UCP Journal *of* Law & Legal Education
Vol. 3, Issue 2 (January – June 2025)

Digital Colonialism: Big Tech's Impact on Pakistan and the Global South

Usama Bin Zafar*

Abstract

This paper analyses digital colonialism as a contemporary form of neocolonialism, with emphasis on its impact on Pakistan's data governance and cybersecurity framework. It investigates how multinational technology corporations, backed by international institutions, shape regulatory structures, deepen economic dependency, and erode national sovereignty in the Global South. The study employs a doctrinal legal approach, supported by a comparative analysis of international instruments and domestic statutes. Pakistan's Personal Data Protection Bill 2023 and the Prevention of Electronic Crimes Act 2016 are critically evaluated against benchmarks such as the European Union's General Data Protection Regulation and India's Digital Personal Data Protection Act 2023. Primary and secondary sources, complemented by expert insights, inform the assessment of enforcement capacity, institutional design, and compliance with global norms. Findings indicate that Pakistan's legal regime remains fragmented and weakly enforced, leaving it vulnerable to surveillance capitalism, unregulated cross-border data flows, and tax avoidance by Big Tech. The Digital Nation Pakistan Act 2025, while ambitious, further illustrates regulatory incoherence by prioritising state control over user rights and omitting safeguards comparable to international best practice. The paper contributes to legal scholarship by situating Pakistan's experience within a Third World Approaches to International Law framework, showing how global trade and regulatory regimes reinforce asymmetries. It concludes with policy reforms aimed at strengthening privacy protection, enhancing enforcement, and advancing digital sovereignty.

Keywords: Digital Protection and Privacy, Cybersecurity Law, Digital Sovereignty, Surveillance Capitalism, Big Tech Regulation.

* Judicial Law Clerk, Islamabad High Court, Islamabad, Pakistan. email: usamabinzafar44@gmail.com

Article History: Received: 20 May 2025; Received in revised form: 29 September 2025; Accepted: 16 October 2025
Available online: 20 October 2025
DOI: https://doi.org/10.24312/ucp-jlle.03.02.558

Introduction

The world stands on the brink of a digital renaissance. The Fourth Industrial Revolution is reshaping the global economy and altering relations between the North and South. At its centre lies "data", the lifeblood of the digital economy, collected and monetised largely by Western technology corporations. This arrangement is often presented as altruistic, promising growth for developing countries. Yet beneath the language of digital progress lies an imperial project seeking to consolidate a new global order.

This paper examines how Western powers, through Big Tech and international institutions, drive this project of digital colonialism. It asks: how does digital colonialism reshape the legal and policy space of developing countries, and what specific vulnerabilities in Pakistan's governance framework make it especially exposed? By situating Pakistan within wider Global South struggles, the paper highlights how digital dependency is entrenched through both domestic weaknesses and international regimes.

The objective of this research is to identify the policy gaps that compromise Pakistan's digital sovereignty and to propose actionable interventions through comparative legal analysis, drawing on how other jurisdictions have sought to safeguard their autonomy in the face of global technological dominance.

This study employs a qualitative, comparative legal methodology to examine Pakistan's data governance framework within the context of digital colonialism. The analysis relies on primary, secondary, and tertiary sources, each serving a distinct role in the research process.

Primary sources include enacted Acts, tabled bills, regulatory notifications, and international treaties and agreements. These materials were examined through in-depth textual analysis of their provisions to determine the scope of state authority over data, the allocation of enforcement powers, and the design of institutional responsibilities. This analysis established the baseline for identifying gaps in Pakistan's legal framework and assessing the extent to which it protects or compromises digital sovereignty.

Secondary sources consist of peer-reviewed journal articles, academic monographs, and policy reports. They provided the conceptual foundation for this study, particularly in relation to

digital colonialism, sovereignty, surveillance capitalism, and dependency. Sources were selected for their academic credibility, focus on the Global South, and relevance to the intersection of law and technology. The literature was synthesised thematically and compared with findings from primary sources to expose points of convergence and divergence.

Tertiary sources comprise expert insights gathered through semi-structured interviews with legal scholars, regulators, and practitioners in data protection. Their contributions were coded thematically to identify recurring concerns, including weak enforcement, fragmented mandates, and risks of regulatory capture. These perspectives were triangulated with primary and secondary materials to test whether theoretical critiques align with practical constraints observed in Pakistan's regulatory environment.

The comparative element evaluated regulatory models from the European Union, India, and Kenya. These jurisdictions were selected because they reflect distinct approaches to reconciling cross-border data flows with digital sovereignty. Each was assessed against three indicators: legislative comprehensiveness, enforcement mechanisms, and institutional independence. Lessons from these models were then applied to Pakistan to generate actionable policy interventions.

This study is limited to governance and legal aspects of data protection. It does not address technical mechanisms such as encryption, network security, or engineering standards. Its contribution lies in systematically combining in-depth textual analysis of legislative provisions, critical scholarship, and practitioner perspectives to provide a nuanced account of Pakistan's vulnerabilities and to propose targeted reforms for strengthening digital sovereignty.

Literature Review

This paper draws on a structured body of primary, secondary, and tertiary sources to situate the debate on digital colonialism. Primary sources, including legislation, policy briefs, and international agreements, provide formal grounding for understanding how states regulate data and where authority is exercised or ceded. Secondary sources, in the form of scholarly articles, academic studies, and policy papers, offer theoretical

interpretations of concepts such as digital imperialism, surveillance capitalism, and the commodification of data. These works frame the global power asymmetries that shape digital governance. Tertiary sources, derived from insights of data privacy experts and practitioners, highlight the practical challenges of enforcement and ensure that policy recommendations remain anchored in institutional realities.

The scholarship identifies recurring themes. Studies on digital imperialism emphasise how international trade regimes and institutional arrangements constrain regulatory autonomy in the Global South. Work on surveillance capitalism highlights the monetisation of human behaviour through data extraction, raising questions of privacy and state sovereignty. Research on data commodification examines how everyday digital interactions generate value that is appropriated without compensation, particularly from populations in developing countries. Together, these strands provide a conceptual framework for analysing how Big Tech reproduces global hierarchies.

Historical Context

It is pertinent to briefly elaborate on the historical context of colonialism before delving into the nuances of digital colonialism. In the annals of colonial history, Africa witnessed the incursion of earlier colonialists, drawn by the prospect of abundant resources (Anand 1962). International Legal Scholar Michael Kwet (2019) aptly explains how the early European powers navigated the shores of Africa in pursuit of valuable commodities like diamonds, gold, and other precious minerals, establishing colonial outposts across the continent. The exploitation of these resources fuelled the industrial revolution in colonial powers, often involving forced labour and exacerbating the exploitation of Indigenous populations (Kwet, 2019).

Similarly, in India, the East India Company epitomised classical colonialism. Exploiting the rich resources of India, the corporation exported raw cotton to the 'Dark Satanic Mills' of Victorian England, only to ship back manufactured cloth, generating vast profits (Arora & Thapliyal, 2019). India's famed handloom industry was decimated, exemplifying how the economic pursuits of

colonial powers undermined local industries (Arora & Thapliyal, 2019).

Unlike their colonial predecessors, today's colonialists operate in the digital arena, with the modern slogan being to conquer the digital realm (Coleman, 2019). Similar to the East India Company's historical role, multinational corporations (MNCs), specifically Big Tech entities, play a pivotal role. Despite lacking direct representation in traditional international legal structures, these corporations wield considerable influence. Their power is threefold: structural power derived from substantial economies, instrumental power allowing them to shape institutions and influence policymaking, and discursive power involving the systematic production of knowledge and the shaping of political discourses (Arora & Thapliyal, 2019). Besides dictating the practical dimensions in the digital landscape, the tripartite power structure also moulds the global ideology around data, technology, and their impact on sovereignty in the digital age. In essence, Big Tech corporations are a representation of contemporary East India Companies, which establish a form of digital imperialism which transcends national borders.

Defining Digital Colonialism

Digital colonialism, as defined by Danielle Coleman, often without explicit consent, is a decentralised extraction, control, and commercial use of data from citizens by employing communication networks developed and owned primarily by Big Tech companies (Coleman, 2019). This subtle form of colonialism can be regarded as a contemporary manifestation of neocolonialism, extending the historical power dynamics into the digital landscape of former colonies.

Digital colonialism, similar to neocolonialism, is characterised by the dominance of developed Western nations and powerful tech corporations that exert control and exploitation over data. This control influences cultural narratives and moulds the global digital infrastructure, thus reflecting the historical patterns of cultural influence through the lens of neocolonial relationships.

Digital colonialism embodies the modern-day ‘economic dependency theory’, where developing states fall short of the digital infrastructure to fully capitalise on their data, thus being dependent

on Big Tech corporations from the West (*Muhammad, 2024*). In essence, digital colonialism illustrates the economic imbalances. It is also reminiscent of power structures of neocolonialism in today's digital age.

Structural and Operational Mechanics

Before digging deep into the dynamics of digital colonialism, it becomes crucial to understand its structure and the operational mechanisms that follow. Digital colonialism unfolds through various dimensions, from economic dominance to cultural influence and surveillance capitalism. The primary actors in this complex structure are Western Big Tech giants, which include but are not limited to Google, Meta (Facebook, WhatsApp, and Instagram), Uber, TikTok, among others (Coleman, 2019). These Big Tech corporations harness significant technological prowess for extensive and expansive data harvesting.

Through collaboration with the second key actors, consulting and advertising firms, they employ targeted advertising strategies to maximise profits through personalised messages (Coleman, 2019). Moving on to the third actors that involve local entities enlisted by Big Tech services to advance their specific agendas within their respective countries. Citizens become both the data sources and targets of personalised ads, representing the commodified labour within this intricate structure (Coleman, 2019).

This collaboration of actors highlights the pervasive nature of digital colonialism, where foreign powers control the technological landscape, forge narratives, and commodify individuals' digital labour for economic gains. Besides the three actors, international institutions play a substantial role in the creation of tech hegemony. These institutions are pivotal reasons why third-world countries struggle to cast off the yoke of colonialism. The perverse role played by these hegemonic institutions is discussed below.

International Institutions as Tools for Hegemony

B.S. Chimni (2004), an Indian international legal scholar known for his contributions to Third World Approaches to International Law (TWAIL), has aptly characterised international institutions as tools for legitimising the hegemony of the West.

Developing upon Gramsci's concept of hegemony, in his works, he makes a compelling case that international institutions, such as those established under the Bretton Woods system (IMF, World Bank), are often structured in a way that serves the interests of powerful states, particularly the global North (Chimni, 2004). He critiques these institutions for promoting neoliberal economic policies that may not be in the best interest of developing countries (Chimni, 2004).

In his recent work, 'International Institutions Today: An Imperial Global State in the Making', Chimni (2004) presents a compelling argument on how the World Trade Organisation (WTO) is another institution within this framework, acting as the corporate heart, advancing the interests of Big Tech while undermining the economic sovereignty of Third World nations. The influence of Western powers over the WTO is evident in various instances. For example, the Doha Development Agenda (DDA), initially designed to address the aspirations of the Third World, has been largely discarded in favour of advancing the principles of Neo-Globalisation (Chiming, 2004). This shift is marked by a focus on deregulation, decentralisation, and privatisation, reflecting the interests of digitally advanced states and powerful entities like Big Tech corporations (Kelsey, 2018).

The introduction of 'new issues' for WTO negotiation, particularly the controversial push for the liberalisation of electronic commerce (e-commerce), exemplifies this alignment with Western interests (Kelsey, 2018). Influenced by giants like Apple, Amazon, Google, Microsoft, and Facebook, these digitally advanced states seek to deregulate e-commerce, facilitating an unrestricted flow of data across borders to maintain oligopolistic control over developing country markets (Gurumurthy, Vasudevan, & Chami, 2017). This pattern echoes historical instances where the WTO served the interests of Western powers, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), shaping public international law to favour private interest (Gurumurthy, Vasudevan, & Chami, 2017).

In a similar vein, Big Tech companies aim to codify their interests into WTO law, utilising mega-market trade agreements like the Trans-Pacific Partnership 2016 (TPP), both independently and as bargaining chips (Chimni, 2004). Notably, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership, 2018 (CPTPP) chapter on e-commerce reinforces market freedoms, limits

regulatory autonomy, and impedes developing countries' ability to realise the economic value of their data, perpetuating the digital divide (*Agrawal & Mishra, 2022*). Thus, WTO, characterised as a hegemonic institution, operates without being held accountable for the consequences of its actions. This creates a Kafkaesque scenario where the people of Third World nations find themselves unable to hold either their own governments or the WTO responsible for the erosion of their domestic e-commerce industry.

Big Tech Wreaking Havoc on the Global South: An International Perspective

By monopolising the digital landscape, Big Tech corporations exercise direct authority over computer-mediated experiences, influencing political, economic, and cultural domains (Chimni, 2004). This contemporary imperial control and its consequences are discussed below:

Surveillance Capitalism

Digital colonialism's foremost consequence is the rise of surveillance capitalism, a concept extensively scrutinised by Harvard Professor Shoshana Zuboff (2019) in her seminal work, ‘The Age of Surveillance Capitalism.’ Zuboff's (2019) exploration delves into the exploitation of user data by tech companies, predominantly in the West, for economic gains, effectively converting surveillance into a profitable business model.

Surveillance capitalism, according to Zuboff (2015), flips the traditional dynamics between people and capitalists, turning populations into subjects for data extraction. It hinges on collecting 'behavioural surplus'—extra data from our online activities (Zuboff, 2015). Think about it: every 'like,' purchase, or app log-in gets recorded and scrutinised for patterns, guiding targeted ads. Tech giants, including Google, keep widening their surveillance scope, gathering more data without even seeking informed consent. Similar to digital colonialism, it is stripping away our humanity by making us nothing more than data vessels. Zuboff (2015) aptly categorised it as a form of tyranny, thus warning about the potential manipulation fuelled by our personal data. We are not individuals anymore; we are just data points in the world of surveillance capitalism (Zuboff, 2015). Moreover, it also undermines our dignity,

yet another concerning aspect of this digital era. Surveillance capitalism is not just a technological concept, but it is a product of human-based business mode that relies on platforms and algorithms; hence, Zuboff has underscored the need for accountability; the companies making decisions must be held responsible for the wider implications of our online actions and decisions.

As illustrated by Michael Kwet (2018), the bedrock of surveillance capitalism lies in Big Data, as vast data collections are made intelligible by taking advantage of advanced statistics and artificial intelligence. Often referred to as the 'new oil,' this commodification of data transforms the intimate details of individuals' lives into a raw material for exploitation and profit (Kwet, 2018). This phenomenon thus results in profound implications, influencing user decisions based on purchasing capacity and exerting control over the information accessible to a vast audience. The nonfungible nature of operating systems further entrenches less affluent users into specific communication channels, echoing historical colonial practices of resource control (Wittkower, 2008).

Illicit Financial Flows (IFFs) and Tax Avoidance

Digital colonialism has also unleashed significant consequences on the economies of third-world countries, exemplified by illicit financial flows (IFFs) and rampant tax avoidance by multinational corporations (Iyer, Achieng, Borokini, & Ludger, 2021). The term IFFs encompasses various methods to minimise tax payments, including transfer mispricing, treaty shopping, and strategic location of assets. In Africa, tech giants like Google have exploited tax regulations and schemes like the ‘Double Irish Dutch Sandwich,’ resulting in annual tax avoidance losses estimated by the OECD to be $50 to 80 billion (Iyer, Achieng, Borokini, & Ludger, 2021). The United Nations Economic Commission for Africa (UNECA) places the value even higher, at about $89 billion. Uber's tax avoidance practices further exemplify this trend, with the company circumventing tax payments by categorising itself as a technology company rather than a taxi service (Iyer, Achieng, Borokini, & Ludger, 2021).

Data Extraction and Consumer Exploitation

Another major consequence of digital colonialism is the widespread extraction of data, especially by Western tech companies in Africa. Exploiting minimal data protection legislation, these companies collect user data, including consumer identities and behaviours, for profit. An example is WhatsApp's recent privacy policy update, allowing the sharing of user data with Facebook (Iyer, Achieng, Borokini, & Ludger, 2021). This aspect can also be better understood with a case study of Facebook's Free Basics initiative (Iyer, Achieng, Borokini, & Ludger, 2021). Presented as philanthropy, this initiative provides free access to basic online services without data charges. However, it collects user data stored on Facebook's servers, granting access to valuable insights on user behaviour (Solon, 2017). In India, protests against Free Basics led to its cancellation, with people arguing that it deepened Facebook's monopoly power, subjected users to censorship and surveillance, and highlighted the potential consequences of unchecked data extraction (Kwet, 2019).

Commodification of Digital Labour

In the neoliberal economy, the principles of free-market capitalism ease the exchange of commodities. However, the digital realm introduces a distinct form of capitalism, where users themselves become commodities through the extraction of their data (Wittkower, 2008). As Bruce Schneier (2015) aptly observes, 'If you're getting something for free, then you are the product yourself,' takes on profound meaning in this context. Big Tech Corporations, such as Google and Facebook, use vast troves of user data, utilising advanced technologies and algorithms to transform personal details into a valuable commodity (Wittkower, 2008). This process mirrors a new-age form of colonisation, where humans unwittingly become resources exploited for economic gain. Importantly, users generally do not give explicit consent to exchange their data, which these corporations then furnish to third parties for targeted advertising. Predictive algorithms use the extracted data to tailor advertisements to users (Wittkower, 2008). Notably, the concept of the commodification of labour and surplus value, as outlined by Karl Marx, becomes relevant here (Marx, 1867/1990). The raw data generated by unpaid human labour is the production, the refined data

by the Tech Corporation serves as the commodity, and the profits generated by selling this commodity to targeting companies constitute the surplus value, and the vicious cycle continues.

Contextualising Digital Colonialism in Pakistan

Like its fellow developing nations, Pakistan finds itself vulnerable to the dominance of Big Tech corporations, forming a concentrated oligopoly that permeates all sides of governance and societal movements operating in the digital realm. The vulnerabilities of Pakistan in the digital realm are explained below:

Conflict of Digital Sovereignty with Continued Dependency

Pakistan grapples with the challenge of achieving digital sovereignty while relying heavily on Northern corporations due to the absence of specific legislation safeguarding privacy rights (Pinto, 2018). The Global Cybersecurity Index (GCI) for 2020 underscores vulnerabilities, scoring Pakistan at 64.88 (Tribune, 2019). Establishing platforms like Facebook faces hurdles rooted in infrastructure limitations, economic barriers, and regulatory complexities. With only 46% internet penetration and 21% of the population using the internet, significant disparities in digital access persist (World Bank Group, 2022). Economic constraints, regulatory hurdles, and limited access to advanced technology compound the challenges. To overcome these barriers, a comprehensive strategy is required that addresses infrastructure gaps, promotes digital literacy, and fosters a favourable regulatory environment.

Pakistan's Compromises and Contradictions

It is a bitter reality that there is a lack of digital sovereignty in Pakistan, and the nation bears responsibility for this predicament. Pakistan’s involvement with international agreements such as the Trans-Pacific Partnership (TPP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) is translucent evidence of it. Pakistan is among seventeen developing nations that became part of the 'Friends of E-Commerce for Development,' seeing liberal e-commerce as a means to digital growth (Arora & Thapliyal, 2019). In contrast, countries such as India and other least developed nations, ones that align with the African group, resisted these agreements, recognising their

discordance with the aspirations of the developing world (Arora & Thapliyal, 2019). This is testimony to the fact that Pakistan has always bought into the 'myth of development' and pursued short-term gains without considering the broader consequences.

Pakistan needs to wake up to the reality that the promises of economic development under neoliberalism often fall flat when it comes to developing nations. For instance, CPTPP's Chapter 14 on Electronic Commerce exemplifies how such provisions prioritise market freedoms while constraining domestic regulatory autonomy (Leblond, 2019). This means no localisation measures or customs duties on data transfers, robbing developing countries of the economic benefits tied to their data. And let us not forget the complete absence of provisions for technology transfer and capacity building, leaving developing nations struggling to keep up with the digital revolution.

Could not a neoliberal framework that handcuffs restrictions on data flow, bans digital duties, and couldn't care less about nurturing local digital infrastructure seem like a raw deal for Pakistan? It is high time for Pakistan to learn from its past, step away from a CPTPP-style framework, and reclaim control over its digital sovereignty.

Data Privacy Legislation Gaps in Pakistan

The successive governments in Pakistan have introduced various pieces of legislation aimed at addressing data privacy concerns, making strides on the domestic front. It has recognised the right to privacy as a fundamental right enshrined in Article 14(2) of the Constitution of 1973. These notable legislative efforts include the Prevention of Electronic Crimes Act, 2016 (PECA) and the recently approved Personal Data Protection Bill, 2023 (PDPB) (Rehman, 2022). However, despite these efforts, the data of Pakistani residents is largely unprotected and vulnerable as a legislative vacuum persists in these legislations.

The swift adoption of Pakistan's 2023 Personal Data Protection Bill (PDPB) raises significant concerns, especially in light of its hurried enactment without due stakeholder engagement. The evident emulation of General Data Protection Regulation (GDPR), without adapting to Pakistan's unique context, signals a rushed legislative approach that overlooks the nation's distinctive dynamics (Akif, 2023). A comparison with India's Digital Personal Data Protection Bill, 2023 (DPDPA), offers valuable insights,

highlighting the pitfalls in Pakistan's current legislation (Akif, 2023). The Indian Data Protection bill is not without its flaws. Nonetheless, being a sister jurisdiction, it can serve as a constructive guide for Pakistani policymakers.

It is clear through the Central government's decision to adopt a graded enforcement strategy, the legislative approach in India's DPDPA is aimed at curbing the influence of Big Tech corporations. It entails the implementation of the law initially for major tech entities such as Amazon, Microsoft, Google, and Apple (Barik, 2023). In contrast, Pakistan demonstrates no clear legislative intent to mitigate the impact of big tech, as is evident from its Data Protection Act, which has promptly been established without a similar phased enforcement strategy. Yet another inherent flaw in Pakistan's PDPB lies in its heavy reliance on 'free, specific, informed, and unambiguous' consent under Section 6. Though it might appear reasonable, it utterly disregards the prevalence of dark patterns used by companies which are used to manipulate users into granting consent for extensive data processing activities. Such manipulative practices in the absence of robust safeguards pose a genuine threat to individual privacy, an issue better addressed in India's DPDA. Additionally, the incorporation of 'legitimate interests' in Pakistan’s context, which lacked clarity and safeguards, created potential room for misuse. The problem with this ground lies in its inherent vagueness: it allows data controllers to determine for themselves what constitutes a “legitimate” purpose, often without meaningful oversight or a requirement to balance such interests against the privacy rights of individuals. This ambiguity can easily be exploited to justify invasive data practices, mass profiling, or retention of personal information under broad claims of business necessity or innovation. In contrast, India has opted for a more specific and protective framework by wisely excluding *‘legitimate interests’* as a lawful basis for data processing, thereby narrowing the space for abuse and ensuring that any data processing must rest on explicit consent or clearly defined lawful grounds

Moreover, failing to align with the GDPR's clear scope reveals a significant legislative gap, especially considering the exclusion of national security issues. Pakistani policymakers need to reassess their approach, emphasising a nuanced understanding of conflicting interests, the protection of individual rights, and a forward-thinking stance to foster innovation and economic growth.

Akin to the comprehensive approach seen in India's DPDA, Pakistan's legislative efforts require a more inclusive and participatory dialogue with stakeholders. Thus, a recalibration is required of Pakistan's data protection legislation to address the identified shortcomings, and in the process, it can draw lessons from the more considered approach taken by India, its regional counterpart.

Taxation Challenges

Big Tech corporations that operate in Pakistan, such as Google and Meta, are present without full-fledged offices, evading local taxation (Hassan, 2023). Unlike in India, where Google pays substantial taxes on its reported revenue of INR 5,593 crore (about $757 million), in Pakistan, Google operates through a branch liaison office, Google Asia Pacific Pte. Ltd., based in Singapore (Hassan, 2023). This setup shields these companies from income tax and GST in Pakistan, as they exploit bilateral treaties like double taxation agreements. In Pakistan, the profit of Google is not disclosed (Hassan, 2023). This tax-free operation, coupled with jurisdictional issues, poses significant hurdles even if Pakistan establishes a data protection regime, as these laws may remain inapplicable due to the lack of local offices and the local court's jurisdiction.

Nexus of Big Tech and State Surveillance

There is an inextricable link between state oppression and how Big Tech corporations operate in Pakistan. State authorities and intelligence agencies also benefit from ineffective legislation for data privacy, and social media spaces in Pakistan are used by these agencies for silencing dissent, manufacturing consent, and spreading propaganda, as Ismat Shahjahan, a political worker and the President of Women Democratic Front, explains, 'Technology is susceptible to ideology; this was the case with old technology and is now also what is happening in regard to Big Tech in Pakistan (Rehman, 2022). Section 32 of the PDPB mandates organisations to share sensitive personal data with the government based on vague grounds such as 'public order' or 'national security'. Under the guise of these vague terms, the state seeks to establish a 'panopticon' for stifling dissent and shaping public opinion through propagandist measures.

This places Pakistan in a precarious position, akin to being caught between the devil and the deep blue sea. In the context of surveillance, the citizens' data becomes vulnerable to the dual influence of the profit-driven local state apparatus and Big Tech corporations from the West. Thus, 'digital authoritarianism' is another manifestation of digital colonialism in Pakistan.

A Failed Attempt: The Digital Nation Pakistan Act 2025

A more recent legislation introduced with the promises of transforming Pakistan into a digital nation is the Digital Nation Pakistan Act 2025, enacted on January 29, 2025. Lauded by the Pakistani media as a game-changer legislative piece that would redefine the digital landscape of Pakistan by enabling the digital economy, digital society, and digital governance (*The Nation*, 2025). The heightened expectations of imminent progress hope to bring about an accelerated economic development, enhanced public service, and foster citizen well-being (*Modern Diplomacy*, 2025).

The 30 Provisions Act submits several key aspects pertaining to data exchange, digital identity and digital governance. One of the notable aspects of the Act is that it defines 'data governance' as a set of processes ensuring effective security and management of data (Digital Nation Pakistan Act, 2025, s. 2(f)). Moreover, it also introduces a Data Exchange Layer, a framework that licenses standardised data sharing between the government and private enterprises while making sure the integrity, security and accessibility (Digital Nation Pakistan Act, 2025, s. 2(e)).

It also commemorates three distinctive yet overlapping regulatory bodies (Digital Nation Pakistan Act, 2025, ss. 3–10). First in line is the National Digital Commission, whose mandate is limited to the approval of substance and strategy for delivering the National Master Plan (Digital Nation Pakistan Act, 2025, ss. 5, 11). Hence, one of the pivotal tasks that comes under its ambit is ensuring coordination amongst federal, provincial and sectoral bodies; to review cases of non-compliance. Second in line is the Pakistan Digital Authority, which is created with the purpose of developing, updating and, most importantly, implementing the Masterplan (Digital Nation Pakistan Act, 2025, ss. 6–8). Lastly, the Oversight Committee, as the name suggests, is an independent watchdog established to review the performance of the Pakistan

Digital Authority and subsequently report its findings to the National Digital Commission (Digital Nation Pakistan Act, 2025, s. 9(1)).

The bodies crowded by the Government and bureaucracy have their more than fair share of flaws. Although a fair attempt to enlist 18 'permanent members' in the Commission such as chairpersons of FBR, Nadra, PTA, SECP, State bank, Prime minister, ministers and provincial minister yet its failure to include the chairperson of the Competition Commission of Pakistan suggests that the drafters are unaware of the critical need to balance innovation and competition in the digital economy (Darr, 2025). With the surging rise in the digital companies that operate on data-driven models and algorithms, the presence of the Competition Commission of Pakistan becomes ever more important to ensure that these firms don't harm the competition or the consumers through their unfair practices, especially when in a position of dominance. Moreover, in cases of mergers and acquisitions in the digital economy that come under the mandate of the Competition Commission of Pakistan, they require careful and detailed scrutiny because these firms' data acts as a currency. The data sharing due to these acquisitions can result in privacy concerns and data exploitation without explicit informed consent. Secondly, the vague eligibility requirements for the members of authority reflect the fundamental lack of clarity as to their specific mandate (Darr, 2025). Furthermore, the set-up is designed in a way that it is neither answerable to the legislature nor the judiciary, and also fails to impart how a Masterplan would be devised (Darr, 2025). These shortcomings of the regulatory bodies poke holes in the effectiveness of the Act, thus choking any hopes that it projected of developing Pakistan as a digital nation and resolving the challenges that the digital age brings.

However, the fractures aren't just over yet because the Digital Nation Pakistan Act 2025, when brought into light with the European Union's General Data Protection Regulation (GDPR) and various other US data protection laws such as the New York SHIELD Act or California Consumer Privacy Act (CCPA), a whole new bunch of shortcomings are exposed. However, since the Act does not explicitly and in precise form define the user rights, the concerns around personal data protection and potential misuse of sensitive information by private entities and government remain

unresolved, with cybersecurity yet another important element missing (Bukhari, Haq, & Shakoori, 2025). The Act lacks user rights and protection, making it less protective of individual privacy as compared to GDPR and US state laws. Despite being the latest legislation enacted in 2025, it lacks the provisions requiring informed user consent for data, something that the GDPR framework provides through consent-based data collection (*General Data Protection Regulation [GDPR], 2016, arts. 4(11), 6–7*), thus giving individuals significant control over their data. Moreover, there is an absence of strict obligations on data controllers, making it more liable to unauthorised access and potential breaches (Bukhari, Haq, & Shakoori, 2025). It is also ambiguous on the cross-border regulations and doesn't provide transparent provisions on international data transfers, thus exposing the Pakistani users to possible privacy risks in the process of data sharing (Bukhari, Haq, & Shakoori, 2025). In addition, the Digital Nation Pakistan Act 2025 fails to mandate the pseudonymisation techniques and anonymisation, thus exposing the data and compromising the individual's privacy. No doubt that the Act, in light of these flaws, is motivated by the need to consolidate the government's ownership, control, and manipulation of the digitisation process, thus failing to provide a comprehensive framework and structure that can address the challenges presented by the evolving digital colonialism.

However, unfortunately, following the footsteps of its predecessors, the Act falls short on its promises and is yet another failed and incomplete attempt at resolving the issues posed by the digital age, i.e., digital colonialism and the evils that follow. True to what Amber Darr (2025) suggested that the Act hides more than it reveals.

Policy Recommendations

To address the impact of Big Tech in Pakistan and the Global South, I have taken a novel approach to craft these recommendations by actively involving data privacy analysts. The recommendations, finding support from the perspectives and work of various data analysts, provide innovative solutions to resolve the problems posed by digital colonialism.

Global Standards of Data Privacy Legislation

The international statutes and conventions that align with the best practices have effectively countered the challenges and problems of the digital era and will provide a valuable design through which Pakistan can establish its own robust and effective data privacy legislation. First of all, the General Data Protection Regulation (GDPR) provides a detailed framework for transparent and responsible use of data. Moreover, issued in 1980, the Organisation for Economic Co-operation and Development (OECD) Guidelines impart a prized perspective and insights into resolving the cross-border data flow problems and challenges *(OECD, 1980, p. 2)*. Furthermore, the International Covenant on Civil and Political Rights (ICCPR) 1966 is another imperative statute that guarantees the protection of personal data through Article 17, right to privacy. International Telecommunication Union (ITU) Standards can play a vital role in further shaping the global norms in this domain (*ITU-T D.1141*, 2025). In addition, the Council of Europe Convention for the Protection of Individuals can help enhance the regulatory considerations with regard to Automatic Processing of Personal Data (Convention 108). Besides these international conventions and statutes, Pakistan can also learn from the domestic legislation model employed by other developing countries, such as India's DPDA. Another notable learning experience is the effectiveness of Kenya's approach reflected in Kenya's Data Protection Bill (2018), which is shaped to confront the issues created by Big Tech Companies. Thus, it can guide Pakistan in creating a robust regulatory framework. Seeking guidance from these global best practices, Pakistan can craft data privacy laws that not only address the unique challenges posed by the influence of Big Tech corporations but also safeguard individuals.

Revamping Tax Policies for Big Tech

The Federal Board of Revenue (FBR) should revamp its tax policies to cater for the challenges posed by the digital era. Laws should be passed so that these tech companies are mandated to establish a local physical presence, thus ensuring that they fall under Pakistani jurisdiction. Moreover, for Pakistan's economic independence, the local presence of tech firms must be encouraged.

In addition, the double taxation treaties with countries hosting these tech giants must be revised to prevent tax evasion and boost revenue. Furthermore, FBR should provide incentives and help facilitate the setup of data centres and offices of Big Tech Companies such as Google and Facebook within the country. Thus, fostering collaboration between the FBR and local/international tech entities would help balance global innovation with local capabilities, which will become pivotal in resolving these tax challenges.

Effective Cybersecurity Measures

To respond to the challenges posed by data colonialism, an attempt could be made to formulate an effective and constitutionally sound Cyber Security in Pakistan through valuable insights drawn from Julie E. Cohen's (2000) essay 'Examined Lives: Informational Privacy and the Subject as the Object'. Cohen's (2000) recommendations emphasise three key issues that must be addressed. Firstly, the legislation should define protection boundaries to exclude constitutionally privileged uses of personally identified data, besides carefully navigating the delicate balance between ownership and speech concerns. Secondly, it must establish clear parameters for meaningful and informed consent regarding the collection, exchange, and use of such data. Lastly, it should ensure responsible practices within the context of digital colonialism by subsuming additional safeguards to hold the data processing industry accountable to individuals and the broader society. These suggestions would ensure that the legislation is tailored to the specific digital dynamics of Pakistan, thus providing a solid foundation besides fostering a robust framework for Cybersecurity.

Inclusion of Data as a Resource under PSNR and NIEO

Pakistan, alongside the rest of the Global South, in an attempt to pursue a more equitable global economic order, should advocate for the inclusion of data as a resource within the frameworks of the New International Economic Order (NIEO) and Permanent Sovereignty over Natural Resources (PSNR) (Anghie, 2004). This policy recommendation aligns with the foundational principles of PSNR as it recognises data as a resource, emphasising

ownership, national control, and the right to derive maximum benefit from vital resources, including digital ones. Within the broader context of NIEO, the proposal supports fair trade practices, balanced wealth distribution, and empowerment of developing nations in the digital era. It urges these nations to collectively press for the acknowledgement of data as a central resource, ensuring that global economic structures, particularly within the WTO, consider the economic aspirations of the developing world in the contemporary landscape of digital colonialism.

TRIPS Framework: Charting Paths for Digital Governance

Fostering Data Ownership, Empowering Workers, and Embedding Corporate Social Responsibility, Pakistan should actively pursue comprehensive digital governance by engaging in international discussions, particularly within the framework of TRIPS, recognising the evolving nature of data as a valuable asset (Evans, 2018). While TRIPS may not directly address data ownership, its contribution to the broader framework of intellectual property rights can be leveraged.

Digital Empowerment: Activism and Unions for Change

To confront the escalating influence of Big Tech in countries like Pakistan, where the battleground is increasingly digital, there is a dire need for the establishment and reinforcement of digital activist organisations and digital trade unions. Pakistan should prioritise the establishment, facilitation, and strengthening of digital rights trade unions. It will help empower the workforce in the digital sector by advocating not just for improved working conditions but also equal rights and protection from exploitation. In the ever-evolving technological landscape, Pakistan can improve and solidify its efforts through educational programs and campaigns that will aim to enhance workers' awareness of their rights.

CSR Mandate: Ensuring Ethical Data Practices in Tech Companies

Technology companies in Pakistan need to integrate a Corporate Social Responsibility (CSR) mandate. This mandate

would ensure enforcement of secure and ethical data use practices while, in the process, requiring explicit user consent for data collection. Tech companies can actively promote responsible data handling and safeguard user privacy by embedding these CSR principles into their operations. This approach would ensure an effective and comprehensive digital governance framework in Pakistan.

Policy: Strengthening Protections Against Mass Surveillance

To resolve the problems caused by mass surveillance in Pakistan, a robust legislative framework needs to be established and implemented, which clearly defines and regulates surveillance activities, along with explicit legal consequences for violations. The first step in this direction would be amending the existing Personal Data Protection Bill (PDPB), which includes inch-perfect and unambiguous definitions of terms such as 'national interest' and 'public importance.' Thus, it would help establish a legal structure that would not just protect but also uphold the individual privacy rights. The revised legislation should incorporate accountability mechanisms to ensure transparency and prevent misuse. It should also mandate the concept of 'informed consent.' Thus, Pakistan can ensure a more secure and privacy-conscious digital environment by ultimately adopting this detailed approach.

Advancing Digital Democracy: Embracing FOSS and Cultivating a Digital Commons

Free and Open-Source Software (FOSS) represents a global movement that advocates transparency, collaboration, and user autonomy in software development. It emerged in the 1980s through the Free Software Foundation (FSF), founded by Richard Stallman, and was later expanded by the Open-Source Initiative (OSI), emphasising that software should remain freely accessible, modifiable, and shareable. FOSS has become the backbone of modern digital infrastructure, powering major systems like Linux, Android, and Apache, and serving as a counterbalance to the monopolistic tendencies of proprietary software. By promoting openness and collective innovation, FOSS enhances national digital sovereignty and supports capacity building within developing

economies (Free Software Foundation, n.d.; Open-Source Initiative, n.d.).

Strategically, Pakistan should embrace the principles of the Free and Open-Source Software (FOSS) movement. It will help ensure navigating the ever-evolving digital power landscape, besides countering the challenges and issues posed by proprietary software. The Government of Pakistan, in order to achieve this, must take the lead in promoting FOSS adoption in public institutions. It should also highlight the core values of user freedom and collaboration. Besides, its laws should be implemented to ensure explicit support in establishing digital commons for the growth and development of FOSS. These initiatives could be further reinforced by enabling protection and community ownership from proprietary dominance.

Moreover, creating open knowledge platforms motivated by successful models such as Wikipedia would facilitate creating a collaboratively managed and open knowledge repository. Furthermore, in the struggle of advancing digital democracy, educational initiatives can play a key role by raising awareness of FOSS benefits; however, safeguards should be put in place to prevent corporate interference. Gaining insights from previous cases where tech companies attempted to obstruct the shift toward open software ecosystems will be crucial in ensuring a sustainable and inclusive digital future for Pakistan.

Conclusion

In developing nations such as Pakistan, digital colonialism has become a critical obstacle to sovereignty and self-determination. The extraction of data, concentration of infrastructural power, and external shaping of governance frameworks reproduce older patterns of dependency in new digital forms. This research was an effort to examine these dynamics through the lens of Pakistan's legal framework, situating its experience within the broader discourse on the Global South and exposing how structural vulnerabilities compromise its ability to exercise control over its digital future.

The study adds value by linking broad critiques of digital imperialism to the specific gaps within Pakistan's legal and institutional framework. Through comparative legal analysis and practitioner insights, it exposed how fragmented legislation, weak

enforcement, and reliance on external infrastructure sustain dependency. In doing so, it bridged a gap in existing literature, which has often addressed digital colonialism in abstract terms without situating it in concrete regulatory contexts.

The findings underscore that digital sovereignty is neither an abstract aspiration nor a rhetorical claim but a measurable and urgent policy objective. By demonstrating how Pakistan's vulnerabilities map onto global structures of power, the research contributes a timely perspective to an evolving debate that carries implications well beyond Pakistan. Its impact lies in reframing digital colonialism as both a national and transnational governance challenge, one that must be confronted if developing nations are to secure autonomy, protect citizens, and shape a more equitable digital future.

References

Arora, P., & Thapliyal, S. (2019). *Digital colonialism and the World Trade Organization*. TWAILR. https://twailr.com/digital-colonialism-and-the-world-trade-organization/

Anand, R. P. (1962). Role of the "new" Asian–African countries in the present international legal order. *American Journal of International Law, 56*, 383–390.

Agrawal, B., & Mishra, N. (2022, August 26). *Addressing the global data divide through digital trade law. Trade, Law & Development, 14*(2). https://doi.org/10.2139/ssrn.4276764

Akif, O. (2023, October 30). Pakistan, India and the love for 'data protection.' *DAWN.* https://www.dawn.com/news/1784472

Anghie, A. (2004). *Imperialism, Sovereignty, and the Making of International Law.* Cambridge University Press. https://kingdomofhawaii.wordpress.com/wp-content/uploads/2011/04/anghie-imperialism-sovereignty-and-the-making-of-international-law.pdf

Barik, S. (2023, August 10). Data protection law transition period to be granted, Big Tech first in line, says MoS IT. *The Indian Express*. *https://indianexpress.com/article/technology/data-*

protection-law-transition-period-to-be-graded-big-tech-first-in-line-says-mos-it-8884871/

Bukhari, H., Haq, I., Shakoori, A. R. (2025, February 21). Digital Nation Act: a critique. *Business Recorder.* https://www.brecorder.com/news/40349203

Coleman, D. (2019). Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws. *Michigan Journal of Race and Law,* Volume 24:417. https://doi.org/10.36643/mjrl.24.2.digital

CPTPP Chapter 14: Electronic Commerce, Arts 14.3, 14.11, and 14.13.

Chimni, B.S. (2004). International Institutions Today: An Imperial Global State in the Making. *European Journal of International Law,* 15(1), 1-37. https://doi.org/10.1093/ejil/15.1.1

Cohen, J.E. (2000). Examined lives: Informational privacy and the subject as object. *Georgetown University Law Center,* 52, 1373-1437. https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub

Darr, A. (2025, March 8). Digital confusion in Pakistan. *DAWN.* https://www.dawn.com/news/1896580

Digital Nation Pakistan Act, No. 30 of 2025 (Pakistan).

European Parliament and Council of the European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119,* 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Evans, M. (2018). Why data is the most important currency used in commerce today.

Free Software Foundation. (n.d.). *What is free software?* https://www.gnu.org/philosophy/free-sw.html

Gurumurthy, A., Vasudevan, A., & Chami, N. (2017). The grand myth of cross-border data flows in the trade deals. *IT for Change.* *https://itforchange.net/sites/default/files/1470/dataflow-11am.pdf*

Hassan, T. (2023, August 7). Does big tech evade taxes in Pakistan, and what can we do about it? *Profit.* *https://profit.pakistantoday.com.pk/2023/08/07/does-big-tech-evade-taxes-in-pakistan-and-what-can-we-do-about-it/*

Iyer, N., Achieng, G., Borokini, F., & Ludger, U. (2021). Automated imperialism, expansionist dreams: Exploring digital extractivism in Africa. *Pollicy.* https://archive.pollicy.org/wp-content/uploads/2021/06/Automated-Imperialism-Expansionist-Dreams-Exploring-Digital-Extractivism-in-Africa.pdf

International Telecommunication Union. (2025, April). *ITU-T Recommendation D.1141: Policy framework and principles for data protection in the context of big data related to telecommunication/ICT services.* ITU. https://www.itu.int/rec/T-REC-D.1141

Kwet, M. (2019, March 13). *Digital colonialism is threatening the Global South*. Al Jazeera. https://www.aljazeera.com/opinions/2019/3/13/digital-colonialism-is-threatening-the-global-south

Kelsey, J. (2018). How a TPP-style e-commerce outcome in the WTO would endanger the development dimension of the GATS acquis. *Journal of International Economics, 21*(2), 273–295.

Kwet, M. (2018, June 29). Break the hold of digital colonialism. *Mail and Guardian*. https://mg.co.za/article/2018-06-29-00-break-the-hold-of-digital-colonialism/

Leblond, P. (2019, October). *Digital trade at the WTO: The CPTPP and CUSMA pose challenges to Canadian data regulation* (CIGI Papers No. 227). Centre for International Governance Innovation. https://www.cigionline.org/static/documents/documents/no.227.pdf

Muhammad, S. (2024, December 16). *Digital colonialism: Navigating new forms of servitude in Industry 4.0.* ROADS Initiative. https://theroadsinitiative.org/digital-colonialism-navigating-new-forms-of-servitude-in-industry-4-0/

Marx, K. (1990). *Capital: A critique of political economy* (Vol. 1, B. Fowkes, Trans.). Penguin Classics. (Original work published 1867)

Modern Diplomacy. (2025, March 22). *Pakistan leaps into the digital age.* Modern Diplomacy. https://moderndiplomacy.eu/2025/03/22/pakistan-leaps-into-the-digital-age/

Organisation for Economic Co-operation and Development. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.* OECD Publishing. https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Open-Source Initiative. (n.d.). *The open-source definition (annotated).* https://opensource.org/osd

Pinto, R.A. (2018). Digital sovereignty or digital colonialism? *Sur-International Journal on Human Rights.*

Rehman, Z. (2022, June 9). *Platforms of oppression: Conceptualising digital colonialism in the Pakistani context.* Digital Rights Monitor. https://digitalrightsmonitor.pk/platforms-of-oppression-conceptualising-digital-colonialism-in-the-pakistani-context/

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world.* W. W. Norton & Company.

Solon, O. (2017, June 27). It's digital colonialism: How Facebook's free internet service has failed its users. *The Guardian.* *https://www.theguardian.com/technology/2017/jul/27/facebook-free-basics-developing-markets*

The Nation. (2025, July 16). Pakistan's digital future: ADB highlights roadmap for economic growth and inclusive development. https://www.nation.com.pk/16-Jul-2025/pakistan-s-digital-future-adb-highlights-roadmap-for-economic-growth-inclusive-development

Tribune. (2019, February 13). Pakistan ranked among least cyber secure countries. *The Express Tribune.* *https://tribune.com.pk/story/1909680/pakistan-ranked-among-least-cyber-secure-countries*

Wittkower, D.E. (2008). Revolutionary industry and digital colonialism. *Philosophy Faculty Publications,* 6. https://digitalcommons.odu.edu/cgi/viewcontent.cgi?article=1006&context=philosophy_fac_pubs.

World Bank Group. (2022). Individuals Using the Internet (% of Population) - Pakistan. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=PK.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *New York: Public Affairs.*

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology,* 30, 75-89. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754