THE ARCHITECTURE OF DOMINANCE: BIG TECH, DIGITAL COLONIALISM AND THE SEARCH FOR A RIGHTS-BASED REGULATORY ORDER

Rishika Bahri, Amity Law School, Amity University, Noida

ABSTRACT

The twenty-first century has witnessed the emergence of a small number of technology corporations principally Meta, Google (Alphabet), Amazon, Apple and ByteDance as quasi-sovereign actors exercising unprecedented regulatory, economic and epistemic power across national borders. This paper examines the intersection of three critical dimensions of this phenomenon: the theoretical construct of digital colonialism, the human rights consequences of unregulated platform power, and the architecture of international economic law as an enabler of corporate dominance. Drawing upon critical political economy, postcolonial legal theory and doctrinal analysis of Indian and international law, the paper advances three principal arguments.

First, that the contemporary digital economy reproduces and extends colonial structures of extraction and domination, constituting what may be described as digital colonialism; second, that Big Tech corporations function as neo-imperial actors whose operations directly implicate the full spectrum of human rights, including the rights to privacy, freedom of expression, equality and development; and third, that the prevailing framework of international economic law comprising WTO e-commerce disciplines, TRIPS obligations, digital trade agreements and bilateral investment treaties operates as an architecture of digital empire, constraining the regulatory sovereignty of states in the Global South. The paper pays particular attention to the constitutional and regulatory framework of India, examining landmark judicial precedents including Justice K.S. Puttaswamy (Retd.) v Union of India and Shreya Singhal v Union of India, as well as the Digital Personal Data Protection Act 2023 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

In its conclusions, the paper calls for a human rights regulatory approach in both international and national arenas to support binding human rights due diligence requirements for businesses, human rights carve-out provisions in digital trade agreements, and a robust national data protection and competition policy for India.

Keywords: Digital Colonialism; Big Tech Regulation; Human Rights and Technology; Surveillance Capitalism; Platform Governance; International Economic Law; Data Sovereignty; Indian Constitutional Law; Privacy; Freedom of Expression.

I. Introduction

In 2023, Facebook reported over three billion monthly active users a figure exceeding the population of any nation-state. Google processes over 8.5 billion search queries daily[1], functioning as the epistemic gateway through which most of humanity accesses knowledge. Amazon Web Services underpins a significant proportion of the world's digital infrastructure. These figures are not merely statistical curiosities; they are indices of an unprecedented concentration of private power that demands sustained legal and political scrutiny.

The early decades of the twenty-first century have seen the emergence of a class of technology companies known as Big Tech, who have gone beyond their nature as purely business firms to become quasi-sovereign entities on the global stage. They wield regulatory power through content moderation policies, algorithms that rank information, terms of use of online platforms, rules of data management, and access to essential digital infrastructure. In contrast with state regulators, Big Tech firms are not bound by constitutions and the protections they offer, human rights treaties, and democratic oversight processes. This phenomenon has been termed a "governance gap" in scholarship on law.

The regulatory void has far-reaching consequences when it comes to human rights. The communication channels used by billions of people to communicate and engage in political discourse are regulated by corporate policies that are designed to censor speech, facilitate surveillance, reproduce discrimination, and centralize capital. In the Global South, and especially in developing nations such as India, where the technology required to connect online is monopolized by foreign firms, there is an added dimension to the problem. Scholars have coined the term “digital colonialism” to refer to the practice of foreign tech companies harvesting value from developing nations.[2]

The paper argues that to comprehend Big Tech governance, it is necessary to deal with three

[1] Deanna Ballew, “The Importance of Digital Customer Experiences”, A Guide to Digital Customer Experience, Acquia, Feb 26, 2024

[2]Ulises A. Mejias and Nick Couldry, 'Colonialism, Data, and the Digital Turn' (2019) 24(2) Environment and Planning D: Society and Space 336, 338.

separate but connected theoretical discourses at the same time: theories of digital colonialism, doctrines of international human rights laws, and principles of international economic laws. The combination of these discourses uncovers a structure of problematics where the legal system currently in place is not just unable to control Big Tech, but in some ways contributes to its rise and power.

The research approach is primarily doctrinal and interdisciplinary, utilizing sources such as international conventions, national laws, judgments issued by courts in India and abroad, studies from international organizations like UNCTAD, OECD, and the United Nations Human Rights Council, and literature on surveillance capitalism, post-colonialism, and digital governance. Comparative citations from the EU's Digital Services Act (DSA)[3] and Digital Markets Act (DMA)[4] may be used where applicable to demonstrate both the strengths and weaknesses of current regulatory frameworks.

II. Theoretical Foundations: Digital Colonialism, Surveillance Capitalism and Platform Power

A. Digital Colonialism as A Structural Concept

Digital colonialism serves as the overall analytic framework for the paper. This involves the domination and exploitation of digital technology, as well as data processing and knowledge generation, by corporations and governments mainly located in the Global North, to the detriment of the independence, development, and sovereignty of the Global South. Although some consider the notion problematic due to romanticisation of past colonialism and the neglect of the distinct characteristics of the current digital system, it remains useful because it helps understand the power imbalances within today's digital world.

Colonialism relied on natural resource extraction and coerced labour. Digital colonialism uses another strategy – that of behavioural data extraction and digital infrastructure concentration. As UNCTAD points out, the digital economy creates around USD 11.5 trillion worth of revenue each year. However, 90 percent of this revenue ends up in companies based in the United States or China[5]. This comparison with classical extractivism holds analytical weight.

[3] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act)
[4] Digital Market Act, Regulation (EU) 2022/1925
[5] UNCTAD, Digital Economy Report 2021: Cross-Border Data Flows and Development: For Whom the Data

Just as economies of colonialism funnelled resources from the periphery to the centre, economies of the digital age funnel behavioural data from the Global South to the North, creating wealth for companies located in just a few cities.

Key characteristics of digital colonialism include: Asymmetric market power, dependence on infrastructure, epistemic dominance, and asymmetric regulation. In the Global South, which includes India, African countries, and Latin American countries, communication, online payment processing, cloud computing services, educational services, and governance systems are dependent on the platforms owned by other nations. Such dependencies are neither random nor accidental; they have been created due to the network effects that create monopolies within the platform market. Once critical mass has been reached, the cost of switching to another alternative becomes prohibitive for both users and regulators alike.

B. Surveillance Capitalism: Commodification Of Human Experience

The concept of surveillance capitalism, developed by Shoshana Zuboff, provides the most comprehensive theoretical account of how data extraction is operationalised within contemporary capitalism.[6] Surveillance capitalism, according to Zuboff, refers to an economic paradigm characterized by the appropriation of the experience of humans as free raw materials, turning them into behavioural data and generating predictions using the behavioural data in order to sell them to businesses in need of such services – mainly advertisers wishing to manipulate people's behaviours. It is quite a different concept from previous capitalism. In industrial capitalism, the raw material involved was natural resources, whereas in surveillance capitalism, the raw material is human experience in its entirety – emotions, preferences, social interactions, and cognition.

The Facebook whistleblower Frances Haugen, testifying before the United States Senate in October 2021, internal research conducted by Facebook showed that Facebook's algorithms promoted hate speech, misinformation and polarization because these types of posts produced high engagement and, as a consequence, increased the profits from advertising[7]. This example

Flow (United Nations, 2021) p 11; World Bank Group, World Development Report 2021: Data for Better Lives (World Bank, 2021) p 6.

[6]Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (PublicAffairs, 2019) pp 8–9.

[7] Frances Haugen, Testimony before the United States Senate Committee on Commerce, Science and Transportation (6 October 2021).

demonstrates the intrinsic logic of surveillance capitalism, since this business model is incentivized by harm as it produces higher engagement. This has significant consequences not only for democracy but for people's psychological well-being. In the case of India, when social media websites were involved in communal misinformation campaigns during the general elections, the functioning of surveillance capitalism affects the functioning of democracy guaranteed by the Constitution and by Article 25 of the ICCPR[8].

C. Platform Capitalism and Market Concentration

Nick Srnicek's theory of platform capitalism highlights the importance of platforms' structure as the central organisational form of modern capitalism. Platform companies act as intermediaries bringing together different communities of users through control over infrastructure that makes such interactions possible. Their business model relies upon accumulation of data and positive feedback loop when the larger number of users makes the company more valuable and difficult to beat by newcomers. This leads to the so-called "winner-takes-all" or "winner-takes-most" market structures that feature extremely high concentration levels. High concentration levels have many important implications for governance and right protection. First, it allows platforms to impose their own conditions as there are no alternatives for businesses and individuals using platforms' services; second, high concentration creates opportunities for rent generation; third, but most importantly, it generates structural accountability problems.

The European Commission's 2018 investigation into Google's Android operating system found that Google had abused its dominant market position by requiring device manufacturers to pre-install Google Search and Chrome, foreclosing competition.[9] In India, the Competition Commission of India's 2020 Market Study on E-Commerce similarly identified anticompetitive practices by major platforms operating in the Indian market, including self-preferencing, exclusive arrangements and manipulation of search algorithms to favour affiliated products.[10]

[8] International Covenant on Civil and Political Rights, Article 25

[9]European Commission, Antitrust: Commission fines Google EUR 4.34 billion for illegal practices regarding Android mobile devices (Case AT.40099, 18 July 2018).

[10]Competition Commission of India, Market Study on E-Commerce in India: Key Findings and Observations (CCI, 2020).

D. Data Colonialism and the Coloniality of Power

The concept of data colonialism, introduced by Ulises A. Mejias and Nick Couldry, is the most explicit link connecting the history of colonialism to current data practices[11]. According to the authors, data colonialism expands the scope of colonialism, which relies on the principle of extraction, to the sphere of digital, where the object of exploitation is human life via behavioral data collection. This leads to radical changes in the interaction between human beings and economic systems: engagement in digital processes is a necessary requirement for existence in today's world, and this engagement becomes a source of data that is exploited by corporations for profit.

The theory of the coloniality of power by Anibal Quijano adds to our understanding of this issue[12]. According to Quijano, colonialism goes far beyond political independence and includes economics, culture and knowledge systems. In the digital age, the idea of coloniality takes on new dimensions in the form of the predominance of Western technologies and cultural values built into algorithms, the control of technological know-how by developed countries and the marginalisation of knowledge systems of developing nations.

India, which was liberated from the shackles of colonization almost two hundred years after gaining its political independence in 1947, finds itself particularly vulnerable to re-colonization via technologically dependent digital imperialism. Constitutional efforts by the Indian government to establish digital sovereignty via innovations like India Stack, Unified Payments Interface, and Digital Personal Data Protection Act 2023[13] must be seen as an attempt to counter the threat of digital neo-colonization, with the Preamble of its Constitution emphasizing justice, liberty, and equality of citizens in the digital era[14].

III. Big Tech as Neo-Imperial Actors: Power Across Four Domains

A. Communication: Platforms As Gatekeepers of Speech

Control over the means of communication is perhaps the most significant part of big tech power

[11] Mejias and Couldry (n 1) 337–339.
[12] Anibal Quijano, 'Coloniality of Power, Eurocentrism and Latin America' (2000) 1(3) Nepantla: Views from South 533, 540.
[13] The Digital Personal Data Protection Act, 2023, August 11, 2023, Act 22 of 2023.
[14] Constitution of India 1950, Preamble; Nandan Nilekani, 'India Stack and the Digital Public Infrastructure Model' (2022) 15(2) Information Technology for Development 5.

today. In our increasingly digital age, social media has come to dominate people's methods of communication and accessing information and participating in conversations. Facebook (now Meta), WhatsApp, Instagram, Twitter (X), TikTok, and YouTube act as the new gatekeepers of speech, with decisions regarding whether certain communications are seen, heard, or stifled. These decisions are made privately, behind closed doors, by corporations that cannot be democratically held accountable for their actions.

Engagement-maximizing algorithms, which encourage users to share certain kinds of content on social media platforms, tend to promote content that evokes strong emotions, including outrage, fear, and contempt, rather than information that is based on facts. According to a study carried out by researchers at MIT and published in Science in 2018, fake news stories were 70%[15] more likely to be circulated on Twitter compared to real news stories, and fake news stories diffused much faster and reached wider audiences.[16]

The constitutional significance of these dynamics for India is acute. The Supreme Court of India in *Anuradha Bhasin v Union of India* held that the freedom of the press and the freedom to practise any profession through the internet are protected under Articles 19(1)(a) and 19(1)(g) of the Constitution, and that any restriction must satisfy the dual tests of necessity and proportionality.[17] This principle has direct implications for private platforms that unilaterally suppress or amplify speech without procedural safeguards, particularly when Indian state actors are complicit in or direct such actions. The phenomenon of zero-rating whereby telecom operators provide free access only to certain platforms further entrenches the dominance of Big Tech in the Global South, raising fundamental questions about net neutrality and equality of access that implicate Article 14 of the Constitution.

B. Information: Search Engines and the Governance of Knowledge

Big Tech exercises decisive power over the production, organisation and dissemination of knowledge. Google's dominance in the global search engine market stood at approximately 92% as of 2023, making it the sole arbiter of online information visibility for most users.[18] By

[15] Aryan Roy, "DPDP Act 2023 Vs. GDPR: A Structural and Institutional Comparative Analysis For Indian Multinational Compliance", International Journal for Legal Research & Analysis (IJLRA) (ISSN: 2582-6433)
[16] Soroush Vosoughi, Deb Roy and Sinan Aral, 'The Spread of True and False News Online' (2018) 359(6380) Science 1146.
[17] Anuradha Bhasin v Union of India (2020) 3 SCC 637, paras 24–26.
[18] StatCounter, Search Engine Market Share Worldwide (2023), available at gs.statcounter.com (last accessed 1 August 2025).

determining how information is indexed, ranked and displayed, Google shapes what users know, how they understand the world, and which knowledge producers gain audiences. This power is exercised through proprietary algorithms that, while presented as neutral and objective, are influenced by commercial incentives, technical design choices and embedded cultural biases.In the context of digital colonialism, control over information flows reflects broader patterns of epistemic dominance, where knowledge production and dissemination are centralised in the Global North. Languages other than English receive disproportionately poor algorithmic treatment, marginalising the knowledge systems, cultural expressions and news ecosystems of the Global South. For India a linguistically diverse nation with 22 scheduled languages under the Eighth Schedule of the Constitution this algorithmic bias represents a structural form of cultural discrimination that impairs rights protected under international human rights instruments.

C. Identity: Algorithmic Profiling and the Governance of Individuals

A defining feature of Big Tech power is its ability to construct and govern digital identities through algorithmic profiling. Platforms collect vast quantities of behavioural data search histories, purchasing patterns, geolocation data, social connections and communication content to generate detailed profiles of individuals that are both predictive and prescriptive. These profiles determine what content users see, what advertisements they receive, what economic opportunities are available to them and how they are categorised within digital systems. The individual becomes, as Zuboff observes, not merely a user of a platform but a data-mining site from which value is continuously extracted.[19]

This case judgment by the Supreme Court of India is one of the most significant cases dealing with data protection and serves as the basis of the constitutionality challenge to such practices[20]. In this case, the nine-judge bench unanimously held that the right to privacy is a fundamental right within the meaning of Article 21, where they also defined informational privacy to include the right of an individual's control over his/her information, as stated by Judge D.Y. Chandrachud: "Informational Self-Determination".

The problem is aggravated by the discriminatory nature of algorithmic profiling. Studies have found that prediction algorithms deployed in areas such as hiring, loans, insurance, and policing

[19]Zuboff (n 3) p 100.
[20] AIR 2017 SUPREME COURT 4161, (2017) 6 BOM CR 78, AIR 2017 SC (CIV) 2714

not only sustain but exacerbate discrimination against disadvantaged groups. In India, this discrimination will cover discrimination on the basis of caste, religion, gender, and disability, all of which fall within the ambit of Articles 14 and 15 of the Constitution[21]. The case of Farmer v Facebook Inc, heard in the United States District Court, highlights the impact of algorithmic bias through legal injury[22].

D. Infrastructure: Cloud Computing and Digital Sovereignty

Big Tech's dominance is rooted in its control over the infrastructural backbone of the digital economy, beyond communication and information, . Cloud computing services provided by Amazon Web Services, Microsoft Azure and Google Cloud form the foundation upon which digital applications, businesses and public services operate. This concentration creates deep structural dependencies that have significant implications for the sovereignty, security and economic development of dependent states. Critical questions arise as to which legal regime governs data stored on servers in foreign jurisdictions, whether states can access such data for regulatory or law enforcement purposes without violating territorial sovereignty or individual privacy rights, and whether the terms on which cloud services are provided reflect the bargaining power of corporate providers rather than the regulatory interests of host states.

E. Case Studies: Manifestations of Platform Power

There are many case studies that illustrate the concrete human rights consequences of unregulated platform power. The integration of data between WhatsApp and Facebook in 2021 affecting over 400 million Indian users without their meaningful consent demonstrated how platform consolidation enables the unilateral rewriting of the privacy bargain between corporations and users. The Cambridge Analytica scandal revealed a more alarming dimension: the systematic harvesting of personal data from approximately 87 million Facebook users to construct psychographic profiles used to target voters with tailored political messaging in the United States, United Kingdom, Kenya and India.[23] For India where elections involve approximately 900 million eligible voters the implications of unregulated political micro-

[21] The Constitution of India, Article 15 and 16
[22] [22]Farmer v Facebook Inc 592 F Supp 3d 948 (ND Cal 2022).
[23]Cambridge Analytica LLC, In the Matter of (Federal Trade Commission, File No. 1823107, 2019); UK Information Commissioner's Office, Investigation into the Use of Data Analytics in Political Campaigns (ICO Report, 2018).

targeting for democratic integrity are profound.

The role of Facebook in the Rohingya crisis represents the most devastating manifestation of unregulated platform power documented to date. The 2018 UN Fact-Finding Mission on Myanmar concluded that Facebook had been used to incite violence and hatred targeting the Rohingya minority, and that the platform had substantively contributed to the atrocity crimes committed against that community.[24] Despite warnings from civil society, Facebook had failed to invest adequately in Burmese language moderation resources a direct consequence of the cost-minimisation logic of surveillance capitalism that illustrates how the digital colonial relationship translates into catastrophic human rights violations.

The deployment of NSO Group's Pegasus spyware through vulnerabilities in WhatsApp to surveil journalists, activists, lawyers and politicians in multiple countries including India illustrates the intersection of platform power and state surveillance.[25] The Supreme Court of India constituted a technical expert committee in 2021 to investigate allegations that Indian citizens' devices had been compromised, raising fundamental questions about the accountability of private technology intermediaries that facilitate state surveillance and the adequacy of constitutional protections for digital privacy under Article 21.

IV. International Economic Law and the Architecture of The Digital Empire

A. The WTO E-Commerce Moratorium and Fiscal Asymmetry

The rapid expansion of the digital economy has not occurred in a legal vacuum. It has been facilitated and structured by the rules and institutions of international economic law trade law, investment law and emerging digital trade frameworks. This paper argues that the prevailing international economic law framework, though formally neutral in its terms, has in practice enabled and entrenched the dominance of Big Tech corporations, functioning as what may aptly be described as the architecture of the digital empire.

One of the most significant and contested features of this architecture is the WTO e-commerce moratorium, which prohibits member states from imposing customs duties on electronic

[24]United Nations Human Rights Council, Report of the Independent International Fact-Finding Mission on Myanmar (A/HRC/39/64, 2018) para 74.
[25]WhatsApp LLC v NSO Group Technologies Ltd (ND Cal 2019) Case No 4:19-cv-07123; Writ Petition (Civil) No 1126 of 2022, Foundation for Media Professionals v Union Territory of Jammu and Kashmir (Supreme Court of India, pending).

transmissions. Originally introduced as a temporary measure in 1998, the moratorium has been repeatedly extended over more than two decades, effectively acquiring the character of a permanent rule despite persistent and principled objections from developing countries. A 2019 UNCTAD study estimated that the moratorium costs developing countries approximately USD 10 billion annually in foregone tariff revenues that would otherwise be available to fund public services and development programmes.[26] This loss disproportionately affects countries in the Global South, which rely more heavily on tariff revenues, while primarily benefiting the home economies of dominant digital corporations principally the United States and China. India and South Africa have been the most vocal critics of the moratorium within WTO forums, arguing that its continuation entrenches structural inequalities by locking in asymmetrical benefits.

B. TRIPS And the Consolidation of Technological Monopoly

The Agreement on Trade-Related Aspects of Intellectual Property Rights plays an equally significant role in shaping the legal infrastructure of digital empire. By establishing global minimum standards for the protection of intellectual property, TRIPS has enabled Big Tech corporations to secure global recognition and enforcement of their most valuable assets proprietary algorithms, software systems, data processing techniques and platform architectures.[27] These protections create and maintain the technological monopolies upon which Big Tech dominance rests, effectively constituting a legal pillar of the digital empire.

The US Supreme Court's decision in *Google LLC v Oracle America Inc*[28], which addressed the boundaries of copyright protection for software interfaces, indirectly illustrates the extent to which intellectual property regimes protect the algorithmic systems through which Big Tech maintains control over the digital economy.[29] For developing countries, TRIPS obligations create significant constraints on domestic policy space. The Indian Patents Act 1970, as amended in 2005 to comply with TRIPS, illustrates the tensions that arise when developing countries must align domestic intellectual property policy with international obligations shaped primarily by the interests of technology-exporting nations.

[26]UNCTAD, E-Commerce and Development Report 2019 (United Nations, 2019) p 6.
[27]Agreement on Trade-Related Aspects of Intellectual Property Rights (15 April 1994) 1869 UNTS 299, Articles 1–3.
[28] 593 U.S. (2021), 141 S. Ct. 1183, Google LLC v. Oracle America, Inc.
[29]Google LLC v Oracle America Inc 593 US (2021) 141 S Ct 1183.

C. Cross-Border Data Flows and the Erosion of Digital Sovereignty

One important characteristic of modern digital trade law is that of the focus placed on international data transfers. Although international data transfers are key to the operation of the global digital economy, they pose challenges relating to sovereignty, security and the capabilities of states in protecting the rights of their people. Where information collected by states is kept and analysed abroad, it is then regulated by foreign law and terms of service agreements and becomes less susceptible to state regulation and security controls.

The UN Human Rights Council's 2014 Resolution on the Right to Privacy in the Digital Age recognised that unlawful surveillance and interception of digital communications, facilitated by cross-border data flows, violate international human rights law.[30] The tension between free data flows mandated by trade agreements and data sovereignty required by human rights obligations represents one of the most acute structural conflicts within contemporary international law a conflict that existing adjudicatory forums are ill-equipped to resolve because they lack the jurisdiction, expertise or mandate to weigh commercial interests against human rights considerations.

D. Bilateral Investment Treaties and Regulatory Chill

In addition, Bilateral Investment Treaties and the investment provisions of trade treaties offer yet another level of protection for Big Tech companies. In these treaties, foreign investors are given significant rights, including guarantees against expropriation, fair and equitable treatment, and non-discrimination, with these rights being enforced by Investor-State Dispute Settlement procedures that enable corporations to bring cases against state actions in international arbitration tribunals independent of domestic law[31]. It is common knowledge that Investor-State Dispute Settlement procedures create a regulatory chill. The mere possibility of international arbitration discourages states from taking regulatory actions that may negatively impact the interests of the investors. Any measures such as data localization, digital taxes, and algorithmic disclosure would likely face challenges under investment protection provisions.

India's adoption of a revised Model BIT in 2016, which significantly curtails the scope of ISDS and requires exhaustion of domestic remedies before investors may resort to international

[30]United Nations General Assembly, The Right to Privacy in the Digital Age (A/HRC/27/37, 2014) paras 19–22.
[31] India Model Bilateral Investment Treaty 2016, Articles 13–16.

arbitration, represents a deliberate and constitutionally grounded policy response to this risk.[32] This revision reflects the constitutional imperative under Articles 38 and 39 to prioritise the public interest over investor convenience.

V. Human Rights in the Digital Age: Constitutional and International Dimensions

A. Privacy and Informational Self-Determination

“Right to privacy is the most critically impacted human right in the era of big tech governance." The protection of privacy at the international level is provided in Article 17 of the ICCPR[33], which states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence," and this provision has been held by the United Nations Human Rights Council that this principle has full applicability in the cyberspace. At the domestic level, the Indian Constitution, in its nine-judge bench judgement, has made the right to privacy a part of the fundamental rights under Article 21 of the Constitution.[34]

The significance of *Puttaswamy* for Big Tech regulation extends beyond the formal resolution of a constitutional question. The judgment articulated a rich and multidimensional understanding of privacy that encompasses bodily integrity, informational self-determination and the autonomy of personal development. Justice Chandrachud's concurring opinion specifically addressed the threat of surveillance technologies and data profiling, observing that personal data shared in one context may be deployed in an entirely different context in ways that violate reasonable expectations of privacy. This contextual understanding of informational privacy provides the constitutional foundation for demanding that Big Tech companies comply with privacy norms regardless of the formally private character of their activities.

B. Freedom of Expression and The Private Censor

The constitutional guarantee of freedom of speech and expression under Article 19(1)(a) of the Constitution is subject to the reasonable restrictions enumerated in Article 19(2). The architecture of Big Tech content moderation, however, operates outside this constitutional framework: platforms make decisions about what speech is amplified, restricted or removed pursuant to their own private community standards, without legal authorisation, procedural

[32]ibid, Article 15 (exhaustion of local remedies requirement).
[33] International Covenant on Civil and Political Rights, Article 17
[34] Justice K.S. Puttaswamy (Retd.) v Union of India

safeguards or judicial oversight. The Supreme Court's reasoning in *Anuradha Bhasin* that restrictions on the exercise of constitutional rights through digital infrastructure require justification and procedural accountability implies a broader constitutional principle that supports mandatory transparency, procedural safeguards and mechanisms for independent review of content moderation decisions.

The European Court of Human Rights' decision in *Delfi AS v Estonia* established that states have positive obligations under the European Convention on Human Rights to regulate online platforms to prevent violations of fundamental rights.[35] An analogous framework in India, grounded in the Supreme Court's evolving positive rights jurisprudence and the state's obligations under the ICCPR, could provide the doctrinal foundation for imposing content moderation accountability obligations on Big Tech platforms operating in India.

In the Supreme Court's landmark judgment in *Shreya Singhal v Union of India*[36] Section 66A[37] of the Information Technology Act 2000 as unconstitutional was struck down it established that restrictions on online speech must satisfy the standards of legality, necessity and proportionality derived from Article 19(2).[38] Applied to private platform governance, this principle supports the argument that content moderation systems should be subject to equivalent legal constraints, including transparency requirements and procedural safeguards for affected speakers.

C. Equality, Non-Discrimination and Algorithmic Bias

Article 14 of the Constitution of India guarantees equality before the law and equal protection of the laws, while Article 15 prohibits discrimination on specified grounds. These provisions, read alongside Articles 17 and 26 of the ICCPR, create obligations of non-discrimination that are directly engaged by the discriminatory dimensions of algorithmic systems. Empirical research has established that predictive systems used in employment, credit, housing and other high-stakes domains systematically disadvantage marginalised communities. In the Indian context, this encompasses discrimination on grounds of caste, religion, gender and disability.

[35]Delfi AS v Estonia App No 64569/09 (Grand Chamber, European Court of Human Rights, 16 June 2015) paras 110–117.
[36] Shreya Singhal v. Union of India, (2015) 5 SCC 1, Alternative Citation: AIR 2015 SC 1523; MANU/SC/0329/2015
[37] Information Technology Act 2000, Section 66A
[38]Shreya Singhal v Union of India AIR 2015 SC 1523, paras 19–23.

The EU's General Data Protection Regulation has made significant progress in this area, establishing a right not to be subject to solely automated decision-making with significant effects, together with obligations of transparency and human review.[39] India's Digital Personal Data Protection Act 2023 addresses this dimension less comprehensively, focusing primarily on the rights to correction and erasure rather than on obligations of algorithmic non-discrimination and explainability. Closing this legislative gap is a matter of constitutional necessity.

D. The Right to Development and Digital Economic Equality

Beyond the civil and political rights most directly implicated by Big Tech's content moderation and data practices, the right to development articulated in the UN Declaration on the Right to Development 1986 and reflected in the ICESCR is engaged by the structural dimensions of digital colonialism. The concentration of value in a small number of corporations domiciled in the Global North, at the expense of developing countries from which that value is extracted, constitutes a structural impediment to the realisation of the right to development.

India's constitutional framework, with its Directive Principles of State Policy under Articles 38 and 39 directing the state to promote distributive justice and ensure that the material resources of the community are distributed to subserve the common good, provides a domestic constitutional anchor for demanding that digital economic regulation be oriented towards development and social justice rather than corporate interest.[40]

VI. India's Regulatory Response: Law, Policy and Constitutional Imperative

A. The Digital Personal Data Protection Act 2023

India's regulatory response to Big Tech has evolved substantially over the past decade, culminating in the enactment of the Digital Personal Data Protection Act 2023 (DPDPA). The DPDPA establishes a comprehensive framework for the collection, processing and protection of personal data, conferring on data principals a suite of enforceable rights including the right to information, the right to correction, the right to erasure and the right to grievance redress.[41]

[39]European Parliament and Council, Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data (General Data Protection Regulation) [2016] OJ L119/1, Articles 13, 22.
[40]Constitution of India 1950, Articles 38 and 39 (Directive Principles of State Policy).
[41]Digital Personal Data Protection Act 2023 (India), Sections 4–8 and Section 13.

The Act imposes significant obligations on data fiduciaries, including requirements of consent, purpose limitation and data minimisation, providing for the first time a statutory data protection framework grounded in the constitutional principles articulated in *Puttaswamy.*

Several features of the DPDPA warrant critical scrutiny. The Act's approach to cross-border data transfers establishing a whitelist of countries to which personal data may be transferred reflects an attempt to balance the economic benefits of data flows with the imperative of protecting informational self-determination. However, the breadth of governmental exemptions from the Act's requirements may undermine its effectiveness as a protection against state-sponsored surveillance a concern underscored by the Pegasus allegations. The independence of the Data Protection Board from executive influence, critical to its credibility, has also been questioned on grounds of appointments process and accountability structure.

B. The IT (Intermediary Guidelines) Rules 2021 And Platform Accountability

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 represent India's most significant effort to impose direct regulatory obligations on social media intermediaries. The IT Rules require significant social media intermediaries defined as those with over 5 million users to appoint a Grievance Officer, a Chief Compliance Officer and a Nodal Contact Person resident in India; to process user complaints within specified time periods; to publish transparency reports on content moderation; and, in the case of messaging platforms, to identify the first originator of specified categories of unlawful messages upon government or judicial order.[42]

The traceability requirement the obligation to identify the first originator of messages has generated significant controversy from freedom of expression and privacy perspectives. Technically, this requirement may be impossible to implement on end-to-end encrypted messaging platforms without creating backdoors that fundamentally compromise the security of communications for all users. Constitutional challenges to the IT Rules, including challenges to the traceability requirement and to provisions relating to digital news publishers, are pending before the Supreme Court, raising questions about the compatibility of these provisions with

[42] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (India), Rules 3 and 4.

Articles 14, 19 and 21 of the Constitution[43].

Evaluated against international standards, the IT Rules represent an ambivalent regulatory development. On the one hand, the transparency and grievance redress obligations they impose are consistent with the human rights-based accountability framework proposed by the UN Special Rapporteur on Freedom of Expression. On the other hand, provisions that create governmental powers to direct content removal without judicial oversight and mechanisms that could enable the identification of anonymous speakers may inadequately protect freedom of expression and be susceptible to abuse by state actors with interests in silencing dissent.

C. Competition Regulation and Market Power

The Competition Commission of India has emerged as an increasingly assertive regulator of Big Tech market power. The CCI's 2020 Market Study on E-Commerce identified significant anticompetitive practices by dominant platforms, including self-preferencing (favouring affiliated products in search rankings), exclusive arrangements with sellers and manipulative display practices. The CCI subsequently initiated enforcement proceedings against Google in the smart television and Play Store markets, resulting in orders against anticompetitive conduct in 2022 reflecting a growing domestic regulatory assertiveness[44].

The intersection of competition law and privacy regulation with the CCI treating WhatsApp's 2021 privacy policy change as both a potential abuse of dominant position and a privacy violation reflects the recognition that in platform markets, the exploitation of personal data and the exclusion of competition are structurally linked practices.

D. Digital Public Infrastructure and Technological Sovereignty

One of the most unique contributions made by India to the discussion around Big Tech is the development of Digital Public Infrastructure in opposition to platform dependency. The India Stack – which consists of such public goods as Aadhaar, UPI, DigiLocker, among others – offers the ability to deliver digital services via interoperable, publicly-owned systems. In particular, the Unified Payments Interface, which processes more than 10 billion transactions monthly by 2023, proves that digital public goods can easily compete with commercially driven

[43] Constitution of India, Article 14, 19 and 21.
[44] Competition Commission of India v Google LLC (Case No 39 of 2018); Competition Commission of India v Google LLC (Case No 14 of 2021).

platforms[45]. Thus, digital sovereignty, which means that digital public infrastructure is developed instead of regulating foreign entities, has received a lot of attention internationally and might serve as an example for other developing countries.

VII. Towards A Rights-Based Regulatory Framework

A. At the International Level

The foregoing analysis demonstrates that the current architecture of international economic law insufficiently accounts for human rights and that existing soft law frameworks principally the UN Guiding Principles on Business and Human Rights are inadequate to address the scale and nature of Big Tech's impact on fundamental rights. Reforming this architecture requires a multi-level strategy that reorients both binding treaty obligations and soft law governance towards a human rights baseline.

First, binding human rights due diligence obligations should be imposed on Big Tech corporations through a UN treaty on business and human rights. A treaty that imposes mandatory human rights impact assessment, transparency and remediation obligations on digital corporations enforceable through a combination of domestic courts, international supervisory mechanisms and trade conditionality would represent a qualitative advance on the UNGPs' "protect, respect and remedy" framework.

Second, digital trade agreements should be reformed to incorporate enforceable human rights carve-outs that permit states to adopt data localisation, platform regulation and algorithmic transparency measures necessary to protect privacy, cultural diversity and democratic participation. The model of the GATT's general exceptions provisions should be adapted for the digital context, with explicit recognition of privacy and freedom of expression as legitimate grounds for regulatory measures. Critically, the burden of proof should rest on the party challenging such measures to demonstrate that they are disproportionate or disguised trade restrictions.

Third, the WTO e-commerce moratorium should either be terminated or replaced by a more equitable framework that includes adequate compensation mechanisms for the revenue

[45] Confederation of Indian Industry and Boston Consulting Group, India's Digital Future: Realising the USD 1 Trillion Opportunity (CII-BCG Report, 2022) p 17.

foregone by developing countries. Fourth, ISDS mechanisms in digital trade-relevant investment agreements should be reformed to exclude regulatory measures in human rights-sensitive domains including data protection, content regulation and digital competition policy from their scope. India's revised Model BIT of 2016 provides a template that other developing countries could usefully adopt.

B. At the Domestic Level in India

At the domestic level in India, several specific reforms are necessary to realise the rights-based regulatory vision advanced in this paper. With respect to the DPDPA, three priorities are paramount. First, the Act's broad governmental exemptions should be significantly narrowed to ensure that state actors are subject to equivalent data protection obligations as private entities. Second, the Data Protection Board should be reconstituted with stronger institutional independence, including security of tenure for members, transparent appointments processes and financial autonomy from the executive. Third, the Act should be amended to incorporate algorithmic transparency and non-discrimination obligations on significant data fiduciaries, enabling regulators and affected individuals to identify and challenge discriminatory automated decision-making.

With respect to the IT Rules 2021, the traceability requirement should be suspended pending a full constitutional review by the Supreme Court. The Competition Commission of India should be equipped with enhanced resources, technical expertise and expanded powers to address the structural market dominance of digital platforms. Specific reforms should include the introduction of ex ante structural remedies such as interoperability obligations and data portability requirements that address the source of market power rather than merely penalising its exercise. Finally, India should continue and deepen its investment in digital public infrastructure as a structural alternative to corporate platform dependence, with governance frameworks that ensure accountability, transparency and protection of individual rights.

VIII. Conclusion

The problem of Big Tech regulation in the era of digital colonialism constitutes one of the most important legal and political questions of the twenty-first century. In this regard, this essay has made the case for the importance of approaching this issue from a perspective that incorporates the theoretical framework of digital colonialism, the principles of international human rights

law, and international economic law into an interdependent structure.

Four key findings emerge from the discussion above. Firstly, the role played by Big Tech corporations has evolved beyond their function as market players to become neo-imperial entities wielding quasi-sovereign powers related to communication, information, identity and infrastructure on a global scale, free from any mechanism of accountability imposed on sovereign states. Secondly, while the concept of digital colonialism has been used more as a rhetoric than reality, it should be understood as an actual situation arising from data expropriation, infrastructural dependency, and epistemological domination. Thirdly, in relation to the unique Indian context, characterized by a legacy of colonialism and commitment to sovereignty and self-determination, the possibility of digital re-colonization constitutes a formidable challenge.

Finally, the current legal framework governing international economics, that is, the WTO moratorium on e-commerce, TRIPS compliance, digital trade pacts and BITs, is the very architecture of digital empire. Reforming such architecture requires more than tweaks in existing laws; it calls for a complete realignment of international economic law around the principles of human rights.

Fourth, the human rights implications of Big Tech are manifold, complex and squarely addressed in India's constitutional framework. The right to privacy, freedom of speech, equality and development, as enshrined in Articles 19, 21 and 14 respectively, are directly affected by uncontrolled platform dominance. In addition, such rights are also guaranteed under the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). Puttaswamy, Shreya Singhal and Anuradha Bhasin are landmark decisions of the Supreme Court which provide a firm basis for evolving a rights-oriented regulatory regime although certain issues related to horizontal effect of rights as well as limits of platform censorship may have to be explored further.

Big Tech regulation needs to be considered in the broader context of being a constitutional mandate and not a mere question of policy. According to Justice Chandrachud, as mentioned in Puttaswamy, "the right to privacy does not lie in abeyance at the altar of technology." This is essential because it is the dignity, equality, and liberty of over a billion Indians and billions elsewhere around the Global South that will need to be safeguarded through regulations that keep up with the enormous power of these digital platforms.