Journal of
International Criminal Law
www.iclj.ir

Volume 2, Issue 4, 2024

Prosecution and Extradition of Cybercriminals in the International Criminal System: Challenges and Solutions for Strengthening Judicial Jurisdiction

Sahar Mohammadi*[1], Kiomarth Kalantarei[2]

1. PhD Student, Department of Criminal Law and Criminology, Gorgan Branch, Islamic Azad University, Gorgan, Iran. (Corresponding Author)
2. Professor, Department of Criminal Law and Criminology, Faculty of Law and Political Science, University of Mazandaran, Babolsar, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
***Pages:* 1-11**

Corresponding Author's Info
ORCID: *0009-0002-5395-6957*
TELL: *+9835302801*
Email:
saharmohammadi1374@yahoo.com

Article history:
Received: *03 Aug 2024*
Revised: *08 Oct 2024*
Accepted: *11 Nov 2024*
Published online: *21 Dec 2024*

Keywords:
Cybercriminals, Judicial Jurisdiction, Prosecution, Extradition.

ABSTRACT

Cybercrimes, due to their transnational nature, technical complexity and rapid occurrence, have become one of the major challenges for criminal justice systems at the international level. The prosecution and extradition of cybercriminals, especially in a context where domestic and international laws often have serious contradictions, face numerous legal, technological and political issues. This paper examines the concept and characteristics of cybercrimes, analyzes the challenges involved in the prosecution and extradition of such crimes from legal, technological and international cooperation perspectives and evaluates the role of international conventions such as the Budapest Convention and organizations like INTERPOL. In the final section, solutions for strengthening judicial jurisdiction through harmonizing international laws, advancing judicial technologies and enhancing international cooperation are provided. The findings indicate that achieving justice in the realm of cybercrimes requires an integrated international approach that effectively tackles these challenges through the use of advanced technologies and cross-border cooperation.

How to Cite This Article: Mohammadi, S & Kalantarei, K (2024). "Prosecution and Extradition of Cybercriminals in the International Criminal System: Challenges and Solutions for Strengthening Judicial Jurisdiction". *Journal of International Criminal Law*, 2(4): 1-11.

فصلنامه حقوق جزای بین‌الملل

www.iclj.ir

انجمن علمی فقه جزای تطبیقی ایران

دوره دوم، شماره چهارم، زمستان ۱۴۰۳

تعقیب و استرداد مجرمان سایبری در نظام کیفری بین‌المللی: چالش‌ها و راهکارهای تقویت صلاحیت محاکم قضایی

سحر محمدی*[۱]، کیومرث کلانتری[۲]

۱. دانشجوی دکتری، گروه حقوق کیفری و جرم‌شناسی، واحد گرگان، دانشگاه آزاد اسلامی، گرگان، ایران. (نویسنده مسؤول)

۲. استاد، گروه حقوق کیفری و جرم‌شناسی، دانشکده حقوق و علوم سیاسی، دانشگاه مازندران، بابلسر، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱-۱۱

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۹-۰۰۰۲-۵۳۹۵-۶۹۵۷

تلفن: ۹۸۳۵۳۰۲۸۰۱+

ایمیل: saharmohammadi1374@yahoo.com

سابقه مقاله:

تاریخ دریافت: ۱۴۰۳/۰۵/۱۳

تاریخ ویرایش: ۱۴۰۳/۰۷/۱۷

تاریخ پذیرش: ۱۴۰۳/۰۸/۲۱

تاریخ انتشار: ۱۴۰۳/۱۰/۰۱

واژگان کلیدی:

مجرمان سایبری، صلاحیت قضایی، تعقیب، استرداد.

چکیده

جرایم سایبری به‌دلیل ماهیت فرامرزی، پیچیدگی فنی و سرعت بالای وقوع، به یکی از چالش‌های جدی نظام‌های کیفری در سطح بین‌المللی تبدیل شده‌اند. تعقیب و استرداد مجرمان سایبری، به‌ویژه در فضایی که قوانین داخلی و بین‌المللی تناقض‌های جدی دارند، با مشکلات متعدد حقوقی، تکنولوژیکی و سیاسی مواجه است. این مقاله با بررسی مفهوم و ویژگی‌های جرایم سایبری، چالش‌های موجود در تعقیب و استرداد این جرایم را از منظر حقوقی، فناوری و تعاملات بین‌المللی تحلیل کرده و نقش کنوانسیون‌های بین‌المللی نظیر کنوانسیون بوداپست و سازمان‌هایی همچون اینترپل را ارزیابی می‌کند. در بخش پایانی، راهکارهایی برای تقویت صلاحیت محاکم قضایی از طریق هماهنگ‌سازی قوانین بین المللی، ارتقای فناوری‌های قضایی و تقویت همکاری‌های بین‌المللی ارائه شده است. نتایج نشان می‌دهد که تحقق عدالت در حوزه جرایم سایبری مستلزم ایجاد رویکردی یکپارچه و بین‌المللی است که با بهره‌گیری از فناوری‌های پیشرفته و همکاری فراملی به مقابله مؤثر با این چالش‌ها بپردازد.

مقدمه

با گسترش روزافزون فناوری اطلاعات و ارتباطات، جرایم سایبری به یکی از پیچیده‌ترین و گسترده‌ترین چالش‌های پیش روی نظام‌های حقوقی و کیفری تبدیل شده است. این جرایم که در محیط مجازی و اغلب فراتر از مرزهای جغرافیایی رخ می‌دهند، نه‌تنها امنیت اطلاعات و داده‌های افراد و سازمان‌ها را تهدید می‌کنند، بلکه ثبات اقتصادی، اجتماعی و حتی سیاسی جوامع را نیز به خطر می‌اندازند. سرعت وقوع، ناشناسی مرتکبان و ماهیت فرامرزی این جرایم، مقابله با آن‌ها را برای محاکم قضایی و نهادهای اجرایی دشوار کرده است.

در این میان، تعقیب و استرداد مجرمان سایبری یکی از مهم‌ترین دغدغه‌های نظام کیفری بین‌المللی به‌شمار می‌رود. عدم هماهنگی قوانین ملی، تناقض در تعریف جرایم سایبری میان کشورها و فقدان سازوکارهای مؤثر برای همکاری‌های بین‌المللی، موانعی جدی در مسیر اجرای عدالت ایجاد کرده‌اند. از سوی دیگر، پیشرفت سریع فناوری و بهره‌گیری مجرمان از ابزارهای پیشرفته، کارایی روش‌های سنتی تعقیب و استرداد را کاهش داده است.

این مقاله با هدف تحلیل چالش‌های موجود در تعقیب و استرداد مجرمان سایبری و ارائه راهکارهایی برای تقویت صلاحیت محاکم قضایی تدوین شده است. در ابتدا، مفهوم و ویژگی‌های جرایم سایبری و چالش‌های مرتبط با آن‌ها مورد بررسی قرار می‌گیرد، سپس با مرور مبانی قانونی و کنوانسیون‌های بین‌المللی، نقش نهادهایی مانند اینترپل و یوروپل در مدیریت این بحران‌ها ارزیابی خواهد شد. درنهایت، راهکارهای مؤثر برای مقابله با این چالش‌ها و تقویت تعاملات بین‌المللی ارائه می‌شود. این پژوهش بر این باور است که تنها از طریق رویکردی جامع و هماهنگ می‌توان به مقابله‌ای مؤثر با جرایم سایبری و تحقق عدالت کیفری دست یافت.

۱- مفاهیم

۱-۱- مفهوم جرایم سایبری

جرایم سایبری به هرگونه فعالیت غیرقانونی اطلاق می‌شود که در آن رایانه، شبکه یا سامانه‌های دیجیتال به‌عنوان ابزار، هدف یا محیط ارتکاب جرم مورد استفاده قرار می‌گیرند که در قانون مجازا اسلامی (تعزیرات) اصلاحی سال ۱۳۷۵ مصادیق آن مورد اشاره قانون‌گذار ایران قرار گرفته است. انواع جرایم سایبری شامل موارد زیر است:

دسترسی غیرمجاز (هک): نفوذ به سامانه‌های رایانه‌ای برای دستیابی به اطلاعات حساس.

سرقت داده: استخراج غیرقانونی اطلاعات از پایگاه‌های داده بدون مجوز (ماده ۷۴۰).

کلاه‌برداری اینترنتی: استفاده از روش‌هایی مانند فیشینگ برای دسترسی به اطلاعات مالی یا شخصی قربانیان (ماده ۷۴۱).

باج‌افزار: نرم‌افزارهای مخربی که داده‌ها را رمزگذاری کرده و برای بازیابی آن‌ها درخواست پرداخت می‌کنند (Holt *et al*, 2022: 50).

جاسوسی سایبری: دسترسی به اطلاعات حساس سازمانی یا دولتی برای مقاصد جاسوسی (ماده ۷۳۱).

به‌طور کلی، جرایم سایبری دارای ویژگی‌هایی متمایز از سایر جرایم هستند که از آن جمله می‌توان به فرامرزی‌بودن (عدم محدودیت جغرافیایی و نیاز به همکاری‌های بین‌المللی)، سرعت وقوع (امکان ارتکاب جرم در چند ثانیه و تخریب سریع سیستم‌ها)، ناشناسی (استفاده از ابزارهای پیشرفته مانند رمزگذاری و شبکه‌های ناشناس که شناسایی مجرمان را دشوار می‌سازد) و پیچیدگی فنی (بهره‌گیری از فناوری‌های پیشرفته که روند شناسایی و مقابله با جرایم را برای نهادهای قانونی چالش‌برانگیز می‌کند) اشاره کرد (Zhou *et al*, 2024: 424).

– مفهوم تعقیب: تعقیب کیفری مجموعه اقداماتی است که توسط نهادهای قانونی یا حکومتی برای بررسی، پیگیری و رسیدگی به شکایات، تظلمات و جرایم جنایی انجام می‌شود. این فرآیند، براساس قانون، ممکن است با شکایت افراد خصوصی (در جرایم قابل گذشت) یا به دستور دادستان به‌عنوان نماینده منافع عمومی (در جرایم غیرقابل گذشت) آغاز شود (شاکری و هادی‌زاده، ۱۳۹۵: ۱۴۲).

– مفهوم استرداد مجرم: استرداد مجرم فرآیندی حقوقی و بین‌المللی است که طی آن یک کشور متهم یا محکوم به

ارتکاب جرم را به کشوری دیگر که خواهان اوست، تحویل می‌دهد. این درخواست معمولاً زمانی مطرح می‌شود که جرم در کشور درخواست‌کننده اتفاق افتاده یا متهم به آن کشور گریخته باشد. استرداد معمولاً براساس معاهدات دو یا چندجانبه بین کشورها انجام می‌شود. درصورت نبود معاهده، ممکن است به اصل عمل متقابل استناد شود. استرداد تنها در مورد جرایمی اعمال می‌شود که در قوانین هر دو کشور جرم تلقی شوند و معمولاً شامل جرایم سنگین مانند قتل، تروریسم یا فساد مالی است. مجرمان سیاسی (مانند مخالفان حکومت) معمولاً مسترد نمی‌شوند. اگر احتمال شکنجه یا محاکمه ناعادلانه وجود داشته باشد، برخی کشورها از استرداد خودداری می‌کنند. کشور درخواست‌کننده باید دلایل کافی برای تقاضای استرداد ارائه دهد. درخواست توسط دادگاه یا مراجع مربوطه در کشور دریافت‌کننده بررسی می‌شود. پس از تأیید، متهم به کشور درخواست‌کننده تحویل داده می‌شود. استرداد برای تضمین اجرای عدالت، جلوگیری از فرار مجرمان از مجازات و تقویت همکاری‌های بین‌المللی در مبارزه با جرم و جنایت صورت می‌گیرد (کلانتری، ۱۴۰۱: ۲۲-۲۵).

مثال: اگر فردی مرتکب جرمی در کشور «الف» شده و به کشور «ب» فرار کند، کشور «الف» می‌تواند از کشور «ب» درخواست استرداد او را براساس معاهدات موجود یا اصل عمل متقابل ارائه دهد.

۲- چالش‌های موجود در تعقیب و استرداد مجرمان سایبری

جرایم سایبری به‌دلیل ویژگی‌های فرامرزی، ناشناسی و پیچیدگی‌های فنی، نظام‌های حقوقی ملی و بین‌المللی را با چالش‌های قابل توجهی مواجه کرده‌اند. این چالش‌ها در ابعاد مختلف حقوقی، تکنولوژیکی، سیاسی و اجتماعی قابل بررسی هستند.

۲-۱- چالش‌های حقوقی

عبارتند از موارد ذیل‌الذکر که در ادامه به تشریح هریک خواهیم پرداخت.

در سطح جهانی، هیچ چهارچوب جامع و واحدی برای تعریف و تعقیب جرایم سایبری وجود ندارد. بسیاری از کشورها قوانین ملی متفاوتی دارند که با استانداردهای بین‌المللی تطابق ندارند. این مسأله باعث سردرگمی در اجرای قوانین استرداد می‌شود (Holt *et al*, 2022: 95). یکی از مسائل اساسی در جرایم سایبری تعیین محل ارتکاب جرم است. به‌دلیل ماهیت فرامرزی این جرایم، مشخص‌کردن این‌که کدام کشور صلاحیت قضایی دارد، پیچیده است (Goodman & Sofar, 2013: 54). کشورها تعریف‌های متفاوتی از جرایم سایبری دارند. این اختلاف‌ها موجب می‌شود برخی از جرایم در یک کشور قانونی و در کشور دیگر غیرقانونی تلقی شوند (Zhou *et al*, 2024: 431).

۲-۲- چالش‌های تکنولوژیکی

مجرمان از فناوری‌های پیشرفته مانند شبکه‌های ناشناس و رمزگذاری برای پنهان‌کردن هویت و موقعیت جغرافیایی خود استفاده می‌کنند که شناسایی و ردیابی آن‌ها را دشوار می‌سازد (Finklea & Theohary, 2013: 58). ابزارهای قانونی و تکنولوژیکی نهادهای قضایی غالباً قادر به همگام‌شدن با پیشرفت‌های سریع فناوری نیستند. این مسأله موجب ایجاد شکاف در تعقیب مجرمان سایبری شده است (Zhou et al, 2024: 425).

۲-۳- چالش‌های سیاسی

در مواردی، منافع سیاسی دولت‌ها موجب می‌شود که همکاری‌های لازم در زمینه استرداد مجرمان سایبری صورت نگیرد. این مسأله به‌ویژه در شرایطی که جرم در یک کشور علیه منافع کشور دیگر ارتکاب یافته باشد، برجسته است (Goodman & Sofar, 2013: 92). نهادهای بین‌المللی مانند اینترپل و یوروپل هنوز نتوانسته‌اند سازوکارهای جامعی برای تضمین همکاری بین کشورها ایجاد کنند. نبود توافقات جامع موجب کاهش اثربخشی تعقیب بین‌المللی شده است (Holt *et al*, 2022: 120).

۲-۴- چالش‌های اجتماعی و فرهنگی

تفاوت‌های فرهنگی میان کشورها موجب شده است که برخی از رفتارها در یک فرهنگ به‌عنوان جرم تلقی شود، درحالی‌که در فرهنگ دیگر قانونی باشد (Zhou *et al*, 2024: 438). جرایم سایبری اغلب حقوق بنیادین افراد، مانند حریم خصوصی

و آزادی بیان، را تحت تأثیر قرار می‌دهند. این مسأله باعث ایجاد حساسیت‌های اجتماعی و فرهنگی در پیگیری این جرایم شده است (Finklea & Theohary, 2013: 132).

لذا جرایم سایبری به‌دلیل ویژگی‌های خاص خود، مانند فرامرزی‌بودن، ناشناسی مجرمان و پیچیدگی‌های فنی، چالش‌های زیادی را برای نظام‌های حقوقی، سیاسی، اجتماعی و تکنولوژیکی به‌همراه دارند. در سطح حقوقی، نبود چهارچوب جهانی و اختلاف در تعاریف قانونی کشورهای مختلف، اجرای مؤثر قوانین و استرداد مجرمان را دشوار می‌سازد. در ابعاد تکنولوژیکی، پیشرفت‌های سریع فناوری و استفاده مجرمان از ابزارهای پیچیده برای مخفی‌کردن هویت و موقعیت خود، شناسایی و تعقیب مجرمان را با مشکل مواجه کرده است. از نظر سیاسی، اختلافات منافع میان کشورها و نبود همکاری‌های مؤثر بین‌المللی، مانع از اقدامات هماهنگ در پیگیری این جرایم می‌شود. همچنین تفاوت‌های فرهنگی و حساسیت‌های اجتماعی نیز تأثیر زیادی بر پیگیری این جرایم دارند، به‌ویژه هنگامی که حقوق بنیادین افراد مانند حریم خصوصی و آزادی بیان تحت تأثیر قرار می‌گیرد. بنابراین برای مقابله با این چالش‌ها، نیاز به هم‌افزایی در سطح بین‌المللی، تطابق قوانین و هماهنگی میان نهادهای مختلف کشورها وجود دارد. در ادامه به تحلیل و بررسی مبانی قانونی و بین‌المللی جرایم سایبری پرداخته خواهد شد تا نشان داده شود که چگونه این چهارچوب‌ها می‌توانند نقش مؤثری در مقابله با تهدیدات فضای سایبری ایفا کنند و در عین حال، نقاط ضعف و مشکلات موجود در آن‌ها برای پیشگیری از جرم و تعقیب مجرمان برطرف گردد.

۳- مبانی قانونی و بین‌المللی

برای مقابله با جرایم سایبری و پیگیری مجرمان در سطح بین‌المللی، چهارچوب‌های قانونی متعددی ایجاد شده است. این چهارچوب‌ها شامل کنوانسیون‌های بین‌المللی، نقش سازمان‌های بین‌المللی نظیر اینترپل و یوروپل و بررسی صلاحیت محاکم ملی و بین‌المللی هستند.

۳-۱- کنوانسیون‌های بین‌المللی مرتبط

۳-۱-۱- کنوانسیون بوداپست (۲۰۰۱)

کنوانسیون بوداپست یا «کنوانسیون جرایم سایبری» که توسط شورای اروپا تدوین شد، مهم‌ترین سند بین‌المللی برای مقابله با جرایم سایبری است. این کنوانسیون جرایم سایبری را تعریف و دسته‌بندی می‌کند و بر همکاری‌های بین‌المللی در تحقیقات و استرداد مجرمان تاکید دارد. همچنین کشورهای عضو را ملزم به تطبیق قوانین داخلی خود با مفاد کنوانسیون می‌کند. (پورقهرمانی، ۱۳۹۶: ۱۶) کنوانسیون بوداپست به‌عنوان اولین چارچوب جامع قانونی، تأثیر زیادی در توسعه همکاری‌های بین‌المللی داشته است، اما چالش‌هایی نظیر محدودیت عضویت کشورها (مانند چین و روسیه که عضو نیستند) همچنان وجود دارد.

۳-۱-۲- معاهدات دو یا چندجانبه

علاوه بر کنوانسیون بوداپست، کشورها معاهدات دو یا چندجانبه‌ای را برای تقویت همکاری‌های حقوقی در پیگیری مجرمان سایبری امضا کرده‌اند. برای مثال، ایالات متحده و اتحادیه اروپا توافق‌نامه‌هایی در زمینه به اشتراک‌گذاری اطلاعات و تحقیقات مشترک امضا کرده‌اند. (Finklea & Theohary, 2013: 90)

۳-۲- نقش اینترپل و یوروپل در پیگیری مجرمان سایبری

اینترپل از طریق برنامه «واحد جرایم سایبری جهانی»، به کشورها در شناسایی و پیگیری مجرمان سایبری کمک می‌کند. نقش‌های کلیدی اینترپل عبارت‌اند از:

ایجاد یک شبکه اطلاعاتی جهانی برای تبادل اطلاعات جرایم سایبری.

هماهنگی عملیات‌های مشترک میان کشورها (Holt *et al*, 2022: 128).

یوروپل به‌ویژه در اتحادیه اروپا نقش مؤثری در مقابله با جرایم سایبری ایفا می‌کند. مرکز جرایم سایبری اروپا موسوم به EC3 که تحت نظارت یوروپل فعالیت می‌کند، بر موارد زیر تمرکز دارد:

- تحلیل داده‌های جرایم سایبری در کشورهای عضو.

– ارائه ابزارهای پیشرفته شناسایی مجرمان سایبری به مقامات محلی (Zhou et al, 2024: 428).

۳-۳- بررسی صلاحیت محاکم ملی و بین‌المللی

۳-۳-۱- محاکم ملی

صلاحیت محاکم ملی در جرایم سایبری بستگی به محل ارتکاب جرم، محل اقامت متهم یا قربانی و تأثیر جرم دارد. با این حال، به‌دلیل فرامرزی‌بودن جرایم سایبری، کشورها اغلب با چالش‌هایی نظیر تعیین مرزهای صلاحیت و تضاد قوانین مواجه هستند. چندان در نظام قضایی ایران، ماده ۶۶۴ قانون آیین دادرسی کیفری با هدف تعیین صلاحیت دادگاه‌های ایران در مقابله با جرایم رایانه‌ای و سایبری، به‌ویژه در موارد فرامرزی، نقش مهمی در حفظ امنیت سایبری، حاکمیت ملی و حمایت از حقوق افراد ایفا می‌کند. این ماده با بهره‌گیری از اصول مختلف صلاحیت قضایی، ازجمله قلمرو سرزمینی، پرچم، حمایت واقعی و صلاحیت جهانی محدود، تلاش می‌کند تا جرایم سایبری پیچیده را در داخل و خارج از کشور تحت پیگرد قرار دهد.

۳-۳-۲- محاکم بین‌المللی

در حال حاضر، محاکم بین‌المللی تخصصی برای رسیدگی به جرایم سایبری مقرره واحدی وجود ندارد. با این حال، پیشنهادهایی برای تأسیس «دادگاه بین‌المللی جرایم سایبری» مطرح شده است که می‌تواند به این چالش‌ها پاسخ دهد (Holt *et al*, 2022: 145).

بدین‌ترتیب می‌توان چنین استنباط کرد که مبانی قانونی و بین‌المللی جرایم سایبری، اگرچه نقش مهمی در ایجاد نظم و امنیت در فضای سایبری ایفا می‌کنند، اما همچنان با چالش‌های قابل توجهی مواجه‌اند که از هماهنگی ناکافی میان نظام‌های حقوقی مختلف، پیچیدگی‌های فنی و محدودیت‌های همکاری بین‌المللی ناشی می‌شود. برای بهره‌گیری مؤثر از این چهارچوب‌ها، تقویت تعاملات بین‌المللی، بازنگری و هماهنگی قوانین ملی با استانداردهای جهانی و توسعه فناوری‌های پیشرفته حقوقی ضروری است. با چنین اصلاحاتی، می‌توان امیدوار بود که این مبانی به ابزاری کارآمد برای پیشگیری از جرایم سایبری و تعقیب مؤثر مجرمان تبدیل شوند و امنیت فضای سایبری را در سطح جهانی تضمین کنند، لذا ما در ادامه به ارائه راهکارهای تقویت صلاحیت محاکم قضایی پرداخته و هریک را مورد ارزیابی قرار می‌دهیم.

۴- راهکارهای تقویت صلاحیت محاکم قضایی

برای مقابله مؤثر با جرایم سایبری و تقویت صلاحیت محاکم قضایی در تعقیب و استرداد مجرمان، نیاز به مجموعه‌ای از راهکارها در سطح ملی و بین‌المللی وجود دارد. این راهکارها در چهار بعد اصلی شامل تدوین قوانین هماهنگ، ارتقای فناوری‌های قضایی، تقویت آموزش و ظرفیت‌سازی و افزایش نقش سازمان‌های بین‌المللی قابل بررسی هستند.

۴-۱- تدوین قوانین هماهنگ در سطح بین‌المللی

یکی از چالش‌های اساسی در پیگیری جرایم سایبری، عدم هماهنگی در قوانین ملی کشورها است. به‌منظور تقویت صلاحیت محاکم قضایی، تدوین استانداردهای حقوقی مشترک در سطح جهانی ضروری است. این استانداردها می‌تواند شامل تعریف یکسان از جرایم سایبری، مقیاس‌های مشابه برای مجازات‌ها و شفاف‌سازی در زمینه صلاحیت قضایی باشد.

توافق‌نامه‌ها و کنوانسیون‌های بین‌المللی نظیر کنوانسیون بوداپست، باید به‌روزرسانی شوند و کشورهای بیشتری به عضویت آن‌ها درآیند تا یکپارچگی در نظام حقوقی بین‌المللی تقویت شود.

یکی‌دیگر از جنبه‌های مهم تقویت صلاحیت محاکم قضایی، توسعه همکاری‌های مؤثر بین‌المللی در زمینه استرداد مجرمان سایبری است. این همکاری‌ها باید شامل تسهیل در تبادل اطلاعات، مستندسازی سریع و رسیدگی به درخواست‌های استرداد باشد (Holt *et al*, 2022: 150).

۴-۲- ارتقای فناوری‌های قضایی

توسعه ابزارهای پیشرفته ردیابی و شناسایی مجرمان سایبری از طریق فناوری‌های نوین مانند هوش مصنوعی و یادگیری ماشین می‌تواند به‌طور چشم‌گیری کارآیی سیستم‌های قضایی را افزایش دهد. این ابزارها قادرند حجم بالای داده‌ها را تجزیه و تحلیل کنند و نقشه‌های پیچیده جرم را در فضای سایبری شبیه‌سازی نمایند. یکپارچه‌سازی سامانه‌های اطلاعاتی قضایی

در سطح بین‌المللی، تسهیل اشتراک‌گذاری داده‌های مربوط به جرایم سایبری و هم‌افزایی میان سازمان‌های مختلف می‌تواند به بهبود سرعت رسیدگی به پرونده‌ها کمک کند. ایجاد پایگاه‌های داده مشترک که شامل سوابق و اطلاعات مربوط به مجرمان سایبری باشد، در این زمینه اهمیت زیادی دارد (Finklea & Theohary, 2013: 105).

۴-۳- تقویت آموزش و ظرفیت‌سازی

یکی از الزامات ضروری در تقویت صلاحیت محاکم قضایی، آموزش مستمر و تخصصی قضات، مأموران پلیس و دادستان‌ها در زمینه جرایم سایبری است. این آموزش‌ها باید شامل شناسایی، تجزیه و تحلیل و رسیدگی به مسائل پیچیده دیجیتال و سایبری باشد. به‌علاوه، پرورش مهارت‌های ویژه در زمینه فناوری‌های نوین نیز باید در اولویت قرار گیرد. تحقیقات علمی و پژوهشی در زمینه جرایم سایبری باید تقویت شود تا راهکارهای حقوقی و فنی جدید برای مقابله با این جرایم ارائه گردد. همکاری میان دانشگاه‌ها و نهادهای قضایی می‌تواند موجب ارتقای ظرفیت‌های قانونی و فنی در این حوزه شود (Zhou *et al*, 2024: 430).

۴-۴- نقش سازمان‌های بین‌المللی

سازمان‌های بین‌المللی نظیر اینترپل، یوروپل و سازمان ملل باید نقش فعال‌تری در نظارت و اجرای قوانین مربوط به جرایم سایبری ایفا کنند. این سازمان‌ها می‌توانند به‌عنوان هماهنگ‌کننده‌های بین‌المللی عمل کنند و مقامات محلی را در تعقیب و استرداد مجرمان حمایت نمایند. یکی از راهکارهای پیشنهادی برای تقویت صلاحیت قضایی در تعقیب مجرمان سایبری، ایجاد دادگاه‌های تخصصی در سطح بین‌المللی است. این دادگاه‌ها می‌توانند به‌طور اختصاصی به جرایم سایبری رسیدگی کنند و با برخورداری از قضات متخصص، به‌طور مؤثرتری به پرونده‌ها رسیدگی نمایند (Goodman & Sofar, 2013: 73).

۵- مطالعه تطبیقی

در این بخش، به بررسی تجربیات کشورهای پیشرو در مقابله با جرایم سایبری پرداخته می‌شود. کشورهای مختلف باتوجه به منابع، قوانین و رویکردهای حقوقی متفاوت، شیوه‌های خاصی برای مقابله با جرایم سایبری اتخاذ کرده‌اند. این مطالعه تطبیقی، به‌ویژه در کشورهای پیشرفته مانند ایالات متحده آمریکا، اتحادیه اروپا و سنگاپور، می‌تواند برای تقویت همکاری‌های بین‌المللی در زمینه مقابله با این نوع جرایم مفید واقع شود.

۵-۱- ایالات متحده آمریکا

ایالات متحده به‌عنوان یکی از پیشروترین کشورها در زمینه مقابله با جرایم سایبری، مجموعه‌ای از قوانین و ابزارهای حقوقی برای شناسایی و تعقیب مجرمان سایبری به‌کار گرفته است.

آمریکا در سطح ملی قوانینی نظیر Computer Fraud and Abuse Act 1986 (CFAA) و Electronic Communications Privacy Act 1986 (ECPA) برای مبارزه با جرایم سایبری به تصویب رسانده است. این قوانین به وضوح جرایم سایبری مانند هک، سرقت اطلاعات و کلاه برداری اینترنتی را تعریف می‌کنند و مجازات‌های خاصی را برای آن‌ها پیش‌بینی می‌نمایند. آمریکا با کشورهای مختلف، به‌ویژه کشورهای اروپایی و آسیایی، قراردادهای دو یا چندجانبه جهت استرداد مجرمان سایبری امضا کرده است. علاوه‌بر این، آمریکا به‌طور فعال در سازمان‌هایی چون اینترپل و یوروپل در زمینه تعقیب مجرمان سایبری مشارکت دارد (Finklea & Theohary, 2013: 101).

۵-۲- اتحادیه اروپا

اتحادیه اروپا یکی از نهادهای مهم بین‌المللی است که قوانین جامعی برای مقابله با جرایم سایبری دارد.

اتحادیه اروپا با تصویب (Directive 2013/40/EU of the European Parliament and of the Council) و (General Data Protection Regulation 2016 (GDPR)) چهارچوب حقوقی قوی برای مقابله با جرایم سایبری ایجاد کرده است. این مقررات شامل الزاماتی برای حفاظت از داده‌های شخصی و مقابله با جرایم سایبری می‌شود و به شدت از همکاری بین کشورهای عضو اتحادیه اروپا حمایت می‌کند.

قانون عمومی حفاظت از داده‌ها (GDPR) اتحادیه اروپا در تاریخ ۲۷ آوریل ۲۰۱۶ تصویب شد و از ۲۵ می ۲۰۱۸ اجرایی گردید. هدف اصلی این قانون، حفاظت از داده‌های شخصی افراد و تضمین آزادی جابه‌جایی این داده‌ها در اتحادیه اروپا است. GDPR جایگزین دستورالعمل حفاظت از داده‌ها شد و تلاش می‌کند تا چهارچوبی هماهنگ برای حفاظت از داده‌های شخصی فراهم کند.

تدابیر این قانون قانون برای مبارزه با جرایم سایبری و حفاظت از داده‌ها شامل موارد زیر است:

حق حفاظت از داده‌ها به‌عنوان یک حق اساسی: این قانون تأکید می‌کند که حفاظت از داده‌های شخصی یکی از حقوق اساسی افراد است که باید با سایر حقوق اساسی مانند آزادی بیان متعادل شود.

تعریف و محدودیت‌ها: قانون شامل داده‌های شخصی افراد شناسایی شده یا قابل شناسایی می‌شود.

پردازش داده‌های حساس (مانند اطلاعات ژنتیکی یا زیستی) با شرایط خاصی مجاز است.

داده‌های ناشناس از شمول این قانون خارج هستند.

مبنای قانونی برای پردازش: پردازش داده‌ها باید برمبنای قانونی مشخص صورت گیرد، مثلاً رضایت کاربر، ضرورت انجام یک قرارداد یا اجرای وظایف عمومی.

شفافیت و اطلاع‌رسانی: سازمان‌ها موظفند که فرآیندهای پردازش داده‌ها را شفاف‌سازی کنند و کاربران را از نحوه جمع‌آوری و استفاده از داده‌هایشان آگاه نمایند.

امنیت داده‌ها: تدابیر امنیتی فنی و سازمانی برای حفاظت از داده‌ها در برابر دسترسی غیرمجاز یا نقض داده‌ها ضروری است.

حقوق افراد: کاربران حق دسترسی به داده‌های خود، حق تصحیح و حق فراموش‌شدن (حق حذف داده‌ها) را دارند.

پیشگیری و کاهش جرایم سایبری: شرکت‌ها موظف به اجرای تحلیل تأثیر حفاظت از داده‌ها برای ارزیابی ریسک‌ها هستند و درصورت نقض داده‌ها، اطلاع‌رسانی سریع به مقامات نظارتی و افراد آسیب‌دیده الزامی است.

نظارت و ضمانت اجرا: مقامات نظارتی در هر کشور عضو اتحادیه اروپا نظارت بر اجرای GDPR را برعهده دارند. جریمه‌های سنگین مالی برای عدم رعایت قانون تعیین شده است.

پردازش خودکار و پروفایل‌سازی: استفاده از تصمیم‌گیری خودکار مبتنی‌بر پردازش داده‌ها، مانند پروفایل‌سازی، باید با ملاحظات اخلاقی و شفافیت همراه باشد.

این چهارچوب جامع با هدف تقویت اعتماد کاربران به فضای دیجیتال و افزایش امنیت سایبری، راهکارهای مؤثری برای مقابله با جرایم سایبری و تضمین حفاظت از حقوق افراد ارائه می‌دهد.

همچنین اتحادیه اروپا در ایجاد شبکه‌هایی برای تبادل اطلاعات درخصوص جرایم سایبری، به‌ویژه در سطح کشورهای عضو و کشورهای همکار، بسیار فعال است. همکاری‌های بین‌المللی با کشورهای ثالث نیز از اولویت‌های اصلی اتحادیه در مقابله با این جرایم به‌شمار می‌رود (Radoniewicz, 2025: 38).

۵-۳- سنگاپور

سنگاپور یکی از کشورهای آسیایی پیشرو در زمینه مبارزه با جرایم سایبری است که در سال‌های اخیر به‌سرعت در راستای بهبود قوانین و ظرفیت‌های قانونی در این حوزه گام برداشته است.

سنگاپور با تصویب Computer Misuse Act (CMA) در سال ۱۹۹۳، قانون‌گذاری در زمینه جرایم سایبری را آغاز کرد و به‌طور پیوسته این قانون را باتوجه به تحولات جدید در فناوری‌های دیجیتال به‌روزرسانی کرده است. در این قانون، جرایم مختلف سایبری، ازجمله هک، تخریب داده‌ها و دسترسی غیرمجاز به سیستم‌های اطلاعاتی تحت پیگرد قانونی قرار گرفته‌اند. همچنین این کشور به‌عنوان یک کشور آسیایی در زمینه همکاری‌های بین‌المللی، به‌ویژه در زمینه استرداد مجرمان سایبری و همکاری با نهادهای بین‌المللی مانند

اینترپل و یوروپل، عملکرد مثبتی داشته است. همچنین سنگاپور در زمینه تبادل اطلاعات با کشورهای منطقه‌ای و بین‌المللی همکاری‌های قابل توجهی دارد (Broadhurst & Chang, 2013: 53).

تجربیات این کشورها نشان می‌دهد که تدوین قوانین جامع و به‌روز برای مقابله با جرایم سایبری ضروری است. قوانین باید ضمن پوشش جرایم نوظهور، شفاف و عملیاتی باشند. همکاری‌های بین‌المللی از طریق قراردادهای دو یا چندجانبه و عضویت در نهادهای بین‌المللی نظیر اینترپل و یوروپل، اهمیت به‌سزایی در مبارزه با جرایم فراملی دارد. پیشگیری و آگاهی‌بخشی به موازات اقدامات اجرایی، از طریق ارتقای آگاهی عمومی و افزایش امنیت سایبری، می‌تواند نقش مؤثری در کاهش جرایم سایبری ایفا کند. استفاده از فناوری‌های پیشرفته و تحلیل داده‌ها، مانند تحلیل داده‌های بزرگ و هوش مصنوعی، می‌تواند به بهبود شناسایی و تعقیب مجرمان کمک کند. برای کشورهایی که قصد تقویت ظرفیت‌های حقوقی و اجرایی خود در زمینه مقابله با جرایم سایبری را دارند، الگوگیری از تجربیات موفق کشورهایی چون آمریکا، اتحادیه اروپا و سنگاپور می‌تواند بسیار مؤثر باشد. این تجربیات همچنین نشان می‌دهد که ترکیبی از رویکردهای ملی و بین‌المللی، راه حلی کارآمد برای مقابله با جرایم سایبری است. در همین راستا در ادامه به رویکرد نظام حقوقی ایران پیرامون تعقیب و استرداد مجرمان سایبری می‌پردازیم.

۵-۴- رویکرد حقوق کیفری ایران

رویکرد حقوق کیفری ایران نسبت به تعقیب و استرداد مجرمان سایبری به دو بخش قابل تقسیم است: ۱- تعقیب داخلی مجرمان سایبری؛ ۲- استرداد مجرمان در سطح بین‌المللی.

۵-۴-۱- تعقیب داخلی مجرمان سایبری

ایران در مقابله با جرایم سایبری قوانین متعددی تصویب کرده که مهم‌ترین آن قانون جرایم رایانه‌ای مصوب ۱۳۸۸ که بعدها به‌عنوان فصل سی‌ام کتاب پنجم قانون مجازات اسلامی مصوب ۱۳۷۵ تعیین و اضافه شد. این قانون به بررسی و جرم‌انگاری بسیاری از جرایم سایبری پرداخته و ابزارهای قانونی برای تعقیب مجرمان را فراهم کرده است.

ماده ۷۲۹ تا ۷۵۳ این قانون، به تعریف و جرم‌انگاری جرایم نظیر دسترسی غیرمجاز، شنود غیرمجاز، جعل رایانه‌ای، تخریب داده‌ها و اخلال در سامانه‌های رایانه‌ای یا مخابراتی می‌پردازد. همچنین ماده ۶۶۴ قانون آیین دادرسی کیفری صلاحیت محاکم ایران را درخصوص جرایم سایبری با تأکید بر معیار سرزمینی (ارتکاب جرم در ایران) و معیار شخصیت مجرم (اگر مرتکب ایرانی باشد) مشخص می‌کند. طبق قانون مجازات اسلامی (مصوب ۱۳۹۲)، اصل صلاحیت سرزمینی (ماده ۳) و اصل صلاحیت شخصی (ماده ۷) امکان تعقیب مجرمان خارجی یا ایرانی که مرتکب جرایم سایبری در یا علیه ایران شده‌اند، فراهم می‌کند.

۵-۴-۲- استرداد مجرمان سایبری در سطح بین‌المللی

ایران عضو کنوانسیون بوداپست (کنوانسیون جرایم سایبری) نیست، اما با استناد به قانون استرداد مجرمان مصوب ۱۳۳۹ و معاهدات دو یا چندجانبه، امکان استرداد مجرمان سایبری وجود دارد که ذیلاً به مهم‌ترین موارد اشاره می‌کنیم:

ماده ۱: استرداد براساس معاهده، توافق یا اصل مقابله به مثل امکان‌پذیر است.

ماده ۳: جرایمی که هم در کشور درخواست‌کننده و هم در ایران جرم‌انگاری شده باشند، قابلیت استرداد دارند (اصل جرم‌انگاری مضاعف).

ماده ۶: استرداد در جرایم سیاسی یا در مواردی که ماهیت جرم اقتصادی یا نظامی است، قابل اعمال نیست (کلانتری، ۱۴۰۱: ۲۲).

ایران در برخی موارد براساس توافقات دو یا چندجانبه با کشورها، همکاری برای استرداد مجرمان سایبری را انجام می‌دهد. به‌عنوان مثال، توافق‌نامه‌های دوجانبه با برخی کشورهای منطقه و همکاری با اینترپل در زمینه استرداد مجرمان. همچنین ایران از طریق پلیس بین‌الملل (اینترپل) برای شناسایی و تعقیب مجرمان سایبری که فراتر از مرزهای کشور فعالیت می‌کنند، اقدام می‌کند. این امر مطابق با ماده ۲۸ آیین‌نامه سازمان اینترپل و اصول حقوق کیفری بین‌المللی انجام می‌شود.

علیرغم مقررات فوق چالش‌ها و کاستی‌هایی در این زمینه مشهود است که ذیلاً به آن‌ها اشاره کرده و پیشنهادهایی را ارائه می‌نماییم.

عدم عضویت در کنوانسیون بوداپست: این موضوع باعث محدودیت در همکاری‌های بین‌المللی ایران در حوزه جرایم سایبری شده است.

نبود معاهدات دوجانبه کافی: برخی کشورها هنوز توافقات دوجانبه برای استرداد مجرمان سایبری با ایران ندارند.

جرم‌انگاری مضاعف: تفاوت در تعریف جرایم سایبری میان قوانین داخلی ایران و سایر کشورها گاه مانع استرداد می‌شود.

برای بهبود وضعیت تعقیب و استرداد مجرمان سایبری، پیشنهاد می‌شود:

تصویب قوانین جدید یا اصلاح قوانین موجود: تطبیق قوانین داخلی با معیارهای بین‌المللی مانند کنوانسیون بوداپست.

تقویت همکاری‌های بین‌المللی: انعقاد معاهدات دوجانبه با کشورهای دیگر برای تسهیل استرداد.

ارتقای تعامل با اینترپل: استفاده بهینه از ظرفیت این سازمان در شناسایی و استرداد مجرمان.

این رویکردها می‌تواند ایران را در مقابله مؤثرتر با جرایم سایبری یاری کند و موجب ارتقای امنیت سایبری در کشور شود.

نتیجه‌گیری

جرایم سایبری به‌دلیل ویژگی‌های خاص خود، ازجمله فرامرزی‌بودن، سرعت بالای وقوع و ناشناسی عاملان، چالش‌های بی‌سابقه‌ای برای نظام‌های قضایی و قانونی در سطح جهانی ایجاد کرده است. این جرایم که به‌طور فزاینده‌ای در دنیای دیجیتال رواج پیدا کرده‌اند، نه‌تنها تهدیداتی جدی برای امنیت اطلاعات و حریم خصوصی شهروندان به‌همراه دارند، بلکه همچنین به چالش‌های مهمی در زمینه همکاری‌های بین‌المللی، استرداد مجرمان و اعمال عدالت در سطح جهانی تبدیل شده‌اند. مطالعه تطبیقی میان کشورهای پیشرو نظیر ایالات متحده آمریکا، اتحادیه اروپا و سنگاپور، نشان می‌دهد که هر کشور باتوجه به ظرفیت‌های قانونی، زیرساخت‌های فناوری و ساختارهای بین‌المللی، راهکارهای مختلفی را برای مقابله با جرایم سایبری به‌کار گرفته است، ازجمله این راهکارها می‌توان به تصویب قوانین ملی، توسعه همکاری‌های بین‌المللی و استفاده از فناوری‌های نوین مانند هوش مصنوعی و سامانه‌های یکپارچه برای ردیابی مجرمان سایبری اشاره کرد.

با این حال، چالش‌های فراوانی همچنان وجود دارد، ازجمله تناقضات قانونی بین کشورهای مختلف، کمبود شفافیت در صلاحیت‌های قضایی و ناهماهنگی در تعریف و طبقه‌بندی جرایم سایبری که می‌تواند بر روند تعقیب و استرداد مجرمان تأثیرگذار باشد، به‌علاوه پیشرفت‌های سریع فناوری و ضعف ابزارهای قانونی موجود، ایجاد هماهنگی‌های بین‌المللی مؤثر در برخورد با این جرایم را دشوار کرده است.

در این راستا، تقویت همکاری‌های بین‌المللی، تدوین استانداردهای مشترک حقوقی، به‌روزرسانی قوانین باتوجه به تحولات تکنولوژیک و تقویت آموزش و ظرفیت‌سازی برای مقامات قضایی و اجرایی، ازجمله راهکارهایی هستند که می‌توانند به تقویت صلاحیت محاکم قضایی در مقابله با جرایم سایبری کمک کنند. از طرف دیگر، نقش سازمان‌های بین‌المللی مانند اینترپل و یوروپل در تسهیل همکاری‌های میان‌کشوری و نظارت بر اجرای قوانین بین‌المللی، اهمیت زیادی دارد.

درنهایت، برای مقابله مؤثر با جرایم سایبری و تقویت صلاحیت محاکم قضایی در سطح جهانی، نیازمند یک رویکرد یکپارچه و هماهنگ در سطح بین‌المللی هستیم که در آن، همکاری‌های بین‌المللی، هم‌افزایی فناوری‌های نوین و آموزش و ظرفیت‌سازی در کنار یکدیگر قرار گیرند تا بتوانند به‌طور مؤثری به امنیت فضای سایبری و حقوق شهروندان در برابر تهدیدات دیجیتال پاسخ دهند.

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

تعارض منافع: تدوین این مقاله، فاقد هرگونه تعارض منافعی بوده است.

سهم نویسندگان: نگارش مقاله به‌صورت مشترک توسط نویسندگان انجام گرفته است.

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

تأمین اعتبار پژوهش: این پژوهش بدون تأمین اعتبار مالی سامان یافته است.

منابع و مآخذ

الف. منابع فارسی

– پورقهرمانی، بابک (۱۳۹۶). «مطالعه تطبیقی سازکارهای حمایت از بزه‌دیدگان جرایم رایانه‌ای در حقوق کیفری ایران و اسناد بین‌المللی با تأکید بر کنوانسیون بوداپست». *پژوهشنامه حقوق کیفری*، ۱۵: ۱–۳۶.

– شاکری، ابوالحسن و هادی‌زاده، رضا (۱۳۹۵). «اصل تفکیک مقام تعقیب از مقام تحقیق در حقوق ایران». *پژوهشنامه حقوق کیفری*، ۱۳: ۱۴۱–۱۶۳.

– کلانتری، کیومرث (۱۴۰۱). *مجموعه قوانین و مقررات همکاری‌های بین‌المللی ایران و کشورهای جهان در زمینه کیفری*. چاپ دوم، تهران: انتشارات مجد.

ب. منابع انگلیسی

- Broadhurst. R & Chang, L (2013). Cybercrime in Asia: Trends and challenges.

- Directive 2013/40/EU of the European Parliament and of the Council. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jladsc2015&div=41&id=&page=

- Finklea, K & Theohary, C.A (2013). Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement. Congressional Research Service.

https://www.researchgate.net/publication/282725911_Cybercrime_Conceptual_issues_for_congress_and_US_law_enforcement

- Goodman, S & Sofaer, A (2013). *The Transnational Dimension of Cyber Crime and Terrorism*. Stanford University, Hoover Institution Press.

- Holt, T; Bossler, A & Seigfried-Spellar, K (2022). *Cybercrime and Digital Forensics: An Introduction*. 3rd Ed., London: Routledge.

- Radoniewicz, F (2025). *Cybercrime and the Law An Analysis of Legal Governance in Europe*. https://www.routledge.com/Cybercrime-and-the-Law-An-Analysis-of-Legal-Governance-in.

- Zhou. Y; Tiwari, M; Bernot, A & Lin, K (2024). "Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality". *Asian Journal of Criminology*, 19: 419–439.