

Article

Artificial Intelligence and the Reconceptualization of Digital Sovereignty: A Political–Philosophical Analysis

Tran Quoc Hung 

Faculty of Social Sciences, Ho Chi Minh City University of Banking, Ho Chi Minh City 700000, Vietnam; hungtq@hub.edu.vn

Abstract

This article explores the topic of digital sovereignty from the vantage point of the theory of politics, maintaining that AI disrupts the traditional Westphalian principle of state sovereignty. Drawing on the normative frame of Roberts and the comparative analyses of Larsen and Kurbalija, it illustrates the three competing philosophical models of digital self-determination: the liberal market model (United States), the techno-legal rights model (European Union), and the cyber-sovereignty model (China), and evaluates the normative presumption. It furthermore assesses these models in light of emerging legislative patterns in Vietnam, arguing that true digital sovereignty requires more than technical infrastructure but a philosophically cohesive conception of collective self-determination in an increasingly interconnected world. The article concludes with an outline for a relational account of digital sovereignty incorporating autonomy/interdependence.

Keywords: digital sovereignty; artificial intelligence; political philosophy; self-determination; data governance; Vietnam

1. Introduction

The rapid spread of artificial intelligence (AI) infrastructure and applications into the public and private spheres reopens fundamental questions of political philosophy: Who rules the digital realm? On what normative basis can a state claim authority over data flows, algorithmic systems, and digital infrastructure? These issues have been encapsulated under the controversial term “digital sovereignty,” a buzzword among politicians, legal scholars, and technologists, lacking substantial critical conceptual rigor. Classical concepts of sovereignty, ranging from Bodin’s potestas absoluta to the Westphalian principle of non-intervention, assume a stable geometric relationship among political power, territorial space, and legal jurisdiction. AI, on the other hand, transcends borders, is created by private firms unaccountable to any one state, and encodes value systems potentially inimical to the people upon whom it governs [1]. With respect to this, AI is more than a policy concern; it is a philosophical concern: it compels us to rethink the ontological and normative bases of state sovereignty in the digital era.

2. The Philosophy of Sovereignty in the Digital Age

Sovereignty has been among the principal tenets of organization in modern political philosophy. In the classical sense, sovereignty refers to the supremacy, absoluteness, and indivisibility of a political authority over a specific geographical area and its people [2]. Hobbes [3] justified this power in social contract theory: sovereignty is the by-product of a pact between people, forging a collective body to get out of the state of nature. The



Academic Editor: Fabien Paillusson

Received: 26 May 2026

Revised: 9 July 2026

Accepted: 7 August 2026

Published: 12 August 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1648 Westphalian settlement entrenched this notion in international law, promoting non-intervention in the affairs of sovereign states.

Roberts [4] notes that identifying digital sovereignty as a concept expands its subjects beyond the state to include individuals and corporations, not just the state as an object of sovereignty. This multiplication is philosophically relevant, as it marks a disruption in the Westphalian conflation of sovereignty with the nation state in the digital sphere. Larsen [5] also contends digital sovereignty is the ability to “own control over your own digital fate, which means the entire AI supply chain from data to hardware and software,” among other things. This broad view suggests that sovereignty in the digital age is more about being able to do things than about legal status—being able to shape their own technological future.

The concept of digital sovereignty is consequently ensnared in a dichotomy between two conflicting philosophical traditions. It is a legitimate successor to the statist tradition of Westphalian sovereignty, which is based on territorial control and jurisdictional authority. It embodies the perspective on capabilities articulated by Amartya Sen and Martha Nussbaum [6]; however, the essence transcends mere formal power, encompassing the ‘actual ability [to] function’ within one’s technological environment. It is not easy to bring these two traditions together. In fact, a lot of the current debate is about how to deal with sovereign insecurities that exist in both traditions.

Kurbalija [7] adds four further layers of digital sovereignty: infrastructure (cables, data centers, and chips); software and standards (algorithms, source code, and technical standards); data (ownership, storage, and circulation); and AI knowledge (cloud computing services and AI models). This layered ontology has the virtue of being philosophically clarifying since it reveals that digital sovereignty is not a two-state dichotomy but a high-dimensional spectrum and that states can be sovereign in one tier and non-sovereign in another. For example, a country might have robust legal regulations concerning the storage of data and yet rely on AI models built in another country to process that data, an illustration of what can be termed the paradox of formal sovereignty without substantive autonomy.

Another philosophical question is said to be the relation of digital sovereignty to cosmopolitan values. The European Commission [8] indicates that digital sovereignty should not be associated with protectionism or disconnection from the global web of relations but with strategic autonomy in a globalized and interconnected world. In a struggle to align sovereignty with cosmopolitan openness, the latter formulation raises the question of whether ‘authentic self-determination’ is possible when one is so thoroughly enmeshed in technologically based external systems. China’s equivalent restatement, the idea of cyber-sovereignty advanced by President Xi Jinping, tips the balance the other way by asserting that every state has the right to govern its own information space—a restatement of the principle of noninterference in informational sovereignty—but one that accords greater value to territorial control than to global connectivity or epistemic exchange.

3. The Sociopolitical Challenge of AI in the Context of Digital Sovereignty

AI exacerbates the contradictions within the digital sovereignty in four distinct but interconnected empirical dimensions.

3.1. Technical and Infrastructural Dependency

The creation and use of advanced AI systems depend on having access to computational infrastructure, high-performance chips, cloud computing platforms, and large-scale data storage that is currently limited to a handful of technologically advanced nations and

private companies. Kurbalija [7] notes that reliance on foreign AI infrastructure generates structural vulnerabilities: a state may lose effective control over essential governance and economic functions if critical AI systems or the data it processes are located outside the state's boundaries. From a philosophical perspective, this reliance is a sort of heteronomy, a state of being in which the conditions for self-governance of a political community must be determined by other decisions that were made elsewhere and which it did not have real participation in or sign off on.

AI can also be used to accelerate censorship and information warfare, making it faster and easier for governments to produce disinformation and conduct more advanced surveillance. This observation raises a further issue: the state can be held responsible for protecting its citizens from external interference, but the citizen also has to protect themselves against their state. One could say that digital sovereignty, in that sense, is two-sided (highlighting its external/internal dimension), a dimension that is often obscured by traditional sovereignty thinking and its statist focus.

3.2. *Legal and Jurisdictional Fragmentation*

The consequence of cross-border data flows is what legal scholars have derogatorily called “jurisdiction shredding”; the identical data is beholden to conflicting obligations in multiple legal systems at the same time. The United States CLOUD Act, for example, bestows the right of the American judiciary to the data of US companies located abroad, thus undermining the data sovereignty of other states [7]. This legal extraterritoriality presents a philosophically interesting problem for the Westphalian model of sovereignty, in that sovereignty in the digital realm cannot be guaranteed by territorial borders only but must be supplemented by engagement with the norms and regimes of international digital governance.

3.3. *Economic Disparities and Concentration of AI Power*

Froman [9] describes what he calls the AI sovereignty paradox: the real danger to smaller states is not that AI systems will become too powerful in some abstract way but that AI capabilities will become increasingly concentrated among a handful of states. Froman [9] notes that the United States holds approximately 75% of the world's AI supercomputing power and that the US and China together dominate AI models, cloud services, and semiconductors. This consolidation constitutes a form of structural injustice, systematically disadvantaging states that lack the resources to invest in AI infrastructure.

3.4. *Socio-Cultural Heteronomy*

Most large language models (LLMs) and other AI systems are trained based on data from high-resource languages and cultural contexts, namely English and Mandarin. The introduction of this type of technology at the language and cultural level of minority peoples could lead to what Floridi [1] terms informational imperialism, in which a dominant set of epistemological paradigms is systemically privileged over local knowledge systems and cultural identities. Meanwhile, synthetic media produced by AI—from deepfakes to disinformation—undermines the sources of public knowledge and weakens a community's ability to engage in rational collective self-governance, a key component of substantive democratic sovereignty.

4. Three Models of Digital Sovereignty: A Comparative Philosophical Analysis

4.1. *The Liberal Market Model: The United States*

United States digital policy is organized around the principles of market competition, private innovation, and national security [9]. It is not so much guided by an explicit theory of state power in cyberspace as by the deliberate absence of one. Philosophical analysis, however, reveals that this apparent absence is itself a substantive philosophical position and one with deep internal contradictions that cannot be resolved within its own conceptual framework. The model invokes, in different registers, three distinct liberal traditions: Lockean property theory, Millian expressive freedom, and Nozickian libertarianism. Examining each reveals not convergence but conflict. Locke's labor theory holds that an individual acquires rightful property by mixing their labor with an unowned resource [10]. Applied to the digital sphere, this theory appears to ground a right to data generated through one's own online activity. But the argument encounters an immediate inversion: in the actually existing US platform economy, it is corporations, not users, that acquire ownership of data generated through users' activity. The platform captures the data product of millions of users' labor through Terms of Service agreements that Locke's framework has no mechanism to legitimize, since Locke's theory of original acquisition presupposes that the laborer owns their labor product, not that they may waive that right in a boilerplate contract they did not meaningfully negotiate. The US model, then, is an inversion of Locke in that it uses the language of property rights to describe rights that it ultimately denies to those who produce the data. The Millian axis is equally unstable. Mill's [11] principle of harm states that the government may interfere with expression only when it results in direct harm to others; in the absence of harm, epistemic diversity and unfettered exchanges of ideas are intrinsically desirable. Early internet governance, for instance, invoked this principle to oppose content regulation. But disinformation generated by AI and algorithmic amplification of false content and synthetic media that cannot be told apart from genuine speech challenge the harm principle on its own: the harms are diffuse, probabilistic, systemic, and causally opaque rather than immediate and traceable. Mill's framework was designed to resolve disputes between discrete speakers and publicly identifiable victims, and thus the conceptual hardware for contemplating harms that arise through statistical aggregation and feedback dynamics at scale is simply not there. The Nozickian [12] minimal-state case for treating data as an area of unjustified coercion absent demonstrable harm (the threat to life and liberty supports the intervention) is impoverished already and becomes even more reductive, as it systematically discounts structural harms (including relational ones) that are real yet diffuse. The most important role for government in the digital economy is thus as a referee who mitigates market failure and protects the competitive structure from encroachment, but this referee role is normatively unsupported if the normative framework underpinning this role cannot handle the type of systemic harm AI creates.

This model is a constitutive tension between liberal universalism and geopolitical particularism. The United States has long promoted a "free and open" internet predicated on the liberal assumption that free flow of information is inherently beneficial. But the CLOUD Act, semiconductor export controls, and restrictions on foreign technology platforms demonstrate a more particularist reasoning: that national security concerns may trump liberal openness when the stakes are too high [5]. This vacillation between principled cosmopolitanism and pragmatic realpolitik reveals what Carl Schmitt [13] would read as the friend–enemy nexus underpinning liberal universalism concealed. The United States' advocacy for porous borders of information flow is only as wide as those borders serve its geopolitical interests and no further. The normative integrity of the liberal market

model is thus truly dubious: it is based on a tension that is never fully resolved between its Lockean–Millian foundations, which provide universally applicable rationales for digital openness, and a Schmittian exceptionality thinking that reinstates national particularity whenever the universalist matrix proves strategically inconvenient.

4.2. *The Techno-Legal Rights Model: The European Union*

The European Union provides the most philosophically sophisticated form of digital sovereignty and is one that ties democratic values and fundamental rights with techno-legal regulation. The EU's model reflects what Larsen [11] dubs techno-legal governance: the use of law to shape the normative fabric of the digital environment.

The philosophical underpinning is mainly Kantian, but identifying this affiliation is only a terminus a quo; the task of argumentation is to show in what way the general Kantian principles lead to the specific structure of EU digital law and in which points of that structure they are put under strain. Kant's Formula of Humanity gives a non-consequentialist basis for data protection that is not contingent on showing calculable harm. The automated treatment of personal information without informed consent transforms people into optimization instruments: Their attention, actions, and preferences are raw material for value-extraction schemes run on platforms answerable to shareholders rather than the people whose data they process. Each key design element of the GDPR can be translated as an application of the Formula of Humanity. The informed consent rule expresses respect for rational autonomy: it requires that individuals be provided with the information and authentic option to make use of their ability for self-determination in relation to the informational aspect of their existence. The principle of purpose limitation means that data may not be used for secondary purposes inconsistent with what persons originally consented to. The right to explanation in automated decision-making (one of the most philosophically important and contentious aspects of EU AI regulation) reflects the insight that algorithmic opacity undermines the capacity for rational self-governance that Kant holds to be the anchor of personhood: a person who is subject to an opaque algorithmic decision cannot meaningfully contest it through autonomous reasoning. The idea of informational Selbstbestimmung (informational self-determination) is not taken from Kant himself but rather formulated in the German Federal Constitutional Court's Volkszählung decision (1983), which translated Kantian autonomy into the constitutional domain of state data-gathering. This doctrinal genealogy is important: it reveals that the Kantian philosophical underpinning has been institutionally theorized through constitutional adjudication rather than simply rhetorically invoked. The EU model also takes inspiration from Habermasian communicative rationality [14]: the rightfulness of digital governance emanates from the character of the deliberative practices through which it rules rather than the substance of such rules. This can be seen in the multi-stakeholder regulatory design of the EU and its emphasis on transparency and public participation in AI regulation. Yet the Kantian–Habermasian rubric contains a profound inner contradiction that the EU model has failed fully to address. Kant's autonomy and Habermas's communicative rationality are based on an atomistic notion of the rational subject: the individual who makes autonomous decisions or who participates in deliberation is assumed to be a rational agent standing on her or his own. But the relational account to be developed in Section 5 of this paper claims that digital sovereignty can only be made sense of through the lens of constitutively embedded agents, whose ability to exercise self-determination is determined by the relational structures (economic, cultural, infrastructural) of which they are a part. The EU's Kantian framework is thus at odds with the relational conditions of possibility for actual informational self-determination: a framework built on the ideal of

individual rational autonomy has few resources with which to understand the structural and collective aspects of digital power.

The GAIA-X initiative is a pan-European federated data infrastructure that is trying to fill the gap left by US and Chinese cloud providers. It is a wonderful example of both the goals and the problems with this approach. True digital sovereignty is not just about laws. A country must also enforce those laws. A country that makes laws for high data protection standards but does not have its own cloud infrastructure is and will always be dependent on foreign providers who may or may not accept its normative commitments. This tension between normative ambition and infrastructural dependency has also been flagged from within the EU's own ethics apparatus: the European Group on Ethics in Science and New Technologies [15], in its Opinion on democracy in the digital age, warns of the expansion of Big Tech into the provision of public-sector goods and services and calls for a deliberate rebalancing of public and private responsibility in the digital sphere, lest dependence on privately owned infrastructure hollow out the very capacity for democratic self-governance that EU digital law is meant to protect. This concern reinforces the point made above: legal rights without infrastructural capacity risk producing a merely formal sovereignty, one whose exercise depends on the goodwill of private corporations answerable to shareholders rather than citizens.

4.3. *The Cyber-Sovereignty Model: China*

China's digital sovereignty regime draws on a layered philosophical tradition that requires careful disaggregation and, crucially, critical evaluation of whether its philosophical claims are genuine expressions of those traditions or selective appropriations that suppress their normatively significant elements. The Confucian stratum supplies a communitarian ontology: in the classical Confucian framework, the individual is constitutively embedded in hierarchical social relationships (wulun, 五伦) whose harmonious maintenance (he, 和) is the primary social benefit. Individual rights claims that disrupt collective harmony lack the moral primacy they enjoy in liberal theory. In the digital age, the concept is interpreted as a right for national governments to regulate information flows in the name of social cohesion or national interest. The idea of rectification of names (zhengming, 正名), the Confucian tenet that in social relations things must be correctly "named," is echoed in China's determination to dominate the epistemic space. But such chanting of Confucian philosophy is philosophically challengeable in one very particular and demonstrable way. Classical Confucianism is not merely a totalizing theory of collective subordination; it has an influential tradition of remonstrance (jian, 諫), the obligation of ministers and scholars to admonish a misguided ruler, and the doctrine of minben (民本, the people as the foundation), which makes political legitimacy contingent on the ruler's sincere service to the common good. Part of Confucian communitarianism's normative strength comes exactly from that accountability structure: that the community's right to exert authority over individual members is itself grounded in the fact that the community's rulers are accountable to the very community they govern. Xi's cyber-sovereignty doctrine keeps the first—namely, that individuals' informational freedom should be subordinate to collective authority—but systematically severs the second: those means of popular deliberation, critical remonstrance, and political responsibility that render Confucian communitarianism normatively defensible, rather than authoritarian. This selective appropriation is therefore not a genuine instantiation of Confucian political philosophy but a distortion that retains the vocabulary of collective harmony while eliminating the conditions that give that vocabulary its normative content. The Leninist layer compounds this problem: a vanguard party that claims to embody the collective will a priori cannot be subject to the public correction that Confucian remonstrance requires. The Schmittian element introduces a further and

deeper internal contradiction. Schmitt's [13] friend–enemy distinction holds that the political is constituted by existential antagonism. But classical Confucian political philosophy is premised on a fundamentally different ontology: it understands legitimate order as a harmonious relationship, not antagonistic differentiation. The introduction of a Schmittian logic of informational enmity (treating transborder data flows as carriers of hostile influence to be repelled) is in direct tension with the Confucian framework invoked to legitimize it, since Confucianism seeks to extend and order relationships, not sever them at a friend–enemy frontier. The philosophical architecture of Chinese cyber-sovereignty is therefore not merely composite but internally contradictory. It combines a communitarian premise drawn from Confucianism with an antagonistic logic drawn from Schmitt that the Confucian framework itself would reject. This internal contradiction has practical consequences: a doctrine of digital sovereignty that claims communitarian foundations but enacts Schmittian exclusion cannot coherently appeal to the normative resources of either tradition without confronting the deep incompatibility between them. The model's philosophical claims are, in this sense, less a coherent political philosophy than a post-hoc legitimization of decisions made on other grounds.

Kurbalija [7] argues that China has developed a digital ecosystem that is largely self-sufficient, encompassing communication platforms, payments, and cloud computing services that replace Western equivalents, and at the same time, it enforces strict data localization rules for personal and business data that it deems sensitive. This scheme provides a reasonable level of technical sovereignty at a very high normative cost: it suppresses epistemic freedom, alienates the global commons of knowledge, and is said to have enhanced state surveillance of citizens. From a perspective of normativity, the Chinese model illustrates how sovereignty claims can be mobilized not only to resist external subjugation but also internal subjugation of a political community, a dialectical possibility that Westphalian sovereignty theorizing has historically ruled out.

5. Towards a Relational Notion of Digital Sovereignty

The above considerations indicate that none of the three prevalent conceptions of digital sovereignty, taken by themselves, are philosophically sufficient. The liberal market model fails to properly address global structural inequalities in access to AI power. In the cyber-sovereignty model, state authority is equated with the “common good” of the political community it claims to represent. While the techno-legal rights model is normatively sophisticated, it assumes or materially requires domestic technological capacity, a condition that many states currently do not have.

This article presents relational digital sovereignty as a more philosophically adequate account. This concept is informed by four converging intellectual traditions, each of which addresses a dimension of the problem that the others leave underspecified. The account draws, first, on the relational turn in political philosophy [6,16], according to which autonomy and self-determination are not pre-social properties of isolated individuals or states but are constituted through relationships of recognition, cooperation, and mutual accountability. This philosophical premise finds a rigorous sociological counterpart in the relational sociology developed by Pierpaolo Donati, notably in *Transcending Modernity with Relational Thinking* [17], which argues that social relations constitute a reality in their own right, irreducible either to the individuals who enter into them or to society conceived as a supra-individual whole, and that subjects are simultaneously internal and external to the relations that constitute them. Applied to digital sovereignty, this relational-realist ontology supports the claim advanced here that a political community's capacity for self-determination is not a self-standing possession but an emergent property of its relations with other states, corporations, and international institutions. Applied to digital

sovereignty, this relational ontology entails that meaningful digital self-determination cannot be achieved through national self-sufficiency alone, but only through just and equitable participation in structures of global digital governance. Second, and more specifically, the account draws on Couldry and Mejias's [18] framework of data colonialism. They contend that the prevailing mode of data extraction by global platforms mirrors colonial relations of appropriation: in the same way that historical colonialism extracted raw materials from peripheral regions to produce value for metropolitan centers, contemporary data capitalism extracts behavioral and relational data from users (vastly concentrated in the Global South) to produce value for platform corporations headquartered in the United States and China. It is not simply a metaphor; it is a statement about a structural homology between two forms of relation that are oriented to extracting value from less powerful actors. For the theory of digital sovereignty, this conception has a definitive implication: digital sovereignty cannot adequately be theorized at the level of state-to-state relations alone, because the primary site and dynamic of digital power asymmetry ultimately resides in the platform-to-user relations that span and cut across state boundaries. A relational account of digital sovereignty must address both dimensions. Van Dijck, Poell, and de Waal [19] extend this analysis by demonstrating how platform logics (datafication, commodification, and selection) systematically reconfigure public institutions and civic self-governance across all social domains; their work makes clear that platform architectures are not neutral intermediaries but sites of power that determine whose values and interests are encoded into the digital infrastructure through which political life is increasingly conducted, thereby rendering purely state-centric accounts of digital sovereignty structurally incomplete. Third, Fraser's [20] distinction between redistribution and recognition identifies two irreducible dimensions of justice that the relational account must address simultaneously. Redistribution concerns the equitable allocation of material resources and, in the digital context, access to computational infrastructure, AI capabilities, and the economic value generated by data. Recognition concerns the equal standing of different cultural, epistemic, and linguistic communities in the shared social world. Fraser argues that these two dimensions cannot be collapsed into each other: a purely redistributive approach that does not address misrecognition will fail to achieve justice, and a purely recognitional approach that ignores material inequality will similarly fail. Applied to digital sovereignty, this means that a relational account must address both the structural inequalities in the global distribution of AI capabilities, the redistribution dimension that Froman's [9] AI sovereignty paradox makes visible, and the epistemic and cultural misrecognition embodied in the dominance of English-language, Western-trained AI systems over minority languages and knowledge systems. Vietnam's AI Law's insistence on Vietnamese-language AI development is, on this analysis, simultaneously a redistributive demand and a recognitional one. Fourth, the account draws on the infrastructure studies tradition in science and technology studies. Star and Ruhleder [21] established that infrastructure is not a neutral substrate but a relational achievement: it becomes infrastructure in relation to organized practices, and its governance is therefore inherently political. DeNardis [22] developed this insight for internet governance specifically, demonstrating that the governance of technical infrastructure—protocols, routing architectures, and domain name systems—embeds political choices that are invisible precisely because they are infrastructural. Musiani et al. [23] elaborated the "infrastructural turn" in internet governance scholarship, arguing that who controls the material substrate of digital communication determines, in ways that no amount of legal regulation can fully compensate, who effectively exercises digital sovereignty. Pohle and Thiel [24] brought these insights to bear on digital sovereignty specifically, arguing that relational frameworks must account for the layered materiality of digital infrastructure, not merely its normative superstructure. Bratton [25], in *The Stack: On Software*

and Sovereignty, extends this argument to a planetary scale, demonstrating that layered computational infrastructure—from undersea cables and data centers to cloud operating systems and user interfaces—constitutes a new form of sovereignty that operates across, beneath, and through territorial state authority; on his account, who governs the stack governs political life, and no amount of legal regulation at the state level can substitute for control of the infrastructural substrate itself. Together, these four traditions—relational political philosophy, data colonialism theory, the redistribution/recognition framework, and infrastructure studies—enable a conception of digital sovereignty that is at once more empirically adequate and more normatively demanding than any of the three models examined above. Digital sovereignty is not merely about what states may do within their territories; it concerns the relational conditions under which all political communities and the individuals and cultural communities within them can participate on genuinely equal terms in shaping the digital environments that increasingly constitute the conditions of political life.

The third philosophical pillar of the relational model requires careful engagement with Rawlsian justice and with the specific limitations of Rawls's own account that must be acknowledged before his framework can be applied to global digital governance. In *The Law of Peoples* [26], Rawls explicitly declined to extend the difference principle, the requirement that social and economic inequalities be arranged to maximally benefit the least advantaged, to the global order. His reasoning was that the difference principle is justified only within domestic societies, which constitute closed cooperative schemes whose members share a common institutional framework; the global order, on Rawls's view, lacks the dense cooperative structure that would generate equivalent obligations across states. This significant limitation has been challenged vigorously by cosmopolitan political philosophers. Theorists like Beitz [27] have argued that the global economy of interdependence already is a cooperative scheme of the type that Rawls asks for, and his own principles of justice require a global difference principle when applied to the actual facts of international relations. Pogge [28] extended this line of argument by showing that wealthy nations were not only obligated to ameliorate global poverty but were also actively culpable in imposing the global institutional order that produced it—a duty of justice rather than merely one of humanitarian aid. The relational account proposed here follows Beitz and Pogge in asserting that the deep structural global AI economy interdependencies (data, algorithms, computational infrastructure, and AI knowledge that is heavily concentrated among a few states and firms, while the rest depend on them) are precisely the kind of cooperative scheme that creates obligations of justice. On this Beitz-Pogge interpretation of Rawlsian justice, any regime of digital sovereignty (even if applied in such a way as to allow “balance”) that systematically favors more technically advanced states, whether through data extraterritoriality, chip export controls, or the structural asymmetries of AI platform economics, is unjust, even if it is formally compliant with international law. The AI sovereignty paradox elaborated by Froman [9] is therefore not merely an economic problem but a problem of global distributive justice. A relational notion of digital sovereignty draws these strands together: states possess legitimate claims to meaningful participation in digital infrastructure and data governance, but these claims must be balanced against citizens' rights to epistemic openness; the global distribution of AI capabilities is a matter of justice imposing obligations on technologically advanced states; and participation in reformed multilateral institutions of digital governance is both a means and a constitutive element of genuine digital self-determination.

These normative commitments have policy implications that differ from those of all three competing conceptions analyzed above. Relationality versus liberal market model: The relational approach claims that market-based solutions are inadequate to ensure a fair

distribution of AI capabilities. Against the model of cyber-sovereignty, it argues that even the sovereignty of states cannot override the right of their citizens to informational freedom. In contrast to the existing techno-legal rights model, it insists that the normative basis of digital regulation be articulated in a manner that is genuinely inclusive, rather than simply exporting the norms and expectations of economically powerful states to those who lack the capacity to oppose them.

6. Vietnam's Legislative Architecture: A Test for Philosophical Frameworks

Vietnam's interaction with digital sovereignty thus serves as a valuable test case for the kinds of philosophical frameworks discussed above and, in particular, for the relational account of digital sovereignty developed in Section 5. As a middle-income, post-socialist state with a single-party system and fast-digitalizing economy, Vietnam exhibits a hybridization of the European rights-based model and the Chinese model of data localization and state surveillance, though it lacks the domestic technological capacity of either.

Vietnam has incorporated an element of the logic of cyber sovereignty in its Cybersecurity Law, mandating foreign digital platforms to set up domestic offices and store the data of Vietnamese users within the country—a data localization condition. The Law on Personal Data Protection and the Law on Data, which will enter into force in 2026, introduce the most extensive licensing-and-supervisory scheme for data governance [29]. Taken together, these laws suggest a possible understanding of a state-managed data sovereignty approach: one that claims territorial dominance over flows of data but that tries to be open to global commerce and finance. And the AI Law, which imposes requirements of transparency and ethics on AI systems and prioritizes Vietnamese-language AI development as cultural and linguistic self-determination [30], brings a normative aspect that transcends mere technical regulation. The explicit representation of Vietnamese-language AI as a shield (*lá chắn*) reflects a view of sovereignty at once political and knowledge-based: the capacity to govern not only the flow of data but also the epistemic lenses through which citizens come to understand themselves and the world. This is similar to philosophical ideas of linguistic self-determination being a prerequisite for political self-governance.

We know, from preceding perspectives, the strengths and limitations of philosophical models above are shown in Vietnam's approach. The EU model has a techno-legal rights framework that comes with some important normative weapons, the right of citizens to have informational self-determination, but it assumes there are national technological capabilities that Vietnam does not have. The Chinese model of cybersovereignty and its associated protocols of data localization and platform administration could lead to the closure of epistemic openness and civil liberties. Trying to strike a balance between these two positions, Vietnam is in the process of building a legal framework; whether it can find its own way between the philosophical [31] and the practical remains an open question.

A related but especially important tension has been the balance between digital sovereignty and economic growth. Foreign capital, global supply chains, and access to foreign-developed AI tools are all vital to Vietnam's technology sector. A demand for strict data localization may be a formal victory for digital sovereignty, but it could introduce economic challenges so severe that they effectively prevent the growth of any kind of AI industry at home, yet another version of the paradox of formal sovereignty without substantive autonomy discussed in Section 2. Froman's [9] insight that smaller states risk not only being dwarfed by superior AI systems but also being left economically isolated by AI agglomeration applies directly to Vietnam's strategic position. Huynh's [32] political-economy analysis of Vietnam's AI infrastructure regime substantiates this claim empirically: Vietnam's legal architecture liberalizes foreign investment in data centers and

cloud services, for example, through recent partnerships with foreign chipmakers, while reserving state discretion over access to national databases and cross-border data transfers, a hybrid arrangement that Huynh characterizes as negotiated dependency rather than techno-nationalist autonomy. This framing lends further empirical support to the paradox of formal sovereignty without substantive autonomy identified above.

7. Conclusions

In this article we are led to argue that AI is an ontological challenge to classical security and, ultimately, sovereignty, and that none of the three predominant conceptualizations of digital sovereignty—the liberal market conception, the techno-legal rights conception, and the cyber-sovereignty conception—are philosophically sufficient on their own. All three models rest on normative assumptions that prove insufficient when confronted with the realities of global AI development.

Vietnam's new laws show how challenging it is to solve the problem in theory and practice. Vietnam's balancing act between data localization and an open economy, as well as cultural self-determination and global integration, represents an emerging, if still incomplete, response to the tensions inherent in digital sovereignty. The relational approach developed in this article suggests that these pressures could not be fully addressed within the conceptual grammar of classical sovereignty theory but rather required a more fluid, interdependent, and justice-oriented understanding of digital self-determination. There are several additional open questions that deserve further philosophical attention.

What is the proper balance between the normative importance of national digital sovereignty and the rights of individuals to exist as epistemically free and informationally self-determined agents? Perhaps there are institutional arrangements through which a truly global AI governance could be made more attentive to the wants and needs of less technologically advanced states. And what understanding of the common good (national, regional, or global) should guide the building of AI systems that by necessity go beyond the borders of any particular political community? These issues are likely to continue being of relevance—possibly even increasingly so—as AI reshapes the conditions for political life around the world.

Funding: This research received no external funding.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Floridi, L. The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philos. Technol.* **2020**, *33*, 369–378. [CrossRef] [PubMed]
2. Bodin, J. *On Sovereignty: Four Chapters from the Six Books of the Commonwealth*; Franklin, J.H., Ed. and Translator; Cambridge University Press: Cambridge, UK, 1992.
3. Hobbes, T. *Leviathan*; Andrew Crooke: London, UK, 1651.
4. Roberts, H. Digital sovereignty and artificial intelligence: A normative approach. *Ethics Inf. Technol.* **2024**, *26*, 70. [CrossRef]
5. Larsen, C. The geopolitics of AI and the rise of digital sovereignty. *Brookings Institution*, 8 December 2022. Available online: <https://www.brookings.edu/articles/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/> (accessed on 9 July 2026).
6. Nussbaum, M.C. *Creating Capabilities: The Human Development Approach*; Harvard University Press: Cambridge, MA, USA, 2011.
7. Kurbalija, J. Global digital sovereignty shaped by infrastructure, services, data and knowledge. *Digital Watch Observatory*, 5 March 2026. Available online: <https://dig.watch/updates/global-digital-sovereignty-shaped-by-infrastructure-services-data-and-knowledge> (accessed on 9 July 2026).
8. European Commission. *Open But Not Powerless: Towards a Common Understanding of EU Digital Sovereignty*; JRC Report No. JRC144908; Publications Office of the European Union: Luxembourg, 2025.

9. Froman, M. The AI sovereignty paradox at home and abroad. *Council on Foreign Relations*, 27 February 2026. Available online: <https://www.cfr.org/articles/the-ai-sovereignty-paradox-at-home-and-abroad> (accessed on 9 July 2026).
10. Locke, J. *Two Treatises of Government*; Laslett, P., Ed.; Cambridge University Press: Cambridge, UK, 1988.
11. Mill, J.S. *On Liberty and Other Essays*; Gray, J., Ed.; Oxford University Press: Oxford, UK, 2008.
12. Nozick, R. *Anarchy, State, and Utopia*; Basic Books: New York, NY, USA, 1974.
13. Schmitt, C. *The Concept of the Political*; Schwab, G., Translator; University of Chicago Press: Chicago, IL, USA, 2007.
14. Habermas, J. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*; Rehg, W., Translator; MIT Press: Cambridge, MA, USA, 1996.
15. European Group on Ethics in Science and New Technologies. *Opinion on Democracy in the Digital Age*; Opinion No. 33; Publications Office of the European Union: Luxembourg, 2023. [CrossRef]
16. Young, I.M. *Justice and the Politics of Difference*; Princeton University Press: Princeton, NJ, USA, 1990.
17. Donati, P. *Transcending Modernity with Relational Thinking*; Routledge: Abingdon, UK, 2021.
18. Couldry, N.; Mejias, U.A. *The Costs of Connection: How Data Is Colonizing Human Life and Appropriating it for Capitalism*; Stanford University Press: Redwood City, CA, USA, 2019.
19. van Dijck, J.; Poell, T.; de Waal, M. *The Platform Society: Public Values in a Connective World*; Oxford University Press: Oxford, UK, 2018.
20. Fraser, N. Rethinking recognition. *New Left Rev.* **2000**, 3, 107–120. [CrossRef]
21. Star, S.L.; Ruhleder, K. Steps toward an ecology of infrastructure: Design and access for large information spaces. *Inf. Syst. Res.* **1996**, 7, 111–134. [CrossRef]
22. DeNardis, L. *The Global War for Internet Governance*; Yale University Press: New Haven, CT, USA, 2014.
23. Musiani, F.; Cogburn, D.L.; DeNardis, L.; Levinson, N.S. (Eds.) *The Turn to Infrastructure in Internet Governance*; Palgrave Macmillan: London, UK, 2016.
24. Pohle, J.; Thiel, T. Digital sovereignty. *Internet Policy Rev.* **2020**, 9, 1–19. [CrossRef]
25. Bratton, B.H. *The Stack: On Software and Sovereignty*; MIT Press: Cambridge, MA, USA, 2015.
26. Rawls, J. *The Law of Peoples*; Harvard University Press: Cambridge, MA, USA, 1999.
27. Beitz, C.R. *Political Theory and International Relations*; Princeton University Press: Princeton, NJ, USA, 1979.
28. Pogge, T. *World Poverty and Human Rights: Cosmopolitan Responsibilities and Reforms*; Polity Press: Cambridge, UK, 2002.
29. Shivhare, S.; Thong, J.I.K.; Paulger, D. FPF Releases Updated Issue Brief on Vietnam’s Law on Protection of Personal Data and the Law on Data. Future of Privacy Forum. 2026. Available online: <https://fpf.org/wp-content/uploads/2026/01/January-2026-FPF-Issue-Brief-Making-Sense-of-Vietnams-Latest-Data-Protection-and-Governance-Regime-1.pdf> (accessed on 9 July 2026).
30. Doan, N. AI Law 2025: A “shield” protecting national culture and digital sovereignty. *Dan Tri News*, 5 March 2026. Available online: <https://dantri.com.vn/cong-nghe/luat-ai-2025-la-chan-bao-ve-van-hoa-va-chu-quyen-so-quoc-gia-20260304124836653.htm> (accessed on 9 July 2026).
31. Giang, T. Vietnam will announce an updated AI strategy and AI law. *Government Newspaper*, 15 September 2025. Available online: <https://baohinhphu.vn/se-co-ban-cap-nhat-chien-luoc-ai-quoc-gia-va-luat-ai-102250915130224143.htm> (accessed on 9 July 2026).
32. Huynh, H. *Digital Sovereignty or Dependency? The Political Economy of AI Infrastructure in Vietnam*; SSRN Working Paper No. 5314114; SSRN: Amsterdam, The Netherlands, 2025. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.