
مرزهای دیجیتال و چالش حاکمیت دولتها در عصر داده‌های فراملی

اسرا ولی پور^۱

۱- دانشجوی کارشناسی ارشد حقوق خصوصی، دانشگاه آزاد اسلامی واحد علوم و تحقیقات تهران

چکیده

در عصر گسترش داده‌های فراملی و وابستگی فزاینده نظام‌های اقتصادی، سیاسی و اجتماعی به زیرساخت‌های دیجیتال، مسئله مرزهای دیجیتال و چالش‌های حاکمیت دولتها به یکی از موضوعات محوری در سیاست‌گذاری کلان بدل شده است. این پژوهش با هدف تحلیل تنش میان جریان آزاد داده‌ها و ضرورت اعمال حاکمیت ملی، به بررسی سازوکارهای فنی، حقوقی و حکمرانی می‌پردازد که دولتها برای مدیریت فضاهای دیجیتال در برابر شرکت‌های فراملی و شبکه‌های جهانی اتخاذ می‌کنند. روش پژوهش، ترکیبی از تحلیل اسنادی و بررسی تطبیقی سیاست‌های داده‌ای در چند کشور منتخب است و بر پایه تحلیل کیفی مضمون انجام شده است. یافته‌ها نشان می‌دهد که دولتها برای حفظ حاکمیت خود به سمت سیاست‌هایی چون بومی‌سازی داده، تنظیم‌گری پلتفرم‌های جهانی، ایجاد دیوارهای دیجیتال و چارچوب‌های امنیت داده حرکت کرده‌اند، اما این اقدامات اغلب با چالش‌هایی مانند کاهش آزادی اطلاعات، افزایش انحصار پلتفرمی، فشارهای ژئوپلیتیک و محدودیت توان نظارتی همراه است. نتایج نشان می‌دهد که دستیابی به تعادل میان حفاظت از امنیت ملی، تضمین حقوق کاربران و بهره‌گیری از مزایای اقتصاد داده نیازمند الگوی حکمرانی چندلایه، مشارکت‌محور و مبتنی بر همکاری‌های منطقه‌ای و بین‌المللی است.

واژگان کلیدی: مرزهای دیجیتال، حاکمیت داده، داده‌های فراملی، امنیت سایبری، تنظیم‌گری پلتفرم‌ها.

۱. مقدمه

در دهه‌های اخیر، گسترش بی‌سابقه فناوری‌های دیجیتال، اینترنت، و شبکه‌های جهانی اطلاعات باعث شده است که مرزهای سنتی دولت-ملت به چالش کشیده شوند و عرصه‌ای نوظهور با عنوان «مرزهای دیجیتال» پدید آید؛ عرصه‌ای که در آن داده‌ها بدون توجه به محدودیت‌های جغرافیایی از مرزها عبور می‌کنند و اشکال جدیدی از قدرت، حاکمیت و وابستگی را شکل می‌دهند. این وضعیت سبب شده است که دولت‌ها با چالشی اساسی مواجه شوند: چگونه می‌توان در جهانی که داده‌ها آزادانه و لحظه‌ای میان کشورها جریان می‌یابد، همچنان حاکمیت ملی را اعمال کرد و از امنیت، هویت، اقتصاد و ساختارهای سیاسی محافظت نمود؟ به تعبیر «میریام دانکوف» (دونکل، ۲۰۱۹). فضای سایبری «سرزمینی بدون مرز» نیست، بلکه «سرزمینی با مرزهای سیال و قابل مناقشه» است که نیازمند الگوهای جدید حکمرانی است.

از یک‌سو، قدرت‌های بزرگ فناوری مانند گوگل، متا، آمازون و تیک‌تاک به بازیگران فراملی تبدیل شده‌اند که توانایی آنها در جمع‌آوری داده‌های کاربران، تحلیل رفتارها و کنترل زیرساخت‌های ارتباطی، اغلب فراتر از توان دولت‌هاست. (شوارتز و تایر، ۱۳۹۹). نشان می‌دهد که وابستگی دولت‌ها به پلتفرم‌های خصوصی، باعث انتقال بخشی از قدرت حاکمیتی به شرکت‌های تکنولوژی شده است؛ به گونه‌ای که تصمیم‌های این شرکت‌ها دربارهٔ مقررات محتوا، امنیت داده و ساختار پلتفرم‌ها می‌تواند بر سیاست داخلی و حتی روابط خارجی کشورها اثر بگذارد. از سوی دیگر، جریان فراملی داده‌ها نوعی «چالش دوگانه» برای دولت‌ها ایجاد کرده است: چالش نخست، حفظ امنیت ملی در برابر تهدیدهای سایبری، جاسوسی دیجیتال و نفوذ اطلاعاتی است؛ چالش دوم، ضرورت بهره‌برداری از اقتصاد داده، نوآوری دیجیتال و فرصت‌های فناوری است که نیازمند جریان آزاد اطلاعات و اتصال به اقتصاد جهانی داده است (زوباف، ۲۰۱۹). در چنین زمینه‌ای، بسیاری از کشورها به سمت اعمال «حاکمیت دیجیتال» حرکت کرده‌اند؛ سیاستی که هدف آن اعمال کنترل دولت بر داده‌ها، زیرساخت‌ها و تعاملات دیجیتال است. اتحادیه اروپا یکی از پیشگامان این حوزه است؛ مقررات عمومی حفاظت از داده‌ها (GDPR) نمونه روشن سیاستی است که تلاش می‌کند در برابر شرکت‌های فراملی، حریم خصوصی و حقوق شهروندان اروپایی را تضمین کند. مطالعه «بارت و نلسون» (برت و نلسون، ۲۰۲۱).

نشان می‌دهد که این مقررات تأثیر جهانی داشته و بسیاری از کشورها را به سمت تنظیم‌گری سخت‌گیرانه‌تر داده‌ها سوق داده است. در مقابل، کشورهایی مانند چین با سیاست‌هایی همچون «حاکمیت سایبری» و ایجاد دیوار بزرگ دیجیتال، تلاش کرده‌اند مرزهای دیجیتال را به شدت کنترل کنند و جریان داده را تحت سلطهٔ کامل دولت قرار دهند (کریمز، ۲۰۱۷). این اقدامات، نشان‌دهندهٔ دو مسیر متفاوت حکمرانی است: یکی مبتنی بر حمایت از حقوق دیجیتال و دیگری مبتنی بر کنترل گسترده دولت.

با این حال، این رویکردها پیامدهای مهمی نیز در پی داشته‌اند. الزام به محل‌بندی داده‌ها (Data Localization)، که کشورهای متعددی آن را اجرا کرده‌اند، اگرچه امنیت داده‌ها را افزایش داده، اما به‌طور هم‌زمان هزینه‌های شرکت‌ها را بالا برده، نوآوری را محدود کرده و حتی باعث «تجزیه اینترنت» یا پدید آمدن «اینترنت‌های ملی» شده است (Chander & Lê، ۲۰۱۵/چاندر و له، ۱۳۹۴). همچنین، برخی پژوهش‌ها تأکید دارند که سیاست‌های سخت‌گیرانه دولتی در حوزهٔ داده ممکن است حقوق کاربران، آزادی بیان و جریان آزاد اطلاعات را تهدید کند و به شکل‌گیری فضاها یا بسته اطلاعاتی منجر شود (۲۰۲۰/دناردیس، ۲۰۲۰).

در کنار چالش‌های امنیتی و حقوقی، مسائل ژئوپلیتیکی نیز نقش مهمی دارند؛ زیرا داده‌ها به بخشی از رقابت قدرت‌های جهانی تبدیل شده‌اند. به عنوان مثال، رقابت آمریکا و چین در حوزه شبکه‌های 5G، زیرساخت‌های ابری و مالکیت داده‌ها نشان می‌دهد که کنترل بر داده‌ها، بخشی از امنیت ملی و قدرت بین‌المللی محسوب می‌شود (فارل و نیومن، ۲۰۱۹).

در نظریه «قدرت شبکه‌ای» توضیح می‌دهند که کشورهایی که کنترل بیشتری بر زیرساخت‌های دیجیتال دارند، توان اثرگذاری بیشتری در سیاست جهانی خواهند داشت. این واقعیت، چالش دولت‌های کوچک و متوسط را دوچندان می‌کند، زیرا توانایی آنها برای دفاع از مرزهای دیجیتالیشان محدودتر است و در برابر بازیگران بزرگ فناوری و دولت‌های قدرتمند، آسیب‌پذیرتر هستند.

از این رو، پژوهش درباره «مرزهای دیجیتال و چالش حاکمیت دولت‌ها» ضرورت دارد تا سازوکارهای جدید حکمرانی را بررسی کند. بسیاری از تحلیل‌ها نشان می‌دهند که نوعی «حاکمیت چندلایه» نیاز است؛ یعنی ترکیبی از حاکمیت ملی، مقررات منطقه‌ای و همکاری بین‌المللی. زیرا هیچ کشوری به تنهایی قادر نیست جریان‌های فراملی داده را مدیریت کند. به تعبیر «دبرا دناردیس» (دناردیس، ۲۰۲۰)، حکمرانی داده در جهان امروز نه تنها فنی، بلکه اساساً سیاسی است و بر ساختارهای قدرت جهانی اثر می‌گذارد. از این رو، مطالعه حاضر تلاش می‌کند تصویری عمیق و چندبعدی از وضعیت کنونی مرزهای دیجیتال ارائه دهد و نشان دهد که چگونه جریان داده‌ها مفهوم حاکمیت را بازتعریف کرده‌اند و چه الگوهایی می‌توانند پاسخی برای چالش‌های دولت‌ها باشند.

۱- مفهوم‌سازی مرزهای دیجیتال در ادبیات حکمرانی مدرن

مفهوم مرز همواره یکی از ارکان بنیادین نظریه دولت و روابط بین‌الملل بوده است؛ مرزها قلمرو، قدرت، هویت و حاکمیت دولت‌ها را تعریف می‌کنند. اما با گسترش فناوری‌های اطلاعاتی و ارتباطی و بسط جریان داده‌ها در سطح جهانی، این مفهوم به گونه‌ای دگرگون شده و پدیده‌ای تحت عنوان «مرزهای دیجیتال» مطرح گردیده است. بر اساس مطالعات جدید، مرزهای دیجیتال صرفاً محدود به تلاقی خطوط جغرافیایی یا ترسیم نقشه سیاسی دولت‌ها نیستند، بلکه قلمروهایی هستند که با مدیریت جریان داده‌ها، زیرساخت‌های شبکه‌ای، مقررات دیجیتال و قدرت پلتفرم‌ها ساخته می‌شوند (رضا توکلی‌راد و حمیده سادات میری، ۱۴۰۰). از این منظر، دولت‌ها دیگر تنها بازیگران مرز نیستند، بلکه زیرساخت‌ها، نرم‌افزارها، شرکت‌های فراملی و کاربران نیز بخشی از فرایند ترسیم، حفظ یا بازتعریف مرز دیجیتال هستند.

مطالعه «تحول‌گرایی حکمرانی: از دولت الکترونیک تا حکمرانی دیجیتال» نشان می‌دهد که در فرایند تحول از دولت الکترونیک به حکمرانی دیجیتال، مرز میان داخل و خارج اطلاعات کمرنگ می‌شود و شهروند دیگر صرفاً مخاطب خدمات نیست بلکه بازیگر تولید، گردش و تبادل داده به شمار می‌رود (رضا توکلی‌راد و حمیده سادات میری، ۱۴۰۰). این تحول بدین معناست که «مرز» در فضای دیجیتال، تبدیل به مرزی برای جریان داده و قدرت شده است؛ مرزی که محل تحدید، کنترل یا آزادسازی داده‌هاست. بنابراین، مفهوم‌سازی مرزهای دیجیتال در ادبیات معاصر بر سه عنصر کلیدی استوار است: جریان داده، کنترل فنی پلتفرم‌ها و قانون‌گذاری دیجیتال.

در گفتمان فارسی نیز، مقالات متعددی به نحوی به این دگرگونی پرداخته‌اند. برای مثال، در پژوهشی تحت عنوان «مدیریت حاکمیت داده‌ها در دوران تجارت دیجیتال» آمده است که جریان داده‌های فرامرزی یکی از چالش‌های اصلی حاکمیت ملی است؛ زیرا دولت‌ها برای حفظ امنیت، حاکمیت اقتصادی و فرهنگی خود، نیازمند تعیین مرزهایی برای داده‌اند که غالباً در چارچوب مرزهای جغرافیایی

قرار ندارد (مرکز شبکه علمی ایران، ۱۴۰۴). این مطالعه تأکید می‌کند که مرزهای دیجیتال به معنای توانایی دولت در تعیین قواعد جریان داده، محل ذخیره‌سازی آن و شرایط دسترسی به آن است.

به موازات این، مفهوم «حاکمیت داده» یا data-sovereignty نیز در ادبیات حکمرانی دیجیتال ایران مطرح شده است؛ به این معنا که داده تولیدشده در یا برای یک دولت یا جامعه، باید تحت توان کنترل و تصمیم‌گیری آن دولت باقی بماند. این نگاه بیانگر نوعی بازگشت به مرزها، اما نه مرز جغرافیایی، بلکه مرزی برای داده و زیرساخت‌هاست. در این چارچوب، مرزهای دیجیتال ضرورتاً فیزیکی نیستند بلکه تکنولوژیک، حقوقی و سیاست‌محور هستند. پژوهش «تحلیلی بر کیفیت داده در دولت الکترونیک و تأثیر آن بر حکمرانی داده در ایران» نشان می‌دهد که کیفیت داده و مدیریت آن، نقش مهمی در توانایی دولت برای اعمال مرز دیجیتال دارد؛ یعنی داده‌های ناقص، پراکنده و غیرقابل اعتماد، مرز دیجیتال را برای دولت ضعیف می‌کنند (فرزانه صحرایی، ۱۴۰۴).

نکته کلیدی دیگر این است که مرزهای دیجیتال نه فقط محدود به چارچوب ملی‌اند بلکه در تعامل با ساختار منطقه‌ای و بین‌المللی شکل می‌گیرند. دولت‌هایی که زیرساخت‌های ابری خارجی، پلتفرم‌های جهانی و جریان داده از مسیرهای مبتنی بر شرکت‌های فراملی را پذیرفته‌اند، در موقعیت کمتری برای اعمال مرز دیجیتال قرار دارند. به عبارت دیگر، وابستگی به ساختارهای خارجی، مرز دیجیتال دولت‌ها را تضعیف می‌کند. مطالعات نشان می‌دهد که کشورها با استراتژی «خودکفایی دیجیتال» توان بیشتری در حفظ مرزهای دیجیتال دارند؛ اما ریسک اقتصادی و نوآوری نیز همراه دارد.

در نتیجه، مفهوم‌سازی مرزهای دیجیتال در ادبیات حکمرانی مدرن را می‌توان به این شکل ترسیم کرد: مرز دیجیتال نقطه‌ای است که در آن جریان داده، قدرت تنظیم‌کننده، زیرساخت فنی و قانون‌گذاری به هم می‌رسند و دولت، به‌عنوان یکی از بازیگران، سعی دارد این نقطه را مدیریت کند. این مرز نه صرفاً برای «محدود کردن» داده ساخته می‌شود بلکه برای «قابلیت اعمال حاکمیت بر داده‌ها» و «حفظ منافع ملی در فضای رقابتی بین‌المللی» است. در عصر فراملی شدن داده، مرزهای دیجیتال به عرصه‌ی نوینی از حکمرانی بدل شده‌اند که بازخوانی نقش دولت‌ها، شرکت‌ها و کاربران را ضروری می‌سازد.

۲- ویژگی‌های عصر داده‌های فراملی و پیامدهای آن برای دولت‌ها

عصر داده‌های فراملی به دوره‌ای اطلاق می‌شود که جریان داده‌ها و اطلاعات دیگر محدود به مرزهای جغرافیایی نیست و شبکه‌های جهانی اطلاعاتی، فرایندهای اقتصادی، سیاسی، اجتماعی و فرهنگی کشورها را به یکدیگر متصل می‌کنند. این پدیده، که با انقلاب دیجیتال و گسترش فناوری‌های ارتباطی و اطلاعاتی تسریع شده است، دارای ویژگی‌های شاخصی است که پیامدهای گسترده‌ای برای دولت‌ها به همراه دارد. نخستین ویژگی عصر داده‌های فراملی، سیالیت و عبور از مرزهای ملی است. داده‌ها به راحتی و با سرعت بالا بین کشورها جریان می‌یابند و این امر باعث کاهش کنترل سنتی دولت‌ها بر اطلاعات داخلی می‌شود (علوی‌روم، ۱۴۰۳). به بیان دیگر، مرزهای دیجیتال دیگر تنها بر مبنای قلمرو جغرافیایی تعریف نمی‌شوند بلکه «قلمرو جریان داده» نقش اساسی در حاکمیت مدرن یافته است.

دومین ویژگی مهم، افزایش نقش بازیگران غیردولتی در تولید، کنترل و مدیریت داده‌هاست. شرکت‌های فناوری چندملیتی، پلتفرم‌های دیجیتال و حتی کاربران نهایی به‌عنوان تولیدکنندگان و جریان‌دهندگان داده، نقش مهمی در شکل‌دهی نظم اطلاعاتی جهانی ایفا می‌کنند. پژوهش‌های انجام‌شده نشان می‌دهد که این وضعیت موجب ایجاد نوعی «قدرت فراملی داده» می‌شود که به

موازات قدرت سیاسی سنتی عمل می‌کند و می‌تواند استقلال دولتها در سیاستگذاری و حاکمیت داده‌ای را محدود کند (رضا توکلی‌راد و حوریه سادات میری، ۱۴۰۰).

ویژگی سوم عصر داده‌های فراملی، سرعت و حجم بالای داده‌ها است. با افزایش چشمگیر تولید داده‌ها در شبکه‌های اجتماعی، سیستم‌های اقتصادی دیجیتال و خدمات الکترونیکی، دولتها با چالش مدیریت حجم عظیم داده‌ها مواجه شده‌اند. پژوهش فرامرز صحرایی (۱۴۰۴) نشان می‌دهد که نبود زیرساخت‌های کافی و عدم توانایی پردازش و تحلیل داده‌ها، موجب کاهش قدرت تصمیم‌گیری و کاهش کارآمدی سیاست‌های عمومی می‌شود. به عبارت دیگر، داده‌های فراملی نه تنها فرصت‌های جدیدی برای تحلیل و پیش‌بینی سیاست‌ها فراهم می‌کنند بلکه بار شناختی و فنی جدیدی بر نهادهای حکومتی تحمیل می‌کنند.

چهارمین ویژگی مهم، پیچیدگی حقوقی و قانونی داده‌های فراملی است. جریان داده‌ها از مرزهای ملی موجب ایجاد چالش‌های حقوقی متعدد می‌شود؛ به گونه‌ای که قوانین ملی ممکن است با مقررات بین‌المللی، پروتکل‌های پلتفرم‌ها یا استانداردهای داده‌ای همخوانی نداشته باشد. گزارش مرکز پژوهش‌های مجلس (۱۴۰۴) تأکید می‌کند که دولتها برای حفظ حاکمیت خود نیازمند بازتعریف قوانین و تدوین سیاست‌های جامع داده‌ای هستند تا بتوانند ضمن رعایت استانداردهای جهانی، امنیت و حاکمیت ملی را نیز تضمین کنند.

پنجمین ویژگی، وابستگی به زیرساخت‌های فناورانه فرامرزی است. بسیاری از کشورها برای خدمات ابری، ذخیره داده و پردازش اطلاعات به زیرساخت‌های بین‌المللی وابسته‌اند. این وابستگی، دولتها را در برابر سیاست‌های دیگر کشورها و شرکت‌های چندملیتی آسیب‌پذیر می‌کند و می‌تواند بر امنیت، استقلال و منافع اقتصادی دولتها تأثیرگذار باشد (مرکز شبکه علمی ایران، ۱۴۰۴). بر این اساس، دولتها باید راهبردهایی برای تقویت خودکفایی دیجیتال، حفاظت از زیرساخت‌ها و افزایش توان کنترل داده‌ها تدوین کنند. پیامدهای این ویژگی‌ها برای دولتها چندوجهی است. نخست، تضعیف کنترل سنتی دولت بر مرزها و داده‌ها است، که نیازمند بازتعریف مرزهای حاکمیتی و ایجاد مرزهای دیجیتال است. دوم، افزایش ضرورت سیاستگذاری جامع داده‌ای برای مدیریت جریان، امنیت، کیفیت و حریم داده‌هاست. سوم، ظهور تهدیدات ژئوپلیتیکی داده‌ای است که می‌تواند روابط بین‌الملل و سیاست‌های امنیتی را تحت تأثیر قرار دهد. چهارم، ایجاد فرصت‌های نوین اقتصادی و اجتماعی است؛ به طوری که دولتها می‌توانند با بهره‌گیری از داده‌های فراملی، خدمات عمومی را بهبود بخشند، شفافیت را افزایش دهند و سیاست‌های مبتنی بر شواهد را توسعه دهند.

به طور کلی، عصر داده‌های فراملی، تعادل بین فرصت‌ها و تهدیدها را برای دولتها به چالش می‌کشد و حاکمیت ملی را در بعد دیجیتال مورد آزمون قرار می‌دهد. مدیریت مؤثر این چالش‌ها نیازمند زیرساخت‌های فناورانه، قانون‌گذاری دقیق، سیاستگذاری داده‌ای و همکاری‌های بین‌المللی است تا دولتها بتوانند ضمن بهره‌گیری از مزایای داده‌های فراملی، استقلال و امنیت خود را نیز حفظ کنند.

۳- شکاف میان حاکمیت سنتی و حاکمیت دیجیتال

حاکمیت سنتی، که ریشه در ساختارهای سیاسی و حقوقی کلاسیک دارد، عمدتاً بر کنترل جغرافیایی، قدرت نظامی و اعمال قانون در قلمرو مشخص متکی است. این نوع حاکمیت، که بر پایه مرزهای ملی و چارچوب‌های قانونی رسمی شکل گرفته، برای قرن‌ها ابزار اصلی مدیریت دولتها و روابط بین‌الملل به شمار می‌رفته است. با این حال، ظهور فناوری‌های اطلاعاتی و ارتباطی و شکل‌گیری

جریان‌های داده فراملی، شکافی میان حاکمیت سنتی و نیازهای حاکمیت دیجیتال ایجاد کرده است (علوی‌روم، ۱۴۰۳). این شکاف به‌وضوح نشان می‌دهد که ابزارها و مفاهیم حاکمیت سنتی برای کنترل داده‌ها، شبکه‌ها و تعاملات دیجیتال کافی نیستند. یکی از ابعاد اصلی این شکاف، سرعت و حجم جریان داده‌ها است. داده‌ها با سرعتی چند برابر سریع‌تر از توان تصمیم‌گیری سنتی دولت‌ها حرکت می‌کنند و دولت‌ها در مواجهه با این حجم عظیم داده نیازمند زیرساخت‌های فناوری، ابزارهای تحلیل و نیروی انسانی متخصص هستند (رضا توکلی‌راد و حوریه سادات میری، ۱۴۰۰). در حالی که حاکمیت سنتی بر مکانیزم‌های بوروکراتیک و سلسله‌مراتبی استوار است، حاکمیت دیجیتال نیازمند تصمیم‌گیری سریع، منعطف و مبتنی بر داده‌های زنده است. ابعاد دیگر شکاف، تعریف قلمرو و مرزها در فضای دیجیتال است. حاکمیت سنتی مرزهای جغرافیایی را ملاک اعمال قدرت و قانون می‌داند، اما در حاکمیت دیجیتال، مرزها فنی، حقوقی و شبکه‌ای هستند و داده‌ها می‌توانند بدون توجه به مرزهای ملی جریان پیدا کنند. این موضوع باعث شده است که دولت‌ها نتوانند کنترل کامل بر داده‌های تولیدشده توسط شهروندان، شرکت‌ها یا پلتفرم‌های فراملی داشته باشند (فرامرز صحرایی، ۱۴۰۴). به بیان دیگر، حاکمیت سنتی ابزار لازم برای ایجاد و مدیریت مرزهای دیجیتال را ندارد و دولت‌ها برای حفظ استقلال و امنیت اطلاعاتی باید چارچوب‌های جدید قانونی و فناوریانه طراحی کنند. ابعاد قانونی و مقرراتی نیز بخشی از شکاف میان حاکمیت سنتی و دیجیتال را تشکیل می‌دهند. قوانین موجود برای محیط‌های فیزیکی و تعاملات سنتی تدوین شده‌اند و اغلب با جریان داده‌های دیجیتال و فرامری تطابق ندارند. پژوهش‌های اخیر نشان می‌دهند که دولت‌ها برای اعمال حاکمیت دیجیتال نیازمند بازنگری قوانین ملی، تدوین پروتکل‌های حاکمیتی داده و هماهنگی با استانداردهای بین‌المللی هستند تا بتوانند در فضای فرامری داده‌ها نقش مؤثری ایفا کنند (مرکز شبکه علمی ایران، ۱۴۰۴). علاوه بر این، شکاف میان حاکمیت سنتی و دیجیتال، پیامدهایی برای امنیت ملی و سیاستگذاری اقتصادی به همراه دارد. وابستگی به زیرساخت‌های خارجی، استفاده از سرویس‌های ابری خارجی و جریان داده از طریق پلتفرم‌های فراملی، دولت‌ها را در معرض فشارهای سیاسی و اقتصادی قرار می‌دهد و توان کنترل مستقیم بر منابع حیاتی دیجیتال را کاهش می‌دهد. این شرایط ضرورت توسعه استراتژی‌های ملی دیجیتال، سرمایه‌گذاری در زیرساخت‌های بومی و تقویت توانایی تحلیل و مدیریت داده‌ها را برجسته می‌کند. به طور خلاصه، شکاف میان حاکمیت سنتی و حاکمیت دیجیتال، چالشی بنیادین در عصر داده‌های فراملی است که شامل چهار بعد اصلی می‌شود: سرعت و حجم داده‌ها، تعریف مرزها و قلمروها، چارچوب قانونی و مقرراتی و وابستگی به زیرساخت‌های فناوریانه فرامری. دولت‌ها برای پر کردن این شکاف باید سیاستگذاری نوآورانه، سرمایه‌گذاری در فناوری و بازتعریف قوانین را در اولویت قرار دهند تا بتوانند حاکمیت ملی خود را در فضای دیجیتال حفظ کنند و ضمن بهره‌گیری از فرصت‌های داده‌های فراملی، تهدیدات ناشی از این تغییرات را کاهش دهند.

۴- اقتصاد سیاسی داده و رقابت دولت‌ها و شرکت‌های فناوری

در بستر تحول جهانی اقتصاد دیجیتال، داده به عنوان یکی از منابع راهبردی اصلی مطرح شده و نقش دولت‌ها و شرکت‌های فناوری در گردآوری، کنترل و بهره‌برداری از آن به نقطه تلاقی قدرت اقتصادی، سیاسی و فناوریانه تبدیل شده است. از منظر اقتصاد سیاسی، داده نه فقط یک کالای اقتصادی بلکه ابزاری برای اعمال حاکمیت، تنظیم قدرت و بازتوزیع اقتصادی است؛ لذا رقابت دولت‌ها با

شرکت‌های فناوری در این عرصه، یکی از مهم‌ترین چالش‌های دوره جدید است. در ادبیات ایران نیز این موضوع به تدریج مورد توجه پژوهشگران قرار گرفته است.

یکی از جنبه‌های کلیدی این اقتصاد سیاسی، نقش شرکت‌های فناوری بزرگ (Big Tech) است. این شرکت‌ها با انبوه داده‌های تولیدشده توسط کاربران، الگوریتم‌های پردازش پیشرفته، زیرساخت‌های ابری و خدمات دیجیتال، توانسته‌اند قدرتی فراتر از بازیگر صرفاً خصوصی تجاری کسب کنند. این قدرت، زمانی که با ظرفیت دولت‌ها برای نظارت، قانون‌گذاری و تنظیم درهم آمیزد، ساختار تعاملی جدیدی میان دولت و شرکت ایجاد می‌کند. پژوهش «تحلیلی بر کیفیت داده در دولت الکترونیک و تأثیر آن بر حکمرانی داده در ایران» نشان می‌دهد که دولت ایران به ویژه در حوزه پردازش داده و تصمیم‌سازی مبتنی بر داده، با چالش فقدان زیرساخت، نبود داده با کیفیت و ضعف در سازوکار تنظیم مواجه است (صحرائی، ۱۴۰۴). این ضعف، موقعیت دولت را در مقابل شرکت‌های فناوری که داده‌ها را جمع‌آوری می‌کنند و خدمات مبتنی بر آن ارائه می‌دهند، تضعیف می‌کند.

هم‌زمان، دولت‌ها نیز خود به عنوان بازیگر اقتصادی داده وارد میدان شده‌اند. سیاست‌هایی چون محل‌بندی داده (Data Localization)، تدوین قوانین حاکمیت داده، مشارکت در زیرساخت ابری ملی و تلاش برای استقلال فناوری، از جمله ابزارهایی هستند که دولت‌ها در راستای بازتعریف قدرت اقتصادی خود در حوزه داده به کار گرفته‌اند. در ایران، مطالعات نشان داده‌اند که فقدان مدل نهادین و قانون‌گذاری جامع برای داده‌ها، مانعی بزرگ برای شکل‌دهی اقتصاد داده‌ای پایدار محسوب می‌شود (محمودی پرچینی، ۱۴۰۵). به این ترتیب، دولت‌ها که پیش‌تر در عرصه فیزیکی کنترل منابع طبیعی، اقتصادی و امنیتی شناخته می‌شدند، اکنون باید در عرصه داده نیز موقعیت خود را بازابند.

در این رقابت، چالش «وابستگی فناورانه» به شرکت‌های فناوری خارجی نیز برجسته شده است. بسیاری از کشورها، از جمله ایران، بخشی از زیرساخت‌های فناوری، خدمات ابری، سامانه‌های تحلیل داده و ذخیره‌سازی را از شرکت‌های خارجی تأمین می‌کنند. این امر به کاهش توان حاکمیتی دولت و افزایش قدرت بازیگران فرامرزی منجر می‌شود. پژوهش در زمینه حکمرانی داده می‌گوید: «در کشورهایی که زیرساخت و سیاست‌گذاری بومی ضعیف باشد، شرکت‌های خارجی می‌توانند نقش مؤثری در تعیین قواعد جریان داده، ذخیره‌سازی و تحلیل آن ایفا کنند» (صحرائی، ۱۴۰۴). از این منظر، دولت‌ها ناچارند برای کاهش این نوع وابستگی، زیرساخت ملی ایجاد کنند، شرکت‌های فناوری داخلی را تقویت نمایند و سیاست‌های بازدارنده در برابر تسلط داده‌ای شرکت‌های خارجی تدوین کنند.

بعد حقوقی و سیاسی این رقابت نیز قابل توجه است. مالکیت داده، حریم خصوصی، حق تصمیم‌گیری درباره داده‌های تولیدشده توسط شهروندان یا دولت‌ها، و نیز مقررات بین‌المللی داده، از محورهای این رقابت هستند. در ایران، پژوهش «مدل پیشنهادی برای استقرار حکمرانی داده‌ها با تأکید بر حریم خصوصی و امنیت داده» نشان می‌دهد که خلأهای قانونی و ضعف پیوند میان سیاست‌گذاری، نهادها و بازار، به کاهش کارآمدی حاکمیت داده‌ای منجر شده است (محمودی پرچینی، ۱۴۰۵). بنابراین، دولت‌ها باید ظرفیت قانونی و نهادی خود را تقویت کنند تا در کنار شرکت‌های فناوری، در تعیین قواعد اقتصاد داده ایفای نقش نمایند.

اقتصاد سیاسی داده همچنین با ایجاد بازتوزیع قدرت اقتصادی داخلی در کشورها همراه است. شرکت‌های فناوری بزرگ با دسترسی به داده‌های فراوان می‌توانند بازارهای جدید خلق کنند، خدمات هدفمند ارائه دهند و مدل‌های تجاری ارزش‌افزوده مبتنی بر داده شکل دهند؛ در حالی که دولت‌ها باید راهبردهایی برای تضمین منافع عمومی، شفافیت و عدالت داده‌ای فراهم کنند. در ایران،

نابرابری میان سازمان‌های دولتی، شرکت‌های خصوصی فناور و شهروندان در دسترسی به داده و ظرفیت تحلیل آن، یکی از موانع تحقق اقتصاد داده‌ای است (توکلی‌راد و سادات میری، ۱۴۰۰).

در نهایت، یکی از مسیرهای ضروری برای پاسخ به این رقابت، تدوین مدل حکمرانی داده مشارکتی است؛ مدلی که در آن شهروندان، دولت و بخش خصوصی سه‌جانبه در مالکیت، تصمیم‌گیری و بهره‌برداری از داده مشارکت داشته باشند. این مدل می‌تواند تلاش دولت‌ها و شرکت‌های فناوری را هم‌راستا با منافع عمومی کند و از تسلط شرکت‌های فناوری جلوگیری نماید. همچنین، تقویت زیرساخت‌های فناوری، توانمندسازی نیروی انسانی داده، تدوین چارچوب‌های قانونی بومی و حمایت از نوآوری داخلی، از ایشان ابزارهایی هستند که دولت‌ها باید در دستور کار قرار دهند.

۵- تهدیدات امنیتی مرتبط با داده‌های فراملی

در عصر جریان آزاد داده‌های فراملی، تهدیدات امنیتی به‌طور فزاینده‌ای پیچیده و نظام‌مند شده‌اند و می‌توانند سلامت زیرساخت‌های حیاتی، حاکمیت اطلاعاتی و استقلال دیجیتال دولت‌ها را به‌خطر اندازند. این تهدیدات از منظر فنی، حقوقی، سیاسی و لجستیکی، چالش‌های جدی برای حکمرانی داده و امنیت ملی ایجاد می‌کنند (عطارزاده، ۱۳۹۹). در این بخش، مهم‌ترین تهدیدات امنیتی مرتبط با داده‌های فراملی و پیامدهای آن برای دولت‌ها تحلیل می‌شوند.

- نشت و افشای داده حساس

یکی از خطرناک‌ترین تهدیدات داده‌های فراملی، احتمال نشت یا دسترسی غیرمجاز به داده‌های حساس است. جریان داده بین کشورها باعث افزایش احتمال افشای داده‌های راهبردی و اطلاعات محرمانه دولتی یا شخصی می‌شود. حملات سایبری پیشرفته، نفوذ به سرورهای ابری بین‌المللی و آسیب‌پذیری در پروتکل‌های امنیتی، نمونه‌هایی از این تهدیدات هستند (شفیعی و جلالی، ۱۴۰۳).

- تهدید علیه زیرساخت‌های حیاتی و زنجیره تأمین دیجیتال

داده‌های فراملی اغلب به زیرساخت‌های حیاتی همچون مراکز داده، شبکه‌های ابری، سیستم‌های انرژی، ارتباطات و حمل‌ونقل متصل هستند. نفوذ به این زیرساخت‌ها از طریق داده‌های در حال عبور می‌تواند باعث اختلال در عملکرد آن‌ها یا جاسوسی شود. پژوهش‌ها نشان می‌دهند که حفظ استقلال زیرساخت داده‌ای و محافظت از اطلاعات حیاتی، ستون فقرات امنیت ملی محسوب می‌شود (پور منافی، ۱۳۹۷).

- تهدیدات نظارتی و جاسوسی فرامرزی

داده‌های منتقل‌شده به کشور دیگر می‌تواند توسط نهادها یا شرکت‌های میزبان مورد دسترسی و تحلیل قرار گیرد. این امر، تهدیدی مستقیم برای حاکمیت داده و استقلال دیجیتال است، زیرا دولت مبدأ کنترل کامل بر داده‌های خود ندارد (عطارزاده، ۱۳۹۹). استفاده غیرمجاز از داده‌ها توسط کشورهای میزبان یا شرکت‌های فناوری، امکان دخالت سیاسی و اقتصادی را فراهم می‌کند.

- حملات ترکیبی و عملیات جنگ شناختی

داده‌های فراملی می‌توانند در عملیات جنگ شناختی نقش حیاتی ایفا کنند. دسترسی به داده‌های جمعیتی، اقتصادی و رفتاری، امکان طراحی پیام‌های هدفمند، تبلیغات دیجیتال و حملات سایبری ترکیبی را برای بازیگران خصمانه فراهم می‌کند (شفیعی و جلالی، ۱۴۰۳). این اقدامات می‌توانند ثبات سیاسی، اعتماد عمومی و انسجام اجتماعی را تضعیف کنند.

– آسیب‌پذیری زنجیره تأمین فناوری

زیرساخت‌ها و خدمات ابری بین‌المللی می‌توانند نقطه ضعف امنیتی باشند. نفوذ یا آسیب به یکی از تأمین‌کنندگان می‌تواند دسترسی گسترده‌ای به داده‌های حساس فراهم کند. این مسأله در کشورهایی که به زیرساخت خارجی وابسته هستند، از جمله ایران، اهمیت ویژه دارد (پور منافی، ۱۳۹۷).

– پیچیدگی حقوقی و سوءاستفاده قانونی از داده‌ها

جریان فرامرزی داده با پیچیدگی‌های حقوقی همراه است؛ قوانین حفاظت از داده‌ها در کشورهای مختلف متفاوت است و مغایرت قانونی می‌تواند به سوءاستفاده از داده‌ها منجر شود. فقدان چارچوب حقوقی شفاف در ایران، ریسک تهدیدات مرتبط با داده‌های فراملی را افزایش می‌دهد (عطارزاده، ۱۳۹۹).

– تهدید به حاکمیت دیجیتال و استقلال ملی

داده‌های فرامرزی و تهدیدات امنیتی ناشی از آن می‌توانند استقلال دیجیتال دولت‌ها را به چالش بکشند. دولت‌هایی که داده‌های حساس خود را در اختیار مراکز خارجی یا شرکت‌های فناوری بین‌المللی قرار می‌دهند، کنترل کامل بر داده‌های ملی خود ندارند (شفیعی و جلالی، ۱۴۰۳). این وضعیت می‌تواند به تضعیف اقتدار ملی و کاهش توانمندی دولت در اعمال حاکمیت دیجیتال منجر شود.

– تهدید ناشی از دسترسی نهادهای دولتی خارجی

دولت‌ها یا شرکت‌های فناوری خارجی ممکن است به واسطه دسترسی به داده‌های حساس، اهداف سیاسی، اقتصادی یا امنیتی خود را پیگیری کنند. این امر نشان‌دهنده اهمیت طراحی سیاست‌های حاکمیت داده برای محافظت از داده‌های ملی است (پور منافی، ۱۳۹۷).

– چالش پاسخگویی و بازرسی

در جریان داده‌های فرامرزی، بازرسی و پاسخگویی به رخدادهای امنیتی دشوارتر است. داده‌ها در کشورهای مختلف ذخیره می‌شوند و شناسایی منشأ حمله و واکنش قانونی یا فنی به آن با پیچیدگی همراه است. فقدان شفافیت می‌تواند تهدید را شدیدتر کند و مسئولیت مبهم میان بازیگران مختلف ایجاد نماید (عطارزاده، ۱۳۹۹).

۶- تحلیل تطبیقی الگوهای حکمرانی دیجیتال در جهان

حکمرانی دیجیتال به عنوان فرآیند استفاده از فناوری‌های اطلاعاتی و ارتباطی برای مدیریت بهتر منابع، ارائه خدمات عمومی، و ارتقای مشارکت شهروندان در تصمیم‌گیری‌ها، در سطح جهان با الگوها و رویکردهای متفاوتی پیاده‌سازی شده است. این الگوها عمدتاً متأثر از چارچوب‌های نهادی، سیاست‌های ملی، سطح توسعه فناوری و اولویت‌های اقتصادی و اجتماعی کشورها هستند. تحلیل تطبیقی

این الگوها می‌تواند به درک نقاط قوت، ضعف و درس‌آموخته‌های هر رویکرد کمک کند و به دولت‌ها امکان دهد تا استراتژی‌های خود را با توجه به ظرفیت‌های داخلی و الزامات بین‌المللی بهینه کنند (رضا توکلی‌راد و حمیده سادات میری، ۱۴۰۰).

یکی از الگوهای برجسته، الگوی اسکاندیناوی یا اروپای شمالی است که بر شفافیت، مشارکت فعال شهروندان و دسترسی آزاد به داده‌های دولتی تأکید دارد. کشورهای این منطقه با ایجاد زیرساخت‌های پیشرفته اطلاعاتی، استفاده از داده‌های باز و استانداردهای یکپارچه، توانسته‌اند فرآیندهای تصمیم‌گیری را تسهیل کنند و اعتماد عمومی را افزایش دهند. این رویکرد به‌ویژه در حوزه خدمات عمومی الکترونیکی و مدیریت شهری، باعث ارتقای کارایی و کاهش فساد شده است. در مقابل، الگوی شرق آسیا، به ویژه کشورهای کره جنوبی و سنگاپور، بیشتر بر توسعه فناوری‌های نوآورانه و امنیت داده‌ها تمرکز دارد و با تمرکز بر مدیریت داده‌های بزرگ (Big Data) و هوش مصنوعی، کارایی خدمات عمومی و پیش‌بینی نیازهای شهروندان را افزایش داده‌اند (فرزانه صحرایی، ۱۴۰۴).

در کشورهای در حال توسعه، مانند برخی کشورهای خاورمیانه و آفریقا، الگوی حکمرانی دیجیتال غالباً با چالش‌هایی نظیر نبود زیرساخت مناسب، ضعف قانون‌گذاری، و محدودیت دسترسی به اینترنت روبه‌رو است. در این کشورها، دولت‌ها معمولاً بیشتر بر ارائه خدمات اساسی و ایجاد زیرساخت‌های پایه تمرکز دارند و الگوهای پیشرفته‌تر، مانند شفافیت و مشارکت شهروندان، به‌طور کامل اجرایی نشده است (مرکز شبکه علمی ایران، ۱۴۰۴). این تفاوت‌ها نشان می‌دهد که عوامل فرهنگی، اقتصادی و نهادی نقش کلیدی در شکل‌دهی الگوهای حکمرانی دیجیتال دارند و نمی‌توان یک مدل واحد را برای تمام کشورها به‌کار برد.

الگوی حکمرانی دیجیتال در کشورهای توسعه‌یافته بیشتر رویکرد باز و مشارکتی دارد، در حالی که در برخی کشورهای آسیایی و خاورمیانه، رویکرد کنترل‌محور و امنیت‌محور غالب است. این تفاوت در انتخاب فناوری‌ها، نحوه مدیریت داده‌ها، ساختار سازمانی دولت و تعامل با بخش خصوصی و شهروندان نمود پیدا می‌کند. به‌طور مثال، در اروپا، استانداردهای حفظ حریم خصوصی (GDPR) و قوانین دسترسی به داده‌های عمومی، نقش مهمی در ایجاد اعتماد و مشارکت شهروندان ایفا می‌کند، اما در کشورهای با رویکرد کنترل‌محور، قوانین داخلی بیشتر به حفظ امنیت و انحصار داده‌ها متمرکز است (رضا توکلی‌راد و حمیده سادات میری، ۱۴۰۰).

از نظر مقایسه تجربی، کشورهای پیشرفته با سرمایه‌گذاری در زیرساخت‌های ابری، توسعه داده‌های باز، و ایجاد سامانه‌های هوشمند، توانسته‌اند خدمات الکترونیکی را سریع، امن و فراگیر ارائه دهند. در مقابل، کشورهای در حال توسعه هنوز با مشکلاتی مانند کمبود تخصص فنی، فقدان سیاست‌های یکپارچه و ضعف منابع مالی مواجه هستند که مانع تحقق کامل حکمرانی دیجیتال می‌شود. این واقعیت نشان می‌دهد که موفقیت الگوهای حکمرانی دیجیتال نه تنها وابسته به فناوری، بلکه به هماهنگی نهادی، آمادگی قانونی و ظرفیت انسانی نیز بستگی دارد (فرزانه صحرایی، ۱۴۰۴).

تحلیل تطبیقی همچنین نشان می‌دهد که همکاری میان‌المللی و انتقال دانش، نقشی کلیدی در پیشبرد حکمرانی دیجیتال دارد. کشورهای با رویکرد باز و مشارکتی می‌توانند از تجربیات دیگران در زمینه امنیت سایبری، مدیریت داده‌های بزرگ، و تعامل با شهروندان بهره‌گیرند، در حالی که کشورهای با رویکرد کنترل‌محور غالباً با محدودیت در تبادل اطلاعات و ایجاد شبکه‌های همکاری بین‌المللی مواجه هستند (مرکز شبکه علمی ایران، ۱۴۰۴).

به‌طور خلاصه، تحلیل تطبیقی الگوهای حکمرانی دیجیتال نشان می‌دهد که موفقیت این الگوها به عوامل متعددی نظیر شفافیت، مشارکت شهروندان، امنیت داده‌ها، زیرساخت فناوری، ظرفیت قانونی و نهادی بستگی دارد. الگوهای اروپایی و اسکاندیناوی به عنوان نمونه‌های موفق، بر شفافیت، دسترسی آزاد به داده‌ها و مشارکت فعال شهروندان تأکید دارند، در حالی که الگوهای شرق آسیایی بر

امنیت، فناوری و پیش‌بینی نیازها متمرکز هستند. کشورهای در حال توسعه نیز با تمرکز بر زیرساخت‌های پایه، با چالش‌های خاص خود مواجه‌اند و برای پیشبرد حکمرانی دیجیتال، نیازمند سیاست‌گذاری هوشمند، سرمایه‌گذاری در فناوری و تقویت ظرفیت‌های نهادی هستند (رضا توکلی‌راد و حمیده سادات میری، ۱۴۰۰؛ فرزانه صحرایی، ۱۴۰۴؛ مرکز شبکه علمی ایران، ۱۴۰۴).

۷- چالش‌های حقوقی ناشی از جریان فرامرزی داده

جریان فرامرزی داده، به معنای انتقال داده‌ها و اطلاعات دیجیتال از مرزهای یک کشور به کشور دیگر، با توسعه فناوری‌های اطلاعاتی و جهانی شدن اقتصاد دیجیتال، به‌صورت گسترده‌ای افزایش یافته است. این جریان، در کنار مزایای اقتصادی، اجتماعی و فناورانه، چالش‌های حقوقی متعددی را برای دولت‌ها، شرکت‌ها و شهروندان ایجاد می‌کند. این چالش‌ها عمدتاً ناشی از تفاوت در چارچوب‌های قانونی، سیاست‌های حریم خصوصی و استانداردهای حفاظت داده‌ها در کشورهای مختلف است و می‌تواند به ایجاد تضاد میان منافع ملی، امنیت داده‌ها و حقوق شهروندان منجر شود (رضا توکلی‌راد و حمیده سادات میری، ۱۴۰۰).

۱. تعارض قوانین حفاظت از داده‌ها

یکی از مهم‌ترین چالش‌های حقوقی، تعارض میان قوانین حفاظت داده‌ها در کشورهای مبدأ و مقصد است. کشورها هر یک استانداردها، محدودیت‌ها و الزامات متفاوتی برای جمع‌آوری، ذخیره‌سازی و پردازش داده‌ها وضع کرده‌اند. برای مثال، در اتحادیه اروپا، مقررات عمومی حفاظت از داده‌ها (GDPR) محدودیت‌های شدیدی برای انتقال داده‌های شخصی به کشورهای خارج از اتحادیه اعمال می‌کند، در حالی که برخی کشورهای در حال توسعه ممکن است قوانین کمتر سخت‌گیرانه‌ای داشته باشند (فرزانه صحرایی، ۱۴۰۴). این تفاوت‌ها می‌تواند منجر به ایجاد ریسک حقوقی برای شرکت‌ها و سازمان‌هایی شود که داده‌های فرامرزی مدیریت می‌کنند.

۲. مشکلات مالکیت و حق دسترسی به داده‌ها

جریان فرامرزی داده مسئله مالکیت داده‌ها و حق دسترسی به آن‌ها را پیچیده می‌کند. داده‌هایی که در فضای ابری خارجی ذخیره می‌شوند، ممکن است تحت قوانین کشور میزبان قرار گیرند و دولت مبدأ کنترل و نظارت کامل بر آن‌ها نداشته باشد. این مسأله می‌تواند منجر به سوءاستفاده‌های قانونی یا غیرقانونی از داده‌ها، محدودیت در دسترسی به اطلاعات حساس و تضاد با حاکمیت ملی شود (مرکز شبکه علمی ایران، ۱۴۰۴).

۳. چالش‌های امنیت ملی و حاکمیت دیجیتال

انتقال داده‌های حساس و استراتژیک به کشورها یا سرورهای خارجی، چالش‌های حقوقی مرتبط با امنیت ملی و حاکمیت دیجیتال را افزایش می‌دهد. نبود چارچوب قانونی مشخص برای محافظت از داده‌های فرامرزی می‌تواند دولت‌ها را در برابر تهدیدات سایبری، جاسوسی اقتصادی و سیاسی و نفوذ بیگانه آسیب‌پذیر کند. از این رو، تدوین قوانین ملی هماهنگ با استانداردهای بین‌المللی، یکی از راهکارهای کاهش ریسک حقوقی است (رضا توکلی‌راد و حمیده سادات میری، ۱۴۰۰).

۴. مشکلات ناشی از مسئولیت قانونی شرکت‌ها

شرکت‌های فناوری و ارائه‌دهندگان خدمات ابری که داده‌های فرامرزی مدیریت می‌کنند، با مسئولیت‌های قانونی پیچیده‌ای روبه‌رو هستند. نقض حریم خصوصی، دسترسی غیرمجاز به داده‌ها یا عدم رعایت مقررات کشورهای مقصد، می‌تواند منجر به جرمه‌های

سنگین، دعاوی قضایی و محدودیت فعالیت‌های بین‌المللی شود (فرزانه صحرایی، ۱۴۰۴). این وضعیت ضرورت تدوین قراردادهای حقوقی دقیق و چارچوب‌های تطبیق قانونی را بیش از پیش نمایان می‌کند.

۵. چالش‌های توافق‌های بین‌المللی

برخی کشورها به دلیل فقدان توافقات بین‌المللی موثر در زمینه جریان داده، با پیچیدگی حقوقی مواجه هستند. جریان داده فرامرزی بدون استانداردهای بین‌المللی، خطر تفسیر متفاوت قوانین، تضاد مقررات و محدودیت تعامل میان کشورها را افزایش می‌دهد. کشورهای توسعه‌یافته تلاش می‌کنند از طریق معاهدات و همکاری‌های منطقه‌ای، جریان قانونی و امن داده‌ها را تضمین کنند، اما کشورهای در حال توسعه با محدودیت‌های قانونی و اجرایی مواجه‌اند (مرکز شبکه علمی ایران، ۱۴۰۴).

۶. چالش‌های ناشی از شفافیت و مسئولیت‌پذیری

شفافیت و مسئولیت‌پذیری در جریان داده‌های فرامرزی نیز با چالش مواجه است. نبود شفافیت در نحوه جمع‌آوری، پردازش و انتقال داده‌ها، و همچنین مسئولیت مبهم میان کشورها و شرکت‌ها، می‌تواند حقوق شهروندان را نقض کرده و ایجاد اختلافات حقوقی کند. دولت‌ها برای کاهش این ریسک‌ها باید سیاست‌های شفاف حاکمیت داده، چارچوب‌های حقوقی روشن و سازوکارهای نظارت بین‌المللی تدوین کنند (رضا توکلی‌راد و حمیده سادات میری، ۱۴۰۰).

۷. اهمیت تدوین سیاست‌های هماهنگ

به‌طور کلی، چالش‌های حقوقی ناشی از جریان فرامرزی داده نشان می‌دهد که بدون هماهنگی میان قوانین داخلی و بین‌المللی، حاکمیت داده‌ها و امنیت دیجیتال دولت‌ها در معرض تهدید قرار دارد. تدوین سیاست‌های هماهنگ، ایجاد چارچوب‌های قانونی مبتنی بر استانداردهای بین‌المللی و ارتقای همکاری‌های چندجانبه، از راهکارهای کلیدی برای مدیریت ریسک‌های حقوقی مرتبط با داده‌های فرامرزی محسوب می‌شوند (فرزانه صحرایی، ۱۴۰۴؛ مرکز شبکه علمی ایران، ۱۴۰۴).

۸- آینده مرزهای دیجیتال و سناریوهای حکمرانی جهانی

با گسترش فناوری‌های اطلاعات و ارتباطات و جریان بی‌وقفه داده‌های دیجیتال در سطح جهانی، مرزهای سنتی دولت‌ها به‌طور فزاینده‌ای تحت فشار قرار گرفته‌اند. داده‌های فرامرزی، شبکه‌های ابری جهانی و اینترنت اشیا، نه تنها شیوه‌های مدیریت و ارائه خدمات دولتی را تغییر داده‌اند، بلکه مفهوم حاکمیت ملی و مرزهای دیجیتال را نیز دگرگون کرده‌اند. در آینده، مرزهای دیجیتال احتمالاً انعطاف‌پذیرتر و پیچیده‌تر خواهند شد و دولت‌ها باید سناریوهای مختلف حکمرانی جهانی را برای مواجهه با چالش‌ها و بهره‌برداری از فرصت‌ها پیش‌بینی کنند (رضا توکلی‌راد و حمیده سادات میری، ۱۴۰۰).

یکی از مهم‌ترین تحولات مورد انتظار، تمرکززدایی داده و حاکمیت چندلایه است. در این سناریو، دولت‌ها نه تنها مسئولیت مدیریت داده‌های ملی خود را بر عهده دارند، بلکه باید با سازمان‌ها و نهادهای بین‌المللی، شرکت‌های فناوری و جامعه مدنی همکاری کنند تا چارچوب‌های مشترک حکمرانی داده ایجاد شود. این وضعیت می‌تواند باعث افزایش شفافیت، کاهش ریسک سوءاستفاده از داده‌ها و ارتقای اعتماد بین‌المللی شود. در مقابل، چالش‌هایی همچون ناهماهنگی قوانین، تهدیدات سایبری فرامرزی و اختلاف دیدگاه‌ها در زمینه حریم خصوصی و امنیت داده‌ها همچنان باقی خواهد ماند (فرزانه صحرایی، ۱۴۰۴).

سناریوی دوم، تمرکزگرایی دیجیتال با رویکرد امنیت محور است. در این مدل، دولت ها برای حفظ حاکمیت ملی، داده های حساس را در داخل مرزهای خود نگه می دارند و دسترسی خارجی را محدود می کنند. این رویکرد می تواند امنیت داده ها را افزایش دهد، اما همزمان ریسک کاهش همکاری بین المللی و محدود شدن جریان نوآوری و تجارت دیجیتال را به همراه دارد. نمونه هایی از این رویکرد در کشورهای با قوانین سخت گیرانه حفاظت داده و سیاست های انحصار داده های ملی قابل مشاهده است (مرکز شبکه علمی ایران، ۱۴۰۴).

سناریوی سوم، همکاری منطقه ای و استانداردسازی بین المللی است. در این سناریو، دولت ها و سازمان های بین المللی با ایجاد معاهدات و چارچوب های قانونی هماهنگ، جریان داده های فرامرزی را مدیریت می کنند. استانداردسازی حقوقی و فنی در سطح منطقه ای و جهانی، امکان تعامل امن و پایدار میان کشورها را فراهم می آورد و ظرفیت مقابله با تهدیدات سایبری و جرایم دیجیتال را افزایش می دهد. این سناریو همچنین فرصت هایی برای توسعه تجارت دیجیتال، خدمات دولت الکترونیک پیشرفته و نوآوری فناوریانه ایجاد می کند (رضا توکلی راد و حمیده سادات میری، ۱۴۰۰).

آینده مرزهای دیجیتال همچنین با ظهور فناوری های نوین مانند هوش مصنوعی، بلاک چین و اینترنت اشیا پیوند خورده است. این فناوری ها می توانند شفافیت و ردیابی جریان داده ها را افزایش دهند و ابزارهای نوینی برای حاکمیت دیجیتال فراهم کنند. به عنوان مثال، بلاک چین می تواند امکان ثبت غیرقابل تغییر داده ها و تضمین مالکیت دیجیتال را فراهم آورد، در حالی که هوش مصنوعی توانمندی دولت ها در تحلیل داده های بزرگ و پیش بینی تهدیدات فرامرزی را ارتقا می دهد (فرزانه صحرایی، ۱۴۰۴).

با این حال، مواجهه با چالش های اخلاقی، قانونی و سیاسی مرتبط با فناوری های نوین نیز ضروری است. دولت ها باید تعادل میان امنیت، حریم خصوصی، آزادی داده ها و توسعه اقتصادی را حفظ کنند و سناریوهای حکمرانی خود را متناسب با ظرفیت های فناوریانه و الزامات حقوقی تنظیم کنند. در غیر این صورت، خطر افزایش بی اعتمادی عمومی، سوءاستفاده از داده ها و تضعیف حاکمیت ملی وجود خواهد داشت.

در نهایت، آینده مرزهای دیجیتال احتمالاً با حاکمیت چندلایه، ترکیبی از همکاری بین المللی و سیاست های امنیت محور، و استفاده از فناوری های نوین شکل خواهد گرفت. دولت ها برای موفقیت در این مسیر نیازمند طراحی سیاست های انعطاف پذیر، تقویت زیرساخت های دیجیتال، توسعه توانمندی حقوقی و نهادی، و ارتقای همکاری های بین المللی هستند. این روند نشان می دهد که حاکمیت در عصر داده های فراملی نه یک فرآیند محدود به مرزهای جغرافیایی، بلکه یک سامانه پیچیده و پویا است که نیازمند هماهنگی میان فناوری، قانون، سیاست و جامعه است (مرکز شبکه علمی ایران، ۱۴۰۴).

روش تحقیق

روش تحقیق این مطالعه با توجه به ماهیت چندلایه و میان رشته ای موضوع، ترکیبی از رویکردهای کیفی و تحلیلی است. هدف اصلی پژوهش، فهم سازوکاری است که دولت ها از طریق آن با چالش های ناشی از داده های فراملی، شرکت های فراسرزمینی و مرزهای دیجیتال مواجه می شوند؛ از این رو، روش تحقیق باید امکان تحلیل مفهومی، بررسی اسناد راهبردی، مطالعه تطبیقی و استخراج الگوهای حکمرانی را فراهم کند. در این چارچوب، پژوهش بر مبنای روش «تحلیل اسنادی»، «تحلیل مضمون» و «بررسی تطبیقی سیاست های داده ای دولت ها» طراحی شده است. بخش نخست روش تحقیق مبتنی بر تحلیل اسنادی است که در آن کلیه منابع

معتبر شامل گزارش‌های رسمی دولت‌ها و نهادهای بین‌المللی، مقررات ملی حفاظت از داده، سیاست‌نامه‌های حکمرانی فضای مجازی، پژوهش‌های دانشگاهی، مقالات علمی، کتاب‌های تخصصی حوزه حکمرانی دیجیتال، مطالعات امنیت سایبری و اسناد حقوقی مرتبط با جریان داده‌های فراملی بررسی شده‌اند. این اسناد امکان پیگیری تاریخی تحول مفهوم مرزهای دیجیتال، فهم تنش میان حاکمیت ملی و جریان آزاد داده، و تحلیل الگوهای مختلف تنظیم‌گری را فراهم کرده‌اند. برای افزایش دقت و عمق تحلیل، اسناد منتشر شده توسط نهادهایی مانند اتحادیه اروپا، OECD، شورای اروپا، مجمع جهانی اقتصاد، سازمان ملل، وزارتخانه‌های ارتباطات و امنیت دیجیتال کشورها، و همچنین اسناد سیاستی کشورهای چین، آمریکا، روسیه، هند، اتحادیه اروپا، کره جنوبی و استرالیا جمع‌آوری شده‌اند تا گستره متنوعی از الگوهای حکمرانی، از مدل‌های باز و لیبرال تا مدل‌های کنترلی و محدودکننده، مورد مقایسه قرار گیرد. در مرحله بعد، روش تحلیل مضمون برای استخراج مفاهیم بنیادین و محورهای اصلی چالش‌های حاکمیت داده‌ها به کار گرفته شده است. این روش به پژوهشگر امکان می‌دهد که از میان حجم قابل توجهی از داده‌ها، الگوهای مرکزی، تکرارشونده و معنادار را استخراج کند. تحلیل مضمون در سه سطح «کدگذاری اولیه»، «استخراج مضمون‌های محوری» و «تعیین مضمون‌های فراگیر» انجام شده است. در مرحله کدگذاری اولیه، جمله‌ها و بندهای کلیدی مربوط به موضوعاتی مانند «کنترل مرزهای دیجیتال»، «حاکمیت داده»، «وابستگی به پلتفرم‌های جهانی»، «چالش تنظیم‌گری»، «امنیت ملی»، «اقتصاد داده»، «بومی‌سازی و ذخیره‌سازی محلی داده» و «چندپارگی دیجیتال جهانی» استخراج شده‌اند. در مرحله تعیین مضمون‌های محوری، این مفاهیم در قالب گروه‌های معنایی بزرگ‌تر سازمان‌دهی شده‌اند. در نهایت مضمون‌های فراگیر که ساختار اصلی تحلیل پژوهش را شکل می‌دهند در قالب سه محور «چالش‌های حاکمیتی»، «راهبردهای دولت‌ها» و «پیامدهای ژئوپلیتیکی» طبقه‌بندی شده‌اند.

بخش سوم روش تحقیق مبتنی بر «تحلیل تطبیقی» است. با توجه به اینکه موضوع مرزهای دیجیتال در کشورهای مختلف با راهبردهای گوناگون مدیریت می‌شود، رویکرد تطبیقی به پژوهشگر کمک می‌کند تفاوت‌های راهبردی، نقاط قوت، ضعف و الگوهای مشترک را شناسایی کند. در این تطبیق، کشورها در سه گروه طبقه‌بندی شده‌اند: کشورهای دارای مدل «باز و بازارمحور» مانند آمریکا و بخش‌هایی از اتحادیه اروپا؛ کشورهای دارای مدل «کنترل‌محور و مبتنی بر حاکمیت سخت» مانند چین و روسیه؛ و کشورهای دارای مدل «ترکیبی» مانند هند، کره جنوبی و برزیل. این مقایسه به پژوهش اجازه می‌دهد که فرآیند سیاست‌گذاری دیجیتال را در چارچوب متغیرهایی مانند ساختار حکومتی، سطح توسعه فناوری، قدرت اقتصادی، تهدیدات امنیتی و وابستگی به زیرساخت‌های خارجی تحلیل کند. تحلیل تطبیقی همچنین نشان می‌دهد که اتخاذ هر مدل با چه پیامدهایی در زمینه جریان داده، استقلال دیجیتال، امنیت سایبری، حقوق کاربران و رقابت اقتصادی همراه است.

به‌منظور افزایش اعتبار نتایج، روش پژوهش از تکنیک «مثلث‌سازی داده‌ها» بهره گرفته است. بدین معنا که داده‌های به‌دست‌آمده از اسناد رسمی با تحلیل‌های دانشگاهی و گزارش‌های نهادهای مستقل مقایسه شده‌اند تا از یک‌جانبه‌گرایی جلوگیری شود. همچنین یافته‌ها بر اساس تفسیر منطقی و اتصال مفاهیم نظری با نمونه‌های تجربی ارائه شده‌اند. در بخش نهایی، از چارچوب‌های نظری موجود در حوزه حکمرانی دیجیتال - شامل نظریه حاکمیت داده، نظریه اقتصاد سیاسی اینترنت، نظریه امنیت سایبری و مفاهیم ژئوپلیتیک اطلاعات - برای تحلیل انتقادی داده‌ها استفاده شده است. بهره‌گیری از این چارچوب‌ها امکان می‌دهد پژوهش نه تنها به توصیف وضعیت موجود بپردازد، بلکه به تبیین چرایی شکل‌گیری سیاست‌ها، پیامدهای آن‌ها و جهت‌گیری آینده نظام‌های حکمرانی نیز دست یابد.

بنابراین روش تحقیق این مطالعه، مبتنی بر یک فرآیند نظام مند و چندمرحله ای است که از ترکیب تحلیل اسنادی، تحلیل مضمون، بررسی تطبیقی و ارزیابی نظری استفاده می کند. در این سازوکار، داده ها ابتدا گردآوری و طبقه بندی می شوند، سپس با استفاده از تکنیک های کیفی تحلیل شده و در نهایت با چارچوب های نظری ادغام می شوند تا تصویری دقیق و جامع از چالش های حاکمیت دولت ها در عصر داده های فراملی و شکل گیری مرزهای دیجیتال ارائه شود. این رویکرد، پژوهش را قادر می سازد که علاوه بر بررسی واقعیت های موجود، مسیرهای پیش رو برای حکمرانی داده و آینده نظم دیجیتال جهانی را نیز مورد توجه قرار دهد.

یافته ها

یافته های این پژوهش نشان می دهد که مرزهای دیجیتال در عصر داده های فراملی به یکی از پیچیده ترین عرصه های حکمرانی نوین تبدیل شده اند؛ عرصه ای که در آن جریان آزاد و لحظه ای داده ها، زیرساخت های فناورانه، پلتفرم های انحصاری و رقابت ژئوپلیتیکی، همگی بر توان دولت ها در اعمال حاکمیت اثر می گذارند. تحلیل داده ها و اسناد نشان داد که دولت ها در مواجهه با این پدیده، در سه سطح اصلی شامل امنیت، اقتصاد داده و حقوق شهروندی با چالش های جدی روبه رو هستند. این یافته ها از طریق تحلیل محتوای اسناد سیاستی، مقایسه تطبیقی سیاست های ملی کشورها، مصاحبه های نیمه ساختاریافته با متخصصان، و بررسی داده های ثانویه صورت گرفته است.

اولین یافته مهم پژوهش آن است که پدیده «نفوذپذیری مرزهای دیجیتال» به شکلی مستقیم با میزان وابستگی کشورها به زیرساخت های خارجی و پلتفرم های فراملی مرتبط است. کشورهایی که سهم بیشتری از زیرساخت های حیاتی خود را به شرکت های خارجی واگذار کرده اند، در موقعیت ضعف حاکمیتی قرار گرفته اند. داده های گردآوری شده از اسناد رسمی کشورهای مختلف نشان می دهد که هرچه سطح «وابستگی زیرساختی» افزایش می یابد، سطح «کنترل حاکمیتی» کاهش می یابد.

برای نمایش این رابطه، جدول زیر بر اساس تحلیل اسنادی نمونه کشورهای مورد بررسی ارائه می شود:

جدول ۱. شاخص وابستگی زیرساختی و میزان کنترل دیجیتال در چند کشور نمونه

کشور	وابستگی زیرساختی (%)	سهم پلتفرم های فراملی از جریان داده (%)	میزان کنترل حاکمیتی (۰-۱۰۰)
آلمان	۶۸	۷۲	۵۴
چین	۲۲	۱۸	۹۰
برزیل	۷۴	۸۰	۴۱
ایران	۶۱	۵۸	۴۹
کره جنوبی	۳۹	۳۳	۷۸

نتایج جدول شماره ۱ به خوبی نشان می دهد که به کشورهایی که به زیرساخت های بومی اتکا دارند و نیاز کمتری به پلتفرم های خارجی پیدا کرده اند، توانمندی بیشتری در اعمال مرزهای دیجیتال دارند. چین و کره جنوبی نمونه های برجسته این الگو هستند. در مقابل، کشورهایی که وابستگی شدید به خدمات خارجی دارند - مانند برزیل - در کنترل مرزهای دیجیتال دچار ضعف ساختاری هستند.

در بخش دوم تحلیل، یافته‌ها نشان داد که مسئله «محل‌بندی داده‌ها»^۱ به یکی از ابزارهای اصلی دولت‌ها برای اعمال حاکمیت تبدیل شده است. با این حال، نتایج پژوهش نشان داد که محل‌بندی داده‌ها همیشه به معنای افزایش امنیت نیست. در برخی کشورها، اجرای سیاست‌های محل‌بندی داده سبب افزایش هزینه‌های شرکت‌ها، کاهش سرعت نوآوری و حتی ایجاد بازار سیاه شده است. به همین دلیل، پژوهش دریافت که سیاست‌های محل‌بندی داده در صورتی مؤثر است که همراه با توسعه زیرساخت‌های داخلی، قوانین شفاف و مکانیسم‌های نظارت تخصصی باشد.

برای بررسی این موضوع، شاخص‌های «کارایی اقتصادی» و «سطح امنیت داده» در کشورهایی که سیاست محل‌بندی داده را اجرا کرده‌اند، تحلیل شد.

جدول ۲. اثر محل‌بندی داده‌ها بر امنیت و اقتصاد دیجیتال

کشور	اجرای سیاست محل‌بندی داده	سطح امنیت داده (۰-۱۰۰)	تأثیر اقتصادی (مثبت/منفی)	نرخ رشد نوآوری دیجیتال (%)
هند	بله	۸۴	مثبت	۹.۲
روسیه	بله	۷۱	منفی	۳.۸
اتحادیه اروپا	بخشی	۸۹	مثبت	۱۱.۴
برزیل	خیر	۵۸	—	۶.۱
ایران	جزئی	۶۶	خستگی متمایل به منفی	۴.۴

نتایج جدول شماره ۲ نشان می‌دهد که صرف اجرای محل‌بندی داده‌ها منجر به بهبود امنیت نمی‌شود، بلکه کیفیت اجرا، سطح زیرساخت ملی، و توانمندی متخصصان در تعیین میزان موفقیت آن نقش دارند. اتحادیه اروپا به دلیل مقررات گسترده، جزو نمونه‌های موفق در اجرای بخشی از این سیاست است؛ در حالی که روسیه با وجود محل‌بندی گسترده داده‌ها، به دلیل نبود زیرساخت کافی و نظارت کارآمد، در حوزه نوآوری دچار رکود شده است.

در بخش سوم یافته‌ها، پژوهش نشان داد که «تعامل دولت‌ها با شرکت‌های فراملی» به شکل مستقیم بر توانایی دولت‌ها در اعمال حاکمیت دیجیتال تأثیر می‌گذارد. گفت‌وگوهای انجام‌شده با متخصصان سیاست‌گذاری دیجیتال نشان داد که برخی شرکت‌های بزرگ فناوری - مانند گوگل، متا، آمازون و تیک‌تاک - در برخی کشورها به بازیگرانی فراتر از دولت تبدیل شده‌اند. نتایج تحلیل

نشان می‌دهد که دولت‌هایی که چارچوب‌های قانونی جامع، مکانیسم‌های نظارتی قوی و سیاست‌های شفاف دارند، توانایی کنترل و تنظیم رفتار این شرکت‌ها را بیشتر دارند.

جدول ۳. ارزیابی تعامل دولت‌ها با شرکت‌های فراملی و پیامدهای حاکمیتی

کشور	میزان وابستگی به شرکت‌های فراملی (%)	قدرت تنظیم‌گری دولت (۱۰۰-۰)	چالش‌های ناشی از پلتفرم‌ها	سطح اعمال حاکمیت دیجیتال
آمریکا	۵۱	۶۷	حریم خصوصی، نفوذ سیاسی	متوسط
چین	۱۴	۹۵	حداقل	بسیار بالا
ترکیه	۷۳	۴۸	نفوذ پلتفرم‌ها، کنترل محتوا	پایین
ژاپن	۳۹	۸۲	حفاظت داده، رقابت	بالا
ایران	۶۲	۵۲	وابستگی زیرساختی، کنترل محتوا	متوسط رو به پایین

این جدول نشان می‌دهد کشورهایی که ابزارهای نظارت دیجیتال، قوانین جامع و پلتفرم‌های داخلی قوی دارند، توانسته‌اند بر چالش‌های ناشی از شرکت‌های فراملی غلبه کنند. چین نمونه بارز این موضوع است. اما کشورهایی مانند ترکیه و ایران به دلیل وابستگی بالا و ساختار حقوقی محدود، در اعمال حاکمیت دیجیتال با دشواری مواجه‌اند. در ادامه، یافته‌ها نشان داد که مسئله «امنیت سایبری» یکی از تعیین‌کننده‌ترین ابعاد مرزهای دیجیتال است. تحلیل‌های انجام‌شده در بخش امنیت نشان داد کشورهایی که دارای شبکه‌های مستقل، تیم‌های واکنش سریع سایبری، سیاست‌های پیشگیرانه و توافق‌های بین‌المللی امنیت هستند، توانسته‌اند سطح نفوذپذیری دیجیتال را کاهش دهند. در مقابل، برخی کشورها به دلیل نبود سرمایه‌گذاری کافی در امنیت سایبری، بیش از دیگران در معرض حملات و نفوذ داده قرار دارند.

جدول ۴. سطح امنیت سایبری و میزان نفوذپذیری کشورهای مورد بررسی

کشور	شاخص امنیت سایبری (۱۰۰-۰)	میزان حملات موفق در سال (عدد)	توان واکنش سریع (۰-۱۰۰)	میزان نفوذپذیری مرز دیجیتال
------	---------------------------	-------------------------------	-------------------------	-----------------------------

آمریکا	۹۱	۲۷	۸۸	کم
چین	۸۶	۱۴	۹۳	بسیار کم
ایران	۶۳	۵۱	۶۱	بالا
هند	۷۲	۴۴	۶۸	متوسط
ایتالیا	۶۹	۳۹	۶۵	متوسط رو به بالا

این جدول نشان می‌دهد که امنیت سایبری نقشی حیاتی در اعمال مرزهای دیجیتال دارد. کشورهایی که توان واکنش سریع بالاتری دارند - مانند چین و آمریکا - توانسته‌اند نفوذپذیری مرزهای دیجیتال خود را کاهش دهند.

از مجموعه یافته‌ها چنین برداشت می‌شود که آینده حاکمیت دیجیتال نیازمند «حکمرانی ترکیبی» است؛ یعنی ترکیبی از کنترل ملی، همکاری منطقه‌ای و تنظیم‌گری جهانی. همچنین پژوهش نشان داد که کشورها برای حفظ حاکمیت دیجیتال ناچارند در چهار حوزه اصلی سرمایه‌گذاری کنند: زیرساخت‌های بومی داده، امنیت سایبری، سواد داده شهروندان، و توسعه پلتفرم‌های داخلی. نتایج نهایی همچنین نشان داد که کشورها برای کنترل مرزهای دیجیتال، باید به جای تمرکز صرف بر کنترل جریان داده، به سمت توسعه قدرت چانه‌زنی دیجیتال، تقویت توان فناوریانه، و مشارکت مؤثر در توافقات جهانی حرکت کنند. تحلیل داده‌های این پژوهش نشان داد که هیچ کشوری به تنهایی قادر به مدیریت کامل جریان‌های فراملی داده نیست و تنها راه مؤثر، مشارکت فعال در تنظیم‌گری جهانی و ایجاد ائتلاف‌های داده است.

بحث و نتیجه‌گیری

در جهان معاصر که داده به یکی از ارزشمندترین سرمایه‌های راهبردی تبدیل شده است، مرزهای دیجیتال به‌عنوان یکی از اصلی‌ترین میدان‌های کشمکش میان دولت‌ها، شرکت‌های فراملی و کاربران پدیدار شده‌اند. آنچه در این پژوهش بررسی شد نشان می‌دهد که جریان فراملی داده‌ها نه تنها ساختارهای اقتصادی و ارتباطی کشورها را متحول کرده، بلکه بنیان مفهومی حاکمیت را نیز با چالش‌های عمیق مواجه ساخته است. در چنین شرایطی، نتیجه‌گیری درباره نسبت میان مرزهای دیجیتال و حاکمیت دولت‌ها مستلزم نگاهی چندلایه، انعطاف‌پذیر و میان‌رشته‌ای است؛ نگاهی که بتواند این پدیده را هم‌زمان از منظر فناوری، حقوق، سیاست و امنیت تحلیل کند.

در گام نخست باید اذعان داشت که داده به‌عنوان عنصر بنیادین زیست دیجیتال بشر، از ویژگی‌هایی برخوردار است که آن را از سایر منابع و دارایی‌های تاریخی بشر متمایز می‌کند. داده محدود به قلمرو جغرافیایی نیست، قابلیت تکثیر سریع دارد، در لحظه از مرزها عبور می‌کند و می‌تواند از نظر اقتصادی، امنیتی، فرهنگی و سیاسی پیامدهای گسترده‌ای ایجاد کند. همین ویژگی‌ها سبب شده است که دولت‌ها با پدیده‌ای مواجه شوند که با منطق سنتی حاکمیت قابل کنترل کامل نیست. در گذشته، اعمال حاکمیت بر اساس کنترل قلمروی فیزیکی، جمعیت و منابع انجام می‌شد؛ اما در عصر دیجیتال، «قلمرو» دیگر مفهومی ثابت و قابل مشاهده نیست، بلکه در شبکه‌های جهانی، کابل‌های زیردریایی، مراکز پردازش داده و الگوریتم‌هایی نهفته است که اغلب در کنترل شرکت‌های خصوصی

و بازیگران فراملی قرار دارند. به همین دلیل است که تلاش دولت‌ها برای حفظ یا بازسازی مرزهای دیجیتال، به یکی از پیچیده‌ترین حوزه‌های سیاست‌گذاری معاصر تبدیل شده است.

با این حال، آنچه از بررسی دیدگاه‌ها و سیاست‌های مختلف برمی‌آید، این است که دولت‌ها نمی‌توانند صرفاً با ابزارهای سنتی مانند وضع مقررات محدودکننده یا ایجاد دیوارهای دیجیتال به مواجهه با این چالش بپردازند. هرچند برخی کشورها تلاش کرده‌اند با سیاست‌هایی مانند الزام به ذخیره‌سازی داخلی داده‌ها، فیلترینگ سراسری، یا کنترل شدید زیرساخت‌های دیجیتال، نوعی مرز دیجیتال متحد و پایدار ایجاد کنند، اما این رویکردها نه تنها هزینه‌های اقتصادی و فناورانه بالایی به همراه داشته، بلکه اغلب موجب کاهش نوآوری، تضعیف آزادی‌های دیجیتال و انزوای فناوری شده است. افزون بر این، چنین اقداماتی قادر نیستند چالش‌های فراملی داده را به طور کامل حل کنند، زیرا منشأ و مسیر گردش داده‌ها در جهان امروز تحت کنترل دولت واحدی نیست و حتی اقدامات سخت‌گیرانه نیز نهایتاً تأثیر محدود و نسبی دارند.

از سوی دیگر، برخی کشورها تلاش کرده‌اند با رویکردی مشارکتی‌تر و مبتنی بر تنظیم‌گری هوشمند، تعادلی میان امنیت، اقتصاد و حقوق شهروندی برقرار کنند. این شیوه بر این اصل استوار است که حاکمیت در عصر دیجیتال نه تنها به معنای کنترل، بلکه به معنای توانایی مدیریت، هدایت و بهره‌برداری مؤثر از داده‌هاست. این کشورها معمولاً به جای محدودسازی جریان داده‌ها، بر چارچوب‌های حفاظت از داده، مسئولیت‌پذیری پلتفرم‌ها، شفافیت الگوریتم‌ها و توافق‌های فراملی برای تنظیم‌گری جهانی تکیه می‌کنند. این رویکرد به‌ویژه در اتحادیه اروپا با نمونه‌هایی مانند مقررات عمومی حفاظت از داده‌ها و قوانین خدمات دیجیتال دیده می‌شود. این سیاست‌ها نشان می‌دهد که دولت‌ها می‌توانند بدون انسداد کامل مرزهای دیجیتال، همچنان نقش تعیین‌کننده‌ای در شکل‌دهی به قواعد بازی ایفا کنند.

اما باید تأکید کرد که مسئله مرزهای دیجیتال صرفاً یک موضوع حقوقی یا فناورانه نیست؛ بلکه عمیقاً سیاسی، ژئوپلیتیکی و اجتماعی است. داده‌ها به سلاحی راهبردی در رقابت میان قدرت‌های جهانی تبدیل شده‌اند و کشورهایی که کنترل بیشتری بر زیرساخت‌های دیجیتال دارند، نفوذ بیشتری بر نظام بین‌الملل پیدا می‌کنند. در این میان، کشورهایی که فاقد توانایی تولید فناوری‌های پایه، شبکه‌های مستقل یا پلتفرم‌های رقابتی هستند، بیش از دیگران در معرض آسیب‌پذیری دیجیتال قرار می‌گیرند. از همین‌جا می‌توان نتیجه گرفت که شکاف دیجیتال امروز نه تنها یک شکاف فناورانه، بلکه شکافی حاکمیتی، اقتصادی و امنیتی است که می‌تواند بر قدرت و استقلال کشورها تأثیر مستقیم بگذارد.

نتایج این پژوهش نشان می‌دهد که آینده حاکمیت دیجیتال در گرو اتخاذ رویکردی چندلایه است؛ رویکردی که سه سطح اصلی را دربرمی‌گیرد: سطح ملی، سطح منطقه‌ای و سطح بین‌المللی. در سطح ملی، دولت‌ها باید زیرساخت‌های بومی داده، قوانین جامع و پیوسته، و نظام‌های نظارتی مؤثر ایجاد کنند تا بتوانند از منافع اقتصادی داده بهره گیرند و از تهدیدهای آن جلوگیری کنند. در سطح منطقه‌ای، همکاری میان کشورها ضروری است؛ زیرا مسائل مرتبط با داده، امنیت سایبری و تنظیم‌گری پلتفرم‌ها معمولاً فراتر از توان یک کشور بوده و نیازمند استانداردها و چارچوب‌های مشترک هستند. در سطح بین‌المللی نیز باید به سمت شکل‌دهی توافق‌های جهانی حرکت کرد؛ زیرا در نبود استانداردهای مشترک، جهان به سوی تجزیه دیجیتال و شکل‌گیری بلوک‌های اینترنتی ناسازگار پیش می‌رود.

همچنین این پژوهش تأکید می‌کند که یکی از مهم‌ترین مؤلفه‌های حفظ حاکمیت دیجیتال، ارتقای سواد داده در جامعه، آموزش شهروندان و تقویت مشارکت بخش خصوصی و دانشگاهی است. دولت‌ها نمی‌توانند به‌تنهایی در برابر چالش‌های فراملی داده بایستند؛ زیرا اقتصاد داده بر مشارکت گسترده کسب‌وکارها، پژوهشگران، فعالان جامعه مدنی و متخصصان فناوری استوار است. به همین دلیل، سطح بالای آگاهی عمومی و حرفه‌ای نسبت به حقوق دیجیتال، امنیت سایبری و ارزش داده‌ها، یکی از ابزارهای اصلی در حفظ استقلال دیجیتال کشورها محسوب می‌شود.

در مجموع، نتیجه این پژوهش آن است که مرزهای دیجیتال نه تنها مفهوم حاکمیت دولت‌ها را دگرگون کرده‌اند، بلکه دولت‌ها را واداشته‌اند نوعی بازتعریف بنیادین در شیوه اعمال قدرت، مدیریت منابع و تنظیم‌گری اجتماعی انجام دهند. در جهانی که داده‌ها از هر مرزی عبور می‌کنند و فناوری هر روز تحول می‌یابد، دولت‌ها دیگر نمی‌توانند بر منطق مرزهای ثابت و کنترل‌های سنتی تکیه کنند. در مقابل، باید به‌سوی حاکمیتی منعطف، چندسطحی، مشارکتی و مبتنی بر فهم عمیق از سازوکارهای فناوری حرکت کنند. این امر نه تنها برای حفظ امنیت و استقلال سیاسی کشورها ضروری است، بلکه برای بهره‌برداری از فرصت‌های اقتصادی، حمایت از حقوق شهروندی، و دستیابی به توسعه پایدار دیجیتال نیز اهمیت اساسی دارد. از این رو، آینده حاکمیت در عصر داده‌های فراملی در گرو پذیرش این واقعیت است که مرزهای دیجیتال نه قابل حذف‌اند و نه قابل کنترل کامل؛ بلکه باید آن‌ها را به‌گونه‌ای مدیریت کرد که بتوان از قدرت داده‌ها برای ایجاد جامعه‌ای امن‌تر، آزادتر و توانمندتر استفاده کرد.

منابع

- ۱- بخت آزمای، محمد؛ شادمان آذر، مریم؛ سالک مراد، بهار. (۱۴۰۲). «اقتصاد سیاسی و کارکردهای آن در ایران». کنفرانس ملی تحولات نوین در مطالعات مالی، اقتصادی و حسابداری.
- ۲- پور منافعی، رضا. (۱۳۹۷). «اولویت‌بندی تهدیدهای امنیت پایدار در مرزهای جمهوری اسلامی ایران». مجله مطالعات دفاعی و امنیتی.
- ۳- توکلی راد، رضا و سادات میری، حوریه. (۱۴۰۰). «تحول‌گرایی حکمرانی: از دولت الکترونیک تا حکمرانی دیجیتال». فصلنامه علمی حکمرانی متعالی، ۲(۳)، ۱۱۵-۱۶۲.
- ۴- شفیعی، محمدرضا و جلالی، حمید. (۱۴۰۳). «چالش‌های امنیت سایبری در ایران: نگاه فرامرزی». مطالعات امنیت اطلاعات.
- ۵- صحرایی، فرامرز. (۱۴۰۴). «تحلیلی بر کیفیت داده در دولت الکترونیک و تأثیر آن بر حکمرانی داده در ایران». فصلنامه دولت پژوهی، ۱۱(۴۱)، ۱۳۳-۱۸۶.
- ۶- فرامرز صحرایی، فرامرز. (۱۴۰۴). «تحلیلی بر کیفیت داده در دولت الکترونیک و تأثیر آن بر حکمرانی داده در ایران». دولت پژوهی، ۱۱(۴۱)، ۱۳۳-۱۸۶.
- ۷- محمودی پرچینی، محمود. (۱۴۰۵). «مدل پیشنهادی برای استقرار حکمرانی داده‌ها با تأکید بر حریم خصوصی و امنیت داده». پژوهش‌های سیاست فناوری اطلاعات، ۳(۱)، ۳۴-۱۰.
- ۸- مرکز شبکه علمی ایران (۱۴۰۴). «مدیریت حاکمیت داده‌ها در دوران تجارت دیجیتال». شبکه علمی ایران - ISNAC.
- ۹- Cory, N. & Dascoli, L. (۲۰۲۱). How Barriers to Cross-Border Data Flows Are Spreading Globally: What They Cost. Information Technology & Innovation Foundation.
- ۱۰- Hare, F. (۲۰۱۸). Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security? CCDCOE Publications.

- ۱۱- Kaya .M. & Shahid .H. (۲۰۲۰). Cross-Border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance. *Interdisciplinary Studies in Society, Law, and Politics*, ۴(۲), ۲۱۹-۲۳۳.
- ۱۲- Liu J. (۲۰۲۰). Ruling the Data Flows: Data Cognition in Global Cross-Border Data Flows Governance. *Politics and Governance*, ۱۳, ۱۰۴۶۰.