Journal of
International Criminal Law
www.iclj.ir

Volume 4, Issue 3, 2026

Criminal Prosecution of Cybercrimes with an International Nature

Farzad Zibaei[1*]

1. Department of Public International Law, Najafabad University, Isfahan, Iran.

ARTICLE INFORMATION

Type of Article:
Original Research
Pages: ***49-61***

Corresponding Author's Info:
ORCID: *0009-0007-5824-4007*
TELL: *+989134000090*
Email: *zibaei.farzad@gmail.com*

Article History:
Received: *11 Dec 2025*
Revised: *24 Dec 2025*
Accepted: *05 Feb 2026*
Published online: *23 Sep 2026*

Keywords:
Cybercrime, International Criminal Prosecution, Criminal Jurisdiction, Mutual Legal Assistance, Extradition of Offenders, Electronic Evidence

ABSTRACT

The increasing spread of cybercrimes and the transboundary nature of cyberspace have presented traditional models of criminal jurisdiction and international cooperation with serious challenges. In many cyber cases, the material element, the harmful outcome, the technical infrastructure, and the identity of the perpetrator and victim are scattered across multiple countries, making it difficult to determine the competent state for prosecution and postponing access to electronic evidence to effective cooperation between states and the private sector. This research, using a descriptive-analytical method and based on a library and document study, explains the conceptual framework of "cybercrimes with an international nature", the principles governing their criminal prosecution, the foundations and conflicts of criminal jurisdiction of states, as well as the mechanisms of judicial and police cooperation in international documents. The 2001 Budapest Convention and recent developments, including the United Nations Convention against Cybercrime, are critically examined in terms of harmonizing criminalization, providing for specific means of obtaining digital evidence, extradition, and mutual legal assistance. The findings show that despite significant progress in strengthening rapid cooperation and specialized networks, conflicts of jurisdiction, slow formal processes, differing human rights standards, and challenges posed by new technologies such as end-to-end encryption and cloud services still constitute significant obstacles to the efficient and rights-based prosecution of cybercrimes of an international nature. Finally, suggestions are made for reforming domestic law, strengthening treaty regimes, and striking a balance between cybersecurity and the protection of fundamental human rights.

How to Cite This Article: Zibaei, F (2026). "Criminal Prosecution of Cybercrimes with an International Nature". *Journal of International Criminal Law*, 4(3): 49-61.

فصلنامه حقوق جزای بین‌الملل

www.iclj.ir

انجمن علمی فقه جزای تطبیقی ایران

دوره چهارم، شماره سوم، پائیز ۱۴۰۵

پیگرد کیفری جرائم سایبری با ماهیت بین‌المللی

فرزاد زیبائی[۱*]

۱. گروه حقوق بین‌الملل عمومی، دانشگاه نجف‌آباد، اصفهان، ایران.

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۴۹-۶۱

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۹-۰۰۰۷-۵۸۲۴-۴۰۰۷

تلفن: ۹۸۹۱۳۴۰۰۰۰۹۰+

ایمیل: zibaei.farzad@gmail.com

سابقه مقاله:

تاریخ دریافت: ۱۴۰۴/۰۹/۲۰

تاریخ ویرایش: ۱۴۰۴/۱۰/۰۳

تاریخ پذیرش: ۱۴۰۴/۱۱/۱۶

تاریخ انتشار: ۱۴۰۵/۰۷/۰۱

واژگان کلیدی:

جرائم سایبری، پیگرد کیفری بین‌المللی، صلاحیت کیفری، معاضدت قضایی متقابل، استرداد مجرمان، ادله الکترونیکی.

چکیده

گسترش فزاینده جرائم سایبری و ماهیت فرا مرزی فضای مجازی، الگوهای سنتی صلاحیت کیفری و همکاری‌های بین‌المللی را با چالش‌های جدی روبه‌رو کرده است. در بسیاری از پرونده‌های سایبری، عنصر مادی، نتیجه زیان‌بار، زیرساخت‌های فنی و هویت مرتکب و بزه‌دیده در چندین کشور پراکنده است و این امر، هم تعیین دولت صالح برای تعقیب را دشوار می‌سازد و هم دسترسی به ادله الکترونیکی را به همکاری مؤثر میان دولت‌ها و بخش خصوصی موکول می‌کند. این پژوهش با روش توصیفی ـ تحلیلی و مبتنی‌بر مطالعه کتابخانه‌ای و اسنادی، به تبیین چارچوب مفهومی «جرائم سایبری با ماهیت بین‌المللی»، اصول حاکم بر پیگرد کیفری آن‌ها، مبانی و تعارض‌های صلاحیت کیفری دولت‌ها و نیز سازوکارهای همکاری قضایی و پلیسی در اسناد بین‌المللی می‌پردازد. کنوانسیون بوداپست ۲۰۰۱ و تحولات جدید از جمله کنوانسیون ملل متحد علیه جرائم سایبری، از حیث هماهنگ‌سازی جرم‌انگاری، پیش‌بینی ابزارهای خاص تحصیل ادله دیجیتال، استرداد و معاضدت قضایی متقابل، مورد بررسی انتقادی قرار گرفته‌اند. یافته‌ها نشان می‌دهد که علی‌رغم پیشرفت‌های قابل توجه در تقویت همکاری‌های سریع و شبکه‌های تخصصی، تعارض صلاحیت‌ها، کندی فرایندهای رسمی، تفاوت استانداردهای حقوق بشری و چالش‌های ناشی از فناوری‌های نوین مانند رمزنگاری سرتاسری و خدمات ابری، هنوز موانع مهمی در برابر پیگرد کیفری کارآمد و در عین حال حقوق‌مدار جرائم سایبری با ماهیت بین‌المللی به‌شمار می‌آیند. در پایان، پیشنهادهایی برای اصلاح حقوق داخلی، تقویت رژیم‌های معاهده‌ای و ایجاد تعادل میان امنیت سایبری و صیانت از حقوق بنیادین بشر ارائه شده است.

مقدمه

پیگرد کیفری جرائم سایبری با ماهیت بین‌المللی در دهه‌های اخیر به یکی از پیچیده‌ترین چالش‌های حقوق کیفری و حقوق بین‌الملل کیفری تبدیل شده است. ماهیت فرا مرزی فضای مجازی، امکان ارتکاب جرم از هر نقطه جهان علیه اهدافی در چندین کشور، استفاده از زیرساخت‌های توزیع‌شده و ناشناسی نسبی مرتکبان، موجب شده است که الگوهای سنتی صلاحیت کیفری، استرداد مجرمان و معاضدت قضایی متقابل، کارایی کافی نداشته باشند. این مقاله با رویکرد تحلیلی ـ توصیفی و با بهره‌گیری از روش کتابخانه‌ای و اسنادی، می‌کوشد چارچوب حقوقی حاکم بر پیگرد کیفری جرائم سایبری با عنصر بین‌المللی را در سطوح ملی و بین‌المللی تبیین و ارزیابی کند و ضمن بررسی اسناد مهمی همچون کنوانسیون بوداپست ۲۰۰۱ شورای اروپا و کنوانسیون تازه تصویب‌شده سازمان ملل متحد علیه جرائم سایبری، ظرفیت‌ها و کاستی‌های آن‌ها را در پاسخ‌گویی به چالش‌های نو پدید فضای سایبری نشان دهد.

پرسش اصلی این است که رژیم کنونی حقوقی بین‌المللی و داخلی تا چه حد امکان پیگرد مؤثر و در عین حال منطبق با استانداردهای حقوق بشر را برای جرائم سایبری فرا مرزی فراهم آورده است و چه اصلاحاتی برای ارتقای کارآمدی و مشروعیت این رژیم لازم است. فرضیه‌ی مقاله آن است که هرچند اسناد موجود به‌ویژه کنوانسیون بوداپست و کنوانسیون جدید ملل متحد، گام مهمی در هماهنگ‌سازی قوانین، تقویت ابزارهای تحقیق کیفری و ارتقای همکاری‌های بین‌المللی برداشته‌اند، اما تداوم تعارض صلاحیت‌ها، فرایندهای کند و بوروکراتیک معاضدت قضایی، اختلافات سیاسی میان دولت‌ها و نگرانی‌ها نسبت به نقض حقوق بنیادین بشر، همچنان موانع جدی بر سر راه پیگرد مؤثر جرائم سایبری با ماهیت بین‌المللی ایجاد می‌کند. مقاله حاضر شامل سه بخش اصلی و یک نتیجه‌گیری است و در آن، نخست چارچوب مفهومی و مبنایی جرائم سایبری با عنصر خارجی و اصول حاکم بر پیگرد کیفری آن‌ها تبیین می‌شود، سپس بنیادهای صلاحیت کیفری دولت‌ها و انعکاس آن‌ها در اسناد بین‌المللی تحلیل می‌گردد، سپس در گام بعدی سازوکارهای همکاری قضایی و پلیسی و چالش‌های عملی آن‌ها بررسی می‌شود و در نهایت، جمع‌بندی و پیشنهادهایی برای اصلاح حقوق داخلی و تقویت رژیم بین‌المللی مبارزه با جرائم سایبری ارائه می‌گردد.

۱- چارچوب مفهومی و مبنایی پیگرد کیفری جرائم سایبری با ماهیت بین‌المللی

۱-۱- تعریف و شاخص‌های جرائم سایبری با ماهیت بین‌المللی

در ادبیات حقوقی، جرم سایبری به رفتارهای مجرمانه‌ای اطلاق می‌شود که موضوع آن داده‌ها و سامانه‌های رایانه‌ای و مخابراتی است یا ارتکاب آن با ابزارها و شبکه‌های الکترونیکی صورت می‌گیرد (شیرزاد، ۱۳۸۸: ۱۲؛ جلالی‌فراهانی، ۱۳۸۴: ۴۶). جرم سایبری بین‌المللی زمانی محقق می‌شود که حداقل یکی از عناصر سه‌گانه آن (عنصر مادی، معنوی، قانونی) به بیش از یک کشور مرتبط باشد. به‌طور مشخص، وجود عنصر خارجی در جرم سایبری به این معناست که محل استقرار مرتکب، محل ورود ضرر یا محل قرارگیری بزه‌دیده در چند کشور مختلف باشد؛ یا زیرساخت‌های فنی مورد استفاده در حوزه‌های صلاحیتی گوناگون پراکنده باشد؛ یا رفتار ارتکابی در یک کشور و نتیجه در کشوری دیگر رخ دهد (جلالی‌فراهانی، ۱۳۹۳: ۳۵). بسیاری از جرائم سایبری ذاتا پتانسیل بین‌المللی دارند و حتی اگر مرتکب و بزه‌دیده در یک کشور باشند، زیرساخت‌های فنی غالبا در چند کشور مستقر است که این امر، بحث صلاحیت کیفری و همکاری بین‌المللی را اجتناب‌ناپذیر می‌کند.

۱-۲- ویژگی‌های فنی و حقوقی فضای سایبر و تأثیر آن بر پیگرد کیفری

پیگرد کیفری جرائم سایبری با چند ویژگی خاص مواجه است که آن را از جرائم سنتی متمایز می‌کند:

۱-۲-۱- سرعت و زودگذری داده‌ها

سرعت و زودگذری داده‌ها، چالش اساسی در پیگرد کیفری جرائم سایبری است، زیرا داده‌های مرتبط با جرم (لاگ‌ها، IP ها، پیام‌ها و ...) به‌سرعت تغییر کرده یا حذف می‌شوند (باستانی، ۱۳۹۰: ۴۷؛ جلالی‌فراهانی، ۱۳۸۴: ۷۳). پویایی و تغییر سریع داده‌ها، به‌دلیل ظرفیت محدود سیستم‌های ذخیره‌سازی و جایگزینی خودکار داده‌های جدید با قدیمی‌تر، می‌تواند منجر به

از بین رفتن اطلاعات مفید در تحقیقات قضائی شود (زیبر، ۱۳۹۰: ۳۵). سیاست‌های نگهداری داده‌ها در برخی سیستم‌ها نیز مشکل‌ساز است، زیرا ارائه‌دهندگان خدمات اینترنتی داده‌ها را تنها برای مدت محدودی نگه می‌دارند و در صورت عدم صدور به‌موقع درخواست‌های قضائی، اطلاعات حیاتی از دست می‌رود (زندی، ۱۳۸۹: ۴۹). ماهیت پویا و تغییرپذیر داده‌ها (مانند IP ها و Session ها) نیز شناسایی فردی را دشوار می‌کند (پوربافرانی، ۱۳۹۶: ۷۶). زمان‌بندی دقیق در حفظ و دسترسی به داده‌ها اهمیت ویژه‌ای دارد و تأخیر در درخواست‌های قضائی می‌تواند به از بین رفتن ادله منجر شود (جلالی‌فراهانی، ۱۳۸۴: ۶۳). اسناد بین‌المللی مانند کنوانسیون بوداپست ۲۰۰۱، اقداماتی برای مقابله با این چالش‌ها پیش‌بینی کرده‌اند. طراحی و پیاده‌سازی سیاست‌ها و ابزارهای مؤثر برای جلوگیری از نابودی زودهنگام داده‌ها در روندهای قضائی ضروری است، زیرا تأخیر در حفظ و دسترسی به داده‌ها می‌تواند پیامدهای جدی برای تحقیقات قضائی داشته باشد (فهیمی، ۱۳۸۰: ۱۳۸).

۱-۲-۲- ناشناسی و استفاده از ابزارهای پنهان‌ساز

ناشناسی و استفاده از ابزارهای پنهان‌ساز، چالش اساسی در پیگرد کیفری جرائم سایبری بین‌المللی است (زیبر، ۱۳۹۰: ۳۷؛ شیرزاد، ۱۳۸۸: ۳۲). شبکه‌های ناشناس‌ساز مانند Tor، با هدایت ارتباطات اینترنتی از طریق لایه‌های مختلف، شناسایی موقعیت جغرافیایی و هویت کاربر را دشوار می‌کنند و در فعالیت‌های غیرقانونی مانند هک و تروریسم کاربرد دارند (اردبیلی، ۱۳۸۱: ۳۶؛ ساعد، ۱۳۸۹: ۵۹). VPNها نیز با پنهان کردن آدرس IP واقعی، از پیگیری اطلاعات جلوگیری می‌کنند. پروکسی‌ها نیز با هدایت ترافیک اینترنتی از طریق سرورهای واسطه‌ای، هویت آنلاین را پنهان می‌سازند (شیرزاد، ۱۳۸۸: ۴۸). شبکه‌های تاریک ، بستری برای فعالیت‌های[1] غیرقانونی فراهم می‌کنند (زندی، ۱۳۸۹: ۵۶). این ابزارها شناسایی و انتساب رفتارهای مجرمانه را پیچیده کرده و اجرای احکام قضائی و همکاری‌های بین‌المللی را با مشکل مواجه می‌کنند (زیبر، ۱۳۹۰: ۳۹؛ فهیمی، ۱۳۸۰: ۱۴۰). استفاده از این ابزارها در کنار تقلب هویتی یا حملات سایبری پیچیده، فرایندهای قضائی را مختل کرده و نیاز به همکاری‌های بین‌المللی، توسعه فناوری‌های شناسایی پیشرفته و تدوین قوانین به‌روز را ضروری می‌سازد.

۱-۲-۳- زنجیره‌ای بودن ادله الکترونیکی

زنجیره‌ای بودن ادله الکترونیکی، چالش مهمی در پیگرد کیفری جرائم سایبری است، زیرا داده‌ها در مکان‌های مختلف و در اختیار شرکت‌ها و نهادهای گوناگون در کشورهای مختلف نگهداری می‌شوند (فامیلی‌زوار جلالی، ۱۳۹۴: ۴۸). پراکندگی جغرافیایی داده‌ها، دسترسی به آن‌ها و پیگرد مجرمان را پیچیده‌تر می‌کند، زیرا هر کشور قوانین خاص خود را دارد (ناصری، ۱۳۸۷: ۶۳). نقش بخش خصوصی در ذخیره‌سازی و پردازش داده‌ها نیز حیاتی است و دسترسی به داده‌ها معمولا به مجوز و همکاری این شرکت‌ها بستگی دارد (زیبر، ۱۳۹۰: ۴۵). پیگرد جرائم سایبری نیازمند همکاری بین‌المللی و هماهنگی میان مراجع مختلف دولتی و قضائی است (پوربافرانی، ۱۳۹۶: ۹۳؛ شیرزاد، ۱۳۸۸: ۷۳). زنجیره‌ای بودن ادله الکترونیکی و نیاز به هماهنگی، در موفقیت پیگرد جرائم سایبری اهمیت فراوانی دارد و عدم هماهنگی می‌تواند منجر به از دست رفتن ادله و نقض حقوق افراد شود. ایجاد سازوکارهای مؤثر برای تسهیل همکاری‌های بین‌المللی و بهبود هماهنگی بین مراجع دولتی و خصوصی ضروری است.

۱-۲-۴- وابستگی شدید به همکاری بخش خصوصی

وابستگی شدید به همکاری بخش خصوصی، ویژگی بارز پیگرد کیفری جرائم سایبری است، زیرا داده‌ها عمدتا توسط ارائه‌دهندگان خدمات اینترنتی و پلتفرم‌های اجتماعی ذخیره می‌شوند (زیبر، ۱۳۹۰: ۴۷). چالش‌ها شامل نقش حیاتی بخش خصوصی در ذخیره‌سازی داده‌ها، مسائل مربوط به حفظ حریم خصوصی و امنیت داده‌ها (پوربافرانی، ۱۳۹۶: ۱۱۳؛ شیرزاد، ۱۳۸۸: ۵۸)، نیاز به تعامل سریع و مؤثر با شرکت‌های فناوری (جلالی فراهانی، ۱۳۹۳: ۵۷) و نیاز به استانداردسازی و شفافیت در فرآیندها است (خداقلی، ۱۳۸۳: ۳۳). بدون مشارکت فعال و سریع شرکت‌ها، پیگرد کیفری جرائم سایبری با مشکلات

[1]- Dark Web

اجرائی روبه‌رو شده و ممکن است به بن‌بست برسد (زندی، ۱۳۸۹: ۷۵؛ ناصری، ۱۳۸۷: ۸۴). این وابستگی، ضرورت تدوین قواعد ویژه در سطح داخلی و بین‌المللی و نیاز به **«زمان واکنش بسیار کوتاه»** را توجیه می‌کند و مبنای شکل‌گیری اسنادی چون کنوانسیون بوداپست و شبکه‌های ۷/۲۴ همکاری فوری بوده است.

۱-۳- اصول حاکم بر پیگرد کیفری در سطح بین‌المللی

هرچند دولت‌ها در اعمال صلاحیت کیفری نسبت به جرائم سایبری، به‌موجب اصل حاکمیت، آزادی گسترده‌ای دارند، اما پیگرد کیفری فرا مرزی باید با اصولی همراه باشد که از سوءاستفاده و نقض حقوق بنیادین جلوگیری کند. مهم‌ترین این اصول عبارت‌اند از:

۱-۳-۱- اصل احترام به حاکمیت و عدم مداخله

اصل احترام به حاکمیت و عدم مداخله در حقوق بین‌الملل، در پیگرد کیفری جرائم سایبری اهمیت ویژه‌ای دارد (ساعد، ۱۳۸۹: ۶۹). چالش‌ها شامل دسترسی مستقیم به داده‌ها یا سامانه‌ها که ممکن است نقض حاکمیت تلقی شود (زیبر، ۱۳۹۰: ۵۰)، پیچیدگی‌های مربوط به معاهدات بین‌المللی و دسترسی به داده‌ها (جلالی‌فراهانی، ۱۳۹۳: ۷۴)، تضاد میان قوانین داخلی و بین‌المللی (پوربافرانی، ۱۳۹۶: ۱۳۴) و دسترسی به سامانه‌های حساس دولتی (حسینی‌خواه، ۱۳۹۰: ۴۳) است. دسترسی به داده‌ها و سامانه‌های کشورهای دیگر باید با رعایت قوانین داخلی، مقررات بین‌المللی و با اخذ مجوزهای قانونی صورت گیرد. عدم رعایت این اصل می‌تواند به نقض حاکمیت کشورها و ایجاد تنش‌های بین‌المللی منجر شود. ایجاد چارچوب‌های قانونی و توافقات بین‌المللی شفاف و مؤثر برای دسترسی به داده‌ها و همکاری‌های قضائی ضروری است.

۱-۳-۲- اصل قانونی بودن جرم و مجازات و پیش‌بینی‌پذیری

اصل قانونی بودن جرم و مجازات و پیش‌بینی‌پذیری در پیگرد جرائم سایبری اهمیت ویژه‌ای دارد (خداقلی، ۱۳۸۳: ۳۹؛ عالی‌پور، ۱۳۹۰: ۵۱). چالش‌ها شامل توسعه صلاحیت‌های گسترده و مبهم بر پایه معیارهایی مانند "اثر" در فضای سایبر (زیبر، ۱۳۹۰: ۵۵؛ صنوبر، ۱۳۹۳: ۵۵)، پیش‌بینی‌پذیری پیامدهای کیفری رفتارها در فضای سایبر (خداقلی، ۱۳۸۳: ۴۲؛ عالی‌پور، ۱۳۹۰: ۵۵) و خطرات استفاده از استانداردهای حقوقی مبهم در جرائم سایبری است. قوانین و صلاحیت‌ها باید به‌گونه‌ای طراحی شوند که شفاف و قابل‌پیش‌بینی باشند و از تفسیرهای گسترده و مبهم جلوگیری شود. توسعه صلاحیت‌های کیفری باید محدود به اصولی باشد که امکان پیش‌بینی‌پذیری برای شهروندان و مقامات قضائی فراهم کند و در چارچوب قوانین حقوق بشر و با رعایت حقوق فردی و حاکمیت کشورها صورت گیرد (نجفی‌ابرندآبادی، ۱۳۸۳: ۳۷).

۱-۳-۳- اصل تناسب و ضرورت در اقدامات تحقیقاتی

اصل تناسب و ضرورت در اقدامات تحقیقاتی در پیگرد جرائم سایبری باید با دقت و رعایت حقوق بنیادین افراد به‌کار گرفته شود (زیبر، ۱۳۹۰: ۵۸؛ عالی‌پور، ۱۳۹۰: ۴۵). چالش‌ها شامل ضرورت و تناسب در استفاده از ابزارهای تحقیقاتی (خداقلی، ۱۳۸۳: ۴۵؛ نجفی‌ابرندآبادی، ۱۳۸۳: ۵۶)، حفظ تعادل بین امنیت و حقوق بشر (نجفی‌ابرندآبادی، ۱۳۸۳: ۳۲؛ جلالی‌فراهانی و باقری‌اصل، ۱۳۸۷: ۳۶)، نظارت قضائی بر استفاده از ابزارهای تحقیقاتی (حسینی‌خواه، ۱۳۹۰: ۶۵؛ سلامتی، ۱۳۸۷: ۳۹) و محدودیت زمانی و مکانی در استفاده از ابزارهای تحقیقاتی (عالی‌پور، ۱۳۹۰: ۶۷؛ جلالی‌فراهانی و باقری‌اصل، ۱۳۸۷: ۴۵) است. ابزارهایی مانند نگهداری فوری داده‌ها، شنود و دسترسی بلادرنگ به داده‌های ترافیکی تنها در مواقع ضروری و تحت نظارت قضائی دقیق به‌کار گرفته شوند و متناسب با شدت جرم و برای دستیابی به هدفی مشروع صورت گیرند. پیگرد کیفری در فضای سایبر باید به‌گونه‌ای انجام شود که حقوق بشر و آزادی‌های فردی رعایت شود و از مداخلات غیرضروری در زندگی شخصی افراد جلوگیری گردد.

۱-۳-۴- اصل احترام به حقوق بشر

اصل احترام به حقوق بشر در تمامی فرایندهای قضائی، به‌ویژه در پیگرد جرائم سایبری، باید رعایت شود (فامیلی‌زوار جلالی، ۱۳۹۴: ۶۴). چالش‌ها شامل حفظ حریم خصوصی افراد (جلالی‌فراهانی، ۱۳۹۳: ۷۶؛ سلامتی، ۱۳۸۷: ۵۶)، آزادی بیان (زیبر، ۱۳۹۰: ۶۴؛ موسوی، ۱۳۹۰: ۳۲)، دادرسی عادلانه (خداقلی، ۱۳۸۳: ۴۹) و منع بازداشت و محکومیت خودسرانه (جلالی‌فراهانی، ۱۳۹۳: ۷۸) است. اقدامات تحقیقاتی و قضائی

در فضای سایبر همواره باید بر مبنای احترام به حقوق فردی و آزادی‌های اساسی انجام شود و هرگونه دسترسی به داده‌ها، نظارت بر ارتباطات یا محدودیت در آزادی بیان باید در چارچوب قانون، با نظارت قضائی و با رعایت حقوق بشر باشد (موسوی، ۱۳۹۰: ۳۸).

۲- صلاحیت کیفری دولت‌ها در مواجهه با جرائم سایبری فرا مرزی

۲-۱- اصول سنتی صلاحیت و کارکرد آن‌ها در فضای سایبری

صلاحیت کیفری در حقوق بین‌الملل کلاسیک بر چند مبنای شناخته‌شده استوار است:

۲-۱-۱- اصل سرزمینی

اصل سرزمینی در تعیین صلاحیت کیفری دولت‌ها نسبت به جرائم اهمیت دارد (حسن‌بیگی، ۱۳۸۴: ۳۶). چالش‌ها شامل تعریف قلمرو سرزمینی در دنیای دیجیتال (حسینی‌خواه، ۱۳۹۰: ۷۸؛ موسوی، ۱۳۹۰: ۴۳)، زیرساخت‌های فنی و کنترل فضای مجازی (حسن‌بیگی، ۱۳۸۴: ۴۲)، تأثیر جهانی‌شدن فضای سایبر بر اصل سرزمینی (زیبر، ۱۳۹۰: ۶۰؛ موسوی، ۱۳۹۰: ۴۸) و تضاد در قوانین و معیارهای صلاحیت سرزمینی (حسن‌بیگی، ۱۳۸۴: ۵۶) است. اصل سرزمینی نیازمند بازنگری و گسترش است و کشورها باید از طریق معاهدات بین‌المللی و همکاری‌های چندجانبه برای دفاع از حقوق حاکمیتی خود در فضای سایبر و حل تعارض صلاحیت‌ها همکاری کنند.

۲-۱-۲- اصل شخصی فعال (تابعیت مرتکب)

اصل شخصی فعال به دولت‌ها امکان می‌دهد جرائم اتباعشان در خارج از کشور را پیگیری کنند (خداقلی، ۱۳۸۳: ۵۳). چالش‌ها شامل شناسایی تابعیت مرتکب در فضای سایبر (حسن‌بیگی، ۱۳۸۴: ۷۸)، تفاوت‌های قوانین ملی در خصوص جرم‌انگاری (حسینی‌خواه، ۱۳۹۰: ۵۸)، تضاد میان حقوق ملی و بین‌المللی و الزام به رعایت حقوق بشر (موسوی، ۱۳۹۰: ۵۲) است. ایجاد چارچوب‌های بین‌المللی هماهنگ و معاهدات دوجانبه و چندجانبه می‌تواند به روشن‌سازی این مسائل کمک کند. این اصل باید به‌طور دقیق با قوانین بین‌المللی و حقوق بشر هماهنگ شود تا از سوءاستفاده‌های احتمالی جلوگیری گردد.

۲-۱-۳- اصل شخصی منفعل (تابعیت بزه‌دیده)

اصل شخصی منفعل یا تابعیت بزه‌دیده یکی از اصول حقوق بین‌الملل کیفری است که به دولت‌ها اجازه می‌دهد درصورتی‌که جرم علیه اتباع آن‌ها در خارج از مرزهای سرزمینی آن کشور ارتکاب یابد، صلاحیت کیفری اعمال کنند. این اصل برخلاف اصل شخصی فعال (که بر اساس تابعیت مرتکب به دولت صلاحیت می‌دهد)، بر اساس تابعیت بزه‌دیده به دولت‌ها این امکان را می‌دهد که در پیگرد جرائم فرا مرزی، حتی اگر جرم در خارج از مرزهای آن‌ها رخ داده باشد، اقدام کنند. این اصل به‌ویژه در جرائم سایبری که اثرات آن به‌سرعت فرا مرزی می‌شود، اهمیت بسیاری دارد.

اولین چالش، پیچیدگی‌های شناسایی تابعیت بزه‌دیده است. در فضای سایبر، به‌ویژه در مواردی که اطلاعات شخصی یا مالی افراد به سرقت می‌رود، شناسایی تابعیت بزه‌دیده می‌تواند به‌ویژه زمانی که اطلاعات در سرورهای خارج از کشور ذخیره می‌شود، پیچیده باشد. درحالی‌که در جرائم سنتی، تعیین تابعیت بزه‌دیده معمولا از طریق شناسایی هویت فرد در دنیای فیزیکی ساده است، در فضای مجازی ممکن است شناسایی تابعیت بزه‌دیده دشوار و پرهزینه باشد. افراد می‌توانند از ابزارهایی مانند VPN، پروکسی یا شبکه‌های ناشناس‌ساز استفاده کنند که هویت و موقعیت جغرافیایی آن‌ها را پنهان کرده و تشخیص تابعیت را پیچیده می‌سازد (زیبر، ۱۳۹۰: ۷۰).

دومین چالش، تضاد با قوانین کشورهای دیگر است. طبق اصل شخصی منفعل، یک دولت می‌تواند صلاحیت خود را برای پیگرد جرائمی که علیه اتباع آن در خارج از کشور رخ داده است، اعمال کند. با این حال، این اصل می‌تواند با قوانین کشورهای دیگر که در آن جرم رخ داده است، در تضاد قرار گیرد. بسیاری از کشورها ممکن است قوانین و مقررات مختلفی برای جرم‌انگاری و پیگرد جرائم داشته باشند و اعمال صلاحیت کیفری بر اساس تابعیت بزه‌دیده ممکن است باعث تداخل صلاحیت‌ها شود. به‌ویژه در جرائم سایبری که در آن ممکن است چندین کشور به‌طور هم‌زمان درگیر باشند، تعارض صلاحیت‌ها می‌تواند به مشکلات حقوقی و اجرائی منجر شود و ممکن است حتی به نقض حقوق بشر یا استفاده ابزاری از

قانون برای اهداف سیاسی منجر گردد (حسینی‌خواه، ۱۳۹۰: ۶۱).

سومین چالش، مشکلات اجرائی در همکاری‌های بین‌المللی است. برای اعمال صلاحیت بر اساس تابعیت بزه‌دیده، نیاز به همکاری میان دولت‌ها در سطح بین‌المللی است. این همکاری‌ها می‌توانند از طریق معاهدات دوجانبه و چندجانبه، موافقت‌نامه‌های استرداد یا موافقت‌نامه‌های معاضدت قضائی صورت گیرند. با این حال، تفاوت‌های گسترده در قوانین داخلی کشورها، به‌ویژه در زمینه حفاظت از داده‌ها، حریم خصوصی و قوانین جزائی، می‌تواند مانع از دستیابی به همکاری‌های مؤثر شود. به‌ویژه در جرائم سایبری که ممکن است شامل دسترسی به داده‌های خصوصی و اطلاعات شخصی باشد، باید از اصول حقوق بشر و استانداردهای بین‌المللی در همکاری‌های قضائی و پلیسی پیروی شود (تقی‌زاده انصاری، ۱۳۸۸: ۵۴).

چهارمین چالش، اثرات فرا مرزی و جهانی‌شدن جرائم سایبری است. جرائم سایبری معمولا اثرات فرا مرزی دارند و ممکن است خسارت‌های آن در کشورهای مختلف مشاهده شود. درحالی‌که اصل شخصی منفعل به دولت‌ها این امکان را می‌دهد که نسبت به جرائمی که علیه اتباع آن‌ها در خارج از کشور واقع می‌شود، صلاحیت داشته باشند، اما جهانی بودن فضای سایبر ممکن است ایجاد صلاحیت‌های موازی و رقابت قضائی میان دولت‌ها را در پی داشته باشد. به‌ویژه در مورد جرائم سایبری که می‌توانند آسیب‌های جدی به زیرساخت‌ها و اقتصادهای ملی وارد کنند، تصمیم‌گیری درباره اینکه کدام کشور باید مسؤولیت پیگرد را بر عهده بگیرد، می‌تواند پیچیده و مشکل‌ساز باشد (خداقلی، ۱۳۸۳: ۶۴).

پیشنهادها برای رفع این چالش‌ها شامل توسعه چارچوب‌های حقوقی بین‌المللی است که صلاحیت‌های بین‌المللی را به‌طور دقیق تعریف کند و از تداخل صلاحیت‌ها جلوگیری کند. همچنین، تقویت همکاری‌های دوجانبه و چندجانبه میان کشورهای مختلف و اصلاح معاهدات موجود می‌تواند به کاهش تضادها و مشکلات اجرائی کمک کند. علاوه‌بر این، توجه ویژه به حقوق بشر و حریم خصوصی در فرآیند پیگردهای کیفری و ایجاد مکانیسم‌های شفاف و قابل‌اعتماد برای همکاری‌های قضائی و پلیسی از اهمیت ویژه‌ای برخوردار است. در نهایت، اصل شخصی منفعل به دولت‌ها اجازه می‌دهد تا در پیگرد جرائم سایبری که علیه اتباع آن‌ها در خارج از کشور ارتکاب یافته است، اقدام کنند، اما این اصل در فضای بین‌المللی با چالش‌هایی نظیر شناسایی تابعیت بزه‌دیده، تضاد با قوانین داخلی و بین‌المللی و مشکلات اجرائی در همکاری‌های بین‌المللی مواجه است که نیازمند اصلاحات حقوقی و تقویت همکاری‌های بین‌المللی است.

۲-۱-۴- اصل حمایتی

اصل حمایتی یکی از اصول مهم در حقوق بین‌الملل است که به دولت‌ها این امکان را می‌دهد که نسبت به جرائمی که امنیت و منافع اساسی آن‌ها را هدف قرار داده‌اند، حتی اگر این جرائم خارج از مرزهای سرزمینی آن‌ها ارتکاب یابند، صلاحیت خود را اعمال کنند. این اصل به‌ویژه در مورد جرائمی که اثرات جدی بر امنیت ملی، منافع اقتصادی، یا زیرساخت‌های حیاتی یک کشور دارند، به‌طور گسترده‌ای کاربرد دارد. یکی از مصادیق بارز این اصل، حملات سایبری علیه تأسیسات حیاتی است که می‌تواند به تهدید جدی برای امنیت ملی، اقتصاد و رفاه عمومی یک کشور تبدیل شود. اولین چالش، تعیین اینکه کدام جرائم در دسته جرائم علیه امنیت ملی قرار می‌گیرند، یکی از مسائل کلیدی در اعمال این اصل است. برای مثال، حملات سایبری می‌توانند تأسیسات حیاتی مانند شبکه‌های انرژی، سیستم‌های بانکی، زیرساخت‌های حمل‌ونقل و تأسیسات دولتی را هدف قرار دهند و خسارات جدی به امنیت ملی و اقتصاد کشور وارد کنند. این نوع جرائم، اگرچه ممکن است در خارج از مرزهای سرزمینی یک کشور انجام شوند، به دلیل اثرات عمیق آن‌ها بر امنیت داخلی کشور، می‌توانند تحت صلاحیت آن کشور قرار گیرند. با این حال، تعریف دقیق امنیت ملی و تعیین اینکه چه نوع حملات سایبری تهدیدی واقعی برای آن به‌شمار می‌آید، چالش‌هایی را در تعیین صلاحیت ایجاد می‌کند (زیبر، ۱۳۹۰: ۷۵).

دومین چالش، تضاد با اصل سرزمینی و دیگر اصول حقوقی است. اصل سرزمینی ایجاب می‌کند که دولت‌ها صلاحیت خود را محدود به سرزمین خود بدانند، اما اصل حمایتی این

محدودیت را در موارد خاصی که امنیت و منافع اساسی دولت تهدید می‌شود، نقض می‌کند. به‌ویژه در جرائم سایبری که می‌توانند اثرات گسترده‌ای در چندین کشور مختلف داشته باشند، ممکن است تضادهایی بین کشورها در خصوص اینکه کدام دولت صلاحیت پیگرد را دارد، بروز کند. برای مثال، اگر حمله سایبری از کشور "الف" علیه تأسیسات حیاتی کشور "ب" انجام شود، هر دو کشور ممکن است ادعای صلاحیت کنند و این می‌تواند به تعارض‌های حقوقی و اجرائی منجر شود (تقی‌زاده انصاری، ۱۳۸۸: ۶۷).

سومین چالش، همکاری بین‌المللی در پیگرد جرائم سایبری است. از آنجا که جرائم سایبری اغلب اثرات فرا مرزی دارند، اعمال صلاحیت حمایتی در چنین جرائمی نیازمند همکاری نزدیک و هماهنگی میان دولت‌ها است. اگر یک دولت بخواهد علیه یک حمله سایبری که از کشور دیگری به تأسیسات حیاتی آن کشور صورت گرفته است، اقدام کند، نیاز به همکاری قضائی و پلیسی با دولت دیگر دارد. این همکاری‌ها می‌توانند شامل تبادل اطلاعات، استرداد مجرمان و همکاری در جمع‌آوری ادله دیجیتال باشند. در این راستا، معاهدات بین‌المللی مانند کنوانسیون بوداپست در زمینه جرائم سایبری، چارچوب‌های قانونی لازم برای این نوع همکاری‌ها را فراهم کرده‌اند، اما پیگیری این امر در عمل ممکن است با مشکلات اجرائی مواجه شود (رحیمی‌نژاد، ۱۳۸۹: ۳۳).

چهارمین چالش، خطر سوءاستفاده از اصل حمایتی برای اهداف سیاسی است. استفاده از صلاحیت حمایتی باید با دقت و بر اساس معیارهای شفاف انجام شود، زیرا این اصل می‌تواند به ابزاری برای اعمال فشار سیاسی بر دیگر کشورها تبدیل شود. به‌ویژه در جرائم سایبری که ممکن است حاوی اطلاعات حساس یا مرتبط با فعالیت‌های تجاری و سیاسی باشند، امکان دارد برخی کشورها از این اصل برای پیگرد مخالفان سیاسی یا اهداف اقتصادی خود استفاده کنند. به‌طور خاص، ممکن است دولت‌ها از حملات سایبری به‌عنوان بهانه‌ای برای نقض حقوق بشر یا سرکوب آزادی‌های سیاسی استفاده کنند (موسوی، ۱۳۹۰: ۸۳).

پیشنهادها برای رفع چالش‌ها شامل ایجاد چارچوب‌های دقیق و شفاف برای تعریف جرائم **«تهدیدکننده امنیت ملی»** است تا اطمینان حاصل شود که تنها حملات سایبری با تأثیرات عمده و واقعی بر امنیت کشور تحت صلاحیت حمایتی قرار گیرند. علاوه‌بر این، تقویت همکاری‌های بین‌المللی در پیگرد جرائم سایبری، به‌ویژه از طریق شبکه‌های همکاری قضائی و پلیسی، می‌تواند به جلوگیری از تضاد صلاحیت‌ها و تسهیل فرآیندهای پیگرد کمک کند. همچنین، لازم است که حقوق بشر و آزادی‌های فردی در فرآیندهای پیگرد جرائم سایبری رعایت شود تا از سوءاستفاده‌های احتمالی جلوگیری گردد (تقی‌زاده انصاری، ۱۳۸۸: ۶۹).

در نهایت، اصل حمایتی به دولت‌ها این امکان را می‌دهد که نسبت به جرائمی که تهدید جدی برای امنیت ملی یا منافع اساسی آن‌ها هستند، حتی اگر این جرائم در خارج از مرزهای آن‌ها ارتکاب یابند، صلاحیت خود را اعمال کنند. این اصل به‌ویژه در جرائم سایبری که اثرات فرا مرزی دارند، بسیار کاربردی است، اما باید با دقت و مطابق با اصول حقوق بشر و قوانین بین‌المللی مورد استفاده قرار گیرد تا از تضادها و سوءاستفاده‌های سیاسی جلوگیری شود.

۲-۱-۵- اصل صلاحیت جهانی

اصل صلاحیت جهانی یکی از اصول مهم در حقوق بین‌الملل کیفری است که به دولت‌ها اجازه می‌دهد نسبت به جرائم خاص و بسیار شدید، مانند نسل‌کشی، جنایت علیه بشریت و جنایت جنگی، حتی اگر این جرائم در خارج از مرزهای سرزمینی آن‌ها ارتکاب یابند، صلاحیت قضائی خود را اعمال کنند. این اصل به‌ویژه در مورد جرائم بین‌المللی که تهدیدی جدی برای صلح و امنیت جهانی محسوب می‌شوند، پذیرفته شده است. طبق این اصل، برخی جرائم به‌دلیل شدت و گستردگی آثارشان به‌گونه‌ای شناسایی شده‌اند که جامعه بین‌المللی بر اساس صلح عمومی و عدالت جهانی می‌تواند به آن‌ها رسیدگی کند، حتی اگر مرتکب یا قربانی جرم هیچ ارتباطی با کشوری که صلاحیت آن را اعمال می‌کند نداشته باشند (رحیمی‌نژاد، ۱۳۸۹: ۳۹؛ کدخدایی و ساعد، ۱۳۹۰: ۸۹).

اولین چالش، تعریف دقیق جرائم مشمول صلاحیت جهانی در فضای سایبر است. در مورد جرائم بین‌المللی سنتی، مانند نسل‌کشی یا جنایت علیه بشریت، شواهد و استانداردهای قانونی به‌وضوح تعریف شده‌اند؛ اما در فضای سایبر، تعیین اینکه کدام جرائم به‌طور خاص به درجه‌ای از شدت و تأثیر می‌رسند که نیاز به اعمال صلاحیت جهانی داشته باشند، ممکن است پیچیده باشد. به‌ویژه، جرائم سایبری سازمان‌یافته یا تروریستی که ممکن است به زیرساخت‌های حیاتی کشورها آسیب بزنند یا امنیت جهانی را تهدید کنند، برای اعمال صلاحیت جهانی نیازمند معیارهای دقیق و قابل اندازه‌گیری هستند. به همین دلیل، بسیاری از نویسندگان و متخصصان حقوق بین‌الملل، امکان گنجاندن جرائم سایبری در دامنه صلاحیت جهانی را مطرح کرده‌اند، اما هنوز این امکان به‌طور عمومی در قوانین بین‌المللی پذیرفته نشده است (زیبر، ۱۳۹۰: ۸۰؛ ساعد، ۱۳۸۹: ۵۶).

دومین چالش، همکاری‌های بین‌المللی و اختلاف در تعریف جرائم سایبری است. حتی اگر برخی کشورها پذیرای صلاحیت جهانی در پیگرد جرائم سایبری تروریستی یا سازمان‌یافته باشند، هنوز تفاوت‌های زیادی در تعریف جرائم سایبری و چگونگی اجرای این صلاحیت در قوانین داخلی کشورها وجود دارد. به‌ویژه در جرائم سایبری که اثرات فرا مرزی دارند، مانند حملات باج‌افزاری یا حملات به زیرساخت‌های حیاتی که ممکن است امنیت ملی کشورهای مختلف را تهدید کنند، دولت‌ها باید همکاری‌های مؤثر و هماهنگ را ایجاد کنند تا به نتیجه‌گیری مشترک دست یابند. بدون چنین همکاری‌هایی، اعمال صلاحیت جهانی در این حوزه به‌ویژه در مورد جرائم سایبری سازمان‌یافته یا تروریستی، دشوار خواهد بود (اردبیلی، ۱۳۸۱: ۴۰؛ ساعد، ۱۳۸۹: ۴۶).

سومین چالش، نگرانی از سوءاستفاده سیاسی از صلاحیت جهانی است. یکی از نگرانی‌های اصلی در مورد صلاحیت جهانی در پیگرد جرائم سایبری، این است که برخی دولت‌ها ممکن است از این صلاحیت به‌طور سیاسی یا ابزاری برای فشار به کشورهای دیگر یا مجازات افرادی که در نظر آن‌ها مخالف سیاسی هستند، استفاده کنند. به‌ویژه در جرائم سایبری که ممکن است شامل مسائل مرتبط با امنیت ملی، جاسوسی یا رقابت‌های سیاسی باشند، نگرانی‌هایی وجود دارد که این ابزار برای سرکوب مخالفان سیاسی یا هدف قرار دادن افراد به دلیل اظهارات یا فعالیت‌های آنلاین آن‌ها به کار رود (سلامتی، ۱۳۸۷: ۴۳؛ موسوی، ۱۳۹۰: ۸۹).

چهارمین چالش، مسائل حقوق بشر در پیگرد جهانی جرائم سایبری است. استفاده از صلاحیت جهانی باید با رعایت اصول حقوق بشر و حقوق فردی صورت گیرد. این اصل ممکن است موجب نقض حریم خصوصی افراد یا آزادی بیان شود، به‌ویژه زمانی که جرائم سایبری به‌طور خاص شامل محتواهای سیاسی، اجتماعی یا اقتصادی باشند. برای مثال، در پیگرد جرائم سایبری که به تضعیف حکومت‌ها یا تهدید امنیت سیاسی مربوط می‌شوند، باید دقت کرد که از این صلاحیت برای سرکوب آزادی‌های فردی یا محدود کردن حق آزادی بیان استفاده نشود (کدخدایی و ساعد، ۱۳۹۰: ۹۲).

پیشنهادهایی برای رفع این چالش‌ها شامل ایجاد معاهده‌ها و چارچوب‌های قانونی بین‌المللی است که تعریف دقیق و مشخصی از جرائم سایبری که مشمول صلاحیت جهانی می‌شوند، ارائه دهند. این معاهدات باید به‌گونه‌ای طراحی شوند که تضمین کنند از صلاحیت جهانی برای پیگرد جرائم سایبری تنها در مواردی استفاده می‌شود که این جرائم واقعا تهدیدی برای صلح و امنیت جهانی باشند و از سوءاستفاده‌های سیاسی جلوگیری شود. همچنین، توسعه همکاری‌های بین‌المللی و فرآیندهای شفاف برای پیگرد جهانی جرائم سایبری ضروری است تا اطمینان حاصل شود که این فرآیند با رعایت اصول حقوق بشر و حاکمیت کشورها انجام می‌شود (سلامتی، ۱۳۸۷: ۵۳).

در نهایت، صلاحیت جهانی در مورد برخی جرائم سایبری، به‌ویژه جرائم سایبری سازمان‌یافته یا تروریستی، به‌عنوان ابزاری برای تأمین امنیت و عدالت بین‌المللی مطرح است. با این حال، برای اعمال مؤثر و عادلانه این صلاحیت، نیاز به توافق‌های بین‌المللی، تعریف دقیق جرائم و مکانیزم‌های همکاری بین کشورها وجود دارد تا از سوءاستفاده‌ها و نقض حقوق بشر جلوگیری شود (اردبیلی، ۱۳۸۱: ۴۷؛ نمامیان، ۱۳۹۰:

۳۲). در فضای سایبری، اصل سرزمینی با چالش جدی مواجه است؛ زیرا تعیین محل وقوع "رفتار" و "نتیجه" دشوار است: آیا محل کلیک مرتکب، محل قرار گرفتن سرور هدف، محل قرار گرفتن بزه‌دیده یا محل وقوع ضرر، قلمرو مرتبط به شمار می‌آید؟ بسیاری از کشورها با توسعه مفهوم "اثر"، هرگونه نتیجه قابل توجه در قلمرو خود را برای اعمال صلاحیت کافی دانسته‌اند؛ اما این رویکرد، در صورت فقدان هماهنگی، می‌تواند به تکثر و تداخل صلاحیت‌ها بینجامد.

۲-۲- تعارض صلاحیت‌ها و راه‌حل‌های پیشنهادی

در جرائم سایبری فرا مرزی، معمولا چندین دولت به‌طور هم‌زمان خود را صالح می‌دانند؛ مثال ساده آن، حمله باج‌افزاری است که از کشور "الف" طراحی شده، سرورهای کنترل آن در کشور "ب" قرار دارد، قربانیان در کشورهای "ج" و "د" هستند و پول‌شویی حاصل از آن در کشور "هـ" صورت می‌گیرد. در این فرض، دست‌کم پنج دولت می‌توانند بر یکی از اصول صلاحیت تکیه کنند.

راه‌حل‌های مطرح‌شده در ادبیات و اسناد بین‌المللی عبارت‌اند از: توافقات دو یا چندجانبه درباره تعیین **«اصل نزدیک‌ترین ارتباط»** و ترجیح صلاحیت کشوری که بیشترین ارتباط واقعی را با جرم دارد؛ پرونده‌محوری و تعیین مرجع تعقیب اصلی از طریق گفت‌وگو میان مقامات دادستانی و پلیسی؛ تأکید بر اصل Ne Bis In Idem (منع محاکمه و مجازات مجدد) در سطح دو یا چندجانبه، به‌ویژه در اتحادیه اروپا و در اسناد مبتنی بر کنوانسیون بوداپست تا از تعقیب‌های موازی و متعارض جلوگیری شود (رحیمی‌نژاد، ۱۳۸۹: ۵۲).

با این حال، نبود یک قاعده واحد جهانی، همچنان موجب ناهمگونی رویه‌ها و گاه رقابت کیفری میان دولت‌ها می‌شود؛ پدیده‌ای که می‌تواند هم به Forum Shopping از سوی متهمان منجر شود و هم به استفاده ابزاری از پیگرد کیفری برای اهداف سیاسی.

۲-۳- صلاحیت کیفری در اسناد بین‌المللی: نمونه کنوانسیون بوداپست و کنوانسیون ملل متحد

کنوانسیون بوداپست درباره جرائم سایبری (۲۰۰۱) نخستین و تا مدت‌ها مهم‌ترین معاهده چندجانبه الزام‌آور در حوزه جرائم سایبری است. این کنوانسیون سه هدف اصلی دارد: هماهنگ‌سازی قوانین کیفری کشورها در خصوص جرائم سایبری، پیش‌بینی ابزارهای ویژه تحقیقاتی برای ادله الکترونیکی و ایجاد رژیم همکاری بین‌المللی کارآمد. در زمینه صلاحیت کیفری، کنوانسیون بوداپست از کشورهای عضو می‌خواهد دست‌کم صلاحیت سرزمینی و صلاحیت مبتنی بر تابعیت مرتکب را نسبت به جرائم مقرر در کنوانسیون برقرار کنند و در عین حال، امکان پیش‌بینی صلاحیت‌های تکمیلی، مانند تابعیت بزه‌دیده را نیز باز می‌گذارد. این کنوانسیون با پذیرش امکان **«صلاحیت‌های متعدد»**، کشورهای عضو را تشویق می‌کند که از طریق مشورت، در مورد مناسب‌ترین محل تعقیب توافق کنند (جلالی‌فراهانی، ۱۳۹۳: ۲۷؛ کدخدایی و ساعد، ۱۳۹۰: ۹۶).

در کنار آن، کنوانسیون جدید ملل متحد علیه جرائم سایبری که متن آن در سال ۲۰۲۴ توسط کمیته ویژه سازمان ملل توافق و در سال ۲۰۲۵ برای امضا در هانوی گشوده شده است، درصدد ایجاد یک چارچوب جهانی‌تر برای مقابله با استفاده مجرمانه از فناوری‌های اطلاعات و ارتباطات است. این کنوانسیون طیفی از جرائم مبتنی بر ICT را جرم‌انگاری کرده و بر تقویت همکاری بین‌المللی در جمع‌آوری و تبادل ادله الکترونیکی تأکید می‌کند؛ هرچند، انتقادهایی نیز از حیث گستره جرائم مشمول، ابهام برخی مفاهیم و خطرهای بالقوه برای حقوق بشر مطرح شده است.

۳- سازوکارهای همکاری قضایی و پلیسی در پیگرد کیفری جرائم سایبری

ماهیت بین‌المللی بسیاری از جرائم سایبری باعث می‌شود که پیگرد مؤثر بدون همکاری سریع و مؤثر میان دولت‌ها و حتی بازیگران خصوصی ممکن نباشد. سه حوزهٔ اصلی همکاری

[1]- Case-By-Case

عبارت‌اند از استرداد مجرمان، معاضدت قضایی متقابل در جمع‌آوری ادله و شبکه‌های تخصصی همکاری فوری.

۳-۱- استرداد مجرمان سایبری و چالش‌های آن

استرداد یکی از مهم‌ترین ابزارهای پیگرد کیفری فرا مرزی است، اما در حوزهٔ سایبر با چند مانع جدی مواجه است:

۳-۱-۱- اصل جرم‌انگاری دوگانه

بسیاری از معاهدات استرداد، شرط می‌گذارند که رفتار مورد درخواست، در هر دو کشور جرم باشد. در جرائم سایبری جدید، ممکن است یک عمل در کشور درخواست‌کننده جرم‌انگاری شده باشد ولی در کشور طرف دیگر هنوز مقرره روشنی نداشته باشد (رحیمی‌نژاد، ۱۳۸۹: ۵۶).

۳-۱-۲- استثنای جرائم سیاسی

اگر رفتار به‌گونه‌ای تفسیر شود که جنبه سیاسی دارد (مثلا هک کردن پایگاه‌های دولتی در چارچوب اعتراض سیاسی)، برخی نظام‌ها می‌توانند استرداد را رد کنند (زیبر، ۱۳۹۰: ۸۰).

۳-۱-۳- منع استرداد اتباع

بسیاری از کشورها اتباع خود را مسترد نمی‌کنند؛ در این حالت، انتقال تعقیب یا اجرای حکم کیفری باید جایگزین شود که خود مستلزم توافق‌های خاص است (نمامیان، ۱۳۹۰: ۴۳).

۳-۱-۴- نگرانی از نقض حقوق بشر در کشور درخواست‌کننده

درصورتی‌که بیم شکنجه، محاکمه ناعادلانه یا مجازات‌های غیرانسانی (مانند اعدام در جرائم اقتصادی) وجود داشته باشد، دادگاه‌های کشور طرف دیگر ممکن است استرداد را مغایر تعهدات حقوق بشری بین‌المللی بدانند (روزنهان و سلیگمن، ۱۳۸۹: ۴۵). کنوانسیون بوداپست، جرائم مشمول خود را برای مقاصد استرداد «جرائم قابل استرداد» تلقی می‌کند، مشروط بر آن‌که حداکثر مجازات آنها حداقلی را (مثلا یک سال حبس یا بیشتر) داشته باشد؛ با این حال، تصمیم نهایی همچنان به معاهدات دوجانبه و قانون داخلی دولت‌ها وابسته است (اردبیلی، ۱۳۸۱: ۵۴).

۳-۲- معاضدت قضایی متقابل و ادله الکترونیکی

معاضدت قضایی متقابل (MLA) در جرائم سایبری، بیش از هر چیز به دسترسی به ادله الکترونیکی مربوط است. مهم‌ترین سازوکارهایی که در اسناد بین‌المللی برای این منظور پیش‌بینی شده‌اند عبارت‌اند از:

۳-۲-۱- حفظ فوری داده‌ها [1]

مقامات یک دولت می‌توانند از دولت دیگر بخواهند داده‌های مرتبط با جرم را فورا و برای مدت معین حفظ کند تا فرصت انجام تشریفات بعدی (مانند دستور تفتیش یا تولید داده) فراهم شود. این نهاد به‌ویژه برای داده‌های ترافیکی و Log ها اهمیت دارد.

۳-۲-۲- دستور تولید داده [2]

مقامات قضایی می‌توانند به ارائه‌دهندگان خدمات در کشور دیگر دستور دهند داده‌های مشخصی را در اختیارشان بگذارند (باستانی، ۱۳۹۰: ۷۵).

۳-۲-۳- تفتیش و ضبط داده‌ها

در مواردی، دسترسی به داده‌ها مستلزم تفتیش فیزیکی تجهیزات یا سرورها در قلمرو دولت طرف درخواست است که نیازمند تصمیم قضایی و رعایت تشریفات آیین دادرسی آن کشور است (روزنهان و سلیگمن، ۱۳۸۹: ۵۷).

۳-۲-۴- جمع‌آوری بلادرنگ داده‌های ترافیکی و شنود محتوایی

برای برخی جرائم جدی، امکان جمع‌آوری بلادرنگ داده‌های ترافیکی یا حتی محتوایی به‌صورت برخط پیش‌بینی شده است؛ این اقدامات، از حیث حقوق بشر و حریم خصوصی بسیار حساس‌اند و باید با ضوابط سخت‌گیرانه همراه باشند. مشکل اساسی در MLA، کندی و پیچیدگی فرایندهای اداری و دیپلماتیک است؛ درحالی‌که ادله سایبری زودگذر است و تأخیر، عملا پیگرد را عقیم می‌کند. برای رفع این مشکل، کنوانسیون بوداپست و پروتکل دوم الحاقی آن (۲۰۲۲) سازوکارهایی مانند درخواست‌های مستقیم سریع به ارائه‌دهندگان خدمات و تقویت

[1]- Expedited Preservation
[2]- Production Order

شبکه نقاط تماس ۷/۲۴ را پیش‌بینی کرده‌اند تا با حداقل تشریفات، راه برای حفظ و تحصیل ادله الکترونیکی باز شود (جلالی‌فراهانی، ۱۳۹۳: ۳۹).

۳-۳- شبکه‌های تخصصی همکاری فوری

در کنار مکانیسم‌های رسمی معاهده‌ای، شبکه‌های پلیسی و قضایی تخصصی، نقش مهمی در پیگرد جرائم سایبری دارند، از جمله:

۳-۳-۱- شبکه ۷/۲۴ کنوانسیون بوداپست

هر کشور عضو موظف است یک «نقطه تماس» دائم تعیین کند که در تمام ساعات شبانه‌روز برای درخواست‌های فوری حفظ داده‌ها و تبادل اطلاعات اولیه در دسترس باشد (جلالی‌فراهانی، ۱۳۹۳: ۳۹).

۳-۳-۲- اینترپل و یوروپل

این سازمان‌ها پایگاه‌های داده و کانال‌های ارتباطی امن برای تبادل سریع اطلاعات عملیاتی در مورد حملات سایبری گسترده، باج‌افزارها و شبکه‌های مجرمانه سازمان‌یافته فراهم کرده‌اند (تقی‌زاده انصاری، ۱۳۸۸: ۳۴).

۳-۳-۳- شبکه‌های منطقه‌ای و ابتکارات گروه‌های کوچک (مانند گروه جی ۷)

این سازوکارها امکان هماهنگی سریع در واکنش به حوادث سایبری بزرگ را فراهم می‌کنند و گاه نقش "آزمایشگاه سیاستی" را برای توسعه استانداردهای جدید بازی می‌کنند. این شبکه‌ها اگرچه جایگزین معاضدت قضایی رسمی نیستند، اما در عمل بخش زیادی از نیاز به اطلاعات ابتدایی و حفظ فوری داده‌ها را تأمین می‌کنند و پلی میان پلیس و دادستانی کشورها ایجاد می‌نمایند (کالریک و یانچوسکی، ۱۳۸۹: ۱۲۰).

۴- چالش‌های نوپدید و روندهای آینده در پیگرد کیفری جرائم سایبری

۴-۱- حاکمیت داده، قوانین حریم خصوصی و تأثیر بر پیگرد کیفری

در دهه اخیر، تصویب قوانین سخت‌گیرانه در حوزه حفاظت از داده‌های شخصی (مانند مقرره عمومی حفاظت از داده‌ها در اتحادیه اروپا) مفهوم **«حاکمیت داده»** را تقویت کرده است. این روند، از یک‌سو برای حفاظت از حریم خصوصی و کنترل افراد بر داده‌هایشان مثبت است، اما از سوی دیگر، می‌تواند دریافت و انتقال ادله الکترونیکی به خارج از کشور را دشوار سازد (کالریک و یانچوسکی، ۱۳۸۹: ۱۱۷).

شرکت‌های فراملی فناوری نیز با استناد به تعارض میان الزامات قوانین ملی محل استقرار خود و دستورات قضایی خارجی، گاه از همکاری در ارائه داده‌ها خودداری می‌کنند یا آن را به تأخیر می‌اندازند. این وضعیت، نیاز به چارچوب‌های شفاف‌تر برای دسترسی فرا مرزی به داده‌ها و توافق‌های مشخص میان دولت‌ها را برجسته کرده است (زیبر، ۱۳۹۰: ۹۵).

۴-۲- فناوری‌های نوظهور: رمزنگاری، خدمات ابری، اینترنت اشیاء

فناوری‌های نوین سه چالش عمده برای پیگرد کیفری ایجاد کرده‌اند:

۴-۲-۱- رمزنگاری سرتاسری [1]

این فناوری امکان شنود و دسترسی به محتوای پیام‌ها را حتی برای ارائه‌دهنده خدمت دشوار یا ناممکن می‌کند؛ بحث‌های تندی درباره الزام شرکت‌ها به ایجاد **«درهای پشتی»**[2] در جریان است و تعارض میان امنیت سایبری، حریم خصوصی و نیازهای پیگرد کیفری همچنان حل‌نشده باقی مانده است (رحیمی‌نژاد، ۱۳۸۹: ۵۴).

۴-۲-۲- خدمات ابری و توزیع جغرافیایی داده‌ها

داده‌های مرتبط با یک پرونده ممکن است در لحظه‌ای در یک کشور و چند دقیقه بعد در مرکز داده کشور دیگر ذخیره شود؛ این امر صلاحیت قضایی و امکان اعمال دستورهای ملی را پیچیده می‌کند (کالریک و یانچوسکی، ۱۳۸۹: ۹۳).

۴-۲-۳- اینترنت اشیاء [3]

[1]- End-To-End
[2]- Backdoor
[3]- Internet of Things (IOT)

گسترش دستگاه‌های متصل (از خودرو و تجهیزات پزشکی تا امکانات شهری) نه‌تنها سطح حملات را افزایش داده، بلکه منابع جدیدی از ادله الکترونیکی ایجاد کرده است که دسترسی به آن‌ها مستلزم تنظیم قواعد خاص است (ناصری، ۱۳۸۷: ۲۸).

۴-۳- تنش میان امنیت و حقوق بشر در کنوانسیون جدید سازمان ملل

کنوانسیون جدید ملل متحد علیه جرائم سایبری، هرچند هدف اعلامی‌اش تقویت مبارزه جهانی علیه جرائم سایبری است، اما از دید بسیاری از نهادهای مدنی و شرکت‌های فناوری، خطر تبدیل شدن به ابزاری برای نظارت گسترده و سرکوب مخالفان سیاسی را در بردارد؛ به‌ویژه آنجا که دایره جرائم مشمول، فراتر از جرائم سایبری "خالص" به برخی جرائم مبتنی بر محتوا (مانند نفرت‌پراکنی یا برخی اشکال بیان آنلاین) گسترش می‌یابد (روزنهان و سلیگمن، ۱۳۸۹: ج۱، ۶۲).

این نگرانی وجود دارد که برخی دولت‌ها، تحت پوشش مبارزه با جرائم سایبری، به محدودسازی آزادی بیان و جرم‌انگاری گسترده رفتارهای سیاسی یا انتقادی در فضای مجازی بپردازند. چالش اصلی جامعه بین‌المللی آن است که میان نیاز مشروع به امنیت سایبری و ضرورت رعایت حقوق بنیادین بشر، تعادل معقولی برقرار کند (پوربافرانی، ۱۳۹۶: ۴۳؛ هاشمی، ۱۳۹۰: ۶۸).

۴-۴- الزامات سیاست‌گذاری برای کشورها (با تأکید بر کشورهای در حال توسعه)

برای کشورهایی که هنوز در حال شکل‌دهی به نظام حقوقی خود در حوزه جرائم سایبری هستند، چند توصیه کلان قابل طرح است:

۴-۴-۱- هماهنگ‌سازی قانون داخلی با استانداردهای بین‌المللی

جرم‌انگاری رفتارهایی مانند دسترسی غیرمجاز، مداخله در داده و سامانه، کلاهبرداری رایانه‌ای و سوءاستفاده از ابزارها، متناسب با الگوی کنوانسیون بوداپست و اسناد جدید ملل متحد، موجب تسهیل همکاری بین‌المللی می‌شود (اردبیلی، ۱۳۸۱: ۵۶؛ هاشمی، ۱۳۹۰: ۵۸).

۴-۴-۲- پیوستن فعالانه به معاهدات و شبکه‌های همکاری

الحاق به کنوانسیون‌های اصلی، مشارکت در شبکه‌های ۷/۲۴ و تقویت پایگاه‌های تماس ملی، شرط لازم برای دسترسی مؤثر به ادله الکترونیکی خارج از کشور و جلب همکاری سایر دولت‌هاست (جلالی‌فراهانی، ۱۳۹۳: ۵۶).

۴-۴-۳- تضمین حقوق بشر در قانون داخلی

پیش‌بینی نظارت قضایی، معیارهای روشن برای استفاده از ابزارهای تهاجمی تحقیق، سازوکار جبران خسارت در صورت نقض حقوق و شفافیت رویه‌ها، اعتماد عمومی به نظام پیگرد کیفری را تقویت می‌کند (هاشمی، ۱۳۹۰: ۷۴).

۴-۴-۴- ظرفیت‌سازی نهادی و فنی

ایجاد واحدهای تخصصی پلیسی و قضایی، آموزش مستمر قضات، دادستان‌ها و ضابطان در حوزهٔ ادله دیجیتال و سرمایه‌گذاری در زیرساخت‌های فنی، پیش‌شرط هرگونه موفقیت در پیگرد جرائم سایبری فرا مرزی است (تقی‌زاده انصاری، ۱۳۸۸: ۴۶).

نتیجه‌گیری

جرائم سایبری با ماهیت بین‌المللی، به‌دلیل فرا مرزی بودن، ناشناسی مرتکبان و وابستگی شدید به داده‌ها و زیرساخت‌های پراکنده، یکی از دشوارترین حوزه‌های پیگرد کیفری را رقم زده‌اند. بررسی انجام‌شده در این مقاله نشان داد که چارچوب‌های سنتی صلاحیت کیفری به‌تنهایی پاسخ‌گوی پیچیدگی‌های فضای سایبر نیستند و نیازمند تفسیر و تکمیل بر مبنای معیارهایی مانند **«نزدیک‌ترین ارتباط»** و **«هماهنگی بین‌المللی»** هستند. کنوانسیون بوداپست و پروتکل‌های الحاقی آن تاکنون کارآمدترین رژیم چندجانبه برای جرم‌انگاری، ابزارهای تحقیق و همکاری بین‌المللی در حوزه سایبر بوده‌اند و تجربه موفق شبکه ۷/۲۴ نشان می‌دهد که بدون سازوکارهای سریع و تخصصی، ادله سایبری از دست می‌رود. کنوانسیون جدید ملل متحد علیه جرائم سایبری فرصتی برای ایجاد چارچوبی جهانی‌تر فراهم کرده است، اما دامنه گسترده

برخی جرائم مشمول و ابهاماتی در خصوص تضمین‌های حقوق بشری، خطر سوءاستفاده از ابزارهای پیگرد و نظارت را گوشزد می‌کند و نیازمند تفسیر و اجرای محتاطانه است. استرداد و معاضدت قضایی متقابل همچنان با موانعی چون جرم‌انگاری دوگانه، استثنای جرائم سیاسی، منع استرداد اتباع و نگرانی‌های حقوق بشری روبه‌روست و رفع این موانع مستلزم اصلاح معاهدات دوجانبه، استانداردسازی رویه‌ها و ارتقای اعتماد متقابل بین دولت‌هاست. فناوری‌های نوین (رمزنگاری، خدمات ابری، اینترنت اشیاء) هم‌زمان که فرصت‌های جدیدی برای توسعه و امنیت ایجاد کرده‌اند، پیگرد کیفری را با معمایی دوگانه میان **«حفظ امنیت و حریم خصوصی»** قرار داده‌اند.

بر این اساس، پیشنهادهای کاربردی مقاله را می‌توان به‌طور خلاصه چنین برشمرد:

الف) در سطح بین‌المللی. تقویت هم‌گرایی میان رژیم کنوانسیون بوداپست و کنوانسیون جدید ملل متحد، به‌گونه‌ای که دولت‌ها ناگزیر به انتخاب میان دو الگوی متعارض نباشند؛ تدوین دستورالعمل‌های تفسیری مشترک برای تضمین رعایت حقوق بشر در اجرای ابزارهای تهاجمی تحقیق و همکاری بین‌المللی؛ توسعه سازوکارهای حل‌وفصل اختلاف در تعارض صلاحیت‌ها و رقابت کیفری میان دولت‌ها.

ب) در سطح ملی. اصلاح و به‌روزرسانی قوانین جرائم رایانه‌ای و آیین دادرسی کیفری با الهام از تجربه بین‌المللی، به‌ویژه در حوزه حفظ فوری داده‌ها، دسترسی به ادله الکترونیکی و شنود قانونی با نظارت قضایی؛ پیش‌بینی صلاحیت‌های تکمیلی در قانون داخلی (مانند صلاحیت مبتنی بر تابعیت بزه‌دیده و حمایت از زیرساخت‌های حیاتی) همراه با تضمین‌های کافی برای جلوگیری از سوءاستفاده؛ ایجاد واحدهای تخصصی در قوه قضائیه و ضابطان دادگستری برای مدیریت پرونده‌های سایبری فرا مرزی، همراه با برنامه‌های آموزش مستمر؛ طراحی سازوکارهای شفاف برای همکاری با بخش خصوصی (شرکت‌های فناوری، ارائه‌دهندگان خدمات ابری و پلتفرم‌ها) و تعیین تکالیف و مسؤولیت‌های آن‌ها در حفظ و ارائه امن داده‌ها.

در نهایت، می‌توان گفت پیگرد کیفری جرائم سایبری با ماهیت بین‌المللی تنها زمانی می‌تواند مؤثر، مشروع و پایدار باشد که سه سطح **«هماهنگ‌سازی قوانین»**، **«تقویت همکاری‌های سریع و تخصصی»** و **«حفظ حقوق بنیادین بشر»** به‌طور هم‌زمان مورد توجه قرار گیرد. نهادهای ملی و بین‌المللی اگر این سه رکن را به‌صورت متوازن تقویت کنند، می‌توانند در برابر موج فزاینده جرائم سایبری، دفاعی کارآمد و در عین حال حقوق‌مدار فراهم آورند.

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 توسط نویسندهٔ مسؤول انجام شده است.

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

منابع و مآخذ

– اردبیلی، محمدعلی (۱۳۸۱). *مفهوم تروریسم*. گزیده مقالات همایش تروریسم از دیدگاه اسلام و حقوق بین‌الملل، تهران: مرکز مطالعات توسعه قضایی و دانشکده علوم قضایی و خدمات اداری.

– باستانی، برومند (۱۳۹۰). *جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری*. تهران: انتشارات بهنامی.

– پوربافرانی، حسن (۱۳۹۶). *حقوق جزای بین‌الملل*. تهران: انتشارات جنگل.

– تقی‌زاده انصاری، مصطفی (۱۳۸۸). *سازمان جهانی پلیس جهانی اینترپل*. تهران: انتشارات جنگل.

– جلالی فراهانی، امیرحسین (۱۳۸۴). *پیشگیری از جرائم رایانه‌ای*. به راهنمایی علی‌حسین نجفی‌ابرندآبادی، تهران: دانشگاه امام صادق (ع).

– جلالی‌فراهانی، امیرحسین (۱۳۹۳). *کنوانسیون جرائم سایبر و پروتکل الحاقی آن (به همراه گزارش‌های توجیهی آن‌ها)*. تهران: خرسندی.

– جلالی‌فراهانی، امیرحسین و باقری‌اصل، رضا (۱۳۸۷). «پیشگیری اجتماعی از جرائم سایبری، راهکاری اصلی برای نهادینه‌سازی اخلاق سایبری»، ف*صلنامه اطلاع‌رسانی و کتابداری ره‌آورد نور*، (۲۴): ۱۰.

– حسن‌بیگی، ابراهیم (۱۳۸۴). *حقوق و امنیت در فضای سایبر*. تهران: مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر.

– حسینی‌خواه، نورالله (۱۳۹۰). *پلیس و جرائم رایانه‌ای*. تهران: انتشارات معاونت تربیت و آموزش ناجا.

– خداقلی، زهرا (۱۳۸۳). *جرائم کامپیوتری*. تهران: انتشارات آریان.

– رحیمی‌نژاد، اسمعیل (۱۳۸۹). *جرم‌شناسی*. تبریز: فروزش.

– روزنهان، دیوید.ال و سلیگمن، مارتین. ای بی (۱۳۸۹). *روان‌شناسی نابهنجاری (آسیب‌شناسی روانی)*. ترجمه: یحیی سیدمحمدی، تهران: ساوالان.

– زندی، محمدرضا (۱۳۸۹). *تحقیقات مقدماتی در جرائم سایبری*. تهران: انتشارات جنگل.

– زیبر، اولریش (۱۳۹۰). *جرائم رایانه‌ای*. ترجمه: محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند و احمد رحیمی مقدم، تهران: گنج دانش.

– ساعد، نادر (۱۳۸۹). *منابع حقوق مبارزه با تروریسم در ایران*. بی‌جا: خرسندی.

– سلامتی، یعقوب (۱۳۸۷). *تروریسم و حقوق بین‌الملل*. هشترود: دانشگاه آزاد اسلامی.

– شیرزاد، کامران (۱۳۸۸). جرائم *رایانه‌ای از منظر حقوق جزای ایران و حقوق بین‌الملل*. تهران: بهینه فراگیر.

– صنوبر، ناصر (۱۳۹۳). *اقتصاد تروریسم*. تهران: بورس.

– عالی‌پور، حسن (۱۳۹۰). *حقوق کیفری فناوری اطلاعات*. تهران: خرسندی.

– فامیلی‌زوار جلالی، امیر (۱۳۹۴). *مسؤولیت بین‌المللی دولت‌ها ناشی از تأمین مالی دهشت‌افکنی با تأکید بر گروه دهشت‌افکن داعش*. به راهنمایی حمید الهویی نظری، تهران: دانشگاه تهران.

– فهیمی، مهدی (۱۳۸۰). «جرائم رایانه‌ای و روش‌های مقابله و پیشگیری از آن». *فصلنامه دیدگاه‌های حقوقی*، دانشکده علوم قضائی و خدمات اداری، شماره ۲۳ و ۲۴.

– کالریک، اندرو. ام و یانچوسکی، لخ (۱۳۸۹). *مقدمه‌ای بر جنگ سایبر و تروریسم سایبر*. ترجمه ابراهیم‌نژاد شلمانی، تهران: بوستان حمید.

– کدخدایی، عباسعلی و ساعد، نادر (۱۳۹۰). *تروریسم و مقابله با آن*. بی‌جا: مجمع جهانی صلح جهانی.

– موسوی، سیدرضا (۱۳۹۰). *پیشگیری وضعی از جرائم سایبری در قالب تدابیر فنی و محدودیت‌های پیش روی آن*. همایش منطقه‌ای چالش‌های جرائم رایانه‌ای در عصر امروز، انجمن‌های علمی، ادبی و هنری، مراغه: دانشگاه آزاد اسلامی.

– ناصری، علی‌اکبر (۱۳۸۷). *هندبوک مجموعه قوانین و مقررات فناوری اطلاعات و ارتباطات (ICT)*. تهران: خرسندی.

– نجفی‌ابرندآبادی، علی‌حسین (۱۳۸۳). *مباحثی در علوم جنایی؛ تقریرات درس جرم‌شناسی مقاطع دکتری و کارشناسی ارشد*. مجموعه دو جلدی به کوشش شهرام ابراهیمی، تهران: دانشگاه شهید بهشتی.

– نمامیان، پیمان (۱۳۹۰). *واکنش‌های عدالت کیفری به تروریسم*. تهران: میزان.

– هاشمی، سیدحسین (۱۳۹۰). *تروریسم از منظر حقوق اسلام و اسناد بین‌المللی*. قم: پژوهشگاه حوزه و دانشگاه.