Journal of Contemporary Law and Society, *Volume 2, Issue 4, December 2025, pp. 192-200*

RESEARCH ARTICLE
Online ISSN: 3139-1079
Doi: 10.18311/JCLS/2025/v2i4/53913

Online ISSN : XXXX-XXXX

Journal of Contemporary Law and Society

Contents available at: *www.informaticsjournals.co.in/index.php/jcls*

JCLS

Digital Colonialism and Data Sovereignty: International and National Legal Perspectives in the Digital Era

Siddharath Shrivastava

Hidayatullah National Law University, Raipur - 493661, Chhattisgarh, India; siddharathshrivastava@gmail.com

Abstract

The Digital power concentrated in the hands of a few Western technology firms has raised the question of digital colonialism, a new form of domination where data, platforms and infrastructure are the new resources of dominance as opposed to land or minerals. Events such as the effects of mass surveillance discussed by Edward Snowden and the scandal of Cambridge Analytica suggest that digital reliance may become a threat to privacy, independence, and even democracy. In most states, particularly in the Global South, this ruling has led to vulnerabilities that reflect the dependency during the colonial period.

This has led to the emergence of the concept of digital sovereignty as a defensive mechanism and the process of re-agency in the digital realm. It can be seen as an attempt by states to ascertain the manner in which data and infrastructures within their jurisdictions are regulated. The European Union focuses on privacy and rights, China on national security and localisation of data, India tries some experiments on digital public infrastructure, South Africa involves foreign technology with local protection, and the United States expands its influence through market-based approaches.

The present article contends that digital sovereignty should be regarded as a political initiative that addresses the question of digital colonialism. It explores how states are redefining autonomy in a global order that remains digital and whose infrastructural and regulatory patterns are shaped by unequal power.

Keywords: *Digital Colonialism, Data Governance, Digital Sovereignty*

1.0 Introduction

In his influential work Code: And Other Laws of Cyberspace (1999/2006), Lawrence Lessig argued that computer code does more than run digital systems; it actively shapes rules, norms, and behaviours that structure everyday life (Lessig, 2009). In this sense, "code is law" because it possesses the capacity to override legal, institutional, and cultural norms, thereby extending its influence into political and economic life. Lessig's insight has been widely applied in areas such as copyright, online speech regulation, and internet governance. Yet one dimension has received far less attention: the global dominance over code and digital infrastructure by the West, particularly the United States, which has profound implications for the sovereignty of states in the Global South.

This imbalance became starkly visible through Edward Snowden's revelations, which exposed the vast scale of U.S. surveillance programs. Snowden demonstrated how enormous quantities of global communications data were intercepted, analysed, and stored often without the knowledge or consent of other states (MacAskill & Dance, 2013). Similarly, the Cambridge Analytica scandal revealed how personal data harvested through platforms like Facebook could be weaponised to manipulate democratic processes in countries far beyond U.S. borders (Cadwalladr & Graham-Harrison, 2018). Together, these

**Author for correspondence*

episodes illustrate a new phase of global dominance, one where technological infrastructure, data flows, and platform economics reproduce and reinforce existing political and economic hierarchies. This phenomenon is now widely described as digital colonialism.

Against this backdrop, digital sovereignty has emerged both as a defensive and a transformative response. At its core, digital sovereignty refers to the ability of a state to govern and regulate digital data, infrastructure, and services within its jurisdiction in line with its own laws, values, and national interests (Pohle & Thiel, 2020). China was among the earliest countries to advocate for sovereign control over cyberspace, embedding it firmly within its national security framework. Similarly, in the aftermath of the Cambridge Analytica revelations, the European Union adopted regulatory and industrial policy measures aimed at protecting fundamental rights and securing technological autonomy. As states grapple with the challenges of control, autonomy, and security in cyberspace, the contours of sovereignty are being redefined. Sovereignty is no longer confined to territorial borders; it increasingly extends into the digital realm, encompassing the infrastructures, platforms, and data flows that underpin global connectivity.

This paper advances the argument that digital sovereignty should be understood primarily as a response to the exploitative tendencies of digital colonialism. To substantiate this claim, it examines how states have developed legal, institutional, and infrastructural measures to reclaim authority over their digital ecosystems, and how these efforts function as resistance to asymmetrical digital power.

1.1 What Is Digital Colonialism?

Colonialism, at its core, was a system of domination where one group subjugated another (McMichael, 2020), creating an unequal power dynamic rooted in the seizure of land and resources (Veracini, 2022). Colonial powers extracted natural wealth and raw materials by exploiting local labour, often justifying this under the guise of "development" by building railways, ports, and other infrastructure (Coleman, 2018). In the present day, colonialism has taken on a new form, no longer about territorial conquest but about digital control. This "digital colonialism" operates through the monopolisation of data, algorithmic governance, and platform dependency. In practice, it means that powerful Western technology companies harvest and use people's data often without informed consent through the very networks and platforms they control (Cadwalladr & Graham-Harrison, 2018).

1.2 Digital and Traditional Colonialism

Digital colonialism can be understood through five interlinked elements that are similar to historical colonial structures: oppression, exploitation, dispossession, monopoly, and dependence (Yılmaz, 2025). Oppression is evident in how a handful of technology companies dominate the global flow of information, much like colonial empires once ruled over vast territories. A clear example is WhatsApp's 2016 privacy policy change in India, which compelled users to share personal data such as names and phone numbers with its parent company and third parties. Users could either accept the terms or delete the app, leaving little room for choice (Supreme Court Observer, n.d.). Exploitation and dispossession are reflected in how ordinary digital activities are converted into monetizable data. For instance, the data brokerage industry, where personal data is commodified and traded, is projected to reach a staggering value of USD 407 billion by 2028 (Datapods, 2023). Monopoly further conforms to this structure, with a few tech giants controlling vast digital ecosystems. Microsoft, for example, commands nearly 70% of the desktop operating system market (StatCounter Global Stats, 2025), creating deep dependency on its platform and leaving little room for meaningful competition.

1.3 Distinct Elements of Digital Colonialism

Alongside these similarities with historical colonialism, digital colonialism carries distinct features. First is the unequal concentration of power, with ownership of software, hardware, and infrastructure resting in the hands of a small number of Western corporations (Kwet, 2019a). This is enabled by three factors: (i) control over financial and intellectual resources by developed countries, (ii) international and domestic legal frameworks such as intellectual property laws that act as barriers to knowledge sharing, and (iii) the ability of wealthy states to invest heavily in research and development, thereby maintaining technological dominance (Conectas, 2023).

Second, digital colonialism is often described as "violent and harmful" because of how central digital technologies have become in perpetuating structural inequalities

(Ricaurte, 2019). A striking example is Kenya's national biometric ID project, implemented in collaboration with a French company, which risked excluding racial, ethnic, and religious minorities from essential services such as jobs, public benefits, and travel (Birhane, 2023). Third, it relies on a discourse of benevolence, where technology corporations present digital tools as inherently beneficial, masking the exploitative structures behind them (Nothias, 2025).

1.4 Impact of Digital Colonialism

The manifestations of digital colonialism are wide-ranging, spanning control over digital infrastructure, cultural influence, economic exploitation, and political power (Holotă & Jebeli-Bakht-Ara, 2025). This control rests on the three pillars of the digital ecosystem: software, hardware, and connectivity (Kwet, 2019b). A 2025 report by Global Trade Research noted that India's economy remains heavily reliant on American software, cloud infrastructure, and social media platforms. A disruption in access could halt digital payments, freeze tax systems, and paralyse key government functions overnight (The Hindu BusinessLine, 2023). Data surveillance, or "dataveillance," further entrenches these dependencies by systematically extracting and monetising human activity. Uber's rapid rise in South Africa demonstrates this well: leveraging its intermediary position, deep financial backing, and data-driven strategies, it amassed a net worth of USD 125 million in just two years, while destabilising local transport economies (Akoob, 2017).

Much like traditional colonialism, digital colonialism has a deep economic, cultural, and political consequences for the Global South. These countries supply two critical resources to the digital economy: cheap labour and cheap raw materials. For example, Chile, Argentina, and Bolivia hold some of the world's largest lithium reserves, crucial for modern technology (Ahmad, 2020), yet workers in Argentina earn wages as low as USD 300 to 1,800 per month, far below standards in wealthier nations. The degree of exploitation and dependence raises a crucial question that how can digital colonialism be resisted, particularly when it is framed as a necessary cost of progress? One possible answer lies in strengthening data sovereignty, which offers a more balanced pathway to protecting national interests while still participating in the global digital economy.

2.0 What Is Digital Sovereignty?

Digital sovereignty refers to the ability of an individual, organisation, or state to exercise control over their own digital environment. This includes the data they generate and rely upon, as well as the hardware and software that underpin digital activity. In other words, digital sovereignty is about being in charge of your digital destiny (World Economic Forum, 2025). According to the Centre for Africa-Europe Relations, digital sovereignty can be understood across three interconnected layers. The first is the physical layer, which involves the infrastructure and technology that support digital systems. The second is the code layer, encompassing standards, rules, and system design. The third is the data layer, which governs the ownership, flow, and use of data (Musoni *et al.,* 2023). The World Economic Forum also highlights these layers as essential to understanding how digital sovereignty functions in practice.

2.1 Approaches To Digital Sovereignty

There are two primary approaches to understanding digital sovereignty. The first is known as the institutional approach. This approach defines digital sovereignty as an attribute of the state, grounded in control over a defined territory and the principle that no state should interfere in the internal affairs of another (Santaniello, 2025a). In essence, it mirrors Thomas Hobbes' classical conception of sovereignty, which regards sovereignty as a function of the state's capacity to enforce its will, both domestically and at the international level. By applying traditional notions of territory, authority, and enforcement to the digital realm, this approach attempts to extend familiar principles of state power to cyberspace.

However, the institutional approach faces significant limitations. Modern legislation illustrates that states now often exercise power beyond their physical borders. For instance, the European Union's General Data Protection Regulation (GDPR), the United States' CLOUD Act, and China's 2017 National Intelligence Law all demonstrate that national authorities can assert influence over data and digital activities that extend beyond their territorial boundaries (Celeste, 2021). Another limitation of this approach is the rise of new sovereign actors, particularly large digital corporations, which increasingly perform functions traditionally undertaken by governments. This includes managing large online communities, setting rules,

and making decisions about permissible content (Pasquale, 2017). For example, Meta has established its own oversight board to decide which content may be removed from its platforms, effectively exercising a form of governance that parallels state authority (Wong & Floridi, 2022).

The second approach, known as the constructive approach, does not treat sovereignty as a fixed, objective fact with rigid attributes; instead, it views sovereignty as a set of claims, narratives, and assertions used by various actors to justify their authority over digital resources (Santaniello, 2025b). One of the most widely cited examples of this approach is indigenous data sovereignty. This concept emphasises the rights of Indigenous peoples to maintain, control, protect, and develop their cultural heritage, traditional knowledge, and traditional cultural expressions, as well as the intellectual property that stems from them (Kukutai & Taylor, 2016). Constructive approaches have been instrumental in mapping the diverse ways in which digital and data sovereignty are claimed across different actors, including individuals, corporations, and states. By analysing these claims, researchers can distinguish between forms of personal data sovereignty, corporate claims, and state-driven assertions, providing a more nuanced understanding of the evolving digital political economy.

2.2 Models of Digital Sovereignty

The governance of digital technologies and data has led to the emergence of distinct models of digital sovereignty, each reflecting the goals and values pursued by different countries. The first is the rights-based model. This model aims to protect citizens' rights while balancing individual freedoms with broader market interests. In this framework, state intervention is seen as a tool to empower citizens online, limiting the dominance of foreign platforms and promoting technological independence through industrial policies and infrastructure development (Fratini *et al.,* 2024a). A notable example is the European Union's GAIA-X initiative, which seeks to create a secure cloud infrastructure capable of competing with US and Chinese tech giants (Flew *et al.,* 2019). Countries such as France, Germany, the United Kingdom, and Brazil embody this model by imposing fines on large corporations and implementing strong market and content regulations designed to promote fairness and protect users (Monsees & Lambach, 2022).

The centralisation model, by contrast, focuses on reshaping digital governance through state-led regulations that often exclude non-state actors from decision-making. This approach emphasises the creation of regulatory bodies and sometimes the replacement of foreign digital operators with domestic alternatives that governments can more easily control (Fratini *et al.,* 2024b). Recentralisation measures in this model are frequently justified on the grounds of national security. Bangladesh, for example, has deployed smart filtering systems and imposed internet shutdowns to manage unrest linked to religious tensions (Rahman, 2023a). Similarly, Russia's 2016 Yarovaya Law requires internet service providers to store texts, calls, and images within the country for six months to support counterterrorism efforts (Rahman, 2023b). Centralisation models thus prioritise control and oversight, sometimes at the expense of market freedoms or broader citizen participation in governance.

Another approach is the state-based model, where digital media and technology are framed as instruments for nation-building and economic growth (Sivetc, 2021). In this model, the line between private sector and public sector actors is often intentionally blurred. China provides a classic example of the state-based model, with the Chinese Communist Party playing a central role in implementing digital strategies. The promotion of domestic companies is a key part of this strategy, reducing dependence on foreign providers while fostering innovation and national competitiveness (Grossman *et al.,* 2020). Today, China holds nearly 30 per cent of global quantum patents, and artificial intelligence is increasingly framed as central to its ambitions for global dominance (Zeng, 2021).

In contrast, the market-oriented model prioritises free-market benefits over state regulation. It values innovation, competition, and corporate autonomy, but in practice, a purely market-driven model does not exist (Fratini *et al.,* 2024c). Even in the United States, home to some of the world's largest and most powerful corporations, federal agencies play a key role in overseeing digital governance, enforcing regulations, and safeguarding citizen rights (Mazzucato, 2014). This illustrates the inherent tension between market freedom and state oversight, highlighting the complexity of applying digital sovereignty in practice.

3.0 Comparative National Approaches To Digital Sovereignty

There is no single international framework for digital sovereignty; instead, it has been shaped by individual

nations according to their legal systems, cultural values, and strategic priorities. For example, the United States generally advocates for a largely unregulated cyberspace in which major technology companies play a dominant role, whereas China has developed a government-led model that emphasises state control over digital infrastructure and data (World Economic Forum, 2025b). Despite differences in approach, digital sovereignty is built upon three interrelated principles: data localisation, privacy, and national security (Vedikaa, 2025).

3.1 The European Union Approach

In the European Union, concerns arose over the economic and social dominance of non-EU technology companies, which were seen as undermining citizens' control over personal data and hampering the ability of EU authorities to enforce their laws (Gueham, 2017). In response, the EU frames digital sovereignty as Europe's capacity to act independently in the digital world (European Commission, 2019). The Union has established itself as a global leader in personal data protection through the General Data Protection Regulation (GDPR). The GDPR reflects a rights-based approach, recognising eight fundamental rights, including the right to data portability and the right to erasure (GDPR, 2016a). It applies not only to any processing activities involving the personal data of EU citizens and residents but also extraterritorially, meaning that entities outside the EU fall under its scope (European Data Protection Board, 2024).

Regarding data localisation, the GDPR imposes strict conditions on international transfers of personal data. Under Article 45, the European Commission can authorise transfers to non-EU countries only if they provide an "adequate" level of protection, including respect for human rights and fundamental freedoms (GDPR, 2016b). Where such adequacy is not established, Article 46 allows transfers only if strong legal safeguards are in place, such as binding contractual clauses (Marelli, 2024). To complement the GDPR, the EU introduced the Data Governance Act (DGA), which regulates data intermediaries and enhances individuals' control over their personal data (Von Dingurth, 2025). Together, the GDPR and DGA reinforce both digital sovereignty and personal autonomy.

3.2 Indian Approach

India's approach to digital sovereignty seeks to balance the so-called digital 'trilemma': generating economic growth that depends on access to data, protecting individual privacy, and safeguarding national security (Observer Research Foundation, 2025). Central to India's digital governance framework is the "India Stack," a collection of large-scale public digital initiatives covering digital identity (e.g., Aadhaar), electronic payments (e.g., UPI), and data exchange (Raghavan *et al.,* 2019). The Data Empowerment and Protection Architecture (DEPA) represent India's first national initiative to allow individuals to exercise personal data rights through a consent-sharing framework. Unlike traditional models, where users provide blanket consent at sign-up, DEPA enables individuals to grant specific, revocable permission at the moment it is needed (Observer Research Foundation, 2025b).

In terms of personal data protection and localisation, India enacted the Digital Personal Data Protection Act 2023, establishing a Data Protection Board to oversee compliance (Doshi & Delgado, 2024). While the Act supports sector-specific data localisation imposed by various state agencies, concerns persist regarding the broad exemptions granted to the central government. India's digital infrastructure reflects a combination of nationhood, self-reliance, and a distinctive approach to data ownership, localisation, and protection. For instance, the 2016 #SaveTheInternet movement opposed Facebook's Free Basics initiative, which offered limited free internet access to lower-income groups, because it represented digital colonialism (Mukerjee, 2016). Unlike China, which has developed a largely independent digital ecosystem, India remains heavily dependent on U.S. digital products and services.

3.3 Approach of China

China has adopted one of the most state-centred approaches to digital sovereignty. In 2010, the government released a white paper outlining its vision of "cyber sovereignty," asserting that the country's internet falls entirely under Chinese jurisdiction (State Council of the People's Republic of China, 2010). For China, cyber sovereignty entails the state's right to govern its digital space without interference from foreign actors. To enforce this principle, the government has implemented extensive measures, including content filtering, censorship, and control via the so-called "Great Firewall" (Anderson, 2012). As a result, Chinese citizens can access only content approved by the Communist Party, while material deemed a threat to national security or public morality is blocked.

In 2021, China introduced the Personal Information Protection Law (PIPL) and the Data Security Law (DSL), which impose strict localisation requirements. The PIPL focuses less on privacy in the Western sense and more on safeguarding personal information deemed sensitive, building on protections in the civil code. The DSL requires that business data be classified according to its importance for national security and public interest, and cross-border transfers must undergo an internal security review before approval. For EU and U.S. companies operating in China, these laws create challenges due to conflicting obligations; for example, the DSL restricts foreign law enforcement access to data stored in China (Wang, 2025), directly conflicting with the U.S. CLOUD Act.

3.4 South African Approach

South Africa is pursuing its own path to digital sovereignty, combining foreign technologies with domestic policies (Jiang & Belli, 2024). The country has invested in digital infrastructure, notably through the South Africa Connect broadband program, to address socio-economic challenges, though rural implementation remains limited. The Cybercrimes Act of 2021, building on the 2017 Bill and the National Cybersecurity Policy Framework, faces enforcement challenges due to resource and skills gaps. In the area of data protection, South Africa leads the continent through the Protection of Personal Information (POPI) Act of 2013, modelled on the EU GDPR, which recognises privacy as a constitutional right (Mabunda, 2021).

3.5 The American Approach

In contrast to these countries, the United States does not frame its policy in terms of digital sovereignty. Rather, it advocates for an open and largely unregulated cyberspace, in which major technology companies play a central role and data—both personal and non-personal—flows freely across borders. This approach reflects the fact that the U.S. is home to global technology leaders such as Google, Amazon, Apple, Meta (Facebook), and Microsoft, which dominate markets in the EU and the Global South. The U.S. CLOUD Act of 2018 further allows U.S. law enforcement to demand access to data held by American companies overseas (U.S. Department of Justice, 2019). In effect, the dominance of U.S. tech firms enables the United States to extend its influence and exercise aspects of digital sovereignty, including conducting criminal investigations, beyond its territorial borders.

4.0 Digital Sovereignty as Response to Digital Colonialism

Digital sovereignty offers a strong idea that can be used to challenge the aspects of digital colonialism. As traditional colonialism operated on the premise of resource exploitation and power disparities, its digital, modern equivalent exists on the principle of resource exploitation and centralised authority controlled by a small number of dominant global actors. Sovereignty, in this case, would be a conscious re-assertion of control and self-determination on our digital lives, on the information, the infrastructure, and the platforms that constitute our everyday reality. In essence, it concerns the redressing of an imbalanced power dynamic in which Western technology firms remain disproportionately influential in the digital economy.

The principle of data ownership is one of the most immediate methods of how digital sovereignty deals with this. With the existing system, it is a common practice to gather data, take it to other countries, and sell it to other companies without the express approval of the real creators. Such steps as data localisation and enhanced privacy protection will specifically work against this trend. Examples of laws intended to maintain data in a domestic jurisdiction are the Data Security Law of China or the Digital Personal Data Protection Act of India, whereby data cannot be taken to a foreign jurisdiction and subjected to foreign law and regulation.

Sovereignty also acts to lower monopoly and dependency through vigorously encouraging homegrown alternatives. Such projects as the GAIA-X project of the European Union or the digital infrastructure of a country such as India (including UPI and DEPA) are judicious measures to reduce dependence on U.S. or Chinese suppliers. These frameworks are not only state control, but they are also aimed at providing citizens and local businesses with the ability to engage in a fairer online setting. The other important point of resistance is legal regulation. The GDPR, in particular, makes the global technology companies obey the European privacy regulations instead of enforcing their own laws independently.

More importantly, digital sovereignty disputes the story of well-intentioned corporate actions that tend to envelop such undertakings. A case in point is the Free Basics program of Facebook in India, which was promoted as a mechanism to make internet services free; the program was seen as a controversial move that included trying to trap internet users in a closed platform, where only one company would be operating. Examining these accounts, sovereignty-oriented approaches demonstrate that all technology is not neutral; it is a severely political phenomenon. Thus, we can comprehend digital sovereignty not as a technical or legal process, but as an extension of opposition to regaining control over the exploitative and monopolistic nature of digital forces.

5.0 Conclusion

Digital colonialism is not just the concept but the reality, by analysing the global practices through which this is indeed happening in the monopolisation of software, hardware and data flow by a few dominant corporations of the West. The case of the Snowden exposés, the Cambridge Analytica scandal, and the growth of platforms like Uber in the Global South all demonstrate how the model of digital infrastructure and individual personal data could be used to generate economic value, political impact, and dependency.

Digital sovereignty, in turn, is an offensive response and a reactive approach to it. The states can alleviate dependency, curb monopolistic activities, and re-establish strategic independence through asserting regulatory control, encouraging domestic digital infrastructure, and protecting data in national jurisdictions. The comparative study of the national strategies, including the Chinese state-centred model, the EU regulatory framework built on the idea of rights, selective localisation of India, along with the innovation-driven efforts, as well as the hybrid model developed in South Africa, proves that sovereignty can be multidimensional and includes legal, infrastructural, and policy-based interventions. Even the U.S. model, which is market-based, explains how corporate hegemony can impose digital dominance across borders, and points to the imbalance that digital sovereignty addresses.

Thus, the article highlights how digital sovereignty is not only a technical or legal practice but a political activity as a whole, which seeks to reestablish power balance in an overall globalised digital economy that has traditionally been biased towards the West. Programs like GDPR, GDIA-X, India Stack, and data localisation legislations are all instances in which governments can safeguard the rights of their citizens, encourage localised innovation, and establish jurisdiction over their data space. When the concept of Colonialism has been redefined in the digital age, there is a need to enhance the concept of digital sovereignty, to fight back against exploitation and allow fair play in the digital economy.

6.0 References

Ahmad, S. (2020). The Lithium Triangle: Where Chile, Argentina, and Bolivia meet. *Harvard International Review*. https://hir.harvard.edu/lithium-triangle/

Akoob, R. (2017). Here's why metered taxis are so p'd off with Uber in South Africa. *The Daily Vox*. https://www.thedailyvox.co.za/heres-why-metered-taxis-are-so-p-d-off-with-uber-in-south-africa-rumana-akoob

Anderson, D. (2012). Splinternet behind the Great Firewall of China. *Queue*, 10(11), Article 40. https://doi.org/10.1145/2390756.2405036

Birhane, A. (2023). Algorithmic colonisation of Africa. In C. Burr & N. Milano (Eds.), *Imagining AI: How the world sees intelligent machines* (pp. 126–142). Oxford University Press. https://doi.org/10.1093/oso/9780192865366.003.0016

Cadwalladr, C., & Graham-Harrison, E. (2018). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Celeste, E. (2021). Digital sovereignty in the EU: Challenges and future perspectives. In L. Belli (Ed.), *Data protection beyond borders* (pp. 211–234). Hart Publishing. https://doras.dcu.ie/25498/1/Celeste_DigitalSovereigntyintheEU.pdf

Coleman, D. (2018). Digital colonialism: The 21st-century scramble for Africa through the extraction and control of user data. *Michigan Journal of Race & Law*, 24(2), 417–441. https://doi.org/10.36643/mjrl.24.2.digital

Conectas Human Rights. (2023). *Digital sovereignty or digital colonialism?* Sur – International Journal on Human Rights. https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism

DataPods. (2023). What your data is actually worth. https://www.datapods.app/en-US/blog/what-your-data-is-actually-worth

Doshi, V., & Delgado, H. E. (2025). Digital statecraft of middle powers: Tech landscape and digital sovereignty in Brazil and India. In M. Jiang & L. Belli (Eds.), *Digital sovereignty in the BRICS countries* (pp. 124–147). Cambridge University Press. https://doi.org/10.1017/9781009531085.009

European Commission. (2019). *Shaping Europe's digital future*. Retrieved December 10, 2025, from https://digital-strategy.ec.europa.eu/en

European Data Protection Board. (2024). *Extraterritorial enforcement of the GDPR*. https://edpb.europa.eu

Flew, T., Martin, F., & Suzor, N. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media & Policy*, 10(1), 33–50. https://doi.org/10.1386/jdmp.10.1.33_1

Fratini, S., *et al.* (2024). Digital sovereignty: A descriptive analysis. *DISO – Digital Sovereignty*, 1(1), Article 146. https://doi.org/10.1007/s44206-024-00146-7

Grossman, D., Beauchamp-Mustafaga, N., Charvonia, M., & Chase, M. S. (2020). *Chinese views of big data analytics*. RAND Corporation. https://doi.org/10.7249/RRA176-1

Gueham, F. (2017). *Digital sovereignty: Steps towards a new system of Internet governance*. Fondation pour l'innovation politique (Fondapol). https://www.fondapol.org/en/study/digital-sovereignty

Holotă, A., & Jebeli-Bakht-Ara, H. (2025). Globalisation and digitalisation: A new form of colonialism? *Proceedings of the International Conference on Business Excellence*, 19(1), 397–408. https://doi.org/10.2478/picbe-2025-0036

Jiang, M., & Belli, L. (Eds.). (2024). *Contesting digital sovereignty* [Preprint]. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1234567

Kukutai, T., & Taylor, J. (Eds.). (2016). *Indigenous data sovereignty: Toward an agenda*. ANU Press. https://doi.org/10.22459/CAEPR38.11.2016

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, 60(4), 3–26. https://doi.org/10.1177/0306396818823172

Lessig, L. (2009). *Code: Version 2.0*. ReadHowYouWant. (Original work published 2006). https://dl.acm.org/doi/10.5555/555000

Mabunda, S. (2021). Cybersecurity in South Africa: Towards a national cybersecurity strategy and best practices. In L. Belli (Ed.), *CyberBRICS: Cybersecurity policies of the BRICS countries* (pp. 227–270). Springer. https://doi.org/10.1007/978-3-030-56405-6_6

MacAskill, E., & Dance, G. (2013). NSA files decoded: Edward Snowden's surveillance revelations explained. *The Guardian*. https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded

Marelli, M. (2024). Transferring personal data to international organisations under the GDPR: The principle of purpose limitation as a barrier to international cooperation. *International Data Privacy Law*, 14(2), 123–139. https://doi.org/10.1093/idpl/ipad009

Mazzucato, M. (2014). *The entrepreneurial state: Debunking public vs. private sector myths*. Anthem Press. https://doi.org/10.2139/ssrn.2744602

McMichael, P. (2020). Colonialism. In E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy* (Winter 2020 ed.). Stanford University. https://plato.stanford.edu/entries/colonialism/

Monsees, L., & Lambach, D. (2022). Digital sovereignty and the reproduction of European identity. *European Security*, 31(3), 385–402. https://doi.org/10.1080/09662839.2022.2101883

Mukerjee, S. (2016). Net neutrality and India's battle to #SaveTheInternet. *Media Asia*, 43(3–4), 173–180. https://doi.org/10.1177/2057047316665850

Musoni, M., Karkare, P., Teevan, C., & Domingo, E. (2023). *Global approaches to digital sovereignty: Competing definitions and contrasting policy* (Discussion Paper No. 344). European Centre for Development Policy Management (ECDPM). https://ecdpm.org/work/global-approaches-digital-sovereignty

Nothias, T. (2025). An intellectual history of digital colonialism. *Journal of Communication*, 75(2), 123–145. https://doi.org/10.1093/joc/jqaf003

Observer Research Foundation. (2025a). *DEPA: Concept and assessment*. https://www.orfonline.org

Observer Research Foundation. (2025b). *Navigating the digital trilemma*. https://www.orfonline.org

Pasquale, F. (2017). From territorial to functional sovereignty: The case of Amazon. *Law and Political Economy Project*. https://lpeproject.org/blog/from-territorial-to-functional-sovereignty-the-case-of-amazon/

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4). https://doi.org/10.14763/2020.4.1532

Ricaurte, P. (2019). Data epistemologies, the coloniality of power, and resistance. *Television & New Media*, 20(4), 350–365. https://doi.org/10.1177/1527476419831640

Raghavan, V., Jain, S., & Varma, P. (2019). India Stack—Digital infrastructure as a public good. *Communications of the ACM*, 62(11), 38–40. https://doi.org/10.1145/3355625

Rahman, Z. (2023). Censorship and content filtering. *Business Post BD*. https://businesspostbd.com/opinion-todays-paper/2023/02/18/censorship-and-content-filtering

Santaniello, M. (2025). Attributes of digital sovereignty: A geopolitical perspective. *Geopolitics*. Advance online publication. https://doi.org/10.1080/14650045.2025.2521548

Sivetc, L. (2021). Controlling free expression "by infrastructure": The case of Turkey's Twitter block. *First Monday*, 26(5). https://doi.org/10.5210/fm.v26i5.11698

State Council of the People's Republic of China. (2010). *The Internet in China* [White paper]. http://www.china.org.cn/government/whitepaper/2010-06/08/content_20207978.htm

StatCounter Global Stats. (n.d.). *Desktop operating system market share worldwide*. Retrieved December 10, 2025, from https://gs.statcounter.com/os-market-share/desktop/worldwide

Supreme Court Observer. (n.d.). *Karmanya Singh Sareen v. Union of India (WhatsApp-Facebook privacy case)*. Retrieved December 10, 2025, from https://www.scobserver.in/cases/karmanya-singh-sareen-union-of-india-whatsapp-facebook-privacy-case-background

The Hindu BusinessLine. (2023). India should develop its own sovereign digital solutions, reduce reliance on US systems: GTRI. https://www.thehindubusinessline.com/economy/india-should-develop-its-own-sovereign-digital-solutions-reduce-reliance-on-us-systems-gtri/article67048509.ece

U.S. Department of Justice. (2019). *Promoting public safety, privacy, and the rule of law around the world: The purpose and impact of the CLOUD Act* [White paper]. https://www.justice.gov/archives/dag/page/file/1153466/download

Vedikaa. (2025). Digital sovereignty and India's data dilemma. *Jus Corpus Law Journal*, 5(2), 45–67. https://www.juscorpus.com/digital-sovereignty-and-indias-data-dilemma

Veracini, L. (2022). *Colonialism: A global history*. Routledge. https://doi.org/10.4324/9781003050599

Von Dingurth, L. (2025). The EU's pursuit of digital sovereignty through legislation. *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, 16(1), 34–56. https://www.jipitec.eu/issues/jipitec-2025

Wang, J. (2025). Transferring data to foreign authorities under the Chinese data protection law. *International Data Privacy Law*. Advance online publication. https://doi.org/10.1093/idpl/ipaf026

Wong, D., & Floridi, L. (2023). Meta's Oversight Board: A review and critical assessment. *Minds and Machines*, 33(1), 1–26. https://doi.org/10.1007/s11023-022-09613-x

World Economic Forum. (2025). What is digital sovereignty, and why does it matter for Europe? https://www.weforum.org/stories/2025/01/europe-digital-sovereignty

Yılmaz, Ö. (2025). The origins of digital colonialism. *İmgelem*, 9(16), 45–68. https://doi.org/10.53791/imgelem.1636282

Zeng, J. (2021). Artificial intelligence and China's authoritarian governance. *Chinese Journal of International Politics*, 14(3), 363–393. https://doi.org/10.1093/cjip/poab003