AI & SOCIETY
https://doi.org/10.1007/s00146-025-02641-y

RESEARCH

Who owns the future? AI, digital sovereignty, and the politics of knowledge

Keerthiraj[1] **· Apoorva Misra**[2]

Received: 7 June 2025 / Accepted: 16 September 2025

Abstract
What we today call "digital sovereignty" is neither a universal concept nor a neutral one. It is a product of specific cultural histories—American liberalism, Chinese statism, and European legalism—each grounded in theological and political trajectories unique to the West. This paper examines how these models—when exported globally—produce epistemic tensions in societies shaped by different traditions of thought. Through four case studies—Aadhaar, GDPR, China's Social Credit System, and ChatGPT—it shows how digital infrastructures are not merely tools of governance, but enactments of particular moral orders. Aadhaar performs modernity through a postcolonial state's imitation; GDPR legislates morality through Europe's juridical universalism; China encodes Confucian ethics via algorithm; and ChatGPT extends Western epistemology under the guise of intelligence. These are not exceptions that require explanation—they are symptoms of a deeper malady: the global circulation of categories that were never born global. What masquerades as universal is, in fact, provincial knowledge on a global tour. This paper, then, is not a call for better models, but for a different conversation—one that begins with civilizational difference, not ends with it. Sovereignty, here, becomes the right to think otherwise—and to build from that thinking.

Keywords Digital sovereignty · Artificial intelligence (AI) · Action–knowledge · Epistemic injustice · Experience · Algorithmic power

1 Introduction

In our present time, increasingly defined by the digitization of everyday life, the idea of sovereignty no longer limits itself to borders, governments, or the physical control of territory. Instead, what we are witnessing is a shift—one that moves sovereignty into a new and indeterminate domain: that of cyberspace, algorithms, and data flows. What is today referred to as "digital sovereignty" gestures toward something broader than conventional state control—it implies the ability to determine and regulate one's digital future. This includes authority over data and the rules that govern the digital sphere (Musoni et al. 2023a, b; Larsen 2022). Yet, as artificial intelligence systems increasingly entangle themselves in economic, political, and social processes, they do not merely remain instruments of governance. They themselves become the site upon which sovereignty is negotiated. The questions, then, are no longer simply about what AI can do, but about who decides what it should do. Who defines the protocols by which it collects data, arrives at decisions, and mediates life in society? More importantly, what kinds of assumptions underlie these decisions? Are these technologies truly universal in scope, or do they reflect the values, norms, and ideologies of specific cultures—particularly those of the West?

From Brussels to Beijing, and from Bengaluru to Washington, these are not rhetorical questions. They are matters of contestation. Western liberal democracies, as is well-known, emphasize privacy and openness, placing the individual at the center. Authoritarian regimes prioritize state control and surveillance. Postcolonial societies, on the other hand, find themselves in a peculiar situation.. And yet, they are compelled to choose between these poles. Many scholars have therefore spoken of this predicament as a new phase of digital colonialism (Mejias and Couldry 2024; Birhane

✉ Keerthiraj
krj492@gmail.com

Apoorva Misra
apoorva.misra@alliance.edu.in

[1] Department of Political Science, GFGC Punjalakatte (Affiliated to Mangalore University), Mangaluru, India

[2] School of Law, Alliance University, Bengaluru, India

Published online: 17 October 2025

2019; Couldry and Mejias 2019). The present paper begins from the intuition that behind these different models of digital governance lie deeper, and often unexamined, assumptions—assumptions about what it means to be human, how societies are imagined, and how knowledge itself is constituted. In other words, it is not merely a question of which digital model a country adopts, but of what kind of anthropology and epistemology such a model presupposes. The claim here is simple: contemporary AI systems are not neutral artifacts. They are the products of specific historical trajectories—namely, Western intellectual traditions.

These traditions include Enlightenment-era notions of the human as an autonomous, rational actor and colonial practices that governed populations through their classification. Marshall Sahlins, in this context, said something rather profound: "Western civilization has been constructed on a perverse and mistaken idea of human nature" (Sahlins 2008). When designers of AI systems rely on such an anthropology—often unknowingly—they risk reproducing that mistake at a planetary scale. Algorithms that categorize faces, prioritize news feeds, or produce text do so by drawing on data that reflects Western experiences, not global ones. When such systems travel beyond their context of origin, they do not adapt. They impose. They encode Western ways of seeing as though they were universal truths, pushing aside other ways of knowing (Barassi 2022). This line of reasoning connects to an older critique within the social sciences. For decades now, it has been argued that Western theories misdescribe non-Western societies because they begin from different premises. If this is true, then one must also ask: do the same theoretical assumptions misdescribe the rest of the world when embedded in technology? This paper answers in the affirmative. Further, it examines how differing conceptions of human beings—and of what counts as knowledge—inform not only AI design but also the very notion of sovereignty in a digital context.

To ground these claims, this paper presents four case studies. Each illustrates how different cultural assumptions shape both technology and governance. First, India's Aadhaar system—a massive biometric identity project—raises issues of surveillance, identity, and what it means to be a postcolonial state. Second, the European Union's GDPR reflects a commitment to autonomy, privacy, and rights that are rooted in a liberal moral philosophy. Third, China's Social Credit System, often criticized, is nevertheless built upon a different vision of governance, one that does not separate ethics from state authority. And fourth, generative AI systems such as ChatGPT—developed in the West and exported globally—have become flashpoints for regulatory anxieties, cultural misalignments, and epistemic clashes. In each case, one finds that what appears as a technical issue is always already a philosophical one. Each model assumes a different kind of person—citizen, consumer, or subject—and a different conception of sovereignty: individual freedom, state authority, or collective responsibility.

If so, what are we to make of the dominant discourse on digital sovereignty? Much of it remains confined within Western conceptual boundaries. The very idea of sovereignty that animates international law—the Westphalian model—emerged from a European context, and it continues to shape how states are expected to act. Even in cyberspace, this notion of bounded control persists. But this leaves little room for alternative imaginations. Can sovereignty also mean the freedom to develop digital tools in line with one's cultural traditions? Can it mean the right not just to control digital systems but to create them differently?

This paper proposes a shift—from sovereignty as control to sovereignty as *experiential autonomy*, or what some traditions might call *action–knowledge*. Instead of relying on abstract principles, this alternative would ground digital governance in the lived practices and normative worlds of different communities. It would ask not what is universally valid, but what is locally meaningful. Such a rethinking could, in turn, open up the human sciences themselves to pluralism and mutual learning. The structure of the paper follows this line of reasoning. First, it unpacks the conceptual links between AI, human nature, and knowledge. Then, it analyzes current models of digital sovereignty (U.S., EU, China), their philosophical underpinnings, and the critiques they have attracted—particularly from the Global South, where the idea of *data colonialism* has gained traction. The case studies then bring these ideas to life, showing how AI systems enact different assumptions in practice. Finally, this paper turns to a constructive task: how might we envision a world where digital systems reflect a plurality of epistemologies, rather than reproduce a single, Western one? In this spirit, the conclusion reflects on what such a transformation would mean—not only for AI governance but for global politics itself.

1.1 AI, epistemology, and assumptions about human nature

We are often told that modern AI systems—from machine learning algorithms to interactive robots—are advanced technologies, impressive in their capabilities yet neutral in their conceptual foundations. But is this characterization accurate? Upon closer scrutiny, one notices that these systems are anything but neutral. They are built upon specific assumptions about human beings, society, and knowledge—assumptions that do not emerge out of nowhere, but rather trace a lineage to Western intellectual traditions. Consider, for instance, the foundational architecture of classical AI. It emerged from the Cartesian conception of the mind: a machine that processes information, governed by logic and rationality as if these were faculties universal to all human

beings (Descartes 1641; Dreyfus 1972). Even today's data-driven AI models carry forward a similar presumption—that human behavior, in its full complexity, can be quantified, modeled, and ultimately predicted, provided one has enough data (Battisti 2024; Calzati 2023). This belief, though rarely questioned, is not universal. It is a product of a particular epistemological tradition, one which seeks general laws and abstractions even at the cost of overlooking contextual and local realities.

What, then, do we teach these machines when we train them? Certainly not the world in its entirety. We teach them a version of the world that is already shaped by specific categorizations and norms. As Veronica Barassi reminds us, "the categories that train AI are not only cultural and dominated by Western thought, but they are also political" (Barassi 2022). To train an AI to recognize "the human body," for instance, is not to give it an abstract universal, but to induct it into a binary—male and female—that emerges from Western biology. Such a classification ignores cultures where gender is fluid or constituted differently (Bartl et al. 2024). Kate Crawford's *Atlas of AI* demonstrates how such divisions—whether of race, gender, or behavior—carry the imprint of Western social hierarchies (Crawford 2021). The result? AI systems that not only replicate but magnify existing social divisions. A content moderation tool, for instance, might flag speech as "extremist" based on Euro-American norms, misrecognizing culturally situated expressions of identity or dissent.. The consequences, as Joy Buolamwini and Timnit Gebru show, are stark: higher error rates, algorithmic discrimination, and a systematic reproduction of epistemic neglect (Buolamwini and Gebru 2018).

What conception of the human lies behind these technologies? One begins to see that it is not a neutral or global anthropology but a Western one: the human as a rational calculator, a bundle of behaviors and preferences to be predicted and optimized. This is the same anthropology found in the idea of *homo economicus*, or in psychometric theories that treat personality as quantifiable traits. Marshall Sahlins had already critiqued this vision when he argued that Western civilization was built upon a mistaken and perverse idea of human nature—namely, one that equates human beings with self-interested desire (Sahlins 2008).

AI, under this model, does not see humans as capable of radical change, growth, or transformation. Instead, it treats freedom as statistical noise and believes that trust, intelligence, or even emotion can be inferred from patterns in data. Such a view aligns with the empiricist and positivist orientations of Western science. And when AI becomes the engine of surveillance capitalism, the presumption is clear: to govern society is to collect, analyze, and predict behaviors—repeating the old aspiration of European sociology to discover laws of social motion (Jones 2024; Gao et al. 2024). These are not universal ideas. They emerge from a specific history. Take, for example, the figure of the individual. Western Enlightenment thought places the individual at the center: autonomous, rational, and possessed of rights. AI systems trained in this context produce personalized experiences, and data regimes emphasize individual consent. But is this how all societies imagine the person? Not quite. In many non-Western traditions, the individual is inseparable from the community. Anthropologists like Marilyn Strathern, working in Melanesia, describe the person not as an autonomous unit but as a *dividual*, constituted through relationships (Strathern 1988). The question then arises: do our AI systems account for such ontologies of personhood? The answer, unfortunately, is no. Current systems rarely accommodate worldviews in which personal data is held collectively, by kinship networks or communities, rather than by isolated individuals or corporations (McDonald and Pan 2020; Tisné, 2020). This oversight is not accidental; it is epistemic injustice in operation—where some knowledge systems, typically Western, are treated as default, and others are dismissed or ignored.

What deepens the problem is this: the obsession with classification and categorization in AI echoes a colonial impulse. In colonial India, the British deployed censuses and ethnographic surveys to enumerate and control populations—classifying people by caste, religion, tribe, and race. These classifications were not innocent; they reshaped indigenous social relations to fit imperial understandings. Today's algorithms, too, engage in similar acts of segmentation: profiling individuals by credit score, purchase history, or risk category. This is not a coincidence. It reflects a continuity of thought: the idea that to govern is to classify from above, to make society legible in James C. Scott's sense—a modernist dream, and a profoundly Western one (Ricaurte 2022; Mollema 2024; Lee 2020; Scott 1998). The effects of these assumptions become visible in the very failures of AI: when a chatbot reproduces racism, when an automated hiring system discriminates, or when a predictive policing algorithm targets minorities. These are not merely bugs in the system. They are symptoms of a deeper problem—the presumption that one epistemology, rooted in Western science and historical biases, can explain all of humanity (Barassi 2022). Binary logic may be adequate for machines. But human lives do not unfold in binaries. When one reduces the world to datasets and categories, one reproduces a vision of society as a technical problem to be solved. In truth, society is not an engineering challenge. It is a web of meanings, lived from within.

The kind of AI one builds depends on the kind of human being one assumes. If the human is understood as a desiring, choosing individual—as in much of Western thought—then AI becomes a tool of behavioral nudging and consumption optimization. But if humans are seen as relational beings, embedded in families, communities, and traditions—as

many non-Western traditions insist—they would call forth different architectures altogether. The Western idea of the individual, shaped by Christian theology and secularized in liberal thought, has become the default input for AI. And it brings with it both affordances and consequences: efficiency, personalization, but also alienation, surveillance, and misrecognition. Suppose the goal were not individual optimization, but social harmony. Suppose we designed AI not to predict desire, but to cultivate ethical living. What would such a technology look like? The answer, perhaps, lies not in better data, but in broader epistemologies.

1.2 Western knowledge systems and postcolonial critique

That the modern world understands *sovereignty* in a particular manner is not a coincidence, nor is it an expression of some universal political truth. Rather, what we call "sovereignty" is a historical construct—a conceptual artifact specific to Western political thought. Its articulation does not begin with modernity; it begins with a theological image. The Peace of Westphalia (1648) is often said to have formalized the modern state system. Yet what it gave us was not a new idea, but the secularized form of an old one: the unchallengeable authority of a Christian God transposed into the political domain (Bauder and Mueller 2021; Lee 2021). Sovereignty became the attribute of the state as divine authority had once been the attribute of God (Schmitt 1922; Lorberbaum 2020; Yarkeev 2021; Aroney 2020). It is here that we must locate the origins of the modern conception—not in empirical experience, but in a theological transformation.

And yet, this theological–political conception did not remain local. Like so many other European inventions, it was universalized—not by argument, but by export. Through colonial expansion and the construction of the international system, the Westphalian model traveled far beyond its birthplace. But such exports always bear epistemic costs. In carrying its own assumptions outward, Europe invalidated those of others. What did not resemble the Westphalian template was declared 'non-political', 'pre-modern', or even 'primitive'. Political organization in Asia, Africa, or the Americas was not studied as political; it was studied as deviation. Anthropology, sociology, political science: these disciplines do not describe the world; they describe Europe's experience of the world. Their theories about Africa or Asia became the foundation for universal disciplines. That postcolonial elites internalized these theories—through Western universities, through textbooks, through language—is not a contingent fact. It is a structural feature of how modern knowledge works (Gagliardone 2024). The result is a disjuncture. The lived realities of postcolonial societies do not align with the conceptual categories inherited from European thought (Couture et al. 2025; Keerthiraj, Misra, and Vang-Phu, 2025). And it is this disjuncture that once again confronts us—now in the realm of digital governance.

We speak of "internet freedom," "data privacy," "cybersecurity"—as though these are universal concerns. But are they? These categories, born in Euro-American contexts, may carry little resonance in the lifeworlds of, say, a rural Indian community or a Confucian township. To speak of digital rights in such places is akin to how colonial anthropology once spoke of "caste" or "tribe" in India—categories imposed to describe what they could not comprehend (Simpson 2020; Misra & Keerthiraj, 2025). The issue is not that these concepts are false because they are Western. It is that they are particular, even when they claim universality. The West, then, is not the model for the rest—it is merely one case among many. Let us now apply this frame to the digital present. What do we find? That the dominant concepts—data protection, freedom of speech, individual rights—are products of specific historical experiences: the rise of capitalist markets, fears of state overreach post-World War II, and the secular liberal image of the individual (Schwartz 1999; Daly 2020a, b). These are valid within their tradition. But they are not the only ways to think digital. And perhaps, they are not the best ways either.

Already, new voices are naming what was once invisible. The terms "digital colonialism" and "data colonialism" do not merely suggest parallels; they expose continuities. What was once extracted—land, labor, and gold—is now harvested as data, attention, and behavioral surplus (Couldry & Mejias 2019; Cristaldi 2024). Facebook does not need gunboats. Google does not require flags. The extractive machine is coded into platforms, not into ports. But the asymmetry is familiar: data flows from the South to the North, wealth accumulates in the West, and legitimacy is conferred upon systems that no one locally shaped. Consent becomes ambiguous. Benefit remains unequally distributed (Warganegara 2024; Holden and Harsh 2024). And what is called "ethics" today often functions as a new kind of gatekeeping: Who defines the ethical? And for whom? To treat digital governance as a domain of abstract rights is to miss what it has become: a new terrain in the struggle for justice. But let us go one step further. Is the very obsession with *sovereignty* itself—this fixation on control, exclusivity, and territoriality—not a peculiarly Western anxiety?

In the West, sovereignty emerged within monarchic and monotheistic traditions. The sovereign was not merely powerful; he was absolute. Not because the people granted it, but because the image came from theology. The model was divine monarchy. In other parts of the world, this was not the case. In India, for instance, the king was not sovereign in the modern sense. His power was always already circumscribed—by Raja Dharma, by social obligations, by cosmic order (Black 2022; Simmons 2021; Adhikary 2023). Authority was contingent, negotiated, and embedded. Here,

the question was not who owns power, but how power must act. What if such a conception were applied to the digital realm? Instead of asserting state or corporate sovereignty, we might begin with communal stewardship. Could health data, ancestral knowledge, genetic information be treated not as proprietary assets but as ethical commons? Could the authority to govern them reside not in centralized structures but in local communities?

As Benjamin Bratton argues in The Stack, digital sovereignty is not located in a single entity but distributed across multiple layers—earth, cloud, city, address, interface, and user—each with its own locus of decision-making (Bratton 2016). This complicates the notion of sovereignty in AI, because the agents in our case studies—a democratic state, an alliance of states, a one-party republic, and a private corporation—operate at different layers of the Stack. Carl Schmitt's famous dictum that "sovereign is he who decides on the exception" (Schmitt 1922) is equally relevant here: the struggle for control over AI is a struggle over who can suspend the ordinary rules in moments of crisis, algorithmic failure, or geopolitical tension. Recognizing these dynamics is crucial for understanding why experiential autonomy cannot simply be sovereignty, but must be safeguarded by structures capable of decisive protection. Such questions do not negate the Western model. They relativize it. They do not reject Europe's past; they provincialize it. As Boaventura de Sousa Santos suggests, we may be entering a *pluriverse*—a world where many conceptions of order coexist (Santos, 2014). In such a world, the European notion of sovereignty, grounded in individualism and nation-states, may share space with Māori *kaitiakitanga* (guardianship), or Islamic *amanah* (trusteeship) (McAllister et al. 2023; Mohamed et al. 2020). These are not variants of the same idea. They are different answers to different questions. In such a world, no model need be universal. Each can be local. And perhaps, only then, can we speak of sovereignty—not as domination, but as dignity.

1.3 Digital sovereignty: Western models and their discontents

"Digital sovereignty" has become a catchphrase in contemporary policy debates. What is less clear, however, is what this term means. The frequency of its use is matched by the ambiguity of its definition. At its most general, digital sovereignty refers to the ability to control one's digital destiny—control over infrastructures, such as data centers and cables, over standards, and algorithms, and over data itself: its generation, movement, and ownership (Tan et al. 2022; Paulsson and Fred 2024; Ganz et al. 2024). But this formal definition tells us very little about how this sovereignty is actually conceived, exercised, or justified. The term acquires meaning only within a political culture, and that culture shapes what is considered legitimate control, what is viewed as a threat, and who is seen as a rightful sovereign. It is therefore unsurprising that the concept has acquired different articulations across the major powers. In each case, one finds not a technical strategy, but a political worldview—projected onto the domain of the digital.

Let us begin with the United States. Historically, the U.S. promoted an image of cyberspace as an open, global arena of innovation and free exchange. This was not a neutral vision. It emerged from liberal political thought, where the individual consumer is king, and where minimal state interference is presumed to produce the greatest public good. Cyberspace, under this view, was to remain borderless, decentralized, and largely governed by market forces. But behind this noble rhetoric stood the economic and strategic interests of Silicon Valley. A borderless internet also meant an internet dominated by U.S.-based corporations. This model, once lauded, now appears more problematic. As Shoshana Zuboff shows, it enabled "surveillance capitalism"—a regime in which a handful of firms collect, analyze, and monetize human experience at industrial scale, with minimal accountability (Zuboff 2019).

This liberal framing, which prioritized corporate freedom and consumer choice, underestimated the extent to which such a system could undermine the sovereignty of other states. U.S. companies operate across the world, collecting data that often falls under U.S. jurisdiction via laws like the CLOUD Act. What began as a vision of openness thus became a structure of dependency and exposure, with foreign users' data stored and regulated far from their home countries (Laniuk 2021; Zygmuntowski 2022). Contrast this with the Chinese model. China, unlike the U.S., makes no attempt to deny that cyberspace is a site of national interest. Under the rubric of "wangluo zhuquan" (cyber sovereignty), it asserts state authority over its domestic digital sphere. This is not merely political ideology. It is rooted in a different moral imagination, one that prizes harmony over freedom, stability over spontaneity. In practice, this means surveillance, censorship, and the creation of parallel systems—databases, platforms, and AI models that reduce foreign dependency (Creemers 2020; Wowor et al. 2024). The Social Credit System is perhaps the most visible expression of this vision: a vast, data-driven mechanism for norm enforcement (Kirk et al. 2020).

To Western eyes, this appears dystopian. And indeed, the U.S. and EU have denounced such practices as violations of human rights (Larsen 2022). But for Beijing, digital sovereignty is a defense—against foreign influence, informational chaos, and what it sees as cultural subversion. The policy is often articulated in civilizational terms, invoking Confucian ideals of order. Rather than seeing cyberspace as inherently global, China argues that each country has the right to govern it according to its own laws and moral codes. In this

model, sovereignty is indivisible: if the state is sovereign, then its digital domain must be under its full control. Europe, meanwhile, has attempted to chart a "third way." The European Union's approach might be described as "regulatory sovereignty." Shaped by historical trauma—memories of fascism, Stalinism, and unchecked capitalism—it emphasizes individual rights and legal oversight. The General Data Protection Regulation (GDPR), passed in (Misra, et al., 2018), embodies this outlook. It grants individuals control over their personal data and extends European norms across borders through extraterritorial application—a phenomenon known as the "Brussels Effect" (Christakis 2020; Siegmann and Anderljung 2022).

In addition, the EU has moved toward greater technological independence through investments in AI regulation, chip manufacturing, and European cloud systems. But there is a paradox here. While the EU excels in regulatory power, it lags behind in technological innovation. Its dependence on American cloud providers and absence of leading AI labs raise the question: can one exercise sovereignty over technologies one does not produce? (Nanni et al. 2024). Critics have suggested that Europe has become a referee without players, a governor of a game played by others. Outside these three poles, other states navigate a more complex terrain. India is a case in point. As a democracy with a colonial past, India embraces the digital economy yet voices strong concerns about data sovereignty. It champions data localization, develops indigenous digital infrastructure (such as India Stack), and seeks to reconcile economic liberalization with national security and social inclusion (Seoane 2021; Prasad 2022). But these goals often pull in different directions.

Elsewhere, in Africa and Latin America, digital sovereignty is often framed in terms of resisting a new digital imperialism. The fear is that these regions will become passive consumers in a global system where others set the rules and reap the profits. Calls for "digital non-alignment"—inspired by the Non-Aligned Movement of the Cold War—have emerged as a way of rejecting both the Silicon Valley and Beijing models (Jiang 2024). The African Union's Data Policy Framework is one such initiative aimed at fostering collective self-determination in digital governance. At the heart of all these discussions lies an older philosophical question: Who rules, and in whose interest? Sovereignty, in its Western articulation, has oscillated between two poles: the state and the individual. But what of communities, tribes, or collectives that do not fit neatly into this binary? These are largely absent from mainstream discourse. Indigenous data sovereignty movements challenge this absence. They assert that data about a people belongs to the people—not to the state, nor to abstract individuals—and that it must be governed according to customary law.

Such perspectives do more than complicate existing models. They reveal the narrowness of the assumptions we have inherited. If we take them seriously, then digital sovereignty must include not only the right of states to regulate and of individuals to consent, but also the right of communities to steward, decide, and define what data means and how it is used. This is not a minor amendment; it is a shift in the ontology of sovereignty itself.

What then do we make of the existing paradigms? Each has its strengths, and each its blind spots. The U.S. model, rooted in freedom, failed to see how market liberty could become a new form of domination. The Chinese model, committed to order, disregards individual dignity. The EU model, rich in norms, risks irrelevance without technological muscle. Postcolonial critique does not merely reject these models. It exposes the limits of their imagination. These frameworks, for all their variation, remain within the conceptual boundaries of Western thought—where the sovereign is either the individual or the Leviathan state, and where the Global South enters only as recipient or object.

1.4 Case studies

1.4.1 Aadhaar: a postcolonial performance of modernity

Aadhaar is not simply a tool; it is a statement. Aadhaar announces, with a clarity only mimicry can produce: "We too can be modern." Introduced by the Indian state in 2009, Aadhaar holds out the promise of inclusion, efficiency, and development. These are not cultural aspirations; they are performances of modern governance—presupposing that governance itself is a technical matter. What leaks is not trust but identity; what excludes is not social form but absent data (Bhardwaj and Cyphert 2020; Prasad 2022; Rajendran 2024). Such a presupposition is not Indian. It belongs to a worldview where problems are engineered failures and solutions are technological fixes. The Indian state, in adopting this posture, does not express its culture; it performs a borrowed imagination. It mimics a modernity conceived elsewhere. Yet this is not a novelty. Aadhaar continues a trajectory that began in colonial times. The urge to classify, catalog, and control through data is not postcolonial invention—it is imperial residue. Anthropometry, fingerprinting, surveillance—these are not technologies of empowerment; they are devices of domination (Sahoo 2023). The irony lies in this: the Indian state, today, speaks in the language of neutral technology, while enacting colonial epistemology in bureaucratic disguise (Masiero and Shakthi 2020; Subramanian 2024).

To call Aadhaar mere imitation is to simplify what is, in fact, a negotiation. Through India Stack, the state claims a digital sovereignty—its own platforms, its own protocols. Aadhaar becomes the vehicle of this sovereignty. But the sovereignty it enacts is mediated through foreign legal categories. Consider, for instance, the idea of privacy as a

fundamental right in the Puttaswamy judgment (Supreme Court of India 2017): it emerges not from Indian jurisprudence but from a liberal Western notion of the individual. More than law, it is the knowledge regime that shifts. In the village, it is not biometric data but the word of the elder, the judgment of the panchayat, that identifies the needy. Aadhaar displaces this form of knowing. It enacts a shift—from relational, lived trust to digital, impersonal verification (Addo and Senyo 2020; Krishna 2020; Nagaraj and Prakash 2021). This is not development. It is epistemic violence. So Aadhaar is not a neutral system. It is a site—one where competing knowledge systems collide. Colonial, postcolonial, bureaucratic, legal, technological: they do not cohere; they contend. In that contest, a new form of internal colonization takes shape. Not through Western rule, but through an Indian state governed by Western categories and global corporate imagination (Sahoo 2023). What we call sovereignty here is not a return; it is a re-inscription.

1.4.2 GDPR: the empire writes back, with law

If Aadhaar is a performance of the desire to be modern, then the GDPR is a performance of a different kind—the attempt of an aging empire to moralize the digital world. In this sense, GDPR is not merely about data. It is about reasserting Europe's role—not as innovator or platform-builder—but as the moral compass of cyberspace (Council of the European Union 2018; Daly 2020a, b; Christakis 2020; Obendiek 2021). This role is born of memory. Europe remembers its horrors: Auschwitz, the Stasi, the consequences of surveillance. It fears the shadows it sees in Big Tech. GDPR, then, becomes an apparatus—not to construct, but to constrain; not to produce, but to regulate (Rubinstein and Margulies 2021; Valtysson et al. 2021). This is sovereignty, not as rule over territory, but as normative authority over others' actions.

Yet here, too, an epistemic assumption is at work. GDPR presupposes a particular anthropology—that of the Enlightenment subject: rational, autonomous, and rights-bearing. This subject must be informed, must consent, must have control over data. But such a subject is not universal. In India, for example, state legitimacy may rest not on privacy but on performance: what works, not what is consented to (Frey and Presidente 2024; Gentile and Lynskey 2022). The divergence is not one of values; it is one of cultures. In exporting GDPR, Europe projects its normative framework onto others. This is not global governance; it is normative imperialism. A law framed in one world now regulates the others. And yet, even within Europe, this law falters—fragmented enforcement, structural delays, and disproportionate burdens on smaller firms (Saemann et al. 2022; Hodges 2021; Pollina and Armellini 2024). Where Aadhaar mimics, GDPR mandates. Where the postcolonial internalizes foreign norms, the Western state externalizes its own. Both enact modernity—not as shared experience, but as unequal epistemology.

1.4.3 China's social credit system: harmony as algorithm

To the Western eye, China's Social Credit System is dystopian—scores, surveillance, and social control. But to stop there is to misunderstand the system entirely. What appears as techno-authoritarianism may well be a civilizational expression—one shaped not by liberal suspicion but by Confucian sensibilities. For the Chinese state, Xin Yong—trustworthiness—is not a right; it is a value embedded in relational ethics. The aim of the Social Credit System is not to shield the individual from the state, but to construct a moral community. In such a society, "the trustworthy roam free," while the untrustworthy are restricted (State Council of the PRC, 2014; Engelmann et al. 2021; Loubere and Brehm 2022; Trauth-Goik and Liu 2022).

This is a sovereignty that draws not from consent or individual rights, but from order, hierarchy, and harmony. It does not begin with the private individual but with the public ethos. The state here does not merely protect; it cultivates (Xu et al. 2023). Western observers call this surveillance. But what, then, are credit scores in the West? Uber ratings? Social rankings on platforms? The forms differ; the logic does not. The distinction lies not in the mechanism, but in the moral justification (Chen and Grossklags 2022; Zou 2021; Devereaux & Peng 2020). China's system makes explicit what other societies obscure: that digital governance is not just about data, but about values. What it reveals is not China's deviation, but the moral foundations of every digital architecture. Here, digital sovereignty becomes a matter of ethical ordering through technological means—not in spite of culture, but because of it.

1.4.4 ChatGPT: algorithms as epistemic agents

ChatGPT is not a law, not a policy, not a state institution. And yet, it governs. Not through enforcement, but through knowledge. What is at stake here is not political sovereignty, but epistemic control: who defines what counts as knowledge in the first place? Though trained on global data, ChatGPT speaks with a Western voice. Its categories, examples, and assumptions reflect the priorities of its creators and the biases of the internet it consumes (Rauhala and Xin 2024; Vetter and McDowell 2023). Even its ethical filters are shaped by liberal anxieties: freedom of speech, misinformation, hate speech—all framed in cultural idioms specific to the West.

Still, the model circulates globally. In Nairobi, Jakarta, or Bangalore, it is used in classrooms, in conversations, in queries. But what knowledge does it reproduce? What assumptions does it naturalize? In giving answers, it teaches—yet

we do not know what curriculum it follows. This is not colonialism of space. It is colonialism of the mind. A subtle form, but no less potent. AI becomes a site where values do not travel as arguments, but as defaults. And in this default, epistemic authority is asserted. To ask whether such systems can be regulated is to ask too little. The question is: can they be decolonized? Can we create systems that think with Indian categories, African traditions, Islamic jurisprudence—not as content modules, but as foundational grammars of thought?

The question of sovereignty becomes visible even in mundane platform decisions. For example, ChatGPT's content moderation protocols—designed largely through Western liberal norms—can unintentionally marginalize indigenous knowledge systems or locally acceptable practices. In non-Western contexts, certain queries about cultural traditions are sometimes rejected as "unsafe" or "biased" according to rules that do not originate from, nor are accountable to, the affected communities. Such moderation acts operate as micro-sovereign decisions, echoing Schmitt's state of exception, where the platform decides what can and cannot be said. From Bratton's perspective, these decisions illustrate the platform layer exercising sovereignty over user experience, independent of national jurisdictions. This is not cultural relativism. It is civilizational realism. If digital sovereignty is to have any meaning in this century, it must include the freedom to know differently—and to build systems that allow such knowing to flourish.

1.5 Toward an alternative digital sovereignty: action–knowledge and experiential autonomy

Having surveyed the landscape of AI and digital sovereignty, it is evident that current approaches oscillate between Western liberal and authoritarian paradigms, each with their own internal logics and blind spots. Is there a way to conceptualize digital sovereignty that moves us beyond choosing either Silicon Valley's libertarian-infused globalism or Beijing's data-driven paternalism? This section proposes elements of a theoretical alternative: one grounded in action–knowledge (the inseparability of knowing and doing) and experiential autonomy (validated by lived experience and local needs).

1.5.1 Experiential autonomy: re-centering lived experience

In classical political theory, sovereignty is a top-down concept—an abstract quality of a state or a legal arrangement. Experiential autonomy, by contrast, starts bottom-up: it asks what do people, communities, on the ground experience in their digital lives, and how can that drive the structuring of power? For example, if a rural community in Kenya sets up and controls its own internet mesh network to ensure connectivity and monitors it according to communal norms, that is experiential autonomy in action – regardless of what the national policy might say. We do not suggest that experiential autonomy, as we define it, constitutes sovereignty in the Schmittian sense. Rather, it is a normative goal that requires protection by sovereign-like powers—capable of deciding in moments of exception—to ensure that diverse cultural ways of being can thrive without being subsumed under dominant epistemologies.

Such an approach resonates with a call to describe and theorize our own experiences as a starting point. Instead of shoehorning Indian or African digital issues into Silicon Valley frameworks (like seeing everything as a "privacy" issue or a "free speech" issue in the Western legal sense), experiential autonomy would encourage articulating issues as they manifest locally. Perhaps, for instance, the key concern in some contexts is community integrity—e.g., preventing social media rumors from sparking violence—which might combine elements of Western "speech regulation" and "security" but is its own problem that needs its own solution. The theoretical alternative emerges from practice ("action–knowledge") rather than abstract principles imported from elsewhere.

1.5.2 Action–knowledge: merging theory and praxis

The notion of action–knowledge suggests that knowledge is not something separate from action; rather, it is generated through action and should guide action in an iterative loop. Applying this to digital sovereignty, one could argue that we shouldn't attempt to design perfect policies in the abstract, but allow communities to experiment with governing digital tools and learn from those experiments to inform theory. This is akin to how open-source software communities operate: through practice (coding, testing, using) they evolve norms and principles (like openness, meritocracy) that then shape further action.

In a more academic vein, decolonial AI scholars advocate for what they term "reverse tutelage" and "reciprocal exchange" (Mohamed et al. 2020). This implies that the traditional flow of knowledge from center (West) to periphery (Rest) must be reversed and made bidirectional. AI developers should learn from marginalized communities ("tutelage" from those usually considered pupils) and incorporate their perspectives. One concrete tactic they suggest is building intercultural dialog into tech design—bringing diverse stakeholders to discuss what values an AI system should uphold in a given context. This resonates with experiential autonomy: it's about including the experience of those who will live with the AI in the decision-making about that AI. Imagine implementing such ideas: when deploying a health AI in a country, the designers engage with local patients, shamans or traditional healers, doctors, and ethicists to understand local beliefs about health and data—perhaps the system is

then tweaked to respect certain privacy around spiritual illness concepts, or to communicate in a culturally resonant way. The experience here is shared and enacted; it's not just the state telling an AI company what to do, it's the people influencing how the AI works for them. This could prevent the kind of experiential distress that Dhareshwar noted when external frameworks dominate because the framework is being co-constructed.

1.5.3 Beyond one-size-fits-all: pluralism and context

A theoretical alternative to Western-centric sovereignty likely embraces pluralism. Rather than seeking a single model (the way "liberal democracy" was touted as a single model), it might accept that digital sovereignty will take different shapes in different cultural settings—and crucially, that's okay as long as it emerges through genuine self-determination and not external imposition. Latin American scholars speak of "technological pluralism" or "autonomy" where indigenous groups run their own digital projects according to their values. pluralism does not mean turning a blind eye to oppression under the guise of culture. It means being aware that Western dominance is one form of oppression, but local elites can oppress too, or states can oppress under "sovereignty" claims. So experiential autonomy should also give space for sub-communities, minorities, and dissenting voices within a society to influence the digital order. A practical example is the concept of "Indigenous Data Sovereignty", which asserts that indigenous peoples have the right to govern data about themselves and benefit from it (Diviacchi 2023). New Zealand, for instance, has incorporated Maori perspectives by establishing Maori data governance charters (West et al. 2020). This introduces a multi-layer autonomy – the state acknowledges a sphere where a group has autonomy. Extending such logic, one might imagine an internet governance model in a diverse country where different cultural or local units have a say over how certain content or data is handled in their context. This idea might seem messy, but it could definitely be more just and hopefully won't be as messy as the current understanding and confusions around digital sovereignty.

1.5.4 Reclaiming knowledge production

Part of reclaiming sovereignty is reclaiming the knowledge production. For example, instead of always citing Silicon Valley innovations, highlight cases like how Aadhaar was conceptually influenced by earlier local ID efforts or how Kenya's M-Pesa mobile money succeeded through local trust networks. By constructing a narrative that digital modernity can have multiple originating points (not just "the West leads, others follow"), psychologic sovereignty is enhanced—people feel they can innovate and govern themselves, not just implement what others made. An alternative perspective might highlight alternative geniuses and visions—say, the engineers of Bengaluru or the policy innovators in Estonia (small country but interesting digital sovereignty approach)—to break the monopoly of imagination.

1.5.5 Ethics of AI: beyond universalism to experientialism

The Western approach to AI ethics often seeks universal principles like the famous OECD AI principles adopted by many countries (OECD 2019). An alternative approach would argue for an experiential ethics. Similarly, the value of transparency in AI might be interpreted differently—some communities might focus on collective accountability rather than an individual's right to explanation. The theoretical alternative would not throw out universal ethics, but rather build a broader foundation that can accommodate multiple ethical rationalities. Arturo Escobar, a Colombian anthropologist, speaks of "design for the pluriverse," meaning design that allows multiple worlds to flourish rather than enforcing a single world order (Escobar 2018). In practice, that could mean designing AI systems that are highly customizable by local jurisdictions or even open source, so communities can tweak them.

1.5.6 Checks and balances: global and local

Experiential autonomy does not mean isolation or absolute local control free of any external critique. This paper acknowledges the need to critique power wherever it resides. So just as we critique Western domination, we also critique, say, how a government might abuse "sovereignty" to silence opponents. The vision would be local communities have say over their digital lives, but higher levels (national, international) provide oversight to ensure fundamental human dignity is maintained (to prevent atrocities, for instance). This is akin to how in federations, local governments have autonomy but federal laws protect individual rights.

We therefore argue for a plural, layered model of digital sovereignty. At its core, experiential autonomy must remain rooted in local cultural frameworks, but it should be shielded by institutional arrangements capable of decisive action against coercive or extractive forces. This requires legal guarantees at the national level, cooperative safeguards at the regional level, and intercultural governance norms at the global level. Only such a layered approach can prevent both the homogenizing tendencies of Western platforms and the authoritarian appropriation of "local" sovereignty. Some concrete proposals aligned with this could be: international agreements that protect cultural diversity online (like requiring tech companies to support less-resourced languages), alongside national laws that devolve certain decisions to

communities (like citizen juries for AI oversight at city level). The key is a dynamic interplay, not a static hierarchy.

1.5.7 The role of action: learning by doing

Finally, "action–knowledge" emphasizes that theory will evolve as we try things out. We might not have a fully fleshed new theory of digital sovereignty yet—but by encouraging pilot projects, community-driven tech governance, and cross-cultural collaborations, we can gather insights to build that theory. For instance, if a coalition of indigenous tribes creates a data sharing protocol that is more equitable than mainstream practices, document it, analyze it, theorize it: maybe it offers a principle of "stewardship" that could enrich global data governance frameworks. In that sense, the alternative approach is experimental and iterative, valuing praxis—informed action–as much as doctrine. For example, the fact that African countries are uniting to protest data extractivism (like in that Brazilian "Emergency Program for Digital Sovereignty" letter) can be seen as a seed of a new concept of digital sovereignty – perhaps one that frames data as part of the commons that must not be enclosed by foreign powers echoing colonial land grabs, as Couldry & Mejias note (Mejias and Couldry 2024).

This is both pragmatic and utopian. Pragmatic because it builds on what is already happening (people finding local solutions), and utopian because it imagines a world where no one civilization's ethos dominates the digital sphere—a truly multi-polar, multicultural cyberspace. This paper has focused on four illustrative case studies—Aadhaar, GDPR, China's Social Credit System, and ChatGPT—to highlight the plurality of digital sovereignty models. While these examples reveal important patterns, they cannot capture the full diversity of approaches, particularly from Africa, Latin America, or smaller Asian states. Our concept of experiential autonomy remains theoretical and requires further empirical investigation across contexts. Additionally, although Schmitt and Bratton are Western theorists, we have engaged them deliberately to expose the limitations of Western frameworks from within and to stage a dialog that can enrich postcolonial critiques.

2 Conclusion

To speak of digital sovereignty today is not to speak only of technology, but of the conceptual frameworks that render technology intelligible. Artificial intelligence, far from being a neutral instrument, embodies certain assumptions—about what it means to be human, about how societies are to be ordered, about who should decide. These assumptions are not self-evident truths; they are products of particular historical trajectories: enlightenment rationality, colonial classification systems, and liberal political theory. Likewise, the very idea of digital sovereignty—whether articulated as the right of the individual or the prerogative of the state—emerges not from a universal human experience, but from the contingencies of Western history: the Westphalian settlement, the social contract, and the anxieties of modern liberalism. The difficulty begins when these contingent forms of thought are projected as universally valid frameworks. They do not simply circulate—they displace. It is no longer the anthropologist or the jurist who explains us. It is now the algorithm that knows best. And what it knows often conflicts with what our communities recognize as right, fair, or just.

In each of the case studies—Aadhaar, GDPR, China's Social Credit System, and ChatGPT—we see not merely models of digital governance. We see a deeper rift: not between civilizations, but between lived worlds and conceptual impositions. The question, then, is not how to adjust local practices to global standards. It is whether we can rethink the standards themselves. This paper proposes one such rethinking, through the lens of experiential autonomy and action–knowledge—that is, by recovering the ways in which communities generate meaning through practice. To decolonize AI is not to reject the West; it is to interrupt the epistemic monopoly that claims to speak for all. It is to ask: who sets the goals of technology, and who remains voiceless? Such a move demands humility—a recognition that no single tradition holds a monopoly on insight. And it demands imagination—the courage to think from the margins, to articulate a digital swaraj: a form of self-rule that shapes the digital not in imitation, but in response to lived realities. We are not facing a confrontation between AI and sovereignty. What confronts us is an opportunity: to build a plural, inclusive epistemology that can orient the technologies of tomorrow toward the good life.

3 Conflict of Interest

The authors declare no competing interests.

Author contributions K. (Dr. Keerthiraj) developed the central thesis, conducted the civilizational and epistemological framing, and authored the case studies on Aadhaar, GDPR, and ChatGPT. A.M. (Dr. Apoorva Misra) contributed the legal and policy analysis, co-authored the section on China's Social Credit System, and helped frame the arguments around digital colonialism and normative frameworks. Both authors collaborated on refining the structure, reviewed the manuscript critically for intellectual content, and approved the final version.

Funding This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data availability No datasets were generated or analysed during the current study.

References

Addo A, Senyo PK (2020) Beyond access: Reconceptualizing digital identification and inclusion through the case of Aadhaar. Acad Manag Proc. https://doi.org/10.5465/ambpp.2020.17762abstract

Adhikary NM (2023) Approaching Kautaliya Arthashastra from the communication perspective. Bodhi Interdiscip J. https://doi.org/10.3126/bodhi.v9i1.61858

Aroney N (2020) Christianity, sovereignty and global law. N/a. https://doi.org/10.2139/ssrn.3518886

Barassi, V. (2022, December 13). AI, the Western illusion of human nature and the human error project. Media@LSE. https://blogs.lse.ac.uk/medialse/2022/12/13/ai-the-western-illusion-of-human-nature-and-the-human-error-project/

Bartl M, Mandal A, Leavy S, Little S (2024) Gender bias in natural language processing and computer vision: a comparative survey. ACM Comput Surv. https://doi.org/10.1145/3700438

Battisti CA (2024) The Cartesian method and its logic. Praxis Filosófica. https://doi.org/10.25100/pfilosofica.v0i60.14465

Bauder H, Mueller R (2021) Westphalian vs. Indigenous sovereignty: challenging colonial territorial governance. Geopolitics 28(1):156–173. https://doi.org/10.1080/14650045.2021.1920577

Bhardwaj, A., & Cyphert, D. 2020. Direct Benefit Transfer Using Aadhaar. In: Advancing the Impact of Design Science: Moving from Theory to Practice, IGI Global, Pennsylvania, pp 185–210

Birhane, A. (2019). The algorithmic colonization of Africa. Real Life Magazine.

Black B (2022) Politics without fear: King Janaka and sovereignty in the Mahābhārata. Religions. https://doi.org/10.3390/rel13100898

Bratton BH (2016) The stack: On software and sovereignty. MIT Press. https://doi.org/10.7551/mitpress/9780262029575.001.0001

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of the 1st Conference on Fairness, Accountability and Transparency, 81, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html

Calzati S (2023) From big data epistemology to AI politics: rescuing the public dimension over data-driven technologies. J Inf Commun Ethics Soc 21(3):358–372. https://doi.org/10.1108/jices-12-2022-0108

Chen M, Grossklags J (2022) Social control in the digital transformation of society: a case study of the Chinese Social Credit System. Soc Sci 11(6):229. https://doi.org/10.3390/socsci11060229

Christakis T (2020) 'European Digital Sovereignty': Successfully navigating between the 'Brussels Effect' and Europe's quest for strategic autonomy. SSRN Electron J. https://doi.org/10.2139/ssrn.3748098

Couldry N, Mejias UA (2019) The costs of connection: How data is colonizing human life and appropriating it for capitalism. Stanford University Press, Redwood

Council of the European Union. (2018, May 25). The general data protection regulation. https://www.consilium.europa.eu/en/policies/data-protection-regulation/

Couture S, Toupin S, Mayoral Baños A (2025) Resisting and claiming digital sovereignty: the cases of civil society and Indigenous groups. Policy Internet. https://doi.org/10.1002/poi3.434

Crawford K (2021) Atlas of AI: Power, politics, and the planetary costs of artificial intelligence. Yale University Press

Creemers R (2020) China's conception of cyber sovereignty: rhetoric and realization. SSRN Electron J. https://doi.org/10.2139/ssrn.3532421

Cristaldi M (2024) Decolonising data in the age of data colonialism: an interview with Professor Nick Couldry. Etkileşim. https://doi.org/10.32739/etkilesim.2024.7.14.271

Daly A (2020a) Neo-liberal business-as-usual or post-surveillance capitalism with European characteristics? The EU's General Data Protection Regulation in a Multi-Polar Internet. https://doi.org/10.2139/ssrn.3655773

Daly A (2020b) Neo-liberal business-as-usual or post-surveillance capitalism with European characteristics? The EU's General Data Protection Regulation in a Multi-Polar Internet. SSRN. https://doi.org/10.2139/ssrn.3655773

de Santos B (2014) Epistemologies of the South: Justice against epistemicide. Routledge, Oxford

Descartes R. 1641 Meditations on first philosophy J Cottingham Trans, Cambridge University Press, Cambridge

Devereaux AN, Peng L (2020) Give us a little social credit: To design or to discover personal ratings in the era of Big Data. J Inst Econ 16:369–387. https://doi.org/10.1017/S1744137419000754

Diviacchi, T. (2023, October 10). Indigenous data sovereignty and open data. PLOS EveryONE. https://everyone.plos.org/2023/10/10/indigenous-data-sovereignty-and-open-data/

Dreyfus HL (1972) What computers can't do: A critique of artificial reason. Harper & Row, Newyork

Engelmann S, Chen M, Dang L, Grossklags J (2021) Blacklists and redlists in the Chinese Social Credit System: Diversity, flexibility, and comprehensiveness. Proceedings of the 2021 AAAI/ACM Conference on AI Ethics and Society ACM. New york

Escobar A (2018) Designs for the pluriverse: Radical interdependence autonomy and the making of worlds. Duke University Press, Jericho

Frey C, Presidente G (2024) Privacy regulation and firm performance: estimating the GDPR effect globally. Econ Inq. https://doi.org/10.1111/ecin.13213

Gagliardone I (2024) Lock-out, lock-in, and networked sovereignty: Resistance and experimentation in Africa's trajectory towards AI. Liinc Em Revista. https://doi.org/10.18617/liinc.v20i2.7319

Ganz A, Camellini M, Hine E, Novelli C, Roberts H, Floridi L (2024) Submarine cables and the risks to digital sovereignty. Minds Mach 34:1–23. https://doi.org/10.2139/ssrn.4693206

Gao Z, Zhang Y, Li L, Papatheodorou T, Zeng W (2024) AI-rays: exploring bias in the gaze of AI through a multimodal interactive installation. ACM Conf Human Fact Comput Syst. https://doi.org/10.1145/3680530.3695433

Gentile G, Lynskey O (2022) Deficient by design? The transnational enforcement of the GDPR. Int Comp Law Q 71:799–830. https://doi.org/10.1017/S0020589322000355

Hodges C (2021) Comments on GDPR enforcement edpb decision 01/020. Inform Privacy Law eJ. https://doi.org/10.2139/ssrn.3765602

Holden K, Harsh M (2024) On pipelines, readiness and annotative labour: political geographies of AI and data infrastructures in Africa. Polit Geogr. https://doi.org/10.1016/j.polgeo.2024.103150

Jiang M (2024) Models of state digital sovereignty from the global South: diverging experiences from China India and South Africa. Policy Internet. https://doi.org/10.1002/poi3.427

Jones J (2024) Don't fear artificial intelligence, question the business model: how surveillance capitalists use media to invade privacy, disrupt moral autonomy, and harm democracy. J Commun Inq. https://doi.org/10.1177/01968599241235209

Keerthiraj, Misra, A., & Vang-Phu, T. 2025 Indias BRICS Engagement A Strategic Lever in South Asia and the Indian Ocean. In: A. Gedikli, S. Erdogan, & H. Çalışkan Terzioğlu (Eds.) Changing the Global Political Economy BRICS Countries and Alternative Relations Strategies, IGI Global Scientific Publishing. Newyork, pp 189–214

Kirk HR, Lee K, Micallef C (2020) The nuances of Confucianism in technology policy: an inquiry into the interaction between cultural and political systems in Chinese digital ethics. Int J Polit Cult Soc 35:129–152. https://doi.org/10.1007/s10767-020-09370-8

Krishna S (2020) Digital identity, datafication and social justice: understanding Aadhaar use among informal workers in South India. Inf Technol Dev 27(1):67–90. https://doi.org/10.1080/02681102.2020.1818544

Laniuk Y (2021) Freedom in the age of surveillance capitalism: lessons from Shoshana Zuboff. Ethics & Bioethics 11:67–81. https://doi.org/10.2478/ebce-2021-0004

Larsen, B. C. (2022, December 8). The geopolitics of AI and the rise of digital sovereignty. Brookings Institution. https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/

Lee H-K (2021) State sovereignty, God's sovereignty, and native sovereignty: the political theology of making new borders. Theology and Praxis. https://doi.org/10.14387/jkspth.2021.75.489

Lee A. 2020 Caste in the census of India. In From Hierarchy to Ethnicity. https://doi.org/10.1017/9781108779678.004

Lorberbaum M (2020) "That Mortall God": a theological critique of sovereignty. Polit Theol 21:22–29. https://doi.org/10.1080/1462317X.2020.1727619

Loubere N, Brehm S (2022) The global age of the algorithm: Social credit Xinjiang, and the financialisation of governance in China. Xinjiang Year Zero. https://doi.org/10.22459/xyz.2021.13

Masiero S, Shakthi S (2020) Grappling with Aadhaar: biometrics, social identity and the Indian state. South Asia Multidiscip Acad J. https://doi.org/10.4000/samaj.6279

McAllister T, Hikuroa D, Macinnis-Ng C (2023) Connecting science to Indigenous knowledge: Kaitiakitanga, conservation, and resource management. New Zealand J Ecol. https://doi.org/10.20417/nzjecol.47.3521

McDonald N, Pan S (2020) Intersectional AI. Proceedings of the ACM on Human-Computer Interaction 4(CSCW2):1–19. https://doi.org/10.1145/3415218

Mejias, U. A., & Couldry, N. (2024). Data grab: The new colonialism of big tech and how to fight back. University of Chicago Press.

Misra A, Keerthiraj. (2025) Integrating Sustainability in India's Tourism Sector: An Uphill Battle. In: Poddar S, Paul B, Luperi M (eds) Sustainable Business Ecosystems and Social Perspectives. IGI Global Scientific Publishing, Newjersey, pp 359–386

Mohamed S, Png MT, Isaac W (2020) Decolonial AI: decolonial theory as sociotechnical foresight in artificial intelligence. Philos Technol 33:659–684. https://doi.org/10.1007/s13347-020-00405-8

Mollema WJT (2024) Decolonial AI as disenclosure. ArXiv. https://doi.org/10.4236/jss.2024.122032

Musoni, M., Karkare, P., Teevan, C., & Domingo, E. (2023). Global approaches to digital sovereignty: Competing definitions and contrasting policy (Discussion Paper No. 344). ECDPM. https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf

Musoni, M., Karkare, P., Teevan, C., & Domingo, E. (2023). Global approaches to digital sovereignty: Competing definitions and contrasting policy. ECDPM Discussion Paper No. 344. https://ecdpm.org/application/files/7816/8485/0476/Global-approaches-digital-sovereignty-competing-definitions-contrasting-policy-ECDPM-Discussion-Paper-344-2023.pdf

Nagaraj, N., & Prakash, A. (2021). Digital biometric authentication and citizens' right to food: Neglect of the 'local' in India's Aadhaar-enabled Public Distribution System. Proceedings of the 14th International Conference on Theory and Practice of Electronic Governance. https://doi.org/10.1145/3494193.3494239

Nanni R, Bizzaro PG, Napolitano M (2024) The false promise of individual digital sovereignty in Europe: comparing artificial intelligence and data regulations in China and the European Union. Policy Internet. https://doi.org/10.1002/poi3.424

Obendiek, A. S. (2021). Take back control? Digital sovereignty and a vision for Europe. https://doi.org/10.48462/OPUS4-3934

OECD. (2019). Organisation for Economic Co-operation and Development principles on artificial intelligence https://oecd.ai/en/ai-principles:contentReference[oaicite:1]{index=1}

Paulsson A, Fred M (2024) Making apps, owning data: Digital sovereignty and public authorities' arrangements to "byte" back. Organization. https://doi.org/10.1177/13505084241246073

Pollina, E., & Armellini, A. (2024, December 20). Italy fines OpenAI 15 million euros over privacy rules breach. Reuters. https://www.reuters.com/technology/italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/:contentReference[oaicite:1]{index=1}

Prasad R (2022) People as data, data as oil: the digital sovereignty of the Indian state. Inf Commun Soc 25(6):801–815. https://doi.org/10.1080/1369118X.2022.2056498

Rajendran P (2024) The impact of digital governance reforms on public service delivery in India: a case study of Aadhaar. AKSELERASI: Jurnal Ilmiah Nasional. https://doi.org/10.54783/jin.v6i2.1058

Rauhala J, Xin T (2024) What culture is ChatGPT's AI? Eur Conf Cyber Warfare and Sec. https://doi.org/10.34190/eccws.23.1.2364

Ricaurte P (2022) Ethics for the majority world: AI and the question of violence at scale. Media Cult Soc 44(4):726–745. https://doi.org/10.1177/01634437221099612

Rubinstein I, Margulies PS (2021) Risk and rights in transatlantic data transfers: EU Privacy Law US Surveillance and the Search for Common Ground. SSRN Electr J. https://doi.org/10.2139/SSRN.3786415

Saemann M, Theis D, Urban T, Degeling M (2022) Investigating GDPR fines in the light of data flows. Proceed Privacy Enhancing Technol 2022(4):314–331. https://doi.org/10.56553/popets-2022-0111

Sahlins M (2008) The Western illusion of human nature: With reflections on the long history of hierarchy, equality and the sublimation of anarchy in the West, and comparative notes on other conceptions of the human condition. Prickly Paradigm Press, Chicago

Sahoo S (2023) Biometric data's colonial imaginaries continue in Aadhaar's minimal data. BJHS Themes 8:205–220. https://doi.org/10.1017/bjt.2023.11

Schmitt, C. (1922). Political theology: Four chapters on the concept of sovereignty (G. Schwab, Trans.). MIT Press, Cambridge

Schwartz PM (1999) Beyond lessig's code for internet privacy: cyberspace filters, privacy-control, and fair information practices. Wis Law Rev 1999(4):743–788

Scott JC (1998) Seeing like a state: How certain schemes to improve the human condition have failed. Yale University Press, London

Seoane M (2021) Data securitisation: the challenges of data sovereignty in India. Third World Q 42:1733–1750. https://doi.org/10.1080/01436597.2021.1915122

Siegmann, C., & Anderljung, M. (2022). The Brussels Effect and artificial intelligence: How EU regulation will impact the global AI market. ArXiv. https://doi.org/10.48550/arXiv.2208.12645

Simmons C (2021) Devotional foundations of earthly sovereignty: conceptualizing sovereignty and the role of devotion in narrative political theology in premodern India. Religions. https://doi.org/10.3390/rel12110911

Simpson A (2020) The sovereignty of critique. South Atl Q 119:685–699. https://doi.org/10.1215/00382876-8663591

State Council of the People's Republic of China. (2014). Planning outline for the construction of a social credit system (2014–2020). http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm

Strathern M (1988) The gender of the gift: Problems with women and problems with society in Melanesia. University of California Press, Suite

Subramanian V (2024) Citizenship in India: parsing the complexity of digital identity systems. Sci Technol Soc. https://doi.org/10.1177/09717218241281940

Supreme Court of India. (2017, August 24). Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors. [Writ Petition (Civil) No. 494 of 2012]. Digital Supreme Court Reports. https://digiscr.sci.gov.in/view_judgment?id=NjEwMg==

Tan, K.-L., Chi, C., & Lam, K.-Y. (2022). Analysis of digital sovereignty and identity: From digitization to digitalization. ArXiv. [No listed]

Tisné, M. (2020). The data delusion: Protecting individual data is not enough when the harm is collective. Stanford Cyber Policy Center. https://cyber.fsi.stanford.edu/publication/data-delusion

Trauth-Goik A, Liu C (2022) Black or fifty shades of grey? The power and limits of the social credit blacklist system in China. J Contemp China 32(137):1017–1033. https://doi.org/10.1080/10670564.2022.2128638

Valtysson B, Jørgensen R, Munkholm J (2021) Co-constitutive complexity: unpacking Google's privacy policy and terms of service post-GDPR. Nordicom Rev 42(Special Issue):124–140. https://doi.org/10.2478/nor-2021-0033

Vetter MA, McDowell Z (2023) Wikipedia's Enlightenment problem: decolonizing Western epistemologies through critical open education practices. AoIR Select Pap Internet Res. https://doi.org/10.5210/spir.v2022i0.13101

Warganegara MRR (2024) Shifting from 'AI solutions' to 'AI coloniality': Resignification of artificial intelligence and digital apartheid. Global South Rev. https://doi.org/10.22146/globalsouth.94333

West K, Hudson M, Kukutai T (2020) Data ethics and data governance from a Māori world view. Emerald Studies in Indigenous Peoples and Policy. Routledge, Oxford. https://doi.org/10.1108/s2398-601820200000006005

Wowor HGA, Sudirman A, Hakiki F (2024) China's great firewall: cybersecurity as strategy for building world cyberpower. JISPO Jurnal Ilmu Sos Dan Ilmu Polit. https://doi.org/10.15575/jispo.v13i2.27713

Xu P, Krueger B, Liang F, Zhang M, Hutchison M, Chang M (2023) Media framing and public support for China's social credit system: an experimental study. New Media Soc. https://doi.org/10.1177/14614448231187823

Yarkeev, A. (2021). Miracle as theological paradigm of sovereign power. N/A. https://doi.org/10.30570/2078-5089-2021-100-1-27-43

Zou S (2021) Disenchanting trust: Instrumental reason, algorithmic governance, and China's emerging Social Credit System. Media Commun 9(2):140–149. https://doi.org/10.17645/MAC.V9I2.3806

Zuboff, S. 2019. The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.

Zygmuntowski J (2022) Surveil and control: a critical review of "The Age of Surveillance Capitalism." IJAR – Int J Action Res. https://doi.org/10.3224/ijar.v18i1.07