Journal of
International Criminal Law
www.iclj.ir

Volume 2, Issue 4, 2024

Cyberspace and the Challenges to National Sovereignty from the Perspective of International Criminal Law and Digital Forensics: A Case Study of the Iraqi Legal System

Mohammed Zia Al-Mahnawi [1], Mahdi Rajaei [*2]

1. PhD Student in Public Law, Faculty of Law, University of Qom, Qom, Iran.
2. Assistant Professor, Department of Public Law, Faculty of Law, University of Qom, Qom, Iran. (Corresponding Author)

ARTICLE INFORMATION

Type of Article: ***Original Research***
Pages: ***133-147***

Corresponding Author's Info:
ORCID: *0009-0007-2091-8619*
TELL: *+980000000000*
Email: *m.rajaei@qom.ac.ir*

Article History:
Received: *00 Dec 2024*
Revised: *00 Dec 2024*
Accepted: *00 Dec 2024*
Published online: *20 Mar 2024*

Keywords:
Cyberspace, National Sovereignty, International Criminal Law, Cybercrime, Judicial Jurisdiction, Digital Evidence.

ABSTRACT

The expansion of cyberspace and the growing dependence of states, institutions, and individuals on digital infrastructure have challenged the traditional concept of national sovereignty, raising issues that can be examined, in significant part, within the framework of international criminal law. The transnational nature of cybercrime means that a criminal act can produce effects in several countries without the perpetrator being physically present in the territory of the affected state. Consequently, traditional principles of criminal jurisdiction face circumstances that were not anticipated when many existing laws were enacted. This study examines the extent to which existing legal frameworks are adequate to address these challenges. It classifies cyberattacks, digital espionage, and attacks against critical infrastructure and analyzes them from the perspectives of international criminal law and digital forensics. The research adopts a legal and comparative approach, drawing on digital forensics to explain the patterns of offending and the transnational characteristics of cybercrime. The findings indicate that although traditional rules of criminal jurisdiction remain an essential basis for regulating judicial relations between states, they are not fully adequate to address the complex and cross-border nature of cybercrime. The absence of a binding hierarchy among competing jurisdictional claims may also lead to jurisdictional conflicts and undermine the principle of sovereign equality among states. Under certain circumstances, attacks against critical infrastructure may extend beyond ordinary transnational crime and become matters of national sovereignty and security. Accordingly, the study highlights the need for coordinated frameworks governing jurisdiction, state responsibility, and the peaceful settlement of disputes. It proposes a multifactor approach based on a "genuine connection" and considerations of international comity. At the domestic level, within the Iraqi legal system, the adoption of a specialized cybercrime law and the strengthening of judicial and technical capabilities are essential requirements for effectively addressing this phenomenon.

This is an open access article under the CC BY license. © 2024 The Authors.

How to Cite This Article: Al-Mahnawi, M. Z & Rajaei, M (2024). "Cyberspace and the Challenges to National Sovereignty from the Perspective of International Criminal Law and Digital Forensics: A Case Study of the Iraqi Legal System". *Journal of International Criminal Law*, 2(4): 133-147.

فصلنامه حقوق جزای بین‌الملل

www.iclj.ir

دوره دوم، شماره چهارم، زمستان ۱۴۰۳

فضای سایبری و چالش‌های حاکمیت ملی از منظر حقوق کیفری بین‌المللی و جرم‌شناسی دیجیتال (مطالعه موردی نظام حقوقی عراق)

محمد ضیاء المحناوی [۱]، مهدی رجائی [۲*]

۱. دانشجوی دکتری، حقوق عمومی، دانشکده حقوق، دانشگاه قم، قم، ایران.

۲. استادیار، حقوق عمومی، دانشکده حقوق، دانشگاه قم، قم، ایران. (نویسنده مسؤول)

اطلاعات مقاله

نوع مقاله: پژوهشی

صفحات: ۱۴۷-۱۳۳

اطلاعات نویسنده مسؤول

کد ارکید: ۰۰۰۹-۰۰۰۷-۲۰۹۱-۸۶۱۹

تلفن: ۹۸۰۰۰۰۰۰۰۰۰+

ایمیل: m.rajaei@qom.ac.ir

سابقه مقاله:

تاریخ دریافت: ۱۴۰۳/۰۶/۱۰

تاریخ ویرایش: ۱۴۰۳/۰۸/۱۴

تاریخ پذیرش: ۱۴۰۳/۰۹/۰۱

تاریخ انتشار: ۱۴۰۳/۱۰/۰۱

واژگان کلیدی:

فضای سایبری، حاکمیت ملی، حقوق کیفری بین‌المللی، جرائم سایبری، صلاحیت قضایی، ادله دیجیتال.

چکیده

گسترش فضای سایبری و وابستگی فزاینده دولت‌ها، نهادها و افراد به زیرساخت‌های دیجیتال، مفهوم سنتی حاکمیت ملی را با چالش‌هایی مواجه ساخته است که بخش مهمی از آن‌ها در قلمرو حقوق کیفری بین‌المللی قابل بررسی است. ماهیت فرامرزی جرائم سایبری موجب شده است که ارتکاب یک رفتار مجرمانه، بدون حضور فیزیکی مرتکب در قلمرو دولت زیان‌دیده، آثار خود را در چندین کشور آشکار سازد و در نتیجه، مبانی سنتی صلاحیت کیفری با وضعیت‌هایی مواجه شوند که در زمان شکل‌گیری بسیاری از قوانین موجود پیش‌بینی نشده بودند. پژوهش حاضر با هدف بررسی میزان کفایت چارچوب‌های حقوقی موجود در مواجهه با این وضعیت، به طبقه‌بندی حملات سایبری، جاسوسی دیجیتال و حملات علیه زیرساخت‌های حیاتی می‌پردازد و آنها را از منظر حقوق کیفری بین‌المللی و جرم‌شناسی دیجیتال تحلیل می‌کند. روش پژوهش مبتنی بر تحلیل حقوقی و تطبیقی است و از جرم‌شناسی دیجیتال برای تبیین الگوهای ارتکاب و ویژگی‌های فرامرزی جرائم سایبری بهره می‌گیرد. یافته‌ها نشان می‌دهد که قواعد سنتی صلاحیت کیفری، اگرچه همچنان مبنای ضروری تنظیم روابط قضایی میان دولت‌ها هستند؛ اما در برابر ماهیت چندلایه و فرامرزی جرائم سایبری کفایت کامل ندارند. نبود سلسله‌مراتب الزام‌آور میان صلاحیت‌های رقیب نیز می‌تواند به تعارض صلاحیت‌ها و تضعیف اصل برابری حاکمیتی دولت‌ها منجر شود. حملات علیه زیرساخت‌های حیاتی نیز در شرایط خاص می‌توانند فراتر از یک جرم عادی فرامرزی، به مسأله‌ای مرتبط با حاکمیت و امنیت ملی تبدیل شوند. بر همین اساس، پژوهش ایجاد چارچوب‌های هماهنگ برای تعیین صلاحیت، مسؤولیت دولت‌ها و حل‌وفصل مسالمت‌آمیز اختلافات را ضروری دانسته و سازوکاری چندعاملی مبتنی بر «ارتباط واقعی» و ملاحظات نزاکت بین‌المللی را پیشنهاد می‌کند. در سطح داخلی نظام حقوقی عراق نیز تصویب قانون تخصصی جرائم سایبری و تقویت ظرفیت‌های قضایی و فنی، از الزامات اساسی مقابله با این پدیده در آن نظام حقوقی است.

خوانندگان این مجله، اجازه توزیع، ترکیب مجدد، تغییر جزئی و کار روی مقاله حاضر به‌صورت غیرتجاری را دارند.

© تمامی حقوق انتشار این مقاله، متعلق به نویسنده می‌باشد.

مقدمه

فضای سایبری را نمی‌توان صرفا امتداد فنی ارتباطات انسانی دانست؛ بلکه این فضا به‌تدریج به حوزه‌ای تبدیل شده است که در آن حدود اعمال اقتدار دولت‌ها، شیوه تحقق جرم و حتی مفهوم قلمرو حقوقی با دگرگونی مواجه شده است. در برداشت سنتی، حاکمیت دولت با اعمال اقتدار عمومی در محدوده جغرافیایی مشخص و کنترل مؤثر بر قلمرو سرزمینی پیوند داشته است (أبوالوفاء، ۲۰۱۵: ۲۹۸). این تصور در فضای سایبری با وضعیتی مواجه می‌شود که در آن یک رفتار مجرمانه می‌تواند در یک کشور آغاز شود، از زیرساخت‌های چند کشور عبور کند و آثار خود را در کشوری دیگر آشکار سازد، بدون آنکه مرتکب برای تحقق رفتار مجرمانه به قلمرو دولت زیان‌دیده وارد شده باشد.

از همین نقطه، مسأله صلاحیت کیفری در فضای سایبری به مسأله‌ای فراتر از تعیین دادگاه صالح تبدیل می‌شود. هنگامی‌که یک رفتار واحد با قلمرو، اتباع، زیرساخت‌ها یا منافع چند دولت ارتباط پیدا می‌کند، تعیین دولت صالح برای تعقیب جرم مستقیما با حدود اعمال اقتدار حاکمیتی آن دولت و احترام به حاکمیت دولت‌های دیگر ارتباط دارد (حسنی، ۲۰۱۱: ۶۷۸). بنابراین، پرسش اصلی آن است که آیا قواعد سنتی حقوق کیفری بین‌المللی و سازوکارهای معاضدت‌های قضایی موجود می‌توانند پاسخگوی جرائمی باشند که از حیث محل ارتکاب، آثار و ادله، ماهیتی فرامرزی و چندلایه دارند؟

این پرسش در مورد عراق اهمیت بیشتری دارد؛ زیرا بخش قابل‌توجهی از ساختار کیفری این کشور همچنان بر قانون مجازات مصوب ۱۹۶۹ استوار است؛ قانونی که در زمان تصویب آن، جرائم سایبری با ویژگی‌های کنونی وجود نداشتند. در چنین شرایطی، مسأله فقط فقدان عناوین کیفری جدید نیست، بلکه نحوه تعیین صلاحیت، جمع‌آوری ادله، همکاری با دولت‌های دیگر و انتساب حمله به مرتکب یا دولت پشتیبان نیز با دشواری مواجه می‌شود.

پژوهش حاضر برای پاسخ به این مسأله، حقوق کیفری بین‌المللی را به‌عنوان چارچوب هنجاری تحلیلی به حملات سایبری، جاسوسی دیجیتال و تعرض به زیرساخت‌های حیاتی در نظر می‌گیرد و جرم‌شناسی دیجیتال را به‌عنوان ابزاری برای شناخت الگوهای ارتکاب، رفتار مرتکبان و عوامل مؤثر بر شکل‌گیری جرائم سایبری به کار می‌بندد. اهمیت این تلفیق در آن است که تحلیل حقوقی بدون توجه به ساختار فنی و جرم‌شناختی فضای سایبری نمی‌تواند منشأ بسیاری از تعارض‌های صلاحیتی و مشکلات انتساب را توضیح دهد و در مقابل، تحلیل جرم‌شناختی نیز بدون توجه به قواعد صلاحیت و مسؤولیت بین‌المللی قادر به تبیین کامل پیامدهای حقوقی رفتارهای سایبری نیست.

ادبیات حقوقی مرتبط با فضای سایبری در سال‌های اخیر به‌طور قابل‌توجهی گسترش یافته است. یکی از مهم‌ترین منابع در این زمینه، تالین[1] است که قواعد حقوقی قابل اعمال بر عملیات سایبری را بررسی می‌کند. در این چارچوب، قاعده ۴ به حاکمیت و قاعده ۶ به تکلیف مراقبت مقتضی اختصاص یافته است (Schmitt, 2017: 7). اهمیت این اثر در آن است که نشان می‌دهد فضای سایبری را نمی‌توان منطقه‌ای خارج از شمول حقوق بین‌الملل دانست؛ با این حال، تالین خود یک معاهده الزام‌آور نیست و بیشتر ماهیت تفسیری و دکترینال دارد.

همچنین گزارش‌های گروه کارشناسان دولتی سازمان ملل متحد در سال‌های ۲۰۱۳، ۲۰۱۵ و ۲۰۲۱ نیز بر قابلیت اعمال حقوق بین‌الملل و منشور ملل متحد نسبت به استفاده از فناوری اطلاعات و ارتباطات تأکید کرده‌اند. با این حال، گزارش ۲۰۲۱ همچنان وجود اختلاف‌نظر میان دولت‌ها درباره جایگاه مستقل اصل حاکمیت در فضای سایبری و ماهیت الزام‌آور تکلیف مراقبت مقتضی را نشان می‌دهد (UN GGE, 2021). بنابراین، هرچند درباره اصل کلی قابلیت اعمال حقوق بین‌الملل بر فضای سایبری توافق قابل‌توجهی شکل گرفته، اما این توافق هنوز به ایجاد نظامی جامع برای توزیع صلاحیت کیفری و تعیین مسؤولیت دولت‌ها منجر نشده است.

در مطالعه دیگری که توسط کملیا و همکارانش در حوزه صلاحیت انجام داده‌اند، نشان می‌دهد که جرائم سایبری در حقوق بین‌الملل موجود از صلاحیت جهانی عام برخوردار نیستند

[1]- Tallinn Manual 2.0

و کنوانسیون بوداپست عمدتا از طریق هماهنگ‌سازی قوانین داخلی و توسعه همکاری قضایی، امکان اعمال صلاحیت سرزمینی و فرامرزی را تقویت می‌کند (Situmeang et al., 2026: 90). از سوی دیگر، رأی دیوان بین‌المللی دادگستری در قضیه کانال کورفو بر تعهد دولت به جلوگیری از استفاده آگاهانه از قلمرو خود برای اعمال مغایر با حقوق سایر دولت‌ها تأکید دارد (ICJ, 1949). با وجود این، درباره ماهیت و دامنه تکلیف مراقبت مقتضی در فضای سایبری هنوز اختلاف‌نظر وجود دارد (Ponta, 2020: 3).

بخش مهمی از مطالعات موجود یا چارچوب حقوق بین‌المللی فضای سایبری را بررسی کرده‌اند یا بر اجرای قواعد در نظام‌های حقوق داخلی تمرکز داشته‌اند؛ درحالی‌که پیوند میان صلاحیت بین‌المللی، قانون‌گذاری داخلی و جرم‌شناسی دیجیتال، به‌ویژه در مطالعات مربوط به کشورهای عربی و عراق، کمتر به‌صورت یکپارچه مورد بررسی قرار گرفته است. نوآوری پژوهش حاضر در همین پیوند قرار دارد یعنی این پژوهش می‌کوشد تا به تحلیل هم‌زمان ساختار حقوقی صلاحیت، مسؤولیت دولت‌ها و ویژگی‌های جرم‌شناختی جرائم سایبری، با تمرکز بر عراق و استفاده از چارچوب‌های بین‌المللی و مطالعات تطبیقی بپردازد.

در همین راستا قلمرو جغرافیایی پژوهش، عراق را به‌عنوان مطالعه موردی اصلی در نظر گرفته و در کنار آن به چارچوب‌های حقوقی کشورهای عربی و اسناد بین‌المللی برای تحلیل تطبیقی استناد می‌کند. انتخاب عراق از آن جهت اهمیت دارد که نظام کیفری این کشور نمونه روشنی از چالش ناشی از استمرار قواعد کیفری سنتی در مواجهه با جرائم دیجیتال را فراهم می‌کند (الشمری، ۲۰۲۱: ۱۶۷).

از نظر زمانی، قلمرو اصلی پژوهش تحولات مرتبط تا سال ۲۰۲۴ را در برمی‌گیرد؛ هرچند برخی منابع مورد استفاده در متن مربوط به سال‌های بعدی هستند. این منابع در مقام ادبیات متأخر برای تکمیل بحث مورد استفاده قرار گرفته‌اند و استفاده از آن‌ها به معنای تغییر محدوده اصلی موضوع پژوهش نیست.

از نظر موضوعی نیز تمرکز مقاله بر صلاحیت کیفری، مسؤولیت دولت‌ها، انتساب، ادله دیجیتال و حملات مؤثر بر حاکمیت ملی است و قصد ندارد همه اشکال جرائم سایبری را به یک میزان بررسی کند. تروریسم سایبری نیز تنها در حد ارتباط آن با موضوع اصلی مورد توجه قرار می‌گیرد. روش پژوهش، تحلیل حقوقی و تطبیقی است و از داده‌های تجربی برای سنجش میزان وقوع جرائم استفاده نشده است. از این‌رو، بررسی تجربی پرونده‌های قضایی، مصاحبه با قضات و متخصصان فنی و تحلیل داده‌های جرم‌شناختی می‌تواند موضوع پژوهش‌های آینده باشد.

بر این اساس، مقاله ابتدا چالش‌های قضایی و تقنینی حاکمیت ملی را بررسی می‌کند و سپس به نقش دادگاه‌های بین‌المللی و داوری در حل اختلافات ناشی از فعالیت‌های سایبری می‌پردازد. در ادامه، انواع حملات سایبری و میزان تأثیر آن‌ها بر حاکمیت و استقلال دولت‌ها تحلیل می‌شود و در نهایت، مسؤولیت دولت‌ها، خلأهای تقنینی و راهکارهای اصلاحی در نظام حقوقی عراق، منطقه‌ای و بین‌المللی مورد توجه قرار می‌گیرد.

۱- چالش‌های قضایی و تقنینی حاکمیت ملی

مسأله حاکمیت ملی در فضای سایبری را نمی‌توان تنها به نبود قانون تخصصی نسبت داد. مسأله بنیادی‌تر، نحوه توزیع صلاحیت میان دولت‌هایی است که یک رفتار سایبری به قلمرو، اتباع، زیرساخت یا منافع آن‌ها ارتباط پیدا می‌کند. در محیط فیزیکی، محل وقوع جرم در بسیاری از موارد قابل شناسایی است، اما در فضای دیجیتال اجزای مختلف یک رفتار مجرمانه ممکن است در چندین قلمرو پراکنده باشند (Schmitt, 2017: 12). بنابراین، پرسش اصلی تنها این نیست که کدام قانون باید اعمال شود؛ بلکه این است که چگونه می‌توان میان ادعاهای هم‌زمان دولت‌ها برای اعمال صلاحیت، ترتیبی ایجاد کرد که هم امکان تعقیب مؤثر جرم حفظ شود و هم حاکمیت برابر دولت‌ها آسیب نبیند. برای روشن شدن این موضوع دو مسأله صلاحیت قضایی و تعارض میان قوانین ملی

[1]- Corfu Channel

و نقش دادگاه‌های بین‌المللی و داوری در حل اختلافات صلاحیتی باید تبیین شود.

۱-۲- مسأله صلاحیت قضایی و تعارض میان قوانین ملی

قواعد سنتی صلاحیت کیفری عمدتا بر قلمرو و تابعیت مرتکب یا بزه‌دیده و در مواردی منافع اساسی دولت‌ها استوار است. این قواعد در فضای سایبری از میان نرفته‌اند، اما نحوه تحقق آن‌ها تغییر کرده است. در حقوق عراق، ماده ۹ قانون مجازات شماره ۱۱۱ سال ۱۹۶۹ مقرر می‌کند که اگر یکی از عناصر جرم در عراق واقع شود یا نتیجه جرم در این کشور تحقق یابد، جرم در قلمرو عراق واقع‌شده تلقی می‌شود. بنابراین، این مقرره تنها بازتاب یک برداشت محدود از اصل سرزمینی نیست و معیار تحقق نتیجه را نیز در تعیین صلاحیت دخالت می‌دهد (جمیل، ۲۰۱۸: ۹۹). اهمیت این حکم در حملات سایبری آشکار می‌شود؛ زیرا ممکن است حمله خارج از عراق آغاز شود، از چندین سرور عبور کند و نتیجه آن در داخل کشور تحقق یابد. از همین رو، ادبیات حقوقی با بازتعریف مفهوم سرزمین جرم و توجه به محل تحقق آثار، تلاش کرده است پاسخ مناسب‌تری برای جرائم اینترنتی ارائه کند. دکترین حقوقی در این حوزه نیز بر همین مبنا در برخی نظام‌ها امکان اعمال صلاحیت را در مواردی مطرح می‌کند که رفتار خارج از کشور انجام شده اما آثار آن بر امنیت یا منافع دولت وارد شده است.

با این حال، گسترش صلاحیت بر مبنای آثار درصورتی‌که بدون معیارهای محدودکننده صورت گیرد، می‌تواند خود به منشأ تعارض تبدیل شود. اگر هرگونه اثر فنی یا اقتصادی در یک کشور برای ایجاد صلاحیت کافی باشد، یک رفتار واحد ممکن است هم‌زمان تحت صلاحیت چند دولت قرار گیرد. در نتیجه، راه‌حلی که برای جبران محدودیت اصل سرزمینی ایجاد شده، ممکن است به گسترش بیش از حد صلاحیت‌ها منجر شود.

پیش‌نویس قانون جرائم سایبری عراق در سال ۲۰۱۱ تلاش کرده بود این خلأ را با گسترش صلاحیت نسبت به جرائمی که خارج از عراق ارتکاب یافته اما آثار آن به عراق می‌رسد، کاهش دهد. با این حال، این پیش‌نویس به قانون لازم‌الاجرا تبدیل نشد و قانون مجازات عمومی همچنان مبنای اصلی رسیدگی به بسیاری از رفتارهای مجرمانه در فضای دیجیتال باقی ماند. استفاده از مقررات عمومی برای رفتارهای جدید، هرچند ممکن است خلأ اجرایی را تا حدی پر کند؛ اما الزاما ویژگی‌های فنی جرم سایبری را پوشش نمی‌دهد و این جرائم نیازمند مطالعه دقیق و ایجاد هنجارهای تخصصی در خصوص آنها است (راضی و عسل، ۲۰۱۲: ۱۵۳).

در پرونده‌های مربوط به اخاذی سایبری نیز مواد ۴۳۰ و ۴۳۱ قانون مجازات عراق برای برخی رفتارهای مبتنی بر تهدید و مطالبه مالی مورد استناد قرار گرفته‌اند؛ درحالی‌که این مقررات اساسا برای جرائم سایبری طراحی نشده‌اند. در چنین وضعیتی ممکن است پرسش‌هایی درباره اصل قانونی بودن جرم و مجازات ایجاد کند، زیرا استفاده از مقررات سنتی نباید به تفسیر موسع و ایجاد عنوان کیفری جدید از طریق تفسیر قضایی منجر شود (ادریس، ۲۰۲۰: ۱۰۱).

در سطح بین‌المللی نیز کنوانسیون بوداپست از طریق ماده ۲۲ چارچوبی برای اعمال صلاحیت نسبت به جرائم موضوع کنوانسیون ایجاد می‌کند (Budapest Convention, 2001). با این حال، هم‌زمانی چند مبنای صلاحیت می‌تواند به تعارض مثبت صلاحیت، رسیدگی‌های موازی و حتی طرح مسأله اصل منع محاکمه یا مجازات مجدد برای یک عمل منجر شود. پرونده‌های مربوط به دستورات فرامرزی تولید داده نیز نشان می‌دهند که دسترسی قضایی به داده‌های واقع در قلمرو دولت دیگر چگونه می‌تواند مرز میان اعمال صلاحیت و احترام به حاکمیت آن دولت را تحت تأثیر قرار دهد (Eurojust, 2025).

در نتیجه، مشکل اساسی در این حوزه فقدان یک سلسله‌مراتب الزام‌آور و جامع میان صلاحیت‌های رقیب است. در صورت تعدد دولت‌های صالح، قدرت فنی و قضایی قوی‌تر یک دولت نباید منجر به آن شود که به‌طور خودکار مبنای اعمال قانون آن دولت بر رفتارهایی قرار گیرد که ارتباط قابل‌توجهی با دولت‌های دیگر دارند. چه‌آنکه از این منظر، اصل برابری حاکمیتی دولت‌ها در ماده ۲(۱) منشور ملل متحد، محدودیتی مهم بر گسترش یک‌جانبه صلاحیت ایجاد می‌کند.

در همین چارچوب، مفهوم «ارتباط واقعی» می‌تواند به‌عنوان یک معیار تحلیلی مورد استفاده قرار گیرد. رأی Nottebohm این مفهوم را در زمینه تابعیت بررسی کرده است و نمی‌توان از آن یک قاعده قطعی درباره صلاحیت کیفری استخراج کرد (ICJ, 1955). با این حال، مفهوم ارتباط واقعی می‌تواند این پرسش را مطرح کند که آیا رابطه یک دولت با جرم، عینی است یا صرفا بر یک تماس فنی و اتفاقی با زیرساخت دیجیتال آن کشور استوار است. چنین معیاری می‌تواند به سنجش شدت پیوند میان دولت و جرم کمک کند و زمینه‌ای برای تنظیم صلاحیت‌های رقیب فراهم آورد. این مسأله در فضای سایبری اهمیت ویژه‌ای دارد؛ زیرا یک حمله سایبری ممکن است از زیرساخت‌های واقع در یک کشور عبور کند، توسط شخصی در کشور دیگری انجام شود و آثار مستقیم یا غیرمستقیم آن در چند کشور تحقق یابد. در چنین شرایطی، صرف قرار داشتن یک سرور، مرکز داده یا مسیر ارتباطی در قلمرو یک دولت، لزوما برای اثبات وجود رابطه میان آن دولت و جرم کافی نیست.

از این منظر، ارتباط واقعی را می‌توان بر اساس مجموعه‌ای از عوامل عینی، از جمله محل وقوع بخش اساسی رفتار مجرمانه، محل تحقق آثار مستقیم جرم، تابعیت یا اقامتگاه مرتکب، وضعیت بزه‌دیده، محل استقرار زیرساخت حیاتی مورد حمله و میزان تأثیر رفتار بر منافع اساسی دولت ارزیابی کرد (الطائی، ۲۰۲۵: ۱۳۸). بنابراین هرچه این عوامل از حیث تعداد و اهمیت، ارتباط بیشتری با یک دولت داشته باشند، ادعای صلاحیت آن دولت از پشتوانه عینی بیشتری برخوردار خواهد بود. در مقابل، هنگامی‌که تنها پیوند موجود، استفاده اتفاقی از یک سرور یا زیرساخت فنی در قلمرو یک کشور باشد، اتکای صرف به این عامل می‌تواند زمینه تعارض گسترده و اعمال بیش از حد صلاحیت کیفری را فراهم کند.

البته، کاربرد این مفهوم باید با احتیاط صورت گیرد؛ زیرا رأی Nottebohm دیوان بین‌المللی دادگستری این مفهوم را در زمینه تابعیت و قابلیت استناد به تابعیت در روابط بین‌المللی مورد بررسی قرار داده است و از آن نمی‌توان مستقیما یک قاعده قطعی و الزام‌آور درباره صلاحیت کیفری، به‌ویژه در فضای سایبری، استخراج کرد (ICJ, 1955). بنابراین، در این پژوهش، ارتباط واقعی نه به‌عنوان یک مبنای مستقل صلاحیت، بلکه به‌عنوان معیاری تحلیلی برای سنجش کیفیت و شدت پیوند میان دولت و جرم مورد استفاده قرار می‌گیرد. چنین رویکردی می‌تواند در موارد تعدد دولت‌های مدعی صلاحیت، به تفکیک ارتباط‌های عینی و اساسی از تماس‌های صرفا فنی و اتفاقی کمک کرده و مبنایی برای تنظیم و هماهنگ‌سازی صلاحیت‌های رقیب فراهم آورد.

۱-۲-۱- معیارهای صلاحیت کیفری و تأثیر آن‌ها بر حاکمیت سرزمینی

اصل سرزمینی همچنان یکی از مبانی اساسی صلاحیت کیفری است، اما در فضای سایبری مفهوم «وقوع جرم در سرزمین» دیگر نمی‌تواند صرفا با محل حضور مرتکب یا دستگاه مورد استفاده او تعیین شود. اجزای مختلف یک رفتار مجرمانه ممکن است در چند نقطه جغرافیایی پراکنده باشند. بنابراین، حفظ برداشت سنتی از سرزمین بدون توجه به این واقعیت می‌تواند موجب خروج بخشی از جرائم فرامرزی از قلمرو مؤثر قواعد کیفری شود.

در مقابل، گسترش بیش از حد مفهوم سرزمینی نیز خطر افزایش دولت‌های دارای صلاحیت را به همراه دارد. عبور داده از یک سرور یا ایجاد یک اثر فرعی نباید به‌تنهایی برای ایجاد صلاحیت کافی باشد؛ زیرا در غیر این صورت، تعداد پیوندهای حقوقی یک جرم سایبری می‌تواند به‌طور نامحدود افزایش یابد. از این‌رو، مسأله اصلی انتخاب میان اصل سرزمینی و اصل غیر سرزمینی نیست، بلکه تعیین معیارهایی برای تشخیص شدت و کیفیت رابطه میان جرم و قلمرو آن است.

در حقوق عراق، اتکای نظام کیفری به قانون سال ۱۹۶۹ این مشکل را تشدید می‌کند؛ زیرا قانون مزبور در دوره‌ای تدوین‌شده که داده، سامانه اطلاعاتی و زیرساخت دیجیتال به‌عنوان موضوعات مستقل در امور کیفری مطرح نبودند. مواد ۴۳۳ و ۴۳۴ این قانون درباره توهین و افترا و ماده ۴۴۱ درباره تخریب اموال منقول، نمونه‌هایی از مقرراتی هستند که انتقال

[1]- Genuine Link

مستقیم آن‌ها به محیط دیجیتال بدون توجه به ویژگی‌های داده و سامانه با محدودیت مواجه است (جمیل، ۲۰۱۸: ۹۵).

بنابراین خلأ تقنینی نه‌تنها بر جرم‌انگاری اثر می‌گذارد، بلکه تعریف قلمرو جرم، تعیین صلاحیت و قابلیت استفاده از ادله دیجیتال را نیز تحت تأثیر قرار می‌دهد.

۱-۲-۲- تعدد دولت‌های متأثر و تعارض صلاحیت قضایی

یک حمله سایبری می‌تواند هم‌زمان با دولت محل استقرار مرتکب، دولت محل زیرساخت، دولت محل تحقق نتیجه و دولت متبوع مرتکب یا بزه‌دیده ارتباط داشته باشد. در چنین شرایطی، تفاوت قوانین ماهوی، آیین دادرسی و معیارهای اثباتی دولت‌ها می‌تواند هماهنگی قضایی را دشوار کند (حمدی، ۲۰۲۳: ۱۹۸).

گزارش‌های گروه کارشناسان سازمان ملل متحد در سال‌های ۲۰۱۳، ۲۰۱۵ و ۲۰۲۱ بر قابلیت اعمال حقوق بین‌الملل و اصول منشور ملل متحد در فضای سایبری تأکید کرده‌اند، اما چارچوب تفصیلی و الزام‌آوری برای توزیع صلاحیت کیفری ایجاد نکرده‌اند. از این‌رو، بخش مهمی از حل تعارض همچنان به قوانین داخلی و توافق‌های دوجانبه و چندجانبه وابسته است (القیسی، ۲۰۲۱: ۳۲۱). این وضعیت زمانی به مسأله حاکمیت تبدیل می‌شود که توانایی فنی یک دولت عملا به ابزار گسترش صلاحیت آن تبدیل شود. بنابراین، تعدد صلاحیت‌ها باید نه فقط از منظر کارآمدی تعقیب جرم، بلکه از منظر برابری حاکمیتی نیز بررسی شود. معیار ارتباط واقعی می‌تواند در این زمینه، در کنار اصل سرزمینی و شخصی، برای سنجش کیفیت پیوند دولت با جرم مورد استفاده قرار گیرد و مبتنی بر این دو معیار تصمیم‌گیری شود که کدام دولت صلاحیت رسیدگی به این جرم را دارند.

۱-۲-۳- دشواری اعمال اصول سرزمینی و شخصی و تعارضات تقنینی

تعارض میان قوانین ملی در فضای سایبری تنها ناشی از تفاوت سطح توسعه تقنینی کشورها نیست؛ بلکه از تفاوت در تعریف خود جرم سایبری نیز ناشی می‌شود. برخی کشورها قوانین تخصصی تصویب کرده‌اند و برخی دیگر همچنان بر قوانین کیفری عمومی تکیه دارند. این تفاوت هنگامی اهمیت می‌یابد که یک رفتار واحد در چند قلمرو آثار حقوقی ایجاد کند. در همین راستا در عراق نیز نبود قانون جامع جرائم سایبری این وضعیت را تشدید کرده است. پیش‌نویس سال ۲۰۱۱ درصدد جرم‌انگاری برخی رفتارهای جدید و ایجاد سازوکارهایی مانند مرکز ملی ادله دیجیتال بود، اما به تصویب نرسید؛ بنابراین، محاکم در بسیاری از موارد ناگزیر از استفاده از قانون مجازات و دستورالعمل‌های پراکنده‌اند؛ دستورالعمل‌هایی که از حیث جایگاه حقوقی الزام‌آور، لزوما با قانون مصوب قابل مقایسه نیستند و در سلسله مراتب حقوقی از جایگاه نازل‌تری نسبت به قانون برخوردارند.

در نتیجه، خلأ موجود را نباید صرفا «عقب‌ماندگی قانون‌گذاری» از فناوری دانست. مسأله اساسی، فقدان هماهنگی میان جرم‌انگاری، صلاحیت، ادله و همکاری بین‌المللی است. حتی اگر دادگاه عراقی صلاحیت خود را احراز کند، ممکن است بدون همکاری دولت محل نگهداری داده یا دولت محل حضور مرتکب نتواند صلاحیت خود را عملا اعمال کند. بنابراین، تعارض تقنینی در فضای سایبری بخشی از مسأله گسترده‌تر حاکمیت دیجیتال است و نیازمند پیوند میان اصلاح قانون داخلی و سازوکارهای همکاری بین‌المللی است.

۲-۲- نقش دادگاه‌های بین‌المللی و داوری در حل اختلافات صلاحیتی

پیچیدگی صلاحیت در فضای سایبری در مواردی به اختلاف میان دولت‌ها منجر می‌شود و در چنین وضعیتی، سازوکارهای بین‌المللی حل اختلاف می‌توانند از تبدیل اختلافات حقوقی به منازعات سیاسی یا امنیتی جلوگیری کنند. با این حال، کارآمدی این سازوکارها به امکان اثبات منشأ حمله، انتساب رفتار و دسترسی به ادله فنی وابسته است و مبتنی بر این امور می‌توان از این سازوکارها بهره برد.

۲-۲-۱- صلاحیت دیوان بین‌المللی دادگستری در اختلافات سایبری

منشور ملل متحد توسل به زور و مداخله در امور داخلی دولت‌ها را منع می‌کند، اما عملیات سایبری پرسش مقدماتی مهمی ایجاد می‌کند: چه زمانی یک عملیات از نقض حاکمیت یا اقدام

خصمانه فراتر می‌رود و به سطحی می‌رسد که قواعد مربوط به توسل به زور یا دفاع مشروع را فعال می‌کند؟

دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه معیار کنترل مؤثر را در بحث انتساب رفتار گروه‌های غیردولتی به دولت مورد توجه قرار داد (ICJ, 1986). اعمال این معیار در فضای سایبری با دشواری بیشتری مواجه است؛ زیرا عملیات دیجیتال می‌تواند از طریق سرورهای واسطه، شبکه‌های ناشناس و گروه‌های نیابتی اجرا شود. از این‌رو این امکان وجود دارد که میان طراح حمله، عامل اجرایی و دولت احتمالی پشتیبان به‌صورت عمدی فاصله ایجاد شود تا انتساب آن حمله به دولت پشتیبان قابل اثبات نباشد. در این موارد دولت نباید اجازه دهد زیرساخت تحت کنترل آن برای عملیات سایبری زیان‌بار علیه دولت‌های دیگر مورد استفاده قرار گیرد. مفهوم علم مفروض در خصوص اطلاع دولت‌ها نیز می‌تواند در شرایطی مطرح شود که دولت با توجه به اوضاع و احوال می‌بایست از فعالیت زیان‌بار مطلع می‌شد (Mestre, 2017: 17). به دیگر سخن زمانی می توان در خصوص دولتی به مفهوم علم مفروض استناد کرد که دولت به‌صورت متعارف باید از این حمله مطلع می‌شد و در این صورت است که دولتی که از زیرساخت‌های او برای این حمله استفاده شده است، مسؤولیت پیدا می‌کند.

علاوه بر این گزارش‌های گروه کارشناسان سازمان ملل نیز بر ضرورت توجه به شواهد فنی و زمینه‌ای در انتساب جرم به یک دولت تأکید کرده‌اند، اما معیار حقوقی واحدی برای آن ایجاد نکرده‌اند؛ در نتیجه به نظر می‌رسد که معیار کنترل مؤثر در برابر ساختار غیرمتمرکز عملیات دیجیتال با دشواری روبه‌روست. در همین راستا دیوان بین‌المللی دادگستری می‌تواند در صورت وجود مبنای صلاحیت، از جمله بر اساس بند اختیاری ماده ۳۶ اساسنامه دیوان، به اختلافات میان دولت‌ها رسیدگی کند. با این حال، وجود صلاحیت رسیدگی با امکان اثبات مسؤولیت یکسان نیست. دولت خواهان باید رابطه میان رفتار مورد ادعا و دولت خوانده را اثبات کند و در اینجا قابلیت دستکاری، تغییر یا از بین رفتن داده‌های دیجیتال اهمیت ویژه‌ای پیدا می‌کند (طلاس، ۲۰۲۰: ۲۰۵). این در حالی است که در فضای سایبری، سرعت تغییر داده‌ها و تعدد قلمروهای محل ذخیره و پردازش آن‌ها موجب می‌شود حفظ زنجیره حفاظتی ادله به یکی از مسائل اساسی اثبات تبدیل شود. بنابراین، محدودیت اصلی در رسیدگی بین‌المللی تنها صلاحیت قضایی نیست؛ بلکه فاصله میان ظرفیت حقوقی رسیدگی و ظرفیت فنی کشف و تحلیل ادله نیز نقش تعیین‌کننده دارد.

۲-۲-۲- نقش دیوان‌های بین‌المللی کیفری

دیوان‌های کیفری بین‌المللی می‌توانند در موارد محدودی با آثار حقوقی عملیات سایبری مواجه شوند، اما «سایبری بودن» یک رفتار، به‌تنهایی موجب ایجاد صلاحیت کیفری بین‌المللی نمی‌شود. صلاحیت دیوان کیفری بین‌المللی بر اساس اساسنامه رم تعیین می‌شود و یک حمله سایبری تنها در صورتی در قلمرو صلاحیت موضوعی دیوان قرار می‌گیرد که عناصر یکی از جرائم مندرج در مواد ۵ تا ۸ مکرر اساسنامه را داشته باشد. در این زمینه، تفکیک میان «کنترل مؤثر» و «مسؤولیت فرماندهی» اهمیت اساسی دارد. کنترل مؤثر در چارچوب مسؤولیت دولت و انتساب رفتار مطرح شده، درحالی‌که مسؤولیت فرماندهی موضوع ماده ۲۸ اساسنامه رم به مسؤولیت کیفری فردی مربوط است (السعید، ۲۰۲۱: ۱۲۵)؛ خلط این دو مفهوم می‌تواند تحلیل حقوقی حملات سایبری را با ابهام مواجه کند.

کنوانسیون بوداپست نیز دادگاه بین‌المللی ایجاد نکرده است، بلکه شبکه‌ای از همکاری‌های رویه‌ای را میان دولت‌ها شکل می‌دهد. نقاط تماس ۲۴ ساعته برای حفظ سریع داده‌ها از مهم‌ترین سازوکارهای آن است، اما کارآمدی این سازوکارها به وجود اختیارات قانونی و ظرفیت فنی در سطح ملی وابسته است (الیسیری، ۲۰۲۳: ۶۷).

در مورد عراق نیز باید گفت فقدان قانون جامع جرائم سایبری، توانایی نظام حقوقی این کشور را در اجرای مؤثر درخواست‌های معاضدت قضایی محدود می‌کند (العبیدی، ۲۰۲۲: ۵۰). از این‌رو، همکاری بین‌المللی بدون اصلاحات داخلی نمی‌تواند تمام خلأهای موجود را جبران کند.

۲-۲-۳- داوری بین‌المللی به‌عنوان سازوکار جایگزین

داوری بین‌المللی نیز می‌تواند در کنار سازوکارهای قضایی رسمی برای حل اختلافات سایبری مورد استفاده قرار گیرد. تعهد دولت‌ها به حل‌وفصل مسالمت‌آمیز اختلافات بر اساس منشور ملل متحد، مبنای عمومی این رویکرد را فراهم می‌کند و گزارش گروه کارشناسان دولتی در سال ۲۰۱۵ نیز قابلیت اعمال اصل حل‌وفصل مسالمت‌آمیز اختلافات را در زمینه فعالیت‌های سایبری مورد توجه قرار داده است (UN GGE, 2015). انعطاف‌پذیری داوری، امکان انتخاب داوران دارای تخصص فنی و قابلیت حفظ محرمانگی می‌تواند در اختلافات سایبری اهمیت داشته باشد. با این حال، فقدان توافق جامع درباره مسؤولیت حملات سایبری، دشواری انتساب و ابهام در مرز میان جرم سایبری و توسل به زور، کارآمدی داوری را نیز محدود می‌کند (ابن‌نجم، ۲۰۱۵: ۱۱۲). افزون بر این، الزام‌آوری رأی داوری اصولا به طرف‌های توافق داوری محدود است. در عراق نیز فقدان قانون تخصصی موجب می‌شود اجرای همکاری‌های بین‌المللی با محدودیت مواجه باشد. بنابراین، توسعه قانون‌گذاری داخلی باید به‌عنوان پیش‌شرط تقویت همکاری قضایی و داوری بین‌المللی مورد توجه قرار گیرد (العنزی، ۲۰۱۹: ۲۱۲).

۳- جرائم سایبری به‌عنوان تعرض به حاکمیت و استقلال ملی

همه جرائم سایبری آثار یکسانی بر حاکمیت ندارند. برخی رفتارها صرفا تعرض به داده یا اموال خصوصی‌اند، درحالی‌که برخی دیگر می‌توانند عملکرد زیرساخت‌های حیاتی، امنیت ملی یا فرآیندهای تصمیم‌گیری دولت را مختل کنند. بنابراین، طبقه‌بندی حقوقی حملات باید بر اساس هدف، شدت، آثار و رابطه آن‌ها با اقتدار حاکمیتی صورت گیرد.

۳-۱- انواع حملات سایبری و طبقه‌بندی حقوقی آن‌ها

حملات نظامی، اقتصادی، جاسوسی و اطلاعاتی گمراه‌کننده از حیث آثار حقوقی یکسان نیستند. تعیین وصف حقوقی هر یک نیازمند بررسی جداگانه است؛ زیرا نمی‌توان صرف استفاده از ابزار دیجیتال را دلیل کافی برای انتساب رفتار به یکی از شدیدترین ممنوعیت‌های حقوق بین‌الملل دانست. در همین راستا لازم است تا در خصص این جرائم بحث شود و انواع آن و طبقه‌بندی آنها در حقوق تعیین گردد.

۳-۱-۱- حملات نظامی و تأثیر آن‌ها بر حاکمیت

یکی از مهم‌ترین مسائل، تعیین رابطه میان حملات سایبری و مواد ۲(۴) و ۵۱ منشور ملل متحد است. گزارش گروه کارشناسان دولتی در سال ۲۰۱۳ تأکید کرده است که منشور نسبت به فضای سایبری نیز قابل اعمال است (UN GGE, 2013). با این حال، این اصل کلی پاسخ نمی‌دهد که هر حمله سایبری چه زمانی به سطح «توسل به زور» یا «حمله مسلحانه» می‌رسد.

دیوان بین‌المللی دادگستری در قضیه نیکاراگوئه در تحلیل مفهوم حمله مسلحانه به شدت و آثار توجه کرده است (ICJ, 1986). در ادبیات حقوقی، این رویکرد برای تحلیل حملات سایبری نیز مورد استفاده قرار گرفته است؛ به‌ویژه در مواردی که حمله موجب تخریب گسترده یا تلفات انسانی مشابه حملات متعارف شود (عبدالصادق، ۲۰۱۹: ۱۱۲). با این حال، حملاتی که بدون تخریب فیزیکی، عملکرد زیرساخت‌های حیاتی را برای مدت قابل‌توجهی مختل می‌کنند، در این چارچوب با دشواری بیشتری قابل طبقه‌بندی‌اند.

این مشکل در حقوق عراق نیز آشکار است. ماده ۳۵۳ قانون مجازات، بر تخریب از طریق مواد منفجره یا وسایل مشابه تمرکز دارد و نمی‌توان آن را بدون تفسیر موسع و احتمالا مغایر با اصل قانونی بودن جرم و مجازات، بر تمام اشکال تخریب دیجیتال سرایت داد و آن را در خصوص این جرم اعمال کرد (عبدالصادق، ۲۰۲۱: ۱۵۴)؛ بنابراین، حتی حمله‌ای که در سطح بین‌المللی ممکن است تهدیدی جدی برای حاکمیت محسوب شود، ممکن است در حقوق داخلی عنوان کیفری متناسبی نداشته باشد.

۳-۱-۲- حملات اقتصادی و جاسوسی

حملات اقتصادی و جاسوسی سایبری نیز باید بر اساس ماهیت و میزان مداخله آن‌ها تحلیل شوند. صرف جاسوسی سایبری لزوما معادل توسل به زور نیست، اما در صورت وجود فشار اجباری و هدف قرار دادن آزادی تصمیم‌گیری دولت، می‌تواند

با اصل عدم مداخله ارتباط پیدا کند (ICJ, 1986). در همین راستا همان‌طور که بیان شد، قواعد تالین نیز میان جاسوسی سایبری در زمان صلح و اشکال نظام‌مند و اجباری آن تمایز قائل می‌شود (Schmitt, 2017). مشکل انتساب جرم و حیطه صلاحیتی در این حوزه نیز پابرجاست. استفاده از سرورهای واسطه و روش‌های پنهان‌سازی می‌تواند تشخیص عامل واقعی را دشوار کند. در حقوق عراق، مواد ۱۵۶ تا ۱۷۹ قانون مجازات برای الگوهای سنتی جاسوسی و جرائم علیه امنیت دولت طراحی شده‌اند و دسترسی غیرمجاز یا تحصیل داده‌های دیجیتال را به‌صورت تخصصی پوشش نمی‌دهند (عطیه، ۲۰۱۵: ۱۱۵)؛ بنابراین، گسترش جاسوسی اقتصادی در محیط دیجیتال می‌تواند فراتر از ظرفیت توصیف‌های کیفری موجود قرار گیرد.

۳-۱-۳- عملیات اطلاعاتی گمراه‌کننده

عملیات اطلاعاتی گمراه‌کننده از دشوارترین اشکال رفتار سایبری از منظر حقوق بین‌الملل است. اصل عدم مداخله با عنصر فشار اجباری و محدود کردن آزادی تصمیم‌گیری دولت‌ها ارتباط دارد؛ بنابراین، صرف انتشار اطلاعات نادرست لزوما به معنای مداخله غیرقانونی نیست و باید میزان، سازمان‌یافتگی و هدف عملیات مورد بررسی قرار گیرد (الطائی، ۲۰۲۰: ۱۵۴). گزارش‌های گروه کارشناسان دولتی سازمان ملل متحد اصول کلی منشور را بر فعالیت‌های سایبری قابل اعمال دانسته‌اند، اما آستانه‌های کمی و کیفی مشخصی برای تشخیص زمان تبدیل عملیات اطلاعاتی به مداخله غیرقانونی تعیین نکرده‌اند. کنوانسیون بوداپست نیز این رفتار را به‌عنوان یک جرم مستقل به‌طور عام جرم‌انگاری نکرده است (Budapest Convention, 2001).

در حقوق عراق نیز مواد ۴۳۳ و ۴۳۴ قانون مجازات برای مقابله با عملیات پیچیده و غیرمتمرکز اطلاعاتی که ممکن است از سوی عوامل خارجی سازمان‌دهی شوند، طراحی نشده‌اند (علی، ۲۰۱۷: ۱۱۵). از منظر جرم‌شناسی دیجیتال نیز ساختار شبکه‌ای این عملیات، تشخیص مرز میان رفتار فردی، فعالیت سازمان‌یافته و عملیات وابسته به دولت را دشوار می‌کند. از همین رو، پیشنهاد ایجاد یک ابزار بین‌المللی برای مقابله با اشکال ناملموس اجبار اطلاعاتی در ادبیات موجود مطرح شده است (عطیه، ۲۰۱۹: ۱۵۰). چنین چارچوبی، در عین حمایت از حاکمیت، باید میان عملیات مداخله‌گر و فعالیت‌های مشروع اطلاعاتی یا آزادی بیان تمایز قائل شود.

۳-۲- مسؤولیت دولت و ضمانت اجراهای کیفری در حملات علیه زیرساخت‌ها

حملات علیه زیرساخت‌های حیاتی اهمیت ویژه‌ای دارند؛ زیرا در این موارد، آثار رفتار ممکن است از خسارت به یک سامانه یا شرکت خصوصی فراتر رود و خدمات عمومی و امنیت ملی را تحت تأثیر قرار دهد. با این حال، تعیین مسؤولیت دولت همیشه از طریق انتساب مستقیم عملیات ممکن نیست. عملیات ممکن است توسط اشخاص خصوصی یا گروه‌های نیابتی اجرا شود و دولت صرفا به دلیل محل استقرار زیرساخت یا عدم اقدام پیشگیرانه با تحقق این جرائم با مسأله مسؤولیت مواجه شود.

۳-۲-۱- مبنای حقوقی مسؤولیت دولت در قبال حملات سایبری

مسؤولیت بین‌المللی دولت‌ها در قبال حملات سایبری بر قواعد عمومی حقوق بین‌الملل، به‌ویژه پیش‌نویس مواد کمیسیون حقوق بین‌الملل درباره مسؤولیت دولت‌ها مصوب ۲۰۰۱، استوار است. مطابق ماده ۲ این پیش‌نویس، تحقق مسؤولیت مستلزم انتساب رفتار به دولت و نقض یک تعهد بین‌المللی است. بر اساس ماده ۴، حملات سایبری انجام‌شده توسط ارکان دولتی در مقام رسمی، اصولا به دولت منتسب می‌شوند. با این‌حال، در حملات سایبری اجراشده توسط گروه‌های هکری غیردولتی یا نیروهای نیابتی، ماده ۸ و احراز دستور، هدایت یا کنترل دولت بر رفتار موردنظر اهمیت می‌یابد (ILC, 2001).

در قضیه نیکاراگوئه (۱۹۸۶)، دیوان بین‌المللی دادگستری معیار کنترل مؤثر را برای انتساب رفتار نیروهای غیردولتی به دولت بررسی کرد. اعمال این معیار در حملات سایبری با دشواری‌هایی همراه است؛ زیرا مهاجمان می‌توانند با استفاده از سرورهای واسطه، ابزارهای ناشناس‌ساز و زیرساخت‌های مستقر در کشورهای مختلف، هویت و منشأ واقعی حمله را پنهان کنند. بنابراین، حمایت مالی یا سیاسی دولت از یک گروه

هکری، به‌تنهایی برای انتساب حملات آن گروه به دولت کافی نیست و باید شواهد مرتبط با عملیات مشخص بررسی شوند.

در کنار انتساب مستقیم، تعهد مراقبت مقتضی نیز در بررسی مسؤولیت دولت اهمیت دارد. به‌عنوان مثال در قضیه کانال کورفو (۱۹۴۹) که از مبانی تاریخی بحث است، به تعهد دولت به جلوگیری از استفاده آگاهانه از قلمرو خود برای اقدامات زیان‌بار علیه سایر دولت‌ها اشاره کرده است (ICJ, 1949). در حوزه حملات سایبری نیز چنانچه دولت از استفاده مخرب از زیرساخت‌های تحت صلاحیت خود آگاه باشد یا با توجه به شرایط انتظار رود که از این اقدامات آگاه شود، ملزم است از تحقق این مسائل و حملات جلوگیری به عمل آورد و اگر از مسؤولیت خود خودداری کرده و از اتخاذ اقدامات معقول و امکان‌پذیر اجتناب کند، ممکن است نقض تعهد بین‌المللی محسوب شود. با این‌حال، راهنمای تالین ۲،۰ در این زمینه سندی کارشناسی و غیر الزام‌آور است (Schmitt, 2017: 125).

در عراق نیز ارزیابی مسؤولیت دولت در قبال حملات سایبری مستلزم بررسی قوانین مرتبط، ظرفیت نهادهای امنیت سایبری و توانایی دولت در شناسایی، پیشگیری و پاسخ به حملات علیه زیرساخت‌های حیاتی است. در نهایت، مسؤولیت بین‌المللی صرفا از وقوع حمله یا ضعف نظام داخلی ناشی نمی‌شود، بلکه احراز نقض تعهد بین‌المللی مشخص ضرورت دارد. حال آنکه قانون مجازات عراق مصوب سال ۱۹۶۹ سازوکار تخصصی برای حفاظت پیشگیرانه از زیرساخت‌های حیاتی دیجیتال ندارد (الشمری، ۲۰۲۱: ۱۶۷). بنابراین، وجود تعهد بین‌المللی بدون ظرفیت داخلی برای شناسایی و جلوگیری از حمله، نمی‌تواند به مسؤولیت و پاسخ مؤثر منجر شود.

۳-۲-۲- تکلیف دولت‌ها به جلوگیری از استفاده از زیرساخت‌های خود برای حملات سایبری

گزارش گروه کارشناسان دولتی سازمان ملل متحد در سال ۲۰۱۵ بر این نکته تأکید کرده است که دولت‌ها نباید آگاهانه اجازه دهند قلمرو آن‌ها برای اعمال متخلفانه بین‌المللی از طریق فناوری اطلاعات و ارتباطات مورد استفاده قرار گیرد (UN GGE, 2015). گزارش ۲۰۲۱ این گروه نیز بر حفاظت از زیرساخت‌های حیاتی و همکاری دولت‌ها تأکید کرده است (UN GGE, 2021). با این حال، درباره وضعیت حقوقی دقیق این تعهد اختلاف‌نظر وجود دارد و برخی دولت‌ها آن را قاعده الزام‌آور و برخی دیگر بیشتر هنجاری رفتاری تلقی کرده‌اند (CCDCOE, 2015). افزون بر این، اثبات علم دولت دشوار است؛ زیرا حملات ممکن است بدون اطلاع صاحب زیرساخت انجام شوند. از این‌رو، مفهوم علم مفروض می‌تواند اهمیت داشته باشد، مشروط بر اینکه معیارهای عینی برای اعمال آن وجود داشته باشد (Mestre, 2017: 17).

در عراق، این مسأله با فقدان قانون تخصصی جرائم سایبری و اتکا به قانون مجازات و قانون ارتباطات شماره ۳۴ سال ۲۰۱۲ پیچیده‌تر می‌شود. بنابراین، اصلاح نظام تقنینی داخلی برای اجرای مؤثر هر تعهد بین‌المللی در این زمینه ضروری است. بدین معنا که کشورها باید نظام‌های داخلی خود را مبتنی بر این آموزه‌های بین‌المللی بروز کنند تا امکان و دستاویز قانونی در خصوص این جرائم وجود داشته باشد.

۳-۲-۳- مسؤولیت کیفری و جبران خسارت ناشی از حملات سایبری

مسؤولیت ناشی از حملات سایبری مستلزم بررسی هم‌زمان ابعاد کیفری، بین‌المللی و جبرانی این حملات است. گزارش‌های گروه کارشناسان دولتی سازمان ملل متحد در سال‌های ۲۰۱۳، ۲۰۱۵ و ۲۰۲۱ بر قابلیت اعمال حقوق بین‌الملل، از جمله اصول منشور ملل متحد، در فضای سایبری تأکید کرده‌اند (UN GGE, 2013; UN GGE, 2015; UN GGE, 2021). بر این اساس، حملات سایبری، متناسب با ماهیت و آثار آن‌ها، ممکن است علاوه بر مسؤولیت کیفری مرتکبان، مسؤولیت بین‌المللی دولت‌ها را نیز مطرح کنند؛ البته مسؤولیت دولت مستلزم احراز شرایط انتساب رفتار و نقض تعهد بین‌المللی است.

از منظر حقوق کیفری، جرم‌انگاری دسترسی غیرمجاز به سامانه‌ها، تخریب یا تغییر داده‌ها، شنود غیرمجاز و ایجاد اختلال در عملکرد شبکه‌ها، از ابزارهای اساسی مقابله با حملات سایبری محسوب می‌شود. این در حالی است که در حقوق عراق، اتکای صرف به مقررات سنتی مربوط به تخریب

اموال ممکن است برای پوشش تمام ابعاد این حملات، به‌ویژه سرقت اطلاعات، اخلال در خدمات دیجیتال و آسیب به زیرساخت‌های حیاتی، کافی نباشد (الصغیر، ۲۰۲۱: ۹۰). در مقابل، کنوانسیون بوداپست ۲۰۰۱ با پیش‌بینی جرائم مرتبط با سامانه‌ها و داده‌های رایانه‌ای، چارچوب تخصصی‌تری فراهم کرده است؛ هرچند میزان بهره‌مندی عراق از این چارچوب باید با توجه به وضعیت عضویت و مقررات داخلی آن بررسی شود.

با این‌حال، تعقیب کیفری مرتکبان به دلیل ماهیت فرامرزی حملات سایبری با موانعی مانند ناشناس‌بودن مهاجمان، پراکندگی ادله دیجیتال و دشواری دسترسی به داده‌های ذخیره‌شده در کشورهای دیگر مواجه است. از این‌رو، همکاری قضایی، تبادل اطلاعات، حفظ ادله الکترونیکی و سازوکارهای قانونی استرداد، نقش مهمی در اثربخشی تعقیب کیفری دارند (الشکری، ۲۰۲۰: ۱۱۱).

از سوی دیگر، جبران خسارت ناشی از حملات سایبری باید زیان‌های اقتصادی، هزینه بازیابی سامانه‌ها، اختلال در خدمات عمومی و خسارت واردشده به اشخاص و مؤسسات را در برگیرد. تحقق جبران خسارت مستلزم احراز مبنای مسؤولیت، رابطه سببیت و میزان زیان است. بنابراین، مقابله مؤثر با حملات سایبری مستلزم تلفیق جرم‌انگاری مناسب، همکاری فرامرزی و سازوکارهای مؤثر جبران خسارت است.

نتیجه‌گیری

تحلیل انجام‌شده نشان می‌دهد که نخستین مانع ساختاری در حمایت کیفری از حاکمیت دیجیتال عراق، شکاف میان قانون مجازات شماره ۱۱۱ سال ۱۹۶۹ و ماهیت غیرمادی جرائم سایبری است. مقررات سنتی، به‌ویژه مواد ۳۵۳ و ۴۴۱، عمدتا بر خسارت مادی و ملموس استوارند و به همین دلیل، نمی‌توانند همه اشکال تعرض به داده‌ها، سامانه‌ها و زیرساخت‌های دیجیتال را پوشش دهند. در مقابل، کنوانسیون بوداپست عناوین مستقلی برای رفتارهایی مانند دسترسی غیرمجاز و مداخله در داده‌ها پیش‌بینی کرده است. بنابراین، مشکل عراق صرفا کمبود چند عنوان مجرمانه نیست، بلکه شکاف مفهومی میان ساختار قانون کیفری موجود و ماهیت جرم در محیط دیجیتال است.

یافته دوم به تعدد دولت‌های مرتبط با یک حمله سایبری مربوط می‌شود. یک رفتار واحد ممکن است با قلمرو دولت محل ارتکاب، محل تحقق نتیجه، محل استقرار زیرساخت و تابعیت مرتکب یا بزه‌دیده ارتباط پیدا کند. در نبود سلسله‌مراتب الزام‌آور میان صلاحیت‌های رقیب، این وضعیت می‌تواند به تعارض مثبت صلاحیت و رسیدگی‌های موازی منجر شود. از این منظر، پیشنهاد استفاده تحلیلی از معیار «ارتباط واقعی» می‌تواند به سنجش کیفیت پیوند هر دولت با جرم کمک کند، بدون آنکه این معیار به‌عنوان یک قاعده قطعی صلاحیت کیفری بین‌المللی تلقی شود.

یافته سوم به انتساب حملات سایبری مربوط است. معیار کنترل مؤثر در محیطی که عملیات از طریق سرورهای واسطه و گروه‌های نیابتی انجام می‌شود، با محدودیت‌های اثباتی روبه‌روست. در مقابل، تکلیف مراقبت مقتضی می‌تواند در مواردی که انتساب مستقیم امکان‌پذیر نیست، مسیر دیگری برای بررسی رفتار دولت فراهم کند. تفاوت میان این دو مبنا از نظر تحلیلی اهمیت دارد: نخستین مبنا به انتساب رفتار به دولت مربوط است و دومی به رفتار خود دولت در زمینه پیشگیری و کنترل قلمرو یا زیرساخت آن حملات مربوط می‌شود.

یافته چهارم نشان می‌دهد که عملیات اطلاعاتی گمراه‌کننده شکاف هم‌زمان در حقوق بین‌الملل و حقوق داخلی ایجاد می‌کنند. این عملیات می‌توانند به‌صورت تدریجی و الگوریتمی انجام شوند و بدون استفاده از زور مستقیم، بر ادراک عمومی و تصمیم‌گیری سیاسی اثر بگذارند. در نتیجه، رسیدن آن‌ها به آستانه فشار اجباری لازم برای اعمال اصل عدم مداخله همیشه روشن نیست. در حقوق عراق نیز مقررات موجود برای مقابله با عملیات غیرمتمرکز و حمایت‌شده از خارج طراحی نشده‌اند.

یافته پنجم به مسأله ادله دیجیتال مربوط می‌شود. جمع‌آوری و پذیرش ادله در پرونده‌های فرامرزی مستلزم هماهنگی میان چند نظام حقوقی است. هنگامی‌که داده‌ها در چند کشور ایجاد، منتقل یا ذخیره می‌شوند، حفظ زنجیره حفاظتی و جلوگیری از تغییر یا نابودی آن‌ها به بخش مهمی از فرایند اثبات تبدیل می‌شود. در این شرایط نبود چارچوب هماهنگ برای حفظ سریع داده‌ها و استانداردهای مشترک ادله می‌تواند حتی در

مواردی که صلاحیت قضایی روشن است، تعقیب کیفری را دشوار کند. در این راستا لازم است تا با معیار قرار دادن دستاوردهای و معاهدات بین‌المللی قوانین داخلی کشورها مبتنی بر آنها تهیه شود تا در این خصوص نظام‌های حقوقی بتوانند با یکدیگر کار کنند.

در مجموع، یافته‌های پژوهش نشان می‌دهد که مسأله حاکمیت ملی در فضای سایبری را نمی‌توان با اصلاح یک قاعده منفرد حل کرد. صلاحیت، جرم‌انگاری، انتساب، مراقبت مقتضی، ادله دیجیتال و همکاری بین‌المللی حلقه‌های به‌هم‌پیوسته یک نظام واحدند و ضعف هر یک می‌تواند کارآمدی سایر اجزا را کاهش دهد. بنابراین، حمایت مؤثر از حاکمیت دیجیتال مستلزم رویکردی هماهنگ میان حقوق داخلی، حقوق بین‌الملل و واقعیت‌های جرم‌شناختی فضای سایبری است.

این مقاله پیشنهاد می‌دهد که برای مقابله مؤثر با حملات سایبری، عراق باید در سطح داخلی با تصویب قانون جامع جرائم سایبری، تعیین صلاحیت قضایی، تنظیم قواعد ادله دیجیتال و ایجاد نهادهای تخصصی، ظرفیت قانونی و اجرایی خود را تقویت کند. در سطح بین‌المللی نیز تدوین چارچوب‌های الزام‌آور برای مقابله با حملات سایبری، تعیین معیارهای روشن برای بررسی نقض حاکمیت و حل تعارض صلاحیت‌ها، همراه با ایجاد سازوکارهای دائمی همکاری فنی و قضایی، می‌تواند به شناسایی منشأ حملات و ارزیابی انتساب آن‌ها به دولت‌ها کمک کند. همچنین، استانداردسازی جمع‌آوری و حفظ ادله دیجیتال، تشکیل مراکز ملی جرم‌شناسی دیجیتال و توسعه همکاری‌های منطقه‌ای، فرایند تعقیب مرتکبان و رسیدگی به خسارات ناشی از حملات را تسهیل می‌کند. هدف از این اقدامات، ایجاد شبکه‌ای هماهنگ از همکاری حقوقی و فنی برای مقابله با ماهیت فرامرزی حملات سایبری، ضمن رعایت حاکمیت دولت‌ها و تضمین حقوق اشخاص زیان‌دیده است.

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

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

سهم نویسندگان: نگارش این مقاله به‌صورت مشترک توسط نویسندگان با نظارت علمی نویسنده مسؤول انجام شده است.

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

تأمین اعتبار پژوهش: پژوهش حاضر بدون تأمین مالی انجام شده است.

منابع و مآخذ

الف. منابع فارسی

– أبوالوفا، أحمد (۱۹۹۶). *الوسیط فی القانون الدولی العام*. دارالنهضة العربیة.

– إدریس، أحمد فارس (۲۰۲۵). جریمة الابتزاز السیبرانی: بین التوعیة والتجریم فی ظل التشریع العراقی بحث جامعی، جامعة الموصل.

– ابن‌نجم، محمد سمیر (۲۰۱۸). *المسؤولیة الدولیة عن الهجمات السیبرانیة*. دارالفکر والقانون.

– جمیل، محمود کمال (۲۰۱۸). *القانون الجنائی المعلوماتی: الجرائم السیبرانیة*. دارالنهضة العربیة.

– حسنی، محمود نجیب (۲۰۰۹). *شرح قانون العقوبات: القسم العام*. دارالنهضة العربیة.

– حمدی، یاسر محمد (۲۰۲۳). «تنازع الاختصاص القضائی فی الجرائم المرتکبة عبر الفضاء السیبرانی: دراسة مقارنة بین التشریعات العربیة والاتفاقیات الدولیة». *مجلة الدراسات القانونیة والسیاسیة*، ۹(۲).

– راضی، مازن لیلو، و عسل، علی حمزة (۲۰۱۲). «التنظیم القانونی للجرائم السیبرانیة فی العراق». *مجلة المحقق الحلی للعلوم القانونیة والسیاسیة*، –(۴).

– السعید، نورهان مصطفی (۲۰۲۱). *المسؤولیة الجنائیة الفردیة عن الهجمات السیبرانیة أمام المحکمة الجنائیة الدولیة*. دارالفکر الجامعی.

– الشکری، إیمان طارق (۲۰۲۰). «المسؤولیة المدنیة عن أضرار الهجمات السیبرانیة: دراسة مقارنة». *مجلة المحقق الحلی للعلوم القانونیة والسیاسیة*، ۱۲(۳): ۲۱۰–۲۱۵.

– الشمری، حیدر عبد الرضا (۲۰۲۲). «القصور التشریعی فی مواجهة الجرائم السیبرانیة: دراسة تحلیلیة فی ضوء قانون العقوبات العراقی النافذ». *مجلة العلوم القانونیة*، ۳۷(۱): ۱۲۲–۱۱۰.

– الصغیر، جمیل عبد الباقی (۲۰۲۱). *القانون الجنائی والتکنولوجیا الحدیثة (الطبعة الثانیة)*. دارالنهضة العربیة.

– الطائی، حیدر أدهم عبد (۲۰۲۰). «التنظیم القانونی الدولی للفضاء السیبرانی: دراسة فی ضوء مبدأ عدم التدخل». *مجلة العلوم القانونیة*، ۳۵(۲): ۸۵–۱۱۲.

– طلاس، محمد خلیل (۲۰۲۰). *الإثبات الجنائی للأدلة الرقمیة وتحدیاته أمام المحاکم الدولیة والوطنیة*. المرکز العربی للنشر والتوزیع.

– عبدالصادق، محمد سامی (۲۰۱۸). *المسؤولیة المدنیة عن أضرار الهجمات السیبرانیة بحث جامعی*، کلیة الحقوق، جامعة القاهرة.

– عبدالصادق، محمد سامی (۲۰۲۱). *المسؤولیة المدنیة والجنائیة عن أضرار الهجمات السیبرانیة علي البنیة التحتیة الحیویة*. دارالنهضة العربیة.

– علی، حسین‌علی (۲۰۱۷). *المسؤولیة الجنائیة عن الجرائم السیبرانیة فی التشریع العراقی والتشریعات المقارنة رسالة ماجستیر*، کلیة القانون، جامعة بابل.

– العنزی، محمد عبدالله (۲۰۱۹). *التنظیم القانونی الدولی للفضاء السیبرانی أطروحة دکتوراه*، کلیة الحقوق، جامعة القاهرة.

– العبیدی، علی عبدالستار (۲۰۲۲). «التنظیم القانونی للسیادة الرقمیة فی ضوء اجتهادات المحاکم الإقلیمیة والدولیة». *مجلة الدراسات القانونیة المقارنة*، ۴(۲): ۴۵–۶۰.

– عطیة، عمار ترکی (۲۰۱۵). *الحمایة الجنائیة للمعلومات الإلکترونیة: دراسة مقارنة فی القانون العراقی*. منشورات الحلبی الحقوقیة.

– عطیة، طارق إبراهیم الدسوقی (۲۰۱۹). *الأمن السیبرانی: دراسة قانونیة فی مواجهة الجرائم السیبرانیة*. دارالجامعة الجدیدة.

– القیسی، نوار ضام (۲۰۲۱). *السیادة الرقمیة فی إطار القانون الدولی العام: دراسة فی ضوء التقاریر الدولیة والعمل الدولی المشترک*. دارالنهضة العربیة.

– الیاسری، عمار عباس (۲۰۲۳). *التعاون القضائی الدولی فی مکافحة الجرائم السیبرانیة: دراسة تحلیلیة لاتفاقیة بودابست وتطبیقاتها العربیة*. منشورات الحلبی الحقوقیة.

ب. منابع انگلیسی

- Mestre, L (2017). "The due diligence doctrine under Tallinn Manual 2.0". *Computer Law & Security Review*, 33(3): 15-20.

- Ponta, A (2020). "Security and human rights challenges of cyber due diligence". *Harvard International Law Journal*, 61(2): 2-5.

- Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

- Situmeang, S. M. T., Kamilia, E. R., Lutfiyah, N., & Aurora, D. M. (2026). "Enforcement of the universality principle in combating cybercrime as a transnational crime". *Oñati Socio-Legal Series*, 16(2): 87-92

ج. معاهدات، قوانین و اسناد حقوقی

- Budapest Convention on Cybercrime, Nov. 23, 2001, ETS No. 185(Council of Europe).

- Charter of the United Nations, June 26, 1945, 1 UNTS XVI.

- Communications Law No. 34 of 2012 (Iraq).

- Iraqi Penal Code No. 111 of 1969 (Iraq).

د. احکام دادگاه‌های بین‌المللی

- Corfu Channel (United Kingdom v. Albania), Judgment, 1949 I.C.J. 4 (Apr. 9).

- Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, 1986 I.C.J. 14 (June 27).

- Nottebohm (Liechtenstein v. Guatemala), Second Phase, Judgment, 1955 I.C.J. 4 (Apr. 6).

و. گزارش‌های سازمانی

- CCDCOE. (2015). *2015 UN GGE report: Major players recommending norms of behaviour*. NATO Cooperative Cyber Defence Centre of Excellence.

- Eurojust. (2025). Case studies: *Extraterritorial production orders*. European Union Agency for Criminal Justice Cooperation.

- Iraqi Supreme Judicial Council. (2026). *Wasit Court of Appeals organizes specialized workshop on cyber blackmail* [Press release].

- United Nations Group of Governmental Experts. (2013). *Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security* (A/68/98).

- United Nations Group of Governmental Experts. (2015). Report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (A/70/174).

- United Nations Group of Governmental Experts. (2021). *Report of the Group of Governmental Experts on advancing responsible State behaviour in cyberspace in the context of international security* (A/76/135).

- United Nations Office on Drugs and Crime. (2013). *Comprehensive study on the problem of cybercrime and measures taken by Member States to address it*. United Nations.