده‌اند خواهد بود و شاید به خاطر همین مسئله و مسائل دیگر است که برخی‌ها به فکر کنوانسیون جهانی علیه جرایم سایبر شده-اند چرا که نیازهای جامعه‌ی امروز را برآورده نمی‌کند.[۳]

۲-مبارزه با جرایم سایبری در حقوق بین‌الملل وکنوانسیون بوداپست

مبارزه با جرایم سایبری در سطح بین‌المللی، تحولی اساسی در نظام حقوق جزای بین‌الملل محسوب می‌شود که ضرورت آن از دهه ۱۹۹۰ میلادی با گسترش فناوری اطلاعات به طور جدی احساس شد. کنوانسیون بوداپست که در ۲۳ نوامبر ۲۰۰۱ توسط شورای اروپا به تصویب رسید و در ۲۰۰۴ لازم‌الاجرا

---

[۱] - Goodman, Seymour. E and Kirk, Jessica C and Kirk Megan H; Cyberspace as a medium for terrorists, Technological Forecasting & Social Change, vol 74, 2007, p. 194

[۲] - Denning, Dorothy; Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, in Networks and net wars: the future of terror, crime and militancy, Sponsored by Nautilus Institute,1999, P.281.

[۳] -رضوی فرد، بهزاد؛ موسوی، سیدنعمت الله(۱۳۹۵)، مسئولیت کیفری در فضای سایبر در حقوق ایران، فصلنامه پژوهش حقوق کیفری، دوره۵، شماره۱۶،ص۳۸

گردید، نخستین معاهده بین‌المللی جامع در این حوزه است که چارچوبی حقوقی برای جرم‌انگاری هماهنگ، قواعد آیین دادرسی کیفری در فضای سایبری، و مکانیسم‌های همکاری بین‌المللی فراهم آورده است. این کنوانسیون در چهار فصل اصلی به تعریف جرایم سایبری، دسترسی غیرمجاز، جعل و کلاهبرداری رایانه‌ای، محتوای غیرقانونی، و نقض مالکیت معنوی پرداخته و مواد ۲۳ تا ۳۵ آن به تنظیم ابزارهای همکاری بین‌المللی همچون کمک قضایی متقابل، استرداد مجرمان، و ایجاد شبکه ۲۴/۷ برای پاسخگویی فوری اختصاص یافته است. با وجود دستاوردهای قابل توجه و الحاق بیش از ۷۰ کشور از قاره‌های مختلف، عدم عضویت برخی کشورهای کلیدی همچون روسیه و چین به دلیل نگرانی‌های مربوط به حاکمیت ملی، و همچنین خلأهای موجود در پاسخگویی به جرایم نوظهور مبتنی بر هوش مصنوعی و فناوری‌های غیرمتمرکز، از چالش‌های اساسی این کنوانسیون در تحقق هدف جهانی‌سازی مبارزه با جرایم سایبری به شمار می‌رود.

۲-۱-ضرورت اتخاذ سیاست جنایی هماهنگ بین المللی پلیس در مقابله با جرایم سایبری

پلیس به عنوان یک نهاد اجرایی، نقشی موثر در پیشگیری، مبارزه و کاستن وقوع بزه در جامعه داشته است. وقوع این جرائم برخلاف جرائم سنتی پیشین در محیطی غیر فیزیکی محقق می‌شود و آنچه بیش از پیش وظایف نهادهای پیشگیرانه و کنترل کننده این نوع جرایم از جمله پلیس را خطیر می‌کند، این می‌باشد که روش‌های سنتی، در پیشگیری و مبارزه با این جرایم پاسخگو نیست. ماهیت و ویژگی‌های خاص جرایم سایبری از جمله داشتن ابعاد جهانی و فراملی، فقدان توافق جهانی پیرامون تعریف قانونی واحد از جرایم سایبری، بالا بودن سرعت ارتکاب این جرایم، فقدان رویه‌های مشخص پیرامون همکاری‌های متقابل و بالا بودن هزینه‌های کشف این جرایم، مراجع قضایی و انتظامی را با چالش مواجه نموده است که در حال حاضر کشور ما به هیچ کدام از کنوانسیون‌های مبارزه با جرایم سایبری نپیوسته، اما خصوصیات ویژه جرایم ارتکابی در فضای مجازی، مبنی بر داشتن جنبه فراملی و بین المللی، لزوم حکومت قواعدی از این قبیل را به این دسته از جرایم، بیش از هر چیز دیگری مشخص می‌نماید. در حال حاضر پلیس ضروری است با استفاده از نرم‌افزارهای قدرتمندی که در اختیار او قرار دارد، با گشتزنی و مراقبت در فضای مجازی، در پیشگیری از وقوع جرایم سایبری نقش موثری ایفا نماید. تعامل و همکاری مناسب میان شرکت‌های مخابراتی ارائه کننده این قبیل خدمات و پلیس می‌تواند در فرایند پیشگیری کمک شایانی نموده باشد، آموزش همگانی و همچنین شناسایی و ارائه آموزش‌های خاص به اشخاص و سازمان‌هایی که احتمال می‌رود در معرض جرایم سایبری قرار گیرند یکی دیگر از شیوه‌های پیشگیری از این جرایم است. همچنین به نظر

می‌رسد باید نوعی تبادل اطلاعات در راستای مبارزه با جرایم سایبری انجام گیرد.[1]

استفاده از اینترنت در سطح جهان، چالش‌هایی را در جهت مدیریت و قانونمندسازی ایجاد کرده است. راهبری اینترنت از جمله موضوعات گسترده‌ای از اداره فنی آن تا مباحث عمومی‌تر همچون نظارت بر محتوی می‌شود. با توجه به گستردگی مباحث امنیت فضای مجازی و وسعت تهدیدات، ذینفعان و بازیگران بسیاری در این فضا، به طور برجسته‌ای واکاوی نقش پلیس در زمینه تامین امنیت در فضای مجازی بسیار اهمیت دارد. لذا پلیس به عنوان نماد حاکمیت و ضابط قضایی در پیشبرد سیاست جنایی اجرایی نقش مهمی ایفا می‌نماید. جایگاهی که نهاد پلیس برای تامین امنیت در فضای مجازی دارد تعیین کننده مدل سیاست جنایی است که حاکم بر روابط پلیس با دیگر نهادهای کیفری است. در حقیقت آنچه مهم است درک و برداشت پلیس از نوع ناهنجاری‌هایی که نیازمند پاسخ محسوب شده و ماهیت پاسخ‌های پلیس به ناهنجاری‌های حوزه فضای مجازی و مباحث مرتبط با امنیت است.

در نتیجه، برای مقابله همه جانبه و کارآمد با جرم سایبری ، نیازمند بهره‌گیری از یک سیاست جنایی فراگیر با مشارکت گسترده جامعه مدنی، کاربران سایبری و سازمان‌های مردم نهاد آشکار می‌شود. تبیین نقش پلیس در سیاست‌های تامین امنیت در فضای مجازی، با شناختی جامع از آسیب‌ها و چالش‌های پیش روی پلیس در قبال تهدیدات فضای مجازی، منطبق با سیاست‌های کلی امنیت در تعامل با دیگر نهادها ممکن می‌باشد. النهایه اینکه، پلیس به عنوان یکی از اصلی‌ترین نهادهای مقابله و پیشگیری از تهدیدات فضای مجازی اگر شناخت دقیقی از هنجارهای حاکم بر فضای مجازی، الویت‌های تامین امنیت، ماهیت و ویژگی‌های تهدیدات و تاثیر این تهدیدات بر امنیت فضای حقیقی داشته باشد بهتر می‌تواند در تحقق سیاست‌های کلان امنیت فضای مجازی گام بردارد.[2]

۲-۲-چهارچوب‌های بین المللی همکاری پلیس در مقابله با جرایم سایبری بین المللی

پروسه رشد فنّاوری اطلاعات و ارتباطات وظایف سخت و پیچیده‌ای را برای پلیس خدمتگزار به همراه آورده است و با توجه به این مهم آسیب پذیری کارکنان ناجا در محیط سایبری حتمی بوده و یکی از راهکارهای ممکن در این حوزه، پرداختن به آموزش و مهارت افزایی کارکنان ناجا در پیشگیری از وقوع جرم در فضای سایبر است. همچنین، نقش اطلاعات در ارتقای فنّاوری‌ها و دغدغه‌های اطلاعاتی موجب می‌شود تا تلاش‌هایی برای ارتقای فنّاوری اطلاعات در ناجا صورت بگیرد.ایضاً اینکه، تدبیر و تحدید بحران-ها تنها از طریق شناخت نظم ویژه، منطق و قانونمندی خاص هر بحران میسر است و در این راستا داشتن اطلاعات و اشراف اطلاعاتی از اهمیت بسیاری در پیشگیری از وقوع جرم برخوردار است؛

۱ - میر ترابی وهمکاران(۱۳۹۹) ، نقش پلیس در پیشگیری از جرایم سایبری با تاکید بر قوانین موضوعه ، فصلنامه علمی مطالعات بین المللی پلیس ، دوره یازدهم ، شماره ۴ ،ص ۱۰۹

۲ - محسنی، فرید؛ صوفی زمرد، محسن(۱۳۹۶)، پلیس و چالش‌های اجرایی تامین امنیت سایبری، فصلنامه پژوهش‌های دانش انتظامی، سال بیستم، شماره چهارم،ص۱۸۲

همچنین، مهمترین رسالت و مزیت شبکه‌های رایانه‌ای، اشتراک منابع سخت افزاری و نرم افزاری و دستیابی سریع و آسان به اطلاعات به صورت هدفمند است که این خود زمینه-ای برای ایجاد جرائم رایانه‌ای است؛ علاوه برآن، مهمترین شیوهٔ رایج و تأثیرگذار در فضای مجازی عملیات روانی دشمن است، که اعتقادات، فکر و ذهن حریف را در اختیار می‌گیرد و امروزه کاربرد ویژه‌ای در فضای سایبر دارد؛ با توجه به نیازمندی‌های اطلاعاتی در فضای مجازی و رشد نرم افزارها در این زمینه آسیب پذیری سازمان‌های نظامی و انتظامی را دوچندان نموده است و خود بستری برای ایجاد جرائم رایانه‌ای است؛ به دیگر سخن، آموزش کارکنان ناجا در خصوص جرائم رایانه‌ای و آشنا نمودن کارکنان با قوانین مربوط با این دسته از جرائم بسیار مهم است.[1]

۲-۳-کنوانسیون بین المللی جرایم سایبری بوداپست

معاهده بوداپست در شناسائی بین‌المللی تسلیم میکروارگانیسم‌ها برای استفاده در تشریفات ثبت اختراع که به معاهده بوداپست مشهور است یک معاهده بین‌المللی است که در بوداپست، مجارستان، در تاریخ ۲۸ آوریل ۲۸ ژانویه ۲۰۲۴ میلادی امضا شد. این قانون در تاریخ ۹ اوت ۱۹۸۰ اجرایی شد و سپس در ۲۶ سپتامبر ۱۹۸۰ اصلاح شد. این پیمان توسط سازمان جهانی مالکیت فکری اداره می‌شود. از ژوئیه سال ۲۰۱۹، ۸۲ کشور عضو معاهده بوداپست هستند. الحاق این پیمان برای دولت‌های عضو کنوانسیون پاریس برای حمایت از مالکیت صنعتی سازمان مالکیت صنعتی منطقه‌ای آفریقا (ARIPO)، سازمان ثبت اختراعات اوراسیا (EAPO) و سازمان ثبت اختراعات اروپا (EPO) طبق ماده ۹ پیمان‌نامه مجاز می‌باشد. بر اساس مفاد این معاهده، یک کشور متعاهد که تسلیم میکروارگانیسم‌ها را برای استفاده از تشریفات ثبت اختراعات اجازه داده یا آن را اجباری می‌کند، موظف است که یک میکروارگانیسم را نزد مقام یا مرکز سپرده‌گذاری بین‌المللی بسپارد و بدون در نظر گرفتن این که چه مقام یا مرکزی در داخل یا خارج از آن قلمرو است، نسبت به شناسایی و رسمیت بخشیدن به آن اقدام کند.[2]

۲-۴-سازوکارهای حمایت از بزه‌دیدگان جرایم رایانه‌ای در اسناد بین المللی و کنوانسیون بوداپست

در باب حمایت کیفری که هم نقش پیشگیرانه از وقوع جرایم را داشته و هم نقش پیشگیری از بزه دیدگی را ایفا می‌کند با بررسی قوانین و مقررات موجود در این زمینه مشخص می‌شود که قانونگذار ایران با وجود جرم انگاری برخی رفتارها اصل تناسب جرم و مجازات را با توجه به محیط خاص رایانه‌ای رعایت نکرده است. محیط رایانه‌ای با توجه به ویژگی‌های خاص خودش شایسته تعیین ضمانت جاهای متناسب با آن محیط در راستای حمایت از بزه‌دیدگان جرایم رایانه‌ای است. حمایت از بزه‌دیدگان خاص به ویژه کودکان و زنان از جمله قربانیان مورد توجه در این محیط است که قانونگذاران سعی می‌کنند چتر حمایتی خویش را نسبت به چنین افرادی

---

۱ - کوچی ، سعید(۱۳۹۵) ، نقش مهارت افزایش کارکنان ناجا برای پیشگیری از جرایم فضای مجازی ، فصنامه علمی مطالعات حفاظت و امنیت اجتماعی ، سال یازدهم ، شماره ۴۱ ،ص ۱۳۰

۲ - پورجاهد، محمد (۱۳۹۵)، بررسی حقوقی جرایم سایبری ایران در پرتو کنوانسیون جرایم سایبری، پایان نامه برای دریافت درجه کارشناسی ارشد، رشته حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تفت، ص ۵۶

دوچندان کنند. در باب حمایت شکلی از بزه دیدگان جرایم رایانه‌ای باید گفت که مقنن ایران تا حدودی همگام با اسناد بین المللی از حمایت ویژه خویش دریغ نکرده است و توجه مقنن به صلاحیت ایران در باب رسیدگی به بزه‌دیدگان خاص از جمله سامانه‌های رایانه‌ای و مخابراتی و تارنماهای مورد استفاده یا تحت کنترل قوای سه گانه یا نهاد رهبری و یا توجه به بزه دیدگان اشخاص کمتر از ۱۸ سال و نیز پیش بینی قضات و مراجع تخصصی موید این امر است. پیش بینی ساز و کار ناشی از بزه‌دیدگی جرایم یکی دیگر از مقوله‌های حمایت از بزه دیدگان است که در مقررات خاص جرایم رایانه‌ای غیر قابل ملموس است و انتظار می‌رفت که مقنن در راستای حمایت خاص و ویژه حمایت‌های مالی و معنوی خاص با توجه به آن محیط تعیین می‌کرد. چالش دیگری که ممکن است حمایت از بزه دیدگان جرایم رایانه‌ای را با مشکل مواضع سازد همکاری‌های متقابل میان کشورها است که کنوانسیون جرایم سایبر هم به آن توجه کرده است. موضوع حمایت اجتماعی از بزه دیدگان جرایم رایانه‌ای نه تنها در قوانین خاص مرتبط با جرایم رایانه‌ای بلکه در قوانین عام نیز مورد بی‌مهری قرار گرفته است[۱].

۳-چالش های حقوق جزایی در اجرای همکاری بین المللی بر مبنای کنوانسیون بوداپست

یکی از اساسی‌ترین چالش‌هایی که کنوانسیون بوداپست با آن روبروست، تفاوت‌های بنیادین در نظام‌های حقوقی کشورهای مختلف است. این تفاوت‌ها نه تنها در سطح تعریف و عناصر تشکیل‌دهنده جرایم سایبری بلکه در زمینه اصول بنیادین حقوق جزا نیز خود را نشان می‌دهند. برای مثال، برخی کشورها دسترسی غیرمجاز به سیستم‌های رایانه‌ای را صرفاً در صورت وقوع ضرر مادی قابل مجازات می‌دانند، در حالی که کشورهای دیگر صرف نقض امنیت سیستم را کافی می‌شمارند. این ناهماهنگی در جرم‌انگاری، مشکلات عملی جدی در زمینه استرداد مجرمان ایجاد می‌کند، چرا که اصل مجازات مضاعف که پیش‌شرط بسیاری از معاهدات استرداد محسوب می‌شود، در این موارد تحقق نمی‌یابد. علاوه بر این، تفاوت در سطح مجازات‌های تعیین شده برای جرایم مشابه در کشورهای مختلف، موجب می‌شود که مجرمان سایبری به دنبال پناهگاه‌های امن باشند و از کشورهایی که نظام کیفری سخت‌گیرانه‌تری دارند به سوی کشورهایی با قوانین انعطاف‌پذیرتر مهاجرت کنند.

چالش دیگری که اجرای مؤثر کنوانسیون را با مشکل مواجه ساخته، تنش میان الزامات همکاری بین‌المللی و اصول بنیادین حاکمیت ملی و حفظ حریم خصوصی شهروندان است. ماده ۳۲ کنوانسیون که امکان دسترسی فرامرزی به داده‌های ذخیره شده را بدون نیاز به اخذ مجوز از کشور میزبان سرور فراهم می‌آورد، با واکنش‌های شدید حقوقی و سیاسی مواجه شده است. بسیاری از کشورها این مقررات را نقض حاکمیت ملی خود تلقی می‌کنند و معتقدند که هرگونه جمع‌آوری شواهد دیجیتال از قلمرو یک کشور باید با رعایت

[۱] - پورقهرمانی، بابک (۱۳۹۶)، مطالعه تطبیقی سازوکارهای حمایت از بزه‌دیدگان جرایم رایانه‌ای در حقوق کیفری ایران و اسناد بین المللی با تاکید بر کنوانسیون بوداپست، نشریه پژوهشنامه حقوق کیفری، شماره ۱۵، ص ۳۲

مقررات داخلی آن و از طریق کانال‌های رسمی همکاری قضایی صورت پذیرد. این تنش در مورد کشورهایی که به کنوانسیون نپیوسته‌اند، مانند روسیه و چین که خود منشأ بخش قابل توجهی از جرایم سایبری هستند، حادتر می‌شود. در کنار این مسئله، دغدغه‌های مربوط به حفاظت از داده‌های شخصی و تعارض کنوانسیون بوداپست با مقررات سخت‌گیرانه حریم خصوصی همچون GDPR اروپا، اجرای مؤثر مقررات کنوانسیون را پیچیده‌تر ساخته است.از سوی دیگر، کندی و پیچیدگی فرآیندهای کمک قضایی متقابل که کنوانسیون بوداپست برای تسهیل آنها طراحی شده، در عمل همچنان یکی از مهم‌ترین موانع اجرایی به شمار می‌رود. تحقیقات نشان می‌دهند که پاسخ به درخواست‌های کمک قضایی متقابل گاهی ماه‌ها و حتی سال‌ها به طول می‌انجامد، در حالی که شواهد دیجیتال به دلیل ماهیت فرار و قابل تغییر خود، ممکن است در این مدت از بین بروند یا دستکاری شوند. این مشکل زمانی حادتر می‌شود که داده‌ها در سرورهای ابری ذخیره شده باشند که جایگاه فیزیکی آنها به سرعت تغییر می‌کند و تعیین صلاحیت قضایی را با ابهام مواجه می‌سازد. همچنین، کمبود منابع مالی و انسانی متخصص در بسیاری از کشورها، به ویژه کشورهای در حال توسعه، مانع از اجرای مؤثر تعهدات کنوانسیون می‌شود. این کشورها اغلب فاقد زیرساخت‌های فنی و نیروی انسانی آموزش‌دیده برای تحقیقات سایبری پیشرفته هستند و در نتیجه نمی‌توانند به درخواست‌های همکاری به موقع و کارآمد پاسخ دهند.

۱-۳-بررسی مشکلات ناشی از تفاوت نظام های کیفری ملی در تعقیب جرایم سایبری

تفاوت‌های بنیادین در نظام‌های کیفری ملی، یکی از پیچیده‌ترین موانع در مسیر تعقیب و مجازات مرتکبان جرایم سایبری محسوب می‌شود. این تفاوت‌ها در سه سطح اصلی خود را نمایان می‌سازند: نخست، در سطح جرم‌انگاری که برخی رفتارها در یک کشور جرم تلقی می‌شوند اما در کشور دیگر مشروع یا حداکثر تخلف اداری به شمار می‌آیند. برای نمونه، انتشار برخی محتواهای سیاسی یا مذهبی در فضای سایبری ممکن است در کشوری جرم سنگین تلقی شود اما در کشور دیگر مصداق آزادی بیان باشد. دوم، در سطح عناصر تشکیل‌دهنده جرم که تعریف رکن مادی و معنوی یک جرم سایبری خاص در نظام‌های مختلف متفاوت است. سوم، در سطح ضمانت اجراها که میزان مجازات‌های تعیین شده برای جرایم مشابه در کشورها تفاوت چشمگیری دارد و این امر تأثیر مستقیم بر امکان استرداد مجرمان و اجرای احکام خارجی می‌گذارد. این ناهماهنگی‌ها موجب شده است که مجرمان سایبری با شناخت دقیق از شکاف‌های حقوقی موجود، فعالیت‌های خود را از کشورهایی سازماندهی کنند که نظام کیفری آن‌ها ضعیف‌تر یا در مواردی حتی مصون‌کننده این رفتارها است.

در بعد عملیاتی، این تفاوت‌ها مشکلات جدی در زمینه جمع‌آوری و پذیرش شواهد دیجیتال ایجاد می‌کنند. قواعد اثبات دعوا و استانداردهای پذیرش دلیل الکترونیکی در محاکم مختلف، تفاوت‌های اساسی دارند؛ برخی نظام‌ها معیارهای سخت‌گیرانه‌ای برای احراز صحت و اعتبار شواهد دیجیتال وضع کرده‌اند که با معیارهای کشورهای دیگر همخوانی ندارد. همچنین، اصول حاکم بر تفتیش و بازرسی در فضای سایبری، محدودیت‌های مربوط به نقض حریم خصوصی، و ضوابط نگهداری داده‌ها در کشورهای مختلف به

گونه‌ای متفاوت تنظیم شده‌اند که اغلب شواهد به دست آمده در یک کشور به دلیل نقض قوانین حریم خصوصی یا اصول دادرسی عادلانه، در محاکم کشور دیگر قابل استناد نیستند. علاوه بر این، تفاوت در سطح توسعه فناوری و توانایی‌های فنی دستگاه‌های عدالت کیفری، شکاف عمیقی میان کشورهای توسعه‌یافته و در حال توسعه ایجاد کرده است. بسیاری از کشورهای در حال توسعه فاقد زیرساخت‌های لازم برای تحلیل فورنزیک دیجیتال، ردیابی تراکنش‌های رمزارزی، و شناسایی مرتکبان در شبکه‌های پیچیده سایبری هستند، و این ناتوانی فنی در کنار تفاوت‌های حقوقی، تعقیب جرایم سایبری فرامرزی را تقریباً غیرممکن می‌سازد.

۲-۳-دشواری در تعیین مرجع صالح برای رسیدگی به جرایم با بعد چند ملیتی

تعیین صلاحیت قضایی در جرایم سایبری با بعد فرامرزی، یکی از پیچیده‌ترین مسائل حقوق جزای بین‌الملل محسوب می‌شود که ریشه در ماهیت غیرمادی فضای سایبری دارد. برخلاف جرایم سنتی که معمولاً محل وقوع مشخصی دارند و صلاحیت قضایی بر اساس اصول سرزمینی، شخصی یا حمایتی قابل تعیین است، جرایم سایبری اغلب در فضایی رخ می‌دهند که مرزهای جغرافیایی در آن معنای سنتی خود را از دست داده‌اند. یک حمله سایبری ممکن است توسط فردی در کشور الف طراحی، از طریق سرورهای واقع در کشور ب اجرا، علیه قربانیانی در کشور ج انجام شود، و داده‌های مربوطه در ابرهای مجازی واقع در کشورهای د و ه ذخیره گردند. در چنین سناریویی، تعیین اینکه کدام کشور صلاحیت اولیه برای رسیدگی به جرم را دارد، با ابهامات حقوقی جدی مواجه است. کنوانسیون بوداپست در ماده ۲۲ تلاش کرده است با پذیرش اصول صلاحیت سرزمینی، شخصی و در مواردی صلاحیت جهانی، راهکاری برای این معضل ارائه دهد، اما در عمل تداخل صلاحیت‌ها و تعارض میان ادعاهای صلاحیتی کشورهای مختلف همچنان پابرجاست.

مشکل اصلی زمانی بروز می‌کند که چندین کشور همزمان بر اساس ضوابط مختلف، صلاحیت رسیدگی به یک جرم سایبری را مدعی شوند. در غیاب یک مرجع بین‌المللی واحد برای حل این تعارضات، امکان دارد مرتکب یک جرم سایبری در کشورهای مختلف به اتهامات متعدد و گاه متناقض متهم شود، که این امر نه تنها با اصل منع مجازات مضاعف (non bis in idem) در تعارض قرار می‌گیرد، بلکه موجب سردرگمی و عدم قطعیت حقوقی می‌شود. برای مثال، در پرونده‌های مربوط به نقض داده‌های شخصی یا حملات باج‌افزاری که صدها هزار قربانی در کشورهای مختلف دارند، هر یک از این کشورها می‌توانند بر اساس اصل حمایت از اتباع خود یا اصل سرزمینی به دلیل وجود قربانی در خاک خود، صلاحیت رسیدگی را مطالبه کنند. این وضعیت منجر به رقابت قضایی میان کشورها شده و در بسیاری از موارد به دلیل عدم هماهنگی، پرونده‌ها

بلاتکلیف می‌مانند یا مرتکب به دلیل پیچیدگی‌های حقوقی از مجازات می‌گریزد.[۱]

چالش دیگری که دشواری تعیین مرجع صالح را دوچندان می‌کند، مسئله تعیین محل وقوع جرم در فضای سایبری است. در حقوق جزای سنتی، محل وقوع جرم معمولاً بر اساس نظریه‌های مختلف مانند نظریه محل انجام رفتار مجرمانه، محل تحقق نتیجه، یا نظریه وحدت محل تعیین می‌شود. اما در جرایم سایبری که رفتار مجرمانه و نتیجه آن ممکن است در مکان‌ها و زمان‌های مختلفی واقع شوند و حتی تعیین دقیق این مکان‌ها به دلیل استفاده از فناوری‌های ناشناس‌ساز مانند شبکه‌های VPN و Tor دشوار باشد، اعمال این نظریه‌ها با مشکل اساسی مواجه است. همچنین، برخی جرایم سایبری مانند توزیع بدافزارها یا ایجاد شبکه‌های بات‌نت، ماهیت مستمر دارند و در طول زمان در قلمروهای متعدد اثرات خود را بروز می‌دهند، که تعیین یک محل واحد برای وقوع جرم را تقریباً غیرممکن می‌سازد. این ابهامات حقوقی نه تنها موجب فرار مجرمان از عدالت می‌شود، بلکه منابع محدود دستگاه‌های عدالت کیفری کشورهای مختلف را نیز در تحقیقات موازی و غیرهماهنگ هدر می‌دهد.

۳-۳-خلأهای کنوانسیون بوداپست در پاسخ به جرایم نوپدید و فناوری های غیرمتمرکز

کنوانسیون بوداپست که در آغاز هزاره سوم میلادی تدوین شد، اساساً برای مقابله با جرایم سایبری نسل اول طراحی گردیده است و به همین دلیل در برابر جرایم نوظهور مبتنی بر فناوری‌های پیشرفته، خلأهای قابل توجهی را نشان می‌دهد. یکی از بارزترین این خلأها، عدم پیش‌بینی جرایم مرتبط با هوش مصنوعی و یادگیری ماشین است. امروزه شاهد ظهور جرایمی هستیم که در آنها الگوریتم‌های هوش مصنوعی خودکار به ارتکاب اعمال مجرمانه می‌پردازند، مانند سیستم‌های خودکار کلاهبرداری، بات‌های پیشرفته برای دستکاری بازارهای مالی، یا تولید دیپ‌فیک‌های مجرمانه که قادرند به شیوه‌های بسیار پیچیده هویت افراد را جعل کنند. مسئله اساسی اینجاست که کنوانسیون بوداپست بر مبنای مسئولیت کیفری انسان‌ها تنظیم شده و چارچوب مناسبی برای مسئولیت‌پذیری در مورد جرایم ارتکابی توسط سیستم‌های مستقل هوش مصنوعی ارائه نمی‌دهد. همچنین، جرایم مرتبط با اینترنت اشیاء که امروزه میلیاردها دستگاه متصل را شامل می‌شود و آسیب‌پذیری‌های امنیتی آنها به حملات گسترده سایبری منجر می‌گردد، در متن کنوانسیون مورد توجه قرار نگرفته است. حملاتی که از طریق دستگاه‌های هوشمند خانگی، وسایل پزشکی متصل، یا خودروهای هوشمند انجام می‌شوند، چالش‌های حقوقی خاص خود را دارند که مقررات فعلی کنوانسیون پاسخگوی آنها نیست.

---

[۱] – فتحی، صابر (۱۳۹۶)، **نقش و عملکرد سازمان‌های بین المللی دولتی و غیردولتی در حوزه جرایم سایبری**، پایان نامه برای دریافت درجه کارشناسی ارشد، رشته حقوق بین الملل، دانشگاه پیام نور مرکز تهران،ص۵۹

چالش عمده دیگری که کنوانسیون بوداپست با آن مواجه است، جرایم مبتنی بر فناوری‌های غیرمتمرکز به ویژه بلاکچین و رمزارزهاست. ماهیت غیرمتمرکز این فناوری‌ها که در آنها هیچ مرجع مرکزی برای کنترل یا نظارت وجود ندارد، با رویکرد سنتی کنوانسیون که بر تعامل با ارائه‌دهندگان خدمات اینترنتی و دارندگان داده‌ها استوار است، در تضاد قرار می‌گیرد. در فضای غیرمتمرکز، دیگر نمی‌توان به سادگی از یک شرکت یا سازمان خواست که داده‌ها را حفظ، ارائه، یا حذف کند، زیرا اطلاعات به صورت پراکنده در هزاران گره شبکه ذخیره شده‌اند. استفاده روزافزون از رمزارزها برای پولشویی، خرید خدمات و محصولات غیرقانونی در بازارهای تاریک وب، و پرداخت باج در حملات باج‌افزاری، مشکل جدی تعقیب مالی مجرمان را ایجاد کرده است. اگرچه کنوانسیون در مواد مربوط به جمع‌آوری داده‌های ترافیکی و مالی تدابیری اندیشیده، اما این مقررات برای ردیابی تراکنش‌های رمزارزی که با استفاده از تکنیک‌های پیچیده‌ای همچون میکسرها و تامبلرها ناشناس‌سازی می‌شوند، ناکافی است. علاوه بر این، پلتفرم‌های مالی غیرمتمرکز (DeFi) که امکان انجام تراکنش‌های مالی پیچیده را بدون نیاز به واسطه‌های سنتی فراهم می‌آورند، فضای جدیدی برای ارتکاب جرایم مالی ایجاد کرده‌اند که کنوانسیون بوداپست ابزارهای کافی برای نظارت و کنترل آنها در اختیار مقامات قضایی قرار نمی‌دهد. این خلأهای حقوقی و فنی، ضرورت بازنگری اساسی در کنوانسیون یا تدوین پروتکل‌های الحاقی جامع‌تری را که به طور خاص به این فناوری‌های نوظهور بپردازند، بیش از پیش آشکار می‌سازد.

نتیجه گیری

همکاری‌های بین‌المللی در مقابله با جرایم سایبری، امروزه نه یک انتخاب بلکه یک ضرورت اجتناب‌ناپذیر است. ماهیت فرامرزی فضای سایبری و توانایی مجرمان در بهره‌برداری از شکاف‌های حقوقی میان نظام‌های کیفری ملی، هیچ کشوری را قادر نمی‌سازد که به تنهایی با این پدیده به طور مؤثر مقابله کند. کنوانسیون بوداپست به عنوان نخستین و جامع‌ترین سند بین‌المللی در این حوزه، دستاوردهای قابل توجهی در زمینه هماهنگی قوانین داخلی، تسهیل کمک قضایی متقابل، و ایجاد چارچوبی مشترک برای مبارزه با جرایم سایبری به همراه داشته است. با این حال، یافته‌های این پژوهش نشان می‌دهد که کنوانسیون با چالش‌های جدی در اجرا و خلأهای حقوقی قابل توجهی در پاسخگویی به تحولات فناوری روبروست.تفاوت‌های بنیادین در نظام‌های حقوقی ملی، اعم از تفاوت در جرم‌انگاری، عناصر تشکیل‌دهنده جرایم، و سطح مجازات‌ها، همچنان یکی از اساسی‌ترین موانع در مسیر همکاری بین‌المللی است. این ناهماهنگی‌ها نه تنها استرداد مجرمان و اجرای احکام خارجی را دشوار می‌سازد، بلکه مجرمان سایبری را قادر می‌کند تا با شناخت از شکاف‌های حقوقی موجود، از پناهگاه‌های امن بهره‌برداری کنند. مسئله پیچیده‌تر زمانی است که برخی از کشورهای کلیدی که خود منشأ بخش عمده‌ای از جرایم سایبری هستند، به کنوانسیون نپیوسته‌اند و همکاری قضایی با آنها تقریباً غیرممکن است. علاوه بر این، تنش میان الزامات همکاری بین‌المللی و حفظ حاکمیت ملی و حریم خصوصی شهروندان، به ویژه در مورد دسترسی فرامرزی به داده‌ها، همچنان محل بحث و اختلاف است.

دشواری در تعیین صلاحیت قضایی برای رسیدگی به جرایم با بعد چندملیتی، یکی دیگر از معضلات عمده است که به

طور کامل حل نشده است. در غیاب یک مرجع بین‌المللی واحد برای حل تعارضات صلاحیتی و با توجه به ماهیت غیرمادی فضای سایبری که تعیین محل دقیق وقوع جرم را دشوار می‌سازد، امکان تداخل یا خلأ در صلاحیت‌ها همواره وجود دارد. این وضعیت منجر به سردرگمی حقوقی، هدررفت منابع در تحقیقات موازی، و در نهایت فرار بسیاری از مجرمان از چنگال عدالت می‌شود.

شاید مهم‌ترین یافته این پژوهش، آشکارشدن خلأهای جدی کنوانسیون بوداپست در پاسخگویی به جرایم نوظهور و فناوری‌های غیرمتمرکز باشد. جرایم مبتنی بر هوش مصنوعی، اینترنت اشیاء، دیپ‌فیک، و به ویژه فناوری‌های غیرمتمرکز مانند بلاکچین و رمزارزها، چالش‌هایی را ایجاد کرده‌اند که کنوانسیون در زمان تدوین آنها را پیش‌بینی نکرده بود. ماهیت غیرمتمرکز این فناوری‌ها که در آنها هیچ مرجع مرکزی برای کنترل وجود ندارد، با رویکرد سنتی کنوانسیون مبنی بر تعامل با ارائه‌دهندگان خدمات در تضاد است و ابزارهای حقوقی موجود برای مقابله با آنها ناکافی می‌نماید.

با وجود این چالش‌ها، کنوانسیون بوداپست همچنان مهم‌ترین پایه و اساس همکاری‌های بین‌المللی در مبارزه با جرایم سایبری است و نباید دستاوردهای آن نادیده گرفته شود. راه پیش‌رو، نه کنارگذاشتن ا ین کنوانسیون، بلکه تقویت و تکمیل آن از طریق تدوین پروتکل‌های الحاقی جامع است که به طور خاص به جرایم نوظهور و فناوری‌های پیشرفته بپردازند. همچنین، ضروری است که تلاش‌های دیپلماتیک جدی برای جذب کشورهای کلیدی غیرعضو، به ویژه کشورهایی که منشأ اصلی جرایم سایبری هستند، صورت پذیرد. ایجاد مکانیسم‌های سریع‌تر برای کمک قضایی متقابل، استقرار شبکه‌های ۲۴/۷ برای تبادل فوری اطلاعات در مواقع اضطراری، و تأمین منابع مالی و فنی برای کشورهای در حال توسعه جهت ارتقای توانمندی‌های آنها، از دیگر ضرورت‌های اساسی است.

در نهایت، مبارزه مؤثر با جرایم سایبری مستلزم تغییر نگرش از رویکرد صرفاً کیفری به رویکردی جامع است که همکاری میان بخش عمومی و خصوصی، سازمان‌های بین‌المللی، و جامعه مدنی را در بر گیرد. فناوری به سرعت در حال تحول است و حقوق باید بتواند با این سرعت همگام شود. کنوانسیون بوداپست گام مهمی در این مسیر بوده است، اما مسیر هنوز طولانی است و نیازمند اراده سیاسی قوی، همکاری فراگیر بین‌المللی، و نوآوری مستمر در چارچوب‌های حقوقی برای مقابله با تهدیدات دائماً در حال تکامل فضای سایبری می‌باشد.

سپاسگزاری

از معاونت محترم پژوهشی به خاطر حمایت حمایت معنوی در اجرای پژوهش حاضر سپاسگزاری می‌شود.
از آقای دکتر عبدالله علیزاده به خاطر بازبینی متن مقاله و ارائه نظرهای ساختاری تشکر و قدردانی می‌شود.
از داوران محترم به خاطر ارائه نظرهای ساختاری و علمی سپاسگزاری می‌شود.
نگارندگان بر خود لازم می‌دانند از آقای دکتر محمد رسول آهنگران به خاطر مطالعه متن مقاله حاضر و ارائه نظرهای ارزشمند سپاسگزاری نمایند.

منابع

انصاری ، باقر؛ انصاری ، اسماعیل(۱۳۹۱) ، حقوق اطلاعات از منظر تحلیل اقتصادی ، مجله مطالعات حقوق تطبیقی ، دوره ۳ ، شماره ۲

پورجاهد، محمد (۱۳۹۵)، بررسی حقوقی جرایم سایبری ایران در پرتو کنوانسیون جرایم سایبری، پایان نامه برای دریافت درجه کارشناسی ارشد، رشته حقوق جزا و جرم شناسی، دانشگاه آزاد اسلامی واحد تفت

پورقهرمانی، بابک (۱۳۹۶)، مطالعه تطبیقی سازوکارهای حمایت از بزه‌دیدگان جرایم رایانه‌ای در حقوق کیفری ایران و اسناد بین المللی با تاکید بر کنوانسیون بوداپست، نشریه پژوهشنامه حقوق کیفری، شماره ۱۵

جلالی فراهانی، امیرحسین(۱۳۸۹)، کنوانسیون جرایم سایبر و پروتکل الحاقی آن با همراه گزارش توجیهی، چاپ اول، معاونت حقوق و توسعه قوه قضاییه

خداقلی ، زهرا(۱۳۸۴) ، جرایم کامپیوتری ، چاپ اول ، انتشارات آریان

رضوی فرد، بهزاد؛ موسوی، سیدنعمت الله(۱۳۹۵)، مسئولیت کیفری در فضای سایبر در حقوق ایران، فصلنامه پژوهش حقوق کیفری، دوره۵، شماره۱۶

شیرزاد ، کامران(۱۳۸۸) ، جرایم رایانه‌ای ، چاپ اول ، تهران: نشر بهینه فراگیر

عاملی، سعیدرضا(۱۳۹۶)، فلسفه فضای مجازی، تهران: انتشارات امیرکبیر

فتحی، صابر (۱۳۹۶)، نقش و عملکرد سازمان‌های بین المللی دولتی و غیردولتی در حوزه جرایم سایبری، پایان نامه برای دریافت درجه کارشناسی ارشد، رشته حقوق بین الملل، دانشگاه پیام نور مرکز تهران

کوچی ، سعید(۱۳۹۵) ، نقش مهارت افزایش کارکنان ناجا برای پیشگیری از جرایم فضای مجازی ، فصنامه علمی مطالعات حفاظت و امنیت اجتماعی ، سال یازدهم ، شماره ۴۱

لک، بهزاد(۱۳۹۱)، شناسایی و پیشگیری از کمین سایبری در فضای مجازی، مجله کارآگاه، دوره دوم، سال پنجم، شماره۱۸،ص۹۵

محسنی، فرید؛ صوفی زمرد، محسن(۱۳۹۶)، پلیس و چالش‌های اجرایی تامین امنیت سایبری، فصلنامه پژوهش‌های دانش انتظامی، سال بیستم، شماره چهارم

میرترابی، هدیه سادات؛ شیرزاد، هادی؛ آقا کاشی، وهاب(۱۳۹۹)، نقش پلیس در پیشگیری از جرایم سایبری با تاکید بر قوانین موضوعه، فصلنامه علمی مطالعات بین المللی پلیس، دوره یازدهم، شماره ۴

Davis, Benjamin.R; Ending the Cyber Jihad: Combating terrorists explation of the internet with

Denning, Dorothy; Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, in Networks and net wars: the future of terror, crime and militancy, Sponsored by Nautilus Institute,1999

Gallagher, Borchgraze, Cillusso, William H. Webster, Frank J. Cilluffo, Berkowitz, S. Lan ; Cybercrime, Cyber terrorism, Cyber warfare , Averting an Electronic waterloo, Center for Strategic & International Studies,1998

Goodman, Seymour. E and Kirk, Jessica C and Kirk Megan H; Cyberspace as a medium for

Pollitt, Mark.M; Cyberterrorism: Fact or Fancy, Proceedings of the 20th National Information

Systems Security Conference, October 1997

terrorists, Technological Forecasting & Social Change, vol 74, 2007

the rule of low and improved tools for cyber governance, common low conspectus, volume 15, 2006-2007