Submit Date: 27 July 2026
Revise Date: 30 October 2026
Accept Date: 07 November 2026
Initial Publish: 08 November 2026
Final Publish: 20 February 2027

The Encyclopedia of Comparative Jurisprudence and Law

© 2026 the authors. This is an open access article under the terms of the Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

The Transformation of the Concept of Territorial Sovereignty in Light of the Emergence of Virtual Territories: Assessing the Possibility of Recognizing Digital Sovereignty as an Independent Rule of Customary International Law

Hoseinali Enayat Mehri[1]*

1. Assistant Professor, Department of Law, University of Zabol, Zabol, Iran

* Corresponding Author's Email: enayatuoz@gmail.com

ABSTRACT

The rapid development of digital technologies and the expansion of cyberspace have fundamentally challenged the classical model of territorial sovereignty, which is traditionally based on the relationship among state authority, geographical territory, and legal jurisdiction. The emergence of virtual territories, cross-border data flows, cloud infrastructures, transnational platforms, and artificial intelligence systems has made the exercise of state authority increasingly detached from purely physical boundaries. Using a descriptive-analytical approach, this study examines the transformation of territorial sovereignty in the digital environment and evaluates whether digital sovereignty can be recognized as an independent rule of customary international law. The study first clarifies the relationship among territorial sovereignty, cyberspace, virtual territory, and data sovereignty, and then analyzes the evolution of jurisdiction, data control, platform regulation, and the protection of critical digital infrastructure. The findings indicate that states increasingly regard the digital sphere as part of their sovereign interests and seek to consolidate authority over it through legislation, regulation, and the development of national digital infrastructures. However, widespread state practice alone is insufficient to establish a customary rule, as the existence of a corresponding and sufficiently consistent legal conviction is also required. The current international legal landscape reveals continuing disagreement over the meaning, scope, and legal consequences of digital sovereignty. Accordingly, the study concludes that digital sovereignty has not yet crystallized into a fully established independent rule of customary international law. Rather, it is more accurately characterized as an emerging normative concept that may develop into an autonomous customary rule if future state practice and legal conviction become more coherent, consistent, and legally explicit.

Keywords: *Territorial Sovereignty, Digital Sovereignty, Virtual Territory, Cyberspace, Data Sovereignty, Customary International Law.*

How to cite: Enayat Mehri, H. (2026). The Transformation of the Concept of Territorial Sovereignty in Light of the Emergence of Virtual Territories: Assessing the Possibility of Recognizing Digital Sovereignty as an Independent Rule of Customary International Law. *The Encyclopedia of Comparative Jurisprudence and Law*, *4*(6), 1-20.

تاریخ ارسال: ۵ مرداد ۱۴۰۵
تاریخ بازنگری: ۸ آبان ۱۴۰۵
تاریخ پذیرش: ۱۶ آبان ۱۴۰۵
تاریخ چاپ اولیه: ۱۷ آبان ۱۴۰۵
تاریخ چاپ نهایی: ۱ اسفند ۱۴۰۵

دانشنامه فقه و حقوق تطبیقی

تحول مفهوم حاکمیت سرزمینی در پرتو شکل‌گیری قلمروهای مجازی: امکان‌سنجی شناسایی حاکمیت دیجیتال به‌عنوان قاعده مستقل حقوق بین‌الملل عرفی

حسینعلی عنایت مهری[1*]

۱. استادیار، گروه حقوق، دانشگاه ملی زابل، زابل، ایران
* پست الکترونیک نویسنده مسئول: enayatuoz@gmail.com

چکیده

تحولات شتابان فناوری‌های دیجیتال و گسترش فضای سایبری، الگوی کلاسیک حاکمیت سرزمینی را که بر پیوند میان دولت، قلمرو جغرافیایی و صلاحیت حقوقی استوار است، با چالش‌های اساسی مواجه ساخته است. ظهور قلمروهای مجازی، جریان فرامرزی داده‌ها، توسعه زیرساخت‌های ابری، پلتفرم‌های فراملی و سامانه‌های هوش مصنوعی موجب شده است که اعمال اقتدار دولت‌ها دیگر صرفاً به مرزهای فیزیکی محدود نباشد. پژوهش حاضر با رویکرد توصیفی ـ تحلیلی در پی بررسی تحول مفهوم حاکمیت سرزمینی در بستر فضای دیجیتال و امکان شناسایی حاکمیت دیجیتال به‌عنوان قاعده‌ای مستقل در حقوق بین‌الملل عرفی است. در این راستا، ابتدا نسبت میان حاکمیت سرزمینی، فضای سایبری، قلمرو مجازی و حاکمیت داده تبیین می‌شود و سپس تحول الگوهای صلاحیت، کنترل بر داده، تنظیم پلتفرم‌ها و حمایت از زیرساخت‌های حیاتی دیجیتال مورد بررسی قرار می‌گیرد. یافته‌های پژوهش نشان می‌دهد که دولت‌ها به‌طور فزاینده‌ای حوزه دیجیتال را بخشی از منافع حاکمیتی خود تلقی کرده و از طریق قانون‌گذاری، تنظیم‌گری و توسعه زیرساخت‌های ملی درصدد تثبیت اقتدار خود در این حوزه هستند. بااین‌حال، وجود رویه گسترده دولتی به‌تنهایی برای شکل‌گیری قاعده عرفی کافی نیست و اثبات اعتقاد حقوقی مشترک دولت‌ها نیز ضروری است. بررسی وضعیت موجود نشان می‌دهد که هنوز در خصوص ماهیت، حدود و آثار حقوقی حاکمیت دیجیتال اجماع کافی وجود ندارد. بر این اساس، نتیجه‌گیری پژوهش آن است که حاکمیت دیجیتال در وضعیت کنونی بیش از آنکه قاعده‌ای عرفی کاملاً تثبیت‌شده باشد، هنجاری در حال تکوین است که امکان تبدیل‌شدن به قاعده مستقل حقوق بین‌الملل عرفی را دارد، مشروط بر آنکه رویه دولت‌ها و اعتقاد حقوقی آنان در آینده از انسجام و وضوح بیشتری برخوردار شود.

کلیدواژگان: *حاکمیت سرزمینی، حاکمیت دیجیتال، قلمرو مجازی، فضای سایبری، حاکمیت داده، حقوق بین‌الملل عرفی.*

نحوه استناددهی: عنایت مهری، حسینعلی. (۱۴۰۵). تحول مفهوم حاکمیت سرزمینی در پرتو شکل‌گیری قلمروهای مجازی: امکان‌سنجی شناسایی حاکمیت دیجیتال به‌عنوان قاعده مستقل حقوق بین‌الملل عرفی. *دانشنامه فقه و حقوق تطبیقی*، ۴(۶)، ۲۰-۱.

© ۱۴۰۵ تمامی حقوق انتشار این مقاله متعلق به نویسنده است. انتشار این مقاله به‌صورت دسترسی آزاد مطابق با گواهی (CC BY-NC 4.0) صورت گرفته است.

مقدمه

حاکمیت از بنیادی‌ترین مفاهیم حقوق بین‌الملل عمومی و یکی از عناصر تعیین‌کننده در تعریف جایگاه دولت در نظام بین‌المللی است. ساختار کلاسیک حقوق بین‌الملل بر این فرض استوار بوده است که دولت در محدوده سرزمین خود از اقتدار عالی برخوردار است و هیچ قدرت خارجی نمی‌تواند بدون رضایت او در حوزه صلاحیت سرزمینی‌اش مداخله کند. بر این اساس، رابطه میان دولت، سرزمین و اقتدار سیاسی به‌صورت سنتی رابطه‌ای مستقیم و تقریباً جدایی‌ناپذیر تلقی شده است. مفهوم حاکمیت سرزمینی در طول تاریخ حقوق بین‌الملل نه‌تنها ابزار شناسایی حدود صلاحیت دولت‌ها بوده، بلکه به‌عنوان یکی از مبانی نظم بین‌المللی، مرز میان اقتدار داخلی و مداخله خارجی را نیز مشخص کرده است. Fitzpatrick در تحلیل رابطه میان حاکمیت، سرزمین و حاکمیت قانون نشان می‌دهد که سرزمینی‌بودن در ساختار حقوقی دولت مدرن صرفاً یک ویژگی جغرافیایی نیست، بلکه سازوکاری برای سازمان‌دهی اقتدار قانونی و تعیین حدود صلاحیت محسوب می‌شود (Fitzpatrick, 2001). همین پیوند دیرینه میان حاکمیت و قلمرو فیزیکی سبب شده است که بخش مهمی از قواعد حقوق بین‌الملل بر فرض وجود مرزهای جغرافیایی نسبتاً مشخص میان دولت‌ها شکل گیرد.

بااین‌حال، توسعه سریع فناوری‌های اطلاعاتی و ارتباطی، ظهور اینترنت جهانی، گسترش زیرساخت‌های ابری، شکل‌گیری شبکه‌های اجتماعی فرامرزی، افزایش حجم داده‌های دیجیتال و توسعه سامانه‌های هوش مصنوعی، مفروضات سنتی درباره رابطه میان قدرت و قلمرو را با چالش مواجه ساخته است. فضای سایبری نه همانند قلمرو زمینی دارای خطوط مرزی محسوس است و نه می‌توان تمامی فعالیت‌های صورت‌گرفته در آن را به‌سادگی به یک موقعیت جغرافیایی مشخص نسبت داد. Dewan فضای سایبری را محیطی غیرسرزمینی و مجازی توصیف می‌کند که در آن، الگوهای سنتی اعمال حاکمیت دولت‌ها با دشواری‌های بنیادین مواجه می‌شوند (Dewan, 2023). در چنین فضایی، ممکن است کاربر در یک دولت قرار داشته باشد، سرور در دولت دیگری مستقر باشد، شرکت ارائه‌دهنده خدمات در کشور سومی ثبت شده باشد و داده‌ها نیز به‌صورت هم‌زمان در چند مرکز داده در نقاط مختلف جهان پردازش شوند. ازاین‌رو، تعیین اینکه کدام دولت از صلاحیت اصلی برخوردار است و چه نوع پیوندی میان داده، زیرساخت دیجیتال و حاکمیت سرزمینی وجود دارد، به یکی از مسائل پیچیده حقوق بین‌الملل معاصر تبدیل شده است.

تحول یادشده محدود به توسعه فناوری نیست، بلکه ساختار قدرت در نظام بین‌المللی را نیز دگرگون ساخته است. در جهان معاصر، داده و توانایی کنترل جریان اطلاعات می‌تواند همان اندازه اهمیت راهبردی داشته باشد که کنترل بر منابع طبیعی، خطوط ارتباطی، بنادر یا قلمروهای جغرافیایی داشته است. دولت‌ها به‌طور فزاینده‌ای در تلاش‌اند کنترل حقوقی و عملی خود را بر داده‌های تولیدشده در قلمرو یا توسط اتباع خود افزایش دهند. Kazemnejad و Tavakkolifar نشان می‌دهند که مفهوم حاکمیت داده به یکی از موضوعات اصلی حقوق سایبری تبدیل شده و پرسش از مالکیت و کنترل بر داده، به‌ویژه داده‌های تولیدشده از طریق فناوری‌های هوش مصنوعی، ابعاد جدیدی از اقتدار حاکمیتی را آشکار کرده است (Kazemnejad & Tavakkolifar, 2024). از این منظر، حاکمیت دیگر صرفاً به اعمال قدرت بر زمین، آب‌های سرزمینی و فضای هوایی محدود نیست، بلکه توانایی دولت برای تنظیم، حفاظت و کنترل داده‌ها و زیرساخت‌های دیجیتال نیز می‌تواند بخشی از مفهوم نوین اقتدار حاکمیتی تلقی شود.

هم‌زمان، توسعه فناوری موجب گسترش صلاحیت دولت‌ها به حوزه‌هایی شده است که مرز جغرافیایی روشنی ندارند. در حوزه حقوق کیفری، مسئله تعیین صلاحیت در جرایم سایبری نمونه

برجسته‌ای از این تحول است. Fazaeli توضیح می‌دهد که فضای سایبری موجب گذار تدریجی از اتکای مطلق به اصل سرزمینی‌بودن صلاحیت به الگوهایی شده است که در آنها حاکمیت داده و پیوندهای فرامرزی نقش فزاینده‌ای پیدا می‌کنند (Fazaeli, 2021). دسترسی دولت به داده‌هایی که در سرورهای واقع در قلمرو دولت دیگر نگهداری می‌شوند نیز می‌تواند تعارضی مستقیم میان ضرورت اجرای قانون و اصل احترام به حاکمیت سرزمینی دولت خارجی ایجاد کند. Salehi در بررسی دسترسی به اطلاعات مراکز داده متعلق به دولت خارجی، این اقدام را در ارتباط با اصول صلاحیت کیفری سرزمینی و حاکمیت در حقوق بین‌الملل تحلیل کرده و نشان داده است که فناوری‌های دیجیتال توانسته‌اند مرز میان اجرای صلاحیت داخلی و ورود به حوزه حاکمیتی دولت دیگر را مبهم سازند (Salehi, 2019).

این تحولات موجب شده است که مفاهیمی مانند «حاکمیت سایبری»، «حاکمیت داده»، «حاکمیت اینترنتی»، «حاکمیت فناوری» و «حاکمیت دیجیتال» وارد ادبیات حقوقی و سیاسی شوند. هرچند این مفاهیم گاه به‌صورت مترادف به کار می‌روند، اما دامنه آنها یکسان نیست. حاکمیت سایبری بیشتر به اعمال اقتدار دولت در فضای سایبری و کنترل یا حمایت از زیرساخت‌های شبکه‌ای مربوط می‌شود، درحالی‌که حاکمیت دیجیتال مفهومی گسترده‌تر است که می‌تواند داده، زیرساخت، فناوری، پلتفرم، هویت دیجیتال، خدمات ابری و حتی الگوریتم‌ها را دربر گیرد. Haber و Topor در بررسی ظهور «حباب‌های اینترنتی» نشان می‌دهند که دولت‌ها به‌طور فزاینده‌ای می‌کوشند بخشی از فضای اینترنت را در چارچوب اقتدار و نظم حقوقی ملی خود قرار دهند و این روند می‌تواند به شکل‌گیری حوزه‌های دیجیتال نسبتاً متمایز منجر شود (Haber & Topor, 2023). چنین روندی از یک سو با منطق جهانی و باز اینترنت در تعارض است و از سوی دیگر بیانگر تلاش دولت‌ها برای بازتولید اقتدار سرزمینی خود در محیطی است که ذاتاً فرامرزی طراحی شده است.

در سطح نظری، پرسش مهم آن است که آیا قلمرو مجازی را می‌توان به‌عنوان امتداد قلمرو فیزیکی تصور کرد یا اینکه با نوع متفاوتی از فضای حقوقی مواجه هستیم. مفهوم «قلمرو مجازی» در این مقاله ناظر بر مجموعه‌ای از منابع، داده‌ها، زیرساخت‌ها و روابط دیجیتالی است که دولت نسبت به آنها ادعای صلاحیت، کنترل یا حمایت حاکمیتی دارد، حتی اگر همه عناصر مادی این مجموعه در محدوده جغرافیایی آن دولت قرار نداشته باشند. این مفهوم الزاماً به معنای ایجاد قلمرویی هم‌سنگ قلمرو سرزمینی نیست، بلکه تلاشی نظری برای توضیح تغییر در ماهیت پیوند میان دولت و حوزه‌ای است که قدرت عمومی در آن اعمال می‌شود. Zhuk در بررسی مفهوم حاکمیت مجازی و وضعیت حقوقی واحدهای خودخوانده در فضای سایبری نشان می‌دهد که محیط دیجیتال حتی ظرفیت تولید ادعاهای جدید درباره قلمرو، اقتدار و شخصیت سیاسی را نیز ایجاد کرده است (Zhuk, 2023). هرچند چنین نمونه‌هایی الزاماً به معنای پذیرش حقوقی قلمرو دیجیتال نیستند، اما نشان می‌دهند که فناوری قادر است برداشت‌های کلاسیک از قلمرو و اقتدار را وارد مرحله‌ای جدید کند.

در این میان، مسئله اصلی از منظر حقوق بین‌الملل آن است که آیا تحولات مزبور صرفاً نحوه اعمال قواعد موجود را تغییر داده‌اند یا اینکه زمینه پیدایش یک قاعده جدید و مستقل را فراهم کرده‌اند. حقوق بین‌الملل عرفی بر پایه ترکیب رویه عمومی دولت‌ها و اعتقاد حقوقی شکل می‌گیرد. بنابراین، صرف افزایش استفاده دولت‌ها از تعبیر حاکمیت دیجیتال یا گسترش قوانین ملی در زمینه داده نمی‌تواند به‌تنهایی اثبات‌کننده وجود یک قاعده عرفی مستقل باشد. باید بررسی شود که آیا رفتار دولت‌ها از چنان گستردگی، انسجام و تداومی برخوردار است که بتوان آن را به‌عنوان رویه عمومی شناسایی کرد و مهم‌تر از آن، آیا دولت‌ها این رفتار را ناشی

از یک الزام یا حق حقوقی بین‌المللی می‌دانند. Sloan در بحث مسئولیت سایبری و حاکمیت نشان می‌دهد که یکی از مناقشات اصلی در حقوق بین‌الملل معاصر آن است که آیا حاکمیت در فضای سایبری خود یک قاعده مستقل است که نقض آن مسئولیت بین‌المللی ایجاد می‌کند یا اینکه صرفاً اصلی زیربنایی برای سایر قواعد محسوب می‌شود (Sloan, 2023).

تفاوت رویکرد دولت‌ها نیز اهمیت این مسئله را افزایش می‌دهد. برخی دولت‌ها بر ضرورت اعمال کامل حاکمیت در فضای سایبری تأکید می‌کنند، درحالی‌که برخی دیگر از تعبیرهایی استفاده می‌کنند که بیش از آنکه بر مرزبندی دیجیتال تأکید داشته باشد، بر آزادی جریان اطلاعات و کاربرد قواعد موجود حقوق بین‌الملل تمرکز دارد. مطالعه تطبیقی صورت‌گرفته درباره ایران و اندونزی نشان داده است که برداشت دولت‌ها از حاکمیت سایبری می‌تواند به‌شدت تحت تأثیر ساختار سیاسی، امنیتی و حقوقی داخلی آنها قرار گیرد (Lidia Tri Chris Nia et al., 2023). ازاین‌رو، حتی در صورت مشاهده افزایش سیاست‌های ملی در زمینه کنترل اینترنت یا داده، نمی‌توان فوراً نتیجه گرفت که یک opinio juris واحد در سطح بین‌المللی شکل گرفته است.

هدف این پژوهش تحلیل تحول مفهوم حاکمیت سرزمینی در پرتو شکل‌گیری قلمروهای مجازی و ارزیابی امکان شناسایی حاکمیت دیجیتال به‌عنوان یک قاعده مستقل حقوق بین‌الملل عرفی است. پرسش اصلی پژوهش آن است که آیا افزایش رویه دولت‌ها در زمینه کنترل داده‌ها، تنظیم زیرساخت‌های دیجیتال، اعمال صلاحیت نسبت به فعالیت‌های آنلاین و حفاظت از فضای سایبری توانسته است عناصر لازم برای پیدایش یک قاعده عرفی مستقل را فراهم کند یا اینکه حاکمیت دیجیتال همچنان باید در قالب امتداد قواعد کلاسیک حاکمیت سرزمینی تفسیر شود. فرض اصلی پژوهش آن است که حقوق بین‌الملل در حال تجربه مرحله‌ای انتقالی است که در آن مفهوم حاکمیت دیجیتال از سطح یک مفهوم سیاستی فراتر رفته و به سوی تبدیل‌شدن به یک هنجار حقوقی در حال حرکت است، اما هنوز وحدت و انسجام کافی در اعتقاد حقوقی دولت‌ها برای شناسایی آن به‌عنوان یک قاعده کاملاً تثبیت‌شده عرفی وجود ندارد. روش پژوهش توصیفی ـ تحلیلی است و با تمرکز بر ادبیات حقوقی، رویکرد دولت‌ها، مفهوم عرف بین‌المللی و تحول قواعد صلاحیت، تلاش می‌شود نسبت میان سرزمین، فضای مجازی و اقتدار حاکمیتی بازتعریف شود.

مبانی مفهومی و حقوقی حاکمیت سرزمینی و قلمروهای مجازی

مفهوم حاکمیت در حقوق بین‌الملل کلاسیک بر ایده استقلال سیاسی و اقتدار عالی دولت در قلمرو خود استوار است. حاکمیت از یک سو دارای بعد داخلی است و بیانگر برتری قدرت عمومی دولت در برابر اشخاص و نهادهای واقع در قلمرو آن محسوب می‌شود و از سوی دیگر دارای بعد خارجی است که استقلال دولت در برابر سایر دولت‌ها را تضمین می‌کند. در این چارچوب، سرزمین نه‌تنها محدوده جغرافیایی دولت، بلکه بستر حقوقی اعمال حاکمیت است. Fitzpatrick رابطه میان حاکمیت و سرزمینی‌بودن را در بستر حکومت قانون تحلیل کرده و نشان داده است که مفهوم قلمرو به تنظیم توزیع قدرت، تعیین مرز صلاحیت و ایجاد قابلیت پیش‌بینی در روابط بین‌المللی کمک می‌کند (Fitzpatrick, 2001). به همین دلیل، حقوق بین‌الملل سنتی میان وجود دولت، قلمرو مشخص و امکان اعمال اقتدار حقوقی رابطه‌ای نزدیک برقرار کرده است.

اصل سرزمینی‌بودن صلاحیت نیز یکی از نتایج همین پیوند است. بر پایه این اصل، هر دولت نسبت به وقایع، اشخاص و اموالی که در محدوده سرزمینی او قرار دارند از صلاحیت اولیه برخوردار است. بااین‌حال، حقوق بین‌الملل همواره اشکال دیگری از صلاحیت را نیز پذیرفته است؛ ازجمله صلاحیت مبتنی بر تابعیت، صلاحیت حمایتی و در برخی موارد صلاحیت جهانی. ظهور فضای سایبری سبب شده است که مرز میان این مبانی بیش از

گذشته با یکدیگر تداخل پیدا کند. Fazaeli نشان می‌دهد که فضای سایبری به دلیل ماهیت غیرمتمرکز خود، اصل سرزمینی‌بودن را با محدودیت مواجه کرده و موجب شده است که داده به‌عنوان مبنایی جدید برای پیوند میان دولت و موضوع صلاحیت مطرح شود (Fazaeli, 2021). این تحول به این معنا نیست که اصل سرزمینی‌بودن از بین رفته است، بلکه نشان می‌دهد که کارکرد آن در محیط دیجیتال نیازمند بازتفسیر است.

فضای سایبری را نمی‌توان صرفاً به‌عنوان مجموعه‌ای انتزاعی از اطلاعات تصور کرد. این فضا دارای لایه‌های مادی و غیرمادی است. کابل‌های زیردریایی، مراکز داده، سرورها، تجهیزات مخابراتی و رایانه‌ها در قلمرو فیزیکی دولت‌ها قرار دارند و بنابراین تابع قواعد سنتی صلاحیت سرزمینی‌اند. در مقابل، لایه منطقی شبکه، جریان داده و تعاملات دیجیتال ممکن است در یک لحظه از چندین حوزه قضایی عبور کند. Dewan بر همین ویژگی دوگانه فضای سایبری تأکید می‌کند و آن را محیطی می‌داند که از یک سو بر زیرساخت‌های سرزمینی تکیه دارد و از سوی دیگر از منطق غیرسرزمینی و شبکه‌ای برخوردار است (Dewan, 2023). این دوگانگی یکی از دلایل اصلی دشواری در تعیین حدود حاکمیت دولت‌ها در فضای سایبری است.

مفهوم قلمرو مجازی در چنین شرایطی اهمیت پیدا می‌کند. اگر قلمرو در معنای کلاسیک به محدوده‌ای اطلاق شود که دولت در آن از اقتدار انحصاری برخوردار است، قلمرو مجازی را می‌توان حوزه‌ای دانست که دولت در آن ادعای اقتدار حقوقی، تنظیمی یا حفاظتی نسبت به داده‌ها، زیرساخت‌ها و فعالیت‌های دیجیتال مطرح می‌کند. البته این قلمرو فاقد مرز هندسی پایدار است و ممکن است مرزهای آن بر اساس تابعیت کاربران، محل استقرار زیرساخت، منشأ داده یا آثار فعالیت دیجیتال تعیین شود. Zhuk نشان داده است که مفهوم فضای مجازی حتی می‌تواند به مبنایی برای شکل‌گیری ادعاهای نمادین درباره حاکمیت و سازمان سیاسی تبدیل شود (Zhuk, 2023). اگرچه این ادعاها لزوماً از سوی جامعه بین‌المللی به رسمیت شناخته نمی‌شوند، اما اهمیت نظری آنها در این است که نشان می‌دهند محیط دیجیتال ظرفیت ایجاد اشکال جدیدی از تعلق فضایی و اقتدار را دارد.

یکی از مهم‌ترین مؤلفه‌های قلمرو مجازی، داده است. داده در اقتصاد و سیاست معاصر تنها یک محصول جانبی فعالیت‌های انسانی نیست، بلکه به منبعی راهبردی تبدیل شده است که دولت‌ها، شرکت‌ها و بازیگران غیردولتی برای کنترل آن رقابت می‌کنند. Kazemnejad و Tavakkolifar مفهوم حاکمیت داده را در ارتباط با مالکیت و کنترل اطلاعات تولیدشده از طریق هوش مصنوعی بررسی کرده‌اند و بر پیچیدگی تعیین حق کنترل نسبت به داده‌های دیجیتال تأکید دارند (Kazemnejad & Tavakkolifar, 2024). در این چارچوب، دولت ممکن است ادعا کند که داده‌های شهروندان یا داده‌های ایجادشده در قلمرو او باید تحت قواعد ملی پردازش شوند، حتی اگر آن داده‌ها در سرورهای خارج از کشور ذخیره شده باشند. این وضعیت نشان می‌دهد که منطق جغرافیایی صرف نمی‌تواند تمامی اشکال اقتدار دیجیتال را توضیح دهد.

در حوزه اجرای قانون، همین مسئله به‌صورت ملموس‌تری ظاهر می‌شود. دسترسی مستقیم یک دولت به داده‌های ذخیره‌شده در کشور دیگر ممکن است از منظر دولت درخواست‌کننده صرفاً اقدامی برای اجرای قانون داخلی باشد، اما از نگاه دولت میزبان نوعی ورود به حوزه صلاحیت سرزمینی محسوب شود. Salehi با تحلیل مسئله دسترسی به اطلاعات مرکز داده خارجی نشان می‌دهد که چنین اقداماتی می‌توانند با اصل حاکمیت و قواعد صلاحیت سرزمینی در تعارض قرار گیرند (Salehi, 2019). اهمیت این موضوع زمانی بیشتر می‌شود که داده به‌صورت توزیع‌شده یا در فضای ابری ذخیره شده باشد و حتی ارائه‌دهنده

خدمات نیز نتواند موقعیت دقیق فیزیکی تمام نسخه‌های داده را در یک زمان معین مشخص کند.

از این منظر، تحول مفهوم قلمرو را می‌توان در قالب گذار از «قلمرو صرفاً جغرافیایی» به «قلمرو عملکردی» تحلیل کرد. قلمرو عملکردی به این معناست که صلاحیت و اقتدار دولت نه صرفاً بر اساس محل فیزیکی فعالیت، بلکه بر اساس نوع رابطه میان فعالیت دیجیتال و منافع حاکمیتی دولت تعیین شود. اگر یک سامانه دیجیتال مستقیماً خدمات عمومی یک کشور را اداره کند، ممکن است مداخله خارجی در آن حتی در صورت نبود خسارت فیزیکی، تعرض به اقتدار دولت تلقی شود. Sloan در تحلیل مسئولیت سایبری بر این نکته تأکید می‌کند که بحث حاکمیت در فضای سایبری بیش از آنکه به مالکیت فیزیکی زیرساخت محدود شود، با توانایی دولت در کنترل و اداره کارکردهای حاکمیتی خود پیوند دارد (Sloan, 2023). این رویکرد می‌تواند مبنایی برای توسعه مفهوم قلمرو دیجیتال در آینده باشد.

در عین حال، باید میان «قلمرو مجازی» و «فضای سایبری جهانی» تمایز قائل شد. فضای سایبری به‌صورت کلی محیطی جهانی و به‌هم‌پیوسته است، درحالی‌که قلمرو مجازی مفهومی تحلیلی برای توصیف بخش‌هایی از این محیط است که دولت نسبت به آنها ادعای پیوند حقوقی ویژه دارد. Haber و Topor از شکل‌گیری «حباب‌های اینترنتی» سخن می‌گویند؛ وضعیتی که در آن دولت‌ها با استفاده از ابزارهای حقوقی، فنی و سیاستی، بخش‌هایی از فضای اینترنت را از سایر بخش‌ها متمایز می‌کنند (Haber & Topor, 2023). این روند می‌تواند از طریق فیلترینگ، الزامات ذخیره‌سازی محلی، مقررات مربوط به شرکت‌های فناوری خارجی یا کنترل بر دروازه‌های ارتباطی تحقق یابد. اگر این روند تداوم پیدا کند، اینترنت ممکن است از محیطی کاملاً جهانی به مجموعه‌ای از حوزه‌های دیجیتال نسبتاً متمایز تبدیل شود.

مسئله مهم دیگر آن است که حاکمیت دیجیتال نباید با خودمختاری فناورانه یا استقلال اقتصادی یکسان تلقی شود. حاکمیت دیجیتال از منظر حقوق بین‌الملل زمانی اهمیت پیدا می‌کند که دولت ادعا کند نسبت به یک حوزه دیجیتال، حق اعمال اقتدار دارد و سایر دولت‌ها نیز مکلف به احترام به این حق هستند. ازاین‌رو، تأکید صرف بر توسعه فناوری بومی یا کاهش وابستگی به شرکت‌های خارجی برای ایجاد یک مفهوم حقوقی مستقل کافی نیست. Farao و همکاران در بررسی معماری‌های مبتنی بر بلاک‌چین و هویت خودحاکم نشان می‌دهند که فناوری‌های جدید حتی می‌توانند اشکال غیرمتمرکز کنترل هویت و داده را تقویت کنند (Farao et al., 2024). این تحول از زاویه حقوقی اهمیت زیادی دارد، زیرا ممکن است انحصار دولت بر تنظیم هویت و جریان اطلاعات را نیز به چالش بکشد.

تحول در مفهوم حاکمیت در حوزه‌های دیگر حقوق بین‌الملل نیز نشان داده است که حاکمیت مفهومی ثابت و غیرقابل تغییر نیست. Ebrahimifar و همکاران در زمینه ورشکستگی فرامرزی نشان داده‌اند که الگوی حاکمیت سرزمینی مطلق به‌تدریج جای خود را به شکل‌های تعدیل‌شده‌ای از همکاری و جهان‌شمولی داده است (Ebrahimifar et al., 2024). این تجربه نشان می‌دهد که حقوق بین‌الملل می‌تواند بدون حذف اصل حاکمیت، نحوه اعمال آن را با واقعیت‌های فرامرزی سازگار کند. فضای دیجیتال نیز ممکن است روندی مشابه را طی کند؛ به این معنا که حاکمیت سرزمینی از بین نرود، بلکه به‌گونه‌ای بازتفسیر شود که بتواند فعالیت‌های فاقد محل فیزیکی واحد را نیز پوشش دهد.

در چنین چارچوبی، مفهوم حاکمیت دیجیتال را می‌توان به‌عنوان ظرفیت حقوقی و عملی دولت برای تنظیم، حفاظت و اعمال اقتدار نسبت به داده‌ها، زیرساخت‌های دیجیتال، سامانه‌های اطلاعاتی و فعالیت‌های آنلاین دارای پیوند مؤثر با آن دولت تعریف کرد. این تعریف از یک سو با حاکمیت سنتی ارتباط دارد و از سوی دیگر

محدود به عنصر جغرافیا نیست. نکته مهم آن است که چنین تعریفی باید میان اقتدار مشروع دولت و ادعاهای بیش‌ازحد فراسرزمینی تمایز ایجاد کند. اگر هر دولت بتواند صرف وجود دسترسی اینترنتی به قلمرو خود را مبنای اعمال صلاحیت بداند، تعارض‌های صلاحیتی به‌شدت افزایش خواهد یافت. به همین دلیل، مسئله پیوند مؤثر و تناسب باید در هر نظریه‌ای درباره قلمرو مجازی مورد توجه قرار گیرد.

تحول حاکمیت سرزمینی و ظهور حاکمیت دیجیتال

گسترش فضای سایبری موجب شده است که اصل حاکمیت سرزمینی در معرض نوعی بازتعریف عملی قرار گیرد. در حقوق بین‌الملل کلاسیک، هرگونه ورود مادی نیروها یا مقامات یک دولت به قلمرو دولت دیگر بدون رضایت آن دولت می‌توانست تعرض به حاکمیت تلقی شود. در محیط دیجیتال، چنین ورود فیزیکی‌ای وجود ندارد و ممکن است یک عملیات از هزاران کیلومتر فاصله انجام شود، اما آثار آن مستقیماً در زیرساخت‌های حیاتی دولت هدف ظاهر شود. همین ویژگی سبب شده است که حقوق‌دانان درباره این مسئله اختلاف داشته باشند که آیا نفوذ سایبری بدون ایجاد خسارت فیزیکی می‌تواند به‌تنهایی نقض حاکمیت باشد یا خیر. Sloan نشان می‌دهد که اختلاف اصلی در این حوزه به ماهیت حقوقی حاکمیت بازمی‌گردد؛ اینکه آیا حاکمیت خود قاعده‌ای الزام‌آور و قابل نقض است یا بیشتر به‌عنوان اصل بنیادین ساختار حقوق بین‌الملل عمل می‌کند (Sloan, 2023).

حاکمیت سایبری در ابتدایی‌ترین معنا بیانگر استمرار اقتدار دولت در فضای سایبری است. بر اساس این دیدگاه، همان‌گونه که دولت بر زیرساخت‌های فیزیکی واقع در قلمرو خود اقتدار دارد، نسبت به شبکه‌ها، سرورها و سامانه‌های مستقر در آن قلمرو نیز از حقوق حاکمیتی برخوردار است. Dewan تصریح می‌کند که غیرسرزمینی‌بودن فضای سایبری به معنای خارج‌بودن آن از نظم حقوقی دولت‌ها نیست و دولت‌ها همچنان تلاش می‌کنند قواعد حاکمیت را بر این فضا اعمال کنند (Dewan, 2023). بااین‌حال، مشکل از جایی آغاز می‌شود که یک فعالیت دیجیتال هم‌زمان به چند قلمرو مرتبط باشد یا آثار آن بدون ورود فیزیکی به قلمرو دولت دیگر ایجاد شود.

یکی از جلوه‌های تحول حاکمیت، افزایش تأکید بر حاکمیت داده است. داده‌های دیجیتال می‌توانند در چند لحظه میان چندین قلمرو منتقل شوند و همین امر موجب شده است که دولت‌ها برای حفظ اقتدار خود بر اطلاعات مرتبط با شهروندان یا نهادهایشان، قواعد جدیدی وضع کنند. Fazaeli مفهوم حاکمیت داده را در پیوند با تحول صلاحیت کیفری در فضای سایبری بررسی کرده و نشان داده است که کنترل بر داده به‌تدریج در کنار سرزمین به یکی از عوامل تعیین‌کننده صلاحیت تبدیل می‌شود (Fazaeli, 2021). این تحول را می‌توان نشانه‌ای از انتقال تدریجی حاکمیت از تمرکز صرف بر مکان به تمرکز بر رابطه حقوقی میان دولت و داده دانست.

در همین زمینه، تعارض میان دسترسی فرامرزی به اطلاعات و احترام به حاکمیت دولت خارجی اهمیت اساسی دارد. اگر نهاد قضایی یک دولت بتواند مستقیماً به اطلاعات ذخیره‌شده در قلمرو دولت دیگر دسترسی یابد، مرز میان اجرای صلاحیت داخلی و نقض حاکمیت خارجی مبهم می‌شود. Salehi این مسئله را در قالب تعارض میان دسترسی به مرکز داده خارجی و اصل صلاحیت کیفری سرزمینی بررسی کرده و بر ضرورت توجه به حاکمیت دولت میزبان تأکید کرده است (Salehi, 2019). این مسئله به‌ویژه در پرونده‌هایی که شرکت ارائه‌دهنده خدمات در یک کشور، سرورها در کشور دوم و کاربر در کشور سوم قرار دارد، پیچیده‌تر می‌شود.

حاکمیت دیجیتال از حاکمیت سایبری گسترده‌تر است. درحالی‌که حاکمیت سایبری عمدتاً با امنیت شبکه‌ها، نفوذ سایبری و

صلاحیت دولت بر زیرساخت‌های اینترنتی مرتبط است، حاکمیت دیجیتال می‌تواند کنترل بر داده، فناوری، پلتفرم‌ها، هوش مصنوعی، الگوریتم‌ها، هویت دیجیتال و خدمات ابری را نیز شامل شود. Kazemnejad و Tavakkolifar با بررسی مسئله مالکیت بر داده‌های تولیدشده به‌وسیله هوش مصنوعی نشان داده‌اند که تحول فناوری پرسش‌های جدیدی درباره حدود کنترل دولت و اشخاص بر داده ایجاد کرده است (Kazemnejad & Tavakkolifar, 2024). این پرسش‌ها صرفاً موضوع حقوق خصوصی نیستند، بلکه با استقلال فناورانه و توان دولت برای اداره فضای دیجیتال خود نیز ارتباط دارند.

بعد دیگری از حاکمیت دیجیتال، کنترل بر پلتفرم‌های فراملی است. شرکت‌های بزرگ فناوری ممکن است در قلمرو یک دولت ثبت شده باشند، اما خدمات آنها در ده‌ها یا صدها دولت ارائه شود. دولت‌هایی که کاربران این پلتفرم‌ها در آنها حضور دارند، اغلب مدعی صلاحیت بر محتوای منتشرشده، داده‌های کاربران یا شیوه پردازش اطلاعات می‌شوند. این وضعیت باعث می‌شود که پلتفرم‌ها در معرض مجموعه‌ای از الزامات حقوقی متفاوت و گاه متعارض قرار گیرند. Haber و Topor این روند را یکی از عوامل شکل‌گیری حباب‌های اینترنتی می‌دانند که در آنها هر دولت تلاش می‌کند فضای آنلاین قابل دسترس برای شهروندان خود را مطابق ارزش‌ها و قواعد داخلی تنظیم کند (Haber & Topor, 2023). در نتیجه، اینترنت جهانی به‌تدریج می‌تواند به محیطی چندپاره تبدیل شود که در آن مرزهای حقوقی تا حدی جایگزین فقدان مرزهای فیزیکی می‌شوند.

این روند همچنین با مفهوم استقلال دیجیتال ارتباط دارد. دولتی که زیرساخت‌های اساسی ارتباطی، ذخیره‌سازی داده یا خدمات عمومی دیجیتال خود را به‌طور کامل به بازیگران خارجی وابسته کرده باشد، ممکن است در شرایط بحران با محدودیت در اعمال اقتدار سیاسی مواجه شود. از این منظر، حاکمیت دیجیتال نه‌تنها مسئله صلاحیت، بلکه مسئله توان عملی دولت برای حفظ عملکردهای اساسی خود است. فناوری‌های بلاک‌چین و هویت خودحاکم نمونه‌ای از تلاش برای ایجاد ساختارهای جدید کنترل داده و هویت هستند که ممکن است وابستگی به نهادهای مرکزی را کاهش دهند (Farao et al., 2024). در عین حال، توسعه چنین فناوری‌هایی ممکن است اقتدار سنتی دولت را نیز به چالش بکشد؛ زیرا بخشی از کنترل هویت و اطلاعات از ساختارهای دولتی به معماری‌های غیرمتمرکز منتقل می‌شود.

در سطح بین‌المللی، یکی از مهم‌ترین پرسش‌ها مربوط به رابطه میان حاکمیت دیجیتال و اصل عدم مداخله است. اگر یک دولت از طریق عملیات سایبری در سامانه‌های سیاسی یا انتخاباتی دولت دیگر دخالت کند، ممکن است عمل او علاوه بر نقض احتمالی حاکمیت، مصداق مداخله ممنوع نیز باشد. تفاوت میان این دو مفهوم از اهمیت زیادی برخوردار است. اصل عدم مداخله معمولاً نیازمند وجود عنصر اجبار در حوزه‌ای است که دولت هدف حق دارد آزادانه درباره آن تصمیم بگیرد، درحالی‌که نظریه نقض حاکمیت ممکن است آستانه پایین‌تری داشته باشد و برخی نفوذهای غیرمجاز را نیز دربر گیرد. Sloan این تمایز را در چارچوب مسئولیت سایبری مهم می‌داند، زیرا نوع قاعده‌ای که نقض شده است بر ارزیابی مسئولیت بین‌المللی اثر می‌گذارد (Sloan, 2023).

همچنین حاکمیت دیجیتال با مفهوم تمامیت ارضی رابطه‌ای پیچیده دارد. در حقوق بین‌الملل سنتی، تمامیت ارضی عمدتاً ناظر بر مصونیت قلمرو فیزیکی دولت در برابر تجاوز یا تجزیه بوده است. در محیط دیجیتال، ممکن است یک دولت بدون تصرف هیچ بخشی از خاک دولت دیگر، زیرساخت‌های حیاتی آن را مختل کند. اگر اختلال در شبکه برق، سامانه بانکی یا خدمات عمومی از طریق عملیات سایبری ایجاد شود، آثار آن می‌تواند مشابه یک اقدام فیزیکی جدی باشد. در چنین وضعیتی، پرسش این است که آیا

مفهوم تمامیت ارضی باید به «تمامیت عملکردی» نیز گسترش پیدا کند یا خیر. این پرسش یکی از زمینه‌هایی است که می‌تواند در آینده به تحول حقوق عرفی منجر شود.

مفهوم حاکمیت دیجیتال همچنین در تعارض با ایده اینترنت جهانی و آزاد قرار می‌گیرد. رویکرد مبتنی بر اینترنت جهانی بر این فرض استوار است که جریان اطلاعات نباید به مرزهای ملی محدود شود و اتصال شبکه‌ای باید تا حد امکان فرامرزی باقی بماند. در مقابل، رویکرد حاکمیت دیجیتال بر حق دولت برای کنترل داده، محتوا و زیرساخت مرتبط با قلمرو یا اتباع خود تأکید می‌کند. مطالعه تطبیقی Lidia Tri Chris Nia و همکاران نشان می‌دهد که دولت‌ها می‌توانند برداشت‌های متفاوتی از حاکمیت سایبری داشته باشند و این برداشت‌ها بر سیاست‌های داخلی آنها در کنترل و تنظیم فضای آنلاین اثرگذار است (Lidia Tri Chris Nia et al., 2023). چنین اختلافی نشان می‌دهد که هنوز یک الگوی واحد جهانی درباره دامنه حاکمیت دیجیتال شکل نگرفته است.

برخی دولت‌ها حاکمیت را به‌عنوان مفهومی فراگیر می‌فهمند که فضای سایبری نیز به‌طور کامل در قلمرو آن قرار می‌گیرد. این رویکرد معمولاً با تأکید بر امنیت ملی، کنترل محتوا و حفاظت از زیرساخت‌های داخلی همراه است. در مقابل، برخی دیگر بر اعمال قواعد موجود حقوق بین‌الملل بدون ایجاد مفاهیم جدید تأکید دارند. مواضع رسمی دولت‌ها درباره حاکمیت در سایر زمینه‌ها نیز نشان می‌دهد که اصل احترام به حاکمیت و تمامیت ارضی همچنان از جایگاه سیاسی و حقوقی بسیار بالایی برخوردار است. برای نمونه، وزارت امور خارجه چین در سال ۲۰۲۵ در موضع‌گیری رسمی خود بر مخالفت با اقداماتی که حاکمیت، امنیت و تمامیت ارضی ایران را نقض می‌کنند تأکید کرده است (Ministry of Foreign Affairs of the People's Republic of, 2025). هرچند این موضع مستقیماً ناظر بر حاکمیت دیجیتال نیست، تداوم تأکید دولت‌ها بر مصونیت حوزه اقتدارشان نشان می‌دهد که هر نظریه‌ای درباره حاکمیت دیجیتال نیز ناگزیر باید در امتداد همین مبانی اصلی حقوق بین‌الملل تحلیل شود.

تجربه سایر حوزه‌های حقوق فرامرزی نیز نشان می‌دهد که مفهوم حاکمیت قابلیت انعطاف دارد. Ebrahimifar و همکاران در تحلیل تحول ورشکستگی فرامرزی از حاکمیت سرزمینی مطلق به سوی جهان‌شمولی تعدیل‌شده نشان می‌دهند که افزایش روابط فرامرزی می‌تواند موجب بازتفسیر نحوه اعمال صلاحیت دولت‌ها شود، بدون آنکه اصل حاکمیت به‌طور کامل کنار گذاشته شود (Ebrahimifar et al., 2024). در حوزه دیجیتال نیز احتمالاً روند مشابهی در حال وقوع است. دولت‌ها همچنان بر حاکمیت خود تأکید می‌کنند، اما ناچارند بپذیرند که اعمال مطلق و انحصاری صلاحیت در فضایی که از نظر فنی به‌شدت به‌هم‌پیوسته است، امکان‌پذیر نیست.

ازاین‌رو، تحول حاکمیت سرزمینی در عصر دیجیتال را نمی‌توان صرفاً به‌عنوان افول حاکمیت توصیف کرد. آنچه رخ داده است بیشتر نوعی تغییر در شکل اعمال حاکمیت است. دولت از کنترل صرف بر مکان به کنترل بر جریان، داده، زیرساخت و دسترسی حرکت کرده است. در این الگو، قدرت حاکمیتی نه فقط با توانایی بستن مرز فیزیکی، بلکه با توانایی تنظیم دسترسی به شبکه، الزام شرکت‌های خارجی، حفاظت از داده و حفظ عملکرد زیرساخت‌های دیجیتال سنجیده می‌شود. همین تحول زمینه را برای طرح این پرسش فراهم می‌کند که آیا حاکمیت دیجیتال می‌تواند از سطح یک مفهوم توصیفی فراتر رود و به یک قاعده مستقل حقوق بین‌الملل عرفی تبدیل شود.

امکان‌سنجی شناسایی حاکمیت دیجیتال به‌عنوان قاعده مستقل حقوق بین‌الملل عرفی

شناسایی حاکمیت دیجیتال به‌عنوان یک قاعده مستقل حقوق بین‌الملل عرفی مستلزم اثبات دو عنصر اساسی عرف، یعنی وجود رویه عمومی دولت‌ها و وجود اعتقاد حقوقی است. صرف

فراگیرشدن یک رفتار یا سیاست برای ایجاد عرف کافی نیست؛ رفتار دولت‌ها باید از درجه‌ای از گستردگی و انسجام برخوردار باشد و دولت‌ها نیز آن را به دلیل احساس وجود یک حق یا تکلیف حقوقی انجام دهند. این تمایز در حوزه دیجیتال اهمیت زیادی دارد، زیرا بسیاری از اقداماتی که دولت‌ها در زمینه کنترل اینترنت، ذخیره‌سازی داده یا محدودسازی پلتفرم‌ها انجام می‌دهند ممکن است ناشی از ملاحظات سیاسی، امنیتی یا اقتصادی باشد، نه اعتقاد به وجود یک قاعده حقوق بین‌المللی.

از منظر رویه دولت‌ها، شواهد قابل توجهی از گسترش کنترل دولت‌ها بر حوزه دیجیتال وجود دارد. دولت‌ها قوانین گسترده‌ای درباره حفاظت از داده، امنیت سایبری، جرایم رایانه‌ای، زیرساخت‌های حیاتی و خدمات آنلاین تصویب کرده‌اند. بسیاری از دولت‌ها شرکت‌های خارجی را ملزم می‌کنند از قوانین ملی مربوط به داده یا محتوا تبعیت کنند، حتی اگر این شرکت‌ها در قلمرو آنها ثبت نشده باشند. Fazaeli این تحول را در قالب گذار از صلاحیت سرزمینی کلاسیک به الگویی که حاکمیت داده در آن نقش بیشتری دارد تحلیل می‌کند (Fazaeli, 2021). گسترش چنین قوانینی نشان می‌دهد که دولت‌ها به‌طور فزاینده‌ای حوزه دیجیتال را بخشی از قلمرو مشروع تنظیم‌گری خود می‌دانند.

همچنین رویه دولت‌ها در حمایت از داده و زیرساخت‌های دیجیتال نشان‌دهنده افزایش اهمیت این حوزه برای اقتدار عمومی است. Kazemnejad و Tavakkolifar بر این نکته تأکید کرده‌اند که حاکمیت داده در ارتباط با فناوری‌های جدید به یک مسئله حقوقی مستقل تبدیل شده است (Kazemnejad & Tavakkolifar, 2024). الزام به ذخیره داده در داخل کشور، کنترل بر انتقال داده به خارج، تعیین ضوابط پردازش اطلاعات حساس و محدودکردن دسترسی خارجی به پایگاه‌های داده دولتی، نمونه‌هایی از رویه‌هایی هستند که می‌توانند در ارزیابی شکل‌گیری حاکمیت دیجیتال مورد توجه قرار گیرند.

بااین‌حال، وجود رویه گسترده به‌تنهایی کافی نیست. باید مشخص شود که آیا این اقدامات از الگوی نسبتاً مشترکی پیروی می‌کنند یا خیر. Haber و Topor نشان می‌دهند که افزایش کنترل دولت‌ها می‌تواند به شکل‌گیری حباب‌های اینترنتی و حوزه‌های دیجیتال متمایز منجر شود (Haber & Topor, 2023). این روند از منظر رویه دولت‌ها اهمیت دارد، زیرا بیانگر تمایل به ایجاد مرزهای حقوقی در محیطی است که از نظر فنی فاقد مرز است. بااین‌حال، شیوه و شدت این کنترل در دولت‌های مختلف تفاوت چشمگیری دارد و همین تفاوت ارزیابی انسجام رویه را دشوار می‌کند.

در حوزه اعمال صلاحیت نسبت به داده‌های خارجی نیز رویه دولت‌ها همچنان محل اختلاف است. Salehi نشان داده است که دسترسی به داده موجود در قلمرو دولت دیگر می‌تواند با اصل حاکمیت و صلاحیت سرزمینی تعارض پیدا کند (Salehi, 2019). اگر دولت‌ها به‌طور گسترده چنین دسترسی‌هایی را بدون رضایت دولت میزبان انجام دهند و در عین حال آنها را از منظر حقوق بین‌الملل مجاز بدانند، ممکن است به شکل‌گیری نوعی رویه جدید منجر شود. در مقابل، اگر دولت‌ها همچنان بر ضرورت احترام به صلاحیت سرزمینی تأکید کنند، این رفتار می‌تواند نشانه استمرار قدرت قاعده سنتی حاکمیت باشد. در حال حاضر، شواهد هر دو رویکرد را می‌توان مشاهده کرد.

در بحث opinio juris وضعیت پیچیده‌تر است. یکی از مشکلات اصلی این است که دولت‌ها اغلب در اسناد رسمی خود از واژه حاکمیت استفاده می‌کنند، اما روشن نمی‌کنند که منظور آنها یک قاعده مستقل حقوق بین‌المللی است یا صرفاً اصل کلی استقلال دولت. Sloan نشان می‌دهد که اختلاف درباره وضعیت حقوقی حاکمیت در فضای سایبری هنوز ادامه دارد و برخی دیدگاه‌ها آن را قاعده‌ای مستقل و برخی دیگر صرفاً اصلی سازمان‌دهنده می‌دانند (Sloan, 2023). این اختلاف نظری،

به‌ویژه در میان دولت‌های تأثیرگذار، مانع مهمی برای اثبات وجود opinio juris واحد است.

از سوی دیگر، رفتار و مواضع دولت‌ها درباره حاکمیت در معنای عام همچنان از درجه بالایی از ثبات برخوردار است. دولت‌ها به‌طور مستمر بر احترام به استقلال، امنیت و تمامیت ارضی تأکید می‌کنند. موضع رسمی چین درباره مخالفت با نقض حاکمیت، امنیت و تمامیت ارضی ایران نمونه‌ای از استمرار این رویکرد است (Ministry of Foreign Affairs of the People's Republic of, 2025). اگرچه این نوع مواضع لزوماً درباره فضای دیجیتال نیستند، اما نشان می‌دهند که اصل احترام به حوزه اقتدار دولت همچنان عنصر بنیادین در گفتمان حقوقی دولت‌هاست. پرسش اصلی آن است که آیا این اصل به‌طور مشخص به فضای دیجیتال نیز توسعه یافته و آیا دولت‌ها این توسعه را الزام حقوقی می‌دانند.

مطالعه تطبیقی رویکرد ایران و اندونزی نشان می‌دهد که مفهوم حاکمیت سایبری در عمل می‌تواند از یک دولت به دولت دیگر برداشت متفاوتی داشته باشد (Lidia Tri Chris Nia et al., 2023). همین تفاوت بیانگر این است که هنوز تعریف واحدی از حدود و محتوای حاکمیت دیجیتال وجود ندارد. برخی دولت‌ها ممکن است حاکمیت سایبری را حق کنترل کامل بر جریان اطلاعات تلقی کنند، درحالی‌که برخی دیگر آن را بیشتر به حمایت از زیرساخت و اعمال صلاحیت قانونی محدود می‌کنند. فقدان توافق درباره محتوا، تشکیل قاعده عرفی مستقل را دشوار می‌سازد، زیرا قاعده عرفی باید از حداقل درجه‌ای از قابلیت تعیین و پیش‌بینی برخوردار باشد.

در ارزیابی وجود یک قاعده عرفی مستقل، باید همچنین بررسی شود که آیا حاکمیت دیجیتال چیزی فراتر از کاربرد قواعد موجود ارائه می‌دهد. اگر تمام مسائل مربوط به فضای سایبری را بتوان از طریق حاکمیت سرزمینی، اصل عدم مداخله، منع توسل به زور، قواعد صلاحیت و مسئولیت بین‌المللی حل کرد، ضرورت ایجاد یک قاعده مستقل کاهش می‌یابد. Dewan با تأکید بر ماهیت غیرسرزمینی فضای سایبری نشان می‌دهد که مسئله اصلی، نحوه اعمال حاکمیت موجود در محیط جدید است (Dewan, 2023). از این منظر، حاکمیت دیجیتال ممکن است صرفاً نام جدیدی برای توسعه همان اصل سنتی باشد.

در مقابل، استدلال‌هایی نیز به سود استقلال این مفهوم وجود دارد. نخست آنکه فضای دیجیتال ویژگی‌هایی دارد که در قلمرو فیزیکی وجود ندارد. داده می‌تواند بدون انتقال فیزیکی جابه‌جا شود، یک فعالیت می‌تواند هم‌زمان در چند قلمرو آثار حقوقی ایجاد کند و کنترل بر یک زیرساخت دیجیتال ممکن است بدون هیچ‌گونه حضور فیزیکی اعمال شود. دوم آنکه دولت‌ها به‌طور فزاینده‌ای حوزه دیجیتال را بخشی از امنیت و استقلال خود تلقی می‌کنند. Haber و Topor روند شکل‌گیری فضای اینترنتی تفکیک‌شده را نشانه‌ای از افزایش اهمیت اقتدار ملی در شبکه جهانی می‌دانند (Haber & Topor, 2023). سوم آنکه مفاهیمی مانند حاکمیت داده و استقلال فناورانه به‌تدریج از حوزه سیاست عمومی وارد ادبیات حقوقی شده‌اند.

در حوزه فناوری‌های غیرمتمرکز نیز پرسش از حاکمیت اهمیت جدیدی پیدا کرده است. Farao و همکاران نشان می‌دهند که استفاده از بلاک‌چین و هویت خودحاکم می‌تواند ساختارهای سنتی کنترل داده و هویت را تغییر دهد (Farao et al., 2024). اگر در آینده بخش بزرگی از تعاملات اقتصادی و هویتی بر بستر شبکه‌های غیرمتمرکز انجام شود، دولت‌ها برای حفظ اقتدار خود ناچار خواهند بود قواعد جدیدی برای تعیین صلاحیت ایجاد کنند. چنین تحولاتی ممکن است به تقویت استدلال موافق با شکل‌گیری یک حوزه مستقل تحت عنوان حاکمیت دیجیتال کمک کند.

از منظر نظری، یکی از مناسب‌ترین راه‌ها برای ارزیابی وضعیت کنونی، تفکیک میان سه سطح است. در سطح نخست، حاکمیت

دیجیتال می‌تواند صرفاً یک مفهوم سیاستی باشد که دولت‌ها برای توجیه کنترل بیشتر بر فناوری و داده از آن استفاده می‌کنند. در سطح دوم، می‌توان آن را یک اصل حقوقی در حال ظهور دانست که هنوز عناصر عرفی آن کامل نشده‌اند. در سطح سوم، می‌توان از قاعده عرفی مستقل و الزام‌آور سخن گفت. شواهد موجود بیشتر از سطح دوم حمایت می‌کنند. رویه دولت‌ها در زمینه کنترل داده و زیرساخت گسترده شده است، اما opinio juris هنوز به اندازه‌ای هماهنگ نیست که بتوان از تثبیت کامل قاعده سخن گفت.

تحول سایر شاخه‌های حقوق بین‌الملل نیز نشان می‌دهد که شکل‌گیری قواعد جدید معمولاً تدریجی است. Ebrahimifar و همکاران در بحث ورشکستگی فرامرزی نشان می‌دهند که الگوهای سنتی حاکمیت می‌توانند تحت تأثیر نیازهای فرامرزی به‌تدریج تعدیل شوند (Ebrahimifar et al., 2024). در حوزه دیجیتال نیز ممکن است ابتدا مجموعه‌ای از قواعد پراکنده درباره داده، صلاحیت، امنیت و زیرساخت شکل گیرد و سپس این قواعد در طول زمان در قالب یک مفهوم عام‌تر از حاکمیت دیجیتال همگرا شوند.

در این فرایند، عنصر استمرار نیز اهمیت دارد. بسیاری از سیاست‌های دیجیتال دولت‌ها هنوز نسبتاً جدید هستند و در واکنش به تحولات فناوری شکل گرفته‌اند. بنابراین، ممکن است برای ارزیابی اینکه کدام‌یک از آنها به رویه پایدار حقوقی تبدیل خواهند شد به زمان بیشتری نیاز باشد. از سوی دیگر، حقوق بین‌الملل عرفی الزاماً نیازمند سابقه بسیار طولانی نیست و در صورتی که رویه گسترده و اعتقاد حقوقی روشن باشد، عرف می‌تواند در بازه زمانی کوتاه‌تری شکل گیرد. مسئله اصلی در اینجا نه صرف طول مدت، بلکه درجه انسجام و انگیزه حقوقی دولت‌هاست.

برای شناسایی حاکمیت دیجیتال به‌عنوان قاعده مستقل، باید محتوای آن نیز قابل تعریف باشد. یک قاعده حقوقی نمی‌تواند صرفاً اعلام کند که دولت‌ها در فضای دیجیتال حاکمیت دارند، بدون آنکه حدود این حاکمیت مشخص شود. در این مقاله، می‌توان چهار عنصر را برای تعیین قلمرو مشروع حاکمیت دیجیتال پیشنهاد کرد: وجود پیوند مؤثر میان دولت و موضوع دیجیتال؛ وجود کنترل یا صلاحیت حقوقی قابل اثبات؛ وجود منفعت حاکمیتی اساسی؛ و رعایت تناسب و حقوق سایر دولت‌ها. این عناصر می‌توانند از ادعای نامحدود دولت‌ها نسبت به هر فعالیت آنلاین جلوگیری کنند و در عین حال امکان حمایت از حوزه دیجیتال حیاتی آنها را فراهم سازند.

پیوند مؤثر می‌تواند بر اساس محل زیرساخت، تابعیت اشخاص، منشأ داده، محل بروز آثار یا نقش یک سامانه در انجام وظایف عمومی تعیین شود. کنترل حقوقی نیز به معنای آن است که دولت بتواند بر اساس قوانین معتبر و در چارچوب حقوق بین‌الملل بر موضوع دیجیتال اعمال صلاحیت کند. منفعت حاکمیتی اساسی می‌تواند شامل امنیت ملی، عملکرد خدمات عمومی، حفاظت از فرایندهای سیاسی یا صیانت از داده‌های حساس باشد. در نهایت، اصل تناسب مانع آن می‌شود که دولت به نام حاکمیت دیجیتال ادعای کنترل نامحدود بر فعالیت‌های فرامرزی مطرح کند.

اگر این عناصر در رویه دولت‌ها به‌تدریج تثبیت شوند، امکان شکل‌گیری قاعده‌ای مستقل افزایش خواهد یافت. در وضعیت کنونی، حاکمیت دیجیتال بیش از آنکه قاعده‌ای کاملاً شکل‌گرفته باشد، مفهومی در حال تبدیل‌شدن از سیاست به حقوق است. اهمیت آن در این است که حوزه‌های مختلفی مانند داده، امنیت سایبری، صلاحیت و استقلال فناوری را در یک چارچوب نظری مشترک قرار می‌دهد. همین قابلیت ترکیبی می‌تواند در آینده مبنای شکل‌گیری عرفی مستقل شود، به‌ویژه اگر دولت‌ها در اسناد رسمی

خود صریحاً اعلام کنند که احترام به حوزه دیجیتال سایر دولت‌ها را یک تکلیف حقوقی می‌دانند.

نتیجه‌گیری

تحول فناوری‌های دیجیتال موجب شده است که یکی از بنیادی‌ترین مفاهیم حقوق بین‌الملل، یعنی حاکمیت سرزمینی، با شرایطی مواجه شود که در زمان شکل‌گیری ساختار کلاسیک دولت ـ ملت قابل تصور نبود. حاکمیت سنتی بر وجود قلمرویی مشخص، مرزهای نسبتاً ثابت و امکان انتساب فعالیت‌ها به مکان جغرافیایی معین استوار بود. در مقابل، فضای دیجیتال محیطی شبکه‌ای، سیال، فرامرزی و چندلایه است که در آن داده، زیرساخت، کاربر و ارائه‌دهنده خدمات می‌توانند هم‌زمان به چند نظام حقوقی مرتبط باشند. این تفاوت اساسی سبب شده است که رابطه میان قلمرو و اقتدار حاکمیتی از حالت صرفاً جغرافیایی فاصله بگیرد و به سوی الگویی چندبعدی حرکت کند.

تحلیل انجام‌شده نشان می‌دهد که مفهوم قلمرو در عصر دیجیتال از میان نرفته است، بلکه کارکرد آن دگرگون شده است. زیرساخت‌های فیزیکی فضای سایبری همچنان در قلمرو دولت‌ها قرار دارند و تابع صلاحیت سرزمینی‌اند، اما بخش مهمی از فعالیت‌های دیجیتال را نمی‌توان تنها بر مبنای محل فیزیکی تحلیل کرد. در چنین شرایطی، معیارهایی مانند محل بروز آثار، تابعیت کاربران، منشأ داده، کارکرد زیرساخت و پیوند فعالیت دیجیتال با منافع اساسی دولت اهمیت بیشتری پیدا می‌کنند. این تحول نشان‌دهنده گذار تدریجی از مفهوم صرفاً جغرافیایی قلمرو به نوعی قلمرو عملکردی است.

قلمرو مجازی را نمی‌توان معادل دقیق قلمرو فیزیکی دانست. قلمرو مجازی فاقد مرز مادی و خطوط جغرافیایی ثابت است، اما می‌تواند حوزه‌ای باشد که دولت نسبت به آن ادعای اقتدار حقوقی، تنظیمی یا حفاظتی دارد. این حوزه ممکن است شامل داده‌های شهروندان، زیرساخت‌های حیاتی، سامانه‌های دولتی، پلتفرم‌های فعال در بازار داخلی یا منابع دیجیتال مرتبط با امنیت ملی باشد. در نتیجه، مفهوم قلمرو مجازی بیشتر از آنکه یک مکان باشد، شبکه‌ای از روابط و پیوندهای حقوقی است.

در این چارچوب، حاکمیت دیجیتال را باید از حاکمیت سایبری متمایز دانست. حاکمیت سایبری عمدتاً ناظر بر اقتدار دولت در محیط شبکه‌ای و امنیت زیرساخت‌های سایبری است، درحالی‌که حاکمیت دیجیتال دامنه گسترده‌تری دارد و داده، فناوری، پلتفرم، هوش مصنوعی، هویت دیجیتال و خدمات ابری را نیز دربر می‌گیرد. از این منظر، حاکمیت دیجیتال می‌تواند به‌عنوان بازتاب تحول در ماهیت منابع قدرت دولت در عصر فناوری تفسیر شود. دولت معاصر نه‌تنها باید بتواند بر سرزمین خود اقتدار داشته باشد، بلکه باید بتواند کارکردهای اساسی دیجیتال خود را نیز حفظ و تنظیم کند.

بااین‌حال، شناسایی حاکمیت دیجیتال به‌عنوان یک قاعده مستقل حقوق بین‌الملل عرفی نیازمند احتیاط است. رویه دولت‌ها در زمینه کنترل داده، تنظیم پلتفرم‌ها، حفاظت از زیرساخت‌های دیجیتال و اعمال صلاحیت نسبت به فعالیت‌های فرامرزی به‌طور محسوسی افزایش یافته است. این روند نشان می‌دهد که دولت‌ها حوزه دیجیتال را بخشی از منافع حاکمیتی خود می‌دانند. بااین‌حال، وجود رویه گسترده به‌تنهایی برای شکل‌گیری عرف کافی نیست. لازم است دولت‌ها این رفتار را ناشی از وجود یک حق یا تکلیف حقوقی بین‌المللی تلقی کنند.

در وضعیت کنونی، مهم‌ترین مانع در برابر شناسایی حاکمیت دیجیتال به‌عنوان قاعده عرفی مستقل، فقدان انسجام کافی در اعتقاد حقوقی دولت‌هاست. هنوز توافق روشنی وجود ندارد که آیا نقض حاکمیت در فضای دیجیتال به‌خودی‌خود یک عمل متخلفانه بین‌المللی است یا اینکه باید از طریق قواعد دیگری مانند عدم مداخله، منع توسل به زور یا صلاحیت سرزمینی ارزیابی شود. همچنین دولت‌ها برداشت یکسانی از دامنه حاکمیت دیجیتال

ندارند. برخی آن را حق گسترده کنترل فضای اطلاعاتی می‌دانند و برخی دیگر تنها بر حفاظت از زیرساخت و اعمال قواعد موجود تأکید دارند.

ازاین‌رو، نمی‌توان در شرایط کنونی با اطمینان از وجود یک قاعده کاملاً تثبیت‌شده عرفی تحت عنوان «حاکمیت دیجیتال» سخن گفت. در عین حال، شواهد موجود نیز اجازه نمی‌دهند این مفهوم صرفاً یک شعار سیاسی یا سیاست داخلی تلقی شود. افزایش مداوم قوانین مربوط به داده، گسترش سیاست‌های استقلال دیجیتال، اهمیت فزاینده زیرساخت‌های سایبری در امنیت ملی و تلاش دولت‌ها برای تنظیم بازیگران فراملی، همگی نشان می‌دهند که یک هنجار حقوقی جدید در حال شکل‌گیری است.

بهترین توصیف از وضعیت موجود آن است که حاکمیت دیجیتال در مرحله یک «قاعده عرفی در حال تکوین» قرار دارد. این قاعده هنوز به سطحی از قطعیت نرسیده است که بتوان محتوای آن را کاملاً مشخص و الزام‌آور دانست، اما عناصر اولیه آن در حال ظهورند. اگر در آینده دولت‌ها به‌طور صریح‌تر در اسناد رسمی و مواضع بین‌المللی خود از حق و تکلیف مربوط به احترام به حوزه دیجیتال سایر دولت‌ها سخن بگویند و اگر رویه عملی آنها نیز با این مواضع هماهنگ شود، امکان تبدیل این هنجار در حال ظهور به قاعده عرفی مستقل افزایش خواهد یافت.

برای جلوگیری از تبدیل حاکمیت دیجیتال به ابزاری برای ادعاهای نامحدود فراسرزمینی، لازم است حدود آن بر اساس معیارهای حقوقی مشخص تعیین شود. وجود پیوند مؤثر میان دولت و موضوع دیجیتال، وجود صلاحیت یا کنترل حقوقی واقعی، وجود منفعت حاکمیتی اساسی و رعایت اصل تناسب می‌تواند چارچوب مناسبی برای این منظور فراهم آورد. این معیارها از یک سو امکان حمایت از استقلال دیجیتال دولت‌ها را ایجاد می‌کنند و از سوی دیگر مانع از آن می‌شوند که هرگونه فعالیت آنلاین صرفاً به دلیل قابل دسترس بودن در قلمرو یک دولت، تابع حاکمیت نامحدود آن دولت تلقی شود.

در نهایت، تحول مفهوم حاکمیت سرزمینی در عصر دیجیتال را نباید به‌عنوان پایان حاکمیت یا حذف سرزمین تفسیر کرد. آنچه در حال رخ‌دادن است، بازآرایی رابطه میان اقتدار، قلمرو و فناوری است. سرزمین همچنان بنیان اصلی سازمان سیاسی دولت باقی می‌ماند، اما اقتدار دولت به‌طور فزاینده‌ای به حوزه‌هایی گسترش می‌یابد که ماهیت آنها غیرمادی و شبکه‌ای است. حاکمیت دیجیتال محصول همین تحول است و احتمالاً در دهه‌های آینده یکی از مهم‌ترین حوزه‌های توسعه حقوق بین‌الملل خواهد بود. آینده این مفهوم به میزان همگرایی رویه دولت‌ها، روشن‌شدن اعتقاد حقوقی، توسعه معیارهای دقیق صلاحیت و ایجاد توازن میان استقلال دیجیتال دولت‌ها و ماهیت جهانی فضای سایبری بستگی خواهد داشت.

مشارکت نویسندگان

در نگارش این مقاله تمامی نویسندگان نقش یکسانی ایفا کردند.

تعارض منافع

در انجام مطالعه حاضر، هیچ‌گونه تضاد منافعی وجود ندارد.

EXTENDED ABSTRACT

The transformation of territorial sovereignty under the conditions created by virtual environments has become one of the most significant theoretical and normative challenges in contemporary international law. Classical sovereignty was historically constructed around a close relationship among statehood, territory, jurisdiction, and exclusive public authority, with physical borders functioning as the principal means of delimiting the spatial reach of governmental power. Fitzpatrick emphasizes that territoriality has long operated as a central organizing principle through which sovereignty, legal authority, and the rule of law are structured within and among states (Fitzpatrick, 2001). The rise of cyberspace, however, has disrupted the assumption that legally relevant conduct can always be linked

to a single geographical location. Digital interactions may involve users located in one state, servers situated in another, service providers incorporated in a third jurisdiction, and data dynamically processed across several additional territories. Dewan characterizes cyberspace as a non-territorial virtual environment that challenges conventional understandings of sovereignty because the functional geography of digital activity does not correspond neatly to physical borders (Dewan, 2023). This transformation has not eliminated territory from international law, but it has complicated the spatial logic through which state authority is traditionally exercised. The emergence of cloud computing, artificial intelligence, distributed networks, platform economies, cross-border data transfers, and digitally mediated public services has made it increasingly difficult to define sovereignty exclusively through physical control over land, airspace, and territorial waters. At the same time, states have increasingly attempted to preserve regulatory control over digital activities that affect their populations, institutions, security interests, and public functions. The present study therefore examines whether the development of virtual territories and the expansion of state control over digital resources can support the recognition of "digital sovereignty" as an independent rule of customary international law. The central research question is whether contemporary state practice and legal conviction have developed sufficiently to justify treating digital sovereignty as a distinct customary norm rather than merely as an application of traditional territorial sovereignty to a technologically new environment.

The conceptual foundation of this inquiry rests on the distinction between physical territory, cyberspace, virtual territory, data sovereignty, cyber sovereignty, and digital sovereignty. Cyberspace is not wholly detached from territorial reality because its physical layer consists of servers, cables, data centers, communication networks, and hardware located within national jurisdictions; nevertheless, its logical and informational layers are transnational and function through networks that routinely cross multiple borders. Dewan's analysis is particularly relevant because it demonstrates that cyberspace combines territorial infrastructure with non-territorial functionality, thereby producing a hybrid legal environment (Dewan, 2023). Within this environment, the concept of virtual territory may be understood not as a direct equivalent of land territory, but as a legally relevant sphere in which a state claims regulatory, protective, or jurisdictional authority over data, infrastructure, systems, platforms, or digital activities connected to its population or essential public interests. Zhuk's examination of virtual sovereignty further illustrates that digital environments can generate novel claims concerning political authority, territorial imagination, and legal personality, even where such claims are not necessarily accepted by the broader international community (Zhuk, 2023). The concept of data sovereignty adds another dimension to this transformation because control over information has become central to state power, technological independence, security, and economic governance. Kazemnejad and Tavakkolifar show that data sovereignty increasingly raises complex questions regarding ownership, control, and jurisdiction, particularly in relation to data generated through artificial intelligence systems (Kazemnejad & Tavakkolifar, 2024). In this context, digital sovereignty should be treated as a broader concept than cyber sovereignty. Cyber sovereignty generally concerns the application of state authority within cyberspace and the protection of cyber infrastructure, whereas digital sovereignty potentially includes data governance, digital

identity, artificial intelligence, cloud services, technological infrastructures, platform regulation, and control over strategically significant digital ecosystems. The distinction is crucial because the legal recognition of digital sovereignty as an independent rule requires a sufficiently identifiable normative content that goes beyond the simple restatement of already existing territorial jurisdiction.

The practical transformation of sovereignty is particularly visible in the field of jurisdiction. Traditional international law generally gives territorial jurisdiction a primary role, but digital activity frequently creates situations in which several states can plausibly claim regulatory authority over the same conduct. Fazaeli demonstrates that cyber activities have contributed to a gradual shift from exclusive reliance on territorial criminal jurisdiction toward models in which data sovereignty and broader cross-border connections become increasingly important (Fazaeli, 2021). This is evident when states regulate foreign platforms, require compliance with national data-protection obligations, impose local data-storage requirements, or assert jurisdiction over online conduct that produces substantial effects within their territory. The challenge becomes even more acute when law-enforcement authorities seek direct access to data physically stored abroad. Salehi argues that accessing information located in a foreign data center may conflict with the principles of territorial criminal jurisdiction and state sovereignty, especially where such access is undertaken without the consent of the state in whose territory the data infrastructure is located (Salehi, 2019). These developments demonstrate that digital jurisdiction increasingly depends on multiple connecting factors, including territorial location, nationality, the place where effects are experienced, the location of infrastructure, and the relationship between data and the public functions of the regulating state. The evolution of sovereignty in other areas of transnational law also suggests that territorial authority is capable of adaptation rather than simple displacement. Ebrahimifar and colleagues show that cross-border insolvency has evolved from rigid territorial sovereignty toward modified forms of universalism that preserve state authority while accommodating transnational realities (Ebrahimifar et al., 2024). A similar dynamic may be emerging in the digital sphere, where territorial sovereignty is not disappearing but is increasingly supplemented by functional and relational criteria. This suggests that the legal significance of “territory” may gradually extend beyond geography toward a broader conception of effective digital connection, particularly when digital systems are essential to governmental functions, public services, national security, or the protection of citizens’ data.

The emergence of digital sovereignty is also connected to the growing fragmentation of the global internet and the increasing willingness of states to construct distinct national regulatory spaces within a technically interconnected network. Haber and Topor describe the development of “internet bubbles” as an expression of contemporary sovereignty, in which states use legal, technical, and institutional mechanisms to create relatively bounded digital environments within the wider internet (Haber & Topor, 2023). These measures may include content regulation, filtering, licensing requirements, restrictions on cross-border data transfers, mandatory cooperation by foreign platforms, domestic hosting requirements, and the creation of national digital infrastructures. Comparative analysis further demonstrates that states do not interpret cyber sovereignty in identical ways. Lidia Tri Chris Nia and colleagues, in their comparison of Iran and Indonesia, show that the implementation and

conceptualization of cyber sovereignty may vary significantly according to domestic legal structures, security priorities, political institutions, and approaches to internet governance (Lidia Tri Chris Nia et al., 2023). This divergence is important because it weakens the claim that a uniform global understanding of digital sovereignty has already emerged. At the same time, technological developments themselves are modifying the structure of authority. Farao and colleagues discuss blockchain-based systems and self-sovereign identity as technological architectures capable of redistributing control over identity and data away from centralized institutions (Farao et al., 2024). Such developments may paradoxically strengthen the demand for digital sovereignty while simultaneously limiting the state's traditional ability to monopolize regulatory control. States increasingly seek technological autonomy precisely because control over digital infrastructure and data has become closely linked to political independence. Accordingly, digital sovereignty is not simply a question of whether governments can regulate online conduct; it increasingly concerns whether they possess the technological, legal, and institutional capacity to preserve essential functions in digital environments dominated by transnational platforms, foreign infrastructure, and decentralized technologies.

The principal legal issue, however, is whether these developments have produced a customary rule. Customary international law requires both sufficiently general state practice and *opinio juris*, and the existence of numerous domestic laws or digital policies does not automatically establish either element. There is considerable evidence of expanding state practice in areas such as cybersecurity regulation, data localization, control over critical digital infrastructure, restrictions on foreign platforms, and extraterritorial data regulation. Fazaeli's analysis of the movement toward data sovereignty supports the proposition that state jurisdiction is increasingly extending beyond conventional territorial models (Fazaeli, 2021). Similarly, the growing juridical importance of data control reinforces the view that digital resources are becoming integrated into the concept of sovereign authority (Kazemnejad & Tavakkolifar, 2024). Yet the decisive difficulty lies in determining whether states adopt these measures because they believe international law grants them a distinct sovereign right over a digital domain or because they are simply exercising domestic regulatory powers for reasons of security, public order, economic policy, or technological strategy. Sloan identifies this precise uncertainty in the wider debate over cyber responsibility and sovereignty, noting that disagreement persists as to whether sovereignty in cyberspace functions as an independently enforceable rule or merely as a foundational principle underlying more specific norms such as non-intervention and territorial jurisdiction (Sloan, 2023). The persistence of strong state rhetoric concerning sovereignty and territorial integrity also demonstrates that sovereignty remains legally central in interstate relations. China's official opposition to actions violating Iran's sovereignty, security, and territorial integrity illustrates the continued normative importance attached to the protection of the state's sphere of authority (Ministry of Foreign Affairs of the People's Republic of, 2025). Nevertheless, such statements do not by themselves prove that the same legal conviction extends to a distinct digital sphere. The evidence therefore appears stronger for the existence of an emerging normative trend than for a fully consolidated independent customary rule. Digital sovereignty is increasingly visible in state practice, but the necessary *opinio juris* remains fragmented because states differ in both the meaning they

assign to digital sovereignty and the legal consequences they attach to its violation.

The study concludes that the emergence of virtual territories has not displaced territorial sovereignty but has transformed the manner in which sovereignty is conceptualized and exercised. The physical territory of the state remains the foundational spatial basis of international legal authority, yet digitalization has created additional functional spaces in which state power is exercised through control over data, infrastructure, platforms, digital identity, and technological systems. The concept of digital sovereignty therefore represents more than a rhetorical extension of traditional sovereignty, but it has not yet achieved the degree of normative precision and uniform legal acceptance necessary to be recognized without qualification as a fully established rule of customary international law. The most defensible characterization at the present stage is that digital sovereignty is an emerging customary norm whose development depends on the future convergence of state practice and legal conviction. For this norm to mature into an independent customary rule, states would need to articulate more clearly that respect for the digital sphere of other states is required as a matter of international law and not merely as a matter of political prudence or reciprocal restraint. Its legal content would also need to be delimited through objective criteria capable of distinguishing legitimate sovereign interests from excessive extraterritorial claims. A viable framework should therefore require an effective digital connection between the state and the relevant data, system, infrastructure, or activity; a legally recognizable basis of jurisdiction or control; the existence of a substantial sovereign interest such as national security, essential public services, democratic processes, or protection of sensitive data; and compliance with proportionality and the corresponding rights of other states and individuals. On this basis, digital sovereignty may eventually develop into a distinct legal doctrine capable of reconciling state authority with the transnational architecture of cyberspace, but its current status remains transitional, situated between the adaptation of classical territorial sovereignty and the formation of a genuinely new rule of international customary law.

References

Dewan, P. (2023). Cyberspace as a non-territorial virtual space: Unraveling the conundrum of state sovereignty in the cyberspace as a new-domain. *International Journal of Law Management and Humanities*, *6*(2), 1473-1477. https://doi.org/https://doij.org/10.10000/IJLMH.114537

Ebrahimifar, A., Rahimi, F., & Montazer, M. (2024). Cross-Border Insolvency: From Absolute Territorial Sovereignty to Modified Universalism in Light of Customary International Law. *Private and Criminal Law Research*, *20*(4).

Farao, A., Paparis, G., Panda, S., Panaousis, E., Zarras, A., & Xenakis, C. (2024). INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain. *International Journal of Information Security*, *23*(1), 347-371. https://doi.org/10.1007/s10207-023-00741-8

Fazaeli, M. (2021). Criminal Jurisdiction in Cyberspace: From the Territoriality Principle to Global Data Sovereignty. *Criminal Law Research Journal*, *12*(1).

Fitzpatrick, J. (2001). Sovereignty, Territoriality, and the Rule of Law. *Hastings International & Comparative Law Review*, *25*, 303.

Haber, E., & Topor, L. (2023). Sovereignty, Cyberspace, and the Emergence of Internet Bubbles. *Journal of Advanced Military Studies*, *14*(1), 144-165. https://doi.org/10.21140/mcuj.20231401006

Kazemnejad, S., & Tavakkolifar, E. (2024). Data Sovereignty and the Right of Ownership over AI-Generated Data: Legal Challenges and Cyber Requirements. *Journal of Cyber Law*, *1*(3), 61-71. https://www.sid.ir/paper/1782187/en

Lidia Tri Chris Nia, W., Syahidullhaq, M. S., & Pramono, B. K. (2023). Comparative Analysis of Cyber Sovereignty: Case From Indonesia and Iran. *Juss (Jurnal Sosial Soedirman)*, *6*(1), 27. https://doi.org/10.20884/juss.v6i1.7949

Ministry of Foreign Affairs of the People's Republic of, C. (2025). Foreign Ministry spokesperson: China opposes actions that violate Iran's sovereignty, security and territorial integrity.

Consulate General of the People's Republic of China in Bandar Abbas. https://abbas.china-consulate.gov.cn/eng/xwdt/202506/t20250614_11648650.htm

Salehi, J. (2019). Access to the Data Center Information of a Foreign Government in Conflict with the Principles of Territorial Criminal Jurisdiction and Sovereignty in International Law. *International Legal Scientific Quarterly*, *26*(60), 185-210.

Sloan, R. (2023). Cyber responsibility and sovereignty. *Columbia Journal of Transnational Law*, *61*(2), 178-205.

Zhuk, A. (2023). Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society*, *2*(3). https://doi.org/10.1007/s44206-023-00067-x