Digital trade and data sovereignty: Comparative legal frameworks in the EU, US, Africa and China

Godswill Owoche Antai[1], Shishitileugiang Aniashie Akpanke[2], Alex Olajide[3] & Victory Omali Obule [4]

[1] LL.B, LL.M, Ph.D (Calabar), B.L (Kano), Ch;MC (Nigeria), Senior Lecturer and Head of Department, Post-Graduate and Diploma, Kampala International University, Kampala, Uganda, Email: godswill.antai@kiu.ac.ug

[2] LL.B, LL.M, Ph.D (Calabar), B.L, Lecturer, Faculty of Law, University of Calabar, Calabar, Nigeria, Email: shikpansbrain013@gmail.com

[3] LL.B (Calabar), B.L (Lagos), Head of Civil Practice, Gray Attorneys and Solicitors Law Firm, Calabar, Cross River State, Nigeria, Email: princewillalex@gmail.com

[4] LL.B (Calabar), B.L (Enugu), Head of Chamber, Gray Attorneys and Solicitors Law Firm, Calabar, Cross River State, Nigeria. Email: obulevictory@gmail.com

Abstract

The internationalization of business transactions has made transactional data a high-value asset, which has resulted in controversies over data sovereignty. Within the international economy, driven by AI, Cloud Computing, and Mega-Data-Centres, countries often find themselves caught between competing demands to facilitate international data flows and protect sovereignty. This research explores the impact of various approaches to digital governance. Through a comparative methodology, the study combines qualitative analysis of laws and policies under international economic law regimes and theories of digital governance to assess approaches in the larger trading frameworks comparatively. Herein, the four paradigms established include that of the EU, which protects rights at its forefront and has strengthened its laws under GDPR and prospective AI law and schemes such as EuroStack to decrease overdependence on alien "hyperscale clouds," while those of the US are market-driven and open, but threatened by AI security laws and enhanced surveillance powers under FISA/CLOUD Act, the AfCFTA Digital Trade Protocol with its eight Annexes in 2025, signals a historic shift toward harmonized rules for cross-border payments, data flows, and digital identity, although capacity gaps persist within the region. Findings indicate an asymmetry of sovereignty and openness, with sovereignty strategically promoted by all countries, including the EU, China, and other states, with openness advocated by the US, and the hybrid integration approach in Africa. Emerging trends include AI geopolitics, Blockchain ID, and Privacy-Enhancing Technologies, widening sovereignty and governance gaps, and creating "digital silos." In all, this research proposes sovereignty pluralism in the digital era, with ICC and UN/CEFACT's multi-lateral approaches towards interoperable standards under WTO frameworks.

Keywords: Data sovereignty, Digital trade, Cross-border data flows, Comparative legal frameworks, International economic law

Introduction

Digital trade has evolved in recent years to become the foundation for world economies. Data transfer, based on International Chamber of Commerce (ICC, 2024) statistics, adds USD 2.8 trillion to GDP, while world trade in merchandise in 2025 will grow to USD 11 trillion, exceeding trade in merchandise in value (WTO, 2025). These dramatic changes in value are due to the exponential growth in cloud computing, AI, and platform-based business, which requires frictionless data flow from different countries. This dependence has sparked debates on data sovereignty, with each national sovereignty seeking to balance societal openness with sovereignty on security, privacy, and regulation (Mueller, 2020).

Interestingly, in spite of the fast growth in online trade, international governance is fragmented. States formulate different rules to govern their respective jurisdictions, whereas EU rules contain strict rules on protecting data, based on the General Data Protection Regulation (GDPR).

Accordingly, Article 8 of the EU Charter of Fundamental Rights, it could be safely claimed in support of the General Data Protection Regulation, that its regulations apply beyond EU territory. The Charter stipulates 'digital sovereignty' to guarantee any organisation, no matter the jurisdiction, satisfies its stringent guidelines for any organisation processing information belonging to EU citizens. This complies with their perception about controlling data being a crucial activity to validate democratic principles in any digital-based economy. This law, which academics believe to be "Brussels Effect," has produced 'a global gold standard, shaping more than 120 jurisdictions, according to Krook, et.al., (2024), despite increased costs for its adherence, coupled with many other challenges in cross-border data flow, like cloud computing, AI, and face, among many other information-based industries (Antai, 2024).

Moreover, the EU Artificial Intelligence Act (AI Act), though not yet in force, further expands this sovereignty paradigm into algorithmic regulation. It is indeed the world's first comprehensive AI law, initially distinguishing AI systems on the grounds of risk, with obligations commensurate with societal risk. High-risk applications, such as biometric systems, data, or credit scores, require strict transparency obligations, whereas general-purpose models have to undergo an additional compliance check (Njoroge, 2024), although concerns about their limitations to innovation abound.

Again, a critical analysis of China's model theory, it could be asserted that China's model incorporates data localisation/cybersecurity with Data Security laws, which requires data security to be viewed from a national security paradigm (Creemers, 2022). For Africa, there is the African Continental Free Trade Area (AfCFTA) Digital Trade Protocol with aims improve intra-Africa trade from 18% in 2022 to 50% by 2030 to achieve harmonisation despite infrastructural defects exists, while aiming to improve intra-Africa trade from 18% in 2022 to 50% by 2030, in response to Nigeria's report on State House (Shettima, 2025). Although there are bilateral or plurilateral agreements, such as the EU-US Data Privacy Framework (DPF), AfCFTA Digital Trade Protocol, amongst others, there is no agreement regarding cross-border flows in general. It is estimated, for example, that there are over 3,400 U.S. companies that have DPF certification (U.S. Department of Commerce, 2025).

Evidence suggests that openness in regard to data flow is something the United States embraces. These increased surveillance powers under Section 702 of the Foreign Intelligence Surveillance Act (FISA) and territorial application provisions in the CLOUD Act have continued to generate sovereignty issues in other countries. It is, however, important to note that these powers have strengthened with new executive orders regarding restrictions in sharing sensitive data to "countries of concern" such as China, Russia, in its 2025 Department of Justice (DOJ) rule and Executive Order 14117, in which there has been an "about face" in policy (Center for Cybersecurity Policy, 2023).

Contrarily, the Data Security Law, Personal Information Protection Law (PIPL), and the Cybersecurity Law amendment, to be enforced in 2026, have imposed punishments of up to USD 1.4m (Liu, 2023). These laws are necessary from a security perspective, with their scope extending to both local and foreign actors. It is important to mention that although researchers have identified the liberal data model in the U.S., rights-based in the EU, and security-focused in China, there is, in these particular approaches, an essential gap because no comprehensive comparative analysis has yet included these models in frameworks on international economic law on digital governance theory (Edet, Antai & Itafu, 2022).

This research critically questions how different views on data sovereignty shape economic openness in relation to state regulation in the international digital economy.
Notably, within the context of international economic law, international digital trade has not only now become one of the most crucial elements in international trade, but it is largely regulated under diverging and, in some ways, conflicting regulatory policies. By using the comparative legal method in approaching doctrinal analysis, four economic data sovereignty models, from the EU, US, China, and Africa, are compared in this research to analyse their foundations (Antai et al., 2024).

According to Floridi (2022), digital sovereignty pluralism is a conceptually coherent method for examining the co-presence, in a globalised information economy, of different governance models, each with its own underlying principles, values, or paradigm. These values vary from region to region. These different values lead to several disparities in regulations, thereby creating interoperability problems, cross-border regulation, and multilateral regulation. Hence, in seeking to provide answers to its research questions, it proposes to move forward with its framework to understand "digital sovereignty as a legal concept, as well as its utility in geopolitics in constructing patterns in investments, trade, and openness in technology" (Andrade et al., 2025).

The contribution to existing literature exists in two folds. First, it fills the gap in scholastic international economic law, in that it embraces not only policy changes, crucial to doctrinal analysis, but also innovation in technology, such as AI, cloud sovereignty, and Private-Enhanced Technology, in transforming the dualistic nature of digital trade regulation. Secondly, the research offers pragmatic answers to these challenges in proposing ways to achieve harmonisation of regulations, balancing state sovereignty with the efficiency needs of transnational markets.

Theoretical and Conceptual Framework

The conflict between cyber sovereignty and cyber interdependence mirrors paradigm conflicts in international governance (DeNardis, 2014); while statist approaches to cyber sovereignty emphasise management, cyber liberalism stresses openness in governance (Chander & Lê, 2015). Accordingly, David & Brierley (1985) on functionalism view divergence in regulation based on societal needs, while comparative institutionalism places emphasis on governance architectures in shaping respective legal outcomes, according to Hall & Taylor (1996). It is important to mention here that cyber sovereignty remains controversial in international economic laws, specifically regarding global governance theory. Moreover, cyber sovereignty specifically matches statist approaches, explicitly regarding data as some kind of energy resource, or military security, to specifically mandate localisation policies, security-reliability-based regulation in cyber infrastructures, amongst others. Conversely, liberal approaches to cyber sovereignty argue for radically low levels of restrictions to cross-border information flow in their rules, principles, and policy guidelines. Typically, for liberal theorists, there are these general policy arguments usually canvassed to support innovation, productivity gains in cross-border trade, which often result in competitiveness in their respective frameworks (Bradford, 2020).

Going forward, there is no doubt to say that digital sovereignty has evolved to be one of the most debated concepts on issues pertaining to political power, technology, and international diplomatic relations. Notably, scholars have observed that with increasing digital interdependence, there has been a renaissance in which countries have sought to reaffirm sovereignty over cyberspace, refuting earlier views about internet space being out of state grasp or reach. It could also be inferred that policy changes in modern times provide insight into how concepts like digital sovereignty have real-world applications in decision-making in these areas (Bradford, 2020). For example, in 2024, discussions in the EU, which revolved around limiting sovereignty from its draft regulations for cybersecurity certification to enable U.S. cloud companies to participate in certification, sparked major debates on what constitutes EU sovereignty in the face of digital transformation (Kuner, 2021).

Historically, sovereignty relied on the Westphalian model, which stressed territorial sovereignty and state autonomy (Croxton, 1999). Digital technology, on the other hand, together with other forms, disrupted these concepts, as it allowed for immediate cross-border communication flows, which could not be controlled by national sovereignty in any conventional manner (Greenleaf, 2021). Even as it has been asserted that the shift in sovereignty from spatial to infrastructural power is crucial in comprehending power in the modern era of technology. It would not be wrong to assume, therefore, that sovereignty in its modern manifestation not only resides in legal systems, rules, or regulations, international treaties, or telecommunications, human rights, or any other kinds of sovereignty.

Going forward, several theories have evolved from these. One such theory is data sovereignty, whereby data produced under the territorial authority of any given state shall be controlled by such laws. Data sovereignty has, in fact, found resonance in light of the massive data being produced by tech companies, thereby shifting such companies into quasi-sovereign entities. These regulations, such as the Data Governance Act and Data Act, represent data sovereignty not only as a body of laws, but also as a mechanism for realising geo-politics in data sharing, wherein ideals like transparency, trust, and fundamental rights have been embedded in such sharing (Greenleaf, 2021).

Apart from these, it could be apt to point out that in relation to digital sovereignty, there is what is called technological sovereignty, which is more concentrated on maintaining sovereignty in critical infrastructures in the digital space. These could be semiconductors, clouds, or artificial intelligence networks. The Digital Europe Programme in the EU, with its primary focus on high-performance computing in cybersecurity, is an example of such, even with an outlook to minimise structural dependencies on other countries for their needs (Antai et. al., 2025).

On the other hand, there is also the concept of cyber sovereignty, which stresses the right viability of sovereignty in regulating cyber activity on its soil. Moreso, China's cyber governance offers an apt example, with laws such as the Data Security Law and Personal Information Protection Law extending their regulation to not just national space but generally to extraterritorial space. These sovereignty policies have generated controversies about their spread to cyberspace, especially with regard to computational studies revealing cyber sovereignty's role in its regulation ambitions for AI (Aidonojie et al., 2025). Again, it is crucial to point out that sovereignty, from a modern scholarly perspective, is being progressively appreciated for its networked, multi-level character, spread out over states, corporations, standardisation bodies, and supranational entities (Gorwa & Garton, 2020).

Legal Theories in Comparative Analysis

Functionalism and comparative institutionalism provide useful lenses for understanding why regulations on data sovereignty have diverged in each region. Though these regions face common imperatives regarding cross-border flow management, infrastructure security, and balancing innovation with rights, each region's policies have

diverged in response to its unique institutional imperatives (Belli & Jiang, 2024). Functionalism suggests, for example, that each legal frameworks create institutions to meet its needs, yet with varying rules in kind (Musiani, 2021). Here, EU countries like Germany, in cooperation with France, have adopted sovereignty policies such as the sovereign cloud policy and '*Cloud de Confiance*.' On the other hand, in countries like the U.S., sovereignty is expressed in other ways, such as enhanced competitiveness with less stringent, market-driven regulations, such as CCPA/CPRA in California, though overall federal law remains disorganised (Chander & Sun, 2023). Within Africa, these flows are responsive to pressure from institutional incapacity and AfCFTA, with Kenya, for example, passing national law to attract capital with its 'Privacy Law.' China, on the other hand, incorporates sovereignty in its centralised government, with laws such as PSA/DSL, buttressed by firmer police powers for its Cyberspace Administration (Cong, 2024). It is therefore worthy of note to say that comparative institutionalism, on its own, explains with institutional variations, for example, EU states 'enabling institutional frameworks for harmonization, while the incapacity in developing or underdeveloped regions lead to disorganisation in MD laws, such as in U.S., while in AfCFTA, regions like Kenya, for example, align laws for investment, with overall southern Africa insufficient capacity in regional law enactment (Wolff, Adeyemi, & Singh, 2025). It is necessary to affirm that institutional settings have contributed significantly to the course being adopted by data sovereignty regulation in the EU, the US, China, and Africa. (Chander & Sun, 2023).

Within Africa, comparative institutionalism is also applicable in relation to the disparities in state capacity and the maturity of regulation on data sovereignty on the continent. Mauritius, located on the east coast of Africa, in particular, together with other West African countries like Ghana, represent states with data protection agencies that are domestically independent enough to enforce compliance with data sovereignty rules on big companies operating in these jurisdictions. The point to note, regarding these jurisdictions, is, however, based on their enactment and capacity to enforce. Within Ghana, for example, its enactment on Data Protection in 2012 with the appointment of Data Protection Commission for Data Protection Act, culminated in creating an entity to regulate all personal data processing systems, whether undertaken by other countries, meaning foreign companies operating within their jurisdictions (Belli & Jiang, 2024). Its capacity to enforce, through investigation, issuing an enforcement notice, or enforcing compliance, in particular, forms an essential platform for regulation to carry any significance regarding holding big companies accountable for adherence to regulations in processing any individual's private information remotely in Ghana or its associations with its citizens residing there (Belli & Jiang, 2024).

Correspondingly, there is a defined, formalised dedication to data-protection regulation in Mauritius under the Data Protection Act of 2017, where there is a Data Protection Office, controlled by the Data Protection Commissioner, whose autonomy is expressly defined in law (Data Protection Act of Mauritius, 2017). While there are some procedural constraints, like as reports to prosecutors for some orders on enforcement action. Nevertheless, there is, in any case, an administrative framework to endow Mauritius with its capacity to adequately regulate data-protection in complex cross-border business settings in such corporations too (European Parliament, 2024).

Another interesting example, in Nigeria, demonstrates dynamic institutional changes in data governance in Africa. The establishment of the Data Protection Commission is, in itself, with its national Data Protection ACT in 2023, a major institutional leap forward (Ogu, Enyia, & Antai, 2024). Nigeria's Data Protection Commission, for example, has a defined mandate compared to other enactments on such regulation, now possessing powers to issue orders for compliance, undertake necessary investigation, as well as administrative punishment in the form of administrative fines

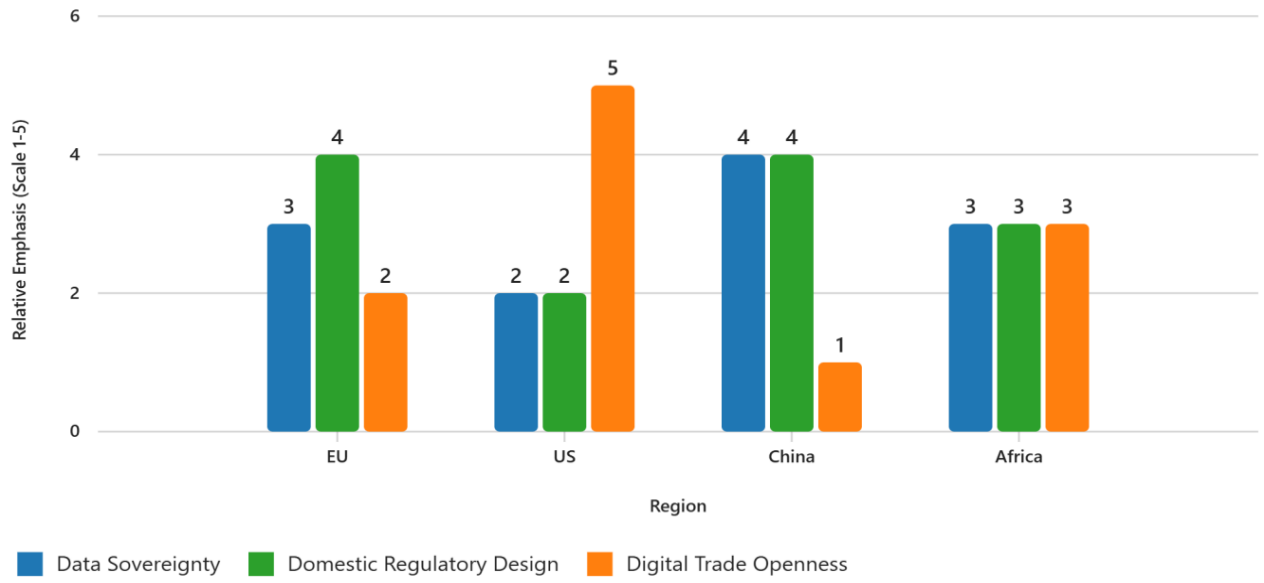
(Nwodo & Amucheazi, 2025). Another example is in Uganda, operating with what is destined to be an increasingly powerful Data Protection Office, with the Data Protection Privacy Act in 2019, operating with significantly more powers to exercise influence on multinational companies operating in its economy (Uwadinma, 2025). Its governance, through its location in a different ministry, shows its capacity to exercise powers to affect decision-making, albeit in a less authoritative capacity, on its supervisory powers over such entities operating in its economic space (Kayeki, 2025).

On the other hand, based on these considerations, countries with less developed institutions usually end up with wide sovereignty laws, which are difficult to operationalise. Regional organisations, such as the African Union, have become forces for harmonisation. These have enabled common standards to be attained through the Data Policy Framework and the AfCFTA Digital Trade Protocol. The development of implementation guidelines for digital trade for countries by the African Union demonstrates their increasing significance in creating common rules for countries with different levels of institutionalisation (Belli & Jiang, 2024).

Conceptual Model

The study puts forward a conceptual framework which seeks to combine data sovereignty, domestic regulatory design, and digital trade openness, based on some constructs from theory proposed by Bignami (2020), Zuboff (2019), and Kuner (2021). Fundamentally, it places sovereignty on data at the hub of its theory, with sovereignty being used to regulate strategic thinking on assertion in practice in regard to vise data produced in national territories. Notably, sovereignty in practice extends beyond territorial claims to be more of a prevailing concept used for regulating data flow, infrastructures for data, or entities finding their way into data processing or transfer. On its critique of surveillance capitalism, it proposes that sovereignty claims are in essence postured in response to the pervasive presence in markets now from those technology companies acting on their markets, which have no constraints in their drive for data flow, basically living in an ‘open world’ (Zuboff, 2019). These entities, in essence, create disparities in their regulated environment, with sovereignty, in essence, being more about constructing ‘regulated worlds.’ It follows from such a view that sovereignty-based regulation assumes different forms, such as those focused on privacy in Europe, security in China, market-based in the United States, or, for example, in Africa, with a view to balancing development, security, or rights. By such a model, national regulation patterns form the second tier in analysis. Such patterns establish substantive regulations on collecting, processing, storing, and transferring data across national borders (Akpanke et.al.,2022).

By contrast, market regulatory patterns encourage free flow to facilitate innovation in new markets. By way of addressing the third dimension, digital trade openness is defined in relation to these policy choices. If national regulations support extensive cross-border data flows, there is openness in digital trade rules, which in turn supports cloud computing, e-commerce, and cross-border platform transactions. More so, the model thereby introduces logical steps, whereby data sovereignty serves as the primary motivator, while national frameworks interpret sovereignty into actionable principles, with these principles again affecting levels of overall digital trade openness (Bignami, 2020).



X-axis: *Regions (EU, US, China, Africa)*
Y-axis: *Relative emphasis (scale 1–5)*
Bars:
Blue: *Data Sovereignty*
Green: *Domestic Regulatory Design*
Orange: *Digital Trade Openness*
Interpretation:

The EU *emphasises sovereignty and regulation but restricts trade openness.*
The US *prioritises trade openness over sovereignty.*
China *strongly emphasises sovereignty and regulation, limiting openness.*
Africa *adopts a hybrid approach with moderate scores across all dimensions.*

Data Sovereignty (Drivers)	Domestic Regulatory Design (Mechanisms)	Digital Trade Openness (Outcomes)
EU: Privacy-centric, rights-based governance	GDPR, Data Act, Cloud de Confiance	Restrictive transfers, adequacy requirements
US: Market-oriented, innovation-driven	CCPA, CPRA, FTC enforcement	Liberal data flows, trade agreements
China: Security-driven, state-centric	PIPL, DSL, CAC enforcement	Highly restrictive, localization mandates
Africa: Hybrid, development + sovereignty	Kenya DPA, POPIA, AfCFTA Protocol	Variable openness, harmonization efforts

Structure of the Table
Column 1 (Blue): *Data Sovereignty – Drivers and normative anchors*
Column 2 (Green): *Domestic Regulatory Design – Key mechanisms and examples*
Column 3 (Orange): *Digital Trade Openness – Resulting outcomes*
Rows include comparative examples:

EU: *Privacy-centric governance → GDPR, Data Act → Restrictive transfers*
US: *Market-oriented approach → CCPA, FTC enforcement → Liberal data flows*
China: *Security-driven sovereignty → PIPL, DSL → Localization mandates*
Africa: *Hybrid model → Kenya DPA, POPIA, AfCFTA → Variable openness*

 https://doi.org/10.59568/IJEBM-2025-2-1-01 Website: https://ijebm.kiu.ac.ug

The Legal Framework in the European Union

The digital governance policy of the EU is viewed as one of the most extensive, ambitious, and regulatory frameworks of its kind in the world. It is grounded in the vision for the establishment of the Digital Single Market, which aims for coordination in regulations on data in all its member states in creating an economic space in which data, services, and innovation move with no friction in between (European Commission, 2024). More than any other project for economic integration, the Digital Single Market encapsulates a constitutional vision which balances market rationality with primary individual rights. More specifically, in contrast to other participants in world affairs, EU policy on data regulation is based on its goal to uphold primary values like dignity, autonomy, and responsibility to democratic institutions, rather than in any other way treating information like any other commodity, based on liberty (Bignami, 2020).

This underlying philosophy is operationalised in a 'thick' network, or 'matte', of legal rules. The GDPR, adopted in 2016, is the 'cornerstone' of EU internet policy. It established common rules for data protection, enhanced individual rights, and extraterritorial obligations on any non-EU company processing 'European' data (Kuner, 2021). On its foundation, the Digital Services Act (DSA) and Digital Markets Act were adopted in 2022 to cope with systemic risks caused by 'dominant operators.' These acts are aimed at 'rebalancing the digital economy.' They lay down 'obligations on 'gatekeeper" companies, including transparency on algorithmic decision-making, while banning anti-competitive practices. The Data Act, adopted in 2024, marks the next milestone in the evolution. It regulates now not only 'personal data, but indeed 'industrial, 'non-personal 'datasets.' It enforces interoperability, 'fairness in data 'access, while protecting 'stability in data from 'foreign 'government intervention. It 'fosters 'strategic 'autonomy.' "This reflects efforts to strengthen 'Europe's strategic autonomy in 'times 'of 'geopolitical risk.

Notably, these tools are based on the constitutional foundations of privacy and data protection, recognising these as substantial rights in Articles 7-8 of its Charter on Fundamental Rights. These foundations make the EU's policy practice unique in its nature, even as data is viewed as an expansion of an individual's entity, requiring secured treatment from all quarters: governments, institutions, or market players (Wolff, Adeyemi, & Singh, 2025). It therefore follows that E.U, more often than not, stands by its rights-based governance frameworks, no matter how such agreements generate tensions between these principles, especially on economic grounds.

Legal Framework in the United States

The United States follows what could be called a 'regulatory philosophy,' which contrasts vastly with what is occurring in Europe with its 'rights-based model.' Rather than being based on constitutional Hanlon's Razor principles or 'full-scale laws,' the U.S. model remains 'market-driven, emphasising innovation, speed, and avoidance of governmental intervention' (Fratini et.al., 2024). It is based on the assumption that 'regulatory flexibility is conducive to success in the online market, such that industry must be allowed to regulate itself in ways that are responsive to new technology.' Interestingly, no overarching federal law regarding data protection has ever existed in the U.S., not like the GDPR in the EU, due to its 'sectoral, piecemeal, and reactive body of law.' These laws cover data issues in several areas, such as healthcare (Agboti et.al. 2024), finance or child data (Gu, 2023).

Characterised by a patchwork of federal laws, the Clarifying Lawful Overseas Use of Data (CLOUD) Act, passed in 2018, specifically defines the American concern with law enforcement's use of digital evidence in general. These laws require tech companies to cooperate with lawful data requests, even if such information is stored in other countries, while creating mechanisms to secure data for foreign governments in given circumstances. These laws demonstrate a utilitarian concern with national security, not with

harmonisation on data privacy (Financial Times, 2025).

On data trade, the United States–Mexico–Canada Agreement (USMCA) shows U.S. support for an open digital market. Its e-data section bans data localisation, ensures international data flows, and bans any action likely to slow digital trade (Wolff, Adeyemi, & Singh, 2025). These features support the American notion of data flow as a foundation for competitiveness and innovation in the economy. On institutional frameworks, while there is no specifically designated national data-protection authority, the consumer-protection agency Federal Trade Commission (FTC) functions as its quasi-national counterpart, using its consumer-protection mandate to deal with unfair or deceptive conduct in data management (Kuner, 2021).

More specifically, in recent years, there has been observed a dynamic shift in regulation from federal to state levels has been observed, with California being at the forefront of these changes. Born out of the California Consumer Privacy Act in 2018, consumers have given legitimate consent to exercise their right to data access, deletion, and opt-out from data sales, which, after modifications from the California Privacy Rights Act, established the California Privacy Protection Agency, the first consumer data regulation agency in the United States (European Parliament, 2024). Other US states, like Virginia, Colorado, and Connecticut, have followed suit in passing their own laws concerning consumer data with varying obligations for companies (Gu, 2023).

It is trite to mention here that, in the post-Big Tech world, American courts have a crucial role to play in regulating the internet. It is they, after all, who have defined, through their interpretations, what constitutes governmental surveillance, contractual obligations for privacy, and whatnot, yet, such as biometrics collection or algorithmic responsibility. Case law on the Fourth Amendment, in other words, remains in its evolving stages, what with American society's understanding regarding its level of privacy in cyberspace, whereas courtroom disputes about consumer contractual obligations, such as those for data portability, reveal how increasingly complex internet technology agreements have become (Kuner, 2021).

The Legal Framework in China

Cyber-governance environment in China rests on an entirely different ideological paradigm: cyber-sovereignty, whereby each country claims inviolable sovereignty over their cyber space, cyber infrastructures, and data resources (Cong, 2024). China's paradigm shifts from those followed in the U.S., in which market liberty is given paramount importance, or in Europe, in which data-protection ethics reign, to being oriented to national security, stability, and state sovereignty. Data, in China's paradigm, is not just an economic good to be strategically optimised for profit gain; it also constitutes an essential resource in national planning.

More so, the legal framework in China is characterised by three groundbreaking laws adopted in the course of the last ten years. The Cybersecurity Law, adopted in 2017, outlined general rules for network operators, defined rules for critical information infrastructure (CII), and required security reviews for technology used in critical industries. Also, on its soil, the Data Security Law, adopted in 2021, identified different types of data with varying levels of national security risks, setting up national frameworks for data management, storage, and cross-border flow. Finally, also in 2021, the Personal Information Protection Law, its first full-scale privacy law, set rules for data processors, secured some individuals' rights, and had extraterritorial applicability to foreign companies processing information on Chinese nationals (Financial Times, 2025).

The mechanisms for implementation are unique in their focus on data localisation and state regulation. "Important data" such as that with strategic value to its infrastructure, security, or large-scale individual data, must be physically hosted on territory controlled by China. "Important data" transferred

to countries overseas is mandatory for export security reviews by state entities to ascertain whether other countries could jeopardise strategic national security concerns (Cong, 2024). Notably, the "Cyberspace Administration of China" is tasked with national regulation, complete with powerful investigation powers, controlling platform regulations, algorithm regulation, and content regulation. China's complete institutional control facilitates its ability to meet strategic imperatives with impressive action speed in its comprehensive regulations, in stark contrast to its counterparts in America, Africa, with China's consistency emphasising its strengths in strategic digital regulation (Wolff, Adeyemi, Singh, 2025).

These strict controls have major implications for cross-border business (Antai et. al., 2024). Data localisation obligations, coupled with security assessments, create tensions with international best practices, which support unlimited cross-border flows, such as those outlined in the WTO e-commerce guidelines or in regional trade agreements such as CPTPP. Thus, from a critical theory point of view, the model in China embodies some underlying tensions with regard to the compatibility with innovation. On one side, the model in China strengthens cybersecurity, serves to facilitate industrial policy, and integrates national objectives with cyber regulation (Antai et. al., 2025). Contrarily, too restrictive regulation, in addition to uncertainties in its adoption, could hamper innovation via too much state regulation, deter high-value foreign investments, and hamper China's entrance into the world's cyber markets (Cong, 2024).

Comparative Analysis

Comparatively, it could be safely assumed that there are underlying philosophical differences in the data regulation posture adopted by the EU, US., or China, since these differences encapsulate underlying philosophical differences in what constitutes appropriate data concepts, regulation, and dissemination in an interconnected world. Indeed, while it could be safely assumed in some quarters, for example, about American, Chinese, or other philosophies on data regulation, in practice, these differences encapsulate several philosophical approaches to regulating and disseminating data in different ways, to different group outcomes, in different ways, depending on whether these platforms, policies, or frameworks align with their philosophical differences on regulating data in these different ways for these different purposes. The E.U., for example, follows what could be described in general philosophical principles, for example, generally speaking, in its adoption of its "rights-based" policy on regulating data, in its adoption of its view on "personal data protection, being deemed to constitute an inviolable human right, in particular, via its 'Charter of Fundamental Rights, Articles 7-8.'

It must be noted, further, that institutional frameworks accentuate these philosophical differences. The EU is known for its extremely legalistic, integrated institutional structure, in which its Data Protection Authorities are supervised by, and in closer coordination with, the European Data Protection Board. These institutions have major powers to investigate, penalise, with fines running into several billion euros, for violations, especially under GDPR (European Parliament, 2024). Secondly, America does not have a nationalised dedicated data/privacy protector. The Federal Trade Commission serves as its major enforcing authority, with judicial powers vested in it for consumer protection, while some sector-wise bodies, with increasing presence from state bodies, for example, the Privacy Protection Agency for California, share these powers (Gu, 2023).

Interestingly, the institutional setup in China diverges vastly from other major nations. Its Cyberspace Administration enjoys overall powers in cybersecurity, data security, and protecting information, with its meticulously integrated respective support from its provinces (Cong, 2024). Its concentrated institutional setup ensures swift policy implementation, aligning with China's 'sovereignty prime' stance.

Looking ahead, cross-border data flow mechanisms solidify this divide. The EU implements adequacy decisions, Standard Contractual Clauses (SCCs), and Binding Corporate Rules (BCRs) to guarantee that data transferred to any third country enjoys an 'essentially equivalent level' of protection (Case C-311/18, 2020). Contrarily, in the US, frictionless data flow is encouraged through its trade agreements like USMCA, banning any localisation obligations, assuring unconstrained data flows (Chander & Sun, 2023); in China, on the other hand, there are extreme localisation obligations for data flow to other countries, aligning with its security-first policy (Cong, 2024).

When compared with multilateral frameworks such as WTO rules, regional rules such as CPTPP, and other models, for example, the U.S. model, the U.S. model's ideal compatibility is with the liberal economic model, encouraging openness in these new markets with few constraints. The EU's model is partially compatible, especially in its regular conflicts with trade rules in its data flow restrictions, based on its concept of data flow rights, acting in essence as any other non-tariff barrier. China's model remains less ideal in these different settings, valuing sovereignty in place of openness in markets (Wolff, Adeyemi, & Singh, 2025). These differences have contributed to what is being called 'digital spheres or blocs' with different ecosystems having different assumptions on issues regarding privacy, security, and trade openness (Bignami, 2020).

A comparison matrix for these models shows their divergent strengths and weaknesses. The EU leads on protecting rights with its use of extraterritorial powers in the GDPR to set global benchmarks. But there's a weakness in being overly complex in governance bureaucracy, resulting in trade tensions with countries promoting open data flow (Kuner, 2021). On innovation, promotion, the U.S. leads, while its disadvantages include its lack of cohesion, consumer safeguards, and compatibility in cross-border data transfer. China, through its model, gets cohesion in its management with strategic alignment to national security, although its exposure could lead to slowed investments with growth in regional connectivity with the world's digital markets (Cong, 2024).

These rival models demonstrate the challenges inherent in coordinating digital regulation in the context of globalisation. These efforts to create interoperable rules via adequacy agreements, trade agreements, or multilateral settings face structural incompatibilities based on competing values. The consequence is that there is now a fragmented information age characterised by competing world views, with multiple governance visions. With increasing levels of digital trade, coupled with new technology such as artificial intelligence, there is likely to be mounting importance given to coordinating these rival models in shaping international law in the years to come (Wolff, Adeyemi, & Singh, 2025).

Challenges and Emerging Trends

The international environment for cyber regulation is in the process of being radically reshaped, being driven by increasing tensions in world geopolitics, changes in economic agendas, and innovation in information and communication technology. Among the most pressing issues in modern-day debates on cyber regulation is, in fact, precisely the increasing nexus between world geopolitics, on one hand, and regulation in cyberspace, on the other. Data flows, cyber infrastructure, platform networks, and other elements in cyberspace are no longer simply viewed or branded as market networks, now being perceived more in terms of strategic networks, which have ramifications for world economic sovereignty, security, and geopolitics (Belli & Jiang, 2024). It is, in particular, the escalating world rivalries, especially those between the United States on one side, China on the other, that have sparked off an increasing divergence in world cyber regulation, with its attendant different visions for internet regulation (Cong, 2024).

Along with these changes in world politics, there has also been increasing importance given to Artificial Intelligence (AI, governance, and data

ethics on the policy agendas (Kisubi, Aidonojie, & Antai, 2024). The increasing use of large-scale AI models, decision-making algorithms, and predictive analytics means that data governance consequences have moved on from concerns regarding security, privacy, etc., to broader concerns regarding bias, explainability, and responsibility (Zuboff, 2019). It is worth noting that the Artificial Intelligence Act of the EU is truly path-breaking in its efforts to regulate AI applications in their entirety from an overarching risk-based perspective, dividing applications into different categories on the basis of societal risk (European Parliament, 2024). Other countries, such as the United States, have adopted more pro-innovation policy initiatives, with an increased dependence on voluntary guidelines, industry regulation, etc., instead of regulation on prescriptive lines (Gu, 2023).

Another new development is the rising prominence of the Global South in discussions on global digital governance. Many developing countries in Africa, Latin America, and South Asia have begun to make their voices heard on the underlying inequalities inherent in prevailing architectures for cross-border data flows, pointing out that these patterns primarily end up benefiting economies that are major technology exporters while hampering 'developmental sovereignty' in other, less powerful countries (Belli & Jiang, 2024).

Digital decolonisation encapsulates these imperatives. It seeks to have digital governance architectures establish more equitable value dynamics by promoting homegrown information and communication technology industries in these countries while lessening their dependence on foray-based internet platforms based in other countries, for example, China, India, or the United States (Ogu etal, 2025). Many such countries are now attempting to establish their own data regulations, bolster their cybersecurity capacity, or engage in regional cooperation to gain more mastery over their respective information environments (Antai, 2024).

Another major paradigm in managing digital governance is regional cooperation (Antai, 2024). International bodies like ASEAN, the African Union, and the Council of Europe are now testing ways in which regions could work together on data security, regional markets in digital, and interoperability across different regions. The African Union's Cybersecurity and Personal Data Protection Treaty, ASEAN's Framework on Digital Data Governance, or Latin American regional initiatives are some evidence of growing regional faith in regionally-led visions that reconcile sovereignty, connectivity, and cyber governance imperatives (Wolff, Adeyemi, & Singh, 2025). These regional initiatives could be testing grounds for any new multilateral rules, providing viable routes to balancing competing visions in cybersecurity, such as visions based on rights, markets, or sovereignty, to create an interoperable world, thereby addressing any likely systemic fragmentation in global regulation at present.

Recommendations

Evidence from increasing disparities in digital governance frameworks bears out the unequivocal need for integrated, harmonised, and balanced frameworks for global data governance. Multilateral frameworks include initiatives to reformulate a Global Framework, which could reconcile principles for trade with new realities in the Digital Era. Debates in sessions on e-commerce in the World Trade Organisation's agendas, together with UNCTAD initiatives for inclusive development in information and communication technology, lay down the groundwork for such initiatives, highlighting elements like transparency, fairness, and integration of views from developing countries (Kuner, 2021).

Another suggestion is to fill the transatlantic and transpacific gaps, which increasingly pose genuine obstacles to interoperability on a global level. By cultivating common underlying principles in transborder trust, such things as common risk evaluation benchmarks, due process for governmental data-access clauses, or home-

country minimum safeguards for data privacy could alleviate tensions between these vastly divergent approaches. Using guidelines in the OECD, G7's Data Free Flow with Trust DFFT agreements, or new bilateral initiatives, policy-makers could create something approaching a modular-pluralistic task environment for cross-border electronic commerce (European Parliament, 2024).

On the national level, countries must implement changes to support balanced data sovereignty, to ensure national decision-making on regulation does not harm economic engagement. These changes must emphasise openness in national data access, compatibility in technology, administrative, and other areas, and mechanisms to guarantee no abuse by governments or corporations. Decision-makers must understand that balanced data sovereignty is not an openness/control divide; instead, it encompasses managing dependence in such a manner to facilitate support for national agendas while being active participants in the international digital economy (Bignami, 2020).

Conclusion

It has become apparent in this analysis that there are vastly different philosophical models in each region about E.U, the U.S, Africa, and China's respective frameworks on digital trade and data sovereignty, resulting in varying architectures for regulating these issues, in each respective region, in ways which inevitably affect varying levels of openness on these regions' respective markets for digital trade. Whereas in E.U, there is a 'rights-based model', whereby 'personal data protection concerns have become a constitutional issue, with 'privacy being woven into the fabric of its digital society'. Conversely to E.U's 'rights-based model', in 'U.S, 'there's a market-centered vision, with innovation, freedom to operate, and industry regulation taking priority, in what's fundamentally 'a conviction in markets, in self-regulation, in small governments', whereas in China, there's 'sovereignty-centered vision, whereby 'digital data policy is embedded in China's national security, 'concealing data to 'building blocks to China's national security resilience'.

The normative contribution of this research, therefore, is to draw attention to the burning need for hybrid forms of regulation to reconcile state sovereignty with global connectivity. It is not sufficient to regulate data economies in today's world, which is marked by state rivalries, state-of-the-art innovation, and new claims to digital equity, to use any individual model of regulation. Rather, there is now a pressing need for a pluralistic, interoperable, and inclusive philosophy for regulating data to guarantee that the world's data economy turns out to be interoperable, secure, and full of respect for all those with whom countries choose to link in their quest for enhanced global connectivity.

The report also points out areas for further research into the future. With increasing interoperability between artificial intelligence and digital trade, many new issues have come to the fore regarding algorithmic responsibility, international AI regulation, and managing high-risk AI applications. Future innovations such as quantum computing will also undermine prevailing security models, including their capacity for resisting encryption attacks, while being able to manage critical infrastructure is becoming an increasing concern for states. Another equally pressing concern is the evolving concept of digital diplomacy, which will have an important role in shaping international state approaches to negotiating new rules for operating in a post-West world order.

It is therefore apt to conclude that the future of digital governance hangs in the balance, pending efforts to achieve appropriate frameworks, which not only support sovereignty, innovation but also provide for the promotion of rights. It is hoped that success in creating frameworks for interoperable, ethical, and appropriate governance architectures could provide a foundation for creating a world order which not only remains dynamic in its economies but also has appropriate ethical

foundations, committed to principles such as dignity, democratic values, and cooperation.

References

1) African Union. (2023). *Protocol on Digital Trade under the AfCFTA Agreement*. Retrieved from https://au.int/en/treaties/protocol-digital-trade
2) Agboti, C. I., Ogbuke, M. U., Ugwu, I. P., Antai, G O., John, D. J., & Igwe, I. (2024). The Legal Framework for Occupational Health and Safety in the Manufacturing Sector: Assessing Compliance and Enforcement Mechanisms in Nigeria. *Pakistan Journal of Criminology 16 (4):* 1451-1463
3) Aidonojie, P. A, Aidonojie, E. C, Antai, G. O, Ekpenisi, C., & Ayuba, D (2025). Constitutional and Legislative Frameworks for Green and Sustainable Environmental Governance in Uganda. *International Journal of Constitutional and Administrative Law*. 1(1): 1-20
4) Akpanke, S. A, Antai, G. O, Iheanacho, L, & Aboh, P. B. (2022). Credit, Securities and Consumer Credit in Nigeria: Impacts, Challenges and Prospects. *The Calabar Law Journal*, 18(1), 1-16.
5) Andrade, T. N. de, Gobbi, M. C., Silva, T. C. da, Holouka, G., Leopoldino, I. M., Barbosa, L. A., … Gandara, F. M. B. (2025). Cybersecurity in the digital era: Geopolitical impacts and structural challenges. *IOSR Journal of Humanities and Social Science*, 30(1), 30–44. https://www.iosrjournals.org/iosr-jhss/papers/Vol.30-Issue1/Ser-6/E3001063044.pdf
6) Antai, G. O, Aidonojie, P. A, Mukhlis, M. M, Maskun, Tajuddin, M. S, & Andi, T. Y (2024). The Crisis in Red Sea Region: Legal and Socio-Economic Impact on International Commerce. *Al-RisalahForum Kajian Hukum dan Sosial Kemasyarakatan* 24 (2): 17-35 https://www.researchgate.net/publication/387947844_The_Crisis_in_Red_Sea_Region_Legal_and_Socio-Economic_Impact_on_International_Commerce
7) Antai, G. O, Iheanacho, L, Ogu, L, Beinomugisha, A., & Okpong, D. E. (2024). Voyage to Taxing Religious Organizations in Nigeria and blocking leakages in the Nigerian Economy: Legal Framework and Matters Arising. *KIU Interdisciplinary Journal of Humanities and Social Sciences*. 5 (2): 17-28
8) Antai, G. O, Obisesan, O. O, Umo, M. E, Hassan, I, & Okpong, D. E (2025). Press Freedom and National Security: The Place of Human Rights in Nigeria's Cybercrime Laws. *NIU Journal of Social Science 11* (1), 301-313
9) Antai, G. O, Obisesan, O. O, Umo, M. E, Okonji, C. I & Okpong, D. E (2025). Analyses of the Applicability of International Arbitration in Investor-State Dispute Settlement in East Africa. *NIU Journal of Humanities* 10 (1), 249-259
10) Antai, G. O. (2024). An Appraisal of the Historical Development of the African Response to Extradition. *Newport International Journal of Current Research in Humanities and Social Sciences*, 4(3). 27-35. Retrieved from <https://doi.org/10.59298/NIJCRHSS/2024/4.3.2735>.
11) Antai, G. O. (2024). Methods of Judicial Cooperation and the Procedure for Enforcement under International Law; Identifying the Nexus between Theory and Practice. *Newport International Journal of Current Research in Humanities and Social Sciences*, 4(3), 80-88. Retrieved from <https://doi.org/10.59298/NIJCRHSS/2024/4.3.8088>.
12) Antai, G.O. (2024). Appraisal of the Legality of the Laws Establishing Faith-based Government Agencies in Nigeria. *IDOSR Journal of Arts and Management* 9(1) 32-42. Retrieved from <https://doi.org/10.59298/IDOSRJAM/2024/9.1.324289>.

13) Belli, L., & Jiang, M. (2024). Comparative perspectives on data governance: Functionalism and institutional design in the digital age. *Journal of Digital Policy & Regulation, 6*(1), 45–67.
14) **Bignami, F.** (2020). *Comparative law and regulation of data privacy: Sovereignty and governance in the digital age*. *International Journal of Constitutional Law*, 18(2), 356–389. https://doi.org/10.1093/icon/moaa012
15) Bignami, F. (2020). Comparative law and regulation of data privacy: Sovereignty and governance in the digital age. *International Journal of Constitutional Law, 18*(2), 356–389. https://doi.org/10.1093/icon/moaa012
16) Bradford, A. (2020). *The Brussels Effect: How the European Union rules the world*. Oxford University Press.
17) Centre for Cybersecurity Policy. (2023, November 30). *Unravelling the impact of USTR's WTO reversal on cybersecurity and global trade*. https://www.centerforcybersecuritypolicy.org/insights-and-research/unraveling-the-impact-of-ustrs-wto-reversal-on-cybersecurity-and-global-trade/
18) Centre for International Governance Innovation. (2023). *Mitigating global fragmentation in digital trade governance: A case study* (CIGI Paper No. 270). https://www.cigionline.org/documents/2250/no.270_EvKNvNN.pdf
19) Chander, A., & Lê, U. P. (2015). Data nationalism. *Emory Law Journal, 64*(3), 677–739
20) Chander, A., & Sun, H. (2023). Privacy and data governance in the United States: Fragmentation and flexibility. *California Law Review, 111*(4), 987–1023.
21) Chetan P. (2025). Convergence and fragmentation in tech-trade governance: Global mechanisms across WTO tracks, digital trade agreements, export controls, and plurilateral data frameworks. *International Research Journal of Modern Engineering and Technology Sciences, 7*(9)
22) Clifford Chance. (2024). *The EU AI Act: Overview of key rules and requirements*. Retrieved from https://www.cliffordchance.com/content/dam/cliffordchance/PDFDocuments/the-eu-ai-act-overview.pdf
23) Cong, Y. (2024). Cyber-sovereignty and China's data governance regime: PIPL and DSL in context. *Journal of Chinese Law and Policy, 12*(2), 55–78.
24) Court of Justice of the European Union. (2015). *Maximillian Schrems v Data Protection Commissioner* (Case C-362/14). ECLI:EU:C:2015:650.
25) Court of Justice of the European Union. (2020). *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* (Case C-311/18). ECLI:EU:C:2020:559.
26) Creemers, R. (2022). Cybersecurity and data governance in China: National security and global implications. *Journal of Cyber Policy, 7*(1), 1–20. https://doi.org/10.1080/23738871.2022.2034567
27) Croxton, D. (1999). The Peace of Westphalia of 1648 and the origins of sovereignty. *International History Review, 21*(3), 569–852.
28) Data Protection Act, 2012 (Act 843) (Ghana). (2012). *An Act to establish a Data Protection Commission and to regulate the processing of personal data*. Accra: Government of Ghana. Retrieved from https://www.dataprotection.org.gh
29) Data Protection Act, 2017 (Mauritius). (2017). *An Act to provide for the protection of the privacy rights of individuals in relation to personal data processing and to establish the Data Protection Office*. Government of Mauritius. Retrieved from https://dataprotection.govmu.org
30) David, R., & Brierley, J. E. C. (1985). *Major legal systems in the world today: An introduction to the comparative study of law* (3rd ed.). London: Stevens & Sons.

31) DeNardis, L. (2014). *The global war for Internet governance*. Yale University Press.
32) Ebers, M. (2024). Truly risk-based regulation of artificial intelligence: How to implement the EU's AI Act. *European Journal of Risk Regulation, 16*(2), 684–703. https://doi.org/10.1017/err.2024.78
33) Edet, J. E., Antai, G. O., & Itafu, O. O. (2022). Sovereign Immunity from Legal and Arbitral Proceedings and Execution against the Assets of a Sovereign State: The Evolving Paradigm. *The Calabar Law Journal*, 18(1), 30-44.
34) Ekpenisi, C., Aidonojie, P. A., Antai, G. O., Akinsulore, A., Okonji, C., & John, D. J. (2024) Legal Issues Concerning the Role of Arbitration in Resolving Corporate Governance Dispute in Nigeria. *NIU Journal of Legal Studies*, 10(1), 5-14. Retrieve from <https://ijhumas.com/ojs/index.php/NIUJLS/article/view/1926>.
35) European Data Protection Board. (2024). *Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*. Retrieved from https://edpb.europa.eu
36) European Parliament. (2024). *Report on European cloud sovereignty and certification frameworks*. Brussels: European Union Publications Office.
37) European Parliament. (2024). *Report on European cloud sovereignty and certification frameworks*. Brussels: Publications Office of the European Union. Retrieved from https://www.europarl.europa.eu/
38) European Union. (2012). *Charter of Fundamental Rights of the European Union* (2012/C 326/02). Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
39) Financial Times. (2025, March 18). US privacy regulation ramps up as states lead the way. *Financial Times*. https://www.ft.com/
40) Floridi, L. (2022). The ethics of digital sovereignty. *Philosophy & Technology, 35*(4), 1–18. https://doi.org/10.1007/s13347-022-00549-9
41) Fratini, S., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). *Digital sovereignty: A descriptive analysis and a critical evaluation of existing models*. *Digital Society, 3*(3), Article 59. https://doi.org/10.1007/s44206-024-00146-7
42) Gorwa, R., & Garton, A. T. (2020). Democratic transparency in the platform society. *Social Media + Society, 6*(2), 1–12. https://doi.org/10.1177/2056305120924755
43) Greenleaf, G. (2021). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report, 170*, 2–6.
44) Gu, Y. (2023). Data adequacy and global trade: Reconciling EU data protection with WTO norms. *Journal of International Economic Law, 26*(1), 45–72. https://doi.org/10.1093/jiel/jlad003
45) Hall, P. A., & Taylor, R. C. R. (1996). Political science and the three new institutionalisms. *Political Studies, 44*(5), 936–957. https://doi.org/10.1111/j.1467-9248.1996.tb00343.x
46) International Chamber of Commerce. (2025). *Data flows.* Retrieved from https://iccwbo.org/global-insights/digital-economy/data-flows/
47) International Institute for Sustainable Development. (2022). *Harnessing Africa's digital economy for sustainable development*. IISD Report. Retrieved from https://www.iisd.org/articles/africa-digital-economy
48) **Kayeki, D.** (2025). *Analysing the challenges in enforcement of data protection laws in Uganda* (LLB dissertation). Uganda Christian University. https://scholar.ucu.ac.ug/.../download
49) Kisubi,E. C, Aidonojie, P. A & Antai G. O (2024). Harnessing Artificial Intelligence for Environmental Waste Management in Uganda: Legal and Policy Implications. *International Journal of Academic*

Multidisciplinary Research (IJAMR) 8 (10). 181-187

50) Krook, J., Winter, P., Downer, J. R., & Blockx, J. (2024). A systematic literature review of AI transparency laws in the EU and UK. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4976215

51) **Kuner, C.** (2021). *Data sovereignty and international data flows: The role of law and policy*. *International Data Privacy Law*, 11(3), 161–175. https://doi.org/10.1093/idpl/ipab014

52) Kuner, C. (2021). Reality and illusion in EU data transfer regulation post Schrems II. *International Data Privacy Law*, *11*(2), 103–118. https://doi.org/10.1093/idpl/ipab002

53) Liu, H. (2023). Data sovereignty and localization in China's digital economy: A legal perspective. *Asia Pacific Law Review*, *31*(2), 145–162. https://doi.org/10.1080/10192557.2023.1234567

54) Mueller, M. (2020). *Will the Internet fragment? Sovereignty, globalization and cyberspace*. Polity Press. Retrieved from https://www.politybooks.com/bookdetail/?isbn=9781509527131

55) Munga, J., Sang, D., & Sambuli, N. (2025). *Digital public infrastructure: A practical approach for Africa*. Carnegie Endowment for International Peace. Retrieved from https://carnegie-production-assets.s3.amazonaws.com/.../DPI%20in%20Africa-1.pdf

56) Musiani, F. (2021). Functionalism and the governance of digital infrastructures: A socio-technical perspective. *Internet Policy Review*, *10*(2), 1–15. https://doi.org/10.14763/2021.2.1550

57) Njoroge, J. W. (2024). Comparative analysis of AI governance in Africa relative to global standards and practices. *IOSR Journal of Computer Engineering*, *26*(5), 19–25. https://doi.org/10.9790/0661-2605031925

58) **Nwodo, F. A. N., & Amucheazi, C. O.** (2025). *Analysis of regulatory strategies to ensure the independence of Nigeria's Data Protection Commission*. *International Data Privacy Law*, 15(1), 91–100. https://doi.org/10.1093/idpl/ipae021

59) Ogu, L, Enyia, J. O., & Antai, G. O (2024). Rights and Challenges Impacting the Protective Framework for Financial Technology Consumers in Nigeria. *International Journal of Economics and Business Management IJEBM-KIU* l (1): 323-340.

60) Ogu, L, George, I. O, Antai, G. O, Hassan, I, & Ekpenisi, C. (2025). Comparative Analysis of the Legal and Policy Framework for Financial Technology in Nigeria and Selected Jurisdictions. *NIU Journal of Legal Studies* 11 (1) 115-128

61) Roper, G. (2025). *What is the Cyberspace Administration of China (CAC)?* Chinafy. https://www.chinafy.com/blog/what-is-the-cyberspace-administration-of-china-cac

62) Schwartz, P. M., & Solove, D. J. (2024). *The PII problem: Privacy and data protection in the United States*. *Harvard Law Review*, 137(2), 745–812.

63) Shettima, K. (2025, January). *Remarks on AfCFTA Digital Trade Protocol and intra-African trade targets*. Nigeria State House Report. Retrieved from https://statehouse.gov.ng/news/afcfta-digital-trade-protocol

64) U.S. Department of Commerce. (2025). *Data Privacy Framework program: Certified organisations list*. Retrieved from https://www.dataprivacyframework.gov

65) **Uwadinma, A. I.** (2025). Data privacy and consumer protection in Nigeria's digital economy: A legal examination of the Nigeria Data Protection Act, 2023. *AUN Journal of Law*, Admiralty University of Nigeria.

66) Wolff, L., Adeyemi, T., & Singh, R. (2025). Comparative institutionalism in digital trade governance: EU, U.S., and Africa. *Global Policy*, *16*(1), 112–129.

67) World Trade Organization. (2025, October 7). *Global Trade Outlook (Volume growth*

forecast) via CNBC https://www.cnbc.com/2025/10/07/wto-hikes-global-trade-forecast-for-2025-slowdown-expected-in-2026-.html

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