# چالش‌های حقوقی حاکمیت داده و تعارض صلاحیت دولت‌ها در فضای سایبر

مریم بحرکاظمی

گروه حقوق، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران.

maryambahrekazemi201@gmail.com

احمدپورابراهیم (نویسنده مسئول)

گروه حقوق، واحد رشت، دانشگاه آزاد اسلامی، رشت، ایران.

apourebrahim@iau.ac.ir

چکیده

تحولات فناورانه و گسترش زیست‌بوم داده‌محور، مبانی سنتی اعمال حاکمیت و صلاحیت دولت‌ها را با چالش مواجه ساخته است؛ زیرا جریان داده برخلاف موضوعات مادی، می‌تواند هم‌زمان در چند قلمرو ایجاد، منتقل، پردازش و ذخیره شود و در نتیجه، رابطه سنتی میان سرزمین و اعمال اقتدار دولت را پیچیده کند. در این میان، حاکمیت داده به یکی از مؤلفه‌های مهم اقتدار دولت‌ها تبدیل شده و نحوه تنظیم دسترسی، پردازش و انتقال فرامرزی داده، زمینه‌ساز تعارض میان صلاحیت‌های ملی شده است. پژوهش حاضر با هدف تبیین تحول مبانی صلاحیت دولت در فضای داده‌محور و بررسی راهکارهای حقوقی مدیریت تعارض صلاحیت‌های ناشی از جریان فرامرزی داده، با تأکید بر ظرفیت نظام حقوقی ایران انجام شده است. روش پژوهش توصیفی ـ تحلیلی و شیوه گردآوری اطلاعات، کتابخانه‌ای و مبتنی بر مطالعه منابع حقوقی، اسناد بین‌المللی، قوانین داخلی و پژوهش‌های فارسی و لاتین است. یافته‌های پژوهش نشان می‌دهد که فرامرزی و چندمکانی شدن جریان داده، کارآمدی انحصاری اصل سرزمینی بودن صلاحیت را کاهش داده، اما موجب زوال این اصل نشده است؛ بلکه ضرورت تکمیل آن با معیارهایی همچون تابعیت، منافع اساسی، ارتباط مؤثر و اثرگذاری واقعی را ایجاد کرده است. همچنین، تفکیک صلاحیت تقنینی، قضایی و اجرایی در فضای سایبر اهمیت اساسی دارد؛ زیرا صلاحیت دولت برای وضع قانون یا رسیدگی قضایی لزوماً مجوز اجرای مستقیم اقدامات نسبت به داده‌ها و زیرساخت‌های واقع در قلمرو دولت دیگر محسوب نمی‌شود.

کلیدواژه‌ها: حاکمیت داده، صلاحیت سایبری، تعارض صلاحیت، داده‌های فرامرزی، صلاحیت سرزمینی، حکمرانی داده.

**Legal Challenges of Data Sovereignty and Jurisdictional Conflicts of States in Cyberspace**

Abstract

Technological developments and the expansion of the global data-driven ecosystem have challenged the traditional foundations of state sovereignty and jurisdiction. Unlike tangible objects, data may be created, transferred, processed, and stored simultaneously across multiple jurisdictions, thereby complicating the traditional relationship between territory and the exercise of state authority. In this context, data sovereignty has become an important component of state power, while the regulation of cross-border access to, processing of, and transfer of data has increasingly generated conflicts among national jurisdictions. This study aims to examine the transformation of the foundations of state jurisdiction in the data-driven cyberspace and analyze legal approaches to managing jurisdictional conflicts arising from cross-border data flows, with particular emphasis on the capacity of the Iranian legal system. The research adopts a descriptive-analytical methodology, and data have been collected through library research, including the study of legal sources, international instruments, domestic legislation, and Persian and foreign scholarly literature. The findings indicate that the cross-border and multi-jurisdictional nature of data flows has reduced the exclusive effectiveness of the territorial principle of jurisdiction, without rendering the principle obsolete. Rather, it has created a need to complement territorial jurisdiction with criteria such as nationality, fundamental state interests, effective connection, and substantial effects. The study further demonstrates that distinguishing between legislative, judicial, and executive jurisdiction in cyberspace is essential, since a state's authority to legislate or adjudicate does not necessarily confer a right to directly enforce measures against data or digital infrastructure located within another state's territory. An assessment of the Iranian legal system shows that although existing legislation.

Keywords: Data Sovereignty, Cyber Jurisdiction, Jurisdictional Conflict, Cross-Border Data, Territorial Jurisdiction, Data Governance.

مقدمه

تحولات چند دهه اخیر در حوزه فناوری‌های ارتباطی و ظهور فضای سایبر به‌عنوان بستر غالب تعاملات اقتصادی، سیاسی و اجتماعی، موجب تغییر بنیادین در ساختارهای کلاسیک حقوق بین‌الملل شده است. در گذشته، نظام حقوقی بین‌الملل عمدتاً بر پایه سرزمین، مرزهای جغرافیایی و اقتدار انحصاری دولت‌ها شکل گرفته بود؛ اما در عصر داده‌محور، عنصر «داده» جایگاه محوری در شکل‌دهی به قدرت و صلاحیت پیدا کرده است. داده‌ها نه تنها ابزار انتقال اطلاعات، بلکه منبع تولید قدرت نرم و سخت در روابط میان دولت‌ها محسوب می‌شوند. از این منظر، حاکمیت بر داده به یکی از مؤلفه‌های جدید حاکمیت ملی تبدیل شده است که بدون آن، دولت‌ها در مدیریت فضای داخلی و تعاملات خارجی با محدودیت‌های جدی مواجه می‌شوند.

اهمیت این موضوع زمانی دوچندان می‌شود که توجه شود فضای سایبر برخلاف قلمروهای فیزیکی، ماهیتی غیرمرزی، غیرمتمرکز و پویا دارد. در چنین فضایی، یک کنش واحد می‌تواند به‌طور هم‌زمان در چندین کشور اثر حقوقی ایجاد کند. برای مثال، ذخیره‌سازی داده در یک کشور، پردازش آن در کشور دیگر و استفاده از آن در کشور سوم، موجب می‌شود که تعیین صلاحیت قضایی و قانونی با پیچیدگی‌های اساسی روبه‌رو شود. در نتیجه، مفهوم سنتی صلاحیت سرزمینی که بر مکان‌محور بودن رفتار حقوقی استوار است، با چالش‌های جدی مواجه شده و نیازمند بازتعریف در چارچوب‌های نوین حقوقی است.ضرورت انجام این پژوهش از آنجا ناشی می‌شود که تعارض صلاحیت دولت‌ها در فضای سایبر صرفاً یک بحث نظری یا دانشگاهی نیست، بلکه پیامدهای عملی گسترده‌ای در حوزه امنیت ملی، اقتصاد دیجیتال، تجارت بین‌الملل و حقوق بشر دارد. دولت‌ها در مواجهه با جرایم سایبری، نقض داده‌ها و فعالیت‌های فرامرزی، اغلب با وضعیت‌هایی روبه‌رو می‌شوند که در آن چندین نظام حقوقی به‌طور هم‌زمان ادعای صلاحیت دارند. این وضعیت نه تنها موجب تداخل در اعمال قوانین می‌شود، بلکه در برخی موارد به عدم اجرای مؤثر عدالت و ایجاد خلأهای حقوقی منجر می‌گردد. از این رو، تحلیل دقیق این تعارض‌ها و ارائه چارچوب‌های نظری برای مدیریت آن‌ها از اهمیت ویژه‌ای برخوردار است.در ادبیات موجود، موضوع حاکمیت داده و صلاحیت سایبری از زوایای مختلف مورد بررسی قرار گرفته است. در میان منابع فارسی، «جعفری» در مقاله‌ای با عنوان «حاکمیت بر فضای سایبر از منظر حقوق بین‌الملل و نظام حقوقی ایران» به این نتیجه می‌رسد که فضای سایبر موجب بازتعریف مفهوم حاکمیت شده و دولت‌ها ناگزیر به پذیرش اشکال جدیدی از اعمال اقتدار در محیط دیجیتال هستند (جعفری، ۱۳۹۸، ص. ۱۱۴). این پژوهش بر نقش دولت در تنظیم فضای سایبر تأکید دارد و بیشتر رویکردی حاکمیت‌محور ارائه می‌دهد.در مقابل، در ادبیات انگلیسی، «Chander & Sun» در اثر خود با عنوان " Data Sovereignty: From the Digital Silk Road to the Return of the State" نشان می‌دهند که دولت‌ها در واکنش به جهانی‌شدن داده، به سمت بازپس‌گیری کنترل بر زیرساخت‌های اطلاعاتی حرکت کرده‌اند، اما این روند با محدودیت‌های ساختاری اقتصاد دیجیتال جهانی و وابستگی متقابل شبکه‌ای مواجه است (Chander & Sun, 2023, p. 42). این دیدگاه بیشتر بر تنش میان حاکمیت ملی و ساختار جهانی داده تمرکز دارد و نقش بازیگران فراملی را برجسته می‌سازد.

با وجود این مطالعات، خلأهای مهمی در ادبیات موجود مشاهده می‌شود. نخست آنکه بسیاری از پژوهش‌ها یا صرفاً بر حاکمیت دولت‌ها تمرکز دارند یا تنها به جریان آزاد داده‌ها می‌پردازند، بدون آنکه تعارض میان این دو را به‌صورت نظام‌مند تحلیل کنند. دوم آنکه کمتر پژوهشی به‌صورت هم‌زمان سه سطح تحلیل حقوق بین‌الملل، ساختارهای فراملی داده و نظام حقوق داخلی را در کنار یکدیگر بررسی کرده است. سوم آنکه در مطالعات موجود، کمتر به مسئله «مدیریت تعارض صلاحیت‌ها» به‌عنوان یک مسئله مستقل و ساختاری پرداخته شده است.تمایز اصلی پژوهش حاضر در همین نقطه آشکار می‌شود. این پژوهش صرفاً به توصیف وضعیت موجود یا تحلیل کلی حاکمیت داده بسنده نمی‌کند، بلکه تلاش می‌کند تعارض صلاحیت دولت‌ها را به‌عنوان

مسئله مرکزی شناسایی کرده و آن را در چارچوبی تحلیلی و چندسطحی بررسی کند. علاوه بر این، این پژوهش سعی دارد میان منطق سرزمینی حقوق کلاسیک و منطق شبکه‌ای فضای سایبر پیوند تحلیلی برقرار کرده و الگویی برای مدیریت این دوگانه ارائه دهد.در نهایت، فرضیه اصلی این پژوهش چنین قابل صورت‌بندی است: هرچه میزان فرامرزی بودن جریان داده‌ها و وابستگی ساختاری دولت‌ها به زیرساخت‌های دیجیتال جهانی افزایش یابد، کارآمدی صلاحیت سرزمینی کلاسیک کاهش یافته و ضرورت حرکت به سمت الگوهای ترکیبی صلاحیتی مبتنی بر همکاری بین‌المللی، تنظیم‌گری چندسطحی و حاکمیت داده‌محور افزایش می‌یابد.این فرضیه تلاش دارد رابطه میان تحول فناوری و تحول حقوقی را در حوزه صلاحیت دولت‌ها تبیین کند و نشان دهد که آینده حقوق بین‌الملل در این حوزه ناگزیر به سمت الگوهای منعطف‌تر و شبکه‌ای‌تر حرکت خواهد کرد.

۱.تحول مبانی حاکمیت دولت در عصر داده‌محور

حاکمیت دولت در ادبیات کلاسیک حقوق بین‌الملل بر یک منطق سرزمینی استوار بوده است؛ منطقی که در آن، مرزهای جغرافیایی معیار اصلی تعیین حدود صلاحیت و اعمال اقتدار عمومی محسوب می‌شدند. در این چارچوب، دولت به‌عنوان یگانه مرجع تنظیم‌کننده در قلمرو خود شناخته می‌شد و کنترل بر اشخاص، اموال و رفتارها درون مرزهای سرزمینی تعریف می‌گردید. با ورود فضای سایبر، این بنیان سنتی با چالش جدی مواجه شده است، زیرا داده و جریان اطلاعات قابلیت تثبیت در یک قلمرو واحد را ندارند و ماهیت آن‌ها ذاتاً فرامرزی است (Choucri & Clark, 2019, 44).در سطح ساختاری، ظهور زیرساخت‌های دیجیتال جهانی و کنشگران فراملی موجب شده است که دولت دیگر تنها بازیگر تعیین‌کننده در تنظیم جریان قدرت نباشد. پلتفرم‌های بزرگ فناوری، ارائه‌دهندگان خدمات ابری و شبکه‌های ارتباطی خصوصی به‌گونه‌ای عمل می‌کنند که عملاً در فرآیند تنظیم و کنترل داده نقش مؤثر و گاه هم‌عرض دولت‌ها پیدا کرده‌اند. این وضعیت موجب شده است که اقتدار عمومی از یک ساختار متمرکز و سلسله‌مراتبی به یک ساختار شبکه‌ای و چندمرکزی تبدیل شود که در آن قدرت میان دولت و بازیگران خصوصی توزیع شده است (Benkler, 2006, 23).ازمنظر حقوقی، این تحول به معنای تضعیف تدریجی پیوند میان سرزمین و صلاحیت است. در فضای سایبر، یک کنش واحد ممکن است در چندین حوزه قضایی تولید، پردازش و اثرگذاری داشته باشد، بدون آنکه بتوان آن را به یک قلمرو مشخص محدود کرد. این ویژگی باعث شده است که معیارهای سنتی حقوق بین‌الملل در تعیین محل وقوع فعل حقوقی ناکافی شوند و تعارض میان صلاحیت‌های ملی افزایش یابد (Maurer, 2016, 392).

تحول مبانی حاکمیت نشان می‌دهد که دولت‌ها در عصر داده‌محور همچنان نقش مرکزی دارند، اما این نقش از انحصارگر اقتدار به تنظیم‌کننده‌ای در یک محیط پیچیده و شبکه‌ای تغییر یافته است. در این الگو، حاکمیت دیگر یک مفهوم ایستا و سرزمینی نیست، بلکه به یک فرآیند پویا و وابسته به جریان‌های داده‌ای و تعامل میان دولت‌ها و بازیگران فراملی تبدیل شده است.در دگرگونی حاکمیت در عصر داده‌محور، باید توجه داشت که مسئله صرفاً تغییر ابزارهای حکمرانی نیست، بلکه تغییر در «منطق تولید و اعمال اقتدار» است. در الگوی کلاسیک، حاکمیت بر کنترل سرزمین و اعمال اقتدار انحصاری در مرزهای مشخص استوار بود، اما در فضای سایبر، محور اصلی قدرت به کنترل جریان داده و معماری اطلاعاتی منتقل شده است. این انتقال موجب شده است که توان دولت‌ها در اعمال حاکمیت بیش از آنکه به مرزهای جغرافیایی وابسته باشد، به ظرفیت فنی و حقوقی آن‌ها در مدیریت داده‌ها وابسته شود.در این چارچوب، نقش بازیگران غیر دولتی به‌ویژه شرکت‌های فناوری و پلتفرم‌های دیجیتال به‌طور چشمگیری افزایش یافته است. این بازیگران در عمل بخشی از کارکردهای تنظیمی دولت را در حوزه دسترسی، پردازش و توزیع داده بر عهده گرفته‌اند و به همین دلیل، ساختار قدرت از حالت سلسله‌مراتبی سنتی به یک وضعیت شبکه‌ای و چندمرکزی تغییر یافته است. نتیجه این وضعیت، شکل‌گیری نوعی حاکمیت تقسیم‌شده است که در آن دولت دیگر تنها مرجع انحصاری تنظیم رفتارها نیست .از منظر حقوقی، این تحول باعث بازتعریف تدریجی مفهوم صلاحیت شده است. در فضای سایبر، کنش‌ها معمولاً در یک نقطه واحد رخ نمی‌دهند، بلکه در فرآیندهای توزیع‌شده میان چندین حوزه قضایی شکل می‌گیرند. همین ویژگی موجب شده است که تفکیک سنتی میان صلاحیت سرزمینی و فرامرزی با دشواری مواجه شود و

تعارض میان نظام‌های حقوقی ملی افزایش یابد. در نتیجه، چارچوب‌های کلاسیک حقوق بین‌الملل در توضیح این وضعیت کارایی محدودتری پیدا کرده‌اند (Maurer, 2016, 392).در نهایت، تحول مبانی حاکمیت نشان می‌دهد که دولت در عصر داده‌محور نه حذف شده و نه تضعیف مطلق یافته است، بلکه در حال بازآرایی در قالبی جدید است. این بازآرایی، حاکمیت را از یک مفهوم ایستا و سرزمینی به یک فرآیند پویا و شبکه‌ای تبدیل کرده است که در آن، قدرت میان دولت، فناوری و بازیگران فراملی به‌صورت مستمر در حال جابه‌جایی است.

۲.فرسایش اصل سرزمینی بودن صلاحیت در فضای سایبر

اصل سرزمینی بودن صلاحیت در حقوق بین‌الملل کلاسیک بر این مبنا استوار است که دولت در محدوده قلمرو جغرافیایی خود، اختیار اعمال اقتدار عمومی و تنظیم رفتارهای واقع‌شده در آن قلمرو را دارد. این اصل در محیط فیزیکی، به دلیل امکان نسبتاً روشن تعیین محل وقوع فعل و آثار آن، مبنایی منسجم برای تعیین قلمرو صلاحیت دولت‌ها محسوب می‌شد. بااین‌حال، ظهور فضای سایبر و گسترش جریان فرامرزی داده‌ها، رابطه سنتی میان «محل وقوع رفتار»، «قلمرو دولت» و «صلاحیت» را با چالش مواجه کرده است. یک رفتار سایبری ممکن است در یک کشور آغاز شود، از زیرساخت‌های ارتباطی واقع در کشور دیگر عبور کند، در قلمرو دولت ثالث پردازش یا ذخیره شود و آثار آن در کشور دیگری تحقق یابد. در چنین وضعیتی، تعیین یک نقطه جغرافیایی واحد به‌عنوان محل وقوع رفتار دشوار شده و زمینه برای اعمال هم‌زمان صلاحیت چند دولت فراهم می‌شود (Choucri & Clark, 2019, p. 88).این وضعیت به معنای زوال اصل سرزمینی بودن صلاحیت نیست، بلکه نشان‌دهنده کاهش کفایت آن به‌عنوان تنها معیار تعیین صلاحیت تقنینی است. در محیط سایبر، عناصر تشکیل‌دهنده یک رفتار ممکن است در چند قلمرو توزیع شوند و در نتیجه، ارتباط میان رفتار و سرزمین دیگر رابطه‌ای ساده و یک‌بعدی نباشد. برای نمونه، محل ارسال و دریافت داده، محل استقرار کاربر یا ارائه‌دهنده خدمت، محل استقرار زیرساخت پردازشی و محل تحقق آثار اقتصادی یا حقوقی رفتار ممکن است متفاوت باشد. ازاین‌رو، تعیین صلاحیت تقنینی دولت نیازمند ارزیابی مجموعه‌ای از پیوندهای واقعی میان رفتار و قلمرو است.این پیچیدگی با توسعه رایانش ابری، ذخیره‌سازی توزیع‌شده و شبکه‌های توزیع محتوا تشدید شده است. داده‌ها در چنین ساختارهایی الزاماً در یک مکان ثابت باقی نمی‌مانند و ممکن است به‌صورت پویا میان مراکز داده واقع در حوزه‌های قضایی مختلف منتقل یا پردازش شوند. در نتیجه، مفهوم «محل استقرار داده» دیگر به‌تنهایی نمی‌تواند معیار مناسبی برای تعیین صلاحیت باشد و همین امر احتمال تعارض میان قوانین دولت‌های مختلف را افزایش می‌دهد (Maurer, 2018, p. 61).باوجوداین، فرامرزی بودن فضای سایبر نباید به کنار گذاشتن معیار سرزمینی منجر شود. وجود یک عنصر واقعی و معنادار در قلمرو دولت همچنان می‌تواند مبنای اعمال قانون آن دولت باشد. تحقق بخشی از رفتار یا نتیجه در قلمرو یک کشور، فعالیت یک سامانه یا زیرساخت در آن قلمرو و یا تحقق آثار مستقیم و قابل توجه رفتار در آنجا، از جمله عواملی هستند که می‌توانند در احراز این ارتباط مؤثر باشند. در حقوق ایران نیز این رویکرد در قلمرو حقوق کیفری قابل مشاهده است. قانون مجازات اسلامی، در کنار پذیرش اصل سرزمینی، در تعیین قلمرو اجرای قوانین کیفری به وضعیت‌هایی توجه کرده است که بخشی از رفتار یا نتیجه جرم در قلمرو ایران تحقق می‌یابد. ماده ۴ قانون مجازات اسلامی از این حیث اهمیت دارد؛ زیرا قلمرو اعمال قانون کیفری ایران را به مواردی که تمام یا بخشی از جرم یا نتیجه آن در ایران واقع شده باشد، تسری می‌دهد. این منطق در فضای سایبر اهمیت ویژه‌ای پیدا می‌کند؛ زیرا ممکن است بخشی از فرآیند ارتکاب در خارج از ایران و نتیجه یا بخشی از عناصر آن در داخل کشور تحقق یابد.

در کنار این مبنای سرزمینی، حقوق ایران در موارد خاص، ارتباط رفتار با منافع اساسی دولت را نیز در تعیین قلمرو اعمال قانون مورد توجه قرار داده است. ماده ۵ قانون مجازات اسلامی نسبت به برخی جرایم ارتکابی در خارج از قلمرو ایران که علیه نظام، امنیت داخلی یا خارجی، تمامیت ارضی یا استقلال جمهوری اسلامی ایران واقع شده‌اند، امکان اعمال قانون کیفری ایران را پیش‌بینی کرده است. اهمیت این حکم در بحث حاضر آن است که نشان می‌دهد ارتباط میان رفتار و دولت الزاماً به حضور

فیزیکی رفتار در قلمرو محدود نیست و در مواردی، ماهیت و آثار رفتار نسبت به منافع اساسی دولت می‌تواند مبنای اعمال قانون قرار گیرد. این مبنا در فضای سایبر، که یک رفتار واحد می‌تواند بدون حضور فیزیکی مرتکب در قلمرو کشور، آثار قابل توجهی بر امنیت یا منافع اساسی آن داشته باشد، اهمیت مضاعفی پیدا می‌کند.البته استناد به این مقررات داخلی نباید به معنای یکسان دانستن صلاحیت کیفری داخلی با صلاحیت تقنینی دولت‌ها در حقوق بین‌الملل تلقی شود. اهمیت آنها در این بحث، نشان دادن این واقعیت است که حتی در نظام حقوقی ایران نیز تعیین قلمرو اعمال قانون صرفاً بر مبنای محل فیزیکی حضور مرتکب صورت نمی‌گیرد و در کنار پیوند سرزمینی، عناصر دیگری مانند محل تحقق نتیجه و ارتباط رفتار با منافع اساسی کشور مورد توجه قرار گرفته‌اند. از این منظر، حقوق داخلی ایران می‌تواند نمونه‌ای از حرکت از برداشت صرفاً مکانی از صلاحیت به سوی الگوی مبتنی بر پیوندهای واقعی و حقوقی میان رفتار و دولت تلقی شود.در کنار معیار سرزمینی، ماهیت فرامرزی فضای سایبر توجه به صلاحیت شخصی و صلاحیت واقعی را نیز ضروری می‌سازد. صلاحیت شخصی می‌تواند بر مبنای تابعیت یا وضعیت حقوقی اشخاص مرتبط با رفتار اعمال شود و صلاحیت واقعی نیز در مواردی مطرح می‌شود که رفتار خارج از قلمرو دولت واقع شده، اما به دلیل ارتباط با منافع اساسی آن دولت، قابلیت ایجاد صلاحیت دارد. بنابراین، فرامرزی بودن رفتار سایبری به‌خودی‌خود موجب خروج آن از قلمرو صلاحیت دولت‌ها نمی‌شود؛ بلکه ضرورت شناسایی و ارزیابی مبنای ارتباط دولت با رفتار را افزایش می‌دهد.از این منظر، تحول فضای سایبر را باید نه به‌عنوان پایان صلاحیت سرزمینی، بلکه به‌عنوان فرسایش انحصار معیار سرزمینی تحلیل کرد. سرزمین همچنان یکی از مبانی اصلی صلاحیت دولت است، اما در محیط داده‌محور، کفایت آن به وجود ارتباط واقعی و معنادار با رفتار وابسته است. این ارتباط می‌تواند از طریق محل وقوع یا آثار رفتار، تابعیت اشخاص مرتبط، موقعیت زیرساخت یا ارتباط رفتار با منافع اساسی دولت شکل گیرد. در نتیجه، معیار سرزمینی در فضای سایبر از یک معیار مستقل و غالب، به یکی از عناصر یک الگوی چندمبنایی برای اعمال صلاحیت تقنینی تبدیل می‌شود .بدین‌ترتیب، چالش اصلی فضای سایبر جایگزین کردن کامل صلاحیت سرزمینی با معیارهای جدید نیست؛ بلکه ایجاد توازن میان صلاحیت سرزمینی، شخصی و واقعی است. چنین رویکردی ضمن حفظ اقتدار دولت در تنظیم فعالیت‌های داده‌محور، از توسعه نامحدود صلاحیت بر مبنای صرف وجود یک ارتباط فنی یا جغرافیایی نیز جلوگیری می‌کند و زمینه را برای مدیریت تعارض میان صلاحیت‌های تقنینی دولت‌ها فراهم می‌سازد.

۳.تعارض صلاحیت‌های ملی در دسترسی فرامرزی به داده‌ها و بازتوزیع اقتدار

فرسایش اصل سرزمینی بودن صلاحیت در فضای سایبر، در مرحله‌ای عمیق‌تر، خود را در تعارض میان صلاحیت‌های ملی نسبت به داده‌های فرامرزی نشان می‌دهد. در نظام سنتی حقوق بین‌الملل، قلمرو مهم‌ترین مبنای اعمال صلاحیت دولت محسوب می‌شد؛ زیرا میان محل وقوع رفتار، قلمرو دولت و امکان اعمال اقتدار عمومی رابطه‌ای نسبتاً روشن وجود داشت. بااین‌حال، در فضای سایبر این رابطه خطی و یک‌سویه با چالش مواجه شده است. یک رفتار واحد ممکن است در کشوری آغاز شود، داده‌های مربوط به آن در کشور دیگری پردازش یا ذخیره شود، ارائه‌دهنده خدمت در کشور ثالث مستقر باشد و آثار حقوقی یا اقتصادی آن در کشور دیگری تحقق یابد. ازاین‌رو، تعیین دولت صالح دیگر صرفاً با شناسایی محل وقوع فیزیکی رفتار امکان‌پذیر نیست و باید مجموعه‌ای از پیوندهای سرزمینی، شخصی و واقعی مورد توجه قرار گیرد (Choucri & Clark, 2019, p. 88).در واقع، فضای سایبر موجب حذف معیار سرزمینی نشده، بلکه مفهوم ارتباط سرزمینی را پیچیده و چندلایه کرده است. موقعیت سرور، محل استقرار ارائه‌دهنده خدمت، محل اقامت یا تابعیت کاربر، محل تحقق آثار رفتار، محل هدف‌گیری فعالیت و میزان ارتباط آن با منافع اساسی دولت، همگی می‌توانند در ایجاد یک رابطه صلاحیتی مؤثر باشند. بنابراین، مسئله اصلی در صلاحیت سایبری یافتن یک «مکان» واحد برای رفتار نیست، بلکه تعیین مهم‌ترین و واقعی‌ترین رابطه میان فعالیت داده‌محور و دولت مدعی صلاحیت است. این تحول با روندهای جدید حکمرانی داده نیز هماهنگ است؛ زیرا افزایش مقررات ملی درباره

انتقال، ذخیره و پردازش داده، هم‌زمان با تلاش دولت‌ها برای حفظ امنیت، حریم خصوصی و منافع اقتصادی، موجب گسترش حوزه‌های هم‌پوشان تنظیم‌گری شده است (OECD/WTO, 2025, pp. 15–18).

در این زمینه، تفکیک میان صلاحیت تقنینی، قضایی و اجرایی اهمیت اساسی دارد. صلاحیت تقنینی ناظر بر اختیار دولت برای وضع قواعد الزام‌آور است؛ صلاحیت قضایی به اختیار مراجع قضایی برای رسیدگی و اتخاذ تصمیم مربوط می‌شود و صلاحیت اجرایی به امکان اعمال مستقیم قدرت عمومی برای اجرای قانون اختصاص دارد. در فضای سایبر ممکن است یک دولت بر اساس وجود ارتباط واقعی با فعالیت، صلاحیت تقنینی یا قضایی خود را توجیه کند، اما این امر الزاماً به معنای برخورداری از اختیار اجرای مستقیم تصمیم خود در قلمرو دولت دیگر نیست. به بیان دیگر، وجود صلاحیت قانونی با امکان اعمال فیزیکی یا فنی آن صلاحیت یکسان نیست. نادیده گرفتن این تمایز می‌تواند موجب خلط میان توسعه صلاحیت تقنینی و مداخله اجرایی فرامرزی شود؛ درحالی‌که مسئله اصلی این پژوهش، تحول مبانی صلاحیت و اقتدار دولت در مواجهه با جریان فرامرزی داده است.تحولات حقوقی اتحادیه اروپا نمونه روشنی از فاصله گرفتن از برداشت صرفاً جغرافیایی از صلاحیت است. مطابق ماده ۳ مقررات عمومی حفاظت از داده اتحادیه اروپا، در شرایط مقرر، حتی پردازش داده اشخاص واقع در اتحادیه توسط اشخاص مستقر خارج از آن نیز می‌تواند مشمول مقررات قرار گیرد؛ مشروط بر اینکه فعالیت با عرضه کالا یا خدمات به این اشخاص یا نظارت بر رفتار آنان ارتباط داشته باشد (European Parliament & Council of the European Union, 2016). در اینجا، محل استقرار پردازشگر تنها عنصر تعیین‌کننده نیست، بلکه موقعیت شخص و ارتباط فعالیت با قلمرو حمایتی اتحادیه نیز مبنای اعمال مقررات قرار می‌گیرد. بنابراین، صلاحیت از یک رابطه صرفاً مکانی به رابطه‌ای کارکردی و مبتنی بر ارتباط واقعی تبدیل شده است.

این تحول از حیث نظری اهمیت زیادی دارد؛ زیرا نشان می‌دهد که سرزمین همچنان مبنای اصلی صلاحیت باقی می‌ماند، اما مفهوم سرزمین دیگر صرفاً به محدوده فیزیکی مرزها خلاصه نمی‌شود. آنچه اهمیت پیدا می‌کند، وجود پیوندی معنادار میان فعالیت و جامعه یا منافع تحت حمایت دولت است. به همین دلیل، اعمال صلاحیت بر فعالیتی که خارج از قلمرو دولت انجام می‌شود، در صورتی می‌تواند توجیه‌پذیر باشد که آثار، مخاطبان، بازار یا منافع اساسی آن به‌طور واقعی با دولت مربوط ارتباط داشته باشد. در غیر این صورت، توسعه صلاحیت می‌تواند به ادعای صلاحیت نامحدود و در نهایت به تعارض میان نظام‌های حقوقی منجر شود.در حقوق ایالات متحده نیز قانون مصوب سال ۲۰۱۸ درباره دسترسی به داده‌های ذخیره‌شده در خارج از کشور، رویکرد متفاوتی را در پیش گرفته است. بر اساس این چارچوب، در موارد مقرر، ارائه‌دهنده خدماتی که تحت صلاحیت ایالات متحده قرار دارد ممکن است مکلف به ارائه داده‌هایی باشد که در اختیار، حضانت یا کنترل او قرار دارد، حتی اگر داده از نظر فیزیکی خارج از ایالات متحده نگهداری شود (U.S. Department of Justice, 2019).این قانون همچنین برای برخی فرایندهای مرتبط با ارسال و دریافت داده‌پیام، قواعد خاصی مقرر کرده است که نشان می‌دهد تحقق آثار حقوقی ارتباط الکترونیکی الزاماً به یک مکان فیزیکی واحد وابسته نیست (قانون تجارت الکترونیکی، ۱۳۸۲).از سوی دیگر، قانون جرایم رایانه‌ای در ماده ۲۸، در تعیین صلاحیت دادگاه‌های ایران، برخی پیوندهای مربوط به داده و زیرساخت را مورد توجه قرار داده است. وجود داده‌های مجرمانه یا داده‌های مورد استفاده برای ارتکاب جرم در سامانه‌ها یا حامل‌های داده موجود در قلمرو ایران و برخی ارتباطات مرتبط با زیرساخت‌های ایرانی می‌تواند در تعیین صلاحیت مورد توجه قرار گیرد (قانون جرایم رایانه‌ای، ۱۳۸۸). این حکم نشان می‌دهد که در حقوق داخلی نیز ارتباط سایبری با قلمرو الزاماً به محل حضور فیزیکی مرتکب محدود نیست و داده و زیرساخت می‌توانند در ایجاد رابطه صلاحیتی مؤثر باشند.

بااین‌حال، ماده ۲۸ قانون جرایم رایانه‌ای را نباید بدون تفکیک مفهومی، مبنای پذیرش صلاحیت تقنینی نامحدود ایران دانست. این ماده در درجه نخست در قلمرو صلاحیت قضایی کیفری قابل تحلیل است و نمی‌توان از آن نتیجه گرفت که ایران در هر موردی که داده یا سامانه‌ای به نحوی با قلمرو کشور ارتباط داشته باشد، حق اعمال یک‌جانبه اقتدار اجرایی در خارج از

قلمرو خود را دارد. چنین تفکیکی برای جلوگیری از همان ایرادی ضروری است که در تحلیل‌های مربوط به صلاحیت سایبری گاه مشاهده می‌شود؛ یعنی یکی دانستن صلاحیت تقنینی، قضایی و اجرایی.از منظر حقوق داخلی، بنابراین می‌توان گفت که قانونگذار ایرانی اصل ارتباط داده و زیرساخت با صلاحیت را پذیرفته است، اما توسعه این ارتباط باید با اصول کلی حاکم بر صلاحیت دولت و ملاحظات حقوق بین‌الملل همراه باشد. به‌ویژه در مواردی که داده در اختیار شخص یا شرکتی خارج از ایران قرار دارد، اعمال مستقیم اقتدار ایران در خارج از قلمرو نمی‌تواند صرفاً بر وجود یک ارتباط فنی استوار شود. در چنین مواردی، استفاده از سازوکارهای همکاری بین‌المللی، درخواست قضایی، همکاری ارائه‌دهندگان خدمات و توافق‌های بین‌دولتی، راهکار حقوقی منسجم‌تری خواهد بود.از این منظر، مسئله اصلی تعارض صلاحیت‌ها در فضای سایبر را باید در تفاوت میان حق تنظیم رفتار و توانایی اجرای مستقیم قانون جست‌وجو کرد. دولت‌ها ممکن است بر اساس معیارهای مختلف، خود را صالح به وضع قواعد درباره یک فعالیت بدانند، اما اجرای آن قواعد نسبت به داده یا زیرساختی که در قلمرو دولت دیگر قرار دارد، نیازمند ملاحظات جداگانه‌ای است. این تفکیک از توسعه بی‌ضابطه صلاحیت جلوگیری می‌کند و امکان می‌دهد که صلاحیت تقنینی دولت در عین حفظ ارتباط با منافع ملی، با اصل احترام به حاکمیت سایر دولت‌ها نیز سازگار باقی بماند.از سوی دیگر، افزایش مقررات ملی درباره جریان داده، اگر بدون هماهنگی میان دولت‌ها صورت گیرد، می‌تواند به چندپارگی حقوقی منجر شود. یک دولت ممکن است انتقال داده را برای حفاظت از حریم خصوصی محدود کند، دولت دیگر ارائه همان داده را برای اجرای قانون الزامی بداند و دولت سوم، ذخیره‌سازی داده را در قلمرو خود شرط کند. در نتیجه، یک فعالیت اقتصادی یا ارتباطی واحد ممکن است هم‌زمان با الزامات حقوقی متعارض مواجه شود. گزارش مشترک سازمان همکاری اقتصادی و توسعه و سازمان تجارت جهانی در سال ۲۰۲۵ نیز بر همین چالش تأکید کرده و نشان می‌دهد که مقررات داده‌ای، ضمن پاسخ به اهداف مشروعی مانند حفاظت از حریم خصوصی و امنیت، در صورت عدم هماهنگی می‌توانند بر جریان‌های فرامرزی داده و فعالیت‌های اقتصادی اثر بگذارند (OECD/WTO, 2025, pp. 15–18).بنابراین، معیار مناسب برای تعیین حدود صلاحیت در فضای سایبر را نمی‌توان صرفاً «محل ذخیره داده» یا «امکان فنی دسترسی» دانست. معیار دقیق‌تر، وجود ارتباط واقعی، معنادار و متناسب میان فعالیت مورد تنظیم و دولت مدعی صلاحیت است. این ارتباط می‌تواند از طریق محل تحقق آثار، موقعیت اشخاص، بازار هدف، تابعیت، ارتباط با منافع اساسی یا کنترل حقوقی بر ارائه‌دهنده خدمت شکل گیرد؛ اما هیچ‌یک از این عناصر نباید به‌صورت مطلق و مستقل از سایر شرایط اعمال شود. ترکیب این عوامل است که می‌تواند مبنای مشروع و متناسبی برای تعیین حدود صلاحیت ایجاد کند.بر همین اساس، بازتوزیع اقتدار در فضای داده‌محور را نباید به معنای تضعیف مطلق دولت دانست. برعکس، دولت همچنان مهم‌ترین بازیگر حقوقی در تنظیم فضای سایبر است، اما اقتدار آن از قالب سنتی و مستقیم خارج شده و به شکل شبکه‌ای و مبتنی بر همکاری اعمال می‌شود. دولت برای تحقق اهداف تنظیمی خود به ارائه‌دهندگان خدمات، زیرساخت‌های دیجیتال و سازوکارهای همکاری بین‌المللی متکی است. بنابراین، حاکمیت داده جایگزین حاکمیت دولت نشده، بلکه ابزارها و شرایط اعمال آن را دگرگون کرده است.در نهایت، تعارض صلاحیت‌های ملی در دسترسی فرامرزی به داده را باید نتیجه هم‌زمان دو تحول دانست: نخست، سیال و چندقلمروی شدن داده و دوم، توزیع ظرفیت عملی کنترل داده میان دولت‌ها و بازیگران خصوصی. پیامد این تحول آن است که صلاحیت دولت‌ها دیگر نمی‌تواند تنها بر مرز جغرافیایی استوار باشد، اما در مقابل، توسعه صلاحیت فرامرزی نیز نمی‌تواند بدون محدودیت پذیرفته شود. راهکار متوازن، پذیرش صلاحیت بر مبنای ارتباط واقعی و اثرگذاری قابل توجیه، تفکیک دقیق صلاحیت تقنینی از قضایی و اجرایی، و در نهایت حرکت از رقابت صلاحیتی به سمت همکاری صلاحیتی است. در چنین چارچوبی، هم اقتدار دولت برای تنظیم فضای داده‌محور حفظ می‌شود و هم از تبدیل فضای سایبر به عرصه‌ای برای ادعاهای هم‌زمان و نامحدود دولت‌ها جلوگیری خواهد شد.

۴.چالش‌های انتساب و اعمال صلاحیت و رویکردهای نوین دولت‌ها در صیانت از حاکمیت داده

در محیط‌های غیرمتمرکز سایبری، تحول معماری شبکه و توزیع فرایندهای تولید، انتقال، پردازش و ذخیره‌سازی اطلاعات، مبانی سنتی انتساب و اعمال صلاحیت دولت‌ها را با چالش جدی مواجه ساخته است. در نظام حقوقی سنتی، شناسایی محل وقوع فعل، هویت مرتکب و محل تحقق نتیجه، امکان نسبت دادن رفتار به شخص و تعیین دولت صالح را تا حد زیادی فراهم می‌کرد؛ اما در فضای سایبر، یک رفتار واحد می‌تواند از یک قلمرو آغاز شود، از زیرساخت‌های مستقر در چند کشور عبور کند، در مراکز داده مختلف پردازش شود و آثار آن در قلمرو دولت دیگری ظاهر گردد. در نتیجه، میان «محل ارتکاب»، «محل پردازش»، «محل ذخیره‌سازی» و «محل تحقق اثر» الزاماً وحدت وجود ندارد و همین گسست مکانی، مبنای سرزمینی صلاحیت را با محدودیت مواجه می‌کند (Choucri & Clark, 2019, p. 88). این وضعیت در شبکه‌های غیرمتمرکز شدت بیشتری دارد؛ زیرا داده الزاماً تحت کنترل یک نقطه مرکزی قرار ندارد و ممکن است میان گره‌ها و زیرساخت‌های متعدد توزیع شود. در چنین ساختاری، تعیین نقطه آغازین کنش و انتساب آن به یک شخص، سازمان یا دولت مشخص، صرفاً از طریق شناسایی یک نشانی فنی یا یک محل فیزیکی امکان‌پذیر نیست و نیازمند بررسی مجموعه‌ای از قرائن فنی و حقوقی است. استفاده از رمزگذاری، مسیرهای چندلایه انتقال داده و سامانه‌های ناشناس‌ساز نیز امکان ردیابی مستقیم جریان اطلاعات را کاهش داده و موجب شده است که داده نه به‌عنوان یک موضوع ایستا، بلکه به‌عنوان عنصری سیال و متحرک در شبکه تحلیل شود (Andress & Winterfeld, 2013, p. 88). از همین رو، انتساب رفتار سایبری باید میان «انتساب فنی» و «انتساب حقوقی» تفکیک قائل شود؛ زیرا شناسایی منشأ فنی یک ارتباط، لزوماً به معنای اثبات مسئولیت حقوقی شخص یا دولت مرتبط با آن نیست. در موارد پیچیده، ممکن است زیرساخت مورد استفاده متعلق به شخص ثالث باشد، مسیر انتقال داده از چند کشور عبور کند و ابزار حمله نیز از سامانه‌ای استفاده کند که مالک آن از فعالیت مجرمانه یا خصمانه اطلاعی نداشته است. بنابراین، صرف وجود ارتباط فنی میان یک فعالیت و قلمرو یک دولت نمی‌تواند به‌تنهایی برای ایجاد مسئولیت یا صلاحیت کافی باشد و باید میان میزان کنترل، ارتباط واقعی و نقش مؤثر هر عامل در شکل‌گیری نتیجه تمایز قائل شد (Bateman et al., 2022, p. 4). پیامد مستقیم این وضعیت، دشوار شدن تعیین صلاحیت است؛ زیرا هرگاه عناصر مختلف یک رفتار سایبری در چند قلمرو پراکنده باشند، بیش از یک دولت می‌تواند با استناد به یکی از این عناصر، صلاحیت خود را مطرح کند. یک دولت ممکن است به محل تحقق اثر استناد کند، دولت دیگر به تابعیت یا اقامت شخص، دولت ثالث به محل استقرار زیرساخت و دولت دیگر به ارتباط فعالیت با منافع اساسی خود. چنین وضعیتی، اگر بدون اعمال معیارهای محدودکننده و اصل تناسب مدیریت شود، می‌تواند به شکل‌گیری صلاحیت‌های موازی و تعارض میان نظام‌های حقوقی منجر شود (Tobanksy, 2011, p. 41). بنابراین، تحول فضای سایبر نباید به معنای کنار گذاشتن اصل سرزمینی بودن صلاحیت تلقی شود؛ بلکه باید گفت که مفهوم ارتباط سرزمینی در این فضا از یک رابطه ساده مکانی به رابطه‌ای مرکب تبدیل شده است که در کنار سرزمین، عناصر شخصی، واقعی و اثرگذاری را نیز دربرمی‌گیرد. در این میان، معیار «اثرگذاری» نیز باید با احتیاط مورد استفاده قرار گیرد؛ زیرا پذیرش هر اثر جزئی یا غیرمستقیم به‌عنوان مبنای صلاحیت، عملاً امکان ادعای صلاحیت نامحدود را برای دولت‌ها فراهم می‌کند. اثر مورد استناد باید واقعی، قابل انتساب، قابل پیش‌بینی و از اهمیت حقوقی کافی برخوردار باشد تا بتواند مبنای موجهی برای توسعه صلاحیت محسوب شود (Choucri & Clark, 2019, p. 88). مسئله در مرحله بعد به نحوه اعمال این صلاحیت بازمی‌گردد. باید میان صلاحیت تقنینی، صلاحیت قضایی و صلاحیت اجرایی تفکیک کرد؛ زیرا ممکن است یک دولت بر اساس ارتباط واقعی میان فعالیت و منافع تحت حمایت خود، حق وضع قواعد یا رسیدگی قضایی داشته باشد، اما این امر الزاماً اختیار اجرای مستقیم تصمیمات خود در قلمرو دولت دیگر را ایجاد نمی‌کند. به‌ویژه هنگامی که دسترسی به داده مستلزم ورود به سامانه یا زیرساختی واقع در خارج از کشور باشد، اقدام مستقیم می‌تواند از حوزه اعمال صلاحیت خارج شده و با اصل احترام به حاکمیت دولت محل استقرار زیرساخت تعارض پیدا کند. ازاین‌رو، گسترش صلاحیت تقنینی نباید با توسعه صلاحیت اجرایی یکسان تلقی شود و همین تفکیک، یکی از الزامات اساسی تحلیل صلاحیت دولت‌ها در فضای سایبر است. در حقوق ایران نیز این تمایز اهمیت دارد.

قانون تجارت الکترونیکی مصوب ۱۳۸۲ با شناسایی «داده‌پیام» و تنظیم آثار حقوقی مربوط به ایجاد، ارسال، دریافت، ذخیره و پردازش آن، داده را به‌عنوان موضوع مستقل روابط حقوقی مورد شناسایی قرار داده است و از این جهت، زمینه حقوقی لازم برای مواجهه با روابط فرامرزی مبتنی بر داده را فراهم کرده است (قانون تجارت الکترونیکی، ۱۳۸۲). همچنین ماده ۲۸ قانون جرایم رایانه‌ای مصوب ۱۳۸۸ در تعیین صلاحیت دادگاه‌های ایران، برخی ارتباطات مربوط به داده و سامانه‌های رایانه‌ای را مورد توجه قرار داده و نشان می‌دهد که ارتباط یک رفتار با داده یا سامانه واقع در قلمرو ایران می‌تواند در تعیین صلاحیت قضایی مؤثر باشد (قانون جرایم رایانه‌ای، ۱۳۸۸). بااین‌حال، این حکم را نباید به معنای پذیرش صلاحیت اجرایی نامحدود تلقی کرد؛ زیرا صلاحیت قضایی برای رسیدگی با امکان اعمال مستقیم قدرت عمومی در قلمرو دولت دیگر متفاوت است. در نتیجه، حتی در مواردی که قانون داخلی مبنای صلاحیت را شناسایی کرده باشد، اعمال عملی آن نسبت به داده یا زیرساخت خارجی باید با قواعد حاکمیت سرزمینی و سازوکارهای همکاری بین‌المللی هماهنگ شود. در سطح بین‌المللی نیز همین ضرورت موجب شده است که دولت‌ها به جای اتکا به مداخله یک‌جانبه، به سمت ایجاد سازوکارهای قانونی برای دسترسی فرامرزی به داده حرکت کنند. کنوانسیون بوداپست درباره جرایم سایبری، در ماده ۳۲، دسترسی فرامرزی مستقیم به برخی داده‌های ذخیره‌شده را در شرایط مشخص پذیرفته است و بدین ترتیب میان امکان فنی دسترسی و مشروعیت حقوقی آن تمایز ایجاد می‌کند (Council of Europe, 2001). دومین پروتکل الحاقی این کنوانسیون نیز با تقویت همکاری میان دولت‌ها و ارائه‌دهندگان خدمات و تسهیل دسترسی به ادله الکترونیکی، درصدد کاهش فاصله میان محل فیزیکی داده و مرجع قانونی نیازمند آن است (Council of Europe, 2021). این تحول نشان می‌دهد که پاسخ مناسب به تعارض صلاحیت‌ها الزاماً افزایش یک‌جانبه قدرت دولت‌ها نیست، بلکه می‌تواند در قالب «همکاری صلاحیتی» و ایجاد مسیرهای قانونی و قابل پیش‌بینی برای دسترسی به داده تحقق یابد. در همین راستا، دولت‌ها در سال‌های اخیر به سمت بازطراحی ابزارهای حقوقی و نهادی برای صیانت از حاکمیت داده حرکت کرده‌اند. این رویکرد به جای تلاش برای کنترل کامل جریان اطلاعات، بر تنظیم تولید، پردازش، انتقال و ذخیره‌سازی داده و همچنین کنترل نقاط حساس زیرساختی متمرکز شده است. به این ترتیب، حاکمیت داده را می‌توان امتداد ظرفیت تنظیمی دولت در محیط دیجیتال دانست؛ ظرفیتی که از طریق قانونگذاری، تنظیم‌گری، الزامات امنیتی و همکاری بین‌المللی اعمال می‌شود، نه صرفاً از طریق کنترل فیزیکی مرزها (Chander & Sun, 2023, p. 74). یکی از مهم‌ترین نمودهای این تحول، سیاست بومی‌سازی داده و الزام به نگهداری برخی داده‌ها در داخل قلمرو ملی است. این سیاست با هدف افزایش دسترسی دولت به اطلاعات حساس، کاهش وابستگی به زیرساخت‌های خارجی و تقویت امنیت داده اتخاذ می‌شود؛ اما نمی‌توان آن را راهکاری مطلق دانست، زیرا جریان طبیعی اطلاعات در شبکه جهانی مستلزم انتقال داده میان حوزه‌های مختلف است و بومی‌سازی گسترده می‌تواند هزینه‌های اقتصادی، فنی و حقوقی قابل توجهی ایجاد کند. ازاین‌رو، رویکرد متناسب‌تر آن است که بومی‌سازی بر داده‌های حساس، زیرساخت‌های حیاتی و اطلاعاتی که ارتباط مستقیم با امنیت یا منافع اساسی کشور دارند متمرکز شود و نسبت به سایر داده‌ها از سازوکارهای انعطاف‌پذیرتر استفاده شود. در کنار بومی‌سازی، دولت‌ها به سمت ایجاد «کنترل نقطه‌ای» بر زیرساخت‌های حیاتی دیجیتال نیز حرکت کرده‌اند؛ به این معنا که به جای تلاش برای کنترل همه جریان‌های اطلاعاتی، نقاطی مانند مراکز تبادل اینترنت، مراکز داده، ارائه‌دهندگان خدمات ابری و دروازه‌های ارتباطی بین‌المللی به‌عنوان نقاط راهبردی برای اعمال سیاست‌های تنظیمی و امنیتی مورد توجه قرار می‌گیرند. چنین رویکردی امکان می‌دهد دولت بدون ایجاد اختلال کامل در جریان آزاد داده، بر بخش‌های حیاتی شبکه نظارت و الزامات حقوقی و امنیتی خود را اعمال کند (Leiter, 2020, p. 223). از منظر امنیتی نیز حاکمیت داده با مفهوم تاب‌آوری دیجیتال پیوند خورده است. توسعه زیرساخت‌های داخلی، افزایش ظرفیت‌های حفاظت از داده، تقویت امنیت سامانه‌های حیاتی و کاهش وابستگی به زیرساخت‌های خارجی، بخشی از تلاش دولت‌ها برای حفظ قابلیت اعمال اقتدار در برابر اختلالات و تهدیدهای سایبری است. بااین‌حال، افراط در این سیاست می‌تواند به قطعه‌قطعه شدن فضای اینترنت، افزایش موانع انتقال

داده و ایجاد شکاف میان شبکه‌های ملی منجر شود؛ بنابراین، حاکمیت داده زمانی کارآمد است که میان استقلال زیرساختی و حفظ پیوستگی شبکه جهانی تعادل ایجاد کند (Chander & Sun, 2023, p. 96).

در این میان، تنظیم‌گری دولت‌ها نیز از الگوی سنتی فاصله گرفته و به سمت تنظیم‌گری ترکیبی حرکت کرده است؛ به این معنا که قوانین داخلی، استانداردهای فنی، الزامات قراردادی، قواعد حفاظت از داده و توافق‌های دوجانبه و چندجانبه به‌صورت مکمل مورد استفاده قرار می‌گیرند. هدف این سازوکارها ایجاد تعادل میان حق دولت برای تنظیم فضای سایبر و ضرورت حفظ جریان‌های مشروع داده است. بنابراین، حاکمیت داده را نمی‌توان معادل کنترل مطلق دولت بر داده دانست؛ بلکه باید آن را ظرفیت دولت برای تعیین قواعد حاکم بر داده‌هایی دانست که با قلمرو، اشخاص یا منافع اساسی آن ارتباط دارند (Polčák & Svantesson, 2017, p. 118). در این چارچوب، نقش پلتفرم‌ها و شرکت‌های فناوری نیز باید به‌درستی تبیین شود. افزایش توانایی این بازیگران در نگهداری، پردازش و انتقال داده به معنای انتقال حاکمیت از دولت به بخش خصوصی نیست؛ بلکه بیانگر آن است که اجرای بسیاری از سیاست‌های عمومی در فضای دیجیتال، بدون همکاری یا تنظیم رفتار این بازیگران امکان‌پذیر نیست. دولت همچنان مرجع اصلی وضع قواعد الزام‌آور است، اما اجرای مؤثر این قواعد به ظرفیت فنی و سازمانی شرکت‌هایی وابسته شده است که زیرساخت‌های ارتباطی و اطلاعاتی را در اختیار دارند (Choucri & Clark, 2019, p. 61). بنابراین، اقتدار دولت در عصر داده‌محور از شکل مستقیم و متمرکز به شکلی شبکه‌ای، تنظیمی و همکاری‌محور تغییر یافته است. این تغییر را می‌توان در رویکردهای جدید مربوط به انتقال فرامرزی داده نیز مشاهده کرد؛ جایی که دولت‌ها از یک‌سو تلاش می‌کنند از اطلاعات اشخاص، امنیت ملی و منافع اقتصادی خود حمایت کنند و از سوی دیگر نمی‌توانند واقعیت فرامرزی بودن جریان داده را نادیده بگیرند. به همین دلیل، ایجاد رژیم‌های انتقال داده، استانداردهای حفاظت از اطلاعات و سازوکارهای همکاری میان دولت‌ها، به یکی از عناصر اصلی حاکمیت داده تبدیل شده است (Chander & Sun, 2023, p. 91). در نهایت، چالش انتساب و اعمال صلاحیت در محیط‌های غیرمتمرکز را باید در پیوند مستقیم با تحول مفهوم حاکمیت داده تحلیل کرد. هرچه جریان داده پیچیده‌تر، توزیع‌شده‌تر و فرامرزی‌تر می‌شود، امکان اتکای صرف به محل وقوع رفتار کاهش می‌یابد و دولت‌ها ناچار می‌شوند از مجموعه‌ای از معیارهای سرزمینی، شخصی، واقعی و اثرمحور استفاده کنند. در عین حال، این تحول نباید به پذیرش صلاحیت نامحدود منجر شود؛ بلکه اعمال صلاحیت باید بر وجود ارتباط واقعی، اثرگذاری قابل توجه، تناسب میان هدف و ابزار و احترام به صلاحیت سایر دولت‌ها استوار باشد. در این چارچوب، حاکمیت داده نه جایگزین حاکمیت دولت، بلکه شکل تحول‌یافته اعمال آن در محیطی است که در آن داده از مرزهای جغرافیایی عبور می‌کند و اقتدار عملی میان دولت‌ها، زیرساخت‌ها و بازیگران خصوصی توزیع شده است (Maurer, 2018, p. 73). بر این اساس، راه‌حل اصلی تعارض صلاحیت‌ها در فضای سایبر را باید نه در بازگشت به سرزمین‌محوری مطلق و نه در پذیرش صلاحیت فرامرزی نامحدود، بلکه در ترکیب صلاحیت مبتنی بر ارتباط واقعی با سازوکارهای همکاری صلاحیتی جست‌وجو کرد؛ رویکردی که ضمن حفظ توان دولت‌ها برای تنظیم و صیانت از داده، مانع تبدیل فضای سایبر به عرصه رقابت نامحدود صلاحیتی میان دولت‌ها می‌شود.

۵.جایگاه حاکمیت داده در نظام حقوق بین‌الملل معاصر

در نظام حقوق بین‌الملل معاصر، حاکمیت داده به‌عنوان امتداد تحول‌یافته مفهوم حاکمیت دولت در مواجهه با فضای سایبر مطرح شده است. این مفهوم در اصل پاسخی به جابه‌جایی مرزهای سنتی اقتدار سرزمینی در اثر جریان‌های فرامرزی اطلاعات است؛ جایی که داده دیگر در چارچوب جغرافیا محصور نیست و در شبکه‌ای جهانی بازتولید می‌شود. در چنین شرایطی، حقوق بین‌الملل با مسئله بازتعریف صلاحیت دولت‌ها در حوزه‌ای مواجه شده که هم‌زمان واجد ابعاد امنیتی، اقتصادی و حقوقی است (حافظنیا، ۱۳۹۰، ۱۲۸).در سطح نظری، حاکمیت داده در تعارض میان دو منطق بنیادین قرار دارد: منطق کلاسیک حاکمیت سرزمینی و منطق شبکه‌ای اینترنت. این تعارض سبب شده است که دولت‌ها در مواجهه با داده‌های فرامرزی، رویکردهای متفاوتی اتخاذ کنند؛ از تأکید بر کنترل داخلی داده تا پذیرش نسبی جریان آزاد اطلاعات. نتیجه این وضعیت،

شکل‌گیری یک نظم حقوقی غیرمنسجم و چندپارچه در حوزه تنظیم داده‌های بین‌المللی است که هنوز به یک قاعده واحد و الزام‌آور نرسیده است (جعفری، ۱۳۹۸، ۱۱۶).در سطح نهادی، یکی از مهم‌ترین چالش‌ها، ضعف سازوکارهای بین‌المللی در تنظیم حاکمیت داده است. در حالی که برخی اسناد و توافق‌های منطقه‌ای تلاش کرده‌اند حداقلی از هماهنگی را ایجاد کنند، اما فقدان یک رژیم جهانی جامع باعث شده است که دولت‌ها همچنان به‌صورت منفرد و بر اساس منافع ملی خود عمل کنند. این وضعیت به افزایش پراکندگی قواعد و تشدید اختلاف در اعمال صلاحیت منجر شده است (ضیایی و شکیب‌نژاد، ۱۳۹۶، ۷۱).بنابراین گسترش فضای سایبر موجب انتقال تدریجی مفهوم حاکمیت از حوزه صرفاً سرزمینی به حوزه اطلاعاتی شده است. در این چارچوب، داده به‌عنوان بخشی از زیرساخت قدرت ملی تلقی می‌شود و دولت‌ها تلاش می‌کنند با ابزارهای قانونی و سیاستی، کنترل بیشتری بر آن اعمال کنند. با این حال، این تلاش‌ها در عمل با محدودیت‌های ساختاری اینترنت و وابستگی متقابل نظام‌های دیجیتال مواجه است (کریمی قهرودی و زارعی، ۱۳۹۹، ۵۴).

یکی از مسائل تعیین‌کننده در نظام حقوق بین‌الملل، نحوه مواجهه با داده به‌عنوان موضوعی فرامرزی و غیرقابل تحدید به مرزهای سرزمینی است. این وضعیت باعث شده است که مفهوم حاکمیت داده به‌تدریج از سطح یک بحث فنی به سطح یک مسئله حقوقی-سیاسی در روابط میان دولت‌ها ارتقا یابد. در این چارچوب، دولت‌ها تلاش می‌کنند میان ضرورت کنترل اطلاعات در قلمرو خود و الزامات تعامل در فضای دیجیتال جهانی تعادل برقرار کنند (کیان‌خواه، ۱۳۹۸، ۱۶۲).در سطح امنیتی و راهبردی، داده به یکی از عناصر اصلی قدرت ملی تبدیل شده است. دولت‌ها از طریق تنظیم جریان داده، محدودسازی دسترسی‌های خارجی و توسعه زیرساخت‌های مستقل دیجیتال، در پی تقویت توان حکمرانی خود هستند. این روند نشان‌دهنده پیوند مستقیم میان امنیت ملی و حاکمیت داده است؛ به‌گونه‌ای که کنترل بر داده به‌عنوان بخشی از سیاست امنیتی دولت‌ها تلقی می‌شود (قادری‌حاجت و نصرتی، ۱۳۹۲، ۴۷).در سطح سیاست‌گذاری عمومی، گسترش فضای سایبر موجب شده است که دولت‌ها به سمت تدوین قوانین داخلی سخت‌گیرانه‌تر در حوزه مدیریت اطلاعات حرکت کنند. این قوانین معمولاً با هدف حفاظت از داده‌های حساس، کنترل جریان اطلاعات و جلوگیری از مداخله بازیگران خارجی طراحی می‌شوند. با این حال، اجرای این سیاست‌ها در عمل با محدودیت‌های ناشی از ماهیت شبکه‌ای اینترنت و وابستگی متقابل نظام‌های ارتباطی مواجه است (ضیایی و شکیب‌نژاد، ۱۳۹۶، ۷۳).در نهایت، در ادبیات تطبیقی نیز تأکید شده است که حاکمیت داده نه یک مفهوم ایستا، بلکه یک فرآیند در حال تحول است که در آن دولت‌ها به‌طور مداوم در حال بازتعریف حدود اقتدار خود هستند. این بازتعریف، تحت تأثیر هم‌زمان عوامل حقوقی، فناورانه و ژئوپلیتیکی شکل می‌گیرد و موجب می‌شود نظام حقوق بین‌الملل در این حوزه همچنان در وضعیت گذار باقی بماند .

۶.چالش‌های حقوق بشری و تعارض جریان آزاد داده با الزامات حاکمیت ملی

اعمال حاکمیت داده در فضای سایبر، اگرچه از منظر دولت‌ها ابزاری برای حفظ امنیت ملی، نظم عمومی، صیانت از زیرساخت‌های حیاتی و تقویت ظرفیت تنظیم‌گری محسوب می‌شود، در صورت فقدان ضوابط روشن و محدودیت‌های حقوقی مناسب می‌تواند به گسترش مداخلات دولت در حوزه حقوق و آزادی‌های بنیادین اشخاص منجر شود. مسئله اساسی در این زمینه آن است که داده از یک سو موضوع اعمال اقتدار عمومی و از سوی دیگر وسیله اعمال و تحقق برخی حقوق فردی است؛ بنابراین، توسعه صلاحیت دولت نسبت به داده‌های فرامرزی باید در نقطه تلاقی میان حاکمیت، امنیت و حقوق بشر ارزیابی شود. دولت از یک سو نمی‌تواند در برابر جرایم سایبری، حملات علیه زیرساخت‌های حیاتی و تهدیدهای امنیتی ناشی از سوءاستفاده از داده‌ها منفعل بماند و از سوی دیگر، استناد کلی به امنیت ملی نباید به مجوزی برای نظارت گسترده، محدودسازی نامتناسب جریان اطلاعات یا مداخله بدون ضابطه در حریم خصوصی اشخاص تبدیل شود؛ زیرا در این صورت، حاکمیت داده از یک ابزار مشروع تنظیم‌گری به وسیله‌ای برای توسعه نامحدود اقتدار عمومی تبدیل خواهد شد ( Brown, 2020, p. 12). یکی از مهم‌ترین جلوه‌های این تعارض، محدودیت دسترسی آزاد به اطلاعات است. دولت‌ها ممکن است برای

حفاظت از امنیت ملی، جلوگیری از انتشار محتوای مجرمانه یا پیشگیری از آسیب به حقوق دیگران، جریان برخی داده‌ها را محدود کنند؛ اما مشروعیت این محدودیت منوط به آن است که میان ضرورت واقعی امنیتی و محدودیت پیش‌دستانه و گسترده تمایز گذاشته شود. هرچه معیارهای محدودسازی کلی‌تر و مبهم‌تر باشند، احتمال تبدیل اقدامات امنیتی به محدودیت آزادی بیان، دسترسی به اطلاعات و مشارکت عمومی در فضای دیجیتال افزایش می‌یابد. ازاین‌رو، مشروعیت اعمال حاکمیت داده صرفاً از هدف اعلام‌شده دولت ناشی نمی‌شود، بلکه ابزار انتخاب‌شده، دامنه مداخله، مدت آن و امکان نظارت بر تصمیم اتخاذشده نیز باید مورد توجه قرار گیرد (Brown, 2020, p. 18). این ضرورت با تضمین‌های حقوق بشری درباره حریم خصوصی و آزادی بیان نیز ارتباط مستقیم دارد. ماده ۱۷ میثاق بین‌المللی حقوق مدنی و سیاسی، مداخله خودسرانه یا غیرقانونی در حریم خصوصی، خانواده، خانه و مکاتبات را منع کرده و ماده ۱۹ همان سند، آزادی بیان و حق دریافت و انتقال اطلاعات را به رسمیت شناخته است. بنابراین، دیجیتالی شدن ابزارهای نظارتی دولت موجب خروج این اقدامات از قلمرو تعهدات حقوق بشری نمی‌شود و هرگونه دسترسی، جمع‌آوری یا پردازش داده باید از مبنای قانونی و توجیه حقوقی کافی برخوردار باشد. در حقوق ایران نیز این محدودیت‌ها فاقد مبنای مطلق نیستند. اصل ۲۲ قانون اساسی، حیثیت، جان، مال، حقوق، مسکن و شغل اشخاص را از تعرض مصون می‌داند و اصل ۲۵ نیز بازرسی و نرساندن نامه‌ها، ضبط و فاش کردن مکالمات و تجسس را جز به حکم قانون ممنوع کرده است. در نتیجه، توسعه ابزارهای نظارت و دسترسی به داده در فضای سایبر را نمی‌توان مستقل از این تضمین‌های قانون اساسی تحلیل کرد. افزون بر این، قانون تجارت الکترونیکی مصوب ۱۳۸۲ نیز با شناسایی داده‌پیام و وضع مقررات مربوط به داده‌های شخصی، پردازش اطلاعات اشخاص را در چارچوب الزامات قانونی قرار داده است. بنابراین، حتی در نظام حقوق داخلی نیز حاکمیت داده به معنای اختیار نامحدود دولت برای دسترسی، جمع‌آوری یا پردازش اطلاعات اشخاص نیست، بلکه اعمال آن باید در حدود قانون و با رعایت حقوق اشخاص صورت گیرد. یکی از مهم‌ترین نگرانی‌ها در این زمینه، گسترش نظارت ساختاریافته بر کاربران در مقیاس وسیع است. دولت‌ها برای شناسایی تهدیدهای سایبری و مقابله با جرایم دیجیتال ممکن است به جمع‌آوری فراداده‌ها، تحلیل الگوهای ارتباطی و پایش جریان‌های اطلاعاتی متوسل شوند. تفاوت اساسی میان نظارت هدفمند مبتنی بر ظن معقول و نظارت گسترده و پیشگیرانه باید در همین نقطه مورد توجه قرار گیرد؛ در حالت نخست، مداخله دولت به هدف و وضعیت مشخصی محدود می‌شود، در حالی که در حالت دوم، حجم گسترده‌ای از داده‌های اشخاص ممکن است بدون ارتباط روشن با رفتار مجرمانه یا تهدید مشخص جمع‌آوری و تحلیل شود. چنین رویکردی خطر شکل‌گیری وضعیت نظارت مستمر را ایجاد می‌کند و می‌تواند حریم خصوصی را با تهدید جدی مواجه سازد (Council of Europe, 2001, p. 52). ازاین‌رو، اصل تناسب باید به‌عنوان یکی از معیارهای اصلی مشروعیت مداخله دولت در داده‌های اشخاص مورد توجه قرار گیرد. هرچه ابزار نظارتی گسترده‌تر باشد، ضرورت ارائه توجیه حقوقی قوی‌تر، محدودسازی دامنه مداخله و پیش‌بینی نظارت قضایی نیز افزایش می‌یابد.دولت‌هایی که ظرفیت بیشتری برای جمع‌آوری، پردازش و تحلیل داده دارند، از توان بیشتری برای تنظیم فعالیت‌های اقتصادی، شناسایی تهدیدهای امنیتی و تأثیرگذاری بر محیط دیجیتال برخوردارند. بنابراین، رقابت بر سر کنترل داده بخشی از تحول مناسبات قدرت در نظام بین‌المللی است و سیاست‌های مربوط به حاکمیت داده در بسیاری از کشورها با سیاست‌های اقتصادی، صنعتی و امنیتی پیوند خورده است (کیان‌خواه، ۱۳۹۸، ص. ۱۶۸). بااین‌حال، اهمیت راهبردی داده نباید به حذف ملاحظات حقوق بشری بینجامد. برعکس، هرچه داده به منبع مهم‌تری از قدرت تبدیل شود، ضرورت حمایت از اشخاص در برابر سوءاستفاده از این قدرت نیز بیشتر می‌شود. بنابراین، حاکمیت داده باید از مفهوم «کنترل» صرف به سمت «تنظیم مسئولانه» حرکت کند؛ به این معنا که دولت علاوه بر ایجاد ظرفیت برای حفاظت از داده و امنیت سایبری، مکلف باشد حدود دسترسی خود و سایر بازیگران به اطلاعات را نیز مشخص کند و برای جلوگیری از سوءاستفاده از داده، سازوکارهای نظارت و پاسخ‌گویی ایجاد نماید. در این چارچوب، اصول قانونی بودن، ضرورت، تناسب، شفافیت و امکان نظارت قضایی باید بر اقدامات دولت حاکم باشد (International Law Commission, 2001, p. 71). در نتیجه، تعارض میان جریان آزاد داده و الزامات حاکمیت ملی را نباید تعارضی مطلق و حل‌ناشدنی دانست؛ بلکه با دو منفعت

مشروع مواجه هستیم که باید در چارچوب معیارهای حقوقی با یکدیگر متوازن شوند. دولت حق دارد برای حفاظت از امنیت ملی، نظم عمومی، حقوق اشخاص و زیرساخت‌های حیاتی، بر داده‌ها نظارت و مقررات لازم را وضع کند، اما این صلاحیت باید به موجب قانون، برای هدف مشروع و با رعایت تناسب اعمال شود. در مقابل، جریان آزاد داده نیز به معنای ممنوعیت هرگونه تنظیم‌گری ملی نیست، بلکه باید به‌عنوان یک وضعیت مطلوب اقتصادی و ارتباطی در نظر گرفته شود که در موارد ضروری و مشخص، امکان محدودسازی آن وجود دارد. از این منظر، راهکار مناسب، ایجاد الگویی چندلایه است که در آن جریان داده اصل مورد حمایت باشد و محدودیت آن تنها در صورت وجود مبنای قانونی، هدف مشروع، ضرورت واقعی و تناسب میان مداخله و هدف اعمال شود. چنین الگویی از یک سو ظرفیت دولت برای صیانت از حاکمیت داده را حفظ می‌کند و از سوی دیگر مانع تبدیل حاکمیت داده به ابزار نظارت نامحدود یا محدودسازی غیرضروری حقوق بنیادین می‌شود. بنابراین، در عصر داده‌محور، حاکمیت دولت زمانی از مشروعیت حقوقی برخوردار خواهد بود که افزایش ظرفیت آن برای کنترل و تنظیم داده، هم‌زمان با افزایش تعهد آن به رعایت حقوق بشر، پاسخ‌گویی و محدودیت‌های قانونی همراه باشد؛ به بیان دیگر، تحول حاکمیت در فضای سایبر نباید به معنای افزایش صرف قدرت دولت باشد، بلکه باید به معنای بازتنظیم قدرت دولت در چارچوب قانون، حقوق بنیادین و همکاری فرامرزی فهم شود.

ضرورت امنیتی به‌تنهایی برای مشروعیت هر اقدام نظارتی کافی نیست؛ بلکه باید احراز شود که اقدام مورد نظر برای دستیابی به هدف مشروع مناسب است، راهکار کم‌محدودکننده دیگری وجود ندارد و شدت مداخله با اهمیت تهدید تناسب دارد. از این منظر، حاکمیت داده زمانی با حقوق بشر سازگار خواهد بود که به جای ایجاد امکان نظارت نامحدود، به تنظیم دسترسی دولت به داده و تعیین حدود روشن برای این دسترسی منجر شود. مسئله زمانی پیچیده‌تر می‌شود که کنترل داده صرفاً در اختیار دولت نباشد و شرکت‌های فناوری، ارائه‌دهندگان خدمات ابری و پلتفرم‌های فراملی نیز در ذخیره‌سازی، پردازش و انتقال اطلاعات نقش داشته باشند. این بازیگران ممکن است حجم عظیمی از داده‌های شخصی و رفتاری کاربران را در اختیار داشته باشند و از طریق شیوه‌های پردازش و مدیریت اطلاعات، بر نحوه دسترسی اشخاص به داده‌ها اثر بگذارند. بنابراین، تهدید نسبت به حقوق بشر در فضای داده‌محور فقط از ناحیه دولت ناشی نمی‌شود و قدرت اطلاعاتی بخش خصوصی نیز در صورت فقدان شفافیت و پاسخ‌گویی می‌تواند حقوق اشخاص را تحت تأثیر قرار دهد (Villeneuve, 2010, p. 97). در چنین شرایطی، دولت از یک سو وظیفه دارد از مداخلات ناروا در حقوق اشخاص جلوگیری کند و از سوی دیگر باید بازیگران خصوصی مؤثر در چرخه داده را نیز تحت الزامات قانونی قرار دهد. ازاین‌رو، حاکمیت داده بیش از آنکه به معنای تمرکز کامل اختیار در دولت باشد، به معنای ایجاد چارچوبی است که در آن همه بازیگران مؤثر بر تولید، پردازش، انتقال و استفاده از داده در برابر قانون پاسخ‌گو باشند. در این چارچوب، رابطه میان حاکمیت داده و جریان آزاد اطلاعات اهمیت اساسی پیدا می‌کند. اینترنت و اقتصاد دیجیتال بر انتقال مستمر اطلاعات میان قلمروهای مختلف استوارند و ازاین‌رو، اعمال محدودیت‌های گسترده بر جریان داده می‌تواند با الزامات ارتباطات، تجارت و همکاری‌های فرامرزی در تعارض قرار گیرد. در مقابل، دولت‌ها نمی‌توانند آثار امنیتی و حقوقی انتقال آزاد و بدون ضابطه اطلاعات را نادیده بگیرند. داده‌های فرامرزی می‌توانند بر امنیت، اقتصاد، افکار عمومی و حتی فرایندهای سیاسی یک کشور اثرگذار باشند و همین امر موجب شده است کنترل جریان داده به یکی از عناصر مهم سیاست عمومی و امنیت ملی تبدیل شود (Hajizain-alabedini, 2007, p. 36). بنابراین، مسئله اصلی انتخاب مطلق میان آزادی جریان داده و کنترل دولتی نیست، بلکه تعیین شرایطی است که تحت آن محدودیت جریان داده بتواند از نظر حقوقی مشروع تلقی شود. این تعارض در تفاوت رژیم‌های ملی تنظیم داده نیز آشکار است. برخی نظام‌های حقوقی بر تسهیل انتقال داده و کاهش موانع فرامرزی تأکید دارند، در حالی که برخی دیگر انتقال داده را به شرایطی مانند ذخیره‌سازی داخلی، رعایت الزامات امنیتی یا اخذ مجوزهای قانونی منوط می‌کنند. تفاوت این رویکردها موجب شده است یک جریان داده واحد در مواردی هم‌زمان تحت تأثیر چند نظام حقوقی قرار گیرد و زمینه تعارض مقرراتی و افزایش هزینه‌های انطباق را فراهم آورد (ضیایی و شکیب‌نژاد، ۱۳۹۶، ص. ۷۴). ازاین‌رو، سیاست بومی‌سازی داده نیز نمی‌تواند راهکاری مطلق برای تأمین حاکمیت ملی تلقی

شود. بومی‌سازی برخی داده‌های حساس و راهبردی می‌تواند دسترسی دولت به اطلاعات مهم و ظرفیت حفاظت از زیرساخت‌های حیاتی را تقویت کند، اما بومی‌سازی گسترده ممکن است جریان طبیعی اطلاعات، فعالیت‌های اقتصادی و همکاری‌های فرامرزی را مختل کند. راهکار متناسب آن است که میان داده‌های حساس و راهبردی از یک سو و داده‌های عادی و کم‌خطر از سوی دیگر تفکیک ایجاد شود و سطح کنترل متناسب با میزان خطر و اهمیت داده تعیین گردد. در سطح امنیتی، این مسئله اهمیت بیشتری پیدا می‌کند؛ زیرا داده‌های فرامرزی ممکن است به‌سرعت در فضای داخلی بازتولید شوند و بر افکار عمومی، ثبات اجتماعی و امنیت داخلی اثر بگذارند. از این منظر، دولت‌ها جریان داده را صرفاً یک فرایند فنی نمی‌دانند، بلکه آن را بخشی از ظرفیت قدرت و امنیت ملی تلقی می‌کنند (قادری‌حاجت و نصرتی، ۱۳۹۲، ص. ۵۲). بااین‌حال، تبدیل امنیت ملی به مبنایی کلی و نامحدود برای کنترل داده می‌تواند نتیجه معکوس داشته باشد؛ زیرا در صورت فقدان معیارهای مشخص، تقریباً هر نوع جریان اطلاعاتی را می‌توان بالقوه تهدیدکننده امنیت دانست و بر همین اساس محدود کرد. بنابراین، تهدید امنیتی باید مشخص، قابل ارزیابی و متناسب با اقدام محدودکننده باشد و صرف احتمال آسیب یا نارضایتی از محتوای اطلاعاتی نباید مبنای کافی برای محدودسازی قرار گیرد (قادری‌حاجت و نصرتی، ۱۳۹۲، ص. ۵۵). در همین راستا، حاکمیت داده را باید در ارتباط با جایگاه فزاینده داده در مناسبات قدرت میان دولت‌ها نیز تحلیل کرد. داده دیگر صرفاً وسیله انتقال اطلاعات نیست، بلکه به منبعی برای تولید قدرت اقتصادی، سیاسی و امنیتی تبدیل شده است.

۷.ارزیابی ظرفیت نظام حقوقی ایران و الگوی مطلوب برای مدیریت تعارض صلاحیت‌های سایبری

ارزیابی ظرفیت نظام حقوقی ایران در مواجهه با تعارض صلاحیت‌های سایبری، مستلزم آن است که مسئله از مفهوم کلی «حاکمیت سایبری» تفکیک شده و مشخصاً در چارچوب صلاحیت دولت نسبت به داده‌ها و رفتارهای دیجیتال بررسی شود. در فضای سایبر، یک رفتار واحد ممکن است در ایران آغاز شود، از زیرساختی در کشور دیگر عبور کند، در چند مرکز داده خارجی پردازش یا ذخیره شود و آثار آن در کشور ثالث تحقق یابد؛ بنابراین، پیوند سنتی میان «محل وقوع رفتار» و «صلاحیت دولت» دیگر همیشه رابطه‌ای مستقیم و قطعی نیست. با وجود این، این تحول به معنای بی‌اعتبار شدن اصل سرزمینی بودن صلاحیت نیست، بلکه نشان‌دهنده ضرورت تکمیل آن با معیارهای دیگری است که بتوانند ارتباط واقعی رفتار دیجیتال با یک دولت را مشخص کنند. ازاین‌رو، در تحلیل وضعیت ایران باید میان صلاحیت تقنینی، صلاحیت قضایی و صلاحیت اجرایی تفکیک شود؛ زیرا دولت ممکن است از نظر تقنینی اختیار وضع مقررات نسبت به داده‌ای را داشته باشد، اما این امر لزوماً به معنای برخورداری مراجع قضایی از صلاحیت رسیدگی یا امکان اجرای مستقیم تصمیم در قلمرو دولت دیگر نیست (جعفری، ۱۳۹۸، ص. ۱۲۳). در نظام حقوقی ایران، قانون جرایم رایانه‌ای مصوب ۱۳۸۸ نقطه مهمی در پذیرش ویژگی‌های خاص محیط دیجیتال محسوب می‌شود. این قانون با جرم‌انگاری رفتارهایی مانند دسترسی غیرمجاز، شنود غیرمجاز، تخریب و اخلال در داده‌ها و سامانه‌های رایانه‌ای، جعل و کلاهبرداری رایانه‌ای و همچنین پیش‌بینی مقررات مربوط به ادله الکترونیکی، چارچوب اولیه‌ای برای واکنش حقوقی به رفتارهای سایبری ایجاد کرده است. بااین‌حال، مسئله تعارض صلاحیت در مواردی که عناصر رفتار در چند کشور پراکنده‌اند، همچنان نیازمند تحلیل تکمیلی است؛ زیرا قانون داخلی می‌تواند حدود صلاحیت مراجع ایرانی را مشخص کند، اما نمی‌تواند به‌تنهایی برای مراجع ایرانی اختیار اعمال اقدامات اجرایی در قلمرو دولت دیگر ایجاد کند. به همین دلیل، هنگامی که داده مورد نیاز یک پرونده در خارج از کشور نگهداری می‌شود یا ارائه‌دهنده خدمت و زیرساخت پردازش‌کننده در حوزه قضایی دیگری قرار دارد، میان «صلاحیت قانونی ایران» و «قابلیت عملی اعمال آن صلاحیت» فاصله ایجاد می‌شود (ضیایی و شکیب‌نژاد، ۱۳۹۶، ص. ۸۲). این تمایز برای جلوگیری از خلط صلاحیت قضایی و اجرایی اهمیت اساسی دارد؛ زیرا صالح بودن دادگاه ایرانی برای رسیدگی به یک رفتار سایبری، به‌خودی‌خود مجوز دسترسی مستقیم به سرور خارجی، توقیف داده خارج از کشور یا الزام یک شرکت خارجی به ارائه اطلاعات را ایجاد نمی‌کند. در چنین مواردی، اجرای صلاحیت نیازمند رعایت حاکمیت دولت محل استقرار داده و استفاده از سازوکارهای همکاری بین‌المللی است. از سوی دیگر، قواعد عام صلاحیت در

قانون مجازات اسلامی نیز نشان می‌دهد که نظام حقوقی ایران صرفاً به صلاحیت سرزمینی محدود نشده و در شرایطی امکان توجه به رفتارهای واقع‌شده خارج از قلمرو را پذیرفته است. بااین‌حال، انتقال این قواعد به محیط سایبر باید با احتیاط صورت گیرد؛ زیرا در فضای دیجیتال، تشخیص محل وقوع رفتار، محل تحقق نتیجه و حتی محل استقرار واقعی داده با دشواری بیشتری همراه است. بنابراین، نمی‌توان هر نوع ارتباط فنی یا موقتی داده با ایران را مبنای کافی برای توسعه صلاحیت دانست، بلکه باید وجود رابطه‌ای واقعی و معنادار میان رفتار مورد نظر و قلمرو، اتباع یا منافع اساسی ایران احراز شود. در این چارچوب، معیار «اثرگذاری واقعی» می‌تواند در کنار اصل سرزمینی به‌عنوان معیار تکمیلی مورد استفاده قرار گیرد؛ مشروط بر اینکه اثر مورد استناد، واقعی، قابل پیش‌بینی، قابل انتساب و از نظر حقوقی قابل توجه باشد. پذیرش بی‌ضابطه معیار اثرگذاری، خود می‌تواند به توسعه نامحدود صلاحیت و افزایش تعارض میان دولت‌ها منجر شود؛ بنابراین، استفاده از آن باید با معیار ارتباط مؤثر و اصل تناسب همراه باشد (Koh, 2012, p. 58). در بعد تقنینی، مسئله دیگر به نحوه تنظیم انواع مختلف داده بازمی‌گردد. نمی‌توان تمام داده‌های موجود در فضای سایبر را از حیث ارزش اقتصادی، امنیتی، حاکمیتی و حقوق بشری یکسان تلقی کرد. داده‌های مربوط به امنیت ملی، زیرساخت‌های حیاتی، اطلاعات حساس دولتی و داده‌هایی که افشای آنها می‌تواند منافع اساسی کشور را تهدید کند، طبیعتاً نیازمند سطح بالاتری از حمایت و کنترل هستند؛ در مقابل، داده‌های عمومی و بسیاری از داده‌های تجاری باید با رعایت الزامات قانونی امکان گردش مشروع و فرامرزی داشته باشند. چنین رویکردی مانع از آن می‌شود که مفهوم حاکمیت داده به کنترل مطلق دولت بر تمامی جریان‌های اطلاعاتی تبدیل شود و در عین حال امکان حفاظت از منافع اساسی کشور را حفظ می‌کند (Polčák & Svantesson, 2017, p. 163).

در حقوق داخلی ایران نیز حرکت به سوی تنظیم‌گری داده‌محور باید با توجه به همین تمایز انجام شود و میان حفاظت از داده‌های حساس و ایجاد محدودیت برای جریان عادی اطلاعات تفاوت گذاشته شود. در این میان، قانون تجارت الکترونیکی نیز با شناسایی برخی حمایت‌های مرتبط با داده و اطلاعات و پذیرش اعتبار ادله و اسناد الکترونیکی، ظرفیت مهمی برای شکل‌دهی به محیط حقوقی داده در ایران ایجاد کرده است؛ بااین‌حال، همچنان میان این قواعد و مسائل پیچیده مربوط به دسترسی فرامرزی، انتقال بین‌المللی و تعارض صلاحیت دولت‌ها فاصله وجود دارد. از منظر اجرایی، این خلأ اهمیت بیشتری پیدا می‌کند؛ زیرا بخش قابل توجهی از داده‌های مورد نیاز تحقیقات سایبری ممکن است نزد شرکت‌ها و ارائه‌دهندگان خدماتی قرار داشته باشد که در خارج از ایران مستقرند. در چنین شرایطی، اعمال مستقیم قدرت اجرایی ایران در قلمرو دولت دیگر می‌تواند با اصل احترام به حاکمیت آن دولت تعارض پیدا کند. راه‌حل منطقی، توسعه سازوکارهای همکاری قضایی، تبادل اطلاعات، حفظ فوری ادله و درخواست قانونی دسترسی به داده‌هاست. کنوانسیون بوداپست درباره جرایم سایبری، هرچند عضویت یا عدم عضویت هر دولت آثار خاص خود را دارد، از مهم‌ترین نمونه‌های تلاش بین‌المللی برای ایجاد سازوکارهای همکاری در زمینه جرایم سایبری و ادله الکترونیکی است و می‌تواند از منظر تطبیقی برای طراحی سازوکارهای داخلی و بین‌المللی مورد توجه قرار گیرد (Council of Europe, 2001). در همین راستا، همکاری بین‌المللی نباید صرفاً به مرحله پس از وقوع جرم محدود شود، بلکه باید شامل سازوکارهای روشن برای شناسایی مرجع صالح، حفظ داده، انتقال ادله، احراز اصالت اطلاعات و تعیین حدود دسترسی به داده نیز باشد. چنین رویکردی به‌جای رقابت میان صلاحیت‌های ملی، به سمت هماهنگی صلاحیتی حرکت می‌کند و احتمال آن را کاهش می‌دهد که چند دولت به‌طور هم‌زمان و بدون معیار مشخص مدعی صلاحیت نسبت به یک رفتار واحد شوند (Tintor, 2023, p. 91). از سوی دیگر، تقویت حاکمیت داده نباید بدون توجه به حقوق بنیادین اشخاص دنبال شود. گسترش ظرفیت دولت برای دسترسی، جمع‌آوری و پردازش داده‌ها اگر فاقد حدود قانونی و نظارت مؤثر باشد، می‌تواند به گسترش نظارت نامتناسب و تضعیف حریم خصوصی منجر شود. بنابراین، هرگونه اعمال صلاحیت نسبت به داده‌های اشخاص باید بر مبنای قانون و با رعایت ضرورت، تناسب و هدف مشروع صورت گیرد. در این معنا، حاکمیت داده را نباید مترادف با اختیار نامحدود دولت برای کنترل اطلاعات دانست؛ بلکه باید آن را مجموعه‌ای از اختیارات قانونی و مسئولیت‌های دولت برای تنظیم و صیانت از داده‌های مرتبط با قلمرو، اشخاص و منافع اساسی خود تلقی کرد. این برداشت با

ایده حاکمیت مسئولانه نیز سازگار است؛ یعنی دولت ضمن برخورداری از اختیار تنظیم‌گری، در اعمال آن با محدودیت‌های ناشی از حقوق اشخاص و حاکمیت سایر دولت‌ها مواجه است (Wagner, 2020, p. 795). بر این اساس، الگوی مناسب برای نظام حقوقی ایران، نه کنار گذاشتن اصل سرزمینی و نه پذیرش صلاحیت گسترده و نامحدود دولت، بلکه تکمیل صلاحیت سرزمینی با معیارهای ارتباط مؤثر، تابعیت، منافع اساسی و اثرگذاری واقعی است. در این الگو، اصل سرزمینی همچنان نقطه آغاز خواهد بود و معیارهای دیگر تنها در مواردی به کار گرفته می‌شوند که رابطه کافی و قابل دفاع میان رفتار سایبری و دولت ایران وجود داشته باشد. همچنین باید میان صلاحیت تقنینی و قضایی از یک سو و صلاحیت اجرایی از سوی دیگر تفاوت گذاشت؛ به این معنا که دولت می‌تواند در حدود ارتباط صلاحیتی خود برای رفتارهای سایبری قانون وضع کند و دادگاه‌های آن نیز در صورت وجود مبنای قانونی به موضوع رسیدگی کنند، اما اجرای اقدامات مادی خارج از قلمرو تابع قواعد حاکمیت سرزمینی و همکاری بین‌المللی خواهد بود. چنین تفکیکی از توسعه بی‌ضابطه صلاحیت جلوگیری کرده و در عین حال امکان واکنش مؤثر به رفتارهایی را که آثار واقعی آنها در ایران تحقق یافته است فراهم می‌کند. در نهایت، بررسی وضعیت ایران نشان می‌دهد که مسئله اصلی، فقدان کامل مبانی حقوقی برای اعمال صلاحیت سایبری نیست؛ بلکه پراکندگی قواعد، عدم تفکیک روشن انواع صلاحیت، دشواری دسترسی فرامرزی به داده و فقدان سازوکار جامع برای هماهنگی صلاحیتی است (جعفرنیا و کریمی قهرودی، ۱۳۹۹، ص. ۹۲). ازاین‌رو، اصلاح وضعیت موجود باید به سمت ایجاد یک چارچوب منسجم حرکت کند که در آن اصل سرزمینی، تابعیت، منافع اساسی و اثر واقعی در کنار یکدیگر قرار گیرند، اما هیچ‌یک به‌تنهایی موجب توسعه نامحدود صلاحیت نشود. در چنین چارچوبی، حاکمیت داده به معنای توانایی دولت برای تنظیم داده‌های مرتبط با قلمرو و منافع اساسی خود خواهد بود، در حالی که اعمال این اقتدار باید با صلاحیت سایر دولت‌ها، الزامات همکاری بین‌المللی و حقوق بنیادین اشخاص سازگار باشد.این رویکرد ضمن حفظ اقتدار حقوقی ایران در فضای سایبر، از تبدیل حاکمیت داده به ابزار مداخله نامحدود جلوگیری می‌کند و می‌تواند مبنایی منسجم برای مدیریت تعارض صلاحیت‌های ناشی از جریان فرامرزی داده فراهم آورد.

## نتیجه‌گیری

بررسی حاکمیت داده و تعارض صلاحیت دولت‌ها در فضای سایبر نشان می‌دهد که تحول فناوری، مبانی سنتی اعمال اقتدار دولت را با چالش مواجه کرده است؛ بااین‌حال، این تحول به معنای زوال حاکمیت یا بی‌اعتباری اصل سرزمینی نیست، بلکه بیانگر ضرورت بازتنظیم مبانی و حدود صلاحیت دولت در محیط داده‌محور است. داده برخلاف اشیای مادی، ممکن است هم‌زمان در فرآیند تولید، انتقال، پردازش و ذخیره‌سازی با چند قلمرو ارتباط داشته باشد و همین ویژگی، تعیین یک محل واحد برای وقوع رفتار و در نتیجه اعمال صلاحیت انحصاری یک دولت را دشوار می‌سازد. بنابراین، مسئله اصلی پژوهش نه حذف صلاحیت سرزمینی، بلکه تبیین حدود کارآمدی آن و شناسایی معیارهای تکمیلی برای مواجهه با رفتارهای سایبری فرامرزی است. یافته‌های پژوهش نشان داد که در چنین محیطی، تفکیک میان صلاحیت تقنینی، قضایی و اجرایی اهمیت اساسی دارد؛ زیرا دولت ممکن است بر مبنای ارتباط سرزمینی، شخصی یا واقعی، صلاحیت قانون‌گذاری و رسیدگی نسبت به یک رفتار سایبری داشته باشد، اما این امر لزوماً به معنای برخورداری از اختیار اجرای مستقیم اقدامات در قلمرو دولت دیگر نیست. به‌ویژه در مواردی که داده یا زیرساخت پردازش آن در خارج از کشور قرار دارد، اعمال صلاحیت اجرایی بدون رضایت یا همکاری دولت محل می‌تواند با اصل حاکمیت سرزمینی تعارض پیدا کند. ازاین‌رو، یکی از نتایج اساسی پژوهش آن است که وجود صلاحیت و امکان اجرای صلاحیت دو مسئله متفاوت‌اند و حقوق فضای سایبر باید این تمایز را به رسمیت بشناسد. بررسی تحولات فضای سایبر همچنین نشان داد که اصل سرزمینی، اگرچه همچنان نقطه آغاز تعیین صلاحیت است، به‌تنهایی پاسخ‌گوی همه موقعیت‌های چندمکانی داده نیست. در کنار آن، معیارهایی همچون تابعیت، منافع اساسی دولت، ارتباط مؤثر و به‌ویژه اثرگذاری واقعی می‌توانند در موارد مناسب نقش تکمیلی ایفا کنند؛ مشروط بر اینکه استفاده از آنها به ارتباط واقعی، قابل

انتساب و از نظر حقوقی قابل توجه محدود شود. در غیر این صورت، توسعه معیار اثرگذاری می‌تواند خود به ابزاری برای گسترش نامحدود صلاحیت دولت‌ها و تشدید تعارضات بین‌المللی تبدیل شود. بنابراین، نتیجه پژوهش از پذیرش یک صلاحیت مبتنی بر «اثر صرف» حمایت نمی‌کند، بلکه بر صلاحیت ترکیبی و محدودشده بر اساس ارتباط مؤثر و تناسب تأکید دارد. از سوی دیگر، یافته‌ها نشان داد که تعارض صلاحیت‌ها صرفاً ناشی از کاستی قواعد حقوقی نیست، بلکه با ساختار اقتصادی و فنی فضای دیجیتال نیز ارتباط دارد. وابستگی دولت‌ها به شرکت‌های فناوری، ارائه‌دهندگان خدمات ابری، شبکه‌های ارتباطی و سایر زیرساخت‌های فراملی موجب شده است که بخشی از ظرفیت عملی کنترل داده در اختیار بازیگرانی قرار گیرد که در قلمرو یک دولت واحد مستقر نیستند. ازاین‌رو، حاکمیت داده دیگر صرفاً به معنای کنترل مستقیم دولت بر اطلاعات نیست، بلکه به توانایی دولت برای تنظیم، حفاظت و اعمال اقتدار قانونی نسبت به جریان‌های داده‌ای مرتبط با قلمرو و منافع اساسی خود تبدیل شده است. این وضعیت ضرورت همکاری میان دولت‌ها و نیز تنظیم مسئولیت و تکالیف بازیگران خصوصی را افزایش می‌دهد. در این میان، راهبردهایی مانند بومی‌سازی مطلق داده یا کنترل کامل جریان اطلاعات، اگرچه ممکن است در کوتاه‌مدت ظرفیت کنترل ملی را افزایش دهند، در بلندمدت می‌توانند به چندپارگی مقررات، افزایش هزینه‌های اقتصادی، محدود شدن جریان مشروع اطلاعات و تشدید تعارض میان نظام‌های حقوقی منجر شوند. بنابراین، حاکمیت داده کارآمد را نمی‌توان با قطع یا محدودسازی حداکثری جریان داده یکی دانست، بلکه باید میان حفاظت از داده‌های حساس و امکان گردش مشروع داده‌های عمومی و تجاری تمایز ایجاد کرد. در خصوص نظام حقوقی ایران، یافته‌های پژوهش نشان می‌دهد که حقوق داخلی از طریق مقرراتی مانند قانون جرایم رایانه‌ای، قانون مجازات اسلامی و قانون تجارت الکترونیکی، مبانی اولیه لازم برای مواجهه با رفتارهای دیجیتال و ادله الکترونیکی را فراهم کرده است، اما این ظرفیت‌ها هنوز برای مدیریت همه ابعاد تعارض صلاحیت‌های فرامرزی کافی نیستند. مهم‌ترین چالش در این زمینه، نه فقدان مطلق مبنای صلاحیت، بلکه پراکندگی قواعد، نبود چارچوب جامع برای دسترسی فرامرزی به داده و دشواری اجرای تصمیمات نسبت به داده‌ها و زیرساخت‌های خارج از قلمرو ایران است. از این منظر، تقویت حقوق داخلی باید در جهت ایجاد هماهنگی میان قواعد صلاحیت و سازوکارهای همکاری قضایی و بین‌المللی صورت گیرد، نه صرفاً از طریق توسعه یک‌جانبه دامنه صلاحیت دولت. همچنین یافته‌ها نشان داد که هرچه وابستگی یک پرونده به داده‌های خارج از قلمرو بیشتر باشد، اهمیت همکاری بین‌المللی افزایش می‌یابد؛ زیرا هیچ دولت واحدی نمی‌تواند صرفاً با اتکا به قانون داخلی خود، دسترسی نامحدود به زیرساخت‌ها و داده‌های واقع در قلمرو دولت دیگر پیدا کند.

در نتیجه، آینده اعمال صلاحیت سایبری بیش از آنکه در رقابت برای توسعه حداکثری صلاحیت ملی باشد، در هماهنگی میان صلاحیت‌های ملی و ایجاد سازوکارهای همکاری برای دسترسی قانونی به داده و ادله الکترونیکی قرار دارد. در این چارچوب، همکاری صلاحیتی نه جایگزین حاکمیت دولت، بلکه ابزار اعمال منظم و مشروع آن خواهد بود. از سوی دیگر، گسترش حاکمیت داده باید با رعایت حقوق بنیادین اشخاص همراه باشد. دسترسی دولت به داده، نظارت بر جریان اطلاعات و پردازش داده‌های کاربران باید تابع قانون، ضرورت و تناسب باشد و نمی‌تواند صرفاً با استناد کلی به امنیت ملی توجیه شود. بنابراین، الگوی مطلوب باید به‌گونه‌ای طراحی شود که افزایش ظرفیت دولت در حفاظت از داده‌های حساس، به گسترش نامحدود نظارت و محدودسازی حقوق اشخاص منجر نشود. بر این اساس، فرضیه پژوهش مبنی بر اینکه فرامرزی شدن جریان داده و وابستگی دولت‌ها به زیرساخت‌های دیجیتال جهانی، کارآمدی انحصاری صلاحیت سرزمینی را کاهش داده و حرکت به سمت الگوی ترکیبی صلاحیت را ضروری ساخته است، تأیید می‌شود؛ اما این تأیید با یک قید مهم همراه است: صلاحیت ترکیبی نباید به معنای رها شدن از معیارهای محدودکننده و پذیرش صلاحیت نامحدود دولت‌ها باشد، بلکه باید بر پایه ارتباط واقعی، اثرگذاری قابل توجه، منافع اساسی و احترام به حاکمیت سایر دولت‌ها اعمال شود. بنابراین، دستاورد اصلی پژوهش را می‌توان در ارائه این برداشت دانست که آینده صلاحیت در فضای سایبر نه در حذف اصل سرزمینی و نه در بازگشت کامل به انحصار سرزمینی، بلکه در ترکیب سنجیده اصل سرزمینی با معیارهای تکمیلی و سازوکارهای همکاری بین‌المللی قرار دارد. در چنین

الگویی، صلاحیت تقنینی، قضایی و اجرایی جایگاه مستقل خود را حفظ می‌کنند؛ حاکمیت داده به اختیار مطلق دولت تبدیل نمی‌شود؛ معیار اثرگذاری واقعی تحت ضوابط محدودکننده به کار می‌رود؛ و دسترسی به داده‌های خارج از قلمرو از طریق سازوکارهای همکاری و احترام به حاکمیت سایر دولت‌ها صورت می‌گیرد. برآیند این یافته‌ها آن است که نظام حقوقی مطلوب برای ایران نیز باید از یک‌سو ظرفیت دولت را برای حفاظت از داده‌های حساس و منافع اساسی کشور حفظ کند و از سوی دیگر، با ایجاد قواعد روشن درباره تعارض صلاحیت، دسترسی فرامرزی به داده، همکاری قضایی و حدود مداخله اجرایی، از توسعه بی‌ضابطه صلاحیت جلوگیری نماید. در نهایت، حاکمیت داده در عصر سایبر را باید حاکمیتی مسئولانه، محدود به قانون، مبتنی بر ارتباط مؤثر و همراه با همکاری فرامرزی دانست؛ الگویی که در آن اقتدار دولت، جریان مشروع داده و حقوق بنیادین اشخاص در تعادل قرار می‌گیرند و از تبدیل فضای سایبر به عرصه رقابت نامحدود صلاحیتی دولت‌ها جلوگیری می‌شود.

منابع


۱. احمدی‌نیاز، حسین. (۱۳۸۵). نقش سازمان‌های بین‌المللی بر حاکمیت دولت‌ها. تهران: پرتو بیان.

۲. بهمنی، محمدسعید. (۱۳۹۱). تأثیر اقدامات در فضای سایبری بر امنیت ملی کشورها با تأکید بر سایت ویکی‌لیکس (پایان‌نامه کارشناسی ارشد). دانشگاه آزاد اسلامی واحد تهران مرکزی.

۳. جعفرنیا، امید، و کریمی قهرودی، محمدرضا. (۱۳۹۹). اهمیت و الزامات حاکمیت فضای سایبری. چهارمین کنفرانس ملی دانش و فناوری مهندسی برق، کامپیوتر و مکانیک.

٤. جعفری، افشین. (۱۳۹۸). حاکمیت بر فضای سایبر از منظر حقوق بین‌الملل و نظام حقوقی جمهوری اسلامی ایران. رهیافت انقلاب اسلامی، ۱۳(٤۹)، ۱۰۹–۱۳۲.

۵. حاجی زین‌العابدینی، محسن. (۱۳۸۷). حاکمیت بر اینترنت و مدیریت اطلاعات. فصلنامه اطلاع‌رسانی و کتابداری، (۱۹).

٦. حافظ‌نیا، محمدرضا. (۱۳۹۰). جغرافیای سیاسی فضای مجازی. تهران: سمت.

۷. زمانیان، جواد. (۱۳۹۰). براندازی نظام در فضای سایبری (پایان‌نامه کارشناسی ارشد). مؤسسه آموزش عالی شهید اشرفی اصفهانی.

۸. ضیایی، سیدیاسر، و شکیب‌نژاد، احسان. (۱۳۹٦). قانون‌گذاری در فضای سایبر. مجله حقوقی بین‌المللی، ۳٤(۵۷).

۹. ضیایی، سیدیاسر، و شکیب‌نژاد، احسان. (۱۳۹٦). قانونگذاری در فضای سایبر: رویکرد حقوق بین‌الملل و حقوق ایران. مجله حقوقی بین‌المللی، ۳٤ (57). https://doi.org/10.22066/cilamag.2017.27971

۱۰. علوی، سید حسین، حسینی، محمدرضا، و رامک، مهراب. (۱٤۰۲). بررسی چگونگی اعمال حاکمیت بر قلمرو سایبری ملی به مثابه قدرت نرم در پرتو حقوق بین‌الملل. فصلنامه علمی مطالعات قدرت نرم، ۱۳(٤)، ۳۵–۵٤.

۱۱. قادری‌حاجت، مصطفی، و نصرتی، حمیدرضا. (۱۳۹۲). فضای سایبر؛ چالش‌های فراروی حاکمیت و امنیت پایدار. پژوهشنامه جغرافیای انتظامی، ۱(۲).

۱۲. کریمی قهرودی، محمدرضا، و زارعی، وحید. (۱۳۹۹). حاکمیت فضای سایبری. تهران: مؤسسه آموزشی تحقیقاتی صنایع دفاعی.

۱۳. کیان‌خواه، احسان. (۱۳۹۸). چالش‌های راهبردی حکمرانی با گسترش فضای سایبر. امنیت ملی، ۹(۳٤)، ۱۵۳–۱۷٤.

۱٤. مظاهری، مسعود، صلاحی، سهراب، و مرادی، مریم. (۱٤۰۱). به‌کارگیری قدرت نرم علیه حاکمیت دولت‌ها از طریق جریان آزاد اطلاعات. مطالعات قدرت نرم، ۱۲(۳۰)، ۱۸۵–۲۰٤.

15. Andress, J., & Winterfeld, S. (2013). Cyber warfare: Techniques, tactics and tools for security practitioners. Syngress.
16. Arsić, K. (2024). Sajber prostor i međunarodno pravo: Analiza i domašaji konvencije Saveta Evrope o visokotehnološkom kriminalu. Zbornik Udruženja za međunarodno krivično pravo.
17. Bateman, J., Beecroft, N., & Wilde, G. (2022, December 19). What the Russian invasion reveals about the future of cyber warfare. Carnegie Endowment for International Peace.
18. Benkler, Y. (2006). The wealth of networks: How social production transforms markets and freedom. Yale University Press.
19. Brown, D. (2020, May 26). It's Time to Treat Cybersecurity as a Human Rights Issue. Human Rights Watch. [Human Rights Watch](https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue?utm_source=chatgpt.com)
20. Chander, A., & Sun, H. (2023). Data sovereignty: From the digital silk road to the return of the state. Oxford University Press .
21. Chen, C., Ko, K., & Lee, J.-Y. (2010). North Korea's internet strategy and its political implications. The Pacific Review, 23(5), 649–670. https://doi.org/10.1080/09512748.2010.522249
22. Choucri, N., & Clark, D. D. (2012). Integrating cyberspace and international relations: The co-evolution dilemma (ECIR Working Paper No. 2012-3). MIT Political Science Department.
23. Choucri, N., & Clark, D. D. (2019). International relations in the cyber age: The co-evolution dilemma. MIT Press.
24. Council of Europe. (2001, November 23). Convention on Cybercrime (Budapest Convention) (ETS No. 185). Council of Europe.
25. Gordić, J. (2022). Sajber napadi sa aspekta međunarodnog i unutrašnjeg prava. Baština, 57.
26. International Law Commission. (2001). Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries. United Nations.
27. Klug, T., & Baig, R. (2023, February 13). Fact check: Russia's disinformation campaign targets NATO. DW.
28. Koh, H. H. (2012). International law in cyberspace. Harvard International Law Journal, 54.
29. Leiter, A. (2020). Cyber sovereignty: A snapshot from a field in motion. Harvard International Law Journal, 61 .()
30. Lin, H., & Zegart, A. (Eds.). (2019). Bytes, bombs, and spies: The strategic dimensions of offensive cyber operations. Brookings Institution Press.
31. Masters, J. (2023, February 14). Ukraine: Conflict at the crossroads of Europe and Russia. Council on Foreign Relations.
32. Maurer, T. (2016). Proxies and cyberspace. Journal of Conflict and Security Law, 21(3), 383–403. https://doi.org/10.1093/jcsl/krw015
33. Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.
34. Polčák, R., & Svantesson, D. J. B. (2017). Information sovereignty: Data privacy, sovereign powers and the rule of law. Edward Elgar Publishing .
35. Tintor, Lj. (2023). Međunarodna odgovornost države u digitalnom (sajber) prostoru. Srpski Godišnjak za Međunarodno Pravo.
36. Tobanksy, L. (2011). Basic Concepts in Cyber Warfare. Military and Strategic Affairs, 3.
37. Troianovski, A., & Safronova, V. (2022, March 4). Russia takes censorship to new extremes, stifling war coverage. The New York Times.
38. Villeneuve, N. (2010). Barriers to cooperation: An analysis of the origins of international efforts to protect children online. In R. Deibert et al. (Eds.), Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace. MIT Press.
39. Wagner, B. (2020). Against sovereignty in cyberspace. International Studies Review, 22(4), 779–804.
40. Choucri, N., & Clark, D. D. (2019). International relations in the cyber age. MIT Press.

41. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), CETS No. 185. Council of Europe.

42. Council of Europe. (2021). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Council of Europe.

43. Council of the European Union. (2023). Council adopts EU laws on better access to electronic evidence. Council of the European Union.

44. European Parliament, & Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Official Journal of the European Union.
45. Lin, H., & Zegart, A. B. (2019). Bytes, bombs, and spies: The strategic dimensions of offensive cyber operations. Brookings Institution Press.

46. Maurer, T. (2018). Cyber mercenaries: The state, hackers, and power. Cambridge University Press.

47. OECD/WTO. (2025). Economic implications of data regulation: Balancing openness and trust. OECD Publishing.

48. U.S. Department of Justice. (2019). Promoting public safety, privacy, and the rule of law around the world: The CLOUD Act. U.S. Department of Justice.