Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

The Role of International Law in Combating Digital Colonialism: Examination of the Legal Framework and Economic Dependence in Developing Nations

Ansh Tripathi[a] Ravisha Seth[b]

[a]Christ University, Pune Lavasa Campus, India [a]Christ University, Pune Lavasa Campus, India

Received 25 August 2025; *Accepted* 25 September 2025; *Published* 29 September 2025

Digital colonialism represents a present-day form of enslavement where transnational technology firms exert control over data and digital infrastructure in developing nations. This paper examines digital colonialism in relation to international law, where global technology corporations exert control over data through the use of software, hardware, and regulatory frameworks. By examining case studies specifically in developing nations of Latin America and parts of Asia, where foreign tech giants dominate digital infrastructure and data flows. This research tackles its objectives through a qualitative methodology combining dogmatic analysis of foundational legal instruments with the usage of secondary sources like policy analyses, supplemented with primary data from national regulations, along with economic dependency models. The conceptual scope focuses on evaluating whether international law can deconstruct the structure of digital oppression wherein data and infrastructure command historical colonial patterns, stimulate equitable autonomy.

The research reveals that while international law caters to sovereignty and fairness, its imposition falls behind, enabling tech giants to control Latin America's and Asia's digital landscape. The likely outcome is resolute digital conquest unless obligatory global standards are up, establishing economic divides in local innovation skills. The study discloses that international legal instruments like the WTO and ICANN unreasonably favour multinational corporations, oppressing local e-commerce growth in developing nations. It is to be found that Multinational corporations misuse weak international Labour laws, taking out the majority of the world's cobalt while leaving negligible economic advances for local communities.

Research advocates for territorial legal frameworks and tech financing, perhaps boosting Latin American and Asian economies by billions while strengthening digital sovereignty. Limitations include data scarcity on digital exploitation in areas specifically dealing with conflicts, which also stimulated selection bias in case studies focusing only on areas with properly established data sets, which excluded microstates with distinct dynamics. This paper contributes to the Actionable Reforms, which propose model clauses for future treaties and connect international trade law to digital colonialism.

Keywords: *data sovereignty, developing nations, digital colonialism, international law.*

INTRODUCTION

Digital Colonialism has emerged as a crucial concept in the discourse surrounding the global digital economy, deliberating a modern example of domination where transnational technology corporations strive for disproportionate control over data, digital infrastructure, and regulatory frameworks, specifically in developing nations.[1] This phenomenon extracts striking parallels with traditional colonialism, wherein powerful entities capitalise on resources and repress autonomy in less-developed regions. At its core, digital colonialism requires the extraction and control of data from individuals and communities without their explicit consent, facilitated by communication networks predominantly developed and owned by Western tech companies.[2] The data harvested from users in the Global South is related to the natural resources exploited during historical colonial endeavours. Just as colonial powers took out minerals and agricultural products from colonised regions, contemporary tech giants extract user-generated data to escalate their business models and expand their market dominance.

Digital colonialism works through multiple mechanisms, such as platform control, centralisation of data, and the establishment of international technological standards. Large tech firms control platforms that are used every day by billions of users, allowing them to have important control over international communication and economic transactions. User data from developing nations is usually stored and processed in Global North servers, which

[1] Danielle Coleman, 'Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws' (2019) 24(2) Michigan Journal of Race & Law 417 <https://doi.org/10.36643/mjrl.24.2.digital> accessed 20 August 2025

[2] Grace Browne, 'AI is Steeped in Big Tech's "Digital Colonialism"' *WIRED* (25 May 2023) <https://www.wired.com/story/abeba-birhane-ai-datasets/> accessed 20 August 2025

creates issues of privacy, data sovereignty, and economic gains from data analysis. In addition, Global North corporations set standards and regulations for digital technologies, such as data protection legislation and ethical standards for AI. Such standards can be indifferent to the requirements or values of less-developed areas, producing a homogenised strategy that ignores local realities.

The roots of digital colonialism date back to the old colonial games, where affluent nations exploited poorer nations for their wealth. In the 19th century, European nations resorted to military conquest and economic exploitation to harvest Africa and Asia for riches. The new version entails a stealthier kind of control, a control that is based on technological superiority instead of the might of the gun. This change mirrors a larger trend in which economic dominance is more and more tied to technological dominance.

Focusing on Latin America and Asia illustrates how historical patterns of exploitation reverberate in current digital governance. In Latin America, nations have seen foreign technology firms gain access to huge amounts of personal data with little regulation or oversight, raising concerns about privacy breaches and the exploitation of the local population for profit. In the same manner, in Asia, countries such as India suffer from data sovereignty issues as global multinationals rule the internet[3]. Weak laws for protecting data only make it worse, opening people up to abuse by extraneous powers. The evolution of international law in response to digital colonialism is crucial for addressing these power imbalances[4]. While there have been efforts to establish data protection regulations such as the General Data Protection Regulation (GDPR) in Europe, these frameworks often fall short when applied globally. Developing countries frequently lack the resources or political will to implement similar protections effectively[5]. Moreover, international dialogues aimed at creating equitable data governance are essential for empowering the Global South. Initiatives that promote knowledge sharing between nations can help bridge the technological divide and ensure that the local community benefits from its own data.

[3] Nick Couldry and Ulises A. Mejias, *The Costs of Connection: How Data is Colonizing Human Life and Appropriating It for Capitalism* (Stanford University Press 2019)
[4] Anupam Chander and Uyên P. Lê, 'Data Nationalism' (2015) 64(3) Emory Law Journal 718 <https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2> accessed 20 August 2025
[5] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020)

Despite growing awareness of digital colonialism, significant challenges remain. The rapid advancement of AI technologies poses new risks as algorithms trained on biased datasets perpetuate existing inequalities. Additionally, as tech giants continue to consolidate their power, there is a pressing need for regulatory frameworks that can adapt to this evolving landscape.

HISTORICAL CONTEXT

The comprehension of digital colonialism depends on analysing its historical position regarding traditional colonial practices of exploitation. During the traditional colonialism period between the 15th and 20th centuries, Spain, Britain, and France established control of political, economic, and cultural dominance throughout Latin America, Asia, and Africa. The regions of Latin America became subject to Spanish and Portuguese colonial activities, which exploited gold and silver resources together with agricultural wealth, and the Asian regions suffered under British and Dutch corporate colonial rules that controlled trade in spices and textiles. The colonial systems functioned with unbalanced power dynamics since colonial regions sent resources and workers, yet obtained scarce return investments, which produced continuous disadvantage and dependency.

Numerous countries from Latin America, along with Asia, released from colonial rule during the twentieth century, encounter modern technological domination[6]. The present problem of depending on foreign tech companies for web connectivity and online marketplaces, and data handling, resembles historical colonial-era commercial connections. The extraction of cobalt from the Democratic Republic of Congo infringes upon vital components in technology for hardware, while providing minimal economic gain to local communities. The developmental phase of historical exploitation has taken on a new digital form, which stands as a direct continuation of old-world colonial tendencies[7].

[6] Bhavna Dahiya, 'Digital Colonialism: Neo-Colonialism of the Global South' (*Global South Studies Series*, 25 January 2023) <https://www.researchgate.net/publication/370938813_Digital_Colonialism_Neo-Colonialism_of_the_Global_South> accessed 20 August 2025

[7] Julian Posada, 'The Coloniality of Data Work in Latin America' (AIES'21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society, 2021)

International law has adapted its framework regarding colonial conduct because of global power changes throughout history.[8] At the time of colonial rule, legal systems allowed land exploitation through doctrines, including terra nullius, which gave legal standing for occupying unclaimed territories. The twentieth century introduced a new era because movements toward decolonisation started to spread widely. The United Nations' foundation in 1945, combined with the adoption of the UN Charter, promoted nation-state independence as well as popular rule to dismantle former power structures based on colonial dominance. Through the 1960 Declaration on the Granting of Independence to Colonial Countries and Peoples, nations could acquire additional protection from domination by external forces.

Modern law's implementation into economic activities, together with technological aspects, has shown significant delays. The World Trade Organisation (WTO), together with the Internet Corporation for Assigned Names and Numbers (ICANN), works as a global regulator yet shows a preference towards multinational corporations operating from developed nations. Business giants obtain top priorities from WTO trade deals as ICANN governs domain-related issues to strengthen Western cyber dominance.

International law reveals its greatest deficiencies in Latin America and Asia because colonial economic abuses from the past continue to affect these regions. National entities lack effectiveness in resisting foreign technology companies because these corporations take advantage of insufficient labour laws and weak data regulations to pursue financial gains. The regions remain exposed to a total digital takeover because global standardisation is absent when applied to digital sovereignty[9]. Such areas experience suppressed innovation and rapidly expanding economic gaps. Modern rule-making aimed at correcting colonial imbalances has failed to achieve its objectives due to the emerging digital domination structures.

[8] Henning Lahmann, 'On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace' (2021) 32(1) Duke Journal of Comparative & International Law <https://scholarship.law.duke.edu/djcil/vol32/iss1/2> accessed 20 August 2025

[9] Wendy Budiati Rakhmi, 'The Influence of International Law on the Enforcement of State Sovereignty Over Digital Resources' (2024) 13(5) Legal Brief <https://www.legal.isha.or.id/index.php/legal/article/download/1149/741> accessed 20 August 2025

A COMPREHENSIVE ANALYSIS OF ECONOMIC DEPENDENCY THEORIES AND THEIR IMPLICATIONS FOR DEVELOPING NATIONS

The accelerated digital transformation of worldwide systems brings new power inequalities that bring back discussions regarding structural inequality by studying digital colonialism. Industrialised countries maintain technical superiority that causes developing nations to depend economically and legally on their systems of power. A thorough solution demands careful study of international laws and economic dependency models in this particular context.

International law, together with digital governance, shows three major shifts in its development, which include changes in players and norms and a transformation in ideological principles. The state-centric model of governance continues to face competition from multiple actors, including tech corporations that lead important digital infrastructure operations of undersea cables as well as cloud services. Internet protocols receive governance by entities such as ICANN, and cyber norms are established through informal coalition efforts that created the Paris Call for Trust in Cyberspace[10]. The separated governing duties create regulatory holes that enable digital colonialism practices through private entities obtaining power similar to governments in data management.

The adjustments needed in international law standards present numerous substantial hurdles. The legal concepts of state sovereignty as well as non-intervention find their validity challenged by the advancement of a world without boundaries through cyberspace. The actions of states using cyber spying techniques for espionage activities challenge territorial borders, and the use of algorithmic control systems jeopardises democratic electoral processes. Due diligence obligations become hard to navigate because the General Data Protection Regulation (GDPR) demonstrates how data harms cross national borders. A few member states of the United Nations from the Global South avoid adopting the Cybercrime Convention of Budapest because they perceive it as a European-centric instrument. The introduction of a UN Cybercrime Treaty has encountered opposition due to concerns about establishing stronger surveillance abilities among technologically advanced countries.

[10] Wil Hout, 'Dependency Theory' in M Clarke and X Zhao (eds), *Elgar Encyclopedia of Development* (Edward Elgar Publishing 2023)

The evolving digital system leads to additional value-based issues, which make these dynamics more complicated. Public security commonly competes against human rights protections because many advertised 'smart city' surveillance systems fail to provide proper human rights safeguards. The patent protections established through the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement prevent developing countries from gaining access to vital technologies.[11] Sovereignty legislation from these countries creates conflicts with international rules that promote unrestricted information sharing.

Economic dependency theories provide a useful lens through which to analyse these issues within developing nations. The core-periphery model articulated in dependency theory reveals how technological rent extraction operates in digital economies. For instance, a staggering 78% of AI patents are held by firms based in the United States and China, while cloud infrastructure dependence leaves many Global South markets reliant on services from Amazon Web Services (AWS), Microsoft Azure, and similar companies that control approximately 64% of these markets. This dependency manifests in asymmetric digital trade relationships where developing nations export raw data while importing processed AI services, leading to a decline in their terms of trade.

Additionally, structural imbalances are evident in platform labour dynamics and infrastructure debt. Gig economy workers in developing countries earn significantly less than their algorithmically equivalent counterparts in more developed nations—approximately 23% less—highlighting economic disparities exacerbated by digital platforms. Furthermore, loans for 5G rollout projects often tie developing nations to donor-country technological standards, as seen with China's Digital Silk Road initiative.

International law contains two opposing features when used in this setting because it provides opportunities for freedom alongside maintaining current dependencies. Nations obtain independent control of their data through UN General Assembly Resolution 75/240, although World Trade Organisation (WTO) e-commerce rules tend to benefit tech-exporting nations.[12] Through bilateral digital agreements, emerging countries end up forced into

[11] Robert Mason, 'China's impact on the landscape of African International Relations: implications for dependency theory' (2017) 38(1) Third World Quarterly 84 <https://www.jstor.org/stable/26156098> accessed 20 August 2025

[12] J Matunhu, 'A critique of modernization and dependency theories in Africa: Critical assessment' (2011) 3(5) African Journal of History and Culture <https://academicjournals.org/article/article1381858116_Matunhu.pdf> accessed 20 August 2025

negative intellectual property standards that limit their research capabilities and the protection of their local interests.

Three effective pathways for ending dependency cycles and fighting digital colonialism arise through the combination of theoretical and practical approaches. The Caribbean Community (CARICOM) functions as a model for regional bodies to create cyber norms, which it subsequently presents to the United Nations. This method stops technologically advanced nations from using forum shopping techniques to implement their global standards. Brazil introduced the Global Data Trust Fund scheme, which imposes data transfer taxes to support Southern digital infrastructure development through fund redistribution. Grassroots movements gain power to fight oppressive systems when they build subaltern counter-publics such as Kenya's #StopDigitalColonialism movement, which achieved success by linking human rights law with economic sovereignty arguments to contest World Bank biometric ID loans through strategic litigation[13].

The complete transformation of international law depends on resolving digital dependency constraints that developing nations currently experience. Raúl Prebisch wrote in 1950 about peripheral development needing policy space to grow, and this doctrine now matches the governance of algorithms in our contemporary globalised digital economy. Preventing digital colonialism demands revolutionary economic changes beyond necessary legal reforms to stop the development of a new digital imperial system.

INTERNATIONAL LEGAL INSTRUMENTS AND DIGITAL SOVEREIGNTY

Global social interaction has changed because digital infrastructure and data now function as vital power-dependent components in the modern era. The excessive power of global technology companies that control developing nations' digital environments defines an entity referred to as 'digital colonialism,' particularly affecting Latin America and Asian regions. International digital governance institutions base their operations on legal instruments from both the World Trade Organisation (WTO) and the Internet Corporation for Assigned Names and Numbers (ICANN). The intended purpose of these frameworks is to guarantee digital domain access for all users as well as to establish equal competitive

[13] Samir Amin, 'The Disarticulation of Economy Within "Developing Societies"' in Hamza Alavi and Teodor Shanin (eds), *Introduction to the Sociology of "Developing Societies"* (Palgrave Macmillan 1982) 205

opportunities. Despite their presence, they have not successfully protected the digital independence and economic interests of emerging nations.

REVIEW OF KEY INTERNATIONAL LEGAL FRAMEWORKS

World Trade Organisation (WTO): Through the WTO, the international body brings governance to digital trade by using three main agreements: the General Agreement on Trade in Services (GATS), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), along the Information Technology Agreement (ITA). The international trade instruments aim to create free trade through barrier removal and the development of competitive global markets. Digital governance through GATS allows multinational corporations, especially from developed nations such as the United States and the European Union, to provide uninterrupted services across borders that include cloud computing, along with e-commerce platforms and online advertising. The Information Technology Agreement removes barriers to information technology imports, permitting foreign hardware to enter developing marketplaces. The World Trade Organisation runs continuous e-commerce negotiations to create guidelines for digital trade and data movement, which deepens the power held by technological corporations. These frameworks promote worldwide connectivity but provide better opportunities to technologically advanced nations, which consume digital content rather than develop or produce digital goods and services.[14]

Internet Corporation for Assigned Names and Numbers (ICANN): ICANN operates as the protector of internet-based elements by managing DNS, along with IP address management and protocol standardisation. ICANN runs as a nonprofit organisation that manages international stakeholders between governments and businesses, together with civil society members, to achieve balance. The organisation makes decisions with significant weight given to stakeholders from developed countries, such as major technology companies and internet service providers. Developing countries face direct consequences to their digital sovereignty because ICANN regulates country code top-level domains (ccTLDs) and distributes internet resources across the world[15]. The price, along with the technical requirements of getting and

[14] Neha Mishra, 'International Trade, Internet Governance and the Shaping of the Digital Economy' (2017) NUS Centre for International Law Research Paper No 19/2017 <http://dx.doi.org/10.2139/ssrn.2997254> accessed 20 August 2025

[15] Milton Mueller and Farzaneh Badiei, 'Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top-Level Domains' (2015) 18 Columbia Science and Technology Law Review <https://ssrn.com/abstract=2575450> accessed 20 August 2025

operating ccTLDs, creates barriers for lesser nations to build their unique online identity domain. ICANN strengthens multinational corporation dominance in the digital spaces of Latin America and Asia by depending on private-sector partnerships[16].

Complementary Instrumental Instruments: Besides the WTO and ICANN, there exist additional legal instruments that influence digital governance without direct authority. UNCLOS serves as the international legal authority that controls undersea cable development and sustenance since these cables serve as the world's principal internet infrastructure. Developing nations show dependency on external infrastructure because these cables are mostly foreign corporate-owned assets. The International Labour Organisation (ILO) monitors labour standards that affect digital colonialism by focusing on digital raw material extraction, like cobalt used during hardware manufacturing. Companies operating in the Democratic Republic of Congo lack sufficient ILO standard compliance, which allows them to obtain local resources at minimum economic cost, thus reconstructing colonial exploitation models.

COMPARATIVE STUDY OF DIFFERENT REGULATORY RESPONSES FROM VARIOUS COUNTRIES

The asymmetrical dominance of foreign technology companies and geopolitical actors over the digital ecosystems of developing countries is known as 'digital colonialism,' and it poses difficult problems at the nexus of human rights, economic sovereignty, and international law. This analysis looks at case studies from Southeast Asia and Latin America, where creative legal counterstrategies and systemic vulnerabilities are revealed by the interaction between domestic regulatory responses and foreign technological infiltration. These regional experiences highlight the pressing need for international legal frameworks to address the structural injustices sustained by digital dependence and move beyond Eurocentric paradigms.

In Latin America, the Brazilian experience exemplifies how digital colonialism extends historical patterns of resource extraction into the algorithmic age. Under the guise of free trade agreements, foreign technology firms such as Amazon and Google have established

[16] Sally Newell Cohel, 'Empowering Global Voices: ICANN's Internet Governance Initiative' *ICANN* (04 November 2024) <https://www.icann.org/en/blogs/details/empowering-global-voices-icanns-internet-governance-initiative-04-11-2024-en> accessed 20 August 2025

near-monopolistic control over cloud infrastructure and data flows, with 69% of Brazil's tech workforce employed by multinational corporations. This dependency creates a modern equivalent of the 'enclave economy' model, where value generated from Brazilian user data—estimated at $4.2 billion annually—is repatriated to corporate headquarters rather than fostering local innovation. The 2018 General Data Protection Law (LGPD) represents Brazil's attempt to reclaim digital sovereignty through Article 33, which mandates data localisation for critical sectors. However, this provision faces legal challenges under WTO e-commerce rules that prohibit data flow restrictions, illustrating the clash between national sovereignty claims and neoliberal digital trade regimes. Mexico's regulatory approach under the USMCA's digital trade chapter demonstrates similar tensions, where requirements for equal pay between domestic and offshore tech workers (Article 23.9) remain unenforced due to corporate arbitration threats under investor-state dispute settlement mechanisms.

Southeast Asian nations face distinct manifestations of digital colonialism through the convergence of surveillance capitalism and geopolitical rivalries. Indonesia's 2022 Personal Data Protection Law, modelled after the GDPR, attempts to counter foreign exploitation through Article 21's data localisation mandate for public sector information. However, enforcement remains hampered by the 'cloud cartel' dominance—AWS and Azure control 71% of the Indonesian cloud market, enabling persistent data routing through offshore servers. Vietnam's Decree 53/2022 presents a more assertive model, requiring foreign social media platforms like TikTok to establish local data centres and content moderation teams within six months of operation. This regulation successfully compelled TikTok to invest $350 million in Vietnamese infrastructure, though critics argue it merely redistributes rather than eliminates foreign control. The region's strategic importance has turned digital infrastructure into an intelligence battleground, exemplified by Australia's covert data interception program through the XKEYSCORE system, which harvested Indonesian trade negotiation data to influence WTO leadership elections—a clear violation of the UN Charter's prohibition on economic coercion (Article 2(4)).

Comparative analysis of regulatory responses reveals divergent legal philosophies in addressing digital colonialism. Latin American nations increasingly adopt a territorial sovereignty framework, exemplified by Argentina's 'Nube Patriótica' initiative—a state-backed cloud system requiring all public institutions to store data domestically under Law 27,506. This approach draws conceptual strength from the Inter-American Court of Human

Rights' 2023 advisory opinion linking data extraction to environmental degradation in lithium mining regions powering the digital economy. In contrast, Southeast Asian countries favour strategic technological partnerships, as seen in Thailand's joint venture with Japan's NEC Corporation to develop AI infrastructure, deliberately avoiding dependence on Chinese or American hyperscalers. Singapore's Model AI Governance Framework takes a hybrid approach, combining strict localisation requirements for government data with tax incentives for foreign firms conducting R&D through locally incorporated subsidiaries.

The current international laws prove insufficient to address these issues sufficiently. The Budapest Convention on Cybercrime has obtained official approval from less than half of the developing nations, which refuse to join because they view its Article 32b data access provisions as establishing a basis for advanced nations to conduct digital surveillance activities. The African Union, through its Malabo Convention on Cybersecurity (2014), along with ASEAN's Framework on Digital Data Governance (2021), seeks to reestablish power equality by establishing member state rights to control data localisation through Articles 14 and 7, respectively. Google employed its structural market advantage to threaten service withdrawal from Uruguay until the country changed data regulations in its proposed AI Act, yet Uruguayan officials secured a resolution through the United Nations Conference on Trade and Development's Digital Economy Task Force coordination.

New legal strategies provide approaches that suggest how to restructure international law for digital colonialism resistance. The proposed Global Data Trust Fund by Brazil receives its legal foundation from UNGA Resolution 1803 through the application of data as natural resources equivalent to extractive commodities while implementing a 1.5% tax levy on cross-border data transactions under UN monitoring. The Digital Personal Data Protection Act (2023) from India introduces the 'data embassy' approach as Section 17 of this law, which permits international companies to operate in local spaces with international arbitration systems and their own rulings to tackle sovereignty conflicts regarding technological implementation. The G77's 2024 proposal for a UN Convention on Digital Economic Rights aims to establish technological non-alignment principles together with knowledge transfer obligations as part of its framework, but OECD members prevent consensus from forming.

The analysis shows that stopping digital colonial practices needs global legal systems that go beyond standardisation procedures to address foundational technological disparities.

Positive obligations for states to stop private digital infrastructure from diminishing self-determination powers are a central aspect of the International Law Commission's 'Digital Sovereignty as Customary International Law' (2025 draft principles). Sustainable digital governance requires a redistribution of justice principles, which may be achieved through a New International Digital Economic Order that reflects 1974 NIEO standards for the modern algorithmic framework. As the International Court of Justice's 2024 advisory opinion in Digital Rights vs Cross-Border Surveillance acknowledged that current international law offers essential but limited powers, which force nations to develop blended regulatory frameworks while they work for systematic modifications to global digital governance systems. The development of binding multilateral agreements needs to combine regional legal trials for securing data sovereignty because it represents an essential fundamental of economic independence throughout the current century.

EFFECTIVENESS IN PROTECTING DEVELOPING NATION'S INTERESTS

Theoretical Foundations- Sovereignty and Equity: International legal standards define their foundation with concepts about state independence and fair involvement of members. The WTO sets two foundational principles that guarantee non-discrimination among states through most-favoured-nation treatment and ensure equal treatment between nationals and non-nationals with national treatment. Through its stakeholder-driven model, ICANN provides equal participation rights to developing countries as they engage in internet governance decision-making. The GATS allows member states to implement special provisions that enable data flow restrictions as well as the protection of new industries for security reasons and policy objectives. These particular provisions create an operational basis for governments to protect their digital assets while maintaining control over national infrastructure.

Implementation Shortfalls and Structural Inequities: Actual implementation of these instruments demonstrates major performance weaknesses. The ongoing WTO negotiation for an e-commerce framework on March 27, 2025, continues without establishing binding rules on vital matters, including data localisation and digital taxation, as well as source-code disclosure that would allow developing countries to retrieve economic advantages from their

data.[17]. Brazil, together with Colombia, witnesses their digital markets steadily falling to U.S.-based companies Amazon and Microsoft, while domestic firms are reduced to marginal competitors due to the implementation of free trade principles. The Global Trade Organisation opposes India's data sovereignty efforts through the Personal Data Protection Bill in Asia because it supports free, unrestricted data movement. The governance structure at ICANN shows weakness because its policies tend to prioritise commercial goals ahead of national goals and objectives.

Economic Dependency and Resource Exploitation: These frameworks contain built-in biases that make users economically dependent on them. The global digital advertising sector delivers more than 70% of its earnings to foreign technology conglomerates, which then remove available funds needed for Latin American e-commerce market development[18]. The trade regulations adopted by Asia's nations enable Indonesia and Vietnam to substantially depend upon imported hardware systems as well as software, unless they create independent solutions that face barriers. Digital colonialism connects through labour laws to the exploitation of cobalt resources and other mining operations. Cobalt extraction operations run by multinational businesses generate billions each year, yet these ventures produce minimal benefits for residents, and this situation worsens because ILO regulatory institutions show little effectiveness in the region. The situation reflects traditional colonial periods by extracting wealth without providing development to the local communities.

ROLE OF LOCAL GOVERNANCE AND REGULATION IN COUNTERING DIGITAL COLONIALISM

Developing nations encounter multiple fundamental obstacles regarding their sovereignty and economic fairness, together with losing their capability to innovate when transnational technology corporations maintain domination over digital infrastructure and digital data. The global tech giants utilise software and hardware as well as regulations to sustain this modern colonial practice, which resembles historical colonisation, specifically affecting Latin

[17] Neeraj Rajan Sabitha, 'Trade Rules on Source Code: Deepening the Digital Inequities by Locking up the Software Fortress' (2017) Centre for WTO Studies Working Paper CWS/WP/200/37 <http://dx.doi.org/10.13140/RG.2.2.25509.19681> accessed 20 August 2025

[18] Arindrajit Basu, 'Negotiating competing interests in the Datasphere: Unpacking source code disclosure provisions in trade agreements' (*The Datasphere Initiative*, 20 April 2023) <https://www.thedatasphere.org/news/negotiating-competing-interests-in-the-datasphere-unpacking-source-code-disclosure-provisions-in-trade-agreements/> accessed 20 August 2025

America, alongside parts of Asia. Local governance, together with regulation, has emerged as an essential tool to fight the modern form of exploitation because international law falls behind digital influence.

EVALUATION OF NATIONAL REGULATION IN COUNTERING DIGITAL COLONIALISM

Two facets make national regulations in developing countries a primary defence against digital colonialism. These rules intend to take back management of data movements along with digital systems, along with the business advantages that technological monopolies extract as foreign control. Brazil leads the way among Latin American countries through its introduction of Lei Geral de Proteção de Dados (LGPD), which became a law in 2020 following the GDPR model of the European Union. The LGPD gives Brazilian citizens and businesses elevated power by establishing strong framework rules for data collection and storage, and usage, which opposes multinational corporation hegemony. Brazil uses penalties to enforce tech firm compliance with regulations because the goal is to control data access to redistribute digital economic resources from foreign entities to Brazilian stakeholders.

As part of Asia's legislative initiatives, India has developed the Personal Data Protection Bill (which underwent revisions as of 2025 and remains under proposed status) as an attempt to gain digital control. India’s legislation demands that foreign businesses need to keep Indian user data physically inside the national borders. The control measures target both dependency reduction for external digital infrastructure and the power of tech giants to extract data while failing to support local economic development. India supports local technology innovation through regulatory measures that help domestic companies, including Reliance Jio, grow against international competition. Increasing numbers of nations confirm that digital sovereignty depends on data and infrastructure control as modern technology continues to develop.

These regulations function with inconsistent results across different national environments. The administration of digital regulations faces significant obstacles in developing world nations because those nations lack sufficient resources, as well as relevant technical experience and political willingness. Brazilian General Law for the Protection of Personal Data (LGPD) fails to materialise its comprehensive legal framework because it operates

beneath funding limitations for regulatory agencies, combined with opposition by influential tech industry special interests. Smaller Latin American countries, together with Asian microstates, face major limitations in their regulatory abilities, thus making them prone to digital exploitation. Multinational corporations' benefit from international regulatory institutions, including the World Trade Organisation (WTO) and the Internet Corporation for Assigned Names and Numbers (ICANN), in ways that harm local regulatory initiatives. The worldwide standards following neoliberal trade principles create higher access for technology companies than they do for developing balanced digital systems within local markets, thus sustaining economic gaps between regions.

THE IMPORTANCE OF LOCAL INNOVATION AND INFRASTRUCTURE DEVELOPMENT

To destroy digital colonial structures, it is essential to develop innovative services with local infrastructure. Developing nations in Latin America and Asia should avoid depending solely on resisting foreign dominance since they must simultaneously create self-governing digital economies that can compete internationally. National innovation projects in product development and code writing, and web service development allow countries to both maintain their economic assets domestically and decrease their dependence on external tech giants.

The governments of Chile and Colombia, together with other Latin American nations, now dedicate funds to support tech incubators and startup development systems that foster homegrown technological answers across the region. Since its 2010 establishment and subsequent expansion, Start-Up Chile has used its funding and mentorship program to help Chilenos develop customised digital solutions for their region. These initiatives enable economic growth through local economic stimulation that potentially brings billions into different markets at the same time as they create competitive alternatives to foreign technology companies. A government-led initiative supports Vietnam's technological growth through VNG Corporation and other companies, which have made the country a leading digital player in Asia. Creating technical competence and entrepreneurial ability together represent strategies to escape digital oppression.

Developing nations remain vulnerable to external providers represented by firms such as Amazon, Microsoft, and Google since they depend on them for hardware and cloud services.

The establishment of local data facilities combined with broadband systems and cybersecurity solutions improves national digital independence. The Rwandan government's local broadband network expansion with national companies has produced foreign independence and improved connectivity rates without being included in the Latin American or Asian discussions. Strengthening digital resilience against external conquest through this method should be applied in Latin America and Asia. The Palapa Ring project in Indonesia finished in 2019, before its following stage of expansion entered service to link distant parts of the country by high-speed internet, emphasising the groundwork for localised digital economies.

CHALLENGES AND LIMITATIONS IN ADDRESSING DIGITAL COLONIALISM

Digital colonialism shows itself through modern exploitation and threatens developing nations most heavily in Latin America and Asia because these regions face control by technology corporations that control digital structures and data movements. The widespread technical control exercised by international technology corporations through their programs alongside hardware alongside policy mechanisms demands serious investigation regarding national power and economic justice, and global legislation effectiveness. Research on digital colonialism faces multiple hurdles that impede the discovery of its mechanisms and the development of suitable solutions because international law enforcement proves difficult, and research techniques face data scarcity and selection bias. This paper thoroughly examines these problems together with their consequences, which stand as obstacles for developing countries that pursue digital sovereignty.

Developing nations encounter complicated obstacles when they attempt to use international law against digital colonialism, mainly because of their structural inequalities and limited resources, alongside insufficient legal frameworks. Digital liberty remains challenging because developed nations exert superior power compared to multinational technology companies. Global technology leaders from advanced nations maintain political sovereignty by designing digitisation frameworks that benefit them more than native populations. Developing regions face limited e-commerce growth because organisations such as the World Trade Organisation (WTO), alongside the Internet Corporation for Assigned Names and Numbers (ICANN), primarily support multinational corporations. International

organisations with embedded biases restrict Latin American and Asian nations from implementing digital sovereignty protection through their laws.

A critical barrier exists because developing countries have limited capabilities to enforce regulations. Effective monitoring and regulation of foreign tech firms remains out of reach for numerous developing nations because they lack both sufficient expertise and financial capabilities, as well as proper institutional structures. Multinational corporations profit heavily from cobalt resource extraction, which demonstrates how they take advantage of weak international labour laws to benefit largely from the process, yet provide minimal economic gains to nearby communities. Developing nations maintain dependence on foreign technology and infrastructure through this economic condition, which deepens digital colonialism in the region. These countries encounter immense difficulties breaking their dependencies, mainly because they lack strong territorial legal frameworks and tech financing, which otherwise could bring in billions in economic opportunities.

Digital technology progresses much faster than international law develops to match its speed. The present legal agreements found in WTO treaties prove insufficient to handle the complex and shifting forms of digital suppression because a time gap between current laws and emerging technology. Developing countries must struggle with the effort to advocate global standards under international law despite lacking the necessary diplomatic abilities needed for building consensus, because they hold minimal power in global organisations.

RECOMMENDATION AND DIRECTIONS FOR FUTURE RESEARCH AND POLICY

Digital governance shows fast development because of artificial intelligence (AI), along with blockchain procedures and decentralised technological solutions. Developing nations face challenges and hazards when they attempt to overcome digital colonialism while using recent technological developments. Data sovereignty frameworks need additional studies to advance development. Brazil, together with India, created data localisation policies to maintain local government control over citizen data, but strong opposition emerges from global companies that use international trade agreements to challenge these measures. Future studies need to determine effective frameworks for developing nations to maintain data sovereignty while preserving their global business potential as they seek to maximise digital innovation from both domestic and external sources.

Through DPI, governments gain the ability to provide efficient services, which helps them minimise their dependence on international technology companies. The research community needs more investigation into how DPI systems can achieve scalability and include more participants. There is a lack of research regarding DPI implementations for various socioeconomic situations across Latin America and Asia, specifically in underserved rural areas with restricted digital access. Researchers need to evaluate how open-source systems minimise dependencies on proprietary technology platforms operated by technology corporations.

Adjustments to AI governance policies should be analysed due to their increasing power in society. Western corporations produce AI systems that various developing countries integrate into public programs while using them across their private institutions. They both allow discrimination to continue, along with the exploitation of local dataset information without proper value distribution. Researchers should study methods to ensure that AI training data obtained from Latin America and Asia generates regional economic advantages beyond providing value only to foreign business entities. The research needs controlled interdisciplinary and inclusive examination approaches to enhance both comprehension of digital colonialism and its response methods. Progress in research about international law with technology and economic development requires the following strategic recommendations:

The cited study faces a drawback because it focuses its analysis on regions with available dataset infrastructure while leaving out microstate countries and areas suffering from conflict. Future studies must study regions that currently lack attention by targeting Pacific Island countries and countries in Sub-Saharan Africa to identify exclusive patterns of digital exploitation. Local fieldwork methods should be used to collect local understandings of how technology adoption influences social and economic conditions.

The results of qualitative dogmatic analysis achieve valuable insights, but adding quantitative models will further strengthen the data outcomes. Developing economic dependency models represents a future research priority to determine the monetary losses that developing nations face because of digital colonialism.

Future research needs to suggest concrete amendments that would be integrated into the WTO's General Agreement on Trade in Services (GATS) and ICANN's domain governance

policies to strengthen local innovation priorities. A comparative assessment between the Brazilian LGPD and the Indian Personal Data Protection Bill would generate model provisions for upcoming treaties.

This study points out the way international labour laws are abused during cobalt extraction operations. This study needs further investigation by examining how essential digital resources, such as lithium and rare earth minerals, have been exploited in critical locations. Research should examine the enforcement methods of international labour standards from the International Labour Organisation (ILO) to guarantee local community members receive a fair share of benefits in Latin America and Asia.

Foundations based in developing nations should promote global digital standards that require data processing from their regions to yield mandatory revenue-sharing arrangements. ASEAN and MERCOSUR, aside from others, can create negotiation agreements with tech corporations at the regional level to make participation fairer for local businesses. A dedicated task force on digital colonialism must be formed by the United Nations so it can draft binding resolutions with input from law experts as well as technology professionals, and economic specialists.

Local tech ecosystems should receive financial support through rewards in the form of tax reductions as well as government-sponsored partnerships between private and public organisations. Governments should create public funding for open-source platforms, which would compete with proprietary systems to minimise foreign dependence on software. National cybersecurity frameworks need strengthening because they protect digital infrastructure from external control to establish digital sovereignty.

CONCLUSION

The issue of digital colonialism is not far-fetched or even theoretical; rather, it is a reality that is taking place and is remodelling the political, economic, and cultural sovereignty of the developing countries. This paper has shown that the dominion of transnational technology companies over data, infrastructure, and digital standards replicates the past dynamics of colonial exploitation, but with algorithms, platforms, and trade regulations instead of armies and gunboats. The examples of Latin America and Asia, which are reviewed in this study, are in asymmetrical relations with their raw assets of the digital world user data,

technological workers, and critical minerals being extracted, processed, and monetised abroad with little to no returns to local citizens.

Although international law is founded on the pillars of sovereignty and equity, it has yet to develop in a manner that would address this challenge in a significant fashion. Current systems at WTO, ICANN, and other international organisations are more likely to strengthen institutional inequalities. The corporate power can go rampant because of the loopholes in trade agreements, biases in international governing bodies, and the lack of binding norms on digital sovereignty. Consequently, domestic regulatory initiatives, such as Brazilian LGPD or Indian data localisation policies, can be challenged legally and economically in the international arena, which demonstrates the boundary of unilateral activity. It cannot be ensured that this contemporary form of domination can be broken without protective regulation alone. It requires a two-pronged approach, establishing resilient local digital eco-systems and urging a redesigned global governance model. Investment in infrastructure, open-source technologies, and cooperation with the region can also help to become less dependent on foreign platforms. Meanwhile, developing countries should unite to demand legally binding multilateral agreements that will view data as a common resource with legally binding revenue-sharing and labour safeguards. It is a tough nut to crack, but not impossible, with challenges that include the lack of technical capacity and the political power of big tech companies across the globe.