Review article

Confluence of the Two Concepts of Sovereignty and Data in the Digital Age: A Narrative Review

Mohammad Mohsen Salehzadeh [1] ,*Sepehr Ghazinoory [2] ,Farideh Bahrami [3]

1. PhD student in Science and Technology Policy, Tarbiat Modares University, Tehran, Iran.
2.Professor, Department of Information Technology Management, Faculty of Management and Economics, Tarbiat Modares University, Tehran, Iran.
3.Senior Researcher in Technology Management,HEC Montreal Business School, Montreal, Canada.

Use your device to scan and read the article online

Citation: Salehzadeh.M, Ghazinoory.S, Bahrami.F (2026). [Confluence of the Two Concepts of Sovereignty and Data in the Digital Age: A Narrative Review (Persian)]. *Journal Strategic Studies of Public Policy,* 16(58), 154-191.https://doi.org/10.22034/sspp.2026.2087033.3914

https://doi.org/10.22034/sspp.2026.2087033.3914

CC BY NC

Received: 05 Mar 2026
Accepted: 05 May 2026
Available Online: 20 Jun 2026

Keywords:
Sovereignty, Digital Sovereignty, Data Sovereignty, Narrative Review

ABSTRACT

The concept of sovereignty in domains beyond its political origin has paved the way for debates among various political, economic, and social discourses. The expansion of emerging technologies such as data and artificial intelligence, along with the rise of giant multinational corporations acting as shadow Sovern, has acted as a catalyst to intensify these discussions. One of the most important objectives of establishing sovereignty in the form of a unified leadership has been to create the necessary conditions for controlling various national resources by its legitimate authority. The emergence of giant technology companies, which have defined their revenue model based on data as the emerging asset of the new era, combined with the exploitation of this resource by major powers to realize their economic, political, social, and geopolitical goals, has made the need to pay attention to digital sovereignty more pressing than ever. In this article, using the narrative review method, we aim to cover a broader spectrum of related studies so that we can provide a general summary of sources related to digital sovereignty and data sovereignty. This method, which is discourse-based, collects various sources through a unique lens specific to each author. Despite similarities between this method and systematic reviews, the purpose of employing this approach lies in its flexible and interpretive nature compared to systematic methods. In this article, the concept of sovereignty from the perspective of political science is briefly addressed, and four categories of this concept are presented. Given the increasing dominance of multinational corporations and their confrontation with other key actors in the sovereignty domain (governments and citizens), as well as the growing interconnection between the digital sphere—especially data—and national sovereignty, an attempt has been made to introduce and explain a threefold classification (state sovereignty, corporate sovereignty, and multi-stakeholder sovereignty) by utilizing control as one of the main pillars of sovereignty, while also presenting policies adopted by leading countries under each of these interpretations.

*** Corresponding Author:**

Sepehr Ghazinoory

Address: Faculty of Management and Economics, Tarbiat Modares University, Tehran, Iran.
E-mail: ghazinoory@modares.ac.ir

مقاله‌مروری

تلاقی دو مفهوم حاکمیت و داده در عصر دیجیتال: یک مرور روایی

محمد محسن صالح‌زاده [۱]، *سپهر قاضی‌نوری [۲]، فریده بهرامی [۳]

۱. دانشجوی دکتری سیاست‌گذاری علم و فناوری، دانشگاه تربیت مدرس، تهران، ایران.

۲. استاد، گروه مدیریت فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران.

۳. پسادکترای مدیریت فناوری اطلاعات، دانشگاه HEC Montreal، کانادا.

تاریخ دریافت: ۱۴ اسفند ۱۴۰۴
تاریخ پذیرش: ۱۵ اردیبهشت ۱۴۰۵
تاریخ انتشار: ۳۰ خرداد ۱۴۰۵

چکیده

مفهوم حاکمیت در حوزه‌هایی ورای خاستگاه سیاسی خود زمینه‌ساز مناظرات میان گفتمان‌های سیاسی، اقتصادی و اجتماعی مختلف شده است. گسترش فناوری‌های نوظهور مانند حوزه داده و هوش مصنوعی و قدرت‌گرفتن شرکت‌های عظیم چندملیتی در قالب حاکمان در سایه، مانند کاتالیزوری بر تنور این مباحث دمیده‌اند. یکی از مهم‌ترین اهداف استقرار حاکمیت در قامت یک رهبری واحد، ایجاد زمینه‌های لازم برای کنترل منابع مختلف یک کشور توسط حاکمیت قانونی آن بوده است. ظهور شرکت‌های عظیم فناور که مدل درآمدی خود را بر مبنای داده به‌عنوان دارایی نوظهور عصر جدید تعریف کرده‌اند و بهره‌برداری قدرت‌های بزرگ از این منبع در راستای عینیت‌بخشی به اهداف اقتصادی، سیاسی، اجتماعی و ژئوپلیتیکی خود، لزوم توجه به حاکمیت دیجیتال را بیش‌ازپیش یادآور می‌شود. در این مقاله به کمک روش مرور روایت به دنبال پوشش طیف گسترده‌تری از مطالعات مرتبط هستیم تا بتوانیم خلاصه‌ای کلی از منابع مرتبط با حاکمیت دیجیتال و داده را ارائه کنیم. در این روش که بر مبنای گفتمان‌ها شکل می‌گیرد، منابع مختلف با یک لنز منحصربه‌فرد که مختص نویسندگان است گردآوری می‌شوند. علی‌رغم شباهت‌های این روش با مرور نظام‌مند، هدف از به‌کارگیری این روش ماهیت انعطاف‌پذیر و تفسیری آن در مقابل روش نظام‌مند بوده است. در این مقاله به‌صورت اجمالی به مفهوم حاکمیت از منظر علوم سیاسی پرداخته شده و دودسته بندی چهارگانه از این مفهوم ارائه گردیده است. باتوجه‌به قدرت‌گرفتن بیش‌ازپیش شرکت‌های چندملیتی و تقابل آنان با سایر بازیگران کلیدی حوزه حاکمیت (دولت‌ها و مردم) و شکل‌گیری یک ارتباط تنگاتنگ میان حوزه دیجیتال و به‌خصوص حوزه داده با حاکمیت کشورها، تلاش شده است تا با بهره‌گیری از لنز کنترل به‌عنوان یکی از اصلی‌ترین بنیان‌های حاکمیت، یک دسته‌بندی سه‌گانه (حاکمیت دولتی، حاکمیت بنگاهی و حاکمیت چند ذی‌نفعی) معرفی و تشریح شده و سیاست‌های کشورهای پیشرو در هر کدام از این خوانش‌ها ارائه شود.

کلیدواژه‌ها:
حاکمیت‌حاکمیت دیجیتال‌حاکمیت‌داده، مرور روایت

* نویسنده مسئول:
سپهر قاضی‌نوری
نشانی: گروه مدیریت فناوری اطلاعات، دانشگاه تربیت مدرس، تهران، ایران.
رایانامه: ghazinoory@modares.ac.ir

مقدمه

مفهوم حاکمیت[1] به عنوان یکی از نهادهای اصلی جامعه بین‌الملل، در سالیان اخیر و به تکرار مورد دست اندازی قدرت‌های بزرگ قرار گرفته است (شورای روابط خارجی[2]، ۲۰۲۳؛ دی‌لوکا[3]، ۲۰۲۵؛ جورج[4]، ۲۰۱۵). در عرصه مجازی نیز، با گسترش فناوری های دیجیتال و قدرت گرفتن شرکت های چند ملیتی، مفهوم حاکمیت دستخوش تغییرات جدی شده است و کیفیت این تغییرات به گونه‌ای است که زمینه را برای شکل‌گیری بحث و چالش میان گفتمان‌های سیاسی، اقتصادی و اجتماعی مختلف فراهم می‌کند (جارویس[5]، ۲۰۲۶؛ وودز[6]، ۲۰۲۳؛ زوباف[7]؛ ۲۰۱۵، ۲۰۱۹).

حاکمیت اساسا به دنبال رهبری یکتا و استقرار قدرتی واحد و بدون خدشه در فرایند تصمیم‌گیری، برقراری و حفظ نظم در داخل یک کشور است (بریتانیکا[8]، ۲۰۲۶؛ کوتور و توپین[9]، ۲۰۱۹). یکی از صورت های استقرار این رهبری واحد، کنترل حاکمیت بر منابع خود است که در طول تاریخ چه در عرصه حقیقی ، چه در عرصه مجازی همواره در میانه کشاکش بازی قدرت نقش‌آفرینان بین‌المللی بوده است (مورگنشا[10]، ۲۰۰۶، ص۱۲۴؛ روپرت و همکاران[11]، ۲۰۱۷؛ اسلاتر و مک‌کورمیک[12]، ۲۰۲۱). زیست امروزی ما در مقایسه با دهه‌ها و حتی سده‌های گذشته به دلیل ظهور نوع جدیدی از دارایی دستخوش تغییرات عظیمی شده است (آلیمو و کالینیکوس[13]، ۲۰۲۴؛ لو[14]، ۲۰۲۱؛ بیگو و همکاران[15]، ۲۰۱۹؛ پیچی‌یانو[16]، ۲۰۱۵). شرکت‌های عظیم فناور، مدل درآمدی خود را بر مبنای این دارایی جدید تعریف کرده و قدرت‌های بزرگ در راستای عینیت‌بخشی به اهداف اقتصادی، سیاسی، اجتماعی و ژئوپلیتیکی خود قالب و بستری جدید جهت بهره‌برداری از آن فراهم ساخته‌اند. استعمار نوین، با وجود اینکه مانند استعمار کهن بر مبنای ۴ اصل اکتشاف، گسترش، استثمار و نابودی عمل می کند (مخیاس و کلدری[17]، ۲۰۲۴)، اما به دنبال شکل‌دهی به نوع جدیدی از نظم اجتماعی است. پیامدهای عدم مقاومت در برابر استعمار داده به‌صورت خزنده و آرام گسترش می‌یابد که در میان‌مدت آثار چنین پدیده‌ای ناگوار و غیرقابل‌بازگشت خواهد بود.

در چنین بستری، پرداختن به حاکمیت دیجیتال بیش‌ازپیش اهمیت یافته و عدم توجه به آن می‌تواند همگان را تحت تاثیر خود قرار دهد (فلوریدی[18]، ۲۰۲۰). منظور از حاکمیت دیجیتال، ظرفیت جامعه و یا دولت برای تعریف، حکمرانی[19]، اعمال قدرت و کنترل فناوری‌ها، داده و زیرساخت‌های ضروری برای خودمختاری[20]، خلاقیت، تنوع فناوری[21] و توسعه اجتماعی-فنی مبتنی بر ارزش‌های خود

1. Sovereignty
2. Council on Foreign Relations
3. de Luca
4. George
5. Jarvis
6. Woods
7. Zuboff
8. Britannica
9. Couture & Toupin
10. Morgenthau
11. Ruppert et al.
12. Slaughter & McCormick
13. Alaimo & Kallinikos
14. Liu
15. Bigo et al.
16. Picciano
17. Mejias & Couldry
18. Floridi
19. Govern
20. Self-Determination
21. Technodiversity

است (شیاوی و همکاران[۲۲]، ۲۰۲۵؛ پوله و تیل[۲۳]، ۲۰۲۰). چنین ظرفیتی خود را در قالب تلاش دولت ها برای مقابله با خروج اطلاعات زندگی خصوصی شهروندان و داده های حساس دولتی، توسعه فناوری های بومی و ملی، محلی سازی و کنترل جریان داده، نرم‌افزار و سخت‌افزار، استانداردها و پروتکل‌ها، فرایندها و خدمات، زیرساخت، قانون‌گذاری و محدودسازی دسترسی به فضای مجازی نشان داده است (فلوریدی ، ۲۰۲۰؛ کوتور و توپین، ۲۰۱۹).

در اینجا، منظور از «کنترل»، توانایی تأثیرگذاری (مانند وقوع، خلق و یا تخریب آن) بر یک عنصر و پویایی‌های آن (مانند رفتار، توسعه، عملکرد و تعاملات آن) است که شامل قابلیت بررسی و اصلاح هرگونه تخطی و انحراف از چنین تأثیری است (فلوریدی ، ۲۰۲۰). از این منظر، «کنترل» می‌تواند درجات مختلفی داشته باشد و فراتر از آن، می‌تواند تجمیع یا منتقل شود.

نبرد برای حاکمیت دیجیتال، کشمکشی مهم میان گروه‌های مختلف است که در طی آن اتحاد و تعارضات گوناگون بر مبنای منافع و فرصت‌ها شکل می‌گیرد. آشکارترین نوع این هماوردها، رویارویی شرکت‌های چندملیتی با دولت‌ها و عدم تقارن‌های موجود میان این دو بازیگر است. از یک سو بنگاه‌ها عهده‌دار طراحی، تولید، فروش و نگهداری فضای دیجیتال‌اند که به‌خودی‌خود قدرت و کنترل بالایی را برای آنها به ارمغان آورده (کرونین[۲۴]، ۲۰۲۳؛ کمپس[۲۵]، ۲۰۲۳؛ سیناتو[۲۶]، ۲۰۲۴؛ مخیاس و کلدری، ۲۰۲۴) و از سوی دیگر، دولت‌ها از قدرت تنظیم‌گری و قانون‌گذاری حوزه دیجیتال برخوردارند که چنین امکانی شکلی قدرتمند از کنترل رایانیکی[۲۷] را به ارمغان می‌آورد (اگیون و همکاران[۲۸]، ۲۰۲۳).

اصولا سپهر اطلاعات[۲۹] یک قلمرو فیزیکی به‌حساب نیامده و داده مانند نفت و سایر منابع سنتی، منبعی محدود، کمیاب، رقابتی، طبیعی و تجدیدناپذیر نیست. دارایی‌های دیجیتال، اغلب خصوصی[۳۰] و تابع نیروهای بازار بوده و نمایه‌هایی که از ما ساخته می‌شود تنها تحت مالکیت و بهره‌برداری دولت‌ها نیست؛ بلکه شرکت‌های چندملیتی با ماهیت جهان‌گرایی خود نیز از این امتیاز برخوردارند (فلوریدی، ۲۰۱۴، ۲۰۲۰). با توجه به تمام پیچیدگی‌های ذکر شده و تاکید اصول روابط بین‌الملل بر حاکمیت مستقل کشورها، کماکان با نقض مکرر و تزلزل این اصل در دو ساحت حقیقی و مجازی طرف هستیم. با حرکت دولت‌ها به سمت حاکمیت دیجیتال، سؤال اصلی آن است که در مواجه با این نقض ها و تزلزل ها، پاسخ کشورها چگونه است؟

در این مقاله و با کمک روش مرور روایت، ابتدا به‌صورت اجمالی مفهوم حاکمیت در بستر تاریخی، مفهوم‌پردازی و هستی‌شناسانه بررسی و در بخش بعد نمود این حاکمیت در عرصه دیجیتال بررسی خواهد شد. در این بخش سه باور غالب نسبت به حاکمیت (دولتی، عامه وشرکتی) معرفی شده و رویکرد برخی از کشورها نسبت به آن مطرح خواهد شد. در بخش بعد، نمود این مفهوم در قالب حاکمیت داده بررسی و به بحث حاکمیت قوی ، ضعیف و

22. Schiavi et al.
23. Pohle & Thiel
24. Cronin
25. Kamps
26. Sainato
27. Cybernetic
28. Aghion et al.
29. Infosphere
30. https//:aithority.com/technology/analytics-۸۳/of-your-data-is-held-by-companies-you-probably-dont-know-average-persons-data-held-by-۳۵۰-brands/

وجوه مختلف حاکمیت داده (کنترل، خودگردانی، ادراک آگاهانه، حریم خصوصی، مالکیت، امنیت، پذیرندگی و مسئولیت) اشاراتی خواهیم داشت. در انتها به مفهوم کنترل به‌عنوان یکی از اصلی‌ترین بنیان‌های حاکمیت می‌پردازیم.

مبانی نظری

فن-ملی‌گرایی

فن-ملی‌گرایی[۳۱] نوعی از اندیشه رقابتی سازمان‌یافته است که تبادلات فرامرزی فناورانه را به‌صورت مستقیم به امنیت ملی یک کشور متصل می‌کند. این رویکرد مروج مداخلهٔ قوی و جدی دولت در مقابل کشورهای فرصت‌طلب یا متخاصم و همچنین سایر بازیگران غیردولتی سایر کشورهاست (مور[۳۲]، ۲۰۱۹؛ ساکس[۳۳]، ۲۰۲۰). در فن-ملی‌گرایی، رهبران کشورها به‌دنبال کسب برتری های ژئوپلیتیک اند؛ چراکه باور دارند جهان وارد دورهٔ جدیدی شده است. در این جهان نو، رقابت سازمان یافته‌ای میان قدرت‌های ژئوپولیتیک شکل‌گرفته است. رقبایی که ارزش‌های ایدئولوژیک، نظام‌های سیاسی و مدل‌های اقتصادی اساساً متفاوتی دارند (فرل و نیومن[۳۴]، ۲۰۱۹؛ گارسیا – هررو[۳۵]، ۲۰۱۹). این دکترین بر این مبنا استوار است که قدرت‌های رقیب به‌دنبال اعمال سازوکارهای مبتنی بر فناوری هستند که استانداردهای کاملاً متفاوتی در حوزه‌های امنیت داده، نظارت و مراقبت و مالکیت فکری را اجرا و تقویت می‌کنند (کاپری[۳۶]، ۲۰۲۰؛ لگرین[۳۷]، ۲۰۲۰). استفاده از فناوری به‌عنوان ابزاری برای رشد اقتصادی، به‌عنوان یکی از پیشران های دیدگاه فن-ملی‌گرایی مطرح است؛ چراکه امنیت اقتصادی بخشی از امنیت ملی یک کشور را شکل می‌دهد (دیناردیس[۳۸]، ۲۰۱۵؛ اونت[۳۹]، ۲۰۱۹). به همین دلیل رقابت فناورانه، مانند کنترل استانداردهای فناورانه، به‌عنوان بخشی کلیدی از «رقابت قدرت بزرگ[۴۰] » قابل‌طرح است (مور، ۲۰۱۹). به همین دلیل کشورها به‌دنبال فناوری‌های پیشرفته‌ای مانند هوش مصنوعی، پردازش کوانتومی، کلان داده، رباتیک، شبکه‌های نسل پنج، اینترنت اشیا و زیست‌شناسی مصنوعی[۴۱] و غیره هستند تا به کمک آن‌ها نسل بعدی قدرت نظامی، صنعتی و اطلاعاتی را شکل دهند (دیناردیس، ۲۰۱۵؛ راجان[۴۲]، ۲۰۱۸).

فن-جهانگرایی

در رویکرد فن-جهانگرایی، فناوری به عنوان عامل تبدیل جهان به دهکده جهانی معرفی می‌شود. تصور برخاسته از مدل رشد اقتصاد نئوکلاسیک به طور مشخص بر مبنای رویکرد فن-جهانگرایی بنا

31. Techno Nationalism
32. Moore
33. Sachs
34. Farrell & Newman
35. Garcia-Herrero
36. Capri
37. Legrain

38. DeNardis
39. Evenett
40. Great power competition
رقابت قدرت بزرگ شامل کشورهای رقیبی با سطح منافع، نفوذ و تاثیرگذاری جهانی می شود که با هدف تبدیل شدن به بازیگری برجسته و سرآمد در سیاست بین‌المللی با یکدیگر رقابت می کنند
Costa ,D ,2022) .October .(13 Great power| Definition ,Meaning ,Government & ,India .Encyclopedia Britannica .https//:www.britannica.com/topic/great-power

41. synthetic biology
شاخه‌ای از علم است که در آن ارگانیسم‌ها برای اهداف مفیدی بازطراحی شده و به منظور اکتساب قابلیت های جدید مهندسی می‌شوند
42. Rajan

شده بودند. در این رویکر تصور می‌شد که فناوری به صورت رایگان و ورای مکان و ملیت در اختیار همگان قرار دارد (ریکپ و لاندوال[43]، ۲۰۲۱، ص. ۱۵۵). از این منظر ملت‌ها (که از منظر این رویکرد به عنوان یک سازمان منسوخ شده تصور می‌شوند) در بهترین حالت به عنوان یک محمل و بستر موقت برای فعالیت نیروهای فن-جهانگرایی عمل می‌کنند و به دلیل جهانی شدن فناوری‌های جدید محکوم به زوال و نابودی‌اند (استری و نلسون[44]، ۱۹۹۵؛ اجرتون[45]، ۲۰۰۷). این رویکرد بر توسعه سریع و جهان‌گیر فناوری (فناوری‌های دیجیتال، اتصالات اینترنتی و سیستم‌های ارتباطی) و افزایش تجارت بین‌المللی و نقش‌آفرینی گسترده‌تر شرکت‌های چندملیتی و نقش آن در نابودی مرزهای ملی متمرکز بوده و هدف خود را در قالب جامعه جهانی به هم پیوسته بیان می‌کند (مونترزو[46]، ۲۰۰۱؛ استری و نلسون، ۱۹۹۵، ص. ۷۹- ۸۰).

حاکمیت

در علوم سیاسی، منظور از حاکمیت، سرپرستی مطلق یا به‌عبارتی قدرت یکتا و بدون خدشه در فرایند تصمیم‌گیری و برقراری و حفظ نظم در داخل یک کشور است (بریتانیکا، ۲۰۲۶). اما در عرصه دیجیتال نمود این حاکمیت در مواجه با ذینفعان به گونه دیگری رقم می‌خورد و مبنای مناقشات مختلفی میان این ذینفعان (دولت-ملت‌ها، بنگاه‌ها، گروه‌های اجتماعی و شهروندان) شده است (پوله[47]، ۲۰۲۰؛ پوله و تیل، ۲۰۲۰). از منظر دولت-ملت‌ها حاکمیت به عنوان یک ویژگی و خصیصه مختص آنها تعریف می شود. خااستگاه این دیدگاه از کنترل انحصاری دولت‌ها بر یک قلمرو مشخص و برابری همه دولت‌ها در قوانین بین‌المللی و پایبندی به عدم مداخله در امور داخلی کشورها سرچشمه می‌گیرد (سانتانیلو[48]، ۲۰۲۵). در مواجه با چنین رویکرد دولت محوری، منتقدان بیان می‌کنند که اعمال قوانین و هنجارهای حاکمیت در حکمرانی فضای دیجیتال نه تنها صحیح نبوده بلکه حکمرانی نهادهای فراملی در بخش خصوصی را تهدید می‌کند (مولر[49]، ۲۰۱۹). از سوی دیگر با قدرت گرفتن شرکت‌های عظیم فناور در سطح بین‌المللی مفهوم حاکمیت سکوها[50] و شرکت‌ها[51] مطرح می‌شود که قدرت خود را بر فضای مجازی و مرزهای مجازی آن اعمال می‌کنند که نیاز به شکل جدیدی از حاکمیت دیجیتال را طلب می‌کند (کوهن[52]، ۲۰۱۷؛ فلوریدی، ۲۰۲۰).

حاکمیت دیجیتال و داده

زمانی که از حاکمیت دیجیتال صحبت به میان می آید، منظور توانایی یک ملت، سازمان و حتی یک فرد برای اعمال کنترل بر سرنوشت دیجیتال خود است. هدف از اعمال حاکمیت اطمینان از حفظ خودگردانی[53] بر داده‌ها، زیرساخت و فناوری در مواجه با وابستگی روزافزون به شرکت‌های فناور خارجی است. تمرکز این رویکرد بر کاهش وابستگی به این شرکت‌ها و ترویج امنیت، حریم خصوصی، انطباق با مقررات و تقویت توانمندی‌های بومی دیجیتال و نوآوری است (شوماکر و کرک[54]، ۲۰۲۵). حاکمیت دیجیتال، ظرفیت جامعه و یا دولت برای

43. Rikap & Lundvall
44. Ostry & Nelson
45. Edgerton
46. Montresor
47. Pohle
48. Santaniello
49. Mueller
50. Platform Sovereign
51. Corporate Sovereignty
52. Cohen
53. Autonomy
54. Schoemaker & Kirk

تعریف، حکمرانی[55]، اعمال قدرت و کنترل فناوری‌ها، داده و زیرساخت‌های ضروری برای خودمختاری[56]، خلاقیت، تنوع فناوری[57] و توسعه اجتماعی-فنی مبتنی بر ارزش‌های خود است (اسکیاوی و همکاران[58]، ۲۰۲۵؛ پوله و تیل، ۲۰۲۰). در اقتصاد داده و از بعد مفهوم‌پردازی، زمانی که از حاکمیت داده صحبت می‌کنیم به قابلیت فراهم‌آور داده برای کنترل داده اشتراک گذاشته شده صحبت می‌کنیم (عباس و همکاران[59]، ۲۰۲۴). از منظر حاکمیت داده، داده دیجیتال تابع قوانین و ساختار حکمرانی کشور و یا منطقه‌ای است که در آن جمع‌آوری و یا نگهداری می‌شود (فلیندرز و اسمالی[60]، ۲۰۲۴).

روش شناسی

مرور روایت[61] به عنوان یکی از روش‌های ترکیب[62] دانش، از سنت پژوهشی متمایزی نشات گرفته و قرابت بیشتری با پارادایم های سوبژکتیویست و تفسیرگرایی دارد (سوکرا[63]، ۲۰۲۲؛ گرین و همکاران[64]، ۲۰۱۸). هرچند این روش به عنوان رویکردی غیر سیستماتیک از سوی منتقدان آن معرفی می‌شود، لیکن اهمیت بالای آن در حوزه های پژوهشی و آموزشی علوم اجتماعی و انسانی امری اثبات شده است (سوکرا، ۲۰۲۲؛ گرین و همکاران، ۲۰۱۸). اگر در روش مرور نظام مند، پژوهشگر به دنبال تمرکز بر یک سوال مشخص در یک زمینه مشخص و با روشی از پیش تعریف شده برای ترکیب یافته های مطالعات مشابه است؛ در روش مرور روایت، پژوهشگر به دنبال پوشش دادن طیف گسترده تری از مطالعات بوده تا بتواند خلاصه ای کلی همراه با تفسیر و نقد خود از منابع را ارائه کند (گرگوری و دنیس[65]، ۲۰۱۸). گرچه در مواردی می‌توان مرور نظام‌مند را به عنوان رویکردی ایده‌آل برای پاسخ به برخی پرسش های مشخص مطرح نمود اما فقدان تأمل انتقادی متفکرانه و تفسیری می‌تواند منجر به ارائه نتایجی تهی از معنا، گمراه‌کننده و بالقوه مضر شود (سوکرا، ۲۰۲۲).

بر خلاف رویکرد مرور نظام‌مند، مرور روایت زمینه را برای ترکیب دیدگاههای مختلف فراهم کرده و مرور را بر مبنای دیدگاه منحصر به فرد پژوهشگر شکل می دهد. به همین دلیل بینش های حاصل از این دو روش با یکدیگر متفاوت خواهند بود چرا که مرور روایت تابع زمینه فردی، سازمانی و یا تاریخی انجام مرور است. سه مدل متداول از انواع مختلف مرور روایت شامل به روزترین[66]، انتقادی و یکپارچه است (سوکرا، ۲۰۲۲).

هدف مرور روایت، می‌تواند توصیف وضعیت کنونی یک موضوع، ارائه بینش‌هایی در جهت پیشرفت آن، ارائه نظریات جدید و یا بررسی شواهد موجود از منظرهای متفاوت و غیرمعمول باشد. بنابراین، بهره‌گیری از این روش از جهت توجه به حوزه هایی که کمتر به آنان پرداخته شده و نیز ارائه بینش های نو و روش تفکر جدید در حوزه های توسعه یافته ، حائز اهمیت است. به همین دلیل انتخاب ما در نگارش این مقاله مدل بهروزترین بوده که در آن تلاش شده تا خلاصه ای از پژوهش های صورت

55. Govern
56. Self-Determination
57. Technodiversity
58. Schiavi et al.
59. Abbas et al.
60. Flinders & Smalley
61. Narrative review
62. Synthesis
63. Sukhera
64. Green et al.
65. Gregory & Denniss
66. State-Of-The-Art

گرفته در گذر زمان با هدف آگاهی بخشی و بر مبنای سوگیری پژوهشی مشخص- که بر مبنای جهان بینی نگارنده[۶۷] است- ارائه شود. در مدل بهروزترین، سه هدف اصلی دنبال می‌شود: اول، در حال حاضردرک ما نسبت به مفهوم مورد بحث (در پژوهش ما مفهوم حاکمیت مدنظر است) در چه موقعیتی قرار دارد؟ دوم، چطور به این موقعیت رسیده ایم؟ و در آخر به کدام سمت باید حرکت کنیم؟

شاید تصور انجام یک تحلیل نظام‌مند در این حوزه جذاب به نظر برسد؛ اما ما در این پژوهش به دنبال ارائه تحلیلی کیفی از مجموعه‌ای از منابع دست دوم و خاکستری در مورد طیف گسترده‌ای از برداشت‌ها و معانی مرتبط با مفهوم حاکمیت به صورت عام، و در بستر دیجیتال و داده به صورت خاص بوده‌ایم. اصل روش‌شناسانه‌ای که در این تحقیق مصراً به آن پایبند بودیم، انتخاب منابعی بود که به طور مشخص از واژه حاکمیت (در عنوان، چکیده و متن) در بستر دیجیتال و داده استفاده کرده باشند.

لذا این مقاله، یک مرور نظام‌مند و جامع بر تمام موارد منتشر شده در این حوزه نیست و به دنبال پیروی از رویکرد مرور روایتی است؛ که در آن به دنبال نشان دادن گستردگی کاربرد مفهوم حاکمیت به طور عام و نمود آن در بستر داده به طور خاص است. لذا این مقاله تلاشی برای بررسی مفهوم حاکمیت در برخی از مکتوبات و منابع انگلیسی‌زبان است که در طول مسیر پژوهش با آن برخورد داشته‌ایم. به‌منظور انتخاب این منابع، جست‌وجوی اولیه گسترده‌ای در مقالات، کتاب‌ها، و سایر مستندات با استفاده از پایگاه‌های استنادی متداول مانند اسکوپوس و گوگل اسکالر انجام گرفت. جست‌وجوی ما بر مبنای عبارات «حاکمیت[۶۸]»، «حاکمیت دیجیتال[۶۹]» و «حاکمیت داده[۷۰]» شکل گرفته است. همچنین با جست‌وجو در فضای مجازی، یک تصویر کلی از مطالبی که در خبرگزاری‌ها و جراید منتشر شده بود، بدست آمد. از طریق این فرایند، حدود ۲۰ سند شامل مقالات و کتاب‌های مرتبط به دست آمد. در جدول یک به دلایل انتخاب، محل انتشار، میزان ارجاعات و نوع این منابع اشاره شده است.

در مرحله بعد و پس از خلاصه نمودن منابع اولیه، منابع دیگری از طریق رویکرد نمونه‌گیری گلوله‌برفی به مجموع داشته‌های ما افزوده شد که مجموع اسناد را به عدد ۱۲۵ رساند.

کنکاشی پیرامون مفهوم حاکمیت

از بعد معرفت‌شناختی، واژه حاکمیت مفاهیم گوناگونی داشته است. از منظر علوم سیاسی، حاکمیت به معنای سرپرستی مطلق و قدرت واحد و بدون خدشه در فرایند تصمیم‌گیری، برقراری و حفظ نظم در داخل یک کشور است (بریتانیکا، ۲۰۲۶؛ پوله و تیل، ۲۰۲۰). مفهوم حاکمیت به چهار صورت قابل‌درک است: اول حاکمیت داخلی[۷۱] است که به کنترل حقیقی یک قدرت سازمان‌دهی‌شده داخلی بر کل آن کشور اطلاق می‌شود. دوم حاکمیت به‌هم‌وابستگی[۷۲] است که کنترل حقیقی تحرکات موجود در مرزهای یک کشور را شامل می‌شود. سوم حاکمیت بین‌المللی و قانونی[۷۳] است

۶۷. مقاله حاضر طی مطالعات رساله دکتری نگارنده اول گردآوری و نگاشته شده است که طبعا قرابت بیشتری با جهان بینی او دارد.

68. Sovereignty
69. Digital Sovereignty
70. Data Sovereignty
71. Domestic Sovereignty
72. Interdependence Sovereignty
73. International Legal Sovereignty

جدول ۱: منابع اولیه پژوهش

	عنوان منبع	علت انتخاب	نویسندگان	محل انتشار	ارجاع	نوع منبع
۱	What does the notion of “sovereignty” mean when referring to the digital?	انتخاب این مقاله به دلیل رویکرد تحلیلی آن در بررسی کاربرد مفهوم حاکمیت در حوزه دیجیتال بوده است	Stephane Couture Sophie Toupin	New Media & Society	۵۹۹	مقاله
۲	The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU	انتخاب این مرجع به دلیل پاسخ به پرسش‌های کلیدی پیرامون حاکمیت دیجیتال بوده است. سؤالاتی نظیر چیستی این مفهوم و اهمیت آن	Luciano Floridi	Philosophy & technology	۵۹۷	نامه به سردبیر
۳	Data Sovereignty and Trade Agreements: Three Digital Kingdoms	انتخاب این مرجع به دلیل ارائه یک دسته‌بندی و صورت‌بندی سه‌گانه از حاکمیت داده و تلاش برای بررسی عمیق آن بوده است	Henry Gao	OUP USA	۳۰	فصل کتاب
۴	Data sovereignty: A review	یک مقاله مروری پر استناد که با رویکردی کمی به دنبال نگاشت ادراکات مختلف از مفهوم حاکمیت داده است	Patrik Hummel Matthias Braun Max Tretter Peter Dabrock	Big data & society	۵۵۱	مقاله
۵	The Rise of Data Politics: Digital China and the World	پرداختن به ابعاد پنهان سیاست داده و رویکرد کشور چین در رویکرد آن در حاکمیت داده	Lizhi Liu	Studies in comparative international development	۱۸۱	مقاله
۶	Data grab: the new colonialism of big tech and how to fight back	دو نویسنده کتاب به‌عنوان مبدعان مفهوم استعمار داده دیدگاه‌های خود را در مورد داده و نقش شرکت‌های بزرگ فناور در قالب نوع جدیدی از استعمار مطرح شده است	Ulises A. Mejias Nick Couldry	University of Chicago Press	۲۲۲	کتاب

	عنوان منبع	علت انتخاب	نویسندگان	محل انتشار	ارجاع	نوع منبع
۷	Digital sovereignty	نویسندگان در این مقاله به دنبال ردیابی باز تولید مفهوم حاکمیت دیجیتال به‌عنوان یک دسته‌بندی کلیدی در حوزه دیجیتال اند	Julia Pohle Thorsten Thiel	Internet Policy Review	۷۴۲	مقاله
۸	The Real Cyber War: The Political Economy of Internet Freedom	ارائه دیدگاهی ساختارشکنانه در مورد آزادی اینترنت و امپراتوری نظارت دولتی و شرکتی در کنار پرداختن به رویکردهای دولت‌ها برای استفاده از این بستر در راستای اهدافشان و توصیه به حاکمیت اطلاعات این کتاب را به‌عنوان یک منبع ارزشمند در این فهرست قرار داده است	Shawn M. Powers Michael Jablonski	University of Illinois Press	۲۸۳	کتاب
۹	Sovereignty: Organized Hypocrisy	یکی از پراستنادترین مراجع حوزه روابط بین‌الملل که به طور عمیق به مفهوم حاکمیت می‌پردازد	Stephen D. Krasner	Princeton University Press	۷۹۱۷	کتاب
۱۰	The age of surveillance capitalism: the fight for a human future at the new frontier of power	یکی از شناخته‌شده‌ترین مراجع مرتبط با سرمایه‌داری نظارتی که به طور ویژه به نقش شرکت‌های عظیم فناور و فرایند استخراج داده از جوامع می‌پردازد	Shoshana Zuboff	Profile Books	۲۵۹۶۰	کتاب
۱۱	Beyond control over data: Conceptualizing data sovereignty from a social contract perspective	پرداختن به مفهوم حاکمیت داده از منظر جامعه‌شناختی و بهره‌گیری از لنز قرارداد اجتماعی این مقاله را به‌عنوان اثری قابل‌توجه مطرح می‌کند	E. Abbas Thomas van Velzen H. Ofe G. Kaa Anneke Zuiderwijk M. D. Reuver	Electronic Markets	۵۱	مقاله
۱۲	Data sovereignty: The next frontier for internet policy?	توجه به اقتصاد داده و ماهیت چندوجهی حاکمیت داده علت انتخاب این منبع بوده است	Jonathon Hutchinson Milica Stilinovic Joanne E. Gray	Policy & Internet	۱۴	سرمقاله

	عنوان منبع	علت انتخاب	نویسندگان	محل انتشار	ارجاع	نوع منبع
۱۳	The Digital Innovation Race: Conceptualizing the Emerging New World Order	کتابی ارزشمند از نویسندگانی شناخته شده در حوزه سیاست علم‌وفناوری که در کنار مباحث کلیدی دیگر، داده را به‌عنوان یک دارایی عمومی چارچوب‌بندی می‌کنند	Cecilia Rikap Bengt-Åke Lundvall	Springer	۱۴۵	کتاب
۱۴	Data politics	پرداختن به سیاست داده و تأکید بر ایجاد ادراک صحیح نسبت نقش شهروندان و داده‌هایشان	Evelyn Ruppert Engin Isin Didier Bigo	Big data & society	۴۳۸	مقاله
۱۵	Data Is Power	می‌توان از پرداختن به داده به‌عنوان عامل قدرت آفرین برای کشورها و شرکت‌ها به‌عنوان نقطه قوت این مقاله نام برد	Matthew J. Slaughter David H. McCormick	Foreign Affair	*	مقاله
۱۶	Data Rules: Reinventing the Market Economy	این کتاب چارچوب جدیدی مبتنی بر علوم اجتماعی برای مطالعه بازسازماندهی اقتصادی و اجتماعی برخاسته از داده دیجیتال ارائه می‌کند	Cristina Alaimo Jannis Kallinikos	The MIT Press	۹۱	کتاب
۱۷	How Private Tech Companies Are Reshaping Great Power Competition	نقش شرکت‌های فناور در شکل‌دهی به رقابت قدرت‌های بزرگ است	Audrey Kurth Cronin	The Kissinger Center Papers	۱۶	مقاله
۱۸	Digital Sovereignty + Artificial Intelligence	در این منبع نویسنده تأثیر متقابل سیاست‌های حاکمیت دیجیتال بر توسعه هوش مصنوعی را بررسی می‌کند و پویایی میان این دو مفهوم را باتوجه‌به سه مورد کشورهای چین و ایالات متحده و مجموعه اتحادیه اروپا مورد مداقه قرار می‌دهد	Andrew Keane Woods	Oxford University Press	*	فصل کتاب

	عنوان منبع	علت انتخاب	نویسندگان	محل انتشار	ارجاع	نوع منبع
۱۹	Sovereignty | Definition, Characteristics, Types, History, & Facts	یکی از معتبرترین دانشنامه‌های موجود در جهان	Britannica Editor	Encyclopedia Britannica	*	دانشنامه
۲۰	Sovereignty	یکی از معتبرترین مراجع موجود که از سال ۱۹۹۵ شروع به کارکرده است	Dan Philpott	Stanford Encyclopedia of Philosophy	*	دانشنامه

که به‌رسمیت‌شناختن رسمی حاکمیت یک کشور توسط سایر کشورهای مستقل خواهد بود و در آخر، حاکمیت وستفالی[۷۴] است که بر مبنای آن هیچ قدرت دیگری در یک کشور به‌غیراز حاکمیت داخلی و مستقل آن وجود ندارد و به رسمیت شناخته نمی‌شود (کراسنر[۷۵]، ۲۰۰۱، ص. ۲۰). باآنکه سابقه استفاده از مفهوم حاکمیت به دوران روم باستان باز می‌گردد (هولیس[۷۶]، ۲۰۱۲) اما کاربرد امروزی آن ارتباط مستقیمی با مفهوم حکومت[۷۷] داشته و معمولاً با اندیشه مؤلفانی چون بودین[۷۸]، روسو[۷۹]، هابز[۸۰] و اشمیت[۸۱] مرتبط است. حاکمیت عموماً به‌عنوان مقام عالی مسلط بر یک ماهیت سیاسی (شیوه حکومتگری[۸۲]) تعریف می شود.

«حاکمیت» شکلی از قدرت است که مشروعیت و ماهیت کنترل‌کنندگی دارد. در شکل‌دهی به دوران مدرن اینکه چه کسی حق اعمال حاکمیت را دارد و چطور و بر روی چه چیزی و برای چه مقصودی از آن بهره می‌برد، نقش داشته ، حایز اهمیت است. امروزه می‌توان اعمال قدرت کنترلی دولت‌ها بر قلمرو، مردمان و منابع موجود در آن را حاکمیت ملی[۸۳] نامید (کراسنر، ۲۰۰۱، ص.۱۱؛ فلوریدی، ۲۰۲۰).

فیلپات[۸۴] (۲۰۱۶، ص.۳)، چهاراصل برای حاکمیت تعریف می‌کند: ۱) دارای قدرت و اختیار است ۲) این قدرت و اختیار برخاسته از نوعی منبع مشروعیت‌زاست که متقابلاً به رسمیت شناخته شده است ۳) این قدرت و اختیار برتر از هر نوع دیگر از قدرت است ۴) این قدرت در بستر یک قلمرو تعریف می‌شود. لازم به ذکر است که نباید مفهوم قلمرو را محدود به مرزهای سرزمینی در نظر گرفت؛ بلکه این مفهوم به منابع درون یک محدوده مانند زیرساخت‌های انسانی، فضای هوایی، دریایی و مواد معدنی زیر سطحی آن محدوده نیز گسترش می‌یابد (هولیس، ۲۰۱۲). البته امروزه این خوانش سنتی از مفهوم حاکمیت با ظهور توافقات منطقه‌ای و بین‌المللی، شرکت‌های چندملیتی، چالش‌های زیست‌محیطی مانند تغییرات آب‌وهوایی و دنیاگیری

74. Westphalian Sovereignty
75. Krasner
76. Hollis
77. State
78. Jean Bodin
79. Jean-Jacques Rousseau
80. Thomas Hobbes
81. Carl Schmitt
82. Polity

83. National Sovereignty
84. Philpott

بیماری‌ها و به طور مشخص ظهور زیرساخت‌های رادیویی و ارتباطی جهانی و اینترنت دچار چالش شده و به ویژه مفهوم حاکمیت در حوزه دیجیتال از جنبه‌های گوناگونی مورد بحث قرار گرفته است. منظور از مفهوم دیجیتال، تمامی فناوری‌ها، زیرساخت‌ها، داده و محتوایی است که بر مبنای استفاده از تکنیک‌های محاسبات الکترونیکی شکل گرفته‌اند (پیترز[85]، ۲۰۱۶، ص. ۹۴). در سالیان اخیر با رشد استفاده از مقوله حاکمیت در ترکیب با مفاهیمی چون «دیجیتال»، «داده» و «فناوری» و اقبال گروه‌های مختلف ذی‌نفع (دولت‌ها، جنبش‌های مردمی و...) به این مفاهیم، سه نوع باور نسبت به آن، شکل گرفته است (گائو[86]، ۲۰۲۳):

باور اول: حاکمیت دولتی

در دهه‌های گذشته، مفهوم حاکمیت دیجیتال مکررا توسط دولت ها مطرح شده و سه رویکرد کلیدی را دنبال می کند: اولا دولت ها باید اقتدار ازدست رفته خود بر اینترنت را بازیافته و تثبیت کنند؛ ثانیا، از شهروندان و کسب و کارهایشان در برابر چالش های گوناگون محافظت نمایند و ثالثا، به سمت خود مختاری[87] در سپهر دیجیتال حرکت کنند (پوله و تیل، ۲۰۲۰). اصول قلمروخواهی[88] و سلسله مراتب حاکمیت، علی الظاهر در مقابل منظومه شبکه دیجیتال جهانی و دگرگونی‌ها و پویایی زیرساخت های فنی اینترنت جهانی قرار دارد و این ویژگی‌ها به عنوان چالشی برای حاکمیت مطرح می شوند. به همین دلیل، دولت ها به سمت توسعه ابزارهای قانونی و فنی برای حل و فصل مناقشات پیرامون حاکمیت دیجیتال حرکت نموده و با گذشت زمان آنها را بهروزرسانی کرده اند (گلداسمیت و وو[89]، ۲۰۰۶).

اولین تلاش ها برای استقرار حاکمیت در فضای دیجیتال به کشور چین باز می‌گردد. این کشور با تلقی گفتمان لیبرال به عنوان خطری برای برای نظام سیاسی خود، از چنین رویکردهایی حمایت کرد (کریمرز[90]، ۲۰۱۶، ۲۰۲۰؛ جیانگ[91]، ۲۰۱۰، ژنگ و همکاران[92]، ۲۰۱۷). سایر کشورها مانند روسیه با الگوبرداری از سیاست های چین، در این مسیر گام برداشتند(بودنیتسکی و جیا[93]، ۲۰۱۸؛ استادنیک[94]، ۲۰۱۹؛ نوستی[95]، ۲۰۱۵). علی‌رغم وجود برخی تفاوت‌ها میان رویکردهای این دوکشور (بوردرز و همکاران[96]، ۲۰۱۹؛ سیگال[97]، ۲۰۲۰)، شاکله اصلی سیاست‌های آنان بر مبنای مشترک مقابله با نفوذ و تاثیر ایالات متحده بوده است (وی[98]، ۲۰۱۶). نمود این همکاری در شکل گیری انجمن های بین المللی موازی مانند گروه کاری باز برای امنیت سایبری[99] در سازمان ملل (باسو و همکاران[100]، ۲۰۲۱) و همراستایی در سوابق رای این دو کشور در مسائل کلیدی حقوق بین‌الملل مانند مخالفت با کنوانسیون بوداپست به دلیل نقض حاکمیت کشورها از طریق ایجاد دسترسی فرامرزی به داده های مرتبط با

85. Peters
86. Gao
87. Autonomy:
دارا بودن استقلال و در دست داشتن سرنوشت خود
88. Territoriality

89. Goldsmith & Wu
90. Creemers
91. Jiang
92. Zeng et al.
93. Budnitsky & Jia
94. Stadnik
95. Nocetti
96. Broeders et al.
97. Segal
98. Wei
99. The Open-Ended Working Group) OEWG(On Cybersecurity
100. Basu et al.

تحقیقات جرائم سایبری برای سرویس‌های اطلاعاتی قابل مشاهده است (کوروفسکا[۱۰۱]، ۲۰۲۰).

در سوی دیگر، کشور های بلوک غرب از منظری دیگر به حاکمیت دیجیتال پرداخته اند. عمده انگیزه این کشورها ، نگرانی های امنیتی و تلاش آنها برای حفظ استقلال و کنترل در فضای دیجیتال و به خصوص در حوزه زیرساخت بوده است (نیسنباوم[۱۰۲]، ۲۰۰۵؛ هانسن و نیسنباوم[۱۰۳]، ۲۰۰۹).

توجه به مسئلهٔ حاکمیت و عدم تقارن قدرت به‌عنوان عوامل کلیدی خروجی‌های سیاستی از اهمیت ویژه‌ای برخوردارند. از منظر کشورهای جهان جنوب[۱۰۴]، پیش‌نیاز توسعه، استقرار دولتی است که از ظرفیت اجرایی بالا و توانمندی اعمال قانون برخوردار باشد تا بر مبنای این ظرفیت‌ها بتواند فرایند استخراج دانش شرکت‌های بزرگ فناور را محدود کند. در غیر این صورت، آثار مثبت سرمایه‌گذاری‌های داخلی در حوزهٔ دانش، تضعیف خواهد شد (ریکپ و لاندوال، ۲۰۲۱).

از منظر ملی‌گرایی، تمام ملت‌ها حق حکمرانی بر خود را دارند و باید از گزند مداخلات هر عامل خارجی آزاد و در امان باشند. در بلندمدت، این رویکرد به دنبال ایجاد و حفظ یک هویت واحد ملی مبتنی بر خصوصیات مشترک اجتماعی مانند فرهنگ، قومیت، سیاست، مذهب یا سنت‌ها بر بستر تاریخی واحد و مشترک است و ترویج وحدت ملی و یکپارچگی به‌عنوان یکی از اهداف کلیدی پیگیری می‌شود (اسمیت[۱۰۵]، ۲۰۱۳). توجه به این نکته ضروری است که به باور طرفداران ملی‌گرایی، حاکمیت ملی زمانی به خطر می‌افتد که حقوق و قدرت تنظیم‌گری داخلی و کنترل یک دولت مستقل به‌وسیله دست‌اندازی یک هویت-عامل-خارجی نقض شود. ابعاد آزادی و ملی‌گرایی کماکان در عرصه حاکمیت دیجیتال با تمرکز بیشتر بر کنترل داده مطرح است. نمود اصلی کنترل داده در تلاش دولت ها برای محلی سازی داده[۱۰۶] نمایان می‌شود که در آن دولت ها تلاش می کنند تا ذخیره سازی، حرکت و یا پردازش داده را به محدوده های فیزیکی و یا قانونی مشخصی محدود کنند (پوله و تیل، ۲۰۲۰؛ پاندی و ملکوم[۱۰۷]، ۲۰۱۸؛ سلبی[۱۰۸]، ۲۰۱۷).

باور دوم: حاکمیت بنگاهی

از ابتدای قرن بیست‌ویکم، شاهد ظهور نوعی از حاکمیت دیجیتال بنگاهی غیررسمی بوده‌ایم. طرف‌داران این نوع از حاکمیت دیجیتال به خودتنظیم‌گری بنگاه‌ها اعتقاد داشته و آن را کافی می‌دانستند و لذا مداخلات قانونی را غیرضروری و ناخوشآیند برمی‌شمردند. از این منظر هرگونه بازبینی و متعادل‌سازی قدرت دیجیتال بنگاه‌ها تابع رقابت، اقتصاد رها[۱۰۹] و تعادل مبتنی بر بازار است. حاکمیت دیجیتال در این دوران، مبتنی بر بنگاه و بر مبنای جایگاه هژمونیک و یا انحصار رسمی آنها بنا شده است. شرکت‌ها در این ساختار از هر دو جنبه قدرت ساخت و رایانیکی حوزه دیجیتال برخوردار بودند. در این دوران نقش افراد از رأی دهنده - مصرف کننده[۱۱۰] به پیرو - کاربر[۱۱۱] تغییر یافت.

101. Kurowska
102. Nissenbaum
103. Hansen & Nissenbaum
104. Global South
105. Smith

106. Data Localisation
107. Panday & Malcolm
108. Selby
109. laissez-faire
110. Voter-Consumer
111. Follower-User

با تغییر سازوکارهای ارزش‌گذاری شرکت‌ها و ظهور داده به عنوان یک دارایی ارزشمند و منبعی کلیدی در فعالیت این شرکت‌ها، شاهد قدرت‌گرفتن بیش‌ازپیش این شرکت‌های بزرگ فناور هستیم. در چنین وضعیتی با یک تمرکز قدرت اقتصادی مواجهیم که طبیعتاً به تمرکز قدرت سیاسی در دست این شرکت‌ها یعنی حق حاکمیت مردم از آنان گرفته و به این بنگاه‌ها منتقل شده است. توانایی این بنگاه‌ها در دیکته‌کردن مقررات، اعمال قدرت، تغییر جغرافیای یک بخش از صنعت و القای ترس، همگی مبین قدرت یک دولت خصوصی است (خانال و همکاران[۱۱۲]، ۲۰۲۵؛ بوردلان[۱۱۳]، ۲۰۲۴؛ صدیق[۱۱۴]، ۲۰۲۵).

در دورانی که جهان واقعی به طور فزاینده‌ای تحت‌تأثیر و مدیریت دنیای دیجیتال است، لزوم استقرار حاکمیت اجتماعی - سیاسی در هر دو ساحت بیش‌ازپیش احساس می‌شود. چنین هدفی نیازمند تصمیم جدی کشورها در جهت برقراری این حاکمیت است، چرا که شاید بهترین پاسخ به کنترل بنگاه‌های چندملیتی بر عرصه دیجیتال، استقرار این حاکمیت در هر دو قالب رسمی و قانونی و عرصه غیررسمی نیز می‌باشد.

باور سوم: حاکمیت چندذینفعی

رویکرد سوم بر این باور است که تنظیم‌گری(کنترل) اینترنت ورای مرزهای ملت‌ها امتداد می‌یابد و به همین دلیل خارج از حاکمیت دولت‌ها قرار می‌گیرد. این نظر در بیانیه مشهور جان پری بارلو[۱۱۵] در سال ۱۹۹۶ تحت عنوان « بیانیه استقلال فضای مجازی»نمود یافته است:

«دولت‌های دنیای صنعتی، ای غول‌های خسته، من از فضای مجازی آمده‌ام، خانه جدید ذهن. به نمایندگی از آینده، من از شما نمایندگان گذشته می‌خواهم که ما را تنها بگذارید. شما میهمان ناخواسته‌ای هستید که دیگر در جایی که ما گرد هم می‌آیم حاکمیت ندارید.»

این بیانیه به پیشرفت ایده فضای مجازی به عنوان فضایی مستقل که بدون تنظیم‌گری دولت‌ها ظهوریافته و باید مستقل از حاکمیت و دخالت دولت‌ها عمل کند، کمک شایانی کرده است. از این منظر حاکمیت فضای مجازی به‌عنوان نقطه مقابل حاکمیت دولت تفسیر می‌شود.

خوانش‌های امروزی این مفهوم مانند تفسیری که مولر[۱۱۶] (۲۰۱۷) تحت عنوان «حاکمیت عامه در فضای مجازی» ارائه می‌دهد؛ این ایده را مطرح می‌کند که عاملان اصلی حاکمیت فضای مجازی، دولت - ملت‌ها نبوده و باید مردمی باشند که در آن زیست می‌کنند. البته مدل مولر مبتنی بر مشارکت چند ذی‌نفعی است که در آن نهادهای چند ذی‌نفعی به‌عنوان جایگزینی برای دولت‌های ملی عمل می‌کنند و از جنبه‌هایی به‌عنوان رقیب مستقیم حاکمیت مطلق دولت‌ها بر سیاست عمومی در بخش اطلاعات و ارتباطات مطرح می شوند.

از سال ۲۰۰۳ چند ذینفع‌گرایی[۱۱۷] در غالب هماهنگی میان بخش خصوصی، بازیگران غیرانتفاعی و متصدیان بخش دولتی به‌عنوان نقطه کانونی مباحث پیرامون حاکمیت اینترنت مطرح شده است.

112. Khanal et al.
113. Bordelon
114. Siddique
115. John Perry Barlow) A declaration of the independence of cyberspace ,2018) .April.(8 Electronic Frontier Foundation .https//:www.eff.org/cyberspace-independence(
116. Mueller
117. Multistakeholderism

مشخصا ایالات متحده گفتمان چند ذینفع‌گرایی را به عنوان نقطه آغازین هرگونه بحث پیرامون حکمرانی اینترنت بکار گرفته است. اما در عرصه عمل صحنه به گونه دیگری رقم می‌خورد. سیاستگذاران این کشور به دنبال حفظ کنترل خود بر مدیریت اینترنت در داخل ایالات متحده هستند[۱۱۸]. به همین دلیل هرگونه جابه‌جایی در این حق به‌عنوان تضعیف حاکمیت ایالات متحده تصور می شود[۱۱۹]. در سال ۲۰۱۴، اداره ملی اطلاعات و مخابرات[۱۲۰] با اعلام قصد مشروط خود برای واگذاری حق نظارت بر سامانه نامگذاری دامنه[۱۲۱] رویکرد خود را به توسعه نظامی از سازوکارهای چندذینفعی (تاسیس نهادهای گوناگون در لایه‌های مختلف حکمرانی) و مبتنی بر منافع اقتصادی و سیاسی بازیگران ریشه‌دار این عرصه که عمدتاً خاستگاه آمریکایی دارند متوجه نمود (پاورز و جابلونسکی[۱۲۲]، ۲۰۱۵، ص. ۱۲۹-۳۰). همواره اعمال کنترل بر مبادی و ریشه‌ها به عنوان راهبردی حیاتی برای اعمال قدرت مطرح است. در فرآیندهای چندذینفعی که به دنبال ایجاد اجماع میان بازیگران مختلف است؛ هر ذینفع راهکار پیشنهادی را علی‌رغم آن که ممکن است کاملا با علایق خود هماهنگ نباشد می‌پذیرد. اما در ساختار کنونی و با سلطه ایالات متحده و شرکت‌های چند ملیتی چنین هدفی برای عموم ذینفعان ممکن نخواهد بود[۱۲۳].

118. Congressman Robert Goodlatte(R-VA,) November ,2005 ,4 Washington ,D.C
۱۱۹. قطعنامه ۵۰ کنگره ایالات متحده، ۲۲ سپتامبر ۲۰۱۲
120.The National Telecommunications and Information Administration (NTIA)
121. The Domain Name System(DNS)
122. Powers & Jablonski
123. David Edmunds and Eva Wollenberg" ,A Strategic Approach to Multistakeholder Negotiations ",Development and Change,(2001) 32 :doi10.1111/1467-7660.00204 ,53–231

رویکرد کشورها در بحث حاکمیت دیجیتال

از منظر اقتصاد سیاسی، هر کدام از دو رویکرد «آزادی اینترنت» و «حاکمیت اطلاعات» در خدمت مشروعیت‌بخشی به‌نوعی از اقتصاد سیاسی خاص هستند: رویکرد آزادی اینترنت، به سود اقتصادهای غربی است و اهداف جهان‌گرایی را دنبال می‌کند (هگارت و جابلونسکی[۱۲۴]، ۲۰۱۷؛ شیلر[۱۲۵]، ۲۰۱۴). اما حاکمیت اطلاعات به دنبال حمایت از تلاش‌های دولت‌ها برای کنترل و اداره جوامع بسیار پیچیده در دنیایی است که برای ارتباطات بی‌وقفه جهانی طراحی شده‌اند (پاورز و جابلونسکی، ۲۰۱۵، ص. ۲۰۳). از منظر تاریخی، وابستگی میان بخش خصوصی و دولت، نهایتا به ضرر هر دو طرف خواهد بود؛ چرا که وابستگی دولت‌ها به تخصص‌های بخش خصوصی و ظرفیت عملیاتی آنان فرآیند تصمیم‌گیری در دولت را فاسد و محدود می‌کند که امر نهایتا امکان اعمال قانونی که مخالف تمایلات و منافع اقتصادی بخش خصوصی است را از سیاستگذار سلب می‌کند (پاورز و جابلونسکی، ۲۰۱۵، ص. ۲۰۵).

تلاش کشورهای مختلف برای برقراری حاکمیت در فضای مجازی مسبوق به سابقه بوده است:

- به‌عنوان نخستین گام در جهت مشروعیت‌زدایی از خوانش[۱۲۶] فراگیر و قدرتمند اهداف آزادی اینترنت ایالات متحده، پرداختن به انگیزه‌های نهان اقتصادی و ژئو - استراتژیک این کشور که به عنوان پیشران سیاست‌های اطلاعاتی آن عمل می‌کند، از اهمیت بالایی برخوردار است (پاورز و جابلونسکی، ۲۰۱۵، ص. ۲۰۵).

124. Haggart & Jablonski
125. Schiller
126. Rhetoric

- در اتحادیه اروپا انتقادات در زمینه نبود کنترل و استقلال در حوزه تکامل شبکه‌های دیجیتال از گذشته وجود داشته است. در میان سیاست‌گذاران اروپایی تمایل به ایجاد زمینه اقتصادی و قانونی برای نوآوری فناورانه در داخل مرزهای این اتحادیه بیش‌ازپیش احساس می‌شود (براوو[۱۲۷]، ۲۰۲۵؛ اچیکسون[۱۲۸]، ۲۰۲۵؛ کنافو[۱۲۹]، ۲۰۲۵). به باور گروهی از سیاست‌گذاران، حاکمیت دیجیتال به‌عنوان راهکاری برای مقابله با خروج گسترده اطلاعات زندگی خصوصی مردم اروپا و لزوم وجود راهکارهای ملی برای ذخیره داده‌های مردم و دولتها مطرح می‌شود (بلانژه[۱۳۰]، ۲۰۱۲).
- سابقه پرداختن به حاکمیت اینترنت در دو کشور چین و روسیه به سال ۱۹۹۸ باز می‌گردد. هر دو کشور با توسل به این گفتمان در پی مقابله با خوانش آزادی اینترنت ایالات متحده بودند. این موضوع به‌گونه‌ای برای این دو کشور حائز اهمیت بود که حاکمیت اینترنت، مفهومی ورای یک سیاست دیجیتال بوده و به نماد ملی آنان بدل شده است. با این رویکرد، هر دو کشور به دنبال تبلیغ و ترویج هویت ملی خود به‌عنوان یک قدرت بزرگ در عرصه بین‌المللی‌اند. حاکمیت دیجیتال دولتی فراتر از تعریف خشک شبه‌حقوقی آن یعنی حق و قدرت یک دولت بر قلمروی خود است. حاکمیت دیجیتال به‌عنوان صورتی از ملی‌گرایی که با هدف ترویج هویتی مشخص و یا چشم‌انداز ملی از فضای مجازی مطرح است (بودنیتسکی و جیا، ۲۰۱۸).
- دولت آلمان در راستای کسب کرسی ریاست شورای اروپا برنامه ای ارائه کرده که از قصد خود برای استقرار حاکمیت دیجیتال به عنوان یک موضوع کلیدی در سیاست دیجیتال اروپا خبر می دهد (دولت فدرال آلمان[۱۳۱]، ۲۰۲۰، ص. ۱۰). این کشور طی آخرین توافق ائتلافی میان احزاب حاکم خود، حاکمیت دیجیتال را به عنوان یکی از اهداف کلیدی خود مطرح نموده و با اتخاذ این سیاست دو اولویت را دنبال می‌کند: کاهش وابستگی به ارائه دهندگان خدمات دیجیتال غیر اروپایی و ترویج راهکارهای منطبق بر استانداردهای سختگیرانه عملکردی و امنیتی اتحادیه اروپا. هدف اصلی، ایجاد بوم‌سازگانی متشکل از ارائه دهندگان خدمات دیجیتال اروپایی در جهت ایجاد یک زنجیره ارزش قابل اعتماد است. چنین بوم‌سازگانی اعمال کامل سیاست حاکمیت دیجیتال را بر اساس استانداردهای اروپایی ممکن می‌کند (فیشر[۱۳۲]، ۲۰۲۵؛ بن‌سینگر و همکاران[۱۳۳]، ۲۰۲۵).
- دولت فرانسه در سال ۲۰۲۶، از دو ابتکار مکمل، رصدخانه حاکمیت دیجیتال و شاخص تاب‌آوری دیجیتال رونمایی کرد (وزارت اروپا و امور خارجه[۱۳۴]، ۲۰۲۶). رصدخانه حاکمیت دیجیتال وظیفه نگاشت وابستگی های این کشور و اتحادیه اروپا به فناوری های خارجی حوزه ابری، هوش مصنوعی و خدمات امنیت سایبری را برعهده داشته (هانی[۱۳۵]، ۲۰۲۶)، شاخص تاب‌آوری دیجیتال میزان وابستگی به خدمات و محصولات دیجیتال را اندازه‌گیری کرده و خطرات ناشی

127. Bravo
128. Echikson
129. Knafo
130. Bellanger

131. The German Federal Government
132. Fischer
133. Bensinger et al.
134. Miniśtère de l'Europe et des Affaires étrangères
135. Hani

از وابستگی به فناوری‌های خارجی را شناسایی خواهد کرد (هارتمن[۱۳۶]، ۲۰۲۶).

- کانادا چارچوب حاکمیت دیجیتال خود را در سال ۲۰۲۵ منتشر نمود. در این سند عوامل اثرگذار بر توانمندی دولت نظیر عوامل قانونی، امنیتی و غیره بررسی و چالش های پیش روی دولت برای برقراری حاکمیت دیجیتال برجسته شده است. به منظور پاسخدهی به این چالشها، راهکارهای قانونی، حوزه زنجیره تامین و کنترلهای فنی تقویت کننده دولت معرفی و بکار گرفته شده‌اند (دولت کانادا[۱۳۷]، ۲۰۲۵).

به‌عنوان جمع‌بندی این بخش ارائه دسته‌بندی کوتور و توپین می‌تواند راهگشا باشد که چندین تشابه و تفاوت میان کاربردها و برداشت‌های مرتبط با مفهوم حاکمیت دیجیتال را شناسایی کرده است:

- شباهت‌ها:

۱. عمدتاً به کنترل دولت بر فناوری اشاره دارد؛ ولی امروزه در سطوح دیگری (سازمان‌های جامعه مدنی، بومیان، افراد) بکار گرفته می‌شود.

۲. ایده کلی حاکمیت دیجیتال با مفاهیمی چون استقلال، کنترل و خودگردانی به دو صورت کاملا عام مرتبط است:

- ظرفیت کار جمعی (دولت‌ها، اجتماعات، حرکت‌های اجتماعی و غیره) برای نوآوری و/ یا مشارکت در توسعه فناورانه
- امنیت و/یا حریم خصوصی افراد و جمع‌ها و ارتباط آن با مالکیت و کنترل بر داده مرتبط با اشخاص، شهروندان و یا دولت‌ها

۳. استفاده از مفهوم حاکمیت کارایی بلاغی[۱۳۸] نیز دارد. مشخصاً به نظر می‌رسد که این مفهوم به‌عنوان نشانه‌ای برای مقابله با انواع مختلف سلطه‌گرایی بکار می‌رود.

۴. در بسیاری از موارد حاکمیت دیجیتال به‌عنوان ایده مخالف سلطه ایالات متحده بر اینترنت مطرح می‌شود. شکل امروزی کاربرد این مفهوم در تقابل باقدرت شرکت‌های فناور خصوصی مانند گوگل، متا، اپل، مایکروسافت، ایکس و... نمود پیدا می‌کند.

۵. به نظر می‌رسد که حاکمیت دیجیتال برای مفهوم‌پردازی برساخت یا دیدگاه‌های جایگزین و ضدسلطه مطرح می‌شود.

- تفاوت‌ها:

به دلیل تأثیر تفکرات و تبلیغات رقیب در کشورهای ضد سلطه ، شکافی میان تعریف حاکمیت و جامعه مدنی در تفسیر حاکمیت دیجیتال مشاهده می‌شود. به‌عنوان‌مثال در چین، دولت از این مفهوم برای تأکید بر مشروعیت خود در کنترل و پایش داده و شبکه بهره می‌گیرد. برخی از حرکت‌های اجتماعی نیز از مفهوم حاکمیت فناورانه برای محافظت از خود در برابر نظارت دولت‌ها و بخش تجاری استفاده می‌کنند.

در ادامه به رویکرد حاکمیت داده به‌عنوان یکی از اجزا حاکمیت دیجیتال می‌پردازیم. توجه به این موضوع از این جهت حائز اهمیت است که در دنیای امروز داده از جایگاه بسیار ویژه‌ای در سیاست‌های کلان کشورها برخوردار و در عصر هوش مصنوعی توجه به جایگاه آن می‌تواند بسیار راهگشا باشد.

136. Hartmann
137. The Government of Canada) GC(
138. Rhetoric

حاکمیت داده، مفهومی در امتداد حاکمیت دیجیتال

داده به عنوان یکی از ارزشمندترین دارایی‌های دولت و بنگاه‌ها مطرح است (پاینده، ۱۴۰۳؛ دهقان‌پور فراشاه و دهقان‌پور فراشاه، ۱۴۰۳؛ اکبری و همکاران، ۱۴۰۳) که متأسفانه هنوز، درک محدودی نسبت به تأثیرات آن در بازطراحی ارتباطات اقتصادی، ژئوپلیتیکی و امنیتی بین‌الملل وجود دارد. در عصر داده، کشورها بر بستر فناوری‌های گوناگون، حجم عظیمی از داده را تولید می‌کنند[۱۳۹] (گلنون و همکاران[۱۴۰]، ۲۰۲۴). معمولا تصور می‌شود که داده ارزش ذاتی محدودی دارد (آلتونن و همکاران[۱۴۱]، ۲۰۲۱)، اما داده پردازش نشده نیز به‌خودی‌خود از ارزش بالایی برخوردار است به حدی که ارزش‌گذاری بزرگترین بنگاه‌های جهان بر اساس داده‌هایشان صورت می‌گیرد (ولدکامپ[۱۴۲]، ۲۰۲۳). شکوفایی ظرفیت داده، نیازمند مشارکت در اقتصاد داده است. منظور از اقتصاد داده، بوم‌سازگانی جهانی است که عوامل پیشران آن را جمع‌آوری، پردازش و اشتراک‌گذاری داده شکل می‌دهند. بازیگران با اهداف متفاوتی (شامل کسب آورده اقتصادی، اجتماعی و امنیتی) در این بوم‌سازگان مشارکت می‌کنند (سستینو و همکاران[۱۴۳]، ۲۰۲۵؛ استفان[۱۴۴]، ۲۰۲۴).

ماهیت داده به‌عنوان یک منبع رقابت‌ناپذیر[۱۴۵] و تا اندازه‌ای استثناپذیر[۱۴۶] سبب خلق آثاری شده که می‌توانند به‌عنوان محرک رویکردهای مختلف در روابط اقتصادی، ژئوپلیتیکی و امنیتی بین‌الملل عمل کنند (لو[۱۴۷]، ۲۰۲۱؛ آکوئیستی و همکاران[۱۴۸]، ۲۰۱۶؛ چوی و همکاران[۱۴۹]، ۲۰۱۹). به عنوان مثال وزارت صنعت چین در واکنش به استفاده کاربران از کنش‌ور[۱۵۰] اُپن‌کلاو[۱۵۱] موضعی فعالانه برای محدود کردن آن اتخاذ کرده است. علت این امر دسترسی مستقیم این کنش‌ور به داده‌ها بدون وجود کنترل های مرسوم، ناکافی بودن تنظیمات امنیتی و نقص های طراحی آن که منجر به افشای داده شخصی هزاران کاربر شد، بوده است (لی[۱۵۲]، ۲۰۲۵). در سال ۲۰۲۴، در همکاری مشترک دو نهاد قانونی حفاظت از داده فرانسه و هلند، شرکت اوبر به دلیل انتقال داده‌های شخصی به خارج از اتحادیه اروپا و عدم ارائه تضمین‌کافی برای این اقدام، توسط سازمان نظارت هلند[۱۵۳] ۲۹۰ میلیون یورو جریمه شد (هیئت حفاظت از داده‌های اروپا[۱۵۴]، ۲۰۲۴). شرکت پلنتیر[۱۵۵] به عنوان یکی از پیشرفته‌ترین شرکت‌های استخراج‌گر داده در جهان، در یک رسوایی کم سابقه با استفاده از گزارشات اطلاعاتی فلسطینیان ساکن اراضی اشغالی، این امکان را برای ارتش اسرائیل فراهم می‌کرد تا با استفاده از هوش‌مصنوعی این شرکت برای تعیین سرنوشت مرگ و زندگی مردم

۱۳۹. کشور چین در سال ۲۰۲۴ با رشدی ۲۵ درصدی نسبت به سال قبل در حدود ۴۱ زتابایت داده تولید کرده است (شین‌هوا، ۲۰۲۵)

140. Glennon et al.
141. Aaltonen et al.
142. Veldkamp
143. Sestino et al.
144. Stephan

۱۴۵. یعنی به‌صورت نامحدود قابل‌استفاده است

۱۴۶. همواره امکان حذف افرادی که بابت دسترسی به داده پولی پرداخت نکرده‌اند، وجود ندارد

147. Liu
148. Acquisti et al.
149. Choi et al.
150. Agent
151. OpenClaw
152. Lee
153. The Dutch Supervisory Authority (Dutch SA)
154. European Data Protection Board
155. Palantir

تصمیم‌گیری شود (بمفورد[۱۵۶]، ۲۰۲۴). بروز چنین مواردی لزوم توجه به سیاست داده[۱۵۷] را بیش‌ازپیش توجیه می‌کند.

بنا بر تعریف پولاتین - روبن و رایت[۱۵۸] (۲۰۱۴، ص. ۱) حاکمیت داده عبارت است از «تلاش صورت‌گرفته توسط دولت - ملت‌ها به‌منظور محدود ساختن و تحت کنترل درآوردن جریان‌های داده ذیل حوزه‌های قضایی ملی». به باور این دو، حاکمیت داده به‌صورت دو ساختار «حاکمیت ضعیف[۱۵۹] و قوی[۱۶۰]» قابل‌تفسیر است. منظور از حاکمیت ضعیف، راهکارهای محافظت از داده مبتنی بر بخش خصوصی است که بیشتر بر جنبه‌های حقوق دیجیتال حاکمیت داده تأکید دارد. اما در حاکمیت قوی، رویکردهای مبتنی بر حاکمیت دولت با تأکید بر پاسداری از امنیت ملی مطرح می‌شود. به‌عنوان‌مثال، با بررسی رویکردهای حاکمیت داده کشورهای عضو بریکس (برزیل، روسیه، چین، هند و افریقای جنوبی) مشاهده می‌شود که برزیل، هند و آفریقای جنوبی رویکرد حاکمیت ضعیف را دنبال می‌کنند و چین و روسیه رویکرد حاکمیت قوی را در پیش گرفته‌اند. کشور چین از سال ۲۰۱۴ جایگاه کلان‌داده را به سطح راهبرد ملی ارتقا داده است.

حاکمیت داده مفهومی غنی و چندبعدی است که طیف گسترده‌ای از معانی ضمنی (پنهان) بالقوه را شامل می‌شود و توجه به روابط این وجوه، شناسایی و توجه به سازوکارهای این ارتباطات و شرایط زمینه‌ای آن از اهمیت بالایی برخوردار است (ون دن بروک و ون وینسترا[۱۶۱]، ۲۰۱۸).

به طور کلاسیک، حاکمیت داده بیشتر بر جنبه های کنترلی فراهم‌سازان داده[۱۶۲] تمرکز دارد (هلمایر و شرنبرگ[۱۶۳]، ۲۰۲۳) و نقش فقدان «حاکمیت»را در کاهش تمایل به اشتراک‌گذاری داده پررنگ می‌داند (اپریل و همکاران[۱۶۴]، ۲۰۲۱). این مفهوم عموماً از جهاتی با کنترل معنادار و مالکیت داده و زیرساخت‌های آن مرتبط است و معمولاً مفهوم «حاکمیت داده» به‌عنوان «امکان کنترل فراهم‌ساز داده بر داده به اشتراک گذاشته شده» مفهوم‌پردازی-تعریف- می‌شود.

از سوی دیگر توجه به ارتباط میان حاکمیت داده و خودگردانی[۱۶۵] لازم و ضروری است. زیرا تشابهاتی میان این دو مفهوم وجود دارد. هر دو به نوع خاصی از آزادی اشاره دارند که از دخالت خارجی رها بوده و بر آزادی مثبت در پیروی از تمایلات تأکید دارد. بااین‌حال پاسخ به چند سؤال ضروری است: اگر فرض کنیم که تحت کنترل بودن یک فرد بر جریان داده خود برای دستیابی به حاکمیت داده کفایت و بر مبنای آن افراد از حق کنترل خود بر داده‌هایشان استفاده و آن را در اختیار دیگری قرار دهند، پیامد آن چه خواهد بود؟ در این صورت آیا فرد در تصمیم خود مستقل عمل کرده است؟ این دو سؤال منجر به سؤال بنیادی‌تری می‌شود که تعریف ما از استقلال و خودمختاری چیست؟

از منظر دورکین[۱۶۶] (۱۹۷۶) خودمختاری به‌عنوان آزادی از قیدوبند محدودیت‌های خارجی با فرض

156. Bamford
157. Data Politics
158. Polatin-Reuben & Wright
159. Weak Sovereignty
160. Strong Sovereignty

161. Van Den Broek & Van Veenstra
162. Data Provider
163. Hellmeier & Scherenberg
164. Opriel et al.
165. Autonomy
166. Gerald Dworkin

اصالت[۱۶۷] تعریف می‌شود. این بدین معنی است که تأیید یک انتخاب بر مبنای اصالت‌بخشی بر تمایلی با اولویت بالاتر انجام شده است. در تعریفی دیگر بوشامپ و چیلدرس[۱۶۸] (۲۰۱۳: ۱۰۴-۱۰۵) برلزوم قصدمندی[۱۶۹] در انتخاب و تصمیم تأکید می‌کنند؛ یعنی عامل، همان برداشتی از عمل را داشته باشد که قصد کرده و درک کند که می‌خواهد چه‌کار کند و عوامل کنترل‌کننده بیرونی موثر بر عمل، وجود نداشته باشند. به همین دلیل است که به‌صرف وجود «کنترل» سایر شروط (اصالت و قصدمندی) برآورده نمی‌شوند و به همین دلیل است که منظور از حاکمیت داده چیزی ورای کنترل صرف بوده و هدف «نوعی کنترل معنادار» است.

یکی دیگر از وجوه کنترل معنادار ، مفهوم «ادراک آگاهانه[۱۷۰]» است. بین آگاهی و اطلاع تفاوت جدی است. متقاضیان داده به‌صرف ارائه یک بیانیه بلندبالا ادعا می‌کنند که سیاست‌های خود را به فراهم‌ساز داده اطلاع داده‌اند. بر طبق بررسی‌های صورت‌گرفته تنها یک نفر از هر پنج آمریکایی سیاست‌های حریم خصوصی شرکت‌ها را مطالعه می‌کند و تعداد بسیار کمتری بیان می‌کنند که نسبت به مفاد این سیاست‌ها «آگاه» هستند (آکسیه و همکاران[۱۷۱]، ۲۰۱۹). در مطالعه‌ای که توسط اوبار و اودولرف - هرش صورت گرفت ۹۷درصد از مشارکت‌کنندگان با شرایط خدمات و سیاست حریم خصوصی یک شبکه اجتماعی فرضی که بیان می‌کرد، تمام اطلاعات شرکت‌کنندگان را با آژانس امنیت ملی به اشتراک می‌گذارد، موافق‌بودند و ۹۳درصد کاربران پذیرفتند که فرزند اول خود را به‌عنوان هزینه اشتراک به این شبکه اجتماعی فرضی بدهند (ابر و اولدورف-هیرش[۱۷۲]، ۲۰۲۰)!

چنانکه بیان شد صرف داشتن کنترل بر داده برای ایجاد حاکمیت کافی نبوده و مفاهیم دیگری مانند حریم خصوصی، مالکیت، امنیت، پذیرندگی و مسئولیت نیز نقش تعیین‌کننده‌ای دارند(عباس و همکاران، ۲۰۲۴؛ هلمایر و شرنبرگ، ۲۰۲۳؛ هامل[۱۷۳] و همکاران، ۲۰۲۱). به‌عنوان‌مثال در موضوع حریم خصوصی، داده‌های به اشتراک گذاشته شده توسط فراهم‌آورندگان داده می‌تواند خصوصیات کسانی که داده‌هایشان را به اشتراک نگذاشته‌اند را نیز آشکار کند (مک‌کارتی[۱۷۴]، ۲۰۱۶؛ عجم‌اوغلو و همکاران[۱۷۵]، ۲۰۱۷). بنا بر نتایج تحقیقات ارلیش و همکاران[۱۷۶] (۲۰۱۸)، مدل ارائه شده آنان با استفاده از تنها دو درصد از داده ژنتیک جامعه هدف، تقریباً می‌تواند تمامی افراد آن جامعه را شناسایی کند؛ حتی نفراتی که آزمایش ژنتیک را انجام نداده باشند.

در کنار مسئله حریم خصوصی، با گسترش دیجیتالی‌سازی و حکمرانی داده‌محور پیامدهای جانبی منفی دیگری نیز نمایان شده است. به‌عنوان‌مثال داده‌های جعلی، شایعات و تفکرات افراطی با بهره‌گیری از بستر شبکه‌های اجتماعی

167. Authenticity:
داشتن منشأ راست و درست و وارسی پذیر و قابل‌اعتماد بودن که در نتیجه آن اطمینان از درستی پیام و مبدأ آن و انتقال آن حاصل می‌شود
168. Beauchamp & Childress
169. Intentionality:
خصوصیتی ناظر بر اعمال فردی که اهدافی مشخص دارد و رفتارهای خود را در جهت دستیابی به آن اهداف تنظیم می‌کند
170. Conscious Perception
171. Auxier et al.
172. Obar & Oeldorf-Hirsch
173. Hummel et al.
174. McCarthy
175. Acemoglu et al.
176. Erlich et al.

تقویت شده‌اند (پدیده اتاق پژواک[۱۷۷]). پیامد این وضعیت دامن‌زدن به آشوب‌های اجتماعی و قطبیدگی سیاسی است. الگوریتم‌های یادگیری ماشین باقابلیت برجسته‌سازی کلیشه‌های موجود در داده‌ها، می‌توانند اقدامات تبعیض‌آمیز را در ابعاد بسیار وسیع‌تری گسترش دهند. به همین دلیل، دولت‌ها برقراری تعادل میان پیامدهای جانبی مثبت و منفی داده را امری ضروری تلقی می‌کنند. این ضرورت در مواجه با جریان‌های داده بین‌المللی از اهمیت بالاتری برخوردار است. بر خلاف تصور حامیان ساز وکار بازار، تنظیم‌گری اثرات جانبی داده، نیازمند ابزارهای بیشتر و کارآمدتری نسبت به راهکارهای بازاری است(لو، ۲۰۲۱). در نتیجه، بسیاری از دولت‌ها به سمت اتخاذ سیاست‌های حاکمیت داده حرکت کرده‌اند تا از این طریق بتوانند جریان فرامرزی داده را تنظیم کنند.

علاوه بر دغدغه بحث حریم خصوصی، دولت‌ها در پی ملاحظات سیاسی و امنیتی خود موضوعاتی نظیر کنترل راهبردی داده را به‌عنوان سیاست خود انتخاب می‌کنند. به‌عنوان‌مثال، درگذشته به دلیل نبود ظرفیت فناوری‌های بومی و توان تنظیم‌گری در حوزه داده، بسیاری از دولت‌ها برای محافظت از داده شهروندان خود این دارایی را در کشورهایی با بستر تنظیم‌گری و زیرساخت فناوری قوی‌تر ذخیره می‌کردند. اما امروزه با توجه به اهمیت بالا و راهبردی داده و تأثیر آن بر سیاست‌های داخلی و خارجی دولت‌ها، این رویکرد تغییر کرده و حتی کشورهای درحال‌توسعه نیز به سمت اتخاذ سیاست‌های حاکمیت داده‌گرایش پیدا کرده‌اند (هیکس[۱۷۸]، ۲۰۲۱، بلی و همکاران[۱۷۹]، ۲۰۲۴؛ رانا و عزیز[۱۸۰]، ۲۰۲۵).

زمانی که صحبت از حاکمیت داده می‌شود منظورمان این است که داده باید تحت کنترل قوانین و مقررات دولت - ملتی باشد که در آن تولید و پردازش شده است. این رویکرد تلاشی سیاسی در جهت محدود ساختن خدمات داده در قلمرو مرزهای یک کشور است. عموماً سه رویکرد متداول تنظیم‌گری داده در ادبیات ذکر شده است (گائو، ۲۰۲۰، ۲۰۲۳؛ وطن‌پرست[۱۸۱]، ۲۰۲۰): رویکرد مبتنی بر دولت (چین و روسیه)، رویکرد مبتنی بر شهروندان (اتحادیه اروپا) و رویکرد مبتنی بر بازار (ایالات متحده).

رویکرد مبتنی بر دولت

چین با رویکرد دولت‌محوری، چهار سند اصلی برای قانون‌مندی جریان فرامرزی داده منتشر کرده‌است[۱۸۲]. هسته اصلی این قوانین متمرکزسازی داده است (لو، ۲۰۲۱) که بر مبنای آن تمام کسب‌وکارهای فعال در بازار چین می‌بایست داده‌های مشخصی (مانند اطلاعات شخصی شهروندان چین) را در سرورهای داخلی ذخیره کنند. در صورت نیاز به انتقال این اطلاعات به کشور ثالث، دولت چین موظف به انجام یک ارزیابی امنیتی است[۱۸۳]. همچنین قانون این

177. Echo Chambers
178. Hicks
179. Belli et al.
180. Rana & Azeez
181. Vatanparast
182. the Cybersecurity Law/ the Draft Measures on Security Assessment of the Cross-border Transfer of Personal Information of/ 2019 the Draft Measures for Data Security Management of/ 2019 Draft Information Security Technology-Guidelines for Data Cross-Border Transfer Security Assessment of2017
183. Adil Nussipov" ,How China Governs Data ",April ,2020 ,27 https//:medium.com/center-for-media-dataand-society/how-china-governs-data-ff71139b68d2

اجازه را به دولت می‌دهد تا از کسب‌وکارهای خارجی بازدید سرزده بعمل آورد[۱۸۴].

رویکرد مبتنی بر شهروندان

در رویکرد شهروند محور که رویکرد اصلی اتحادیه اروپاست، به دلیل ماهیت خارجی اکثر سکوهای دیجیتالی که داده‌های شهروندان اروپایی را جمع‌آوری می‌کنند (مانند، فیس‌بوک، گوگل، اپل، ایکس، تیک‌تاک و...)، با تصویب قانون عمومی محافظت از داده۱۸۵ ظرفیت‌های قانونی در اختیار شهروندان خو قرار داده شده است.

رویکرد مبتنی بر بازار

رویکرد ایالات متحده به‌عنوان سردمدار رویکرد بازاری با گذشت زمان دستخوش تغییر و تحولاتی شده و به دو بازه تاریخی تقسیم می‌شود: در دوران پیش از ریاست‌جمهوری ترامپ، این کشور سیاست‌های حوزه داده خود را منطبق بر سازوکار بازار تعریف می‌کرد. براین‌اساس تنظیم‌گری حوزه داده به خود شرکت‌های عظیم فناور واگذار شده و نقش دولت به جایگاه تسهیلگری تنزل‌یافته بود. اما پس از روی کار آمدن اول ترامپ در سال ۲۰۱۷ و با افزایش سطح تنش‌ها با چین و همچنین داغ‌شدن بازار فناوری‌های متأثر از داده (مانند هوش مصنوعی) سیاست بازاری جای خود را به رویکردهای دولت‌محور داده است. به‌عنوان نمونه با تصویب قانون منع دسترسی کشورهای خارجی به داده‌های حساس شخصی و دولتی[۱۸۶] در سال ۲۰۲۴، محدودیت‌ها و ممنوعیت‌های جدی بر سر راه تبادلات داده با کشورهای خارجی که از نظر ایالات متحده متخاصم شناخته می‌شوند (چین، روسیه و غیره) ایجاد شده است[۱۸۷].

بحث

این مقاله با تکیه بر چارچوب مفهومی حاکمیت دیجیتال و زیرمجموعه آن حاکمیت داده، نشان می‌دهد که تقابل میان دولت-ملت‌ها و شرکت‌های چندملیتی فناوری، یک دعوای نظری صرف نیست، بلکه بازآرایی بنیادین در ساختار قدرت ژئوپلیتیک جهانی است. یافته‌های حاصل از مرور روایتی اسناد، با تکیه بر چارچوب تحلیلی «کنترل» به عنوان هسته مرکزی حاکمیت، نشان می‌دهد که گذار از حاکمیت سنتی (مبتنی بر کنترل قلمرو جغرافیایی و جمعیت) به حاکمیت دیجیتال (کنترل جریان‌های داده و زیرساخت‌های)، مستلزم بازتعریف رابطه میان دولت، بنگاه‌های چندملیتی و شهروندان است؛ در این راستا، دلالت‌های سیاستی برای ایران بسیار حیاتی است. با توجه به ضعف‌های ساختاری موجود در اسناد ملی قرار گیری کشور در وضعیت پیشا-حاکمیت دیجیتال، جمهوری اسلامی ایران باید از رویکرد انفعالی فاصله گرفته و با تدوین قوانین شفاف تعریف‌کننده متولیان داده و ایجاد «رصدگاه دیجیتال کشور»، وابستگی‌های استراتژیک خود را

184. The Diplomat” ,China‘s Cybersecurity Law: What You Need to Know “,June ,2017 ,1 https//: thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

185. GDPR) General Data Protection Regulation(

186.” Preventing Access to U.S .Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons,“ https//:www.govinfo.gov/content/pkg/FR-۰۸-۰۱-۲۰۲۵/pdf/۳۱۴۸۶-۲۰۲۴.pdf

187. Harry Clark et al” ,.U.S .Data Localization Law Coming Soon :DOJ Issues Final Rule on Certain Data Transfers to’ Countries of Concern 17 ,‘January ,2025 https//:www.orrick.com/en/Insights/2025/01/US-Data-Localization-Law-Coming-Soon-DOJ-Issues-Final-Rule

در زیرساخت‌های نرم و سخت شناسایی و پایش کند تا از خطر استعمار داده توسط شرکت‌های فناور جلوگیری نماید.

از سوی دیگر، نوآوری و دانش‌افزایی این پژوهش در دو بعد روش‌شناختی و نظری قابل تبیین است. از منظر روش‌شناختی، استفاده از مرور روایت به جای مرور نظام‌مند، به پژوهشگر اجازه داد تا طیف گسترده‌تری از گفتمان‌های سیاسی، اقتصادی و اجتماعی مرتبط با حاکمیت را پوشش دهد. برخلاف مرورهای سیستماتیک که ممکن است به دلیل تمرکز بیش‌ازحد بر سوالات خاص و معیارهای ورود سختگیرانه، از ابعاد کیفی و تفسیری پدیده حاکمیت غافل شوند، رویکرد روایتی امکان ترکیب دیدگاه‌های متنوع و ارائه یک تصویر کل‌نگر از پیچیدگی‌های حاکمیت دیجیتال را فراهم کرد. این روش انعطاف‌پذیر به ما اجازه داد تا تناقضات موجود در ادبیات موضوع، مانند تضاد میان آزادی اینترنت و حاکمیت ملی، یا میان سودآوری شرکت‌های فناوری و حقوق شهروندی، را به شکلی عمیق‌تر تحلیل کنیم.

از بعد نظری، نوآوری این مطالعه نه تنها در ارائه یک دسته‌بندی سه‌گانه (دولتی، بنگاهی، چندذینفعی) از حاکمیت دیجیتال است، بلکه با برجسته کردن مفهوم حاکمیت داده فراتر از کنترل صرف (تنها به معنای استقرار داخلی مراکز داده یا قوانین محلی‌سازی داده)، بر وجوهی چون ادراک آگاهانه، مالکیت و خودگردانی تأکید دارد و به دنبال مدل کنترل معنادار است که رویکردی کیفی و تفسیری متمایز از سایر مرورها ارائه می‌دهد. همچنین، پرداختن به وجوه مختلف حاکمیت داده شامل حریم خصوصی، امنیت، پذیرندگی و مسئولیت، نشان می‌دهد که حاکمیت داده یک پدیده تک‌بعدی نیست، بلکه شبکه‌ای پیچیده از روابط قدرت است. این دانش افزایی نظری به سیاستگذاران ایرانی کمک می‌کند تا درک کنند که حاکمیت دیجیتال صرفاً مبحثی امنیتی نیست و به جای نگاه ابزاری مطلق به داده، بلکه ابزاری ژئوپلیتیک برای حفظ خودمختاری در برابر هژمونی شرکت‌های عظیم فناور است که نیازمند حکمرانی چندلایه می‌باشد؛ لذا ضروری است ایران با الگوبرداری انتقادی از تجربیات موفق مانند مدل‌های اروپایی (محور شهروند) یا چینی (محور دولت) و تطبیق آن با بافت داخلی، سواد دیجیتال جامعه را ارتقا داده و بستری قانونی برای مشارکت ذی‌نفعان متعدد فراهم آورد تا از شکاف دیجیتالی و نفوذ نامحدود داده‌های خارجی پیشگیری شود.

جمع‌بندی

همانطور که بیان شد، منظور از حاکمیت دیجیتال، ظرفیت جامعه و یا دولت برای تعریف، حکمرانی، اعمال قدرت و کنترل فناوری‌ها، داده و زیرساخت‌های ضروری برای خودمختاری، خلاقیت، تنوع فناوری و توسعه اجتماعی-فنی مبتنی بر ارزش‌های یک ملت است. نمود این مطلب در ابعاد حاکمیت دولتی، بنگاه و چندذینفعی قابل مشاهده بوده و هرکدام از این سه ضلع به دنبال دستیابی به نوع مطلوب حاکمیت از دیدگاه خود اند. در حاکمیت دولتی، هدف ایجاد و حفظ یک هویت واحد ملی مبتنی بر خصوصیات مشترک اجتماعی مانند فرهنگ، قومیت، سیاست، مذهب یا سنت‌ها بر بستر تاریخی واحد و مشترک است و ترویج وحدت ملی و یکپارچگی به‌عنوان یکی از اهداف کلیدی پیگیری می‌شود. اما در رویکرد بنگاهی، خودتنظیم‌گری بنگاه‌ها هدف اصلی بوده و لذا مداخلات قانونی را غیرضروری و ناخوشآیند برشمرده می‌شود. از این منظر هرگونه بازبینی و متعادل‌سازی قدرت دیجیتال بنگاه‌ها تابع رقابت،

اقتصاد رها و تعادل مبتنی بر بازار است. حاکمیت دیجیتال در این دوران، مبتنی بر بنگاه و بر مبنای جایگاه هژمونیک و یا انحصار رسمی آنها بنا شده است. اما در رویکرد حاکمیت چندذینفعی، با نگاهی رمانتیک و هابرماسی[۱۸۸] به دنبال تنظیم‌گری (کنترل) اینترنت ورای مرزهای ملت‌ها بوده و حاکمیت را خارج از حاکمیت دولت‌ها قرار می‌دهند.

داده به‌عنوان منبعی ارزشمند و راهبردی که گستره کاربردهای آن از حوزه‌های متداول و تخصصی فراتر رفته، توانسته به جایگاه ویژه‌ای در مقایسه با سایر اشکال سنتی منابع دست یابد. بحث حاکمیت داده از یک منظر، رویکردی ضد هژمونی و جایگزین برای تبلیغ و ترویج اقدامات ضد ساختاری در حوزه فناوری اطلاعات است. باقدرت گرفتن شرکت‌های بزرگ فناور و افزایش نفوذ این بنگاه‌ها و مواجهه آنان با حکومت‌های قانونی سبب شده که بهره‌گیری و تملک داده‌های شخصی توسط این شرکت‌ها به‌عنوان نوعی از سلب مالکیت، استعمار، انحصار، جنگ و کودتا بر علیه مردم‌سالاری توصیف شود؛ لذا القای این واقعیت که داده تولید شده توسط ما به هنگام استفاده از خدمات دیجیتال شرکت‌های عظیم فناور به ما تعلق نداشته و تحت مالکیت این شرکت‌ها است، مجدداً این نکته را گوشزد می‌کند که جوامع بیش‌ازپیش نیازمند نقش‌آفرینی مسئولانه و آگاهانه دولت‌های منتخب خود هستند.

از منظری می‌توان حاکمیت داده را تمرکز سیاست داده بر تعاملات راهبردی میان دولت‌های باحاکمیت[۱۸۹] تعریف نمود و از سوی دیگر کنش‌های شکل‌گرفته میان بازیگران دولتی و غیردولتی بر سر جمع‌آوری، پردازش، انتقال، فروش و یا استفاده از داده را نیز می توان با این سیاست‌ها مرتبط دانست. به‌منظور برقراری تعادل میان آثار جانبی مثبت و منفی داده، همان‌طور که بیان شد، بسیاری از کشورها به دنبال حاکمیت داده هستند تا بتوانند جریان‌های داده فرامرزی را کنترل و تنظیم کنند. تعارضات بر سر رویکردهای حاکمیت داده؛ مانند الزامات متمرکزسازی و محلی‌سازی داده (مانند تقابل میان کشور چین و تلاش ایالات متحده برای دسترسی به داده‌های فرامرزی)، می‌تواند زمینه‌ساز بروز مناقشه میان دولت‌ها باشد. این رویکردها از یک‌سو سبب شده تا تنظیم‌گری داده و اتخاذ سیاست‌های حاکمیت داده به‌عنوان یک الزام برای دولت‌ها مطرح باشد و از سوی دیگر بحث «تعهد» در استفاده از داده به دلیل نظارت دولت‌های خارجی و شرکت‌های چندملیتی به یک دغدغه جهانی تبدیل شده است.

در ساحت عمومی، ازآنجا که تبیین مفهوم حاکمیت در عرصه فناوری و به خصوص حوزه داده برای مردم کار آسانی نیست؛ به همین دلیل همواره آگاهی‌بخشی و سواد مرتبط با این حوزه‌ها به‌عنوان جزئی از مفهوم حاکمیت فناورانه مطرح است. کسب آگاهی نسبت به حوزه دیجیتال و اهمیت آن، به کاربران کمک می‌کند تا علاوه بر حفظ حاکمیت خود بر فناوری‌ها، داده و محتوایشان، در تنظیم‌گری این حوزه‌ها نیز نقش‌آفرین باشند. عملا تفاوتی نمی‌کند که در جامعه‌ای زندگی کنید که بر مبنای لیبرال دموکراسی اداره می‌شود و یا ساختار دولت اقتدارگرا بر آن حاکم است. در اولی سازوکار بازار حق

۱۸۸. از دید هابرماس، بازیگران استراتژیک در شرایط درست و پذیرش هنجارهای مشترک، می‌توانند انگیزه‌های سیاسی خود را کنار گذاشته و آنان را وادار می‌کند تا آگاهانه گوش دهند، دیدگاه‌های خود را با یکدیگر انطباق دهند و در نهایت بر سر موضوعی که به عموم جامعه مرتبط است به توافق برسند (Jürgen Habermas, The Theory of Communicative Action, vol. 1, (Boston: Beacon,1984)).

189. Sovereign States

حاکمیت شما را نقض می‌کند و در دیگری کنترل و نظارت خارج از چارچوب قوانین؛ بنابراین ایجاد آگاهی به‌عنوان یکی از گام‌های اولیه جهت دستیابی به حاکمیت لازم و ضروری است.

جمهوری اسلامی ایران به دلیل ضعف‌های جدی در توانمندی‌های حکمرانی (فقدان نهاد مسئول در حوزه دیجیتال/داده و همپوشانی و تعارض منافع جدی به دلیل عدم وجود و یا شفافیت قوانین و غیره)، نبود بسترهای قانونی مناسب در حوزه داده و زیرساخت، ضعف در ظرفیت‌های زیرساختی حوزه فناوری اطلاعات، ضعف سواد دیجیتال عامه جامعه در مرحله پیشا حاکمیت دیجیتال/داده قرار دارد. اما می‌توان با بهره‌گیری از تجارب سایر کشورها و تطبیق سیاست‌های اتخاذ شده توسط آنها گام‌های اولیه را در راستای استقرار حاکمیت دیجیتال/داده برداشت. اولاً، لازم است مجموعه‌ای از قوانین که به طور شفاف متولی و یا متولیان حوزه دیجیتال و داده را تعریف می‌کند و شرح وظایف و حدود اختیارات هر یک را مشخص نماید تدوین گردد. این مهم می‌بایست با مشارکت حداکثری ذی‌نفعان و بازیگران کلیدی انجام گردد و فرایند تصویب این قوانین به طور منظم و شفاف برای جامعه تبین شود. ثانیاً، میزان وابستگی کشور به زیرساخت‌های نرم و سخت حوزه دیجیتال/ داده توسط یک برنامه جامع و با عاملیت «رصدگاه دیجیتال کشور» مشخص شده و این نیازها و کمبودها در جهت اعمال حاکمیت دیجیتال/داده برای کشور با قید فوریت فراهم شود؛ چرا که بدون وجود زیرساخت مناسب عملاً تلاش برای اعمال حاکمیت دیجیتال/داده بی‌معنا خواهد بود. ثالثاً، به طور گستره برنامه‌ای جامع برای بالابردن سواد دیجیتال جامعه در تمامی سطوح تدوین شده و متولیان اقدامات آموزشی/ترویجی مرتبط با آن مشخص و به‌صورت مستمر تحت اشراف «رصدگاه دیجیتال کشور» مورد پایش قرار گیرد. رابعاً، لازم است تا رابطه بخش حاکمیت و شرکت‌ها داخلی و بین‌المللی تحت قوانین جدید بازتعریف شده و مسئولیت نظارت بر حسن اجرای این فرایند برعهده «رصدگاه دیجیتال کشور» خواهد بود.

پیشنهادهای پژوهشی و سیاستی

جمهوری اسلامی ایران به دلیل ضعف‌های جدی در توانمندی‌های حکمرانی (فقدان نهاد مسئول در حوزه دیجیتال/داده و همپوشانی و تعارض منافع جدی به دلیل عدم وجود و یا شفافیت قوانین و غیره)، نبود بسترهای قانونی مناسب در حوزه داده و زیرساخت، ضعف در ظرفیت‌های زیرساختی حوزه فناوری اطلاعات، ضعف سواد دیجیتال عامه جامعه در مرحله پیشا حاکمیت دیجیتال/داده قرار دارد. اما می‌توان با بهره‌گیری از تجارب سایر کشورها و تطبیق سیاست‌های اتخاذ شده توسط آنها گام‌های اولیه را در راستای استقرار حاکمیت دیجیتال/داده برداشت. اولاً، لازم است مجموعه‌ای از قوانین که به طور شفاف متولی و یا متولیان حوزه دیجیتال و داده را تعریف می‌کند و شرح وظایف و حدود اختیارات هر یک را مشخص نماید تدوین گردد. این مهم می‌بایست با مشارکت حداکثری ذی‌نفعان و بازیگران کلیدی انجام گردد و فرایند تصویب این قوانین به طور منظم و شفاف برای جامعه تبین شود. ثانیاً، میزان وابستگی کشور به زیرساخت‌های نرم و سخت حوزه دیجیتال/ داده توسط یک برنامه جامع و با عاملیت «رصدگاه دیجیتال کشور» مشخص شده و این نیازها و کمبودها در جهت اعمال حاکمیت دیجیتال/داده برای کشور با قید فوریت فراهم شود؛ چرا که بدون وجود زیرساخت مناسب عملاً تلاش برای اعمال حاکمیت دیجیتال/داده بی‌معنا خواهد

بود. ثالثاً، به طور گستره برنامه‌ای جامع برای بالابردن سواد دیجیتال جامعه در تمامی سطوح تدوین شده و متولیان اقدامات آموزشی/ترویجی مرتبط با آن مشخص و به‌صورت مستمر تحت اشراف «رصدگاه دیجیتال کشور» مورد پایش قرار گیرد. رابعاً، لازم است تا رابطه بخش حاکمیت و شرکت‌ها داخلی و بین‌المللی تحت قوانین جدید بازتعریف شده و مسئولیت نظارت بر حسن اجرای این فرایند برعهده «رصدگاه دیجیتال کشور» خواهد بود.

ملاحظات اخلاقی

پیروی از اصول اخلاق پژوهش

تمامی اصول اخلاقی در پژوهش این مقاله رعایت شده‌اند.

حامی مالی

این مقاله حامی مالی ندارد.

مشارکت نویسندگان

نویسندگان به یک اندازه در نگارش مقاله مشارکت داشته‌اند.

تعارض منافع

بنابر اظهار نویسندگان این مقاله تعارض منافع ندارد.

منابع

منابع فارسی

اکبری، ایمان؛ دانایی‌فرد، حسن؛ عبدالحمید، مهدی؛ محمودی، مصطفی؛ خسروی، مهدی. (۱۴۰۳). شناسایی و اولویت‌بندی موانع و چالش‌های حکمرانی داده‌محور از منظر به کارگیری هوش مصنوعی و فناوری‌های مبتنی بر داده در بخش عمومی؛ مطالعات راهبردی سیاستگذاری عمومی، ۱۴(۵۱)، ۵۶-۸۱

پاینده، رضا. (۱۴۰۳). طراحی نظام حکمرانی داده در بخش خصوصی با استفاده از روش‌شناسی سیستم‌های نرم (SSM)؛ مورد مطالعه اتاق بازرگانی، صنایع، معادن و کشاورزی ایران؛ مطالعات راهبردی سیاستگذاری عمومی، ۱۴(۵۱)، ۲۲-۴۴

دهقان پور فراشاه، علیرضا؛ دهقان پور فراشاه، افسانه. (۱۴۰۳). واکاوی ملاحظه‌های اخلاقی و سیاستی حکمرانی داده‌محور؛ مطالعات راهبردی سیاستگذاری عمومی، ۱۴(۵۱)، ۱۰۴-۱۲۴

References

Aaltonen, A., Alaimo, C., & Kallinikos, J. (2021). The Making of Data Commodities: Data Analytics as an Embedded Process. Journal of Management Information Systems, 38(2), 401–429. https://doi.org/10.1080/07421222.2021.1912928

Abbas, A. E., Velzen, T. van, Ofe, H., Kaa, G., Zuiderwijk, A., & Reuver, M. D. (2024). Beyond control over data: Conceptualizing data sovereignty from a social contract perspective. Electronic Markets. https://doi.org/10.1007/s12525-024-00695-2

Acemoglu, D., Makhdoumi, A., Malekian, A., & Ozdaglar, A. (2017). Privacy-constrained network formation. Games and Economic Behavior, 105, 255–275. https://doi.org/10.1016/j.geb.2017.08.001

Acquisti, A., Taylor, C. R., & Wagman, L. (2016). The Economics of Privacy (SSRN Scholarly Paper No. 2580411). Social Science Research Network. https://doi.org/10.2139/ssrn.2580411

Aghion, P., Bergeaud, A., & Van Reenen, J. (2023). The Impact of Regulation on Innovation. American Economic Review, 113(11), 2894–2936. https://doi.org/10.1257/aer.20210107

Akbari.I, Danaeefard.H, Abdolhamid.M, Mahmoudi.M, Khosravi.M (2024). [Identifying and prioritizing the obstacles and challenges of data-driven governance from the perspective of applying artificial intelligence and data-based technologies in the public sector (In Persian)]. Journal Strategic Studies of Public Policy, 14(51), 56-81. https://doi.org/10.22034/sspp.2024.2026836.3610

Alaimo, C., & Kallinikos, J. (2024). Data Rules: Reinventing the Market Economy. https://mitpress.mit.edu/9780262547932/data-rules/, ISBN: 9780262547932

Audrey Kurth, C. (n.d.). How Private Tech Companies Are Reshaping Great Power Competition. Henry A. Kissinger Center for Global Affairs. Retrieved 1 October 2025, from https://kissinger.sais.jhu.edu/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition/

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). Americans' attitudes and experiences with privacy policies and laws. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

Bamford, J. (2024). Palantir allegedly enables Israel's AI targeting in Gaza, raising concerns over war crimes. Business and Human Rights Centre. https://www.business-humanrights.org/en/latest-news/palantir-allegedly-enables-israels-ai-targeting-amid-israels-war-in-gaza-raising-concerns-over-war-crimes/

Basu, A., Poetranto, I., & Lau, J. (2021, May 19). The UN Struggles to Make Progress on Securing Cyberspace. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2021/05/the-un-struggles-to-make-progress-on-securing-cyberspace

Beauchamp, T. L., & Childress, J. F. (2019). Principles of biomedical ethics (Eighth edition). Oxford University Press, ISBN: 9780190640873

Bellanger, P. (2012). De la souveraineté numérique: Le Débat, n° 170(3), 149–159. https://doi.org/10.3917/deba.170.0149

Belli, L., Gaspar, W. B., & Jaswant, S. S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. Computer Law and Security Review. https://doi.org/10.1016/j.clsr.2024.106017

Bensinger, V., Kociok, C., Dietrich-Webb, J. P., Radlanski, P., & Enaux, C. (2025, April 22). Digital Policy: Highlights of the German Coalition Agreement 2025 | Insights | Greenberg Traurig LLP. https://www.gtlaw.com/en/insights/2025/4/digital-policy-highlights-of-the-german-coalition-agreement-2025

Bigo, D., Isin, E., & Ruppert, E. (2019). Data Politics: Worlds, Subjects, Rights. Routledge.

Bordelon, B. (2024, May 1). Tech CEO jokes about drone-striking rivals in MAGA-tinged Hill summit. POLITICO. https://www.politico.com/news/2024/05/01/alex-karp-hill-summit-trump-00155571

Bravo, R. (2025, August 29). Macron Vows Retaliation If Europe's Digital Sovereignty Attacked. Bloomberg.Com. https://www.bloomberg.com/news/articles/2025-08-29/macron-vows-retaliation-if-europe-s-digital-sovereignty-attacked

Britannica Editor. (2026, May 5). Sovereignty | Definition, Characteristics, Types, History, & Facts. https://www.britannica.com/topic/sovereignty

Broeders, D., Adamson, L., & Creemers, R. (2019). Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace (SSRN Scholarly Paper No. 3493600). Social Science Research Network. https://ssrn.com/abstract=3493600.

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. European Journal of Cultural Studies, 21(5), 594–613. https://doi.org/10.1177/1367549417751151

Capri, A. (2020). US-China tech innovation race | Hinrich Foundation. https://www.hinrichfoundation.com/research/wp/tech/us-china-tech-innovation-race/

Choi, J. P., Jeon, D.-S., & Kim, B.-C. (2019). Privacy and Personal Data Collection with Information Externalities (SSRN Scholarly Paper No. 3115049). Social Science Research Network. https://doi.org/10.2139/ssrn.3115049

Cohen, J. E. (n.d.). Law for the Platform Economy. Retrieved 6 May 2026, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2991261

Colson, S. L. L., Parry, Jennifer L., Zhang, J., Payne, W. S., & Keeler, T. J. (n.d.). President Trump Announces "America First Investment Policy" | Insights | Mayer Brown. Retrieved 29 September 2025, from https://www.mayerbrown.com/en/insights/publications/2025/04/president-trump-announces-america-first-investment-policy

Council on Foreign Relations. (2023, February 14). Sovereignty: Challenges. CFR Education from the Council on Foreign Relations. https://education.cfr.org/learn/learning-journey/sovereignty-challenges/tanks-sanctions-and-separatists-the-various-challenges-to-sovereignty

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Couture, S., Toupin, S., & Mayoral Baños,

A. (2024). Resisting and Claiming Digital Sovereignty: The Cases of Civil Society and Indigenous Groups. Policy & Internet, 16(4), 739–749. https://doi.org/10.1002/poi3.434

Creemers, R. (2016). Connectivity wars: Why migration, finance and trade are the geo-economic battlegrounds of the future (M. Leonard, Ed.). European Council on Foreign Relations. https://www.jstor.org/stable/resrep21667

Creemers, R. (2020). Governing cyberspace: Behavior, power, and diplomacy (B. van den Berg & D. Broeders, Eds). P. 107. Rowman & Littlefield. scholarlypublications.universiteitleiden.nl/access/item%3A3076638/view

Cronin, A. K. (2023). How Private Tech Companies Are Reshaping Great Power Competition. The Kissinger Center Papers. https://kissinger.sais.jhu.edu/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition/

Daskal, J. (2018). Borders and Bits. Vanderbilt Law Review, 71(1), 179. https://scholarship.law.vanderbilt.edu/vlr/vol71/iss1/3

de Luca, S. (2025, February). Strategic dependencies: Threats to EU sovereignty in communication infrastructure | Think Tank | European Parliament. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2025)767234

Dehghanpour Farashah.A, Dehghanpour Farashah, A(2024). [Analyzing the Ethical and Policy Considerations of Data-Driven Governance (In Persian)]. Journal Strategic Studies of Public Policy, 14(51), 104-124. https://doi.org/10.22034/sspp.2024.2025254.3587

DeNardis, L. (Ed.). (2015). The global war for internet governance. Yale University Press. https://doi.org/10.2307/j.ctt5vkz4n

Dworkin, G. (1976). Autonomy and Behavior Control. The Hastings Center Report, 6(1), 23–28. https://doi.org/10.2307/3560358

Echikson, W. (2025, April 4). Europe's Digital Leaders Call for "Tech Sovereignty". CEPA. https://cepa.org/article/europes-digital-leaders-call-for-tech-sovereignty/

Edgerton, D. E. H. (2007). The Contradictions of Techno-Nationalism and Techno-Globalism: A Historical Perspective. New Global Studies, 1(1). https://doi.org/10.2202/1940-0004.1013

Erlich, Y., Shor, T., Pe'er, I., & Carmi, S. (2018). Identity inference of genomic data using long-range familial searches. Science, 362(6415), 690–694. https://doi.org/10.1126/science.aau4832

European Data Protection Board. (n.d.). Dutch SA imposes a fine of 290 million euro on Uber because of transfers of drivers' data to the US | European Data Protection Board. Retrieved 10 February 2026, from https://www.edpb.europa.eu/news/news/2024/dutch-sa-imposes-fine-290-million-euro-uber-because-transfers-drivers-data-us_en

Evenett, S. J. (2019). Protectionism, state discrimination, and international business since the onset of the Global Financial Crisis. Journal of International Business Policy, 2(1), 9–36. https://doi.org/10.1057/s42214-019-00021-0

Farrell, H., & Newman, A. (2019a). Of privacy and power: The transatlantic struggle over freedom and security. Princeton university press. https://press.princeton.edu/books/hardcover/9780691183640/of-privacy-and-power

Farrell, H., & Newman, A. L. (2019b, April 2). Of Privacy and Power | Princeton University Press. https://press.princeton.edu/books/hardcover/9780691183640/of-privacy-and-power

Feldstein, S. (2025, October 2). The TikTok Deal Is America's White Flag in the Tech War With China. Foreign Policy. https://foreignpolicy.com/2025/09/29/tik-tok-deal-tech-war-china/

Fischer, D. (2025, July 29). Germany's vision for Europe's digital sovereignty and cyber resilience. https://www.pexip.com/blog/germanys-blueprint-for-digital-future-and-cyber-resilience

Flinders, M., & Smalley, I. (2024). What is data sovereignty? https://www.ibm.com/think/topics/data-sovereignty

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy & Technology, 33(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Forristal, L. (2025, September 26). Here's what's happening right now with the US TikTok deal. TechCrunch. https://techcrunch.com/2025/09/26/heres-whats-happening-right-now-with-the-us-tiktok-deal/

Gao. (2020, November 23). Data regulation in trade agreements: Different models and options ahead [Text]. WTO iLibrary. https://doi.org/10.30875/9789287054319c020

Gao, H. (2023). Data Sovereignty and Trade Agreements: Three Digital Kingdoms. In A. Chander & H. Sun (Eds), Data Sovereignty (1st edn, pp. 213–239). Oxford University PressNew York. https://doi.org/10.1093/oso/9780197582794.003.0010

Garcia-Herrero, A. (2019). From Globalization to Deglobalization: Zooming Into Trade. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3496563

George, S. (2015). Shadow Sovereigns: How Global Corporations are Seizing Power. John Wiley & Sons. https://www.wiley.com/en-us/shop/general-introductory-political-science/shadow-sovereigns-how-global-corporations-are-seizing-power-p-9780745697819

Glennon, Kolding, Sundbland, Croce, Micheletti, Raczko, Freitas, Moise, & Osimo. (2024). The European data market monitoring tool: Key facts & figures, first policy conclusions, data landscape and quantified stories : d2.9 final study report. Publications Office. https://doi.org/10.2759/632809

Goldsmith, J., & Wu, T. (2006). Who Controls the Internet?: Illusions of a Borderless World. Faculty Books. https://doi.org/10.1093/oso/9780195152661.001.0001

Gorman,. (n.d.). China's Data Ambitions: Strategy, Emerging Technologies, and Implications for Democracies | The National Bureau of Asian Research (NBR). Retrieved 30 September 2025, from https://www.nbr.org/publication/chinas-data-ambitions-strategy-emerging-technologies-and-implications-for-democracies/

Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: Secrets of the trade. Journal of Chiropractic Medicine, 5(3), 101–117. https://doi.org/10.1016/S0899-3467(07)60142-6

Greenhalgh, T., Thorne, S., & Malterud, K. (2018). Time to challenge the spurious

hierarchy of systematic over narrative reviews? European Journal of Clinical Investigation, 48(6), e12931. https://doi.org/10.1111/eci.12931

Gregory, A. T., & Denniss, A. R. (2018). An Introduction to Writing Narrative and Systematic Reviews—Tasks, Tips and Traps for Aspiring Authors. Heart, Lung and Circulation, 27(7), 893–898. https://doi.org/10.1016/j.hlc.2018.03.027

Haggart, B., & Jablonski, M. (2017). Internet freedom and copyright maximalism: Contradictory hypocrisy or complementary policies? The Information Society, 33(3), 103–118. https://doi.org/10.1080/01972243.2017.1294128

Hani. (2026, January 30). IET EngX. https://engx.theiet.org/b/blogs/posts/france-sparks-europe-s-tech-resilience-pivot

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hartmann, T. (2026, January 26). France launches bid to cut Europe's tech dependence. Euractiv. https://www.euractiv.com/news/france-launches-bid-to-cut-europes-tech-dependence/

Hellmeier, M., & Scherenberg, F. von. (2023). A Delimitation of Data Sovereignty from Digital and Technological Sovereignty. ECIS 2023 Research Papers. https://aisel.aisnet.org/ecis2023_rp/306

Hicks, J. (2021). A 'data realm' for the Global South? Evidence from Indonesia. Third World Quarterly. (world). https://www.tandfonline.com/doi/abs/10.1080/01436597.2021.1901570

Hollis, D. B. (2012). Stewardship versus Sovereignty? International Law and the Apportionment of Cyberspace (SSRN Scholarly Paper No. 2038523). Social Science Research Network. https://papers.ssrn.com/abstract=2038523

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. Big Data & Society, 8(1), 2053951720982012. https://doi.org/10.1177/2053951720982012

Hutchinson, J., Stilinovic, M., & Gray, J. E. (2024). Data sovereignty: The next frontier for internet policy? Policy & Internet, 16(1), 6–11. https://doi.org/10.1002/poi3.386

ICC. (n.d.). Data flows. ICC - International Chamber of Commerce. Retrieved 30 September 2025, from https://iccwbo.org/global-insights/digital-economy/data-flows/

Jarvis, D. (2026, February 26). Technology Sovereignty: Navigating a New Era of Self-Reliance—WSJ. https://deloitte.wsj.com/cio/technology-sovereignty-navigating-a-new-era-of-self-reliance-87d06768

Jiang, M. (2010). Authoritarian Informationalism: China's Approach to Internet Sovereignty. SAIS Review of International Affairs, 30(2), 71–89. https://doi.org/10.1353/sais.2010.0006

Kamps, H. J. (2023, June 29). When companies have more influence than countries. TechCrunch. https://techcrunch.com/2023/06/29/so-who-watches-the-watchmen/

Kapstein, E. B. (with JSTOR (Organization)). (2022). Exporting capitalism: Private enterprise and US foreign policy. Harvard University Press. https://doi.org/10.2307/j.ctv2jhjv8k

Kelly, T. (2025, January 13). Unlimited

Power: How Global Corporations Shape our Everyday Lives. Global Social Challenges. https://sites.manchester.ac.uk/global-social-challenges/2025/01/13/unlimited-power-how-global-corporations-shape-our-everyday-lives/

Khanal, S., Zhang, H., & Taeihagh, A. (2025). Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. Policy and Society, 44(1), 52–69. https://doi.org/10.1093/polsoc/puae012

Knafo, S. (2025, November 6). REPORT on European technological sovereignty and digital infrastructure | A10-0107/2025 | European Parliament. https://www.europarl.europa.eu/doceo/document/A-10-2025-0107_EN.html

Krasner, S. D. (Ed.). (2001). Sovereignty: Organized Hypocrisy. Princeton University Press. https://doi.org/10.2307/j.ctt7s9d5

Kurowska, X. (2020). Governing cyberspace: Behavior, power, and diplomacy (B. van den Berg & D. Broeders, Eds). P. 85. Rowman & Littlefield. https://scholarlypublications.universiteitleiden.nl/access/item%3A3076638/view

Lee, G. (2025). Top tech firms ban OpenClaw over security breach fears—The Korea Times. https://www.koreatimes.co.kr/business/tech-science/20260208/top-tech-firms-ban-openclaw-over-security-breach-fears

Legrain, P. (2020, March 12). The Coronavirus Is Killing Globalization and Empowering Nationalists and Protectionists. https://foreignpolicy.com/2020/03/12/coronavirus-killing-globalization-nationalism-protectionism-trump/

Liu, L. (2021). The Rise of Data Politics: Digital China and the World. Studies in Comparative International Development, 56(1), 45–67. https://doi.org/10.1007/s12116-021-09319-8

McCarthy, M. T. (2016). The big data divide and its consequences. Sociology Compass, 10(12), 1131–1140. https://doi.org/10.1111/soc4.12436

Mejias, U. A., & Couldry, N. (2024). Data grab: The new colonialism of big tech and how to fight back. WH Allen. https://press.uchicago.edu/ucp/books/book/chicago/D/bo216184200.html

Ministère de l'Europe et des Affaires étrangères. (2026, January 26). Algorithms and the public debate – The government sets out its digital-sovereignty and public-awareness initiatives (26 janvier 2026). France Diplomacy - Ministry for Europe and Foreign Affairs. https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/news/article/algorithms-and-the-public-debate-the-government-sets-out-its-digital

Montresor. (2001). Techno-globalism, techno-nationalism and technological systems: Organizing the evidence. Technovation, 21(7), 399–412. https://doi.org/10.1016/S0166-4972(00)00061-4

Moore, T. (2025, September 15). The Corporate Power Reset That Makes Citizens United Irrelevant. Center for American Progress. https://www.americanprogress.org/article/the-corporate-power-reset-that-makes-citizens-united-irrelevant/

Morgenthau, H. J. (2006). Politics among nations: The struggle for power and peace (7. ed). McGraw-Hill Higher Education. https://archive.org/details/politicsamongnat0007morg

Mueller, M. L. (2017). Will the Internet fragment? Sovereignty, globalization, and cyberspace. Polity. https://www.wiley.com/en-us/shop/general-communication-media-studies/will-the-internet-fragment-sovereignty-globalization-and-cyberspace-p-9781509501229

Mueller, M. L. (2020). Against Sovereignty in Cyberspace. International Studies Review, 22(4), 779–801. https://doi.org/10.1093/isr/viz044

Nissenbaum, H. (2005). Where Computer Security Meets National Security1. Ethics and Information Technology, 7(2), 61–73. https://doi.org/10.1007/s10676-005-4582-3

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. International Affairs, 91(1), 111–130. https://doi.org/10.1111/1468-2346.12189

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. Information, Communication & Society, 23(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

OECD. (n.d.). Cross-border data flows. OECD. Retrieved 30 September 2025, from https://www.oecd.org/en/topics/cross-border-data-flows.html

Opriel, S., Skubowius, E., & Lamberjohann, M. (2021). How Usage Control Fosters Willingness to Share Sensitive Data in Inter-Organizational Processes of Supply Chains.

Ostry, S., & Nelson, R. R. (1995). Techno-nationalism and techno-globalism: Conflict and cooperation. Brookings Institution. https://www.researchgate.net/publication/352260501_How_Usage_Control_Fosters_Willingness_to_Share_Sensitive_Data_in_Inter-Organizational_Processes_of_Supply_Chains

Panday, J., & Malcolm, J. (2018). The Political Economy of Data Localization [Data set]. University of Salento. https://doi.org/10.1285/I20356609V11I2P511

Payandeh.R, (2024). [Designing a Data Governance System in the Private Sector Using Soft Systems Methodology (SSM): A Case Study of the Iran Chamber of Commerce, Industries, Mines, and Agriculture (In Persian)]. Journal Strategic Studies of Public Policy,14(51), 34-54. https://doi.org/10.22034/sspp.2024.2027704.3640

Peters, B. (2016). Digital keywords: A vocabulary of information society and culture. Princeton University Press. https://press.princeton.edu/books/paperback/9780691167343/digital-keywords

Philpott, D. (2003). Sovereignty. In The Stanford Encyclopedia of Philosophy (Winter 2007). Metaphysics Research Lab, Stanford University. https://plato.stanford.edu/archives/win2007/entries/sovereignty/

Picciano, B. (2015, October 5). Why Big Data Is The New Natural Resource. Forbes. https://www.forbes.com/sites/ibm/2014/06/30/why-big-data-is-the-new-natural-resource/

Pilkington, E. (2019, November 12). Google's secret cache of medical data includes names and full details of millions – whistleblower. The Guardian. https://www.theguardian.com/technology/2019/nov/12/google-medical-data-project-nightingale-secret-transfer-us-health-information

Pohle, J. (2020, December 15). Digital sovereignty. Www.Kas.De. https://www.kas.de/en/single-title/-/content/digital-sovereignty

Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance? Policy & Internet, 16(4), 672–691. https://doi.org/10.1002/poi3.426

Pohle, J., & Thiel, T. (2020). Digital sovereignty (SSRN Scholarly Paper No. 4081180). Social Science Research Network. https://doi.org/10.14763/2020.4.1532

Polatin-Reuben, D., & Wright, J. (2014). An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. https://www.researchgate.net/publication/309585614_An_Internet_with_BRICS_Characteristics_Data_Sovereignty_and_the_Balkanisation_of_the_Internet

Powers, S. M., & Jablonski, M. (2015). The Real Cyber War: The Political Economy of Internet Freedom (1st ed). University of Illinois Press. https://www.jstor.org/stable/10.5406/j.ctt130jtjf

Rajan, A. (2018, September 8). Techno-nationalism could determine the 21st Century. BBC News. https://www.bbc.co.uk/news/technology-45370052

Rana, V., & Azeez, G. K. (2025, March 19). Southeast Asia's Quest for Digital Sovereignty. https://thediplomat.com/2025/03/southeast-asias-quest-for-digital-sovereignty/

Rikap, C., & Lundvall, B.-Å. (2021). The Digital Innovation Race: Conceptualizing the Emerging New World Order. Springer International Publishing. https://doi.org/10.1007/978-3-030-89443-6

RPEX. (n.d.). CURIA - Documents. Retrieved 29 September 2025, from https://curia.europa.eu/juris/document/document.jsf?docid=228728&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=EN&cid=23121084

Rumsey, M. (n.d.). Influence Abroad: American lobbying at the European Union: Sunlight Foundation. Retrieved 29 September 2025, from https://sunlightfoundation.com/2015/12/16/influence-abroad-american-lobbying-at-the-european-union/

Ruppert, E., Isin, E., & Bigo, D. (2017). Data politics. Big Data & Society, 4(2), 2053951717717749. https://doi.org/10.1177/2053951717717749

Sachs, J. D. (2020). The ages of globalization: Geography, technology, and institutions. Columbia University Press. https://doi.org/10.7312/sach19374

Sainato, M. (2024). Amazon, Tesla and Meta among world's top companies undermining democracy – report | Business | The Guardian. https://www.theguardian.com/business/2024/sep/23/amazon-tesla-meta-climate-change-democracy

Santaniello, M. (2026). Attributes of Digital Sovereignty: A Conceptual Framework. Geopolitics, 31(2), 788–809. https://doi.org/10.1080/14650045.2025.2521548

Schiavi, I., Silveira, S. A. da, & Pasti, A. (2025). Where does digital sovereignty lie in building the Brazilian smart city? Digital Geography and Society, 9, 100137. https://doi.org/10.1016/j.diggeo.2025.100137

Schiller, D. (2014). Communication & Global Power Shifts| Rosa Luxemburg's Internet? For a Political Economy of

State Mobilization and the Movement of Accumulation in Cyberspace | International Journal of Communication. https://ijoc.org/index.php/ijoc/article/view/2045

Schoemaker, E., & Kirk, T. (2025, November 25). Digital sovereignty is now the big goal for small states—Africa at LSE. Africa at LSE - LSE's Engagement with Africa. https://blogs.lse.ac.uk/africaatlse/2025/11/25/digital-sovereignty-is-now-the-big-goal-for-small-states/

Segal, A. (2020, August 10). Peering into the Future of Sino-Russian Cyber Security Cooperation. War on the Rocks. https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/

Selby, J. (2017). Data localization laws: Trade barriers or legitimate responses to cybersecurity risks, or both? International Journal of Law and Information Technology, 25(3), 213–232. https://doi.org/10.1093/ijlit/eax010

Sestino, A., Kahlawi, A., & De Mauro, A. (2025). Decoding the data economy: A literature review of its impact on business, society and digital transformation. European Journal of Innovation Management, 28(2), 298–323. https://doi.org/10.1108/EJIM-01-2023-0078

Siddique, H. (2025, September 15). What did Elon Musk say at far-right UK rally and did his remarks break the law? The Guardian. https://www.theguardian.com/politics/2025/sep/15/what-did-elon-musk-say-at-far-right-uk-rally-and-did-his-remarks-break-the-law

Skonieczny, A. (2017). Corporate Lobbying in Foreign Policy. In A. Skonieczny, Oxford Research Encyclopedia of Politics. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.420

Slaughter, M. J., & McCormick, D. H. (2021, April 16). Data Is Power. Foreign Affairs, 100(3). https://www.foreignaffairs.com/articles/united-states/2021-04-16/data-power-new-rules-digital-age

Smith, A. D. (2013). Nationalism: Theory, Ideology, History, 2nd Edition (1. Aufl). Polity. https://www.wiley.com/en-us/shop/general-introductory-political-science/nationalism-theory-ideology-history-2nd-edition-p-9780745659671

Stadnik, I. (2019). Internet Governance in Russia – Sovereign Basics for Independent Runet. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3421984

Statista. (n.d.). Data centers worldwide by country 2025. Statista. Retrieved 30 September 2025, from https://www.statista.com/statistics/1228433/data-centers-worldwide-by-country/

Stephan, P. B. (2024). Big Data as a National Security Issue | The University of Chicago Legal Forum. https://legal-forum.uchicago.edu/print-archive/big-data-national-security-issue#heading-2

Sukhera, J. (2022). Narrative Reviews: Flexible, Rigorous, and Practical. Journal of Graduate Medical Education, 14(4), 414–417. https://doi.org/10.4300/JGME-D-22-00480.1

The Belfer Center for Science and International Affairs. (2025, July 23). Economics of National Security | The Belfer Center for Science and International Affairs. https://www.belfercenter.org/topics/economics-global-affairs/economics-national-security

The German Federal Government.

(2020). Programme of Germany's Presidency of the Council of the European Union in the Fields of Education, Research and Innovation. https://www.daad-brussels.eu/en/the-german-eu-council-presidency-in-2020/#:~:text=In%20the%20areas%20of%20education,world%20of%20education%20and%20work.

The Government of Canada (GC). (2025, October 31). Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html

Van Den Broek, T., & Van Veenstra, A. F. (2018). Governance of big data collaborations: How to balance regulatory compliance and disruptive innovation. Technological Forecasting and Social Change, 129, 330–338. https://doi.org/10.1016/j.techfore.2017.09.040

Vatanparast, R. (2020). Data and the Elasticity of Sovereignty (SSRN Scholarly Paper No. 3609579). Social Science Research Network. https://doi.org/10.2139/ssrn.3609579

Veldkamp, L. (2023). Valuing Data as an Asset*. Review of Finance, 27(5), 1545–1562. https://doi.org/10.1093/rof/rfac073

Wei, Y. (2016, June 22). China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty. The Henry M. Jackson School of International Studies. https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/

Woods, A. K. (2023). Digital Sovereignty + Artificial Intelligence. In A. Chander & H. Sun (Eds), Data Sovereignty (1st edn, pp. 115–136). Oxford University PressNew York. https://doi.org/10.1093/oso/9780197582794.003.0006

Xinhua. (n.d.). China produces 41.06 ZB of data in 2024. Retrieved 15 February 2026, from https://english.www.gov.cn/archive/statistics/202504/29/content_WS68106c12c6d0868f4e8f22b4.html

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". Politics & Policy, 45(3), 432–464. https://doi.org/10.1111/polp.12202

Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology, 30(1), 75–89. https://doi.org/10.1057/jit.2015.5

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power (First edition). PublicAffairs. dn721805.ca.archive.org/0/items/zuboff-shoshana.-the-age-of-surveillance-capitalism.-2019/Zuboff%2C Shoshana.The Age of Surveillance Capitalism.2019.pdf