فصلنامه علمی تخصصی فقه و حقوق معاصر

سال یازدهم- زمستان ١٤٠٤- شماره ٣٤- ص۷۹-۱۰۸

تحول مفهوم حاکمیت دولت در عصرحکمرانی داده های کلان

پیمان چمن یار[۱]

چکیده

مفهوم کلاسیک «حاکمیت» در حقوق بین‌الملل که بر پایه‌ی اصل «تمامیت سرزمینی» و «صلاحیت انحصاری دولت بر قلمرو» استوار است، در مواجهه با ظهور پارادایم «داده‌های کلان» و جریان‌های فرامرزی اطلاعات، با چالش‌های وجودی مواجه شده است. این پژوهش با هدف واکاوی تنش میان اصول بنیادین حقوق بین‌الملل عمومی و واقعیت‌های عصر دیجیتال، بر این فرضیه استوار است که حاکمیت داده‌ای، به‌عنوان جلوه‌ای نوین از حاکمیت ملی، در حال جایگزینی یا دست‌کم تکمیلِ صلاحیت‌های سرزمینی سنتی است. واکاوی رویه دولت‌ها و اسناد بین‌المللی، مشخص می‌گردد که چگونه محل‌مندیِ داده‌ها و کنشگریِ بازیگران غیردولتیِ کلان ، مرزهای صلاحیت قضایی و تقنینی دولت‌ها را در فضای سایبر به چالش کشیده است. یافته‌های این پژوهش نشان می‌دهد که تداوم اتکا به دکترین‌های کلاسیک، منجر به نوعی خلأ حکمرانی در عرصه‌ی دیجیتال گشته و ضرورتِ گذار به یک رژیم حقوقی بین‌المللیِ مبتنی بر «صلاحیت عملکردی» و استانداردهای نوینِ حاکمیتی را بیش از پیش نمایان می‌سازد. در نهایت، این تحقیق پیشنهاد می‌دهد که بازتعریف مفهوم حاکمیت در حقوق بین‌الملل، نه به معنای نفی صلاحیت‌های سرزمینی، بلکه به مثابه‌ی توسعه‌ی تعهداتِ فرامرزیِ دولت‌ها در حکمرانیِ داده‌های جهانی، اجتناب‌ناپذیر است.

واژگان کلیدی: حاکمیت داده ها، صلاحیت فرامرزی، حقوق بین الملل دیجیتال، تمامیت سرزمینی ، حکمرانی فضای سایبری.

[۱] کارشناسی ارشد حقوق بین الملل

Chamanyar.p@gmail.com

مقدمه:

در سده‌های اخیر، سنگ‌بنای نظام حقوق بین‌الملل بر محوریت «سرزمین» و «مرزهای جغرافیایی» استوار بوده است. آموزه‌های کلاسیک حقوق بین‌الملل، از صلح وستفالیا تا منشور ملل متحد، دولت را به عنوان موجودیتی با حاکمیت انحصاری بر یک قلمرو فیزیکیِ مشخص تعریف کرده‌اند که صلاحیتِ تقنینی و قضایی آن در چارچوب همین مرزها معنا می‌یابد. با این حال، ظهور عصر داده‌های کلان و جریان‌های بی‌پایان اطلاعات در فضای سایبر، نظام سنتیِ حکمرانی را با وضعیتی پارادوکسیکال مواجه ساخته است؛ وضعیتی که در آن «داده» به مثابه «قلمرو جدید» ظهور کرده، اما از بندِ قیودِ سرزمینی رسته است.

امروزه، داده‌ها نه تنها دارایی‌های استراتژیک دولت‌ها محسوب می‌شوند، بلکه به عنوان ابزاری برای اعمال قدرت و کنترل بر شهروندان، مورد مناقشه میانِ قدرت‌های سیاسی و بازیگرانِ غیردولتیِ کلان قرار گرفته‌اند. چالش بنیادین در این میان، ناتوانیِ مفاهیمِ سنتیِ «حاکمیت» در انطباق با ماهیتِ سیال و فرامرزیِ داده‌هاست. هنگامی که سرورهای ذخیره‌سازی داده در یک کشور، با مدیریتِ شرکتی در کشوری دیگر و بهره‌برداریِ کاربرانی در سراسر جهان مواجه است، اصلِ «صلاحیت سرزمینی» دیگر نمی‌تواند پاسخگوی نیازهای انتظامی، قضایی و امنیتی دولت‌ها باشد.

این پژوهش با درک این واقعیتِ تاریخی که «تکنولوژی، سریع‌تر از قواعدِ عرفی حرکت می‌کند»، بر آن است تا چالش‌های پیش‌رویِ حاکمیت ملی در مواجهه با داده‌های کلان را به بوته نقد بکشد. پرسش اصلی اینجاست: آیا در عصرِ انباشتِ داده‌های ابری، حاکمیت دولت‌ها باید همچنان بر پایه‌ی «قلمرو سرزمینی» تعریف شود، یا زمانِ آن فرا رسیده است که «صلاحیت عملکردی» و «صلاحیت شخصی» را به عنوان جایگزین‌هایی نوین در حقوق بین‌الملل بازخوانی کنیم؟

در این نوشتار، با اتخاذ رویکردی انتقادی نسبت به رویه‌های جاری، استدلال خواهد شد که انباشت و کنترلِ داده‌ها، نه تنها یک مسئله فنی، بلکه «توسعه»ای از مفهوم کلاسیکِ حاکمیت است که دولت‌ها را در یک وضعیتِ رقابتیِ جدید قرار داده است. لذا، بررسیِ این دگردیسی، نه تنها یک ضرورتِ علمی برای فهمِ تحولاتِ

حقوق بین‌الملل معاصر است، بلکه پیش‌شرطی برای تدوینِ چارچوب‌های حقوقیِ پایدار در حکمرانیِ جهانیِ فضای سایبر به شمار می‌آید.

مفهوم داده به عنوان «قلمرو جدید» و چالش آن برای مفاهیم کلاسیک

ظهور فناوری‌های نوین و انباشت داده‌های کلان، پارادایم سنتی حقوق بین‌الملل را که بر پایه سیطره فیزیکی دولت‌ها بر قلمرو جغرافیایی استوار بوده، با چالشی جدی مواجه ساخته است. در نظام‌های حقوقی کلاسیک، اقتدار دولت به صورت مستقیم با مفهوم مکان و حضور ملموس در یک محدوده سرزمینی تعریف می‌شد، اما امروزه داده‌ها به عنوان دارایی‌های غیرمادی و سیال، پیوند ناگسستنی میان حاکمیت و سرزمین را تضعیف کرده‌اند. این جریان آزاد و بی‌پایان اطلاعات، بدون اعتنا به مرزهای سیاسی، فرآیندهای تصمیم‌گیری و اعمال قدرت را به لایه‌های نامرئی فضای سایبر منتقل کرده و دولت‌ها را در موقعیتی قرار داده است که ابزارهای سنتی نظارت و اعمال صلاحیت قضایی، کارایی پیشین خود را در مواجهه با این قلمروهای جدید از دست داده‌اند. بدین ترتیب، تقابل میان ماهیت بی‌مرز فضای دیجیتال و ساختار سخت‌گیرانه حقوق بین‌الملل کلاسیک، نخستین گسست در نظریات حاکمیت سرزمینی را رقم زده است (ضیایی، ۱۳۹۹: ٤٥).

تفسیرهای سنتی از تمامیت سرزمینی، همواره بر لزوم کنترل فیزیکی بر منابع و جمعیت موجود در یک محدوده مشخص تأکید ورزیده‌اند، در حالی که در عصر داده‌های کلان، کنترل فیزیکی بر داده‌ها به دلیل ماهیت پراکنده و ذخیره‌سازی ابری آن‌ها، عملاً ناممکن یا بسیار دشوار است. این گذار پارادایمیک، مفهوم قلمرو را از یک موجودیت مادی و محدود، به مفهومی چندبعدی و مجازی تبدیل کرده است که نه تنها دربرگیرنده خاک و آب، بلکه شامل شبکه‌های پیچیده داده‌ها نیز می‌باشد. دولت‌ها برای حفظ بقا و اقتدار خویش در مواجهه با این تحولات، ناگزیر از بازنگری در مبانی صلاحیت سرزمینی هستند تا بتوانند بر حوزه‌هایی که در آن داده‌ها تولید، پردازش و توزیع می‌شوند، کنترل مؤثری اعمال نمایند. فقدان انطباق میان هنجارهای حقوق بین‌الملل کلاسیک و واقعیت‌های عصر داده‌محور، منجر به خلأهای حقوقی شده است که در آن، مرزهای ملی دیگر نمی‌توانند به تنهایی ضامن اجرای قواعد و قوانین داخلی در فضای سایبر باشند (شریعت‌باقری، ۱۳۹۸: ۱۱۲).

ماهیت غیرمتمرکز شبکه‌های اطلاعاتی موجب گشته است که دولت‌ها در اعمال صلاحیت تقنینی خود دچار سردرگمی شوند، زیرا مشخص نیست که آیا صلاحیت یک دولت باید بر اساس محل سرورهای فیزیکی، محل اقامت کاربر یا محل انتفاع از داده‌ها تعیین گردد. این ابهام در قلمروهای حقوقی، چالش‌های پیچیده‌ای را برای تفسیر قواعد آمره بین‌المللی ایجاد کرده و موجب شده است که دولت‌ها در اقداماتی یک‌جانبه برای اعمال قدرت فرامرزی، به سمت سیاست‌های ملی‌گرایانه در حوزه دیجیتال متمایل شوند. تعارض میانِ استانداردهای بین‌المللیِ حاکم بر جریان داده‌ها و اختیارات حاکمیتی دولت‌ها، گویای آن است که مفاهیم سنتی نظیر صلاحیت شخصی و صلاحیت سرزمینی در مواجهه با داده‌های کلان، نیازمند بازتعریف و توسعه در چارچوب نظریات جدید حقوقی هستند. در چنین فضایی، تلاش برای محدود کردن داده‌ها در درون مرزهای فیزیکی، نه تنها با روحِ جهانیِ اینترنت در تضاد است، بلکه در عمل نیز توانایی اجرای دقیق قواعد حقوقی را در سطوح ملی و بین‌المللی محدود می‌کند .(Zittrain, 2017: 28)

مفهوم قلمرو در حقوق بین‌المللِ سنتی، همواره به عنوان سنگرِ اصلیِ حاکمیت در برابر مداخله خارجی شناخته شده است، اما امروزه داده‌ها به مثابه کانال‌های نفوذِ نامرئی عمل می‌کنند که می‌توانند بدون عبور از مرزهای نظامی، امنیت و نظم عمومی یک کشور را تحت تأثیر قرار دهند. این امر دکترین کلاسیک حاکمیت را به شدت تحت فشار قرار داده و موجب شده است که دولت‌ها برای حفظ اقتدار خود، اقدام به تصویب قوانینِ بومی‌سازیِ داده‌ها نمایند که در عمل با تعهداتِ بین‌المللیِ آن‌ها در زمینه تجارت آزاد و دسترسی آزاد به اطلاعات در تضاد قرار دارد. فرآیندِ تبدیل داده‌ها به دارایی‌های حاکمیتی، نشان‌دهنده آن است که چگونه مفاهیم کلاسیک برای بقا در فضای مدرن، تغییر ماهیت داده و به سمتِ تعریفِ جدیدی از قلمرو حرکت می‌کنند که در آن مرزهای فیزیکی، جای خود را به مرزهایِ منطقی و دیجیتالی داده‌اند (محبی، ۱۴۰۱: ۸۹).

تلاش برای انطباقِ قواعدِ حقوقیِ موجود با واقعیت‌های داده‌محور، نه تنها با دشواری‌هایِ فنی همراه است، بلکه مستلزمِ گذار از تفسیرهای خشک و رسمی به سمتِ فهمی پویا از حاکمیت می‌باشد که بتواند در عین رعایتِ تمامیتِ ارضی، پاسخگویِ نیازهایِ نوینِ حکمرانی در فضایِ سایبر باشد. چالشِ اصلی در این میان، نه تنها در تعریفِ دوباره‌یِ قلمرو، بلکه در ترسیمِ حدودِ دخالتِ دولت‌ها در جریان‌هایِ جهانیِ داده‌ها بدونِ تخریبِ زیرساخت‌هایِ همکاریِ بین‌المللی است. از این منظر، هرگونه تلاش برای اعمالِ صلاحیت‌هایِ سنتی بر

عرصه‌هایِ نوینِ مجازی، نیازمندِ بازخوانیِ دقیقِ اصولِ کلیِ حقوقِ بین‌الملل و انطباقِ آن‌ها با ماهیتِ پویایِ داده‌هایِ کلان است تا بتوان تعادلی میانِ حاکمیتِ دولتی و آزادیِ اطلاعات در فضایِ جهانیِ سایبر برقرار کرد (Svantesson, 2020: 55).

تحلیل ساختاری نشان می‌دهد که تکیه بر مفهوم سرزمینیِ کلاسیک در مواجهه با ماهیت غیرمادی داده‌ها، منجر به تقلیل جایگاهِ حقوقی دولت‌ها به نهادهایی ناکارآمد شده است که توانایی اعمالِ کنترلِ مؤثر بر فضای دیجیتال را ندارند. انسجامِ نظامِ حقوق بین‌الملل در گروی عبور از این دوگانگیِ سرزمینی/غیرسرزمینی است؛ چرا که داده‌ها، به عنوان پدیده‌هایی سیال، هیچ‌گونه انطباقی با ذاتِ ثابتِ قلمروهای فیزیکی ندارند و تقابلِ مفهومی میانِ این دو، تنها به تشدیدِ بحرانِ مشروعیتِ صلاحیت‌هایِ دولتی در عرصه‌یِ بین‌المللی می‌انجامد، بدونِ آنکه راهکارِ حقوقیِ پایداری برایِ مدیریتِ این جریان‌هایِ اطلاعاتی ارائه گردد.

بازخوانی نظریه کلاسیک «حاکمیت سرزمینی» در مواجهه با داده‌های غیرمستقر

نظریه کلاسیک حاکمیت سرزمینی که بر ارکان اصلیِ قلمروِ جغرافیایی، جمعیتِ تحتِ اقتدار و حکومتِ مستقر استوار است، همواره به عنوان سنگ‌بنای نظام بین‌المللی عمل کرده و صلاحیت دولت‌ها را در درون مرزهای فیزیکی تضمین نموده است. با ظهور و گسترش شبکه جهانی داده‌ها و استقرار فناوری‌های ذخیره‌سازی ابری، این مفهوم که داده‌ها و اطلاعات بایستی در محدوده سرزمینی یک دولت محصور باشند تا مشمول صلاحیت قضایی آن گردند، با چالش جدی روبرو شده است. در واقع، ماهیت غیرمستقر داده‌ها که به صورت قطعات خرد شده در سرورهای متعدد در اقصی نقاط جهان توزیع می‌شوند، پیوندِ میانِ حاکمیت و سرزمین را که در دکترین وستفالیایی امری بدیهی تلقی می‌شد، به امری انتزاعی و بحث‌برانگیز بدل ساخته است. از این منظر، زمانی که داده‌ها به صورتِ آنی از مرزهای مادی عبور می‌کنند، صلاحیت دولت‌ها بر اساس مکان فیزیکی ذخیره‌سازی، دیگر نمی‌تواند پاسخگوی نیازهای حفاظتی و نظارتی آن‌ها باشد (عراقی، ۱۳۹۹: ۷۲).

در تحلیل حقوقی، اصلِ تمامیت سرزمینی به عنوان ضمانت‌اجرایِ حاکمیت، در عصر داده‌های غیرمستقر دچار فرسایش شده است، زیرا دولت‌ها دیگر قادر نیستند سیطره مطلقِ خود را بر جریان اطلاعاتی که از طریق فضای سایبر وارد یا خارج می‌شود، اعمال نمایند. بر اساس اصولِ مندرج در منشور ملل متحد، دولت‌ها دارای

صلاحیتِ انحصاری بر امورِ داخلیِ خود هستند، اما زمانی که داده‌ها در فضای ابریِ فرامرزی قرار می‌گیرند، تشخیصِ اینکه کدام دولت واجد صلاحیتِ تقنینی یا قضایی است، به یک معضلِ حقوقیِ پیچیده تبدیل می‌شود. برخلاف اشیاء مادی که به راحتی می‌توان آن‌ها را در درون مرزها توقیف یا کنترل کرد، داده‌ها هیچ‌گونه پیوندِ واقعی و دائمی با یک قلمرو جغرافیایی ندارند و همین امر موجب شده است که مفاهیمِ سنتیِ صلاحیتِ سرزمینی در مواجهه با جریان‌هایِ دیجیتال، ناکارآمد به نظر برسند. این وضعیت، نوعی تعارضِ منافع میانِ حاکمیتِ دیجیتالِ دولت‌ها و ماهیتِ فرامرزیِ شبکه‌هایِ اطلاعاتی را پدید آورده است (شعبانی، ۱٤۰۰: ٥٦).

نظریه کلاسیک حاکمیت سرزمینی، در پاسخ به فشارهای ناشی از فناوری داده‌محور، دستخوش تفسیرهای موسعی شده است که سعی دارند صلاحیت دولت را به دارایی‌های دیجیتالیِ موجود در خارج از مرزها نیز تعمیم دهند. با این حال، استفاده از صلاحیت‌هایِ فرامرزی، خود باعث بروزِ تنش‌هایِ دیپلماتیک و تداخلِ صلاحیت‌ها میانِ دولت‌های مختلف گشته و بر ابهامِ حقوقیِ موجود در حکمرانیِ فضای سایبر افزوده است. در شرایطی که داده‌ها به صورتِ غیرمستقر وجود دارند، اصلِ سرزمینیِ کلاسیک دیگر نمی‌تواند به عنوان یک قاعده یگانه و کارآمد برای تعیینِ حقوق و تکالیفِ دولت‌ها عمل نماید. این خلاءِ نظری موجب شده است که بسیاری از محاکم بین‌المللی در پرونده‌هایِ مربوط به حریم خصوصی و امنیت داده‌ها، با استناد به معیارهایِ نوظهوری نظیرِ محلِ دسترسی یا محلِ انتفاع، از رویکردهایِ سنتیِ سرزمینی فاصله بگیرند (Goldsmith, ۲۰۱۸: ۱۱۲).

تنشِ میانِ دکترینِ وستفالیایی و ماهیتِ دیجیتال، به شکافی عمیق در نظم حقوقی بین‌الملل دامن زده که در آن دولت‌ها ناچارند برای جبرانِ ضعفِ نظارتیِ خود، به قوانینِ یک‌جانبه‌ای روی آورند که عملاً موجبِ نقضِ قواعدِ عرفیِ حاکم بر آزادیِ جریانِ اطلاعات می‌شود. در واقع، تلاشی که دولت‌ها برای حفظِ اقتدارِ خود در فضایِ سایبر انجام می‌دهند، اغلب از طریقِ اعمالِ صلاحیت بر سرورهایِ خارجی صورت می‌گیرد که خود، اصلِ عدمِ مداخله در امورِ داخلیِ دولت‌ها را زیر سوال می‌برد. این پارادوکس، نشان‌دهنده آن است که نظریه کلاسیک، توانایی هضمِ ماهیتِ غیرمستقرِ داده‌ها را ندارد و تداومِ اصرار بر انطباقِ این نظریه با شرایطِ نوین، جز به پیچیدگیِ بیشترِ مناسباتِ حقوقیِ بین‌المللی و تضعیفِ حاکمیتِ قانون نخواهد انجامید (کاتوزیان، ۱۳۹۷: ۲۳٤).

چالش اصلیِ پیش‌رو، بازتعریفِ مفهومِ اقتدارِ دولت در جهانی است که در آن، مرزهایِ مادی دیگر مانعی برایِ تبادلِ اطلاعات نیستند. نظریه کلاسیکِ حاکمیت، با تأکیدِ بر مکان‌مندی، در تقابلِ کامل با ماهیتِ پویایِ داده‌ها قرار دارد و این تقابل، دولت‌ها را به سویِ بازنگری در ارکانِ اصلیِ صلاحیتِ خود سوق داده است. اگرچه تلاش‌هایِ بین‌المللی برایِ تدوینِ کنوانسیون‌هایِ نوینِ سایبری در جریان است، اما هنوز هیچ اتفاق‌نظری در موردِ اینکه چگونه می‌توان حاکمیتِ سرزمینی را با دنیایِ داده‌هایِ غیرمستقر آشتی داد، وجود ندارد و این خلاءِ نظری، عرصه را برایِ خودکامگی‌هایِ سایبریِ دولت‌هایِ قدرتمند در توجیهِ صلاحیت‌هایِ فرامرزیِ خود فراهم کرده است .(Karns, 2021: 89)

تحلیل ساختاری گویای آن است که نظریه کلاسیک حاکمیت سرزمینی به دلیلِ اتکایِ مفرط به مولفه‌هایِ جغرافیایی، در مواجهه با ماهیتِ داده‌هایِ غیرمستقر، دچارِ بحرانِ انسجامِ مفهومی گردیده است. تقابل میانِ ثباتِ قلمرو و سیالیتِ داده‌ها، نه تنها قواعدِ سنتیِ صلاحیتِ تقنینی را بی‌اثر ساخته، بلکه موجبِ ایجادِ بی‌نظمی در اعمالِ صلاحیت‌هایِ قضایی نیز شده است؛ به نحوی که تداومِ این رویکردِ کلاسیک، عملاً ظرفیت‌هایِ حاکمیتیِ دولت‌ها را در حراست از حقوقِ شهروندی در فضایِ مجازیِ فرامرزی به حداقل رسانده و ضرورتِ گذارِ قطعی به دکترین‌هایِ نوینِ صلاحیتی را بیش از پیش نمایان می‌سازد.

اصل «عدم مداخله» در امور داخلی و تقابل با جریان فرامرزی داده‌ها

در الگوی کلاسیک (برگرفته از پرونده *نیکاراگوئه*)، مداخله زمانی محقق می‌شود که «عنصر اجبار» برای تحت تأثیر قرار دادن حوزه‌های در صلاحیت انحصاری دولت وجود داشته باشد. اما جریان فرامرزی داده‌ها، ماهیت این اجبار را دگرگون کرده است:

۱. **داده‌ها به مثابه ابزار نفوذ:** دسترسی فرامرزیِ دولت‌ها به داده‌های شهروندانِ دولتی دیگر (مثلاً از طریقِ درخواستِ مستقیم از شرکت‌های ارائه‌دهنده‌ی خدماتِ ابری) بدون توسل به سازوکارهای معاضدت قضایی بین‌المللی، به نوعی «مداخله در صلاحیتِ قضایی» و نقضِ اقتدارِ تقنینیِ دولتِ محل اقامتِ داده‌ها محسوب می‌شود.

۲. **داده‌های کلان و دستکاریِ اراده‌ی ملی:** در سطحی عمیق‌تر، بهره‌برداری از تحلیل‌های کلان‌داده رای جهت‌دهی به افکار عمومی یا دخالت در فرآیندهای انتخاباتیِ یک کشورِ دیگر، اگرچه فاقدِ مؤلفه‌یِ «اعمال زورِ فیزیکی» است، اما به عنوان «اجبارِ ساختاری» شناخته می‌شود. اینجا تقابل میانِ «آزادیِ جریانِ اطلاعات» و «حاکمیتِ دیجیتال» به اوج می‌رسد (منوچهری، ۱٤۰۱: ۱۱۲).

چالش‌های انتساب و «مراقبت بایسته» (Due Diligence)

در حقوق بین‌الملل عمومی، دولت‌ها مکلف‌اند (به موجبِ اصلِ مراقبت بایسته) اجازه ندهند از سرزمین‌شان برای اقدامات زیان‌بار علیه دولت‌های دیگر استفاده شود. در فضای سایبر، این تکلیف با مشکلِ «غیرمستقر بودن» داده‌ها گره خورده است:

- **ابهام در قلمرو:** وقتی داده‌ای در یک سرورِ توزیع‌شده قرار دارد، دولتِ «میزبان» چگونه می‌تواند از «مداخله» علیه دولتِ «مبدأ» جلوگیری کند؟
- **سلبِ مسئولیت دولت‌ها:** این وضعیت باعث شده است که برخی دولت‌ها با بهره‌گیری از «عدم قطعیت در انتساب»، عملاً به جریانِ فرامرزیِ داده‌ها به عنوان ابزاری برای مداخله‌ی نرم در امورِ داخلیِ دیگران نگاه کنند، بدون آنکه مسئولیتِ بین‌المللیِ آن‌ها به‌راحتی قابل اثبات باشد (سادات‌میدانی، ۱۳۹۹: ۸۸).

تحلیل انتقادی: ناکارآمدی رویکرد ایستا

اصرار بر قرائت سنتی از مداخله (که تنها مداخلاتِ آشکار و نظامی را در بر می‌گیرد) باعث شده است که بخشِ وسیعی از «مداخلاتِ سایبری» در یک خلأ حقوقی باقی بمانند. برای دفاع از رساله‌ی دکتری در این حوزه، بایسته است استدلال کنید که **«اجبار» باید بازتعریف شود.**

امروزه، «اجبار» در حقوق بین‌الملل باید شامل مواردی شود که در آن، دولت با بهره‌گیری از زیرساخت‌هایِ داده‌ای، «اختیارِ تصمیم‌گیریِ مستقل» را از دولتِ هدف سلب می‌کند. این همان نقطه‌ای است که «اصل عدم مداخله» باید از قلمرو فیزیکی به «قلمرو داده‌محور» گسترش یابد (Kunz, 2022: 45).

تقابل میانِ جریانِ فرامرزی داده‌ها و اصل عدم مداخله، نشان‌دهنده‌ی یک گسستِ تاریخی در حقوق بین‌الملل است. نظام حقوقی نمی‌تواند با ابزارهای «وستفالیایی» به جنگِ «واقعیت‌های دیجیتال» برود. پیشنهادِ علمی برای رساله‌ی شما این است: **تأسیس «هنجارهای رفتاری در فضای سایبر»** که در آن استخراجِ فرامرزیِ داده‌ها بدون رعایتِ تشریفاتِ قانونی، به عنوان نقضِ ابتداییِ اصلِ عدم مداخله شناخته شود.

دولت‌ها و چالشِ استقلالِ دیجیتال

تحولِ مفاهیم کلاسیک حقوق بین‌الملل در بستر تعاملات الکترونیک، دولت‌ها را با چالش‌های بنیادینی در حفظ اقتدار سرزمینی خویش مواجه ساخته است. در نظام‌های حقوقی پیشین، حاکمیت به عنوان اقتدار بر قلمرو فیزیکی تعریف می‌شد، حال آنکه در عصر دیجیتال، این مفهوم به سوی نوعی استقلال زیرساختی و کنشگری فعال در مدیریت فضای سایبر تغییر جهت داده است. استقلال دیجیتال به معنای توانمندی دولت در اعمال اراده و تدوین سیاست‌های خودگردان بدون وابستگی استراتژیک به پلتفرم‌های خارجی است که اغلب توسط شرکت‌های چندملیتی مدیریت می‌شوند. این وابستگی، نه تنها امنیت ملی را تهدید می‌کند، بلکه موجب تزلزل در اعمال صلاحیت‌های تقنینی و قضایی دولت بر داده‌های متعلق به اتباع می‌گردد. در واقع، بسیاری از دولت‌ها با بهره‌گیری از اصل حاکمیت ملی و با اتکا به منشور ملل متحد که بر برابری حاکمیت دولت‌ها تأکید دارد، در پی ایجاد سپرهای نظارتی بر زیرساخت‌های کلیدی اطلاعاتی خود هستند تا از مداخلات نرم‌افزاری و نفوذهای ناخواسته در شئون حاکمیتی جلوگیری نمایند (ضیایی، ۱۳۹۹: ۱۱۲).

پدیده‌ی استقلال دیجیتال، صرفاً یک داعیه‌ی سیاسی نیست، بلکه ریشه در ضرورت حفاظت از نظم عمومی و حقوق بنیادین شهروندان دارد که در قالب صلاحیتِ سرزمینی دولت بر فعالیت‌های مجازی قابل تبیین است. از دیدگاه حقوق بین‌الملل عمومی، دولت‌ها موظف به تأمین امنیتِ فضایِ زیستِ دیجیتال اتباع خویش هستند و این تعهد، اقتضا می‌کند که کنترلِ فنی و حقوقیِ لایه‌های زیرساختی از دسترسیِ بازیگرانِ غیردولتیِ خارجی خارج گردد. شرکت‌های فناوری با استناد به مدل‌های کسب‌وکار جهانی، اغلب از تن دادن به قوانین داخلی دولت‌ها سر باز می‌زنند که این امر موجب ایجاد خلأهای صلاحیتی در اجرای عدالت می‌گردد. مطابق با ماده ۲ منشور ملل متحد که بر عدم مداخله در امور داخلی دولت‌ها صحه می‌گذارد، تلاش دولت‌ها برای کسب

استقلال در حوزه فناوری، دفاعی مشروع از حریم حاکمیت در برابر نفوذهای سایبری است که می‌تواند تمامیت سیاسی و اقتصادی یک کشور را به مخاطره افکند و نظمِ موجود را برهم زند (موسی‌زاده، ۱٤۰۱: ۸۵).

چالش‌های حقوقی در مسیر استقلال دیجیتال زمانی به اوج می‌رسد که مقررات داخلی دولت‌ها برای محدودسازی یا کنترل جریان داده‌ها، با تعهدات بین‌المللیِ مرتبط با تجارت آزاد و انتقال داده‌ها در سازمان تجارت جهانی تعارض پیدا می‌کند. دولت‌ها در تلاش برای اعمال اقتدار خود بر زیرساخت‌های دیجیتال، اغلب با واکنش‌های حقوقی در قالب اقدامات متقابل یا اعتراضات دیپلماتیک مواجه می‌شوند که تحلیل این تقابل نیازمند بازنگری در معیارهای مراقبت بایسته است. در این میان، تدوین سیاست‌های بومی‌سازی داده‌ها یا الزام به میزبانی محلی سرورها، نمونه‌هایی از تلاش‌های تقنینی برای بازپس‌گیری حاکمیت سایبری است که می‌بایست با حقوق بشر بین‌الملل و اصول آزادی تبادل اطلاعات همخوانی داشته باشد تا به نقض تعهدات بین‌المللی منجر نگردد. حقوق بین‌الملل معاصر باید چارچوبی را تعریف نماید که در آن دولت‌ها ضمن برخوردار بودن از حقِ اعمال صلاحیت بر فضای سایبری قلمرو خود، به استانداردهای حداقلیِ عدم تبعیض و شفافیت پایبند بمانند (جلیلی، ۱٤۰۲: ٤۵).

مسئله‌ی وابستگی به بازیگران بیگانه در لایه‌های نرم‌افزاری، چنان عمیق است که حتی مفاهیم سنتی مالکیت و کنترل را نیز دستخوش تغییر نموده است. زمانی که بخش اعظم داده‌های حساسِ یک کشور در بسترهای ابری که در مالکیت اشخاص حقوقی خارجی است ذخیره می‌گردد، عملاً مفهومِ صلاحیتِ سرزمینی به چالش کشیده می‌شود و دولت به جای اعمال حاکمیت، به نوعی مستأجرِ فضای دیجیتال تبدیل می‌گردد. این وضعیت باعث شده است که اندیشمندانِ حقوق بین‌الملل بر ضرورت تعریفِ جدیدی از صلاحیت عملکردی در فضای سایبر تأکید ورزند تا دولت‌ها بتوانند با ابزارهای حقوقیِ نوین، بر فعالیت‌هایی که تأثیرِ مستقیم بر نظمِ عمومیِ کشور دارند، اعمال نظارت نمایند. اعمال صلاحیت بر این داده‌ها، در پرتوِ حقوقِ بین‌المللِ سایبر، نیازمندِ توافقاتِ چندجانبه‌ای است که ضمنِ احترام به حقِ حاکمیتِ دیجیتال، امنیتِ داده‌ها را در برابر دسترسی‌هایِ غیرمجاز تضمین نماید (شیروی، ۱٤۰۰: ۲۱۰).

تلاش دولت‌ها برای تحقق استقلال دیجیتال، فراتر از یک رویکرد فنی، نشان‌دهنده یک تغییر پارادایم در نظریه حاکمیت است که در آن فضا به عنوان یک دارایی استراتژیک در نظر گرفته می‌شود. با این حال، استفاده از

ابزارهای نظارتی برای تثبیت این استقلال می‌تواند زمینه‌ساز ایجاد حصارهای دیجیتال شود که توازن میان حاکمیت و دسترسی به دانش جهانی را برهم زند. از منظر حقوق عمومی بین‌الملل، چالشِ اصلی در اینجا ایجادِ تعادل بینِ اعمالِ حقِ حاکمیت برایِ حفاظت از زیرساخت‌هایِ حیاتی و رعایتِ حقوقِ بنیادینِ دسترسیِ شهروندان به اطلاعات است که به عنوانِ یک هنجارِ پذیرفته‌شده در اسنادِ بین‌المللیِ حقوقِ بشر شناسایی شده است. لذا دولت‌ها باید از رهگذرِ ایجادِ کنوانسیون‌های منطقه‌ای و جهانی، قواعدی را تدوین نمایند که در آن استقلال دیجیتال به جای انزواطلبی، منجر به تقویتِ نظامِ حکمرانیِ سایبری و مسئولیت‌پذیریِ بین‌المللیِ تمامیِ بازیگران، اعم از دولت‌ها و شرکت‌هایِ بزرگِ فناوری، گردد (ممتاز، ۱۳۹۸: ۱۷۸).

در این بخش، ماهیت حقوقی استقلال دیجیتال به عنوان محملی برای بازتعریف حدود صلاحیت‌های سرزمینی و حفاظتی دولت‌ها در مواجهه با قدرت‌های غیردولتی سایبری مورد ارزیابی قرار گرفت. چالش اصلی در اینجا فقدان یک نظام هنجاری منسجم است که بتواند اقتدار حاکمیتی دولت‌ها را با جریان آزاد داده‌ها در بسترهای جهانی آشتی دهد؛ به گونه‌ای که اعمال صلاحیت‌های دولتی نه به عنوان رفتاری خودسرانه، بلکه به عنوان ضرورتی برای حفظ ثبات و امنیت بین‌المللی در فضای مجازی تلقی گردد و از بروز تنش‌های حقوقی و دیپلماتیک در حوزه فضای سایبر پیشگیری شود.

صلاحیت دولت بر داده‌های اتباع در خارج از مرزها (صلاحیت شخصی)

اعمال صلاحیت بر داده‌های اتباع در خارج از مرزهای سرزمینی، یکی از پیچیده‌ترین مباحث در نظریه حقوق بین‌الملل معاصر است که پیوند عمیقی با مفهوم «صلاحیت شخصی» دارد. در سنت حقوقی کلاسیک، صلاحیت دولت بر پایه قلمرو فیزیکی استوار بود، اما امروزه داده‌های اتباع به عنوان امتداد شخصیت حقوقی یا ابزار ارتباطی آنان، مبنایی برای اعمالِ صلاحیتِ فراسرزمینی ایجاد کرده‌اند. این رویکرد بیان می‌دارد که هر دولتی این حق را دارد که بر فعالیت‌های سایبری اتباع خود، فارغ از موقعیت جغرافیایی سرورها، اعمال اقتدار نماید؛ چرا که داده‌ها، در واقع، بازتابی از هویت و حقوق بنیادین اتباع در فضای مجازی هستند. با این وجود، تسری صلاحیت دولت مبدأ به حوزه‌ی قضایی دولتِ میزبان، همواره با مقاومت‌های حقوقی در قالب اصل عدم مداخله و احترام به حاکمیت سرزمینی دیگر دولت‌ها روبرو بوده است و این پرسش را مطرح می‌سازد که آیا صلاحیت شخصی می‌تواند به تنهایی توجیه‌گرِ اعمالِ قدرتِ قهرآمیزِ سایبری باشد (صدقی، ۱٤۰۰: ۵۵).

اعمال صلاحیت فراسرزمینی بر داده‌ها، غالباً در چارچوب‌های قانون‌گذاری ملی نظیر «قانون ابر» ایالات متحده نمود می‌یابد که به دولت اجازه می‌دهد به داده‌های موجود در سرورهای خارجی دسترسی پیدا کند. این اقدام، اگرچه با هدف تعقیب جرایم بین‌المللی و تضمین امنیت عمومی توجیه می‌شود، اما در تعارض آشکار با صلاحیتِ سرزمینی دولتِ میزبانِ سرور قرار دارد و می‌تواند منجر به ایجاد بحران‌های صلاحیت میان دولت‌ها گردد. حقوق بین‌الملل عرفی در این زمینه همچنان در حال تکوین است و فاقد رویه‌ای یکدست برای حل‌وفصل این قبیل تعارضات می‌باشد. دولت‌هایی که تحت تأثیرِ دسترسی‌هایِ فراسرزمینیِ دولت‌های دیگر قرار می‌گیرند، این اقدام را نقضِ تمامیتِ حاکمیتیِ خود تلقی کرده و آن را به مثابه مداخله در صلاحیت قضایی خویش می‌دانند؛ وضعیتی که مستلزمِ تدوینِ پروتکل‌هایِ همکاریِ دوجانبه یا چندجانبه برایِ جلوگیری از اصطکاک‌های حقوقی بین‌المللی است (بیگ‌زاده، ۱۳۹۸: ۱۱۹).

چالش بنیادین در اینجا، ماهیت «غیرمستقر» داده‌هاست که اصلِ سرزمینی بودن صلاحیت را که در قضایای تاریخی دیوان بین‌المللی دادگستری بر آن تأکید شده بود، به چالش می‌کشد. در زمانی که داده‌ها به صورت قطعه‌قطعه در سرورهای متعدد در اقصی نقاط جهان ذخیره می‌شوند، انتسابِ صلاحیتِ شخصیِ محض به یک دولتِ خاص، بسیار دشوار است و نیازمندِ معیارهایِ پیوندِ سرزمینی یا شخصیِ قوی‌تری می‌باشد. حقوقدانان بر این باورند که صلاحیت بر داده‌های اتباع در خارج از مرزها، تنها زمانی مشروعیت می‌یابد که با رعایت حقوق بنیادینِ شهروندان و حفظِ حریمِ خصوصیِ آنان در فرآیندِ تبادلِ اطلاعات همراه باشد، در غیر این صورت، این صلاحیت به ابزاری برای نظارتِ گسترده و نقضِ اصولِ دادرسیِ عادلانه تبدیل خواهد شد که با روحِ منشورِ ملل متحد در تضاد است (مستقیمی، ۱۳۹۷: ۷۲).

از منظرِ رویه‌یِ قضایی، بسیاری از کشورها تلاش کرده‌اند با انعقادِ توافق‌نامه‌هایِ معاضدتِ قضاییِ دوجانبه ((MLAT، خلأهای ناشی از صلاحیتِ شخصی را پر کنند و از توسل به اقداماتِ یک‌جانبه پرهیز نمایند. با این حال، کُندیِ فرآیندهایِ قضاییِ این توافق‌نامه‌ها در عصرِ سرعتِ سایبری، دولت‌ها را به سویِ استفاده از قوانینِ یک‌جانبه سوق داده است که خود، نشان‌دهنده‌یِ ناکارآمدیِ سیستم‌هایِ کلاسیکِ معاضدتِ قضایی در مواجهه با واقعیت‌هایِ فناوریِ نوین است. در این راستا، بازخوانیِ مفهومِ صلاحیتِ شخصی باید به‌گونه‌ای صورت پذیرد که دولت‌ها ضمنِ حفظِ توانمندیِ اعمالِ اقتدارِ قضایی بر اتباعِ خود، از حقوقِ حاکمیتیِ دولت‌هایِ دیگر در

سرزمین‌شان احترام بگذارند و از اقداماتِ خودسرانه‌ای که می‌تواند تعادلِ بین‌المللی را برهم زند، اجتناب ورزند (زمانی، ۱٤۰۱: ۹۸).

بسیاری از تحلیلگران معتقدند که صلاحیتِ شخصی بر داده‌ها باید تحتِ ضابطه‌یِ «اثراتِ مستقیم» تفسیر گردد، به این معنا که دولت تنها زمانی حق اعمال صلاحیت بر داده‌های خارج از مرز را دارد که فعالیت‌های مرتبط با آن داده‌ها، تأثیرِ مخرب و مستقیم بر منافعِ حیاتی یا نظم عمومی دولتِ متبوع داشته باشد. این رویکرد، در واقع، سعی دارد تا دایره‌یِ صلاحیتِ فراسرزمینی را محدود کرده و از بسطِ نامحدودِ قدرتِ قضاییِ دولت‌ها جلوگیری کند. بدونِ این محدودیت‌هایِ مفهومی، صلاحیتِ شخصی بر داده‌ها می‌تواند به بهانه‌ای برای مداخلاتِ گسترده در قلمروِ سایبریِ دیگر کشورها تبدیل شود و امنیتِ حقوقیِ تجارتِ بین‌الملل و جریانِ آزادِ اطلاعات را به شدت تهدید نماید، بنابراین نیاز به یک اجماعِ هنجاری در حقوق بین‌الملل برایِ تبیینِ دقیقِ محدوده‌هایِ صلاحیتِ شخصی در فضایِ مجازی کاملاً ملموس است (شیروی، ۱٤۰۲: ۱۸۵).

در این بحث، ملاحظه گردید که صلاحیت شخصی به عنوان یکی از مبانیِ اعمالِ اقتدار بر داده‌های خارج از مرز، با چالش‌هایِ جدی در حوزه حاکمیت سرزمینی و تعارض منافع مواجه است. آنچه از تحلیلِ این مبحث حاصل می‌شود، عدم امکانِ استنادِ مطلق به صلاحیتِ شخصی در دنیایِ به هم پیوسته‌یِ دیجیتال است؛ چرا که بسطِ غیرمتناسبِ این صلاحیت، بدونِ در نظر گرفتنِ حاکمیتِ سرزمینیِ دولتِ میزبانِ داده، می‌تواند منجر به هرج‌ومرجِ صلاحیتی و تضعیفِ نظمِ عمومیِ بین‌المللی گردد. ساختارِ فعلیِ صلاحیتِ شخصی، نیازمندِ تحولی بنیادین است تا با ماهیتِ سیالِ داده‌ها و نیازهایِ حاکمیتیِ دولت‌ها در عصرِ فناوری سازگار گردد.

چالشِ محلی‌سازی داده‌ها و تضاد آن با آزادی تجارت

سیاست‌های محلی‌سازی داده‌ها که دولت‌ها را ملزم می‌سازد تا داده‌هایِ تولیدشده توسطِ اتباع یا کسب‌وکارهایِ داخلی را در سرورهایِ فیزیکیِ مستقر در درونِ مرزهایِ خود ذخیره و پردازش کنند، در واقع تلاشی برای بازگرداندنِ حاکمیت به قلمروِ سرزمینی در عصرِ جریانِ بی‌مرزِ اطلاعات است. این تدابیرِ تقنینی با هدفِ تضمینِ دسترسیِ مقاماتِ قضایی و امنیتی به داده‌ها برایِ اعمالِ صلاحیتِ قانونی طراحی شده‌اند، اما در عین حال، مانعی بزرگ بر سرِ راهِ فعالیتِ پلتفرم‌هایِ دیجیتالِ جهانی ایجاد می‌نمایند. از منظرِ حقوق تجارتِ

بین‌الملل، تحمیلِ هزینه‌هایِ اضافی برایِ ایجادِ زیرساخت‌هایِ محلی، نوعی «محدودیتِ غیرتعرفه‌ای» محسوب می‌شود که می‌تواند با تعهداتِ ناشی از «موافقت‌نامه عمومی تجارت خدمات» در تعارض باشد. دولت‌ها با استناد به حقِ حاکمیتِ دیجیتال، استدلال می‌کنند که حفاظت از داده‌هایِ کلان، در زمره امنیتِ ملی قرار دارد، حال آنکه شرکایِ تجاری این اقدامات را ابزاری برای تبعیض میانِ ارائه‌دهندگانِ خدماتِ داخلی و خارجی تلقی می‌نمایند (سیدزاده، ۱٤۰۱: ۱۳٤).

تنش میانِ استقلالِ حاکمیتی و آزادیِ تجارت، در پرونده‌هایِ متعددی در نظام‌هایِ داوریِ بین‌المللی بازتاب یافته است، جایی که دولت‌ها سعی دارند اقداماتِ خود را تحتِ عنوانِ «استثنائاتِ عمومی» یا «حفاظت از حریمِ خصوصی» موجه جلوه دهند. با این حال، شرطِ ضرورت در موافقت‌نامه‌هایِ تجاری ایجاب می‌کند که هرگونه مداخله‌یِ دولتی در جریانِ آزادِ داده‌ها، باید به حداقلِ لازم برایِ رسیدن به هدفِ مشروع محدود گردد و نباید به گونه‌ای طراحی شود که تبعیضِ پنهان علیه خدماتِ خارجی را دامن بزند. در بسیاری از موارد، قوانینِ محلی‌سازی داده‌ها به دلیلِ فقدانِ شفافیت و تحمیلِ بارهایِ اداریِ طاقت‌فرسا، با اصلِ «رفتارِ ملی» مندرج در مقرراتِ سازمانِ تجارتِ جهانی در تضاد قرار می‌گیرند. این تقابلِ حقوقی، دولت‌ها را در یک دوراهیِ دشوار قرار داده است: انتخاب میانِ تثبیتِ اقتدارِ حاکمیتی بر فضایِ سایبر یا پایبندی به تعهداتِ چندجانبه برایِ بهره‌مندی از منافعِ اقتصادیِ جریانِ آزادِ اطلاعات که برایِ رشدِ اقتصادی در عصرِ دیجیتال حیاتی است (حبیبی، ۱٤۰۰: ۹۲).

در سطحی عمیق‌تر، این چالشِ محلی‌سازی، بازتابی از یک پارادوکس در نظامِ حکمرانیِ جهانی است که در آن، مفاهیمِ سنتیِ «کالا» و «خدمت» در بسترِ دارایی‌هایِ دیجیتال تغییر شکل داده‌اند. حقوق بین‌المللِ تجارت، که عمدتاً برایِ مبادلاتِ فیزیکی طراحی شده بود، اکنون در مواجهه با ماهیتِ سیالِ داده‌ها، ابزارهایِ تحلیلیِ کافی برایِ تعیینِ دقیقِ قلمروِ صلاحیتِ دولت‌ها را در اختیار ندارد. دولت‌هایی که سیاست‌هایِ سخت‌گیرانه محلی‌سازی را اعمال می‌کنند، به دنبالِ ایجادِ نوعی «سدِ دیجیتال» هستند که در تقابلِ با روحِ «تجارتِ آزادِ فرامرزی» قرار دارد، چرا که ماهیتِ اینترنت بر پایه دسترسیِ جهانی و سرعتِ بالایِ انتقالِ داده‌ها استوار است. تداومِ این سیاست‌ها می‌تواند به «تکه‌تکه‌شدنِ اینترنت»منجر گردد، وضعیتی که در آن زنجیره‌هایِ تأمینِ جهانی

در حوزه دیجیتال با موانعِ حقوقیِ متعددی مواجه شده و هزینه نهایی برای مصرف‌کنندگان و کسب‌وکارها افزایش می‌یابد (فیض‌بخش، ۱۳۹۹: ۲۱۵).

از سوی دیگر، باید توجه داشت که استانداردهایِ بین‌المللی برایِ جریانِ آزادِ داده‌ها همچنان در حالِ تکوین هستند و هنوز چارچوبِ جامعِ الزام‌آوری که بتواند همزمان حقوقِ حاکمیتیِ دولت‌ها و منافعِ تجارتِ بین‌الملل را تأمین نماید، وجود ندارد. در فقدانِ چنین سازوکاری، کشورهایِ پیشرو در حوزه فناوری با انعقادِ توافق‌نامه‌هایِ دوجانبه، سعی دارند جریان‌هایِ داده‌ایِ موردِ تأییدِ خود را ایجاد نمایند که این امر خود می‌تواند به ایجادِ «بلوک‌هایِ دیجیتال» منجر شود که در تقابل با جهان‌شمول‌بودنِ حقوقِ تجارتِ بین‌الملل است. بررسیِ رویه‌یِ کشورهایِ مختلف نشان می‌دهد که مدل‌هایی که بر «جریانِ آزادِ داده‌ها با اعتماد» (Data Free Flow with Trust) تأکید دارند، بیشترین اقبال را در میانِ بازیگرانِ اقتصادیِ بزرگ به دست آورده‌اند؛ مدلی که تلاش می‌کند بدونِ تحمیلِ محلی‌سازیِ فیزیکی، استانداردهایِ لازم برایِ امنیت و حریمِ خصوصی را تضمین نماید (قربانی، ۱٤۰۲: ۵۸).

در نهایت، تنشِ میانِ محلی‌سازیِ داده‌ها و آزادیِ تجارت، نشان‌دهنده شکستِ قالب‌هایِ حقوقیِ کلاسیک در فهمِ ماهیتِ داده‌هایِ کلان به عنوانِ یک داراییِ همزمانِ استراتژیک و تجاری است. ضرورتِ ایجادِ یک رژیمِ حقوقیِ نوین که در آن ابزارهایِ نظارتیِ دولت‌ها برایِ حفاظت از امنیتِ سایبری، با مکانیسم‌هایِ استانداردِ بین‌المللی برایِ تسهیلِ تجارتِ دیجیتال تلفیق گردد، بیش از هر زمانِ دیگری احساس می‌شود. این رژیمِ احتمالی باید فراتر از رویکردهایِ سنتیِ محلی‌سازی، به دنبالِ تعریفِ استانداردهایِ فنی و حقوقیِ مشترکی باشد که امکانِ «اعمالِ حاکمیت» را بدونِ ایجادِ «موانعِ تجاری» برایِ بازیگرانِ فعال در بازارِ جهانی فراهم آورده و از قطبی‌شدنِ فضایِ سایبر جلوگیری نماید (جعفری، ۱٤۰۱: ۱۱۰).

این مبحث به تبیین تضاد ساختاری میان حاکمیت سرزمینی در قالب محلی‌سازی داده‌ها و اصل آزادی مبادلات در حقوق تجارت بین‌الملل پرداخت. چالش اساسی که در اینجا مشهود است، ناکارآمدی مقررات سنتی سازمان تجارت جهانی در انطباق با واقعیت‌های فنی فضای مجازی و ضرورت بازنگری در مفهوم اعمال صلاحیت دولت‌هاست؛ به گونه‌ای که ضمن حفظ اقتدار دولتی در محافظت از داده‌ها، از ایجاد دیوارهای تعرفه‌ای و

غیرتعرفه‌ای دیجیتال که منجر به اختلال در بازارهای جهانی و تضعیف زنجیره ارزش فناوری می‌گردد، پیشگیری به عمل آید تا ثبات حقوقی در نظام مبادلات بین‌المللی تداوم یابد.

موقعیتِ حقوقیِ شرکت‌های بزرگ تکنولوژی به مثابه شبه‌دولت‌ها

ظهور شرکت‌هایِ فراملیِ فناوری که از نظر توانمندیِ مالی و زیرساختی از بسیاری از دولت‌هایِ کوچک پیشی گرفته‌اند، موازنه قدرتِ سنتی را در حقوق بین‌الملل دگرگون ساخته است. این نهادها، با کنترل بر جریانِ اطلاعات، مدیریتِ پلتفرم‌هایِ اجتماعی و توسعه‌یِ الگوریتم‌هایِ تصمیم‌گیر، عملاً واجدِ کارکردهایی شده‌اند که پیش‌تر در انحصارِ دولت‌ها بود؛ از جمله «قانون‌گذاری» از طریقِ شرایطِ استفاده ، «قضاوت» در فرآیندِ تعدیلِ محتوا و «اجرایِ احکام» با مسدودسازیِ دسترسیِ کاربران. این عملکردِ شبه‌حاکمیتی باعث شده است که مرز میانِ حقوقِ خصوصیِ تجاری و اقتدارِ عمومیِ دولتی در فضای سایبر به شدت مخدوش گردد. بر اساس دیدگاه‌هایِ نوین، شرکت‌هایِ بزرگ فناوری نه تنها بازیگرانِ اقتصادیِ صرف، بلکه حاکمانِ غیرمنتخبِ فضای دیجیتال هستند که نظمِ حقوقیِ داخلی و بین‌المللی را تحتِ تأثیر قرار داده و دولت‌ها را در اعمالِ صلاحیت‌هایِ سرزمینی‌شان با چالش‌هایِ جدی روبرو ساخته‌اند .(Floridi, 2020: 145)

اعمال قدرتِ این بازیگرانِ خصوصی، بدونِ نظارتِ دموکراتیک و پاسخگوییِ قانونیِ متناسب با قدرتِ آن‌ها، مشروعیتِ نظامِ حقوقیِ دولت‌ها را در مدیریتِ حوزه‌هایِ عمومیِ سایبری به چالش می‌کشد. برایِ مثال، زمانی که یک شرکتِ پلتفرمی اقدام به تغییرِ سیاست‌هایِ حریمِ خصوصی می‌کند، عملاً بر حقوقِ بنیادینِ میلیون‌ها شهروندِ چندین کشور اثر می‌گذارد، بدون اینکه در قبالِ این اقدام در برابرِ مرجعِ قانونیِ مشخصی پاسخگو باشد. این وضعیتِ حقوقی، دولت‌ها را واداشته است تا در چارچوبِ «مسئولیتِ شرکت‌هایِ فراملی» در حقوقِ بین‌الملل، به دنبالِ مکانیسم‌هایی برایِ کنترلِ این قدرتِ بی‌حدوحصر باشند. در حقوقِ بین‌المللِ معاصر، این بحث مطرح است که آیا این شرکت‌ها، فراتر از تعهداتِ قراردادی، دارایِ «تعهداتِ حقوقِ بشریِ بین‌المللی» هستند یا خیر؛ موضوعی که در اسنادِ سازمانِ ملل در بابِ کسب‌وکار و حقوقِ بشر نیز به آن اشاره شده است (کدخدایی، ۱٤۰۱: ۱۱۲).

چالشِ حقوقیِ دیگر، تضادِ منافع میانِ مدل‌هایِ کسب‌وکارِ این شرکت‌ها و اهدافِ عمومیِ دولت‌هاست که در قالبِ استفاده از الگوریتم‌هایِ هدایت‌گرِ رفتارِ کاربران مشاهده می‌شود. شرکت‌هایِ فناوری با بهینه‌سازیِ محتوا برایِ افزایشِ نرخِ تعامل، عملاً بر افکارِ عمومی و فرآیندهایِ سیاسیِ داخلیِ دولت‌ها تأثیر می‌گذارند که این امر می‌تواند مصداقِ نوعی «مداخله‌یِ غیرمستقیم» در امورِ داخلیِ دولت‌ها تلقی گردد. در چنین بستری، مفاهیمِ سنتیِ «شرکتِ خصوصی» که بر مبنایِ قراردادهایِ تجاریِ ساده بنا شده‌اند، دیگر برایِ تحلیلِ نقشِ این غول‌هایِ فناوری کفایت نمی‌کنند. حقوقدانانِ برجسته‌ای همچون شوشانا زوبوف، این وضعیت را «سرمایه‌داریِ نظارتی» می‌نامند که در آن شرکت‌ها با جمع‌آوریِ داده‌هایِ رفتاری، شکلی از قدرتِ حاکمیتی را اعمال می‌کنند که دولت‌ها را در پیگیریِ سیاست‌هایِ عمومیِ خود خنثی می‌سازد .(Zuboff, 2019: 98)

از منظرِ حقوقِ مسئولیتِ بین‌المللی، انتسابِ اقداماتِ این شرکت‌ها به دولت‌ها یا مسئولیتِ مستقیمِ خودِ شرکت‌ها، یک معضلِ حقوقیِ حل‌نشده است. اگر دولتی به واسطه‌یِ ناتوانی در تنظیمِ رفتارِ این شرکت‌ها، اجازه دهد که حقوقِ اتباعش در فضایِ مجازی نقض شود، آیا می‌توان آن دولت را مسئول دانست؟ یا اینکه باید رژیمِ حقوقیِ مستقلی برایِ پاسخگوییِ مستقیمِ این شرکت‌ها در مراجعِ قضاییِ بین‌المللی تعریف کرد؟ این مسئله به‌ویژه در پرونده‌هایی که به تخریبِ دموکراسی یا نقضِ حریمِ خصوصی در ابعادِ گسترده مربوط می‌شود، اهمیتِ حیاتی می‌یابد. نبودِ یک «معاهده جهانیِ فضای سایبر» باعث شده است که این شرکت‌ها در خلأ قانونی عمل کرده و با بهره‌گیری از تفاوتِ قوانینِ ملی، استانداردهایِ حقوقیِ خود را بر دولت‌ها تحمیل نمایند که خود نمونه بارزی از افولِ صلاحیتِ تقنینیِ دولت‌ها در عصرِ حاضر است (قاری‌سیدفاطمی، ۱۳۹۹: ۸۸).

در پایان، این موقعیتِ شبه‌حاکمیتیِ شرکت‌هایِ تکنولوژی، پارادایمِ حقوقِ بین‌الملل را از حاکمیتِ انحصاریِ دولت‌ها به سمتِ حکمرانیِ چندلایه سوق داده است. دولت‌ها دیگر یگانه قانون‌گذار در قلمروِ خود نیستند و باید با شرکت‌هایی که از نظر قدرتِ فنی و نفوذِ اجتماعی با آن‌ها رقابت می‌کنند، واردِ تعاملِ ساختاری شوند. این تحول، نیازمندِ بازخوانیِ مفهومِ «بازیگر» در حقوق بین‌الملل و تعریفِ مسئولیت‌هایی است که فراتر از چارچوب‌هایِ کلاسیکِ حقوقِ تجارتِ بین‌الملل است. باید سازوکارهایِ بین‌المللیِ جدیدی تأسیس شود که بتواند قدرتِ این شرکت‌ها را در چارچوبِ حاکمیتِ قانونِ بین‌المللی محدود کرده و از تبدیل شدنِ آن‌ها به

«دولت‌هایِ در سایه» که خارج از دسترسِ عدالت هستند، جلوگیری به عمل آورد تا ثباتِ حقوقیِ نظمِ بین‌المللی حفظ گردد (Smith, 2021: 210).

تحلیلِ این بخش نشان می‌دهد که ماهیتِ قدرتِ شرکت‌های بزرگ فناوری، از یک رابطه‌یِ تجاریِ ساده به یک رابطه‌یِ حاکمیتیِ غیررسمی تغییر یافته است که ساختارهایِ حقوقیِ فعلیِ دولت‌محور را با بحرانِ کارآمدی مواجه کرده است. تقابلِ قدرتِ انحصاریِ این شرکت‌ها با اقتدارِ عمومی، منجر به ایجادِ یک خلأ حکمرانی شده که در آن اصولِ سنتیِ حقوقِ بین‌الملل، از جمله حاکمیت و مسئولیت، با چالشِ انتسابِ قدرتِ واقعی به نهادهایِ غیردولتی مواجه‌اند و این روند، ضرورتِ تدوینِ قواعدِ آمره در فضایِ سایبر را جهتِ تنظیمِ رفتارِ بازیگرانِ شبه‌حاکمیتی بیش از پیش نمایان می‌سازد.

تنش میان حاکمیت داده‌ای دولت‌ها و حقوق بنیادینِ کاربران

دولت‌ها با تمسک به مفهومِ حاکمیت داده‌ای، در پیِ اعمالِ صلاحیت بر جریان‌های اطلاعاتی هستند تا امنیتِ ملی و ثباتِ اجتماعی را تضمین کنند؛ اما این رویکردِ «دولت‌محور» اغلب با حقوقِ بنیادینِ کاربران از قبیل حقِ حریمِ خصوصی، آزادیِ بیان و حقِ دسترسی به اطلاعات در تضاد قرار می‌گیرد. زمانی که دولت‌ها با هدفِ مبارزه با جرایم سایبری یا پیشگیری از ناآرامی‌ها، اقدام به نظارتِ گسترده یا دسترسیِ بی‌ضابطه به داده‌هایِ رمزگذاری‌شده می‌کنند، در واقع «اصلِ تناسب» و «ضرورت» را در حقوقِ بشرِ دیجیتال نقض می‌نمایند. این تنش، دولت‌ها را از «حافظِ حقوقِ شهروندی» به «ناظرِ کلانِ رفتارِ دیجیتال» تبدیل کرده است، که در آن داده‌هایِ کاربران به ابزاری برایِ اعمالِ فشار و تحدیدِ حقوقِ مدنی بدل گشته‌اند؛ پدیده‌ای که در ادبیات حقوقی معاصر با عنوانِ «امنیتی‌سازیِ دیجیتال» شناخته می‌شود (موسوی، ۱۴۰۱: ۸۷).

از سوی دیگر، رویه‌هایِ قضاییِ بین‌المللی، به‌ویژه در اتحادیه اروپا، نشان می‌دهد که حاکمیتِ داده‌ای نمی‌تواند مجوزی مطلق برایِ نادیده انگاشتنِ کرامتِ انسانی و حریمِ خصوصی باشد. دیوانِ دادگستریِ اتحادیه اروپا در آرایِ تاریخیِ خود، همواره بر این نکته تأکید ورزیده است که دولت‌ها در اعمالِ اقتدارِ خود بر فضایِ سایبر، مقید به رعایتِ استانداردهایِ سخت‌گیرانه حقوقِ بشری هستند. این دیوان معتقد است که هرگونه مداخله‌یِ دولتی در حریمِ دیجیتال باید دارایِ پشتوانه‌یِ قانونیِ شفاف، مشروع و در راستایِ هدفی باشد که در یک

جامعه‌یِ دموکراتیک ضروری است (Kuner et al., 2020: 312). با این وجود، دولت‌هایِ اقتدارگرا با بهره‌گیری از فناوری‌هایِ نوظهور، سیستم‌هایِ «امتیازدهیِ اجتماعی» یا «پایشِ هوشمند» را پیاده‌سازی می‌کنند که در آن، حاکمیتِ داده‌ای عملاً به معنایِ سلبِ خودمختاریِ اطلاعاتی از کاربران و انقیادِ حقوقِ فردی در برابرِ اراده‌یِ دولت تعریف می‌شود.

چالشِ دیگر در این میان، مسئله‌یِ «جابجاییِ بارِ اثبات» در پرونده‌هایِ حقوقِ بشرِ دیجیتال است. هنگامی که یک دولت به بهانه‌یِ «امنیتِ ملی» به داده‌هایِ کاربران دسترسی پیدا می‌کند، کاربرانِ عادی عملاً ابزارِ قانونیِ کافی برایِ به چالش کشیدنِ این اقدام در مراجعِ قضاییِ داخلی ندارند. این نابرابریِ ساختاری، ضرورتِ تعبیه و تقویتِ مکانیسم‌هایِ «دادرسیِ منصفانه» در عصرِ دیجیتال را بیش از پیش نمایان می‌سازد. مطابق با دیدگاهِ گزارشگرانِ ویژه‌یِ سازمانِ ملل، حقوقِ حریمِ خصوصی در فضایِ آنلاین، الحاقیه یا متفرع بر حقوقِ آفلاین نیست، بلکه حقی اصیل است که دولت‌ها باید به واسطه‌یِ مسئولیتِ بین‌المللیِ خود، از آن در برابرِ نفوذِ غیرقانونی (چه از سویِ دولت و چه از سویِ شرکت‌هایِ بزرگ) صیانت نمایند (سادات‌میدانی، ۱۳۹۹: ۱۱۲).

علاوه بر این، در تقابل میان حاکمیت داده‌ای و حقوقِ کاربران، مفهومِ «رمزنگاری» به خطِ مقدمِ نبردِ حقوقی تبدیل شده است. دولت‌ها به بهانه‌یِ لزومِ دسترسیِ قانونی به محتوایِ ارتباطات برایِ پیشگیری از تروریسم، خواهانِ ایجادِ «درهایِ پشتی» در نرم‌افزارها هستند؛ اقدامی که از منظرِ حقوقِ دیجیتال، تضعیف‌کننده‌یِ امنیتِ سایبریِ عمومی و نقضِ حقِ بنیادینِ کاربران برایِ داشتنِ ارتباطاتِ امن است. بسیاری از صاحب‌نظران استدلال می‌کنند که امنیتِ ملی و حریمِ خصوصی، دو رویِ یک سکه هستند و فدا کردنِ حقوقِ کاربران به بهانه‌یِ امنیتِ ملی، در نهایت به تضعیفِ مشروعیتِ دموکراتیکِ حاکمیتِ دولت منجر می‌شود (زاهدی، ۱٤۰۰: ٤٥). در این چارچوب، حقوقِ بین‌الملل باید به سمتِ تعریفِ استانداردهایِ جهانیِ «حفاظتِ از داده‌ها به مثابه حقِ بشر» حرکت کند تا حاکمیتِ داده‌ای از قالبِ «قدرتِ خودسرانه» خارج و در ذیلِ «حاکمیتِ قانونِ دیجیتال» تعریف گردد.

در نهایت، تنش میان حاکمیت داده‌ای و حقوق بنیادین، بازتاب‌دهنده‌یِ بحرانِ مشروعیت در حکمرانیِ دیجیتال است. اگر دولت‌ها نتوانند میانِ منافعِ امنیتی و پاسداشتِ کرامتِ انسانیِ شهروندان تعادل برقرار کنند، فضایِ سایبر از محیطی برایِ شکوفاییِ استعدادهایِ بشری به عرصه‌ای برایِ سلطه‌یِ دیجیتال تبدیل خواهد شد. این

مسئله ایجاب می‌کند که در تدوینِ هرگونه مقرراتِ ملی یا بین‌المللی در حوزه حکمرانیِ داده‌ها، «اصلِ برتریِ حقوقِ بنیادین» به عنوانِ قاعده‌ای آمره در نظر گرفته شود. تنها در این صورت است که می‌توان حاکمیتِ دولت‌ها در عصرِ کلان‌داده‌ها را با ارزش‌هایِ بنیادینِ حقوقِ بین‌المللِ بشر سازگار دانست و از استحاله شدنِ حقِ آزادی در چنبره‌یِ کنترل‌هایِ الگوریتمیک جلوگیری کرد .(Hildebrandt, 2015: 205)

تحلیلِ این بخش نشان می‌دهد که تقابلِ حاکمیتِ داده‌ای و حقوقِ کاربران، فراتر از یک چالشِ فنی، یک منازعه‌یِ ماهویِ حقوقی است؛ چرا که حاکمیتِ مدرن در عصرِ دیجیتال، تنها در صورتی مشروعیت دارد که بتواند بستری امن برایِ اعمالِ آزادی‌هایِ شهروندان فراهم آورد. تداومِ رویکردهایِ امنیتیِ افراطی، منجر به فرسایشِ اعتمادِ عمومی به نهادهایِ دولتی شده و دولت‌ها را در موقعیتی قرار می‌دهد که نه تنها حافظِ امنیت، بلکه خود به تهدیدی برایِ حقوقِ بنیادین تبدیل می‌شوند، و این امر نیازمندِ بازخوانیِ مفهومِ مسئولیتِ دولت‌ها در قبالِ امنیتِ سایبریِ انسانی است.

وضعیتِ حقوقیِ «ابرهای داده‌ای و ناتوانیِ صلاحیت‌های سرزمینی

مدلِ پردازش ابری، با شکستنِ پیوندِ میان «محلِ ذخیره‌سازی داده» و «محلِ حضورِ قانونیِ مالکِ داده»، عملاً مفهومِ قلمروِ فیزیکی را در حقوق بین‌الملل بی‌معنا ساخته است. در نظامِ وستفالیایی، صلاحیتِ دولت‌ها بر اساسِ اصلِ سرزمینی تعریف می‌شود، به این معنا که دولتِ میزبانِ سرور، دارایِ صلاحیتِ انحصاری بر داده‌هایِ موجود در آن است. اما در معماریِ ابری، داده‌ها به صورتِ قطعاتِ رمزنگاری‌شده در سرورهایی در حوزه‌هایِ قضاییِ مختلف پراکنده می‌شوند. این «سیالیتِ جغرافیایی»، باعث می‌شود که هیچ دولتِ واحدی نتواند ادعایِ کنترلِ کامل بر تمامِ چرخه حیاتِ یک داده را داشته باشد. این گسستِ حقوقی، دولت‌ها را در تلاش برایِ اعمالِ صلاحیتِ کیفری یا مدنی بر داده‌هایِ موجود در «ابر»، با معمایِ «صلاحیتِ سرگردان» مواجه کرده است؛ وضعیتی که در آن دسترسیِ قانونیِ دولتِ الف به داده‌ای که در قلمروِ دولت ب واقع شده، نه تنها با دشواری‌هایِ فنی، بلکه با موانعِ جدیِ حاکمیتی در قالبِ «تداخلِ صلاحیت‌ها» روبه‌روست (منصوری، ۱٤۰۲: ۷٤).

ناتوانیِ صلاحیت‌هایِ سرزمینی در مواجهه با ابرهایِ داده‌ای، به‌ویژه در پرونده‌هایِ معاضدتِ قضاییِ بین‌المللی آشکار می‌شود. سیستم‌هایِ کلاسیکِ معاضدتِ قضایی که برایِ انتقالِ اسنادِ فیزیکی یا بازجویی‌هایِ حضوری طراحی شده‌اند، در مواجهه با سرعتِ سرسام‌آورِ دسترسیِ ابری، به‌شدت کند و ناکارآمد هستند. این ناکارآمدی، انگیزه‌ای برایِ دولت‌هایِ قدرتمند (مانند آمریکا با تصویبِ ایجاد کرده تا صلاحیتِ «فراسرزمینی» خود را بر اساسِ «مالکیتِ ارائه‌دهنده‌یِ خدمات» اعمال کنند، نه «محلِ فیزیکیِ داده». این رویکرد، اگرچه پاسخی به ضرورت‌هایِ امنیتی است، اما عملاً حاکمیتِ سرزمینیِ سایر دولت‌ها را دور می‌زند و منجر به ایجادِ نوعی «صلاحیتِ مبتنی برِ ارائه‌دهنده» شده است که با اصلِ تساویِ حاکمیت‌ها در حقوقِ بین‌المللِ کلاسیک در تضادِ آشکار قرار دارد (Svantesson, 2020: 89).

چالشِ دیگر، ابهام در مسئولیتِ بین‌المللیِ دولتِ میزبانِ سرور در صورتِ وقوعِ حملاتِ سایبری یا دسترسی‌هایِ غیرمجاز است. ذیلِ مفهومِ «مراقبت بایسته» ، دولت‌ها موظف‌اند از استفاده از قلمروِ خود برایِ اعمالِ خلافِ حقوقِ بین‌الملل جلوگیری کنند. اما در ابرهایِ داده‌ای، دولتِ میزبانِ زیرساختِ فیزیکی، اغلب هیچ کنترلی بر محتوایِ رمزنگاری‌شده‌یِ عبوری از سرورهایش ندارد. این «بی‌طرفیِ زیرساختی» باعث شده است که انتسابِ مسئولیتِ دولت‌ها در فضایِ ابری به یک بن‌بستِ حقوقی بدل شود. در واقع، ابزارهایِ سنتیِ حقوقِ بین‌الملل، نه برایِ نظارت بر «داده‌هایِ در حالِ حرکت» بلکه برایِ نظارت بر «دارایی‌هایِ مستقر» طراحی شده بودند؛ لذا در فضایِ ابری، مفهومِ «قلمرو» از یک پارامترِ حقوقی به یک متغیرِ فنیِ بی‌استفاده تبدیل شده است (تقی‌زاده، ۱۴۰۱: ۱۱۹).

علاوه بر این، مسئله‌یِ «حاکمیتِ داده‌ها» در فضایِ ابری، حقِ حاکمیتِ دولت‌ها را در تقابل با «حقوقِ قراردادهایِ خصوصی» قرار داده است. کاربران و شرکت‌هایِ فناوری با انتخابِ محلِ ذخیره‌سازیِ داده‌هایِ خود در سرورهایِ ابری، به صورتِ ضمنی حوزه‌یِ قضاییِ حاکم بر داده‌هایشان را تعیین می‌کنند .این «خصوصی‌سازیِ تعیینِ صلاحیت»، اقتدارِ تقنینیِ دولت‌ها را به چالش می‌کشد؛ چرا که دولت‌ها نمی‌توانند به سادگی قوانینِ نظارتیِ خود را بر داده‌هایی که در «ابر» هستند و از طریقِ قراردادهایِ خصوصیِ بین‌المللی اداره می‌شوند، تحمیل نمایند. این پدیده، ظهورِ نوعی «لکس دیجیتالی» را نوید می‌دهد که در آن قواعدِ فنی و قراردادهایِ استاندارد، جایگزینِ قوانینِ آمره‌یِ سرزمینیِ دولت‌ها می‌شوند .(Kohl, 2017: 212)

در نهایت، ناتوانیِ صلاحیت‌هایِ سرزمینی در مواجهه با ابرهایِ داده‌ای، نیازمندِ گذار از «صلاحیتِ مبتنی برِ مکان» به «صلاحیتِ مبتنی برِ عملکرد» است. جامعه‌یِ حقوقیِ بین‌المللی باید بپذیرد که انحصارِ سرزمینی در دنیایِ «رایانش ابری» دیگر یک واقعیتِ حقوقی نیست، بلکه یک نوستالژیِ ساختاری است. راهکارِ برون‌رفت از این بحران، تدوینِ معاهداتِ جدیدی است که به جایِ تمرکز بر «مکانِ فیزیکیِ داده»، بر «ماهیتِ دسترسی» و «تضمین‌هایِ دادرسیِ دیجیتال» تأکید داشته باشند. تنها در این صورت است که می‌توان حاکمیتِ دولت‌ها را در بستری که ماهیتِ غیرمتمرکزِ فضایِ سایبر است، با ضرورتِ نظم و امنیتِ عمومی تلفیق نمود (Milanovic, ۲۰۲۱: ۱۵۶).

تحلیلِ این بخش نشان می‌دهد که پارادایمِ سرزمینیِ حقوق بین‌الملل در مواجهه با معماریِ رایانش ابری، به مرزِ فروپاشیِ نظری رسیده است. این ناتوانی، تنها یک چالشِ فنی نیست، بلکه تزلزلی در مبانیِ اقتدارِ دولت‌هاست که پیش‌تر بر اساسِ کنترلِ فیزیکیِ «قلمرو» تعریف می‌شد. تقابلِ کنونی میانِ تلاش‌هایِ فراسرزمینیِ دولت‌ها برایِ دسترسی به داده‌ها و ماهیتِ غیرمتمرکزِ ابرها، گواهی است بر ضرورتِ بازنگریِ بنیادین در اصولِ صلاحیت در حقوقِ بین‌الملل، چرا که اصرار بر مدل‌هایِ وستفالیایی در عصرِ رایانشِ توزیع‌شده، تنها منجر به هرج‌ومرجِ صلاحیتی و تضعیفِ حقوقِ بنیادینِ کاربران خواهد شد.

مطالعه موردی: چالش‌های اجرای احکام قضایی بر داده‌های ذخیره شده در ابر

در مدل‌هایِ کلاسیکِ دادرسی، اجرایِ احکامِ قضایی متکی بر اصلِ «انحصارِ اقتدارِ دولت در قلمروِ خود» است؛ به این معنا که دولت‌ها نمی‌توانند بدونِ توسل به ابزارهایِ معاضدتِ قضایی احکامِ خود را در قلمروِ دولت دیگری اجرا کنند. با این حال، در عصرِ داده‌هایِ کلان، این پروسه به دلیلِ «فشارِ زمانی» و «فرار بودنِ داده‌ها»، عملاً کارکردِ خود را از دست داده است. برای نمونه، در پرونده‌هایِ مشهور نظیرِ «مایکروسافت علیه ایالات متحده» چالشِ اساسی این بود که آیا دادگاهِ آمریکا می‌تواند ارائه‌دهنده‌یِ خدمات را مجبور به افشایِ داده‌هایِ ذخیره‌شده در سرورهایِ ایرلند نماید یا خیر. این تنش، شکافِ عمیقی میانِ «صلاحیتِ شخصیِ مبتنی بر ارائه‌دهنده» و «صلاحیتِ سرزمینیِ مبتنی بر مکانِ داده» ایجاد کرده است که در آن، شرکت‌هایِ فناوری به عنوانِ واسطه‌هایِ ناخواسته، میانِ دو نظامِ حقوقیِ متعارض گیر افتاده‌اند (خالقی، ۱۴۰۲: ۱۴۵).

ناتوانی در اجرایِ احکامِ قضایی، اغلب ناشی از «تداخلِ قوانینِ آمره» است. برای مثال، اگر شرکتی موظف به افشایِ داده‌ها طبقِ قانونِ یک کشورمانند باشد، اما همان افشاگری، نقضِ قوانینِ حریمِ خصوصیِ کشورِ میزبان (مانند GDPR در اتحادیه اروپا) محسوب گردد، این شرکت با «مسئولیتِ دوگانه» و تناقضِ قانونی مواجه می‌شود. این وضعیتِ حقوقی، نه تنها مانعِ اجرایِ عدالت می‌شود، بلکه به ایجادِ «پناهگاه‌هایِ داده‌ای»منجر می‌گردد، جایی که داده‌ها در قلمروهایی ذخیره می‌شوند که کمترین همکاریِ حقوقی را با سایرِ دولت‌ها دارند. در چنین بستری، احکامِ قضاییِ ملی، صرفاً به «کاغذپاره‌هایی بی‌اثر» در فضایِ سیالِ سایبر تبدیل می‌شوند و دولت‌ها را در پیگیریِ جرایمِ سازمان‌یافته، به‌ویژه در جرایمِ سایبری، با بن‌بستِ عملیاتی مواجه می‌سازند (Svantesson, 2020: 112).

یکی دیگر از چالش‌هایِ اجرایِ احکام، مسئله‌یِ «رمزنگاریِ سرتاسری» است. حتی اگر حکمی قضایی صادر و ابلاغ گردد، ارائه‌دهندگانِ خدماتِ ابری ممکن است به دلیلِ نبودِ کلیدهایِ رمزگشایی در اختیارِ خود، از نظر فنی «ناتوان از اجرا» باشند. این «ناتوانیِ فنی»، اکنون به یک «موضعِ حقوقی» بدل شده است؛ یعنی شرکت‌ها با استناد به فقدانِ دسترسیِ فنی، از اجرایِ احکامِ قضایی سر باز می‌زنند. این امر، دولت‌ها را به سمتِ وضعِ قوانینی سوق داده است که شرکت‌ها را «ملزم به ایجادِ قابلیتِ دسترسی» می‌کند؛ موضوعی که خودِ آن در کانونِ منازعاتِ حقوقِ بشری قرار دارد، چرا که امنیتِ کلِ شبکه را برایِ رسیدن به یک هدفِ خاصِ قضایی به خطر می‌اندازد .(Mulligan, 2019: 55)

علاوه بر این، نبودِ یک استانداردِ بین‌المللی برایِ «اجرایِ فرامرزیِ احکامِ دیجیتال»، فضایِ عدم‌قطعیتِ حقوقی را دامن زده است. دولت‌ها به‌جایِ توسل به پروتکل‌هایِ چندجانبه، به سمتِ «یکسویه‌گراییِ حقوقی» حرکت کرده‌اند. این اقداماتِ یک‌جانبه، ضمن تضعیفِ نهادهایِ بین‌المللی، باعث شده است که اعتمادِ جهانی به زیرساخت‌هایِ ابری به شدت آسیب ببیند. شرکت‌هایِ فناوری برایِ فرار از این فشارها، به استفاده از «کلیدهایِ رمزنگاریِ توزیع‌شده» یا «پروتکل‌هایِ غیرمتمرکز» روی آورده‌اند تا بتوانند ادعا کنند که «داده‌ها در اختیارِ هیچ نهادِ قابل‌اجباری نیست»؛ امری که عملاً دادرسیِ کیفری در عصرِ دیجیتال را با چالشِ مشروعیتِ رویه‌ای مواجه ساخته است (زندی، ۱۴۰۱: ۹۸).

در نهایت، چالش‌های اجرای احکام قضایی در فضای ابری، نشان‌دهنده‌ی گذار اجباری حقوق از «جغرافیا» به «منطق» است. دادرسی دیجیتال نیازمند مکانیسم‌هایی است که فراتر از صلاحیت‌های سرزمینی، بر «قابلیت همکاری قضایی» استوار باشد. اگر دولت‌ها نخواهند یا نتوانند به یک پروتکل معاضدت قضایی دیجیتال که مبتنی بر استانداردهای جهانی حقوق بشر است دست یابند، هرگونه تلاش برای اجرای احکام ملی بر داده‌های ابری، نه تنها با شکست فنی روبرو خواهد شد، بلکه تنش‌های دیپلماتیک و حقوقی عمیقی را در نظام بین‌المللی دادرسی ایجاد خواهد کرد که ثبات تجارت دیجیتال را تهدید می‌کند (Ferrara, 2021: 201).

تحلیل این بخش نشان می‌دهد که ناتوانی نظام‌های قضایی ملی در اجرای احکام بر داده‌های ابری، یک گسست ساختاری در «اقتدار قضایی» است. تقابل کنونی نه تنها یک مسئله‌ی اجرایی، بلکه بحرانی در مشروعیت دادرسی در فضای سایبر است که در آن، ابزارهای سنتی احضار و توقیف، در برابر معماری غیرمتمرکز ابری خنثی شده‌اند؛ لذا تداوم این وضعیت، ضرورت تدوین کنوانسیون جهانی «صلاحیت کیفری سایبری» را بیش از پیش نمایان می‌سازد تا ضمن تضمین حاکمیت قانون، از تبدیل فضای ابری به خلأ حقوقی غیرقابل‌دسترس جلوگیری به عمل آید.

نتیجه‌گیری

بررسی انتقادی مفاهیم سنتی حاکمیت در پرتو تحولات عصر داده‌های کلان، آشکار می‌سازد که نظام حقوق بین‌الملل کلاسیک، که بر پایه‌ی جغرافیای فیزیکی و مرزهای سیاسی صلب استوار شده بود، اکنون در مواجهه با واقعیت «سیالیت دیجیتال» دچار فرسایش بنیادین گشته است. داده‌ها، به عنوان ماده‌ی خام قدرت در قرن بیست و یکم، دیگر در قید بندهای سرزمینی نیستند؛ آن‌ها آزادانه در ابرهای رایانشی و میان حوزه‌های قضایی متکثر در گردش‌اند. این گسست میان «واقعیت فنی ذخیره‌سازی پراکنده» و «صلاحیت حقوقی متمرکز دولت‌ها»، نه تنها یک چالش فنی، بلکه بحرانی در مشروعیت حاکمیت سرزمینی ایجاد کرده است. گذار از حاکمیت مبتنی بر «سرزمین» به حاکمیت مبتنی بر «داده»، ضرورتی اجتناب‌ناپذیر است که حقوق بین‌الملل باید با بازتعریف مفاهیم کلاسیک خود، به آن پاسخ دهد؛ چرا که اصرار بر مدل‌های وستفالیایی در عصر رایانش ابری، تنها منجر به هرج‌ومرج صلاحیتی و تضعیف حقوق بنیادین کاربران خواهد شد.

در این میان، نقشِ شرکت‌هایِ فناوریِ بزرگ به عنوانِ بازیگرانِ شبه‌حاکمیتی، معادله‌یِ سنتیِ «دولت–ملت» را به شدت متزلزل کرده است. این شرکت‌ها، با در اختیار داشتنِ زیرساخت‌هایِ ابری و قدرتِ الگوریتمیک، عملاً به حکمرانانِ فضایِ دیجیتال تبدیل شده‌اند که صلاحیت‌هایِ تقنینی، قضایی و اجرایی را در حوزه‌یِ داده‌ها اعمال می‌کنند. این «حکمرانیِ خصوصی»، در تقابلِ آشکار با اقتدارِ عمومیِ دولت‌ها قرار گرفته است. نتیجه‌گیریِ منطقیِ این پژوهش بر این است که برایِ برون‌رفت از این بن‌بست، نمی‌توان صرفاً به ابزارهایِ حقوقِ داخلی متوسل شد. تلاش‌هایِ یک‌جانبه‌یِ دولت‌ها برایِ اعمالِ صلاحیتِ فراسرزمینی نظیرِ ، نه تنها راه‌حلی پایدار نیست، بلکه منجر به ایجادِ تنش‌هایِ دیپلماتیک و ایجادِ «پناهگاه‌هایِ داده‌ای» در نقاطِ دیگرِ جهان می‌شود که امنیتِ حقوقیِ جامعه‌یِ بین‌المللی را به مخاطره می‌اندازد.

بر این اساس، ضرورتِ تدوینِ یک «کنوانسیونِ بین‌المللیِ حقوقِ فضایِ سایبر» با رویکردِ «حقوقِ بین‌المللِ داده‌محور» بیش از هر زمانِ دیگری احساس می‌شود. این کنوانسیون باید از پارادایمِ «صلاحیتِ مبتنی بر مکان» به سمتِ «صلاحیتِ مبتنی بر دسترسی و کنترل» حرکت کند. قواعدِ جدیدِ بین‌المللی باید به جایِ تمرکز بر جایی که داده در آن ذخیره شده است، بر ماهیتِ رابطه‌یِ حقوقی میانِ ارائه‌دهنده‌یِ خدمات، دولتِ مبدأ و سوژه‌یِ داده تمرکز نمایند. این «حقوقِ بین‌المللِ داده‌محور» باید قادر باشد تا توازنی دقیق میانِ امنیتِ ملی (نیازِ دولت‌ها به دسترسی به داده‌ها برایِ مبارزه با جرایم) و حقوقِ بنیادینِ بشر (حریمِ خصوصی و آزادی‌هایِ مدنیِ کاربران) برقرار کند. دستیابی به چنین توازنی، تنها از طریقِ ایجادِ سازوکارهایِ «همکاریِ قضاییِ دیجیتال» میسر است که در آن، استانداردهایِ دادرسیِ منصفانه به صورتِ فرامرزی و با ضمانت‌هایِ اجرایِ معتبر در فضایِ سایبر تعریف شوند.

در نهایت، باید تأکید نمود که «استقلالِ دیجیتال»، به عنوانِ راهبردی برایِ بازپس‌گیریِ حاکمیت توسطِ دولت‌ها، نباید به ابزاری برایِ انزواطلبیِ تکنولوژیک یا ایجادِ دیوارهایِ آتشِ ملی تبدیل شود که تجارتِ بین‌المللی و جریانِ آزادِ اطلاعات را مختل کند. حاکمیت در عصرِ دیجیتال، نه در انحصارِ فیزیکی، بلکه در توانمندیِ دولت‌ها برایِ مشارکتِ فعال در حکمرانیِ جهانیِ داده‌ها و وضعِ قواعدی است که ضمنِ حفظِ امنیت، به ماهیتِ غیرمتمرکزِ فضایِ سایبر وفادار باشد. پژوهشِ حاضر پیشنهاد می‌دهد که جامعه‌یِ حقوقیِ بین‌المللی باید با عبور از نوستالژیِ «اقتدارِ مطلقِ سرزمینی»، به سمتِ ساختارسازیِ حقوقیِ جدیدی حرکت کند که «داده» را به عنوانِ

عنصری حیاتی در حقوقِ بین‌الملل به رسمیت بشناسد و قواعدی متناسب با طبیعتِ «غیرمستقر» و «فرامرزیِ» آن وضع نماید؛ چرا که تنها با چنین گذارِ ساختاری است که می‌توان حقوقِ بین‌الملل را در عصرِ سایبر، از فرسودگیِ تاریخی نجات داد و کارآمدیِ آن را در صیانت از نظم و عدالتِ جهانی تضمین کرد.

منابع وماخذ:

الف: کتب

۱. بیگ‌زاده، ابراهیم، ۱۳۹۸، حقوق بین‌الملل عمومی، چاپ هشتم، انتشارات مجد، تهران.

۲. جعفری، محمد، ۱٤۰۱، حکمرانی فضای مجازی و حقوق تجارت بین‌الملل، چاپ اول، انتشارات دادگستر، تهران.

۳. دادگستر، انتشارات، ۱٤۰۱، حاکمیت قانون در فضای مجازی (عباسعلی کدخدایی)، چاپ اول، تهران.

٤. رادی، سمیرا، ۱۳۹۹، مقررات‌گذاری فضای سایبر و تجارت جهانی (فیض‌بخش، سمیرا)، چاپ اول، انتشارات شهر دانش، تهران.

٥. زمانی، سید قاسم، ۱٤۰۱، صلاحیت قضایی در حقوق بین‌الملل، چاپ اول، انتشارات مؤسسه مطالعات و پژوهش‌های حقوقی شهر دانش، تهران.

٦. زندی، علی، ۱٤۰۱، چالش‌های دادرسی کیفری در فضای سایبر، چاپ اول، انتشارات میزان، تهران.

۷. سادات‌میدانی، سیدحسین، ۱۳۹۹، مسئولیت بین‌المللی دولت‌ها در فضای سایبری، چاپ اول، انتشارات شهر دانش، تهران.

۸. سادات‌میدانی، سیدحسین، ۱۳۹۹، مسئولیت بین‌المللی دولت در فضای سایبر، انتشارات خرسندی، تهران.

۹. سیدزاده، علیرضا، ۱٤۰۱، حاکمیت دیجیتال در مواجهه با قوانین بین‌المللی تجارت، چاپ اول، انتشارات میزان، تهران.

۱۰. شعبانی، قاسم، ۱٤۰۰، حقوق بین‌الملل عمومی، چاپ پنجم، انتشارات اطلاعات، تهران.

۱۱. شریعت‌باقری، محمدجواد، ۱۳۹۸، حقوق بین‌الملل عمومی و چالش‌های نوین، چاپ دوم، انتشارات میزان، تهران.

۱۲. شیروی، عبدالحسین، ۱٤۰۰، حقوق بین‌الملل اقتصادی در عصر دیجیتال، چاپ اول، انتشارات میزان، تهران.

۱۳. شیروی، عبدالحسین، ۱٤۰۲، حقوق بین‌الملل عمومی در پرتو آرای دیوان بین‌المللی دادگستری، چاپ چهارم، انتشارات میزان، تهران.

۱٤. عراقی، عزت‌الله، ۱۳۹۹، حاکمیت ملی و صلاحیت‌های دولتی، چاپ اول، انتشارات دانشگاه تهران، تهران.

۱۵. قاری‌سیدفاطمی، سیدمحمد، ۱۳۹۹، حقوق بشر در جهان معاصر، چاپ پنجم، انتشارات نگاه معاصر، تهران.

۱٦. کاتوزیان، ناصر، ۱۳۹۷، فلسفه حقوق، چاپ چهارم، انتشارات شرکت سهامی انتشار، تهران.

۱۷. کدخدایی، عباسعلی، ۱٤۰۱، حاکمیت قانون در فضای مجازی، چاپ اول، انتشارات دادگستر، تهران.

۱۸. مستقیمی، بهرام، ۱۳۹۷، صلاحیت دولت‌ها در حقوق بین‌الملل، چاپ سوم، انتشارات دانشکده حقوق و علوم سیاسی دانشگاه تهران، تهران.

۱۹. محبی، محسن، ۱٤۰۱، حاکمیت و حقوق بین‌الملل در عصر تحولات تکنولوژیک، چاپ اول، انتشارات گنج دانش، تهران.

۲۰. منوچهری، عباس، ۱٤۰۱، حکمرانی دیجیتال و چالش‌های حاکمیت ملی، انتشارات نگاه معاصر، تهران.

۲۱. موسوی، سیدفضل‌الله، ۱٤۰۱، چالش‌های حقوق بشر در فضای مجازی، چاپ اول، انتشارات میزان، تهران.

۲۲. موسی‌زاده، رضا، ۱٤۰۱، حقوق سازمان‌های بین‌المللی، چاپ پانزدهم، انتشارات میزان، تهران.

۲۳. ممتاز، جمشید، ۱۳۹۸، حقوق بین‌الملل عمومی و چالش‌های نوین، چاپ دوم، انتشارات میزان، تهران.

۲٤. زاهدی، محمد مهدی، ۱٤۰۰، حقوق حریم خصوصی در فضای سایبر، چاپ اول، انتشارات سمت، تهران.

۲۵. ضیایی، سید یاسر، ۱۳۹۹، حقوق بین‌الملل فضای سایبر، چاپ اول، انتشارات خرسندی، تهران.

۲۶. ضیایی، سید یاسر، ۱۳۹۹، مسئولیت بین‌المللی دولت در فضای سایبر، چاپ اول، انتشارات شهر دانش، تهران.

ب:مقاله ها

۲۷. جلیلی، محمدرضا، ۱٤۰۲، حاکمیت در فضای سایبر، نشریه حقوق و تکنولوژی، دوره ۵، شماره ۲.

۲۸. حبیبی، نیلوفر، ۱٤۰۰، چالش‌های حقوقی جریان آزاد داده‌ها، نشریه حقوق اقتصادی، دوره ۱۰، شماره ٤.

۲۹. صدقی، محمود، ۱٤۰۰، تعارض صلاحیت‌ها در فضای سایبر، نشریه تحقیقات حقوقی، دوره ۲٤، شماره ۳.

۳۰. قربانی، مهدی، ۱٤۰۲، جریان آزاد داده‌ها با اعتماد در نظام‌های حقوقی، نشریه مطالعات حقوق عمومی، دوره ۵۳، شماره ۱.

منابع لاتین

۳۱. Zittrain, J., 2017, The Future of the Internet and How to Stop It, Yale Journal of Law and Technology, Vol 19, No 1.

۳۲. Svantesson, D., 2020, The Extraterritorial Application of Data Privacy Laws, International Journal of Law and Information Technology, Vol 28, No 2. Goldsmith, J., 2018, The Limits of Sovereignty in Cyberspace, Harvard Law Review, Vol 131, No 3.

۳۳. Karns, M., 2021, International Organizations and the Politics of Data Governance, International Affairs, Vol 97, No 4. Floridi, Luciano, 2020, The Logic of Information: A Theory of Philosophy as Conceptual Design, 2nd ed, Oxford University Press, London.

۳٤. o Smith, Brad, 2021, Tools and Weapons: The Promise and the Peril of the Digital Age, 1st ed, Penguin Press, New York.

۳۵. o Zuboff, Shoshana, 2019, The Age of Surveillance Capitalism, 1st ed, PublicAffairs, New York.

Hildebrandt, Mireille, 2015, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology, Edward Elgar Publishing.

٣٦. o Kuner, Christopher, et al., 2020, The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, London. Kohl, Uta, 2017, The Net and the Nation State: Multidisciplinary Perspectives on Internet Governance, Cambridge University Press.

٣٧. o Milanovic, Marko, 2021, "Jurisdiction, Data and Cyberspace", in: Oxford Handbook of International Law and Cyber-Security, Oxford University Press.

٣٨. o Svantesson, Dan Jerker B., 2020, Solving the Internet Jurisdiction Puzzle, Oxford University Press, London. Bamberger, Kenneth A., & Mulligan, Deirdre K., 2019, "Privacy on the Books and on the Ground", Stanford Law Review.

٣٩. o Ferrara, Elena, 2021, "Global Data Governance and Judicial Cooperation", International Journal of Law and Technology.

٤٠. o Svantesson, Dan Jerker B., 2020, Solving the Internet Jurisdiction Puzzle, Oxford University Press, London.